UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

METODOLOGÍA DE SEGURIDAD EN REDES DE COMPUTADORAS

TESIS

QUE PARA OBTENER EL TÍTULO DE:
INGENIERO MECÁNICO ELECTRICISTA
ÁREA ELÉCTRICA - ELECTRÓNICA

PRESENTA:
RICARDO JAVIER RAMÍREZ DÍAZ

DIRECTOR DE TESIS:
ING. ORLANDO ZALDÍVAR ZAMORATEGUI

CD. UNIVERSITARIA, DF, JUNIO 2006

DEDICATORIA

A los mejores padres que un hijo pudiera desear: Refugio (q.e.p.d.) y Amalia, por todos sus esfuerzos y sacrificios, gracias por su amor incondicional.

A mi esposa Lupita y a mi hijo Rodrigo, por creer en mí e impulsarme a ser una mejor persona, son mi fuente de inspiración.

A mis sobrinos Arturo (q.e.p.d.), Alejandro, Jesika, Carla, Víctor, Claudia, Guillermo y Mariana, porque son la esperanza de sus padres.

A toda mi familia, que son ejemplo del trabajo en equipo.

AGRADECIMIENTOS

A Dios, por todo lo que me ha dado a lo largo de mi vida.

A mis hermanos, Carlos, Gregorio y Laura, con los que he pasado momentos de inmensa alegría, así como de tristeza.

A mi abuelita Sixta (q.e.p.d.), a mis tíos Ana, Julio, Rita, Darío y Agustín, porque sé que siempre podré contar con ustedes.

A mis suegros, cuñadas y cuñados, por tener fe en mí.

A Alberto Dávila, por apoyarme en el desarrollo de este trabajo.

A Adrián Acuña, por concederme los permisos para realizar los trámites necesarios en el proceso de titulación.

A Orlando Zaldívar, por todo el tiempo dedicado en la revisión de este trabajo.

ÍNDICE

CAPÍTULO 1

INTRODUCCIÓN

Durante los últimos años el valor de la información se ha añadido a la valoración de los activos de una empresa, así como los objetos físicos útiles, las producciones, las infraestructuras, la tesorería y el capital humano que la constituyen. Es por este valor que se hace necesario el establecer medidas para protegerla.

La información en las empresas antes de la aparición de las computadoras se mantenía con el sistema de papel y archiveros y formaba parte de los activos de una oficina; ahora el valor de la información está dado, entre otros aspectos, por su accesibilidad (facilidad y velocidad con que la información se obtiene), precisión, adecuación, puntualidad, claridad, flexibilidad, auditabilidad, compresión, etc.

Hoy en día, la información se manipula en grandes cantidades y puede provenir de lugares distintos, la diferencia entre una empresa y otra del mismo tipo puede ser cómo manejan la información. Los riesgos a los que está expuesta la información cada día son mayores, por lo que es muy importante reducir el impacto económico que causaría su alteración o pérdida y de esta forma mantenerla segura.

Las amenazas a la seguridad informática son mayores cada día, y el número de ataques a todo tipo de organizaciones crece año con año, como lo muestran las estadísticas y las encuestas en seguridad que se realizan por diversas organizaciones a nivel mundial, la sofisticación de los programas llamados malware también se ha incrementado produciendo daños cada vez más serios, la publicación gratuita de cómo ser un hacker y herramientas para efectuar ataques, así como la creación de virus es de fácil acceso a través de Internet, como lo es también la publicación de varios libros con el título de hackers que incluyen además cd’s con las herramientas tratadas en los textos.

La protección de la información es más difícil desde la aparición de las redes de computadoras. Estas redes y especialmente Internet hacen que la información sea un problema global y no aislado a las máquinas internas de la empresa. Las tecnologías aplicadas a la seguridad en redes están en constante desarrollo, especialmente porque no existen estándares ni organizaciones aceptadas por todas las empresas proveedoras de seguridad.

Al diseñar un sistema de seguridad para la empresa para la cual se trabaje, se deberá implantar un sistema que guarde un equilibrio correspondiente entre seguridad y facilidad de uso.

En la práctica siempre existe una relación entre el nivel de seguridad, los costos y el entorno del usuario, teniendo en cuenta que la seguridad es proporcional al costo de las medidas de protección y que la misma es opuesta a los sistemas abiertos que pretenden facilitar el acceso a cualquier usuario, con o sin preparación.

Por lo tanto, la instalación de la seguridad es un problema de ingeniería, un compromiso entre gastos y facilidad de uso frente a protección, resaltando su aplicación de manera general, sin importar el tipo o tamaño de una empresa.

Para proteger la información y lograr cierto grado de seguridad se debe planificar y efectuar diversos servicios de seguridad, tales como definir políticas, efectuar análisis de riesgos, realizar análisis de las medidas de protección, instalación de las medidas adecuadas, mantener un monitoreo continuo para verificar que las medidas implantadas están dando resultados satisfactorios y elaborar planes de contingencia.

El concepto de seguridad en la información va más allá de la simple protección de los datos en el ámbito lógico. Para proporcionar una seguridad más completa, se deben tener en cuenta varios factores, tanto internos como externos y así clasificar los tipos de seguridad en: seguridad física, seguridad de la información, seguridad del canal de comunicación, problemas de autenticación, problemas de suplantación, etc.

Por otro lado, la rápida expansión y popularización de Internet ha convertido a la seguridad en redes en uno de los temas más importantes dentro de la informática moderna. Con tal nivel de interconexión, los virus y los hackers actúan con toda confianza en los equipos de cómputo, aprovechando las deficientes medidas de seguridad tomadas por administradores y usuarios.

Las ventajas de las redes de computadoras al compartir recursos son evidentes, pero muchas veces sólo consideran los riesgos más obvios, y no toman en cuenta otras circunstancias que a menudo ponen en peligro la seguridad de los sistemas. Como ejemplo, se tiene la falla en el suministro de energía eléctrica, así como también el que los respaldos de información no se efectúen de manera correcta. En pocos años, la gran mayoría de las empresas operarán de manera segura a través de la red, gracias a todas las normas que se están dictando y son de obligado cumplimiento, pero esto sólo será posible si los expertos aportan soluciones que garanticen la seguridad de la información.

La informática se considera como la ciencia del tratamiento automático de la información, la cual tiene un tiempo de vida cada vez menor y la rapidez con la que viaja es algo crucial, es por ello que es muy importante cuidar la capacidad para poder transmitirla de forma segura y eficiente, tal vez aún más que su procesamiento y almacenamiento. Los últimos avances en compresión y transmisión de datos digitales, permiten hoy por hoy transferir cantidades enormes de información a velocidades que hace tan sólo unos años eran impensables. En este sentido, las redes de computadoras desempeñan un papel fundamental en la informática moderna.

Hay que tener en cuenta que la complejidad de las redes y su carácter público convierten la protección física de los canales de comunicación en algo sumamente difícil. Uno de los mayores obstáculos que ha tenido que superarse para que las redes puedan desarrollarse, ha sido encontrar lenguajes comunes para que computadoras de diferentes marcas y tipos logren entenderse, en este sentido, el protocolo TCP/IP se ha elegido como estándar de facto en la industria de la informática. En general, todas las redes de computadoras se construyen conceptualmente sobre diferentes capas de abstracción que desarrollan tareas distintas y proporcionan un protocolo unificado a las capas superiores.

En función del tipo de red, con el que se trabaje, las redes de computadoras, se enfrentan a diferentes clases de riesgos, lo cual conduce a tomar medidas de diferente naturaleza para garantizar la seguridad en las comunicaciones.

1.1. Definiciones de seguridad informática

La ISO 17799 la define como la conservación de los principios básicos de seguridad que son la confidencialidad, la integridad y la disponibilidad de la información, como esquemáticamente se muestra en la Figura 1.1.

La norma ISO 17799 es una recopilación de recomendaciones para las prácticas exitosas de seguridad, que toda organización puede aplicar, independientemente de su tamaño o sector y que han demostrado su utilidad práctica en la industria.

ISO 17799 indica que los principios básicos de seguridad, son los principios que rigen todos los demás, y se basan en las características de confidencialidad, integridad y disponibilidad que se deben mantener en la información corporativa.

La International Information Systems Security Certification Consortium $(ISC)^2$ define a la seguridad informática, como la protección de los sistemas computacionales, contra las amenazas a la confidencialidad, integridad y disponibilidad. También menciona que es un campo de estudio, una meta a lograr y una serie de actividades dirigidas para alcanzar ese objetivo.

Internet Security Systems la define como el conjunto de políticas, técnicas, procedimientos, mecanismos, etc., para proteger la información almacenada e intercambiada contra ataques de todo tipo.

Una definición más completa y en la que este trabajo se estará basando para efectuar un análisis y administración de riesgos más completo, lo cual llevará por lo tanto tener una red más segura, es la siguiente:

Conjunto de medidas administrativas, organizativas, físicas, técnicas, legales y educativas, dirigidas a prevenir, detectar y responder a acciones que pongan en riesgo la confidencialidad, integridad y disponibilidad de la información de cualquier organización.

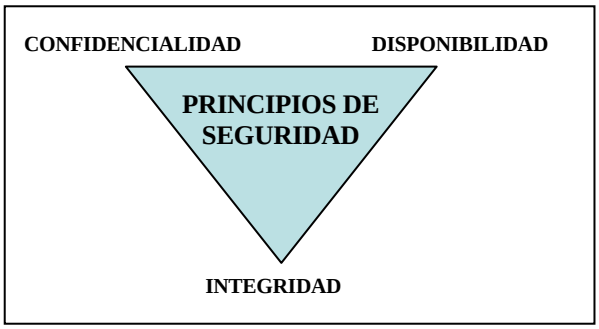


Figura 1.1 Confidencialidad, integridad y disponibilidad

Es conveniente establecer las definiciones referentes a las propiedades de la información para saber a qué amenazas están expuestas y de esta forma implementar los controles necesarios para minimizar los riesgos.

1.1.1. Confidencialidad

La ISO 7498-2 la define como la propiedad de la información que impide que ésta sea revelada o esté disponible a individuos, entidades o procesos no autorizados.

ISO 7498 describe el modelo estándar de referencia OSI (Open Systems Interconnection), que permite la comunicación entre sistemas con diferentes equipos y sistemas abiertos, ante la expansión de las redes de distintos fabricantes y para facilitar la comunicación entre ellos.

Los peligros inherentes a esta propiedad son los accesos no autorizados o públicos a información catalogada como confidencial, ya sea por error, mala configuración o descuido, suplantación de usuarios, instalación de caballos de Troya, acceso físico a material restringido, acceso a servicios confidenciales como correo, servidores de acceso, bases de datos, etc.

1.1.2. Integridad

La ISO 7498-2 la define como la propiedad de que los datos o la información no hayan sido modificados, alterados o borrados, de forma no autorizada.

Garantiza la exactitud de los activos de información contra alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.

Los peligros son borrado o modificación de datos, modificación en archivos de sistema, virus, destrucción o corrupción de respaldos, corrupción de bases de datos, etc.

1.1.3. Disponibilidad

La ISO 7498-2 la define como la propiedad que requiere que los recursos de un sistema abierto sean accesibles y utilizables a petición de una entidad autorizada.

Asegura que los recursos informáticos pueden ser utilizados en la forma y tiempo requeridos. Se refiere a su posible recuperación en casos de desastre.

Los peligros son la caída de servicios externos (DoS), agotamiento de recursos (ancho de banda, disco, sockets, etc.), sufrir una falla en las infraestructuras generales de red (ruteadores, switches), destrucción de configuraciones o servicios, acceso físico a infraestructura básica, sabotaje, etc.

La metodología de análisis de riesgos, desarrollada desde el Consejo Superior de Informática de España (Ministerio de Administraciones Públicas) y denominada MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas) la define como el grado en que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado.

Otra definición: situación que se produce cuando se puede acceder a un sistema de información en un periodo de tiempo considerado aceptable. La disponibilidad está asociada a la fiabilidad técnica de los componentes del sistema de información.

La información puede estar en proceso de transformación, almacenada, o en transmisión; para estos tres estados de la información se utilizan diferentes herramientas para protegerla.

La mejor forma de realizar la seguridad informática correctamente es disponer de la **gente** capacitada adecuadamente, para ejecutar los **procesos** correspondientes (previamente documentados) con las **tecnologías** apropiadas, Figura 1.2.

Esquemáticamente se tiene:

- Gente.
- Procesos.
- Tecnología.

1.1.4. Gente

- Por la habilidad, conciencia y productividad del personal para planear, adquirir, prestar servicios, dar soporte y monitorear los sistemas de información.
- Conocimientos, funciones y responsabilidades.
- Debe ser gente dedicada y estar en constante actualización.

1.1.5. Procesos

- Coherente y repetible.
- Planeado para la seguridad.
- Prevención.
- Detección.
- Reacción.

1.1.6. Tecnología

Incluye hardware y software básico, sistemas operativos, sistemas de administración, de base de datos, de redes, telecomunicaciones, multimedia, etc. Herramientas de seguridad y protección como firewalls, detectores de intrusos, programas antivirus, analizadores de vulnerabilidades, etc.

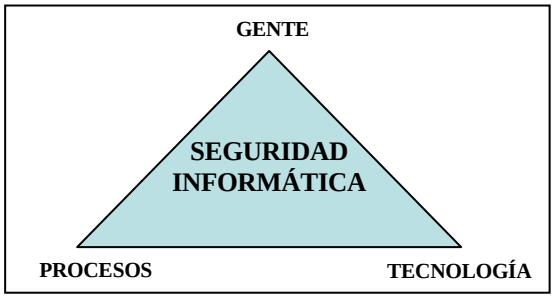


Figura 1.2 Gente, procesos y tecnología

De acuerdo a Gartner Group el porcentaje de interrupciones debido a procesos representa el 40%, a gente también el 40% y resultado de la tecnología sólo el 20%.

La seguridad informática no depende exclusivamente de tecnología; la instalación del mejor firewall y antivirus no garantiza que la información estará libre y a salvo de ataques, como han querido hacer creer algunas empresas que venden estos productos. No existe una “caja negra” que garantice un 100% de seguridad para la información.

Para tener una administración adecuada de seguridad informática, es necesario que gente, procesos y tecnología trabajen de manera conjunta ya que estos tres pilares son la base de una infraestructura de seguridad integral y completa.

Como no existe una solución universal para proteger una red, este trabajo se centrará en establecer los pasos necesarios para la implementación de una metodología de seguridad en redes de computadoras que sirva como base para establecer una correcta medida y forma de protección de la información en redes dentro de una organización, sin importar su tamaño ni su giro, tomando en cuenta estándares internacionales y las consideraciones necesarias para lograr este objetivo, la cual involucra como se acaba de ver a gente, procesos y tecnología; y de esta forma, preservar la confidencialidad, integridad y disponibilidad de la información, Figura 1.3.

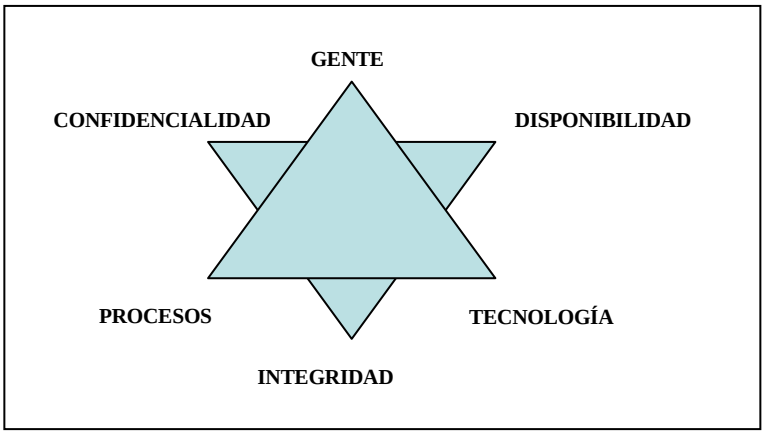


Figura 1.3 Seguridad informática involucra gente, procesos, tecnología, confidencialidad, integridad y disponibilidad

Para todos nosotros es muy claro que cuando salimos de casa cerramos con llave para evitar que gente extraña entre y robe, de acuerdo a lo que se tiene de valor dentro de las casas, algunas personas instalan en su perímetro rejas electrificadas donde el objetivo es, ahuyentar a delincuentes que pretendan ingresar al interior del hogar y lleven de esta forma la sustracción de objetos de valor.

Es común también la instalación de diferentes tipos de alarmas, las cuales activan una sirena en cuanto se interrumpe la continuidad en sus elementos, frecuentemente tienen además sensores que se activan al más ligero movimiento que se efectúe dentro de su campo de alcance.

De manera similar es que se instalen diferentes herramientas en la organización que garanticen un nivel de seguridad adecuado al riesgo que se intenta mitigar.

Las infracciones de seguridad en las organizaciones tienen efectos de gran repercusión y las afectan de diversas formas.

Los resultados de no tener implantadas medidas de seguridad efectivas son varias, incluyendo las siguientes:

- Pérdida de beneficios o ganancias de la organización.
- Perjuicio de la reputación de la organización.
- Pérdida o compromiso de la seguridad de los datos confidenciales.
- Interrupción de los procesos empresariales.
- Disminución de la confianza del cliente.
- Falta de la confianza del inversionista.

La aplicación de la metodología de seguridad en redes de computadoras aquí planteada garantiza llegar a un nivel apropiado de seguridad, la cual redundará en grandes beneficios para la organización que la lleve a la práctica; ya que es más económico implementar medidas de protección a la información que establecer acciones para recuperarla después de que ha sido dañada.

CAPÍTULO 2

SITUACIÓN ACTUAL

Es un hecho que la conciencia a nivel mundial está creciendo en lo que respecta a la seguridad informática, como lo demuestran las certificaciones que aplican a personas, tales como la CISSP (Certified Information System Security Professional), SSCP (System Security Certified Practitioner) avaladas por el Internacional Information Systems Security Certification Consortium (ISC)[2], CISA (Certified Information System Auditor), CISM (Certified Information Security Management) avaladas por ISACA (Information Systems Audit and Control Association), GIAC (Global Information Assurance Certification) avalada por el Instituto SANS (Sysadmin Audit Network Security), dentro de ésta se encuentran varias especializaciones CIDA (Certified Intrusion Detection Analyst), CAIH Certified Advanced Incident Handler, CFA Certified Firewall Analyst, CIX Certified Unix Security Analist, CNT Certified Windows NT Security Analyst, SEC Security Essentials Certified, Security + que quiere decir Security Certified Network Specialist avalada por CompTIA (Computing Technology Industry Association), entre otras.

En México existen asociaciones como la AMAI (Asociación Mexicana de Auditores en Informática) y la ALAPSI (Asociación Latinoamericana de Profesionales en Seguridad Informática), esta última creada en 1995; la primera agrupa, principalmente, a certificados CISA y la segunda a gente certificada CISSP.

Para obtener la certificación CISSP se debe aprobar un examen que consta de 250 preguntas, suministrado por (ISC)², contar con un mínimo de cuatro años de experiencia en áreas de seguridad y además contar con el respaldo y la recomendación de un profesional que obtuvo anteriormente la certificación CISSP.

Este examen dura aproximadamente seis horas y cubre diez áreas de conocimiento que se mencionan a continuación:

1. Metodología y sistemas de control de acceso.
2. Telecomunicaciones y seguridad en redes.
3. Prácticas de administración de seguridad.
4. Seguridad en desarrollo de sistemas y aplicaciones.
5. Criptografía.
6. Modelos y arquitectura de seguridad.
7. Seguridad en las operaciones.
8. Plan de continuidad de negocio y plan de recuperación en casos de desastre.
9. Leyes, investigación y ética.
10. Seguridad física.

Para obtener la certificación SSCP también se debe aprobar un examen, que incluye siete áreas de conocimiento:

1. Control de acceso.
2. Administración de la seguridad.
3. Auditoría y monitoreo.
4. Criptografía.
5. Comunicaciones de datos.
6. Código malicioso y malware.
7. Riesgo, respuesta y recuperación.

Para obtener la certificación CISA se debe aprobar un examen de 200 preguntas y contar con al menos cinco años de experiencia en la auditoría, control o seguridad en sistemas de información profesional.

Las áreas especiales de conocimiento en cuanto a la seguridad de un CISA son el cumplimiento y la auditoría de la tecnología de información (TI), la duración aproximada del examen es de cuatro horas y se basa en cinco áreas de conocimiento:

1. Estándares de auditoría de sistemas de información y prácticas de seguridad y control de sistemas de información.
2. Organización y administración de sistemas de información.
3. Proceso de sistemas de información.
4. Confidencialidad, integridad y disponibilidad de sistemas de información.
5. Desarrollo, adquisición y mantenimiento de sistemas de información.

La certificación CISM se centra exclusivamente en la administración de seguridad de la información. Los candidatos a la certificación CISM deben tener al menos cinco años de experiencia en aplicación de controles en seguridad de la información y un mínimo de tres años de experiencia en administración de seguridad de la información.

En lo que respecta a certificaciones en seguridad para empresas aplica la certificación en el estándar BS 7799-2.

Anualmente, Computer Security Institute (CSI), una organización formada por profesionales y empresas especializadas en seguridad informática, con la colaboración de la oficina de San Francisco del Federal Bureau of Investigation (FBI), realiza una encuesta a los responsables de seguridad informática de organizaciones en los Estados Unidos, publica los resultados y los pone a disposición de todos aquellos que quieran consultarlos, Figura 2.1.

Figura 2.1 Novena encuesta anual de seguridad y crímenes computacionales del CSI/FBI

A lo largo de los años, esta encuesta se ha mostrado como un fiel reflejo de las tendencias en la seguridad informática, tanto en las amenazas más importantes de cada momento, como en determinar los cambios de la percepción de la seguridad en las organizaciones.

Si bien el ámbito de la encuesta se ajusta a organizaciones de los Estados Unidos, debido al carácter global de las amenazas, prácticamente todos los datos se pueden extrapolar a organizaciones de otros países. En muchos casos, lo que se ve en las conclusiones de esta encuesta serán las tendencias que, dentro de varios meses, marcarán las empresas de otros países.

Otras encuestas dignas de mencionar son las efectuadas por la empresa consultora Ernest & Young y la realizada por el CERT (Computer Emergency Report Team) australiano.

Es recomendable que estas encuestas sean consultadas por todos los profesionales y organizaciones que se dediquen de una forma u otra a la seguridad informática.

Dentro de los datos obtenidos en la encuesta de 2004 resaltan los siguientes aspectos:

- El uso no autorizado de computadoras va a la baja respecto al año 2003.
- El impacto económico de las incidencias de seguridad también se ha reducido (141 millones de dólares, mientras que en la edición del año 2003 se estimaba en 201 millones de dólares).
- A diferencia de otros años, el delito informático que causa un mayor impacto económico consiste en los ataques de negación de servicio, como lo muestra la Figura 2.2.

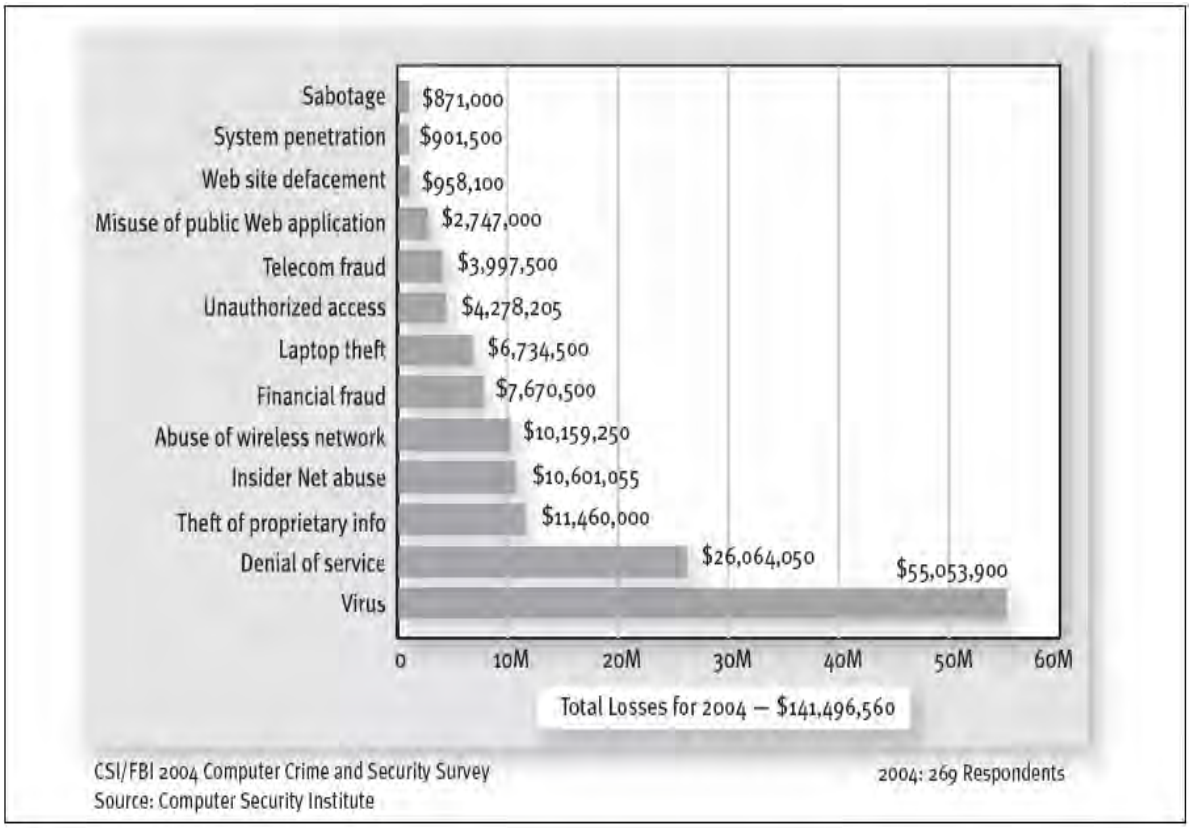


Figura 2.2 Estadísticas por tipo de ataque y monto de pérdidas en dólares

El número de organizaciones que denuncian ante la policía o los juzgados las incidencias de seguridad, también se ha reducido. La causa que se menciona es evitar la mala publicidad.

Se han generalizado la utilización de criterios económicos en la toma de decisión de adquisición de elementos de seguridad. Un 55% aplican criterios de cálculo del retorno de la inversión (ROI) y 25% calcula el valor neto presente (NPV).

Un 80% de las organizaciones realizan auditorías de seguridad.

Son muy raras las organizaciones que externan las actividades de seguridad y aquellas que lo hacen, el porcentaje de actividades externadas es muy bajo.

Para la mayoría de las organizaciones, la formación con objeto de crear una conciencia de seguridad es muy importante, pero casi todas reconocen que invierten poco.

Las pérdidas más graves y de mayor impacto económico eran de información propietaria.

Estas compañías parecían estar haciendo las cosas correctas en lo que respecta a la seguridad de información ya que el 99% de ellas usan software antivirus, el 98% usan firewalls y el 68% usan sistemas de detección de intrusos, Figura 2.3.

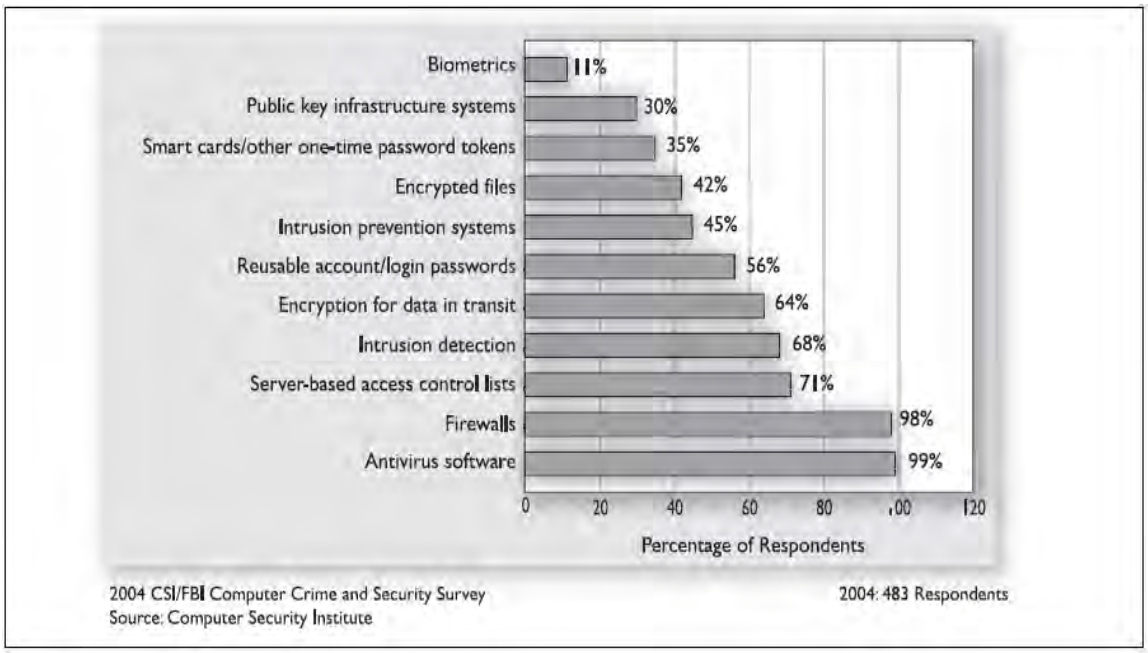


Figura 2.3 Tecnologías de seguridad utilizadas

El 59% descubrieron abuso en los privilegios del empleado para su acceso a Internet (por ejemplo, descargando pornografía o software pirata, o haciendo un mal uso de sistemas de correo electrónico), Figura 2.4.

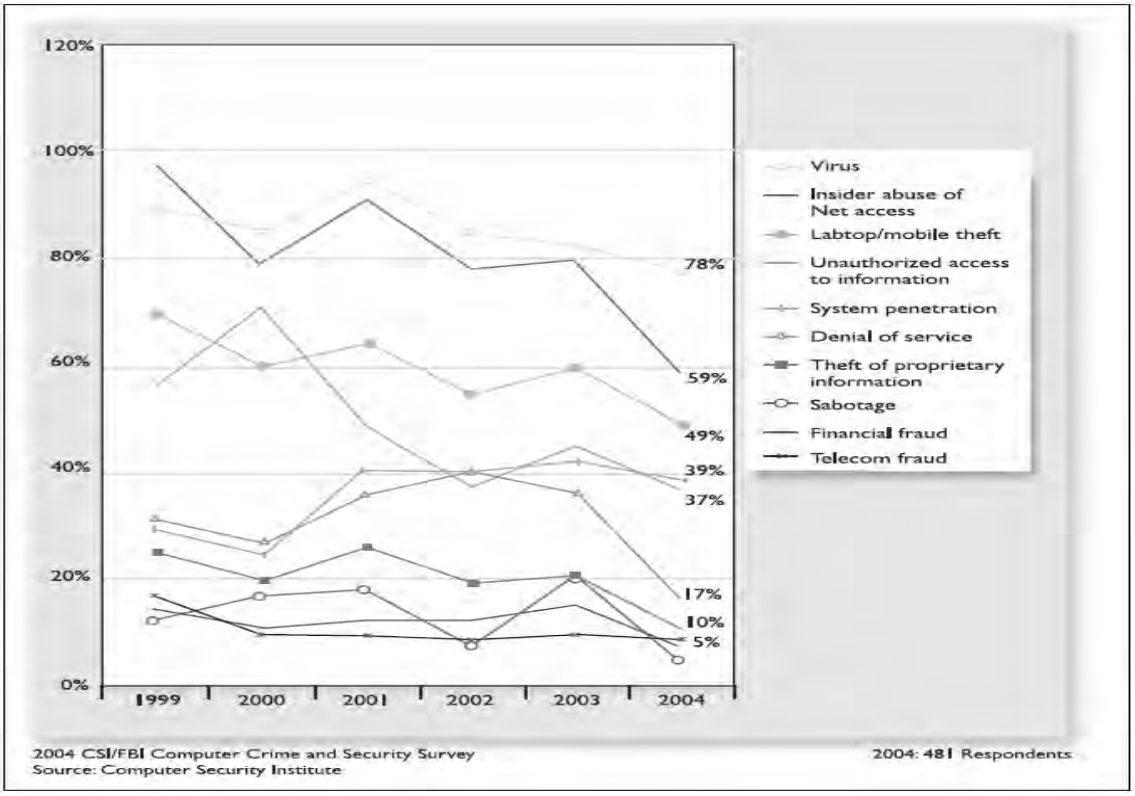


Figura 2.4 Tipos de ataque

Por séptimo año consecutivo, el porcentaje mayor de los encuestados (70%) citó su conexión de Internet como un punto frecuente de ataque, en contraste con sus sistemas interiores (66%), Figura 2.5.

Figure 12. How Many Incidents? From Outside? From Inside?

How Many Incidents? by percentage	1 – 5	6 – 10	>10	Don't Know
2004	47%	20%	12%	22%
2003	38%	20%	16%	26%
2002	42%	20%	15%	23%
2001	33%	24%	11%	31%
2000	33%	23%	13%	31%
1999	34%	22%	14%	29%
How Many Incidents From the Outside?	**1 – 5**	**6 – 10**	**>10**	**Don't Know**
2004	52%	9%	9%	30%
2003	46%	10%	13%	31%
2002	49%	14%	9%	27%
2001	41%	14%	7%	39%
2000	39%	11%	8%	42%
1999	43%	8%	9%	39%
How Many Incidents From the Inside?	**1 – 5**	**6 – 10**	**>10**	**Don't Know**
2004	52%	6%	8%	34%
2003	45%	11%	12%	33%
2002	42%	13%	9%	35%
2001	40%	12%	7%	41%
2000	38%	16%	9%	37%
1999	37%	16%	12%	35%

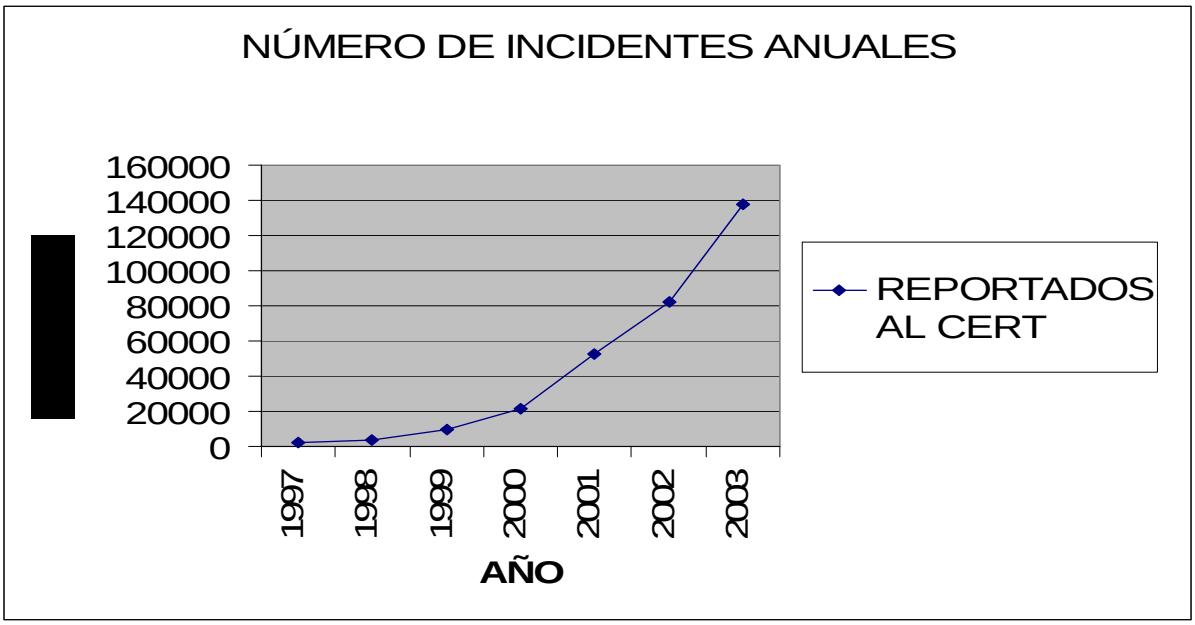
2004 CSI/FBI Computer Crime and Security Survey — 2004: 280 Respondents
Source: Computer Security Institute

Figura 2.5 Ataques internos y externos

Aunque también, la cultura y motivación para los crackers ha ido creciendo, simplemente tómese como muestra las convenciones anuales de hackers en Las Vegas llamada DEFCON, y la de Black Hat en Baltimore. A este tipo de personas se le llama hackers o piratas informáticos.

	1997	1998	1999	2000	2001	2002	2003	2004
Incidentes reportados	2,134	3,734	9,859	21,756	52,658	82,094	137,529	
Vulnerabilidades reportadas	311	262	417	1,090	2,437	4,129	3,784	3,780
E-mail procesados	39,626	41,871	34,612	56,365	118,907	204,841	542,754	717,863
CERT Consultoría, Vendor Notes y Notas de Vulnerabilidad	44	34	20	47	326	375	255	341

Tabla 2.1 Estadísticas de ataques reportados al CERT



Gráfica 2.1 Incidentes reportados

El CERT recibió en 2004, 3780 avisos de vulnerabilidades, aunque al contrario de años anteriores el organismo evita dar un número concreto de incidentes reportados dado el elevado número de éstos, indicando que debido al uso extendido de herramientas de ataque automatizadas no representa un indicador significativo, Tabla 2.1.

La revista CSO magazine en colaboración con el servicio secreto de los Estados Unidos y el CERT efectúan anualmente una encuesta sobre delito informático, y en el año 2003 estimaron las pérdidas en 666 millones de dólares.

Como lo muestra la gráfica 2.1, el daño está aumentando por lo que se refiere a los dos últimos años, en número de ataques y asegurando pérdidas financieras del 50 por ciento, año con año.

2.1. Historia de la seguridad de redes

Las primeras redes empresariales soportaron un poco más que compartir archivos e impresiones. Las Redes de Área Local (LANs Local Area Network,) empresariales de hoy ofrecen recursos para tareas críticas a un grupo de usuarios en constante crecimiento. Es por ello que la seguridad de las redes ha evolucionado de simples contraseñas a una estrategia en múltiples niveles que protege a toda la LAN.

La autenticación y el cifrado estuvieron entre las primeras tecnologías diseñadas para perfeccionar la transmisión de datos digitales de acceso no autorizado. La autenticación puede variar de simples certificados digitales a complejos esquemas de cifrado como PKI (Public Key Infrastructure). Estas tecnologías a nivel paquetes, desarrolladas a finales de los años 70's, necesitan un procesamiento intensivo de ciclos, que puede impactar el rendimiento de la red, la facilidad de su implementación y su escalabilidad. Dentro de los algoritmos actuales de seguridad se encuentran DES (Data Encryption Standard), TDES (Triple DES) y AES (Advanced Encryption Standard), que la organización de estándares de los Estados Unidos designó para reemplazar a DES.

Poco después de la introducción de las computadoras personales, a mediados de los años 80, se presentaron los primeros virus de computadoras, y más tarde el software antivirus. El objetivo de estas aplicaciones es el de monitorear y reparar los daños causados por virus, gusanos, caballos de Troya (conocidos así debido a que entran al sistema sin que se de cuenta el personal operativo) y otros códigos maliciosos. Desafortunadamente para las primeras víctimas, las actualizaciones de los programas antivirus salían después de que el virus había sido descubierto. Además, el software se instalaba en la computadora de escritorio y los usuarios lo podían desactivar.

A medida que las redes de área local se convirtieron en algo común a finales de los años 80 y la gente necesitaba acceso remoto a los recursos de las redes corporativas, las ventas de los módems empezaron a aumentar; desafortunadamente, las conexiones con módems son famosas por su inseguridad. Por lo tanto, los servidores de acceso remoto, que autentican a los usuarios marcando antes de otorgarles acceso a la red, (el servidor recibe una solicitud de acceso vía módem y en lugar de otorgarle permisos de entrada, lo que hace es regresar la llamada al número registrado y autorizado para ese usuario que tiene en su base de datos, y ya después le pide clave de usuario y contraseña), se convirtieron en una manera de asegurar las conexiones remotas.

2.2. Extendiendo las redes locales hasta Internet

El crecimiento rapidísimo de Internet a principios de los 90 creó un conjunto formidable de temas y requerimientos de seguridad. Los firewalls perimetrales pronto se convirtieron en componentes esenciales de la red. Estos dispositivos de hardware auditan, identifican y filtran el tráfico de Internet que entra y sale de la red corporativa. Si bien los firewalls aseguran los límites físicos de su infraestructura de red, no ofrecen protección contra ataques de usuarios internos o a las puertas secundarias de entrada a la red conocidas también como “puertas traseras”.

En los últimos años, las redes privadas virtuales (VPN, por sus siglas en inglés) se han convertido en una forma popular para que los socios estratégicos compartan recursos de la red. Estos túneles dedicados crean conexiones seguras de Internet entre LANs separadas físicamente.

Las VPNs ayudan a combatir el fisgoneo y olfateo que son un preludio a los ataques de los hackers, pero no ofrecen ningún tipo de garantía en contra del ataque en sí.

Los firewalls personales basados en software son relativamente nuevos en el mercado de la seguridad. Operan en conjunto con el sistema operativo residente y sirven para detectar, identificar y filtrar tráfico al extremo final del sistema. Aunque ofrecen una protección distribuida dentro de los firewalls perimetrales o gateways VPN, son relativamente fáciles de desactivar por medio de códigos maliciosos o por los usuarios finales.

Los Sistemas de Detección de Intrusos (IDS, por sus siglas en inglés) son herramientas de seguridad que detectan actividad inapropiada o anormal, ya sea en el sistema anfitrión o en el segmento de red. Están evolucionando rápidamente y requieren de mucho tiempo y conocimientos para configurar y monitorear. Además, generan muchas falsas alarmas.

Como consecuencia a todo lo anterior, actualmente el personal de sistemas realiza la administración central de políticas de seguridad, confía en la resistencia al sabotaje basada en hardware y el complemento a antivirus, firewalls perimetrales, VPNs, firewalls personales e IDSs.

Es un hecho que el uso de Internet en nuestros días se ha incrementado y que existen muchos espacios en Internet que se conocen como sites que proporcionan programas gratuitos, en donde es necesario descargar archivos llamados cookies, dlls, etc., para poder utilizarlos.

Esto es un gran riesgo para la seguridad de las computadoras ya que el mismo usuario está instalando programas que pueden ser caballos de Troya y destruir toda la información del disco,

además de que con el uso del correo se propaga una gran cantidad de virus informáticos y si no se tiene un detector actualizado de éstos, el sistema se convierte en presa fácil.

Si el sistema tiene conexión a Internet, los paquetes viajan por una serie de componentes que pueden ser ruteadores, gateways, puentes, etc., para conectarse con otros sites, al pasar por estos dispositivos pueden ser susceptibles a ser monitoreados por hackers o crackers, para poner "graffitis" en las páginas web de las empresas (en el mejor de los casos), a obtener las contraseñas de administradores y hacer todos los cambios que se les ocurran, inclusive la de borrar información delicada, confidencial e importante para la empresa, sin ninguna restricción, así como la de colocar virus.

En la actualidad, existen empresas que aún no están conectadas en red para realizar sus funciones diarias, teniendo como consecuencias la incompatibilidad de paquetería, pérdida de tiempo y que la información no sea del todo segura y confiable, inclusive el intercambio de información es por medio de discos flexibles, lo que también puede provocar una contaminación de virus, si no tienen en cada computadora un detector actualizado.

En algunas empresas, el jefe de sistemas es el que tiene más experiencia en el negocio, el cual no siempre tiene un perfil informático y en ocasiones no sabe que una gran premisa de la computación es la de respaldar la información, al menos de la que se considere importante, también tiene la idea que las máquinas son infalibles y las pérdidas del negocio pueden ser muchas si a alguna máquina se le daña el disco duro. Por lo tanto, actualmente se ha considerado de gran importancia la creación de políticas y de respaldos. Puntos clave que deben formar parte de una metodología de seguridad en redes de computadoras.

2.3. Origen de ISO 17799

El Instituto Británico de Normas Técnicas (BSI) publicó en 1995 la primera norma técnica de seguridad y la llamó BS 7799, fue redactada con el fin de abarcar los asuntos de seguridad relacionados con el e-commerce.

En mayo de 1999, el BSI publica su segunda versión de la norma, siendo más amplia que la primera, además se incluyeron muchos mejoramientos y perfeccionamientos, dando por resultado que la calidad total de la norma técnica aumentara considerablemente.

En diciembre de 2000, la Organización Internacional de Normas Técnicas (ISO) adoptó y publicó la primera parte de la norma BS 7799, es decir BS 7799-1 bajo el nombre de ISO 17799. La adopción por parte de ISO de la Parte 1 (los criterios de la norma técnica) de BS 7799 recibió gran aceptación por parte del sector internacional.

Desde su publicación, ISO 17799 surge como la norma técnica de seguridad de la información reconocida a nivel mundial y es la norma que más empresas a nivel internacional están utilizando para incorporar las medidas de seguridad que en ella se indican.

2.4. Marco de las recomendaciones

La norma ISO 17799 no incluye la segunda parte de BS 7799 es decir BS 7799-2, que se refiere a la implementación. ISO 17799 es una compilación de recomendaciones para las prácticas exitosas de seguridad que toda organización puede aplicar independientemente de su tamaño o sector. La norma técnica fue redactada intencionalmente para que fuera flexible y nunca indujo a las personas que la cumplían para que prefirieran una solución de seguridad específica. Las recomendaciones de la norma técnica ISO 17799 son neutrales en cuanto a la tecnología, y ayudan a evaluar y entender las medidas de seguridad existentes. Así, la norma discute la necesidad de contar con firewalls, pero no profundiza sobre los tipos de firewalls y cómo se utilizan, lo que conlleva a que algunos detractores de la norma digan que ISO 17799 es muy general y que tiene una estructura muy imprecisa y sin valor real.

La flexibilidad e imprecisión de ISO 17799 es intencional, por cuanto es difícil contar con una norma que funcione en toda la variedad de entornos de tecnología de la información y que sea capaz de desarrollarse con el cambiante mundo de la tecnología. ISO 17799 simplemente ofrece un conjunto de reglas a un sector donde no existían.

2.5. Áreas de control de ISO 17799

Las diez áreas de control son las siguientes:

1. Política de seguridad.
2. Seguridad organizacional.
3. Control y clasificación de los recursos de información (activos).
4. Seguridad del personal.
5. Seguridad física y ambiental.
6. Manejo de las comunicaciones y las operaciones.
7. Control de acceso.
8. Desarrollo y mantenimiento de los sistemas
9. Manejo de la continuidad de la empresa o del negocio.
10. Cumplimiento.

1. Política de seguridad

Objetivo: Proveer la directriz y el soporte de la dirección general de la empresa para la seguridad de la información.

Se necesita una política que refleje las expectativas de la organización en materia de seguridad a fin de suministrar administración con dirección y soporte. La política también se puede utilizar como base para el estudio y evaluación en curso.

2. Seguridad organizacional

Objetivos:

2.1 Administrar la seguridad de la información dentro de la organización.

2.2 Mantener la seguridad de las instalaciones de procesamiento de la información y los activos informáticos accedidos por terceros (proveedores, clientes, etc.).

2.3 Mantener la seguridad de la información cuando la responsabilidad del procesamiento de la información es ejecutada por terceros (outsourcing).

Sugiere diseñar una estructura de administración dentro de la organización que establezca la responsabilidad de los grupos en ciertas áreas de la seguridad y un proceso para el manejo de respuesta a incidentes.

3. Control y clasificación de los recursos de información (activos)

Objetivos: Mantener la protección adecuada de los activos corporativos y garantizar que los activos informáticos reciban un nivel adecuado de protección.

Necesita un inventario de los recursos de información de la organización y con base en este conocimiento, debe asegurar que se brinde un nivel adecuado de protección.

4. Seguridad del personal

Objetivo: Reducir el riesgo de error humano, robo, fraude, abuso de la información, sistemas y equipos. Asegurarse que el personal esté consciente de las amenazas a la información y sus implicaciones. Deberán apoyar la política corporativa de seguridad en contra de accidentes y fallas. A la vez deberán aprender de estos incidentes.

Establece la necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y asuntos de confidencialidad. También determina cómo incide el papel que desempeñan los empleados en materia de seguridad en el funcionamiento general de la compañía. Se debe tener e implementar un plan para reportar los incidentes.

5. Seguridad física y ambiental

Objetivo: Prevenir el acceso no autorizado a las instalaciones para evitar pérdida, robo, daño de los bienes y evitar la interrupción de las actividades productivas. Prevenir el robo de información y de los procesos de la empresa.

Responde a la necesidad de proteger las áreas, el equipo y los controles generales.

6. Manejo de las comunicaciones y las operaciones

Objetivos:

6.1 Asegurar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.

6.2 Minimizar el riesgo de falla de los sistemas.

6.3 Proteger la integridad del software y la información.

6.4 Conservar la integridad y disponibilidad del procesamiento y la comunicación de la información.

6.5 Garantizar la protección de la información en las redes y de la infraestructura de soporte.

6.6 Evitar daños a los recursos de información e interrupciones en las actividades de la organización.

6.7 Evitar la pérdida, modificación o uso indebido de la información que intercambian las organizaciones.

7. Control de acceso

Objetivos:

7.1 Controlar el acceso a la información.

7.2 Prevenir los accesos no autorizados a sistemas de información.

7.3 Garantizar la protección de servicios de red.

7.4 Prevenir los accesos no autorizados a las computadoras.

7.5 Detectar actividades no autorizadas.

7.6 Garantizar la seguridad de la información cuando se utilice cómputo móvil o remoto.

Establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación para proteger contra los abusos internos e intrusos externos.

8. Desarrollo y mantenimiento de los sistemas

Objetivo: Asegurarse que la seguridad del sistema está construida dentro de la aplicación para prevenir pérdidas, abusos, modificaciones de los datos.

Recuerda que en toda labor de la tecnología de la información, se debe implementar y mantener la seguridad mediante el uso de controles de seguridad en todas las etapas del proceso. Debe proteger la confidencialidad, autenticidad e integridad de la información. Los proyectos informáticos y sus actividades de soporte deberán ser conducidos de forma segura.

9. Manejo de la continuidad de la empresa o del negocio

Objetivos: Contrarrestar las interrupciones en las actividades de la empresa y proteger los procesos importantes de la empresa en caso de una falla grave o desastre.

10. Cumplimiento

Objetivos:

10.1 Evitar infringir cualquier norma civil o penal, ley, reglamento, obligación contractual o cualquier requerimiento de seguridad.

10.2 Asegurar la compatibilidad de los sistemas con las políticas y estándares de seguridad.

10.3 Maximizar la efectividad y minimizar las interferencias hacia y del sistema de auditoría del proceso.

Imparte instrucciones a las organizaciones para que verifiquen si el cumplimiento con la norma técnica ISO 17799 concuerda con otros requisitos jurídicos. Esta sección también requiere una revisión a las políticas de seguridad, al cumplimiento y consideraciones técnicas que se deben hacer en relación con el proceso de auditoría del sistema a fin de garantizar que las empresas obtengan el máximo beneficio.

Alinearse con la ISO 17799 no es una tarea fácil, incluso para las organizaciones con más conciencia en la seguridad.

Por eso, se recomienda que la ISO 17799 sea implementada bajo un esquema "paso a paso". El mejor punto de partida es realizar un análisis de la posición y situación de la organización, seguido de una identificación de los cambios necesarios para alinearse con la ISO 17799. A partir de este punto, el proceso de planear e implementar debe ser emprendido metódicamente y abierto al cambio.

En caso de que alguna empresa quiera lograr la certificación en seguridad informática, lo debe hacer bajo el criterio del estándar BS 7799-2, existen seis pasos para lograrla con el BSI (British Standard Institute), los cuales se mencionan a continuación.

Paso 1. Establecer un marco normativo como se describe en el BS 7799-2.

Paso 2. BSI proporcionará un presupuesto de costos y tiempos para una evaluación formal. El tiempo que lleva hacer la verificación del cumplimiento de las recomendaciones normalmente lleva más de seis meses.

Paso 3. Presentar una solicitud formal a BSI.

Paso 4. BSI hará una revisión documental de la evaluación de riesgos, política, alcance, declaración de aplicabilidad y procesos. Esto identificará cualquier debilidad u omisión que se necesite resolver en su sistema administrativo.

Paso 5. BSI llevará a cabo una auditoría en el sitio y hará sus recomendaciones.

Paso 6. Al completar exitosamente esta auditoría, se expedirá un certificado que identifica claramente el alcance del sistema administrativo de seguridad de la información. Esta certificación, será válida por tres años y estará soportado por visitas rutinarias de evaluación (auditorías de mantenimiento) a lo largo de ese tiempo.

La norma internacional ISO 17799 ha sido reconocida a nivel internacional, de tal forma que, por ejemplo, ha sido homologada en España con el nombre de UNE 71501, en Argentina con IRAM – ISO 17799, en Brasil con NBR ISO/IEC 17799; debido principalmente a que involucra a la totalidad de los activos de un sistema de información, llámese hardware, software, estructura de datos y el personal de la organización.

Existen ventajas de que una empresa cuente con la certificación en seguridad informática, una de ellas se fundamenta en que las auditorías que realicen las autoridades sean más precisas y confiables, otra consiste en que el cliente tenga una mayor confianza y esto represente obtener mayores ganancias en cuanto a sus competidores, que se tenga un manejo y planeación de la seguridad de la información más eficiente, y sobre todo una mayor seguridad en que el negocio aún en caso de presentarse un desastre tendrá forma de seguir con sus operaciones críticas.

También permite el cumplir de manera efectiva con los requisitos que de manera legal impongan las autoridades a la organización; llámese Comité de Basilea, Banco de México, Secretaría de Hacienda y Crédito Público, Comisión Nacional Bancaria y de Valores, la Organización para la Cooperación y el Desarrollo Económico, etc.

La gráfica 2.1 pone de manifiesto la necesidad de las empresas de contar con sistemas de seguridad informática acordes a su giro y tamaño.

El estándar ISO 17799 indica qué hacer, pero no dice cómo; la metodología de seguridad en redes de computadoras se enfoca precisamente en este aspecto, pretendiendo ser una guía práctica para la implementación de sistemas de seguridad informática en redes de cómputo de cualquier tipo.

CAPÍTULO 3

RIESGOS, AMENAZAS Y ATAQUES

3.1. Riesgos

Para determinar cuál es la seguridad adecuada en un sistema habrá que estudiar cuáles son los riesgos a los que está expuesto, teniendo en cuenta el valor de la información, los costos de recuperación y evaluar lo que costaría la protección.

Riesgo se define como:

La pérdida potencial que se da como resultado de una relación amenaza-vulnerabilidad, de tal manera, que al reducir la amenaza o la vulnerabilidad se reduce el riesgo.

La incertidumbre de perder, expresada en términos de la probabilidad de tal pérdida.

La probabilidad que una entidad hostil podrá explotarse en un sistema de comunicaciones con propósitos de inteligencia, teniendo como factores la amenaza y la vulnerabilidad.

La combinación de la probabilidad de que una amenaza ocurra, la probabilidad de que la ocurrencia resulte con un impacto adverso y la severidad de éste.

3.1.1. Vulnerabilidad

Debilidad o evento que puede ser aprovechado para violar la seguridad.

Hueco o debilidad de un sistema.

3.1.2. Amenaza

Circunstancia o evento que puede causar un daño (impacto) al violar la seguridad.

3.1.3. Seguro

Libre o exento de todo daño o riesgo.

Se considera que algo está seguro si ninguna amenaza se presenta sobre él o bien si el riesgo de que llegue a realizarse sea estimado mínimo. Ya que un riesgo es el impacto de que una amenaza pueda afectar la habilidad de lograr los objetivos y estrategias de negocio de una organización, hay que establecer controles que ayuden a las organizaciones a alcanzar sus objetivos y estrategias de negocio, evitando o minimizando los impactos que pudiese tener un riesgo, para evitar una exposición, la cual se considera como el impacto potencial que se genera cuando un control no mitiga totalmente un riesgo, antes o después de que dicho riesgo se manifieste.

Para efectuar un mejor análisis de riesgos, éstos se dividen en internos y externos, como primera clasificación, a su vez los riesgos externos se dividen en tres grandes rubros que son,

naturales, humanos y materiales; los riesgos internos se clasifican en robo, sabotaje, destrucción y fraude siendo éstos principalmente de índole de seguridad lógica.

La Figura 3.1[1] muestra los tipos de riesgos que se pueden presentar y sus derivaciones.

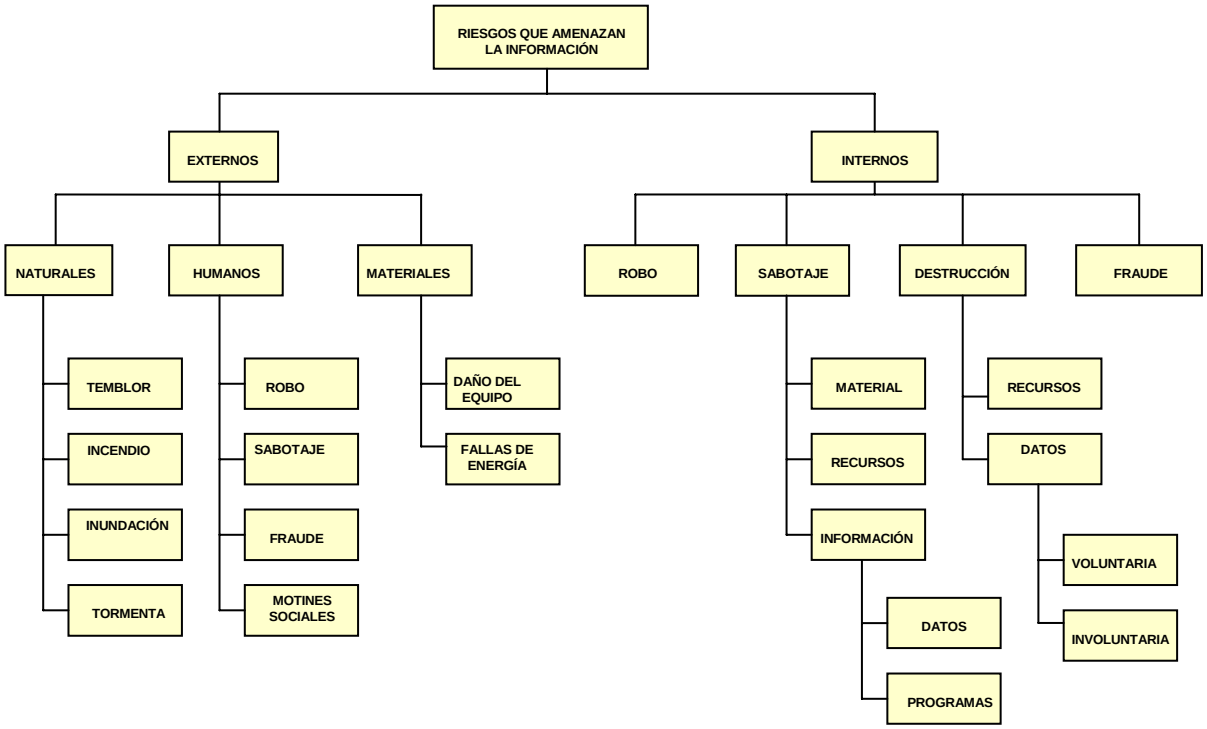


Figura 3.1 Riesgos que amenazan la información

3.2. Análisis de riesgos

En un entorno informático existe una serie de recursos (humanos, técnicos, de infraestructura) que están expuestos a diferentes tipos de riesgos: los normales, aquellos comunes a cualquier entorno, y los excepcionales, originados por situaciones concretas que afectan o pueden afectar a parte de una organización o a toda la misma, como la inestabilidad política en un país o una región sensible a terremotos. Para tratar de minimizar los efectos de un problema de seguridad se realiza lo que se denomina **análisis de riesgos**, término que hace referencia al proceso necesario para responder a tres cuestiones básicas sobre seguridad:

- ¿Qué se quiere proteger?
- ¿Contra quién o qué se debe proteger?
- ¿Cómo se aspira proteger?

[1] Espinosa Sarmiento, Gonzalo. *Análisis de riesgo*. Instituto Tecnológico de Estudios Superiores Monterrey. Sexta Edición. México. 2002. Página 6.

En la práctica existen dos aproximaciones para responder a estas cuestiones, una cuantitativa y otra cualitativa. La primera de ellas es con diferencia la menos usada, ya que en muchos casos implica cálculos complejos o datos difíciles de estimar. Se basa en dos parámetros fundamentales: la probabilidad de que un suceso ocurra y una estimación del costo o las pérdidas en caso de que así sea; el producto de ambos términos es lo que se denomina **costo anual estimado** (EAC, Estimated Annual Cost), y aunque teóricamente es posible conocer el riesgo de cualquier evento (el EAC) y tomar decisiones en función de estos datos, en la práctica la inexactitud en la estimación o en el cálculo de parámetros hace difícil y poco realista esta aproximación.

La segunda aproximación de análisis de riesgos es la cualitativa, de uso muy difundido en la actualidad especialmente entre las consultoras de seguridad (aquellas más especializadas en seguridad lógica, firewalls, pruebas de penetración y similares). Es mucho más sencillo e intuitivo que el anterior, ya que ahora no entran en juego probabilidades exactas sino simplemente una estimación de pérdidas potenciales. Para ello se interrelacionan cuatro elementos principales: las amenazas, por definición siempre presentes en cualquier sistema, las vulnerabilidades, que potencian el efecto de las amenazas; el impacto asociado a una amenaza, que indica los daños sobre un activo por la materialización de dicha amenaza, y los controles o protecciones, contramedidas para minimizar las vulnerabilidades (controles preventivos) o el impacto (controles curativos). Por ejemplo, una amenaza sería un pirata informático que va a tratar de modificar la página web principal; el impacto sería una medida del daño que causaría si lo lograra; una vulnerabilidad sería una configuración incorrecta del servidor que ofrece las páginas, y un control de la reconfiguración de dicho servidor o el incremento de su nivel de parcheado. Con estos cuatro elementos se puede obtener un indicador cualitativo del nivel de riesgo asociado a un activo determinado dentro de la organización, visto como la probabilidad de que una amenaza se materialice sobre un activo y produzca un determinado impacto.

La forma más sencilla de hacer este estudio sería anotar en una columna todas las amenazas posibles, y a un lado, con un valor numérico dentro de una escala, el grado en el que se considera que el sistema estaría expuesto, como lo muestra la Figura 3.2.

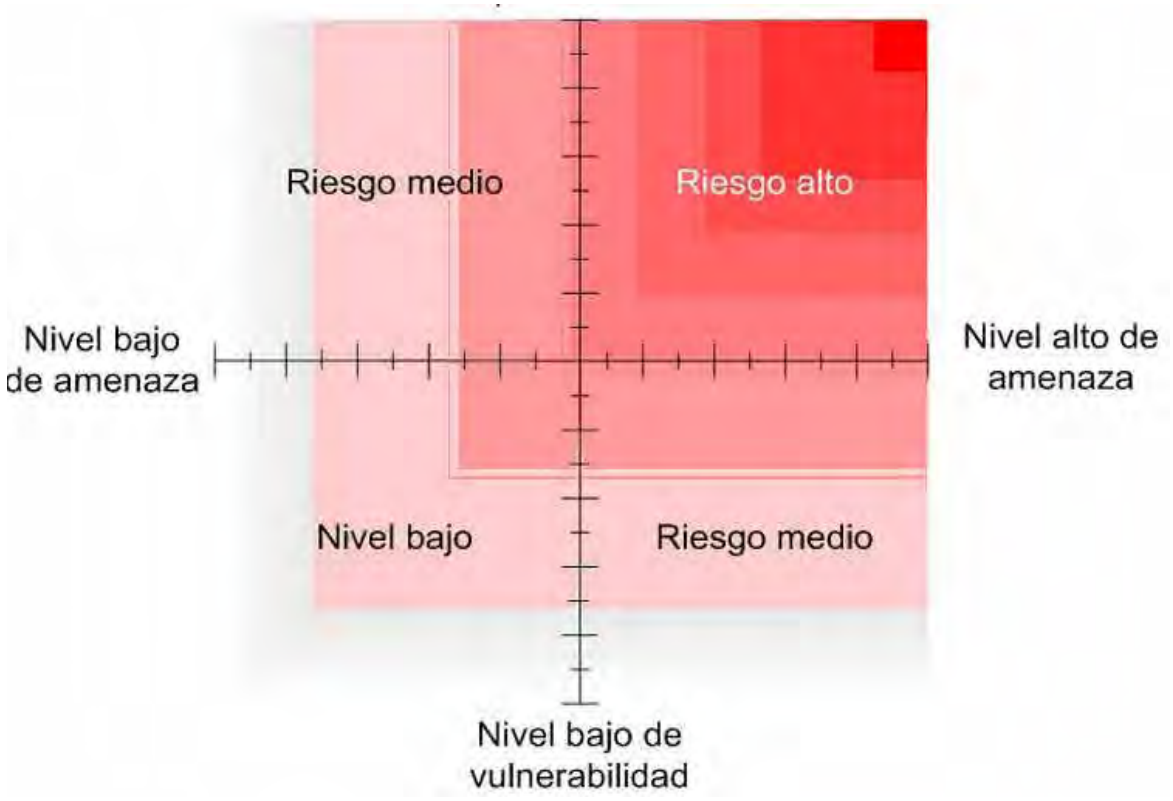


Figura 3.2 Análisis de riesgos

De manera práctica se utiliza la matriz de análisis de riesgo cualitativo, propuesta en el estándar australiano-neozelandés de administración de riesgos, denominado AS/NZS 4360 (Australian/New Zealand Standard 4360).

En este estándar se establecen cinco niveles de probabilidad, Tabla 3.1, cinco grados de impacto, Tabla 3.2 y cuatro categorías de riesgo, Gráfica 3.1, las cuales se explican brevemente a continuación:

NIVEL	DESCRIPCIÓN	PORCENTAJE	SIGNIFICADO
5	CASI CERTEZA	1.00	SE ESPERA QUE OCURRA EN LA MAYORÍA DE LAS CIRCUNSTANCIAS
4	PROBABLE	0.75	PROBABLEMENTE OCURRIRÁ EN LA MAYORÍA DE LAS CIRCUNSTANCIAS
3	POSIBLE	0.5	PODRÍA OCURRIR EN ALGÚN MOMENTO
2	IMPROBABLE	0.25	PUDO OCURRIR EN ALGÚN MOMENTO
1	RARO	0.10	PUEDE OCURRIR SÓLO EN CIRCUNSTANCIAS EXCEPCIONALES

Tabla 3.1 Medidas cualitativas de probabilidad

NIVEL	DESCRIPCIÓN	SIGNIFICADO
5	CATASTRÓFICO	ENORME PÉRDIDA FINANCIERA
4	MAYOR	PÉRDIDA FINANCIERA MAYOR
3	MODERADO	PÉRDIDA FINANCIERA ALTA
2	MENOR	PÉRDIDA FINANCIERA MEDIA
1	INSIGNIFICANTE	BAJA PÉRDIDA FINANCIERA

Tabla 3.2 Medidas cualitativas de impacto

	IMPACTO				
PROBABILIDAD	INSIGNIFICANTE 1	MENOR 2	MODERADO 3	MAYOR 4	CATASTRÓFICO 5
5 CASI CERTEZA	A	A	E	E	E
4 PROBABLE	M	A	A	E	E
3 POSIBLE	B	M	A	E	E
2 IMPROBABLE	B	B	M	A	E
1 RARO	B	B	M	A	A

Gráfica 3.1 Matriz de análisis de riesgo cualitativo

En esta matriz el significado de las letras es el siguiente:

E: Riesgo extremo.

A: Riesgo alto.

M: Riesgo moderado.

B: Riesgo bajo.

De acuerdo a esta matriz debe darse especial atención primeramente a todas las amenazas que signifiquen un riesgo extremo.

La metodología de análisis y gestión de riesgos de los sistemas de información de las administraciones públicas, desarrollada desde el Consejo Superior de Informática de España (Ministerio de Administraciones Públicas) y denominada MAGERIT, trata de manera formal realizar un análisis de riesgos y recomendar los controles necesarios para su minimización. MAGERIT se basa en una aproximación cualitativa que intenta cubrir un amplio espectro de usuarios genéricos, gracias a un enfoque orientado a la adaptación del mecanismo dentro de

diferentes entornos, generalmente con necesidades de seguridad y nivel de sensibilidad también diferentes.

Tras obtener mediante cualquier mecanismo los indicadores de riesgo en la organización, llega la hora de evaluarlos para tomar decisiones organizativas acerca de la gestión de la seguridad y sus prioridades. Se tiene, por una parte el riesgo calculado, resultante del análisis, y este riesgo calculado se ha de comparar con un cierto umbral (umbral de riesgo) determinado por la política de seguridad de la organización; el umbral de riesgo puede ser o bien un número o bien una etiqueta de riesgo (por ejemplo, nivel de amenaza alto, impacto alto, vulnerabilidad grave, etc.), y cualquier riesgo calculado superior al umbral ha de implicar una decisión de reducción de riesgo. Si por el contrario, el calculado es menor que el umbral, se habla de riesgo residual, y el mismo se considera asumible (no hay porque tomar medidas para reducirlo). El concepto de asumible es diferente al de riesgo asumido, que denota aquellos riesgos calculados superiores al umbral, pero sobre los que, por cualquier razón (política, económica) se decide no tomar medidas de reducción; siempre se ha de huir de esta situación ya que, en caso de presentarse la amenaza, provocará pérdidas económicas que afectarán seriamente la operación de la organización.

Una vez conocida y evaluada cualquier forma de riesgos a los que se enfrenta la organización, se puede definir las políticas e implementar las soluciones prácticas (los mecanismos) para minimizar sus efectos. Se explicará con más detalle en los siguientes párrafos cómo dar respuesta a cada una de las preguntas que se han planteado al principio de este punto.

En cada caso particular, el riesgo a cada amenaza puede ser muy distinto. Lógicamente, no corre el mismo riesgo de infección por virus una computadora en la que únicamente se introducen programas originales, que otra utilizada por múltiples usuarios y en la que no hay ningún control sobre los programas que son instalados.

Realizar un análisis de riesgos es uno de los primeros pasos que se lleva a cabo para determinar en qué dirección han de dirigirse los esfuerzos para implementar una seguridad adecuada, que permita detectar cuáles son los puntos vulnerables en donde se deben aplicar o reforzar las medidas de seguridad.

Básicamente los riesgos que corre la información son su pérdida, alteración y robo; pero debido a la diversidad de amenazas, errores humanos y por los diferentes tipos de ataques que se encuentran contenidos en la Figura 3.1, a continuación se explicará cada uno de éstos.

3.2.1. Desastres naturales

Los desastres naturales como temblores, incendios, inundaciones, tormentas, etc., suelen tener consecuencias fatales para los sistemas: daños irreparables en los equipos, pérdida de información y no disponibilidad. La ubicación geográfica y el lugar de instalación física son factores que determinan el riesgo que se corre frente a cada desastre. Al igual que en una zona sísmica el riesgo de terremoto es alto, en un lugar seco rodeado de árboles es mayor el de incendio o en las proximidades de un río es más probable una inundación. Por estos factores se debe tener una estrategia personalizada para cada tipo de organización en una determinada zona geográfica.

3.2.2. Humanos

Este tipo de amenazas se puede dividir en dos clases. La primera, dada por personas malintencionadas y la segunda por personas no malintencionadas. Las personas maliciosas son aquellas que tratan de perjudicar los activos de una organización, ya sea por algún tipo de remuneración o sólo por diversión y pueden ser externas a la organización (como piratas informáticos o intrusos) y personas internas en la organización (como empleados descontentos o saboteadores). En la segunda clase abundan todo tipo de errores humanos originados por la negligencia de personas que desconocen la operación y el manejo de los equipos que sirven para el funcionamiento del sistema informático. Cabe mencionar que este tipo de amenazas son una de las principales causas de pérdida de información.

Hay que tener en cuenta que las amenazas, tales como las de usuarios ignorantes o descuidados, y los desastres naturales, no implican motivos u objetivos; por lo tanto, no se utilizan métodos, herramientas o técnicas predeterminadas para iniciar los ataques. La mayoría de estos ataques o infiltraciones en la seguridad se generan dentro de la organizaciones; rara vez son iniciados por alguien ajeno a la misma.

Robo de la información

Contenida en la base de datos o durante la transmisión.

Hoy en día es muy común que las aplicaciones que se ejecutan a través de las redes utilicen uno o más servidores de base de datos, de aquí el riesgo de que alguna persona no autorizada tenga acceso para modificar los datos. Puesto que el robo no supone la destrucción de la información original, el sistema no se verá afectado. Sus consecuencias son: económicas, tácticas o quizás una amenaza contra la privacidad de las personas. El robo de información es un riesgo que no afecta demasiado a los usuarios particulares, pero que puede tener graves

consecuencias en la organización ultrajada. Si no existen archivos de registro de actividades no quedará constancia de la acción, ya que la información no es sustraída sino copiada.

Sabotaje de información

El sabotaje a un sistema puede estar dirigido contra la información (en forma de destrucción o manipulación) o también tener como objetivo la destrucción de los equipos, por lo que puede afectar tanto a la disponibilidad del sistema como a la integridad de la información contenida. Existen muchas organizaciones que emplean sus transacciones por medio de las redes y sitios web, como son las empresas que comercializan productos tales como libros, discos, artículos electrónicos, incluso los bancos; aquí el riesgo que se corre, por ejemplo, es el que alguien altere el número de una tarjeta de crédito con el que se efectúa un pago electrónico.

Recepción de virus y caballos de Troya

Las consecuencias de que un virus entre en el sistema son la posible destrucción de información y la pérdida de tiempo necesaria para eliminarlo. Este riesgo se presenta comúnmente cuando un usuario recibe un e-mail o instala una aplicación de dudosa procedencia, en donde su contenido es, en la mayoría de los casos, desconocido y que para el usuario puede parecer interesante. Al abrir los archivos anexos que vienen en un e-mail, se instala algún tipo de programa que puede robar los passwords para enviarlos a una dirección externa (caballos de Troya), dañar los dispositivos de almacenamiento de la computadora, principalmente el disco duro, teniendo como consecuencia la pérdida catastrófica de la información almacenada en el dispositivo, o incluso abrir conexiones externas con el equipo del atacante.

Ejecución de código malicioso

Además de los virus y los caballos de Troya, cuando un usuario está visitando páginas web es posible que el navegador descargue código móvil desde el servidor web. En este caso el usuario estará ejecutando desde su propio equipo rutinas de programación que no son visibles para él. Es posible que dichos programas hayan sido escritos con mala intención.

Modificación de paquetes

Este tipo de riesgo se presenta cuando se usan analizadores de protocolos o accediendo de forma no autorizada a servidores de correo para espiar o alterar los paquetes de datos que se transmiten por la red. Lo que se violaría en este riesgo es la integridad. El acceso a la

información y modificación se manifiesta por el borrado, cambiado, añadiendo o sustituyendo datos.

Modificación de páginas web

Este riesgo es uno de los más comunes. Surge de los huecos en la programación o en la configuración del servidor web incluyendo el sistema operativo, el atacante logra modificar el contenido de las páginas HTML, perjudicando la imagen de la organización con sus visitantes y clientes. Ejemplos de este tipo de ataque se muestran en las Figuras 3.3, 3.4, 3.5 y 3.6.

Figura 3.3 Página original del Partido Laboral

Figura 3.4 Página hackeada del Partido Laboral [2]

[2] Gómez Cárdenas, Roberto. *Seguridad Computacional*. Instituto Tecnológico de Estudios Superiores Monterrey. Segunda edición. México. 2001.

Figura 3.5 Página de la CIA original

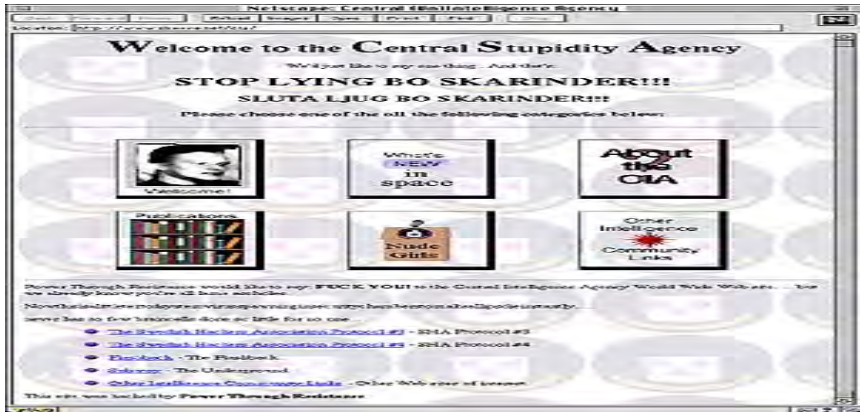


Figura 3.6 Página hackeada de la CIA[3]

Interrupción del correo electrónico

Este riesgo se logra por medio de analizadores de protocolos, y está considerado dentro de los ataques de sabotaje. Hay que tener cuidado con el tipo de información que se envía por medio del correo electrónico. Una medida para evitar que el correo sea leído de forma directa es la utilización del cifrado.

Averiguación de passwords

Existen muchas herramientas de dominio público que sirven para averiguar passwords, incluso si éstos se encuentran crifrados. Normalmente estas herramientas se basan en la copia del archivo que contiene las claves de acceso del sistema, conocido como el "password file", o también pueden interceptar los passwords cuando viajan en la red. Para descubrir los passwords

[3] Gómez Cárdenas, Roberto. *Seguridad Computacional*. Instituto Tecnológico de Estudios Superiores Monterrey. Segunda edición. México. 2001.

cifrados las herramientas utilizan una lista de palabras cifradas que se obtienen de algún diccionario de términos comunes, dicho diccionario depende del idioma y del país. La mecánica consiste en verificar si hay coincidencia entre estas listas cifradas y los passwords obtenidos.

Realización de una radiografía de Intranet

Para este tipo de ataque también se emplean herramientas que están en el dominio público, las cuales se encargan de analizar la red de una organización por medio de una conexión de Internet para dar información, tal como direcciones de servidores, servicios que éstos proveen y la configuración de los mismos. La principal actividad que realizan estas herramientas es la de ejecutar el comando ping por rangos para conocer por dónde pasan los paquetes y así descubrir los ruteadores de la red.

Obtención de huecos de seguridad en los sistemas operativos y servicios instalados

En Internet existen “bibliotecas” completas que relacionan todos los huecos de seguridad para un ambiente en particular e incluyen los programas que explotan dichos huecos, a tales programas se les conoce como exploits. Para reducir un poco este riesgo es necesario instalar las actualizaciones de seguridad de los equipos y los parches que el distribuidor pone a disposición de los usuarios; comúnmente a este tipo de parches se les conocen con el nombre de “services pack”.

Fraude

Realización de transacciones fraudulentas

Este tipo de riesgo se corre cuando una organización emplea el comercio electrónico o el manejo de sus acciones por medio de redes de computadora, un ejemplo de este riesgo es el que corren los bancos cuando una persona no autorizada efectúa algún tipo de movimiento en una cuenta que no es suya. El manipular la información con el fin de obtener un beneficio es lo que se conoce como fraude informático. En los bancos este tipo de fraude actualmente es poco común ya que se emplean avanzadas medidas de seguridad, como detectores de intrusos tanto de host como de red, firewalls, cifrado de datos, etc. Al igual que el robo, no lleva consigo consecuencias para el sistema, esto quiere decir que el equipo no sufre daño alguno.

Motines sociales

En el entorno de trabajo existe la posibilidad de que se realicen motines sociales e impidan el acceso a las instalaciones, debido a esto una de las mejores prácticas de seguridad es que las empresas cuenten con instalaciones alternas que provean de los recursos informáticos para que la operación de la institución no se detenga, esto se debe detallar en el plan de continuidad del negocio donde se especifica entre otras cosas, quién es el encargado de declarar la contingencia, quiénes pertenecen al equipo de respuesta a incidentes así como quiénes de las áreas operativas deben acudir a dicho centro de operaciones.

3.2.3. Materiales

Daño del equipo

El daño o descompostura en los equipos de cómputo afectan básicamente a la disponibilidad del sistema, provocando también una pérdida de información.

Existe una serie de medidas que se pueden tomar en cuenta para disminuir el impacto en caso de que se dañe el equipo, algunas de ellas se mencionan a continuación:

- Configuración de servidores en cluster.
- Configuración de discos en forma de espejo.

Configuración de servidores en cluster, esto quiere decir que se tienen dos equipos conectados entre sí y configurados de manera que si uno de ellos falla, el otro equipo se hace cargo de la operación.

Configuración de discos en forma de espejo, aquí en lugar de tener dos equipos, es el mismo equipo que cuenta con la configuración de que toda la información contenida en sus discos se tiene copia de la misma en otros discos que se llaman espejo, a esto se le conoce como RAID 0 (Redundant Array of Independent Disks, configurados como disk striping without parity), la cual significa que es un arreglo de dos discos donde uno es la copia del otro, esta protección permite un mejor desempeño en lectura y escritura, que otras configuraciones de RAID.

Cuando se tiene una cantidad considerable de información guardada en varios discos la estrategia anterior sería muy cara, por ello en este caso se configura el servidor en sus discos la opción de RAID 5 (Redundant Array of Independent Disks, configurados como striped sets with parity), lo cual quiere decir que es un arreglo de discos en donde la información se guarda en varios de ellos y si algún disco en particular falla se reemplaza por otro y de manera automática la información contenida en el disco dañado se vuelve a generar en el nuevo. Cada

uno de los discos tiene parte de información de los otros, para poder recuperar la información del disco dañado.

Otra estrategia es hacer respaldos de la información, ya sea en cintas o en discos, los cuales son llevados para su resguardo a otras instalaciones, ya sean cajas fuertes de algún banco o se tenga contratados los servicios de un proveedor externo.

Como observación se puede decir que debe haber un adecuado manejo de respaldos de la información para que exista alguna forma de recuperarla y no se vaya a perder de manera definitiva.

Fallas de energía

Una muy posible amenaza a tener en cuenta, es la falla en el suministro de energía eléctrica de los equipos ya que los recursos informáticos son sensibles a las variaciones de tensión y de frecuencia de la corriente eléctrica. Los requerimientos básicos para el suministro de energía eléctrica son dos: calidad y continuidad.

Relacionado con la calidad, se puede destacar que:

Las variaciones de frecuencia deben corregirse con equipos estabilizadores que la mantengan dentro de los rangos establecidos por los fabricantes de los recursos informáticos a alimentar, aunque algunos recursos informáticos de nueva tecnología los llevan incluidos.

Sin electricidad los equipos de cómputo no pueden funcionar, es por ello que las medidas siguientes se deben tomar en cuenta para que la operación no se detenga.

Las variaciones de tensión deben ser manejadas por un sistema de alimentación ininterrumpida (UPS por sus siglas en inglés), de modo que se puedan prevenir los efectos de posibles microcortes. En relación con la continuidad del suministro eléctrico debe tenerse en cuenta que:

Las caídas de tensión pueden ser manejadas por un sistema de suministro ininterrumpible normalmente, pero sólo por tiempo limitado (ya que el desgaste de sus acumuladores es muy rápido y su recarga muy lenta para utilizarlo en cortes sucesivos) y nunca como única alternativa.

Se recibe un suministro normal para cargar baterías y se proporciona un suministro limpio cuando el abastecimiento de energía comercial falla. Sirven para proporcionar energía temporal. Suministran energía eléctrica constante al equipo, soportados por un banco de baterías con una duración nominal de x minutos. Existen "On line" y "Stand by" el tiempo de respuesta en caso de apagón es de milisegundos (cero segundos).

Existen varios productos que disminuyen el impacto provocado por falla en el suministro de energía eléctrica y son de uso común en la industria, ejemplos de esto son las plantas de emergencia, acondicionadores de línea, reguladores y la instalación de tierra física.

Planta eléctrica. Generador electromecánico de energía, trabaja en base a algún combustible, su tiempo de respuesta es de segundos. Pueden funcionar en periodos prolongados de tiempo.

Acondicionadores de línea. Sirven para eliminar las variaciones de voltaje y el ruido eléctrico en grados variantes pero no almacenan energía eléctrica, lo que significa que no pueden contrarrestar interrupciones en el suministro de electricidad.

Reguladores. Suministran voltaje estable a los equipos.

Tierra física. Instalación eléctrica que permite absorber descargas eléctricas, conformada por una varilla de cobre de tres metros, enterrada bajo el nivel del suelo y de preferencia en un lugar con humedad, complementada con sales y carbón para mejorar asimilación de descargas. El suministro eléctrico debe ser independiente del general de todo el edificio, y las tomas de tierra deben ser independientes de las generales del edificio, a suficiente distancia de ellas, correctamente instaladas y rigurosamente mantenidas.

En general, el diseño de las instalaciones eléctricas es uno de los aspectos fundamentales que debe cuidarse cuando se va a diseñar el centro de cómputo, ya que si no se efectúa un buen cálculo sobre la carga que se va a demandar, ocasionaría serios problemas al utilizar el equipo. Por esto, se requiere hacer un análisis sobre todos los equipos y dispositivos que se vayan a utilizar en el centro de cómputo como si fuesen a trabajar todos al mismo tiempo, así se podrá obtener la carga máxima que se pudiera llegar a ocupar. Los equipos de cómputo son de los más sensibles a las variaciones de corriente eléctrica por lo tanto es necesario instalar los equipos de protección mencionados anteriormente.

Caída del servicio

Si por alguna razón, el acceso a un servicio que ofrece un servidor web queda temporalmente bloqueado o con tiempos de respuesta demasiados largos, este tipo de riesgo puede hacer que el sistema se vuelva inoperable. Una forma de reducir las vulnerabilidades a esta amenaza consiste en configurar los servidores para que trabajen en forma de cluster, lo cual quiere decir que están dos máquinas en paralelo y en caso de que una tenga caída del servicio, la otra cubra toda la operación, y pueda seguir proporcionando el servicio.

Las amenazas que se presentan en un sistema de información son muy diversas, pero principalmente se originan por errores humanos ya sean voluntarios o involuntarios y por desastres naturales. Dichas amenazas pueden afectar tanto a la información como a los equipos,

que son, los bienes a proteger en una organización para lograr la disponibilidad del sistema. Es por ello que para combatir y prevenir un ataque es necesario conocer las distintas amenazas que ponen en peligro los sistemas de información.

Para estos tipos de amenazas, el personal de seguridad necesita implementar estrategias preactivas y reactivas, así como políticas de seguridad que deben ser supervisadas y actualizadas constantemente conforme cambie la estructura de una organización.

A continuación se hará un análisis acerca de los hackers, ya que es uno de los mayores temores por parte de las empresas.

Hackers o piratas informáticos

El actual interés en el campo de la seguridad informática es en gran parte debido a la publicidad que se ha hecho de la figura del hacker o pirata informático, temido en el entorno de comunicaciones abierto de las redes IP. Hoy en día, la seguridad es un requisito existente en todo proyecto, diseño o elemento conectado a una red IP.

Los piratas informáticos tienen que lidiar con una gran variedad de herramientas y planteamientos cuyo fin principal es la protección de las redes, tales como firewalls, herramientas de detección de intrusos, utilidades de análisis y correlación de registros o entradas, etc. A pesar de esto y frente a diversos inconvenientes los hackers tienen a su disposición un amplio repertorio de herramientas desarrolladas con el único fin de inutilizar o traspasar los mecanismos de seguridad.

Los hackers para efectuar sus ataques usan una metodología que abarca prácticamente los siguientes puntos.

1. Selección del objetivo y recopilación de información.
2. Acceso inicial.
3. Aumento de privilegios.
4. Ocultar el rastro.
5. Establecer puertas traseras para posteriores accesos.

Para encontrar la definición y origen del término hacker hay que retroceder a los años 60 cuando todavía no existía Internet como hoy se conoce. En aquella época, la informática se basaba en grandes computadoras conocidas como mainframes. Hace algunos años se denominaba hacker a esa persona experta en computación. Estas personas conocían los más recónditos lugares de los sistemas más populares o de algún lenguaje de programación, por lo que ayudaban a encontrar errores y, muchas veces, hasta corregirlos. Por otro lado, en el origen

de esta palabra está el término hack (algo así como golpear con un hacha en inglés) que se usaba en forma familiar para describir cómo los técnicos telefónicos, arreglaban las cajas defectuosas, asestándoles un golpe seco. También mucha gente arregla el televisor dándole una palmada seca en el lateral. Quien hacía esto era un hacker. Otra historia relata cómo las primeras computadoras grandes y defectuosas, se bloqueaban continuamente y fallaban. Los que las manejaban se devanaban los sesos creando rutas para aumentar la velocidad y cosas parecidas. Estas cosas se denominaban hacks y a los que lo hacían se les llamaba hackers.

Realmente, el término hacker se utiliza para denominar aquellos expertos que conocían a la perfección el complicado funcionamiento de estas computadoras, por lo cual era un calificativo totalmente positivo e incluso un halago dentro de la comunidad informática de ese entonces.

Con el paso del tiempo, algunas de esas personas, por diferentes motivos, migraron al lado de los malos, utilizando sus conocimientos para hacer daño a los sistemas de cómputo; desde entonces, el término hacker se ha utilizado también para designar a estos “piratas informáticos”, pero a estos últimos se les conoce específicamente como “crackers”.

3.3. Tipos de atacantes

Actualmente existe una gran diversidad de términos para clasificar a un cierto tipo de atacante, dicha clasificación se da de acuerdo a su experiencia, rama de ataque, intereses, etc., existen varias clasificaciones, a continuación se explica una de ellas.

- Hacker.
- Insider.
- Cracker.
- Bucaneros.
- Lamer.
- Copy-hackers.
- Gurús.
- Phreakers.
- Sneackers.
- Script-kiddies.

3.3.1. Hacker

Persona de perfil brillante que intenta tener acceso no autorizado a un ambiente de cómputo en el cual dicha persona no tiene ningún privilegio o permiso. El propósito de un hacker puede ser entretenimiento, beneficios personales o económicos, robo entre otros. Normalmente ocupan técnicas iterativas o metodologías avanzadas, así como herramientas para interceptar las comunicaciones de terceros para ir escalando su ataque o intrusión.

Dentro de los hackers hay subespecies, las cuales se describen a continuación:

- EL hacker de sombrero blanco es el administrador de sistemas o el experto de seguridad, que tiene una ética muy alta y utiliza sus conocimientos para evitar actividades ilícitas.
- El hacker de sombrero negro, que algunos prefieren llamar craker, es quien disfruta de penetrar en los sistemas de seguridad y crear software dañino (malware).
- En contraste el hacker de sombrero gris, no se preocupa mucho por la ética, sino por realizar su trabajo, si necesita alguna información o herramienta y para ello requiere penetrar en un sistema de cómputo, lo hace, además disfruta poniendo a prueba su ingenio contra los sistemas de seguridad, sin malicia y difundiendo su conocimiento, lo que a la larga mejora la seguridad de los sistemas.

Insider

Intruso que es un usuario interno, es extremadamente más peligroso que un atacante externo. Así pues, asumimos que la intrusión se puede producir con un alto porcentaje de éxito si alguien desde el interior presta su ayuda. La evolución de técnicas existentes, como la emisión de datos a través de protocolos de salida permitidos por proxies y firewalls, dificultan la detección de este tipo de acciones. Para finalizar este punto, cabe mencionar uno de los riesgos más obvios: los antiguos empleados de la corporación.

Cracker

Este acrónimo surgió por el año 1985, y fue inventado por los propios hackers para diferenciar a un intruso que fisgoneaba en una computadora con otro que creaba un virus dañino o copiaba un software. Un cracker se dedica única y exclusivamente a dañar sistemas, ya sean estos electrónicos o informáticos. Por esa razón se les denomina crackers, ya que quebrantan los sistemas de seguridad.

Bucaneros

Estos tipos no saben nada del hacking, pero se las arreglan para contactar con ellos. Son tipos con bastante dinero en busca de negocio. Ven en los hackers una fuente de ingresos y se dedican continuamente en ir detrás de ellos.

Lamer

Esta definición es asignada a un principiante que sólo desea recopilar información y copiarla. Son rápidamente expulsados por los verdaderos intrusos de las redes porque es considerado un charlatán y un loco. Son peligrosos ya que no saben nada y creen tener el mundo en sus manos. Si cae en sus manos un programa generador de virus, éste, lo suelta en la red sólo por molestar y sobresalir. Un lamer rastrea en la basura cibernética de la red, se baja todos los programas y los prueba todos. Es el típico tipo que perjudica a los usuarios de redes, enviando bombas lógicas o virus por la red y ejecuta programas creados por otros.

Copy-hackers

Estos individuos poseen conocimientos técnicos informáticos o electrónicos y habilidad psíquica. Estos tipos, más cercanos a espías, son individuos sin escrúpulos y se dedican a cazar a los buenos hackers para hacerse muy buen amigo de ellos y prometerle cosas buenas a cambio de información. Después, ponen en práctica todo lo que han podido obtener y logran hacer el trabajo verdadero del primer hacker. Cuando lo consiguen ofrecen el sistema y sus servicios a los bucaneros, quienes les pagarán una buena suma de dinero a cambio de lo que quieren. Este proceso es hábilmente seguido en el mundo de la codificación de la televisión vía satélite.

Gurús

Son los maestros y enseñan a los futuros hackers que tienen amplia experiencia sobre los sistemas informáticos o electrónicos y están para enseñar o sacar de cualquier duda. Es como una especie de profesor que tiene a sus espaldas unas cuantas medallitas que lo identifican como el mejor de su serie. El gurú no está activo, pero absorbe conocimientos ya que sigue practicando, pero para conocimiento propio y sólo enseña las técnicas más básicas.

Phreakers

Son tipos con conocimientos de telefonía insuperables. Conocen a fondo los sistemas telefónicos, incluso más que los propios técnicos de las compañías telefónicas.

Sneackers

Estos individuos son tipos que en algún tiempo ocuparon sus conocimientos para hacer daño, y que actualmente emplean dichos conocimientos para proteger los sistemas y las redes. Se pueden considerar crackers reformados.

Script-kiddies

Éstos representan el nivel jerárquico más bajo del hacking y se caracterizan por ejecutar programas llamados exploits sin conocer propiamente su funcionamiento. Los hackers son quienes realmente escriben estos exploits y muchos los ponen “para su estudio” a disposición de los usuarios de Internet.

Muchas personas consideran que, en la práctica, es muy difícil seguir esta clasificación y poder distinguir a unos personajes de otros. En muchos casos, las líneas divisorias pueden tornarse difusas. Por ejemplo: ¿Cuándo se convierte un cracker en excracker? ¿Cómo asegurarse que ya no usará sus conocimientos de forma maliciosa? ¿Realmente se habrá reformado? o por ejemplo: ¿Cuál es la diferencia entre un hacker y un experto en seguridad? ¿Acaso, al final, no hacen actividades similares? En fin, esta clasificación puede suscitar largas discusiones dignas de todo un tratado, el cual queda fuera del objetivo de este trabajo.

3.4. Virus

Un virus es un programa de software que se adjunta a otro archivo o programa, en memoria o en disco, no es un programa independiente y no funciona por sí solo, de forma que debe parasitar a otros programas para poder funcionar, así que al ejecutar el programa infectado también se ejecuta el virus; generalmente esta ejecución implica la copia del código viral (o una modificación del mismo) en otros programas.

Los virus pueden tener varios objetivos, van desde el despliegue de mensajes ocasionando únicamente molestias pero sin dañar a la información, hasta producir el mal funcionamiento del equipo causado por borrar o alterar información.

Aunque la mayoría de los virus se han popularizado en el mundo de las pc´s, los sistemas multiusuarios bajo Unix están igualmente expuestos.

3.4.1. Virus de sector de arranque (boot sector viruses)

Fue el primer virus en ser creado. Se esconde en el código ejecutable del sector de arranque de los discos de inicio, lo que significa que para infectar una computadora había que iniciarla desde un diskette de arranque infectado. Hace quince años aproximadamente, iniciar la

computadora desde un diskette de inicio era algo bastante usual, lo que significó que los virus se distribuían rápidamente, antes de que la gente se diera cuenta de lo que estaba ocurriendo. Este tipo de virus (y también los demás) deben dejar una marca digital para evitar que se infecte repetidamente el mismo objetivo. Es esta firma la que permite los antivirus detecten la infección.

3.4.2. Virus de archivos ejecutables

El virus de archivos ejecutables se adjunta a archivos del tipo .exe o .com. Algunos virus buscaban programas que formaran parte específicamente del sistema operativo y por ello se ejecutaban cada vez que se encendía la computadora, aumentando así sus posibilidades de una exitosa propagación del mismo virus. Existían unas cuantas maneras de adjuntar un virus a un archivo ejecutable, aunque algunas funcionaban mejor que otras. El método más simple y menos sutil era la de sobrescribir la primera parte del archivo con código de virus, lo que significaba que el virus se ejecutaba, pero el resto del programa no funcionaba correctamente. Esto era una clara señal que había una infección, especialmente si el programa era una parte esencial del sistema operativo.

3.4.3. Virus residentes en memoria (terminate and stay resident, TSR)

La sigla TSR viene del DOS y significa que un programa se carga en memoria y queda residente en segundo plano permitiendo a la computadora trabajar en primer plano de manera normal. Estos virus más avanzados podían interceptar llamadas al sistema operativo (system calls) que podrían exponer su existencia y respondían con respuestas falsas, evitando de esta manera su descubrimiento y/o limpieza. Otros se adjuntaban al comando ‘dir’ e infectaban todas las aplicaciones listadas en el directorio. Algunos hasta detenían o borraban los programas antivirus.

3.4.4. Virus polimórfico

Los primeros virus eran bastante fáciles de detectar, ya que poseían una cierta firma digital dentro de ellos para evitar una reinfección o simplemente porque poseían una estructura específica que permitía su detección. Luego aparecieron los virus polimórficos, de poli (muchas) mórficos (formas). Estos virus se modificaban cada vez que se replicaban, reordenando su código, cambiando de cifrado, generando un nuevo código que parecía totalmente distinto al original.

Esto creó un gran problema, ya que las firmas a detectar eran cada vez más pequeñas y los más avanzados sólo se detectaban mediante algoritmos que comparaban combinaciones.

Esto se acentuó por la aparición de kits de generación de virus polimórficos que se distribuyeron en la comunidad de autores de virus que permitían generar cualquier virus como polimórfico.

3.4.5. Virus de macro

Los virus de macro hacen uso de la habilidad de muchos programas de ejecutar código. Los programas como Word y Excel poseen versiones de lenguaje de programación Visual Basic limitados en funciones, pero muy poderosos. Esto permite la automatización de tareas repetitivas y la configuración automática de ciertos parámetros. Estos lenguajes de macros se utilizan maliciosamente para adicionar código viral a los documentos, los cuales copiarán el código viral a otros documentos, lo que resulta en una propagación del virus. Aunque Microsoft ha desactivado esa propiedad en las nuevas versiones, outlook (el programa de correo) ejecutaba cierto tipo de código adicionado a los mensajes de correo de manera automática apenas eran abiertos. Eso significaba que los virus se propagaban rápidamente enviándose a toda la lista de direcciones de correo que había en la computadora infectada.

3.4.6. Gusanos

Son programas independientes capaces de autorreplicarse de un sistema a otro a través de la red; en las máquinas que se instala, produce enormes sobrecargas de procesamiento, que reducen la disponibilidad de los sistemas afectados.

El término gusano, hace referencia a programas completos que pueden funcionar por sí solos capaces de viajar a través de redes de computadoras para realizar cualquier actividad una vez alcanzada una máquina; aunque esta actividad no tiene por qué entrañar peligro, los gusanos pueden instalar en el sistema alcanzado un virus, atacar a este sistema como haría un intruso, o simplemente consumir excesivas cantidades de ancho de banda en la red afectada. Los gusanos son una de las amenazas que potencialmente puede causar mayores daños; no se debe olvidar que el mayor incidente de seguridad de la historia de Unix e Internet fue a causa de un gusano, el famoso “Gusano de Internet” en 1988.

3.4.7. Conejos

Los conejos o bacterias son programas que de manera directa no dañan al sistema, sino que se limitan a reproducirse, generalmente de forma exponencial, hasta que la cantidad de recursos

consumidos (procesador, memoria, disco) se convierte en una negación de servicio para el sistema afectado.

3.4.8. Caballos de Troya

Programa que contiene código malicioso y dañino que parece un programa o archivo inofensivo (no se distribuye automáticamente).

En el libro VIII de *La Odisea* se cuenta la historia de que los griegos, tras mucho tiempo de asedio a la ciudad de Troya, decidieron construir un gran caballo de madera en cuyo interior se escondieron unos cuantos soldados; el resto del ejército griego abandonó el asedio dejando allí el caballo, y al darse cuenta de que el sitio a su ciudad había acabado, los troyanos salieron a inspeccionar ese gran caballo de madera. Lo tomaron como una muestra de su victoria y lo introdujeron tras las murallas de la ciudad sin darse cuenta de lo que realmente había en él. Cuando los troyanos estaban celebrando el fin del asedio, del interior del caballo salieron los soldados griegos, que abrieron las puertas de la ciudad al resto de su ejército (que había vuelto al lugar) y pudieron de esta forma conquistar la ciudad de Troya.

De la misma forma que el antiguo caballo de Troya de la mitología griega escondía en su interior algo que los troyanos desconocían, y que tenía una función muy diferente a la que ellos pensaban, un troyano o caballo de Troya actual es un programa que aparentemente realiza una función útil para quien lo ejecuta, pero que en realidad (o aparte) realiza una función que el usuario desconoce, generalmente dañina.

Sin duda el ejemplo típico de troyano es el falso programa de *login*. Nada más encender una terminal de una máquina aparece el clásico mensaje `login` solicitando el nombre de usuario y contraseña, datos que con toda seguridad la persona que enciende este dispositivo tecleará para poder acceder al sistema. Pero, ¿qué sucedería si el programa que imprime el mensaje en pantalla es un troyano? Cualquier hacker puede crear un código que muestre un mensaje similar, guarde la información leída de teclado (el *login* y el *password*) e invoque después al programa `login` original; tras la primera lectura, se mostrará el también clásico mensaje *`Login incorrect'*, de forma que el usuario pensará que ha tecleado mal sus datos. Cuando el programa original se ejecute, se permitirá el acceso al sistema y ese usuario no habrá notado nada anormal, pero alguien acaba de registrar su *login* y su contraseña.

3.4.9. Spyware

Código que se instala clandestinamente casi siempre desde sitios de Internet que un usuario puede visitar. Una vez instalado buscará en la computadora información que considere de valor;

esto podrá ser estadísticas de la utilización de Internet o el número de tarjeta de crédito. Algunas versiones de spyware inadvertidamente se dan a conocer porque hacen aparecer avisos en el escritorio de la pc de manera constante.

3.5. Ataques

El principio, los ataques involucraban poca sofisticación técnica. Los insiders (empleados inconformes o personas externas con acceso a sistemas dentro de la empresa) utilizaban sus permisos para alterar archivos o registros. Los outsiders (personas que atacan desde afuera de la ubicación física de la organización) ingresaban a la red simplemente averiguando un password válido.

A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar "agujeros" en el diseño, configuración y operación de los sistemas. Esto permitió a los nuevos atacantes tomar control de sistemas completos, produciendo verdaderos desastres que en muchos casos llevó a la desaparición de aquellas organizaciones o empresas con altísimo grado de dependencia tecnológica (bancos, servicios automatizados, etc.).

Estos nuevos métodos de ataque han sido automatizados, por lo que en muchos casos sólo se necesita conocimiento técnico básico para realizarlos. El aprendiz de intruso tiene acceso ahora a numerosos programas y scripts de hacker bulletin boards y web sites, donde además encuentra todas las instrucciones para ejecutar ataques con las herramientas disponibles.

Los métodos de ataque están divididos en categorías generales que pueden estar relacionadas entre sí, ya que el uso de un método en una categoría permite el uso de otros métodos en otras. Por ejemplo: después de crackear un password, un intruso realiza un login como usuario legítimo para navegar entre los archivos y explotar vulnerabilidades del sistema. Eventualmente también, el atacante puede adquirir derechos a lugares que le permitan dejar virus u otras bombas lógicas para paralizar todo un sistema antes de huir.

3.5.1. Eavesdropping y packet sniffing

Muchas redes son vulnerables al eavesdropping o la pasiva intercepción (sin modificación) del tráfico de red. En Internet esto es realizado por packet sniffers, que son programas que monitorean los paquetes de red que están direccionados a la computadora donde están instalados. El sniffer puede ser colocado tanto en una estación de trabajo conectada a red, como a un equipo router o a un gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías. Existen kits disponibles para facilitar su instalación.

Este método es muy utilizado para capturar loginIDs y passwords de usuarios, que generalmente viajan claros (sin cifrar) al ingresar a sistemas de acceso remoto (RAS por sus siglas en inglés). También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mail, entrantes y salientes. El análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones e individuos.

3.5.2. Snooping y downloading

Los ataques de esta categoría tienen el mismo objetivo que el sniffing, obtener la información sin modificarla. Sin embargo los métodos son diferentes. Además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de e-mail y otra información guardada, realizando en la mayoría de los casos un downloading de esa información a su propia computadora.

El snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software. Los casos más famosos de este tipo de ataques fueron: el robo de un archivo con más de 1,700 números de tarjetas de crédito desde una compañía de música mundialmente famosa, y la difusión ilegal de reportes oficiales reservados de la Organización de las Naciones Unidas, acerca de la violación de derechos humanos en algunos países europeos en estado de guerra.

3.5.3. Tampering o data diddling

Esta categoría se refiere a la modificación desautorizada a los datos, o al software instalado en un sistema, incluyendo borrado de archivos. Este tipo de ataques son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de ejecutar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema en forma deliberada. O aún si no hubo intenciones de ello, el administrador posiblemente necesite dar de baja por horas o días hasta verificar y tratar de recuperar aquella información que ha sido alterada o borrada.

Como siempre, esto puede ser realizado por insiders u outsiders, generalmente con el propósito de fraude o dejar fuera de servicio un competidor.

Son innumerables los casos de este tipo como empleados (o externos) bancarios que crean falsas cuentas para derivar fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes o contribuyentes que pagan para que se les anule la deuda por impuestos en el sistema municipal. Múltiples web sites han sido víctimas del cambio de sus páginas por

imágenes terroristas o humorísticas, o el reemplazo de versiones de software para download por otros con el mismo nombre, pero que incorporan código malicioso (virus, troyanos).

La utilización de programas troyanos se encuentra dentro de esta categoría, y refiere a falsas versiones de un software con el objetivo de averiguar información, borrar archivos y hasta tomar control remoto de una computadora a través de Internet como el caso de Back Orifice y NetBus, de reciente aparición.

3.5.4. Spoofing

Esta técnica es utilizada para actuar en nombre de otros usuarios, usualmente para realizar tareas de snoofing o tampering. Una forma común de spoofing es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él, como puede ser el envío de falsos e-mails. El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza éste para entrar en otro, y en otro. Este proceso, llamado looping, tiene la finalidad de evaporar la identificación y la ubicación del atacante. El camino tomado desde el origen hasta el destino puede tener muchas estaciones, que exceden obviamente los límites de un país. Otra consecuencia del looping es que una compañía o gobierno pueden suponer que están siendo atacados por un competidor o una agencia de gobierno extranjera, cuando en realidad está siendo atacado por un insider, o por un estudiante a miles de kilómetros de distancia, pero que ha tomado la identidad de otros.

El looping hace su investigación casi imposible, ya que el investigador debe contar con la colaboración de cada administrador de cada red utilizada en la ruta, que pueden ser de distintas jurisdicciones.

Los protocolos de red también son vulnerables al spoofing. Con el IP spoofing, el atacante genera paquetes de Internet con una dirección de red falsa en el campo from, pero que es aceptada por el destinatario del paquete.

El envío de falsos e-mails es otra forma de spoofing permitida por las redes. Aquí el atacante envía a nombre de otra persona e-mails con otros objetivos. Tal fue el caso de una universidad en USA que en 1998 debió reprogramar una fecha completa de exámenes ya que alguien en nombre de la secretaría había cancelado la fecha verdadera y enviado el mensaje a todos los estudiantes.

Muchos ataques de este tipo comienzan con ingeniería social, la cual se lleva a cabo normalmente por hackers que se hacen pasar por personal de sistemas, quienes les hacen unas cuantas preguntas ya sea para obtener su cuenta de acceso y/o su password; la falta de cultura por parte de los usuarios es la vulnerabilidad que explotan estas personas.

3.5.5. Jamming o flooding

Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más puede utilizarla.

Muchos ISPs (proveedores de Internet) han sufrido bajas temporales del servicio por ataques que explotan el protocolo TCP. Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP (o sea que este ataque involucra también spoofing). El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas.

Muchos host de Internet han sido dados de baja por el "ping de la muerte", una versión trampa del comando ping. Mientras que el ping normal simplemente verifica si un sistema está enlazado a la red, el ping de la muerte causa el reboot o el apagado instantáneo del equipo.

Otra acción común es la de enviar millares de e-mails sin sentido a todos los usuarios posibles en forma continua, saturando los distintos servers destino.

3.5.6. Ping mortal

Algunos ataques eliminan el blanco en lugar de inundarlo con trabajo. Un ejemplo de este tipo es el ping mortal, un paquete ping ilícitamente enorme, que hace que el equipo de destino deje de responder. Muchas implementaciones de routers, la mayoría de los Unix y todas las versiones de Windows se mostraron vulnerables a este ataque cuando se lo descubrió por primera vez hace un par de años. A pesar de que los vendedores lanzaron parches de inmediato, hay todavía cantidades significativas de hosts "no corregidos" en las redes de producción (en especial, las que corren bajo Windows 95).

TCP/IP permite un tamaño máximo de paquete de 64 kilobytes (KB, este máximo está dividido en piezas mucho más pequeñas a través de protocolos de capas más bajas, como Ethernet o token ring, pero dentro de una computadora, paquetes mucho más grandes son posibles). Para lidiar con un paquete de 64 KB, la cola TCP/IP asigna un buffer en memoria de 64 KB. Al recibir una cantidad ilícitamente grande de información, como un ping mortal, el buffer del equipo de destino se desborda y el sistema deja de responder.

3.5.7. Land

Otro método para que un equipo deje de responder es el denominado land attack, en el que se genera un paquete con direcciones IP y puertos de fuente y destino idénticos. Existen diferentes

variantes para este ataque. Una de ellas usa idénticas direcciones IP de fuente y destino, pero no números de puertos.

En pruebas a ruteadores de diferentes marcas sólo algunos identificaron el tráfico correctamente como un land attack cuando ambas direcciones y números de puerto eran idénticos.

3.5.8. Supernuke

Un ataque característico de los equipos con Windows es el supernuke (llamado también a veces winnuke), que hace que los equipos que escuchan por el puerto UDP 139 dejen de responder. Netbios es un protocolo integral para todas las versiones en red de Windows. Para transportar Netbios por IP, Microsoft ideó el Windows Networking (Wins), un esquema que enlaza el tráfico Netbios a puertos TCP y UDP 137, 138 y 139. Al enviar a estos puertos fragmentos UDP, se pueden arruinar equipos Windows que no estén arreglados o disminuir la velocidad del equipo durante un largo tiempo.

3.5.9. Teardrop 2

Otra de las agresiones, data de fines de 1997. Al igual que el supernuke, los ataques Teardrop 2 afectan a fragmentos de paquetes. Algunas implementaciones de colas IP no vuelven a armar correctamente los fragmentos que se superponen, haciendo que el sistema deje de responder.

Windows NT 4.0 fue muy vulnerable a este ataque, hasta que Microsoft lanzó un parche en enero de 1998.

La estrategia de hacer respaldos y tener controles de acceso tanto físicos como lógicos garantizan que la información estará disponible para las personas autorizadas para ello, aún en caso de desastre y de esta forma le permitirá al negocio continuar con sus operaciones críticas aunque sea de forma reducida, la inversión que se requiere para implementar estos controles es mínima comparada con el costo que causaría el no tenerlos, ya que implica muchas horas de trabajo tratando de generar nuevamente toda la información que se deba tener para la operación normal de la empresa.

CAPÍTULO 4

CRIPTOGRAFÍA

Hasta hace pocos años la criptografía sólo resultaba interesante, para agencias de seguridad, gobiernos, grandes empresas y delincuentes. Sin embargo, en poco tiempo, debido al rápido crecimiento de las comunicaciones electrónicas, esta ciencia se ha convertido en un tema sugerente que llama la atención del público en general. Destaca especialmente el cambio que ha sufrido, durante el final del siglo pasado, la orientación de la investigación en criptografía, ya que ha pasado del tema clásico del cifrado y su seguridad, hacia los más actuales campos de las firmas digitales y los protocolos criptográficos. Dicha variación es una consecuencia inmediata del impacto de la informatización en la sociedad, que cada vez demanda más servicios telemáticos seguros.

Así, ante estas situaciones de peligro nacidas a raíz de los nuevos servicios, se hacen necesarias soluciones diferentes. En este capítulo se hace un recorrido por los aspectos más destacables de las facetas de la criptografía. Se reúnen aquí tanto los fundamentos de la base teórica y las descripciones de varios cifrados clásicos, como el análisis de los sistemas de clave secreta y de clave pública más difundidos actualmente. Se presta especial atención a las aplicaciones criptográficas de mayor relevancia, como son la firma digital y la identificación de usuarios para el control de accesos. Finalmente, se describen diversos protocolos criptográficos que permiten resolver en el mundo de las telecomunicaciones situaciones habituales tan simples como guardar un mensaje dentro de un sobre, y tan complejas como firmar un contrato electrónicamente.

4.1. Historia[1]

4.1.1. Criptología

La criptología es una ciencia que estudia los aspectos y contenidos de información en condiciones de secrecía.

Proviene del griego: *criptos* (oculto, secreto) y *logos* (tratado o estudio).

La criptología se divide en:

- Criptografía.
- Criptoanálisis.

[1] Gómez Cárdenas, Roberto. *Criptología*. Instituto Tecnológico de Estudios Superiores Monterrey. Sexta Edición. México. 2002. Página 3.

4.1.2. Criptografía

La criptografía es la técnica, ciencia o arte de la escritura secreta.

Proviene del griego: *criptos* (oculto, secreto) y *graphos* (escritura).

Es el conjunto de técnicas o procedimientos que alteran los símbolos de información sin alterar el contenido, convirtiendo a la información modificada en un conjunto de símbolos sin significado para las partes que no disponen de las técnicas. La Figura 4.1 muestra una clasificación de la escritura secreta.

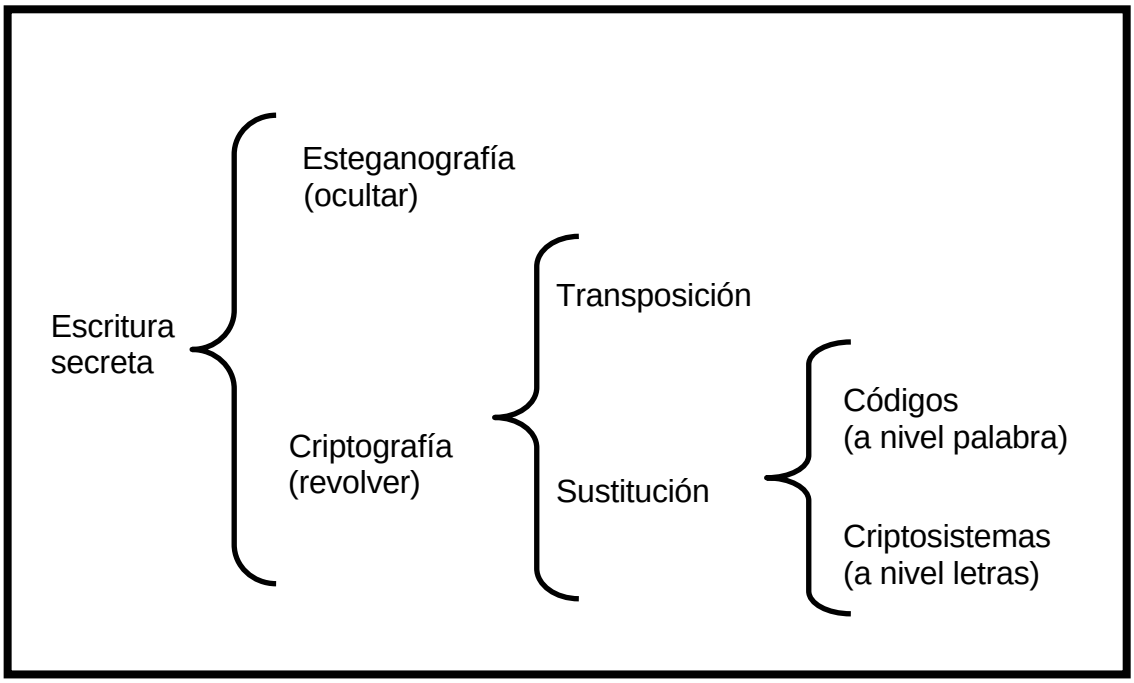


Figura 4.1 Clasificación de escritura secreta

4.1.3. Criptoanálisis

Metodologías y técnicas que permiten recuperar la información que ha sido previamente tratada por un procedimiento criptográfico, sin conocer “a priori” la técnica utilizada para la criptografía.

El principio básico de la criptografía es mantener la privacidad de la comunicación entre dos personas alterando el mensaje original de modo que sea incomprensible a toda persona distinta del destinatario, a esto se debe la autenticación, en la cual la firma del mensaje se utiliza de modo que un tercero no pueda hacerse pasar por el emisor. A la transformación del mensaje original en el mensaje cifrado (criptograma) se le llama cifrado, y a la inversa, el paso del criptograma al mensaje original se le llama descifrado; estos pasos se realizan mediante un conjunto de reglas preestablecidas entre los que se comunican, a la que se le nombra clave. El criptoanálisis es el conjunto de técnicas que intenta encontrar la clave utilizada entre dos que se

comunican, develando así el secreto de su mensaje. La criptología engloba tanto a la criptografía como al criptoanálisis; el éxito de un criptoanalista supone el fracaso de un criptógrafo y viceversa.

Un criptosistema es el conjunto de procedimientos que garantizan la seguridad de la información y utilizan técnicas criptográficas.

El término en inglés es cipher.

El elemento fundamental de un criptosistema es la **"llave"**.

En algunas referencias a la llave se le conoce como clave.

4.1.4. Objetivos de la criptografía

Mantener la confidencialidad del mensaje:

- La información contenida en el mensaje permanece secreta.

Garantizar la autenticidad tanto del mensaje como del par remitente/destinatario:

- El mensaje recibido ha de ser realmente el enviado.
- El remitente y destinatario, han de ser realmente quienes dicen ser y no remitentes y/o destinatarios fraudulentos.

4.1.5. Clasificación seguridad criptográfica

Seguridad incondicional (teórica).

- Sistema seguro frente a un atacante con tiempo y recursos computacionales ilimitados.

Seguridad computacional (práctica).

- El sistema es seguro frente a un atacante con tiempo y recursos computacionales limitados.

Seguridad probable.

- No se puede demostrar su integridad, pero el sistema no ha sido violado.
- Todos los demás sistemas, seguros en tanto que el enemigo carece de medios para atacarlos.

4.1.6. Criptografía y seguridad

En la práctica, la seguridad que ofrece un criptosistema consiste en mostrar que cualquier ataque que tiene una probabilidad de romper la llave requiere de una cantidad infinita de computación.

Un sistema criptográfico se dice inseguro cuando los contenidos de cifrado pueden ser descifrados en un tiempo relativamente corto. Lo que se pretende es que en caso de ser

descifrados se lleve años el proceso, de manera que ya no sea útil para el atacante o que la información descifrada ya no represente una pérdida al dueño de la misma.

4.2. Procedimientos clásicos de cifrado

4.2.1. Transposición

Consiste en “barajar” los símbolos del mensaje original colocándolos en un orden distinto, de manera que el criptograma contenga los mismos elementos del texto claro, pero colocados de tal forma, que resulten incomprensibles.

El método de transposición consiste en una reordenación de los símbolos del mensaje original de modo que éste resulte ilegible. Si un mensaje consta de n letras se podrá transponer de n! (n factorial) formas. La reordenación se puede realizar desde un modo simple: escribiendo el mensaje letra a letra pero al revés, o utilizando complicados esquemas matriciales.

Los métodos básicos de sustitución y transposición se pueden combinar para formar métodos mixtos más seguros ante un ataque criptográfico. Los métodos clásicos han demostrado su ineficacia ante la potencia de cálculo de las modernas computadoras, por lo que no se usan en aplicaciones que necesiten una mínima seguridad, sistemas de cifrado como los usados por algunos procesadores para cifrar textos han sido rápidamente criptoanalizados. El estudio de algoritmos seguros de cifrado es, hoy en día, un terreno fecundo para la investigación en distintas ramas de la ciencia.

Ejemplos de transposición:

- La escítala lacedemonia o skytale staff, Figuras 4.2 y 4.3.
- Transposición en reversa.
- Transposición por columnas.
- Transposición rail fence.
- Transposición redefence.
- Criptosistema Nihilist.

4.2.2. La escítala lacedemonia o skytale staff

Utilizada en el siglo V. A.C. por el pueblo griego lacedemonios.

Consistía de dos varas idénticas, alrededor de una de ellas se envolvía una tira de pergamino.

El mensaje se escribía a lo largo del bastón, se retiraba la cinta y se enviaba.

El destinatario poseía la segunda vara,

La cinta era una sucesión de símbolos de alfabeto griego colocados en un orden no entendible.

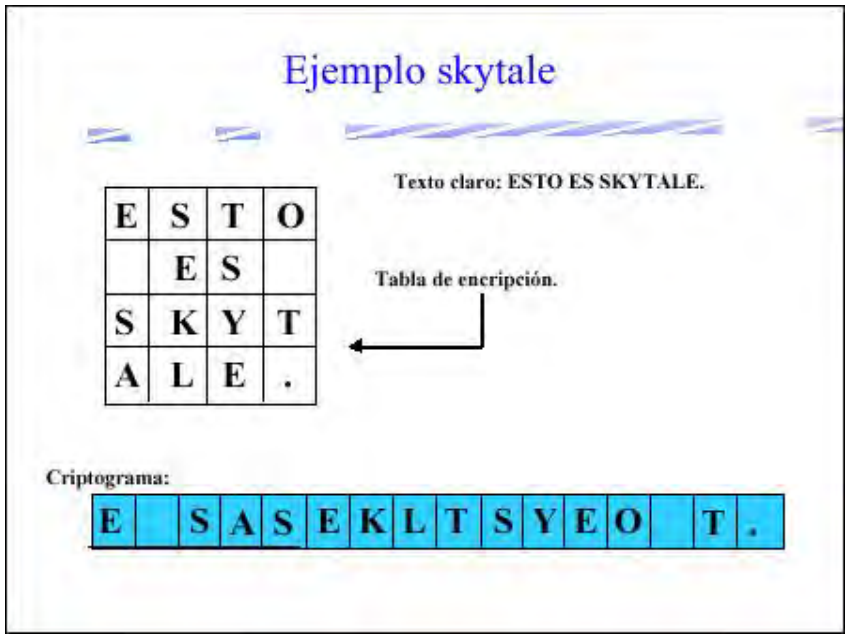


Figura 4.2 Skytale staff

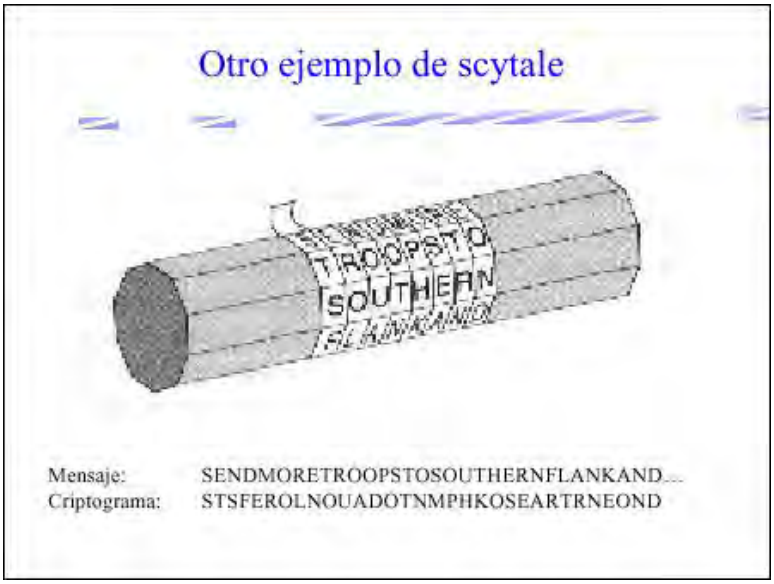


Figura 4.3 Scytale lacedemonia

4.2.3. Transposición en reversa

En la transposición en reversa el criptograma se escribe a partir del último caracter del texto claro hasta el primero.

Texto claro: Esto es una prueba

Criptograma: **abeurp anu se otsE**

4.2.4. Transposición por columnas

Escoger una palabra: *medical*

Numerar las letras en orden alfabético, esto es, a la letra a le corresponde el número 1, como la palabra medical no incluye la letra b entonces a la letra c le corresponde el número 2 a la letra d el número 3 y así sucesivamente, como lo muestra la Tabla 4.1.

m	**e**	**d**	**i**	**c**	**a**	**l**
7	**4**	**3**	**5**	**2**	**1**	**6**

Tabla 4.1. Numeración de letras para la palabra clave *medical*

Mensaje en claro: ***now is the time for all good men to come to the aid of their party***

Se forma una tabla en la que la longitud es la palabra clave, y después se escribe el mensaje abajo de la palabra utilizando varios renglones para ello, si al final no se utiliza toda la tabla, ésta se completa con caracteres de relleno (pueden ser aleatorios), Tabla 4.2.

m	**e**	**d**	**i**	**c**	**a**	**l**
7	**4**	**3**	**5**	**2**	**1**	**6**
N	o	w	i	s	t	h
E	t	i	m	e	f	o
R	a	l	l	g	o	o
D	m	e	n	t	o	c
O	m	e	t	o	t	h
E	a	i	d	o	f	t
H	e	i	r	p	a	r
T	y	***q***	***r***	***x***	***z***	***y***

Tabla 4.2. Mensaje escrito debajo de la palabra clave

El criptograma resulta de la lectura de las columnas, poniéndolas como renglones, empezando con la que tiene el menor número de llave, que en este ejemplo la primera es la que está debajo de la letra a, la segunda es la que está debajo de la letra c, la tercera es la que está debajo de la letra d, y así sucesivamente, al final se obtiene lo que se muestra a continuación en la Tabla 4.3.

1	tfootfaz
2	segtoopx
3	wileeiiq
4	otammaey
5	imlntdr
6	hoochtry
7	nerdoeht

Tabla 4.3. Intercambio de columnas por renglones y ordenados por su número

Finalmente el criptograma queda de la forma siguiente:

Tfootfazsegtoopxwileeiiqotammaeyimlntdrhoochtrynerdoeht

4.2.5. Transposición rail fence

El texto claro es escrito hacia abajo como una secuencia de diagonales y es leído como una secuencia de renglones.

Por ejemplo:

- Texto claro: *meet me after the toga party*
- Con un rail fence de profundidad dos, el cifrado da como resultado la Tabla 4.4:

renglón 1	m	e	m	a	t	r	h	t	g	p	r	y
renglón 2	e	t	e	f	e	t	e	o	a	a	t	

Tabla 4.4 Ejemplo de transposición rail fence de profundidad dos

Para formar el criptograma se concatenan los renglones.

- Criptograma: **m e m a t r h t g p r y e t e f e t e o a a t**

4.2.6. Transposición redefence

Redefence es una variante de rail fence.

El orden de los renglones es definido usando una llave numérica.

Los números de la llave representan el orden de los renglones en el criptosistema rail fence Tabla 4.5.

Ejemplo:

Texto claro: *ESTO ES UNA PRUEBA*

Llave: 312

renglón 1	E	O	U	P	E
renglón 2	S	E	N	R	B
renglón 3	T	S	A	U	A

Tabla 4.5 Ejemplo de transposición redefence

Criptograma resultante de poner primero el renglón tres después el uno y al último el dos: ***TSAUAEOUPESENRB***

4.2.7. Criptosistema Nihilist

El criptosistema de transposición Nihilist fue inventado por los rusos nihilistas (tendencia anarquista de la sociedad rusa del siglo XIX).

Es necesaria una matriz de nxn. Figura 4.4

La misma longitud de la llave es aplicada a renglones y columnas.

Se numeran renglones y columnas de acuerdo a la llave.

Se escribe el texto claro dentro de la matriz y cada letra es pasada a una segunda matriz.

La segunda matriz contiene el criptograma.

El criptograma se forma de acuerdo a las coordenadas originales de la primera matriz, Figura 4.5

Ejemplo:

Texto claro: NIHILIST TRANSPOSITION

Llave: 23145

-	2	3	1	4	5
2	N	I	H	I	L
3	I	S	T	T	R
1	A	N	S	P	O
4	S	I	T	I	O
5	N	@	@	@	@

Figura 4.4 Matriz de 5x5 escribiendo el mensaje de forma ordenada

-	1	2	3	4	5
1	S	A	N	P	O
2	H	N	I	I	L
3	T	I	S	T	R
4	T	S	I	I	O
5	@	N	@	@	@

Figura 4.5 Ordenando las columnas y renglones de acuerdo a la llave, se obtiene el criptograma

Criptograma: SANPOHNIILTISTRTSIIO@N@@@

4.3. Sustitución

Consiste en establecer correspondencia entre las letras del alfabeto en el que está escrito el mensaje original y los elementos de otro conjunto que puede ser el mismo o distinto alfabeto.

El método de sustitución consiste básicamente en sustituir los caracteres del mensaje inicial por otros; los nuevos caracteres pueden ser de cualquier tipo: letras, símbolos, dígitos, etc. Los caracteres iniciales siguen estando en el mismo orden, pero salvo que se conozca la equivalencia entre los nuevos caracteres y los antiguos, el mensaje es ilegible.

Se puede considerar dos tipos de sustitución:

Equivalencia entre alfabetos caracter a caracter.

Utilización de cifra o clave

1) Equivalencia entre alfabetos caracter a caracter. A cada letra del alfabeto ordinario se le hace corresponder un símbolo y el mensaje se cifra cambiando las letras iniciales por su equivalente, si a la letra A se le asigna el símbolo "@" en el mensaje cifrado se tendrá siempre @ en lugar de A.

2) Utilización de cifra o clave. Distinto del anterior porque una vez establecida la correspondencia entre alfabetos (que en este caso pueden ser el mismo) la asignación de caracteres se realiza teniendo en cuenta la posición del caracter en el mensaje y el dígito que le corresponde según la clave, con un ejemplo quedará esto bastante más claro.

Sea el mensaje "SECRETO" y la cifra "23" el mensaje cifrado se consigue (estamos utilizando el mismo alfabeto) adelantando dos letras la primera que se encuentre, tres la segunda, dos la tercera, tres la cuarta y así sucesivamente, el mensaje cifrado será pues: "UHEUGWQ", como se ve la letra "e" del mensaje inicial aparece una vez como h y otra como

g, ya no hay una correspondencia uno a uno entre el alfabeto inicial y los símbolos del mensaje cifrado. Este método se conoce con el nombre Vigenére.

Para descifrar un mensaje cifrado se debe (en principio) conocer la correspondencia entre alfabetos y en su caso conocer también la clave.

4.3.1. Primer criptosistema militar

El primer documento de un criptosistema de sustitución para usos militares aparece en las Guerras Gálicas de Julio César.

César describe cómo enviar un mensaje a Cicero, que estaba sitiado y a punto de rendirse.

El criptosistema reemplazaba letras romanas con letras griegas.

El criptosistema de César consiste en sustituir la primera letra del alfabeto A, por la cuarta D; la segunda, B, por la quinta E, etc.

También conocido como *Ceaser shift cipher*.

Dos alfabetos:

- Alfabeto texto plano/claro: el alfabeto usado para escribir el mensaje original (texto claro).
- Alfabeto criptosistema (o de cifrado): las letras que sustituyen a las letras del alfabeto texto claro.

Otras características

Término matemático: $Yi = Xi \oplus Zi \pmod{26}$

Recuperación del mensaje:

- Se suma nuevamente símbolo a símbolo el criptograma con la inversa de la llave módulo 26.

El proceso es el siguiente, todas las letras en el mensaje original sufren un “corrimiento” de tres lugares respecto del que les corresponde de acuerdo al alfabeto, en este caso a la letra V le corresponde la letra Y, a la E le corresponde la H, a la N la Q, a la I la L, a la D la G, y a la C la F.

Sustituyendo el mensaje VENI VIDI VICI por sus correspondencias queda entonces YHQL YLGL YLFL, como se indica en la Tabla 4.6.

Mensaje:	VENI	VIDI	VICI
Llave:	DDDD	DDDD	DDDD
Criptograma:	YHQL	YLGL	YLFL

Tabla 4.6 Incluye mensaje, llave y criptograma

4.4. Criptosistemas monoalfabéticos

Administradores árabes usaban criptosistemas parecidos al de César.

También usaban criptosistemas que contenían otros tipos de símbolos:

- "a" puede ser reemplazada por "#"
- "b" puede ser reemplazada por "+"
- Un criptosistema de sustitución monoalfabético es el nombre que se le da a cualquier criptosistema en el cual el alfabeto del criptosistema consiste de letras o símbolos, o una combinación de los dos.

Otros criptosistemas monoalfabéticos

- Polybius square
- Checker board

4.4.1. Criptosistema de Polybius

Polybius era un escritor anciano griego que propuso sustituir las letras con números de dos dígitos.

Alfabeto es escrito en una matriz de 5 x 5 con los renglones y columnas numeradas como se muestra en la Figura 4.6

-	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Figura 4.6 Alfabeto ordenado en una matriz de 5 x 5

4.4.2. Ejemplo Polybius square

Para cifrar se debe sustituir cada letra con las coordenadas de la letra en la matriz, Figura 4.7, indicando primero el renglón y después la columna.

Por ejemplo:

F = 21

-	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Figura 4.7 Obteniendo las coordenadas de F en el alfabeto ordenado en una matriz de 5 x 5

Cifrar RENACIMIENTO = 42153311132432241533443 4.

Es más un código que un criptosistema.

Fue usado para transmitir mensajes de larga distancia en la noche usando antorchas.

4.4.3. Checker board

Similar al criptosistema de Polybius square.

La llave está construida por tres palabras.

Dos están en la columna y renglón de la matriz de 5 x 5 y forman las coordenadas de las entradas.

Estas palabras no pueden contener palabras similares para proporcionar coordenadas únicas.

Adentro de la matriz se escribe el alfabeto.

La tercera palabra se escribe adentro de la matriz y se rellenan las otras celdas con el resto del alfabeto.

El cifrado es igual que en Polybius.

Ejemplo utilizando la matriz mostrada en la Figura 4.8.

Columnas GROUP

Renglones WHITE

Primer renglón BOARD

Texto claro: PROTOCOL

Criptograma: TGWUWRTUWRHGWRIO

-	G	R	O	U	P
W	B	O	A	R	D
H	C	E	F	G	H
I	I/J	K	L	M	N
T	P	Q	S	T	U
E	V	W	X	Y	Z

Figura 4.8 Alfabeto ordenado en una matriz de 5 x 5

4.4.4. Criptología en Antiguo Testamento

Entre 800 y 1200, los árabes disfrutan de un período intelectual fuerte.

Europa se encontraba en la oscuridad, las únicas instituciones que motivaban el estudio de escritura secreta eran los monasterios.

Los monjes medievales estudiaban el Antiguo Testamento que contenía ejemplos de criptografía:

- Piezas de texto cifradas con atbash, un criptosistema hebreo de sustitución.

4.4.5. Criptosistema Tabas

Se toma cada letra, se calcula el número de lugares que lo separan de la primera letra del alfabeto.

Se reemplaza con una letra que se encuentra en la misma distancia del final del alfabeto.

En alfabeto español equivale a reemplazar:

- la letra "a", al principio alfabeto, por la letra "z".
- la letra "b" se cambia por la letra "y".

Se debe hacer una distinción entre código y cifrado, con un código se sustituye una palabra o frase del texto original por otra palabra o frase en el texto cifrado. La traducción a una lengua extranjera es un buen ejemplo de código, así se puede transformar el mensaje original "estoy contento" por ":-)" o "emprender la guerra" por "to go to war". El cifrado suele actuar antes sobre caracteres que sobre palabras, utilizando un sistema de signos en el que se transcriben números, letras o símbolos según una clave acordada; se puede, por ejemplo, cifrar el mensaje "emprender la guerra" escribiendo "merpneedlrgaeurra" donde la clave utilizada ha sido: Eliminar los espacios en blanco, tomar las letras de dos en dos y escribirlas cambiando su orden.

Se puede decir que la criptografía es tan antigua como la civilización, cuestiones militares, religiosas o comerciales impulsaron desde tiempos remotos el uso de escrituras secretas; los antiguos egipcios usaron métodos criptográficos, mientras el pueblo utilizaba la lengua demótica, los sacerdotes usaban la escritura hierática (jeroglífica) incomprensible para el resto. Los antiguos babilonios también utilizaron métodos criptográficos en su escritura cuneiforme. El primer caso claro de uso de métodos criptográficos se dio durante la guerra entre Atenas y Esparta, el cifrado se basaba en la alteración del mensaje original mediante la inclusión de símbolos innecesarios que desaparecían al enrollar la lista en un rodillo llamado escítala, el mensaje quedaba claro cuando se enrollaba la tira de papel alrededor de un rodillo (escítala) de longitud y grosor adecuados. Carlomagno sustituía ya las letras por símbolos extraños. En la época de los romanos se utilizó el cifrado César que consistía en cambiar cada letra por la que ocupaba tres lugares más adelante en el abecedario.

4.5. El uso de "Nulos"

4.5.1. Reforzando criptosistemas monoalfabéticos

Uno de las mejoras más simples fue la incorporación de nulos:

- Símbolos o letras que no sustituían ninguna letra del alfabeto de texto plano.
- Blancos que no representan nada.

Ejemplo:

- Sustituir cada letra del alfabeto claro por un número entre 1 y 99.
- Hay 73 números que no representan nada y pueden repartirse en el criptograma con frecuencias variadas.

4.5.2. Una variante de nulos

Los nulos pueden confundir cualquier ataque basado en un análisis de frecuencia.

Una variante es escribir incorrectamente algunas palabras antes de cifrar el mensaje, haciendo difícil aplicar el análisis de frecuencia, por ejemplo:

Thys haz thi ifetkkt off diztaughting thi ballans off frilwenseas

El destinatario, que conoce la llave, puede descifrar el mensaje y después interpretarlo.

4.5.3. El uso de codewords

Otra mejora consistía en introducir *codewords* o códigos de palabras

La sustitución se realiza a un nivel más alto: palabras.

Ejemplo utilizando el código de palabras mostrado en la Tabla 4.7.

Palabra	Código	Palabra	Código	Palabra	Código
asesinar	D	general	£	inmediatamente	08
correo	P	rey	±	Hoy	73
capturar	J	ministro	§	Noche	28
proteger	Z	príncipe	†	Mañana	43

Tabla 4.7 Código de palabras

Mensaje: asesinar al rey hoy

Criptograma: D-±-73

Ventajas y desventajas

Las palabras son menos vulnerables al análisis de frecuencias que las letras.

- En lugar de “atacar” 26 letras, se necesita identificar el valor de cientos o miles de palabras codificadas.
- El tamaño de la llave cambia.
- Es necesario definir un código de palabras, para los cientos o miles de palabras.
- El libro de código sería de cientos de páginas y podría verse como un diccionario.
- Las consecuencias de capturar el libro de códigos son devastadoras.
- Todas las comunicaciones serán transparentes.

4.6. Los nomenclators

Sistema de cifrado basado en sustitución de letras, que es usado para cifrar la mayor parte del mensaje, y una lista limitada de palabras codificadas, Figura 4.9.

Un nomenclator puede consistir de una página que contiene el alfabeto de cifrado y una segunda página que contiene una lista de palabras codificadas.

No es más seguro que un criptograma de letras, la parte principal del mensaje se descifra usando análisis de frecuencia y las palabras pueden adivinarse a partir del contexto.

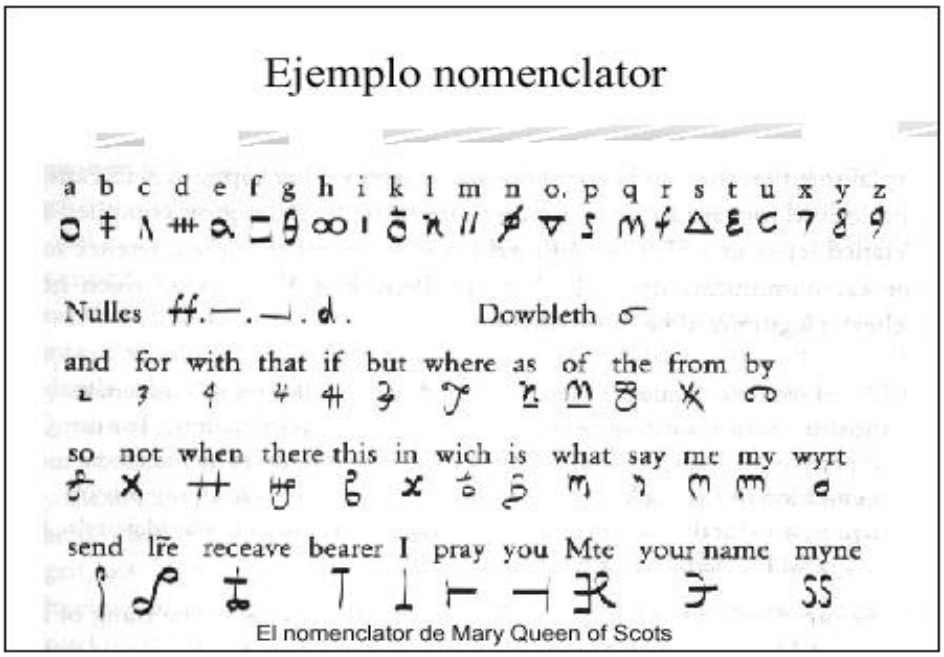


Figura 4.9 Ejemplo nomenclator

4.7. Código vs. criptosistema

Técnicamente un código es definido como una sustitución a nivel de palabras o frases.

Un criptosistema es definido como una sustitución a nivel de letras.

El término cifrar significa “revolver” un mensaje usando un criptograma y codificar involucra revolver usando un código.

El término descifrar significa “interpretar” un mensaje cifrado usando un criptograma y decodificar involucra interpretar usando un código.

Criptosistemas (di)poligráficos

Los símbolos del alfabeto en claro son cifrados en pares (dígrafos).

El análisis de frecuencia es más complicado.

El método de Playfair es un ejemplo de este tipo de criptosistemas poligráficos.

4.7.1. Criptosistema de Playfair

Sistema basado en una matriz de 5 x 5.

En el primer renglón de la matriz escribimos una llave.

- La llave sólo contiene letras diferentes.
- El resto de las celdas se llenarán con el resto de las letras en algún orden que sea fácil de recordar.
- El mensaje es cifrado tomando pares de letras.

4.7.2. Las reglas básicas de Playfair

Si ambas letras se encuentran en el mismo renglón:

- Usar las letras que se encuentran inmediatamente a la derecha de cada letra.
- Imaginar que el final de la derecha de cada renglón está unido con el final izquierdo.

Si ambas letras están en la misma columna, usar las letras que se encuentran inmediatamente abajo de cada letra.

- Imaginar que la parte baja de la columna está conectada con su parte superior.

Si dos letras se encuentran en diferentes renglones y diferentes columnas:

- Cada letra es reemplazada por la letra en el mismo renglón que se encuentra en la columna ocupada por la otra letra.

En el caso de dos letras iguales en un diagrama:

- Insertar una x entre ellas (choose = choxose)

Ejemplo de Playfair, Figura 4.10

	1	2	3	4	5
1	P	I/J	A	N	O
2	B	C	D	E	F
3	G	H	K	L	M
4	Q	R	S	T	U
5	V	W	X	Y	Z

Figura 4.10 Matriz de 5X5 con la llave piano en su primer renglón

Texto claro: Chipre

Llave: piano

Cifrado: ch se reemplaza por hr

ip se reemplaza por ai

re se reemplaza por tc

Criptograma: hraitc

4.7.3. Criptosistemas digráficos

Ventajas

La distribución de frecuencia es mucho más plana.

La variación se vuelve más grande ya que el alfabeto de cifrado es de 676 letras.

La longitud del criptograma es dos veces más corta que la del texto claro.

4.7.4. La propuesta de Alberti

La ejecución María Estuardo reina de Escocia fue una dramática ilustración de la debilidad de la sustitución monoalfabética.

Las intrigas y conspiraciones eran tan habituales durante el reinado de Isabel I de Inglaterra que el gobierno vio absolutamente necesario crear una policía secreta. Su organizador fue el ministro de la reina Sir Francis Walsingham. Durante un viaje a Italia Walsingham se dio perfecta cuenta de la importancia de la criptografía, de gran tradición en aquel país. Walsingham creó una red de agentes secretos que sólo en el continente contaba con 53 hombres.

Gracias a ellos, y a las artes criptoanalistas de un noble holandés, pudo descifrar una carta donde Don Juan de Austria revelaba sus deseos de conquistar Inglaterra. Entonces decidió poner bajo vigilancia a la católica María Estuardo, que llevaba detenida casi 20 años.

La mañana del 15 de octubre de 1586, la reina María Estuardo entraba en la sala de justicia del castillo de Fotheringhay, situado en las marismas de Anglia del Este. Se enfrentaba a una dura acusación: traición y conspirar para asesinar a la reina Isabel, su prima, para hacerse con el trono inglés.

Walsingham ya había conseguido que el resto de los conspiradores confesaran y, por supuesto, los había ejecutado. Ahora su objetivo era demostrar que María era el centro de la conspiración. Y tenía que demostrarlo sin que cupiera el menor resquicio para la duda. Ejecutarla con escasas pruebas comprometería al gobierno inglés.

Para muchos, María era la cabecilla simbólica, pero no estaba claro que estuviera al tanto de lo que maquinaban los conspiradores, un grupo de jóvenes nobles católicos ingleses. Por su parte, María estaba tranquila. Sus cartas sobre la conspiración estaban cifradas y pensaba que Walsingham no había podido romper la complicada cifra.

Pero el secretario de la reina contaba con un gran experto, Thomas Phelippes, un excelente lingüista (hablaba francés, italiano, español, latín y alemán) y uno de los mejores criptoanalistas de Europa e hizo honor a su fama pues fue capaz de descifrar una carta donde se proponía a María el asesinato de su prima. Walsingham esperó la respuesta de la

conspiradora y, el 17 de julio, María Estuardo firmó su sentencia de muerte: daba luz verde a la muerte de la reina.

- Los criptoanalistas ganaban batalla a los criptógrafos.
- Era necesario que los criptógrafos desarrollaran un criptosistema más fuerte.
- Por 1460 el florentino matemático Leon Battista Alberti, escribe un ensayo sobre lo que creía que era un nuevo criptosistema.

Alberti propone usar dos o más alfabetos de cifrado, como se muestra en las tablas 4.8, 4.9 y 4.10 alternándolos durante el cifrado, y confundiendo al posible criptoanalista.

Sin embargo, Alberti nunca pudo desarrollar su concepto y crear un criptograma a partir de sus ideas.

a	b	c	d	e	f	g	h	i	J	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

Tabla 4.8 Alfabeto claro

f	z	b	k	i	x	a	y	m	e	p	l	s	d	h	j	o	r	g	n	q	c	u	t	w	v

Tabla 4.9 Alfabeto de cifrado 1

g	o	x	b	f	w	t	h	q	i	l	a	p	z	j	d	e	s	v	y	c	r	k	u	h	n

Tabla 4.10 Alfabeto cifrado 2

4.7.5. La idea de Vigenére

Blaise de Vigenére es el que desarrolla el criptosistema hasta su forma final.

Utiliza 26 alfabetos de cifrado diferentes.

Primer paso: escribir la tabla Vigenére Tabla 4.11

- Cada línea es un alfabeto recorrido una letra con respecta a la línea anterior.
- Hasta arriba está el alfabeto en claro.
- Es posible utilizar cualquiera de los 26 alfabetos para cifrar el mensaje, en el orden que se desee.

La tabla de Vigenére

CLAVE *TEXTO EN CLARO*

	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	1	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	2	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	3	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	4	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	5	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	6	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	7	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	8	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	9	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	10	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	11	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	12	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	13	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
Ñ	14	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
O	15	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ
P	16	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O
Q	17	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P
R	18	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q
S	19	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R
T	20	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S
U	21	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T
V	22	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U
W	23	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V
X	24	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W
X	25	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X
Z	26	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y

Tabla 4.11 Tabla de Vigenére

El Criptosistema de Vigenére

La llave toma sucesivamente diferentes valores

Término matemático: Yi = Xi $\oplus$ Zi (mod 26)

A una misma letra en el texto claro le pueden corresponder diferentes letras en el texto cifrado.

Recuperación mensaje es análoga al procedimiento de César sólo que para cada letra se utiliza un renglón de la tabla de Vigenére diferente.

Ejemplo de decripción

***** Solamente las cuatro primeras letras del criptosistema.

A	B	C	D	E	F	G	H	I	J	K	**L**	M	N	**Ñ**	**O**	P	Q	R	S	T	U	V	W	**X**	Y	Z

Tabla 4.12 Alfabeto en secuencia normal

L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K

Tabla 4.13 Alfabeto iniciando con la letra L lo cual indica un corrimiento de 11 lugares

O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ

Tabla 4.14 Alfabeto iniciando con la letra O lo cual indica un corrimiento de 15 lugares

U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T

Tabla 4.15 Alfabeto iniciando con la letra U lo cual indica un corrimiento de 21 lugares

P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O

Tabla 4.16 Alfabeto iniciando con la letra P lo cual indica un corrimiento de 16 lugares

Criptograma: AOLXD JUJE PCTY IHT XSMHP

Llave: LOUPL OUPL OUPL OUP LOUPL

Mensaje: PARIS VAUT BIEN UNE MESSE

Para descifrar el mensaje se aplica el procedimiento siguiente:

La primera letra del criptograma A corresponde a la letra P en el alfabeto en texto claro, como se puede verificar en la Tabla 4.13, para la letra O del criptograma se utiliza la Tabla 4.14 y corresponde a la letra A en el alfabeto en texto claro, la letra L del criptograma utilizando la Tabla 4.15 corresponde la letra R en el alfabeto en texto claro, la letra X utilizando la Tabla 4.16 corresponde la letra I en el alfabeto en texto claro, la letra D del criptograma utilizando la Tabla 4.13 corresponde la letra S en el alfabeto en texto claro, y así se continúa, en el orden de la llave.

Características del criptosistema de Vigenére

Resistía a ataques de análisis de frecuencia.

- Las letras más comunes no se repiten con la misma frecuencia.
- Emisor y receptor se ponen de acuerdo en la llave.
- Palabra diccionario, combinación palabras o fabricarlas.
- Sistema pertenece a un criptosistema conocido como polialfabético.
- Utiliza varios alfabetos por mensaje.

Desventajas del criptosistema de Vigenére

El sistema no fue muy adoptado.

- No fue muy aceptado en los próximos dos siglos.
- La naturaleza polialfabética del criptosistema de Vigenére es lo que le da su fuerza, pero lo hace muy complicado de usar.
- El esfuerzo adicional para usarlo desalentó a mucha gente para emplearlo.
- Para muchos propósitos del siglo XVII, los criptosistemas monoalfabéticos fueron adecuados.

Atacando al criptosistema de Vigenére

Debido a su fortaleza al criptosistema de Vigenére se le conoció como *le chiffre indéchiffrable.*

- Los criptógrafos tenían una ventaja sobre los criptoanalistas (siglo XVI, XVII y XVIII).
- La figura más importante de los criptoanalistas del siglo XIX fue Charles Babbage (1791-1871).
- Primera persona que intenta desarrollar máquina universal para resolver problemas.
- Interesado en criptogramas desde muy pequeño.
- Se cree que en 1854 logra resolver el criptosistema de Vigenére.
- Planea escribir libro The Philosophy of Deciphering (no publicado).

4.7.6. Friedrich Wilhelm Kasiski

En la misma época que Babbage, su técnica fue descubierta por Friedrich Wilhelm Kasiski (1805-1881)

- Oficial prusiano retirado.
- En 1863 publica Die Geheimschriften und die Dechiffrir-kunst (Escritura secreta y el arte de decripción).
- La técnica se conoció como la prueba de Kasiski y la contribución de Babbage fue ignorada por mucho tiempo.

En la Edad Media, San Bernardino evitaba la regularidad de los signos (con lo que el criptoanálisis por el método de las frecuencias no era efectivo) sustituyendo letras por varios signos distintos, así tenía un símbolo para cada consonante, usaba tres signos distintos para cada una de las vocales y utilizaba signos sin ningún valor. El libro más antiguo del que se tiene constancia y que trata sobre criptografía es el Liber Zifrorum escrito por Cicco Simoneta en el siglo XIV. En el siglo XV destaca León Battista Alberti que es considerado por muchos el

padre de la criptología; crea la primera máquina de criptografía que consiste en dos discos concéntricos que giran independientes consiguiendo con cada giro un alfabeto de transposición.

En el siglo XVI, Blaise de Vigenére publica Traicté des Chiffres donde recoge los distintos métodos utilizados en su época, el método Vigenére es un método clásico de cifrado por sustitución que utiliza una clave. Carlos I de Inglaterra usó en el siglo XVII códigos de sustitución silábica. Napoleón, en sus campañas militares y en los escritos diplomáticos, usó los llamados métodos Richelieu y Rossignol y para evitar la regularidad de los símbolos asignaba números a grupos de una o más letras.

En el siglo XIX se utiliza ampliamente el método de transposición, consistente en la reordenación según distintos criterios de los símbolos del mensaje. Kerckhoffs escribe el libro "La criptografía militar" en las que da las reglas que debe cumplir un buen sistema criptográfico. En la Primera Guerra Mundial los alemanes usaron el sistema denominado ADFGX en el que a cada combinación de dos letras del grupo ADFGX se le hace corresponder una letra del alfabeto y a la que posteriormente se le hacía una transposición en bloques de longitud 20. El presidente americano Jefferson diseño un cilindro formado por varios discos que se utilizaba como máquina criptográfica. El mayor desarrollo de la criptografía se dio en el periodo de entreguerras por la necesidad de establecer comunicaciones militares y diplomáticas seguras. En 1940 se construyó la máquina Hagelin C-48 consistente en seis volantes unidos por el eje y con distinto número de dientes. En la Segunda Guerra Mundial se construyó por parte alemana la máquina Enigma, Figura 4.11, que se basaba en un perfeccionamiento del cilindro de Jefferson, pero la máquina británica Colossus consiguió descifrar los mensajes cifrados con Enigma. Los americanos construyeron la máquina Magic utilizada para descifrar el código púrpura japonés; los americanos a su vez usaron a los indios navajos con su difícil lenguaje para la transmisión de mensajes.

Figura 4.11 Máquina enigma

Con el desarrollo de la informática en la segunda mitad del siglo XX y con el uso cada vez más extendido de las redes informáticas y del almacenamiento masivo de información se ha dado paso a un gran salto en el estudio de sistemas criptográficos. En 1975 Diffie y Hellman establecieron las bases teóricas de los algoritmos de llave pública, hasta entonces no se concebía un sistema de cifrado que no fuese de clave secreta. En la actualidad se usan distintos métodos criptográficos, el DES (de llave secreta), método RSA, método de Merkle y Hellman, etc.

4.7.7. Método de las frecuencias

El método de las frecuencias consiste en usar la permanencia estadística de los símbolos utilizados después de una sustitución; así, si el símbolo $ es el que más aparece en el criptograma se puede pensar que con bastante probabilidad dicho símbolo corresponderá a la letra E o a la letra A (si el mensaje está en español). Por tanto, cuando se tiene un criptograma lo suficientemente largo (pongamos por ejemplo 100 caracteres) y se sospecha que está cifrado por sustitución simple el primer paso del criptoanálisis debe ser elaborar una tabla con las frecuencias de cada uno de los símbolos, ordenar dicha tabla de mayor a menor; después, se debe asociar los símbolos con los correspondientes (en el mismo orden de mayor a menor) con que aparecen las letras en español. Dicha tabla se puede componer a partir de un texto cualquiera lo suficientemente largo; más o menos se tiene E=17%, A=12%, 0=9%, L=8%, S=8%, N=7%, D=7%, etc. Para mayor información es posible estudiar también la frecuencia con que se dan las letras iniciales y finales de cada palabra o la frecuencia de los grupos de dos letras, etc.

Si se usa el método Vigenére, en el que la sustitución es polialfabética, el primer paso consistirá en descubrir la longitud de la clave, para ello se puede usar entre otros métodos el del estudio de las repeticiones en el texto cifrado, así si se repite un mismo bloque varias veces cada seis símbolos se puede deducir que la longitud de la clave es seis, separando ahora el texto en seis partes se procede como se ha visto en el párrafo anterior. En general todos los métodos clásicos por sustitución son atacables por métodos estadísticos, pues con esos métodos no se pierde la redundancia de la fuente (la frecuencia de las letras en el texto original).

4.8. Clasificación por tipo de llave

Las técnicas de criptografía moderna se pueden clasificar en dos según el tipo de clave utilizado:

1. Criptografía de llave pública o asimétrica.
2. Criptografía simétrica.

4.8.1. Criptografía de llave pública (public key cryptography)

En 1976 Diffie y Hellman publicaron el artículo “New directions in cryptography”. En él proponían un nuevo tipo de criptografía basado en utilizar llaves distintas para cifrar y descifrar, una de ellas se hace pública y la otra es privada de cada usuario. Así todos los usuarios de la red tienen acceso a las llaves públicas, pero únicamente a su llave privada sólo ellos mismos. Estas ideas supusieron la revolución de la criptología, se podía utilizar para confidencialidad (como los sistemas simétricos), autenticación y firma digital, además de solucionar el problema de la distribución de llaves simétricas.

Para cada tipo de servicio se cifra de manera diferente.

Confidencialidad

El emisor cifra el texto con la llave pública del receptor y el receptor lo descifra con su llave privada. Así, cualquier persona puede enviar un mensaje cifrado, pero sólo el receptor, que tiene la llave privada, y el emisor que la ha creado, puede descifrar el contenido.

Autenticación

Se cifra el mensaje o un resumen de éste mediante la llave privada y cualquier persona puede comprobar su procedencia utilizando la llave pública del emisor. El mensaje es auténtico porque sólo el emisor verdadero puede cifrar con su llave privada.

Firma digital

Igual que la autenticación, pero siempre se cifra el resumen del mensaje, cuyo cronograma es la firma del emisor. Así, el emisor no puede negar la procedencia ya que se ha cifrado con su llave privada. Por otro lado, el receptor no puede modificar el contenido porque el resumen sería diferente y se vería que no coincide con la firma descifrada.

Pero el receptor si puede comprobar que el resumen coincide con la firma descifrada para ver si es auténtico. La firma digital lleva implícita la autenticación.

Se puede realizar sistemas completos con autenticación o firma y confidencialidad.

Los algoritmos asimétricos están basados en funciones matemáticas fáciles de resolver, pero muy complicadas de realizar la inversa, por ejemplo la potencia y el logaritmo.

Estas funciones son útiles para criptografía, si la inversa es fácil de calcular conociendo un número concreto, la llave privada. Así, la llave privada y pública están relacionadas matemáticamente, pero esta relación debe ser suficientemente compleja para que el criptoanalista no la pueda encontrar. Debido a esto, las llaves privadas y públicas no las elige el usuario sino que las calcula un algoritmo y, normalmente, son muy largas.

Un algoritmo de llave pública debe cumplir:

- Conocido el criptograma no se puede descifrar el texto ni adivinar la llave.
- Conocido el texto y el criptograma es más caro (en tiempo y/o dinero) descifrar la llave que el valor de la información.
- Conocida la llave pública y el texto no se puede generar un criptograma cifrado con llave privada.

En estos sistemas también funciona el criptoanálisis de “prueba y ensayo” y se puede aplicar las mismas suposiciones que en algoritmos simétricos. Aparte de este método, también hay algoritmos matemáticos para obtener la llave privada desde la pública pero, si el algoritmo es bueno, éstos son más caros que el valor de la información. Para complicar estos sistemas de criptoanálisis se utilizan llaves muy largas.

El inconveniente de estos sistemas es la dificultad de implementación y la lentitud de proceso.

La ventaja es que implementan servicios de autenticación, firma y además no tienen problemas con distribución de llaves: la llave pública puede ser visible por cualquiera y la privada no se transmite nunca.

El algoritmo más utilizado es el RSA (iniciales de sus creadores Rivest-Shamir-Adleman) es de libre circulación para llaves de menos de 512 bits (insuficiente para ciertas aplicaciones).

Únicamente para firma digital también se utiliza el algoritmo DSS (Digital Signature Standard) que ha sido adoptado como estándar por el National Institute for Standard and Technology (NIST).

Para distribuir llaves simétricas también se utiliza el algoritmo Diffie-Hellman, pero no sirve para confidencialidad, autenticación ni firma digital.

La forma de operar es la siguiente:

Aquí se tienen dos llaves o claves, una se hace pública y la otra se mantiene secreta.

M = mensaje de texto simple

E = mensaje cifrado

K1, K2 = llaves de cifrado

E = f(M, K1)

M = f(E, K2)

M = f(f(M, K1),K2)

M = f(f(M, K2),K1)

En otras palabras:

- Si se le envía un mensaje a alguien, lo puede leer decodificándolo con la llave pública.
- Si alguien envía un mensaje lo pueden codificar con la llave pública y se decodifica con la llave secreta.

Rivest-Shamir-Adleman (RSA)

El algoritmo RSA fue desarrollado en 1977 por Ron Rivest, Adi Shamir y Leonard Adleman. RSA es el algoritmo más utilizado de cifrado y está incluido en los navegadores de WWW de Netscape y Microsoft.

Aunque este algoritmo está patentado, la patente expiró el 20 de septiembre del 2000. Como el cifrado de este algoritmo fue publicado antes de patentarlo, se ha estado usando fuera de Estados Unidos por mucho tiempo y es muy popular en el mundo.

Se multiplican dos números primos y después de varias operaciones se generan dos números que son la llave pública y la privada.

- Se toman dos números primos (p, q) de 256 bits
- n = p * q
- Se selecciona un número "e" tal que e y (p-1)*(q-1) no tengan factores comunes
- d = mod((p-1)*(q-1))/ e
- Llave K1 = <e, n>
- Llave K2 = <d, n>
- Donde se debe tener que M < 512 bits

Usando este método se tiene la ventaja de que nunca se envía la llave privada por Internet.

Además de cifrar mensajes también se pueden hacer autenticaciones personales para asegurar que realmente la persona que envió el mensaje es ella, al cifrar un certificado digital. Cuando se recibe este certificado se usa la llave pública de esta persona para descifrarlo.

4.8.2. Criptografía de llave secreta o privada (secret key cryptography)

Es el sistema de criptografía más antiguo. Se utiliza desde los tiempos de Julio César hasta la actualidad. Se caracteriza por usar la misma llave para cifrar y descifrar.

Se tiene una llave o clave secreta para poder decodificar el mensaje enviado.

Toda la seguridad está basada en la privacidad de una llave secreta, llamada simétrica porque es la misma para el emisor y el receptor. El emisor del mensaje genera una llave y después la transmite mediante un canal seguro a todos los usuarios autorizados a recibir mensajes. La distribución de llaves es un gran problema para los sistemas simétricos, hoy en día se resuelve mediante sistemas asimétricos montados únicamente para transmitir llaves simétricas.

Estos sistemas sólo permiten confidencialidad y no autenticación ni firma digital.

Para mantener la confidencialidad delante de un criptoanalista, el algoritmo debe cumplir las siguientes condiciones:

- Conocido el criptograma no se puede descifrar el texto ni adivinar la llave.
- Conocido el texto y el criptograma es más caro (en tiempo y/o dinero) descifrar la llave que el valor de la información.

Para la segunda condición siempre existe el sistema de “prueba y ensayo” para encontrar la llave, es decir, probar todas las llaves posibles hasta encontrar la que descifra el criptograma. La seguridad respecto a este tipo de ataque depende de la longitud de la llave.

Los algoritmos simétricos cifran bloques de texto, el tamaño de los bloques puede ser constante o variable según el tipo de algoritmo.

Tienen cuatro formas de funcionamiento.

1. Electronic CodeBook (ECB).
2. Chipre Block Chaining (CBC).
3. Chipre Feedback (CFB).
4. OutputFeedBack (OFB).

Electronic CodeBook (ECB). Se cifran los bloques de texto por separado.

Chipre Block Chaining (CBC). Los bloques de criptograma se relacionan entre ellos mediante funciones OR-EXCLUSIVA.

Chipre Feedback (CFB). Se realiza una OR-EXCLUSIVA entre caracteres o bits aislados del texto y las salidas del algoritmo. El algoritmo utiliza como entrada los criptogramas.

OutputFeedBack (OFB). Igual que el CFB, se realiza una OR-EXCLUSIVA entre caracteres o bits aislados del texto y las salidas del algoritmo. Pero éste utiliza como entradas sus propias salidas, por lo tanto no depende del texto, es un generador de números aleatorios.

De manera genérica se tiene:

- M = mensaje de texto simple
- E = mensaje cifrado
- K = llave de cifrado
- E = f(M, K) eficiente de calcular
- M = f-1(E, K) fácil de calcular
- M = f'(E) muy difícil de calcular
- M = f''(E, K) difícil de calcular

Problema: se necesita un canal de comunicaciones seguro para enviar las llaves.

Un ejemplo de criptografía de llave secreta es DES.

4.8.3. Data Encryption Standard (DES)

En 1971 IBM inventó un algoritmo de cifrado simétrico basado en la aplicación de todas las teorías existentes sobre criptografía. Se llamó LUCIFER y funcionaba con llaves simétricas de 128 bits. Fue vendido en exclusividad a la empresa de seguros Loyd's.

En 1973 el Nacional Bureau of Standard (NBS) de los Estados Unidos convocó a un concurso para elegir un estándar de cifrado para la seguridad de los documentos oficiales. Este concurso fue ganado en 1977 por los inventores del LUCIFER con una versión mejorada, este algoritmo se denominó Data Encryption Standard (DES). Está descrito en los estándares ANSI X3.92 y X3.106.

Es tan difícil de romper que el gobierno de los Estados Unidos en el pasado prohibió la exportación de software basado en este algoritmo a otros países. Aunque este software está disponible en varios sitios de Internet.

Por cada mensaje una llave se escoge aleatoriamente de entre al menos $2^{(56)} = 7.2 * 10^{(16)}$, llaves. DES utiliza una llave de 56 bits por cada bloque de datos de 64 bits.

El procesamiento de datos puede correr en varios modos e implica 16 fases de operaciones.

Trabaja alternativamente sobre las dos mitades del bloque a cifrar.

Se hace una permutación inicial fija.

Se divide el bloque en dos mitades, derecha e izquierda.

Se realiza 16 veces la operación modular.

Se intercambian las partes derecha e izquierda.

En la vuelta 16 se omite el intercambio, pero termina el algoritmo con una permutación final que es la inversa de la última.

4.8.4. Triple DES (TDES)

Para evitar el problema de la llave corta y continuar utilizando el DES existe un sistema basado en tres iteraciones del algoritmo, llamado triple DES o TDES, que utiliza una llave de 128 bits y es compatible con el DES simple.

Se utiliza una llave de 128 bis (16 de paridad y 112 de llave), se aplican 64 bits a los dos DES y los otros 64 bits al DES inverso (ANTIDES) que se realiza entre los otros dos.

Con tres algoritmos, se podría aplicar tres llaves distintas, pero no se hace así para que sea compatible con el DES. Si la llave de 128 está formada por dos llaves iguales de 64 el sistema se comporta como DES simple.

4.8.5. Pretty Good Privacy (PGP)

PGP realiza criptografía de llave secreta y criptografía de llave pública. PGP utiliza el algoritmo IDEA para el cifrado secreto y RSA para el cifrado público.

International Data Encryption Algorithm (IDEA)

En 1990 Lai y Massey del Swiss Federal Institute of Technology inventaron un algoritmo nuevo denominado IDEA. En 1992 se publicó la segunda versión resistente a ataques de criptología diferencial. Este algoritmo está libre de restricciones y permisos nacionales, trabaja con bloques de texto de 64 bits y utiliza llaves de 128 bits. Este software está patentado y se debe comprar a la empresa ViaCrypt International.

Además de cifrar y descifrar PGP puede verificar firmas digitales y guardar llaves públicas y privadas en archivos especiales llamados "llaveros".

4.8.6. Message Digest

Message Digest es un checksum o hashcode criptográfico. Así como un checksum normal permite detectar cambios en el mensaje, un checksum criptográfico permite detectar cambios malintencionados a un mensaje.

Message Digest es una función de un sólo sentido, porque dado un checksum criptográfico de un mensaje es virtualmente imposible efectuar el proceso inverso; con el checksum reconstruir el mensaje original.

M = mensaje de texto simple

d = message digest o checksum criptográfico

d = f(M) muy difícil de invertir

4.8.7. Firmas digitales

Una firma digital es un message digest cifrado con la llave privada de alguien para certificar el contenido de un mensaje. Una firma digital hace posible que matemáticamente se verifique la autenticidad de la persona que envió el mensaje.

4.8.8. Funciones hash

Las funciones hash sirven para comprimir un texto en un bloque de longitud fija comúnmente llamado resumen. Se utilizan en autenticación y firma digital para:

1. No tener que cifrar todo el texto en los servicios de autenticación y firma digital, ya que este proceso es lento con los algoritmos asimétricos. El resumen sirve para comprobar si la llave privada del emisor es auténtica, no es necesario cifrar todo el texto si no se quiere confidencialidad.

2. Para poder comprobar automáticamente la autenticidad. Si se cifra todo el texto, al descifrar sólo se puede comprobar la autenticidad mirando si el resultado es inteligible, evidentemente este proceso debe realizarse de forma manual. Utilizando un resumen del texto, se puede comprobar si es auténtico comparando el resumen realizado en el receptor con el descifrado.

3. Para comprobar la integridad del texto, ya que si ha sido dañado durante la transmisión o en recepción no coincidirá el resumen del texto recibido con el descifrado.

Las funciones hash son públicas e irreversibles. No cifran, sólo comprimen los textos en un bloque de longitud fija. Son diferentes de las funciones clásicas de compresión de textos, como ZIP. Estas funciones son reversibles e intentan eliminar la redundancia de los textos manteniendo el significado. Las funciones hash no son reversibles, es decir, no se puede recuperar el texto desde el resumen, pero deben cumplir las siguientes condiciones:

1. Transformar un texto de longitud variable en un bloque de longitud fija.

2. Ser irreversibles.

3. Conocido un mensaje y su función hash debe ser imposible encontrar otro mensaje con la misma función hash. Esto se debe cumplir para evitar que los criptoanalistas firmen un mensaje propio como si fueran otra persona.

4. Es imposible inventar dos mensajes cuya función hash sea la misma.

Los algoritmos más utilizados son:

MD5. Inventado en 1992 por Rivest. La longitud del bloque es de 128 bits. Es de libre circulación.

SHA. Inventado en 1994 por la agencia NIST. La longitud del bloque es de 160 bits. Para su utilización se necesita permiso de USA.

La Organización de Estándares de los Estados Unidos (NIST) llevó a cabo un concurso para buscar un algoritmo simétrico estándar que reemplazara a DES. A este sistema le llamaron AES (Advanced Encryption Standard) y el algoritmo AEA (Advanced Encryption Algorithm).

Las propuestas fueron presentadas antes de junio de 1998 y después se realizó una primera ronda para eliminar candidatos. En agosto de 1998 se publicó la lista de los quince algoritmos candidatos, Tabla 4.17.

Nombre del algoritmo	Creadores del algoritmo
CASTd56	EnoBt Technologies, Inc.
CRYPTON	Fu_we Syoemp l_c.
DEAL	Richard Omed_dge, Lars Knudsen
DFC	CNRS - Centre National poux la llecherche Scieptiflque Ecole
DFC	Normale Superieure
E2	NTT - Nippon Telegraph and Telephone Corporation
FROG	TecApro Internacional SA.
HPC	Rich Schroeppel
LOKl97	Lawrie Brown, Josef Pieprzyk, Jennifer Seberry
MAGENTA	Deutsche Telekom AG
MARS	IBM
RC6	RSA Laboratories
RIJNDAEL	Jowi Daeme W Vincent Rijmen
SAFER+	Cylink Corporation'
SERPENT	Ross Anderson, El_ Bihain, Lars Knudsen
TWOFISH	Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson

Tabla 4.17 Lista de los quince algoritmos finalistas

En agosto de 1999 el NIST publicó la lista de los cinco algoritmos que pasaron la primera ronda, fueron:

- MARS.
- RC6.
- Rijndael.
- Serpent.
- TwoFish.

Al final, el ganador fue Rijndael y así de esta forma el gobierno de los Estados Unidos que quería un algoritmo más poderoso que DES logró su objetivo, previendo que con el avance de la tecnología y por utilizar una llave corta, podría ser roto con computadoras cada vez más potentes.

4.9. Certificados de llave pública

Transmisión de llaves públicas

En la criptografía simétrica la transmisión de la llave es un problema importante ya que si se descubre, todo el sistema se rompe. La solución adoptada ha sido enviarla cifrada con un sistema asimétrico. Pero, ¿cuál es el problema de la transmisión de las llaves públicas?

La llave privada no se transmite nunca y, por lo tanto, es segura. El conocimiento de la llave pública no pone en peligro la seguridad del sistema. Pero el problema cuando se recibe una llave pública es ¿cómo saber que la identidad del propietario de esta llave no es falsa? Si una persona se hace pasar por otra y envía llaves públicas a los receptores podrá realizar:

Firmar en nombre de otro.

Realizar transmisiones confidenciales mediante llaves de sesión donde el interlocutor se piensa que se comunica con otra persona.

Este problema es conocido como suplantación de personalidad. La solución no es transmitir la llave pública por un canal secreto, ya que así perdería sus propiedades de pública. La solución son los certificados de llave pública.

En los certificados de llave pública hay los siguientes datos:

- El nombre de un usuario.
- La llave pública de un usuario. Datos e informaciones generales.
- La firma de una tercera persona de confianza.

Así la firma de esta tercera persona asegura que la llave pública pertenece al nombre del usuario. Toda la confianza se basa en la autenticidad de la firma y, por lo tanto, de la llave pública de la tercera persona.

Actualmente todas las llaves públicas se envían en certificados, excepto las primeras de confianza que sirven para firmarlos. Aceptar o rechazar una llave pública depende de la firma que la avala en el certificado. Todos los programas navegadores y de correo actuales están preparados para recibir certificados, comprobarlos y dar un mensaje al usuario de auténtico o no.

Con los certificados el problema de la suplantación de personalidad se ha trasladado de la recepción de llaves públicas a la confianza en las llaves de terceras personas. Para resolver este problema los métodos más utilizados son:

- Niveles de confianza del PGP.
- Autoridades de certificación (CA por sus siglas en inglés).

4.10. Certificados del PGP

Los certificados del sistema de correo PGP funcionan mediante niveles de confianza. El sistema sería ideal si todos los certificados llegaran firmados por una persona a la que se ha comprobado la llave pública, pero no siempre es así. Además, una llave sin certificado sólo es de confianza si se transmite personalmente o mediante un medio de comunicación público (revistas y periódicos), el teléfono o las webs no son vías seguras.

En PGP se asigna dos niveles de confianza a cada llave pública de la base de datos. Estos son:

1. Confianza propia.
2. Confianza para firmar certificados.

Confianza propia. La confianza en llave pública del usuario calculada, según el procedimiento por donde ha venido:

- Directamente. Confianza máxima.
- Por certificado. Depende de la firma de la tercera persona.

Confianza para firmar certificados. Una llave pública puede tener una confianza propia muy alta porque ha llegado por un sistema seguro, pero puede ser que no se pueda confiar en las firmas de certificados de este usuario, porque firme a cualquiera sin confirmar su procedencia.

4.11. Autoridades de certificación

El sistema de PGP sirve para grupos pequeños de usuarios donde siempre hay un enlace entre ellos, aunque sea por una cadena de confianzas de muchas personas. Pero tiene dos inconvenientes:

- No es útil para los millones de usuarios de Internet, no pueden certificarse todos entre sí.
- No es útil para sistemas judiciales. Si se tiene que comprobar la procedencia de una firma y, por lo tanto, de la llave pública, con PGP se han de seguir largas cadenas de usuarios.

Para solucionar estos problemas, se han creado las autoridades de certificación. Son entidades públicas o privadas cuya función es ofrecer confianza en los certificados que firman. Generan llaves públicas y certificados, para usuarios bajo demanda, además de dar a conocer sus llaves públicas para las comprobaciones. Los usuarios se deben identificar personalmente para pedir un certificado a una CA. Es un sistema parecido al carnet de identidad, donde el estado, como entidad de confianza, genera un documento que los bancos y las empresas consideran fiable.

Para descentralizar la gestión de CA’s está previsto crear una estructura jerárquica a nivel mundial. Las CA’s locales son certificadas por otras de nivel superior hasta llegar a la principal que es de confianza en todo el mundo. Así se consigue que la confianza sea mundial, para la red Internet sin fronteras, y que la gestión pueda ser local, para los procesos judiciales y facilitar el proceso de identificación personal.

Actualmente, la CA más conocida es la empresa privada americana VeriSign, además de las empresas de tarjetas de crédito Visa, Mastercard y American Expres. En España las CA más conocidas son FESTE y ACE que gestionan los certificados a través de bancos, notarios o agentes de comercio. Muchas empresas crean sus propias CA privadas para el sistema de correo interno.

CAPÍTULO 5

CONTROLES DE ACCESO

Se puede decir que la seguridad lógica es la forma de aplicar procedimientos que aseguren que sólo podrán tener acceso a los datos las personas o sistemas de información autorizados para hacerlo.

Los objetivos planteados son:

- Restringir el acceso a programas y archivos.
- Los operadores deben trabajar sin supervisión minuciosa y no podrán modificar programas ni archivos que no correspondan.
- Asegurar que se estén utilizando los datos, archivos y programas correctos en, y por el procedimiento correcto.
- Asegurar que la información transmitida sea recibida sólo por el destinatario al cual ha sido dirigida y por ningún otro.
- Asegurar que la información que el destinatario ha recibido sea la misma que ha sido transmitida.

Se debe disponer de sistemas alternativos de transmisión de información entre diferentes puntos.

El ISO 7498-2 define a los controles de acceso como los servicios de seguridad que previenen el uso de un recurso salvo en casos y de manera autorizada; se utiliza un mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

Los controles de acceso pueden implementarse de varias formas, a nivel sistema operativo, de programas aplicativos, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Los controles de acceso constituyen una ayuda importante para proteger al sistema operativo de la red, a los sistemas de información y software adicional; de que puedan ser utilizados o modificados sin autorización, sirven para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con autorización de acceso) y para resguardar la información confidencial de accesos no autorizados.

Las consideraciones relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso solicitado por un usuario, a un determinado recurso son planteadas por el NIST, en el documento llamado “The NIST Handbook Special Publication 800-12”, donde se encuentran resumidos esquemas para dotar de seguridad a cualquier sistema.

El control de acceso es una función de seguridad esencial para proteger los datos y los tratamientos de posibles manipulaciones no autorizadas. En el control de acceso intervienen diversos componentes:

- Identificación y autenticación de usuarios.
- De acuerdo a la función o rol del usuario.

Identificación y autenticación de usuarios

Constituye la primera línea de defensa para la mayoría de los sistemas computarizados, al prevenir el ingreso de personas no autorizadas y es la base para casi todos los controles de acceso, además permite efectuar un seguimiento de las actividades de los usuarios.

Identificación es cuando el usuario se da a conocer en el sistema; y autenticación es la verificación que realiza el sistema de la identificación.

De acuerdo a la función o rol del usuario

El acceso a la información puede ser controlado también, considerando la función o rol del usuario que requiere dicho acceso.

Algunos ejemplos pueden ser:

- Director de sistemas.
- Analista de contabilidad.
- Subdirector de nómina.
- Etc.

Los derechos de acceso a redes, sistemas, aplicaciones, datos; se agrupan de acuerdo con un rol determinado y el uso de los recursos se restringe a las personas autorizadas a asumir dicho rol, cambiar de rol implica salir del sistema para que se actualicen los cambios y volver a ingresar ya con los nuevos derechos.

El uso de roles es una manera bastante efectiva de implementar el control de accesos, siempre que el proceso de definición de roles esté basado en un profundo análisis de cómo la organización opera. Es importante aclarar que el uso de roles no es lo mismo que el uso compartido de cuentas.

Se entienden por privilegios (de acceso) los mecanismos de protección que permiten a ciertos usuarios alterar los controles de seguridad del sistema o de las aplicaciones. La asignación de privilegios especiales innecesarios es una de las causas de vulnerabilidad más frecuentes en los sistemas que han sufrido ataques, por lo que se deberá controlar mediante un procedimiento formal de autorización de privilegios.

Transacciones

Otro planteamiento para implementar controles de acceso en una organización son las transacciones, sería del modo siguiente: la computadora conoce de antemano el número de cuenta que proporciona a un usuario el acceso a la cuenta respectiva, este acceso tiene la duración de una transacción, cuando ésta es completada, entonces la autorización de acceso termina, esto significa que el usuario no tiene más oportunidad de operar.

Limitaciones a los servicios

Las limitaciones a los servicios son controles que se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o que han sido preestablecidos por el administrador del sistema. Un ejemplo de este tipo de control es cuando en un cajero automático se establece un límite para la cantidad de dinero que se puede transferir de una cuenta a otra, y también para los retiros.

Otro ejemplo podría ser cuando los usuarios de una red, tienen permitido intercambiar e-mails entre sí, pero no tienen permitido conectarse para intercambiar e-mails con usuarios de redes externas.

Modalidad de acceso

Adicionalmente a considerar cuando un acceso puede permitirse, se debe tener en cuenta también qué tipo de acceso o modo de acceso se permitirá. El concepto de modo de acceso es fundamental para el control respectivo, los modos de acceso que pueden ser utilizados son:

- Lectura.
- Escritura.
- Ejecución.
- Borrado.

Además existen otras modalidades de acceso especiales, que generalmente se incluyen en los sistemas de aplicación:

- Creación.
- Búsqueda.

Estos criterios pueden ser usados de manera conjunta con otros, por ejemplo, una organización puede proporcionar a un grupo de usuarios acceso de escritura en una aplicación en cualquier momento dentro del horario de oficina, y acceso sólo de lectura fuera de él.

Ubicación y horario

El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de datos o personas. En cuanto al horario, el uso de parámetros como horario de oficina o día de semana son comunes cuando se implementan este tipo de controles, que permiten limitar el acceso de los usuarios a determinadas horas.

Control y auditoría de acceso

Los controles de acceso interno determinan lo que un usuario (o grupo de usuarios) puede o no hacer con los recursos del sistema. Se detallarán cuatro métodos de control de acceso interno.

1. Palabras clave (passwords).
2. Cifrado.
3. Listas de control de accesos.
4. Límites sobre la interface del usuario.

1. Palabras clave (passwords)

Las palabras clave o passwords están comúnmente asociadas con la autenticación del usuario, pero también son usadas para proteger datos, aplicaciones e incluso pc’s. Por ejemplo, una aplicación de contabilidad puede solicitar al usuario un password, en caso de que aquél desee acceder a cierta información financiera. Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo e incluyen una gran variedad de aplicaciones.

2. Cifrado

La información cifrada solamente puede ser descifrada por quienes posean la clave apropiada.

3. Listas de control de accesos

Estas listas se refieren a un registro de:

- Usuarios.
- Los tipos de acceso que han sido proporcionados.

Usuarios (incluye grupo de usuarios, computadoras, procesos), a quienes se les ha proporcionado autorización para usar un recurso del sistema.

Los tipos de acceso que han sido proporcionados.

Hay una gran flexibilidad para el manejo de estas listas, pueden definir también a qué usuario o grupos de usuarios se les niega específicamente el acceso a un recurso. Se pueden implementar listas de control de acceso elementales y avanzadas.

4. Límites sobre la interface del usuario

Estos límites se establecen normalmente en los menús que las aplicaciones tienen, se basan en las listas de control de accesos.

En estos menús, se permite accesar únicamente lo que tiene autorizado cada usuario, de acuerdo a su puesto y función.

Es común que se puedan ver todas las opciones en los submenús, pero no están habilitadas para su ejecución, de esta forma se limita el acceso de los usuarios a los datos contenidos en la base de datos.

Control de acceso externo

Los controles de acceso externo son una protección contra la interacción del usuario con los sistemas, servicios y gente externa a la organización.

El acceso por usuarios externos a la organización da lugar a riesgos si el acceso se produce desde localizaciones con un nivel de seguridad inadecuado. En los casos en los que la organización tenga que permitir este acceso, por necesidad del servicio, debe llevar a cabo un análisis de riesgos específico para determinar las protecciones a implantar; protecciones que deberán acordarse con la otra parte y, en su caso, definirse mediante convenio o contrato.

El acceso por terceros no se autorizará hasta que no se hayan implantado las medidas de protección específicas y firmado el contrato de acuerdo con los terceros estableciendo las características del acceso. El contrato debe especificar los requisitos de seguridad de tales accesos, contener los criterios y las condiciones de seguridad específicos.

Dispositivos de control de puertos

Estos dispositivos autorizan el acceso a un puerto determinado de la computadora y pueden estar físicamente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un módem. Los dispositivos de control de puertos actúan de manera previa e

independiente de las funciones de control de acceso propias de la pc y comúnmente son usados en comunicaciones seriales.

5.1. Firewalls

La seguridad lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

Cuando se habla de seguridad en redes, se requiere que varios requerimientos sean cubiertos. En primer lugar es importante hablar de autenticación, en este caso se debe verificar que los usuarios son quienes dicen ser (confidencialidad) sólo los usuarios autorizados pueden acceder el contenido de los datos (integridad), los datos no pueden ser alterados por terceras partes durante la transmisión de éstos y por último la no repudiación, que consiste en que un usuario no puede negar el hecho de que tuvo acceso a un determinado servicio o datos; de forma práctica: es necesario garantizar que alguien que haya recibido un pago no pueda negar este hecho, así como es necesario garantizar que alguien que haya efectuado un pago no pueda negar haberlo hecho[1].

Hace algunos años, y aún hoy, los firewalls se han visto como algo infalible en contra de los ataques computacionales a sistemas de información. Como su nombre lo indica, ésta es una herramienta de seguridad que se utiliza como si se tratara de erigir una muralla de fuego que rodee los recursos (servidores, información, servicios, etc.) y evitar así penetración de intrusos que los dañen o se aprovechen de ellos.

Lo primero que se hace para implementar un firewall es determinar cuáles son los recursos que se quiere proteger, y hasta dónde se va a proteger, pues esta muralla en realidad no es tan infranqueable sino que solamente abre o permite el paso de quienes estén autorizados, Figura 5.1.

Esto lleva a deducir que se requieren ciertas reglas que determinen qué, quién, y cómo se puede acceder a los diferentes recursos que se encuentran detrás de la muralla. Una vez definido todo esto, se necesita dividir la red en dos partes, una en la que se resguardan los recursos y otra en la que fluye el tráfico de forma normal (DMZ: Zona Desmilitarizada), tal y como se hacía antes de poner la muralla. Esto generalmente se hace con una computadora o un ruteador con dos tarjetas de red y un software en el cual se implantan las reglas que dirigirá el tráfico de entrada hacia la interfaz “segura” así como el tráfico proveniente de la misma.

[1] Gómez Cárdenas, Roberto. *Seguridad Computacional*. Instituto Tecnológico de Estudios Superiores Monterrey. Segunda Edición. México. 2001.

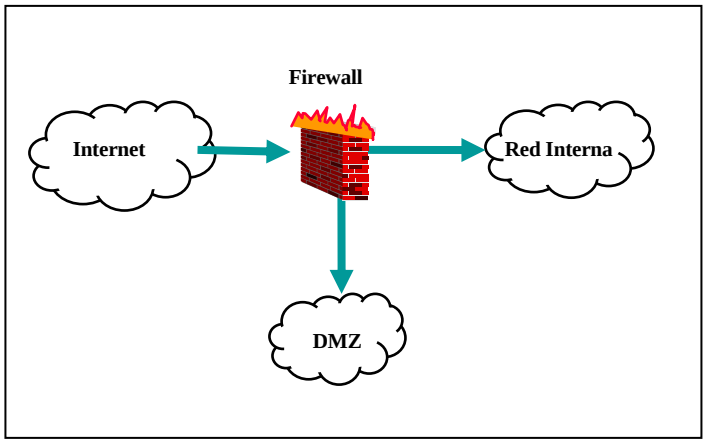


Figura 5.1 Esquema general de una red protegida con un firewall. Dual homed gateway

Un firewall es un sistema o un grupo de sistemas que decide qué servicios pueden ser accedidos desde el exterior (Internet) de una red privada, por quiénes pueden ser ejecutados estos servicios y también qué servicios pueden correr los usuarios de la Intranet hacia el exterior (Internet). Para realizar esta tarea todo el tráfico entre las dos redes tiene que pasar a través de él.

El firewall sólo deja pasar el tráfico autorizado desde y hacia el exterior. No se puede confundir un firewall con un ruteador, un firewall no direcciona información (función que sí realiza el ruteador), el firewall solamente filtra información. Desde el punto de vista de política de seguridad, el firewall delimita el perímetro de defensa y seguridad de la organización. El diseño de un firewall, tiene que ser el producto de una organización consciente de los servicios que se necesitan, además hay que tener presentes los puntos vulnerables de toda la red, los servicios que dispone como públicos al exterior de ella (WWW, FTP, Telnet, entre otros) y conexiones por modem.

Ello no quiere decir que la instalación de un sistema de firewall permita la relajación de la seguridad interna de las máquinas, sino que se podrá distinguir fácilmente entre el interior y el exterior, pudiendo determinar qué comportamiento general se quiere para cada servicio.

Otra característica importante de estos sistemas es que permiten llegar donde los mecanismos de seguridad de los sistemas operativos a veces no pueden.

5.1.1. Beneficios de un firewall

Los firewalls manejan el acceso entre dos redes, si no existiera todos los hosts de la Intranet estarían expuestos a ataques desde hosts remotos en Internet. Esto significa que la seguridad de

toda la red, estaría dependiendo de qué tan fácil fuera violar la seguridad local de cada máquina interna.

El firewall es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque, el administrador de la red escogerá la decisión si revisa estas alarmas o no, la decisión tomada por éste no cambiará la manera de operar del firewall.

Otra causa que ha provocado que el uso de firewalls se haya convertido en uso casi imperativo es el hecho que en los últimos años en Internet han entrado en crisis el número disponible de direcciones IP, esto ha causado que las Intranets adopten direcciones CIRD o direcciones sin clase, las cuales salen a Internet por medio de un NAT (Network Address Traslator), y efectivamente el lugar ideal para alojar el NAT ha sido el firewall.

Los firewalls también han sido importantes desde el punto de vista de llevar las estadísticas del ancho de banda “consumido” por el tráfico de la red, y qué procesos han influido más en ese tráfico, de esta manera el administrador de la red puede restringir el uso de estos procesos y economizar o aprovechar mejor ancho de banda.

Finalmente, los firewalls también son usados para albergar los servicios WWW y FTP de la Intranet, pues estos servicios se caracterizan por tener interfaces al exterior de la red privada y se ha demostrado que son puntos vulnerables.

5.1.2. Tipos de firewalls

Los firewalls pueden clasificarse de acuerdo al tipo de información que filtran. De manera general se puede decir que puede ser un ruteador comercial con capacidad de filtración de paquetes. En este caso el firewall examina el encabezado de los paquetes que van hacia fuera o vienen entrando en la red privada. Las reglas de este firewall permiten dejar pasar el paquete o descartarlo. Las reglas se fijan en función de las direcciones, protocolos en la capa superior, y puertos, básicamente. Otro tipo de firewall se conoce como proxy a nivel circuito. Este firewall establece una conexión a nivel IP, entre un cliente en una interfaz y un servidor en otra interfaz, no analiza los protocolos de la capa superior; la conexión segura es conocida como circuito. Se le considera proxy, pues es el intermediario entre el cliente y el servidor. El último es el proxy a nivel aplicación. Establece una conexión segura a nivel aplicación con el cliente, y por otro lado con un servidor. El diálogo con el cliente y el servidor es independiente. Interpreta el protocolo de aplicación al mismo tiempo que permite el paso o descarta paquetes.

Los firewalls de circuito y aplicación, son intermediarios. Ambos reciben un paquete de su origen y lo “adaptan” para entregarlo al destinatario. El firewall de filtro de paquetes no realiza esta función.

Firewall de filtro de paquetes

Se basa en el tratamiento de los paquetes IP a los que aplica unas reglas de filtrado que le permiten discriminar el tráfico según las indicaciones hechas por el personal que configura este equipo.

Normalmente se implementa mediante un ruteador con dos tarjetas de red, uno de cara al exterior y otro al interior, aunque podría utilizarse cualquier máquina con dos tarjetas de red y un software adecuado para filtrado de los paquetes IP.

Al tratar paquetes IP, los filtros que se podrán establecer serán a nivel de direcciones IP, tanto fuente como destino. Normalmente, se establece una lista de filtros por interfaz que se aplicarán a cada paquete independiente de los anteriores, o si forma parte de una determinada comunicación para un cierto servicio.

Algunos filtros de paquetes permiten establecer filtros también a nivel de puertos TCP o UDP, con lo que se podrá filtrar qué servicios se dejan pasar o no, por ejemplo el puerto 80 es el que especifica el servicio http y deberá estar abierto si la computadora es un servidor web.

La lista de filtros se aplica secuencialmente, de forma que la primera regla que el paquete cumpla marcará la acción a realizar (descartarlo o dejarlo pasar). La aplicación de las listas de filtros se puede hacer en el momento de entrada del paquete o bien en el de salida o en ambos.

Aunque no puede parecer importante lo es, pues tiene que ver con el tratamiento del “address-spoofing” uno de los ataques utilizados con más frecuencia para saltarse la protección establecida por un firewall, el cual consiste en generar paquetes IP con direcciones falsas.

Los filtros de paquetes son una buena solución, pero tienen sus limitaciones a la hora de tratar los servicios como tales, pues para ellos cada paquete es independiente.

Además, existen servicios como DNS o FTP, que dificultan realizar una configuración segura de un filtro de paquetes.

Son muy pocos los sistemas de filtrado de paquetes que se basan en la propia información para aceptar o negar un paquete. Esta posibilidad, aunque tiene un elevado costo, puede utilizarse por ejemplo, para evitar la entrada de archivos infectados con virus en una red interna.

Ventajas del filtrado de paquetes

La protección centralizada es la ventaja más importante del filtrado de paquetes. Con un único ruteador con filtrado de paquetes situado estratégicamente puede protegerse toda una red. Si sólo existe un ruteador con salida a una red insegura, independientemente del tamaño de la red interna, podrá controlarse todo el tráfico en dicho ruteador.

Firewall de nivel de aplicación

Es el extremo opuesto de los filtros de paquetes. En lugar de basarse en el filtrado del flujo de paquetes, tratan los servicios por separado, utilizando el código adecuado para cada uno.

Es probablemente el sistema más seguro, ya que no necesita tratar complicadas listas de acceso y centraliza en un solo punto de gestión los servicios.

Además, permite controlar y recoger información de cada uno de los servicios por separado.

Los gateways a nivel de aplicación son prácticamente la única solución efectiva para el tratamiento seguro de aquellos servicios que requieren permitir conexiones iniciadas desde el exterior (servicios como FTP, telnet, correo electrónico).

En realidad, lo que se utiliza es una puerta de acceso para cualquier servicio.

Al ser esta puerta de uso obligatorio, se puede establecer en ella los criterios de control que se requieran.

Atravesada la puerta, puede ocurrir que el propio gateway de nivel de aplicación ofrezca el servicio de forma segura o que establezca una conexión con la pc o servidor que realmente ofrece el servicio, teniendo en cuenta que este último debe estar configurado para aceptar conexiones tan sólo desde el gateway de nivel de aplicación por este servicio.

Firewall de nivel de circuito

Se basan en el control de las conexiones TCP y actúan como si fuesen un cable de red: por un lado reciben las peticiones de conexión a un puerto TCP; y por otro, establecen la conexión con el destinatario deseado, si se han cumplido las restricciones establecidas, copiando los bytes de un puesto al otro.

Este tipo de firewalls suelen trabajar conjuntamente con los servidores proxy utilizados para la acreditación, es decir, comprobaciones sobre máquina fuente, máquina destino, puerto a utilizar. Una acreditación positiva, significa establecer la conexión.

Son el tipo de firewall más adecuado para el tratamiento de las conexiones salientes.

5.1.3. Firewalls basados en certificados digitales

Este tipo de firewalls son extremadamente seguros y con una gran funcionalidad. Su popularidad no ha sido muy grande porque hasta hace muy poco tiempo no existían distribuidores de certificados digitales universales. Actualmente este defecto está cambiando a nivel mundial.

Existen varias consideraciones a tener en cuenta al momento de implementar un firewall entre Internet y una Intranet (red LAN).

Todo lo que no está específicamente permitido se niega. Aunque es una postura radical es la más segura y la más fácil de implementar relativamente, ya que no hay necesidad de crear accesos especiales a los servicios.

Lo que no es específicamente negado se permite. Ésta no es la postura ideal, por eso es más que todo usada para subdividir la Intranet, ya que en una Intranet lo importante es compartir los recursos y no restringirlos de manera indiscriminada. No es recomendable para implementar entre una LAN e Internet, ya que es muy vulnerable, porque está abierto a todo menos a lo que específicamente se indica.

Quizás uno de los pasos más importantes al instalar y configurar un firewall, sea trabajar con las interfaces de red. Cada interfaz debe ser configurada manualmente, habilitada y probada por el administrador. Esta tarea cambia de plataforma a plataforma. También es recomendable configurarlas desde la herramienta de administración del firewall.

Existen otras consideraciones a tomar en cuenta cuando se desea implementar un firewall. Entre las más importantes está que el firewall no puede informar nada acerca de las redes que se encuentran dentro de la red protegida. Esto implica que los usuarios de las redes deben conectarse en el firewall antes de acceder a otras redes. De igual forma, para que un usuario externo pueda conectarse a un host de la red interna, éste debe conectarse primero al firewall.

El mismo principio anterior se aplica para el correo electrónico, todo correo que vaya a un host externo o a un host de la red interna debe pasar por el firewall. El firewall no debe montar ningún sistema de archivos vía NFS, o dejar alguno de sus sistemas de archivos listos para montarse. Si no son necesarios, compiladores y cargadores deben borrarse. La seguridad de los passwords debe ser reforzada al máximo. El firewall no debe confiar en ningún otro host.

Un firewall se compone de dos tipos de componentes, un ruteador selectivo y un bastión-host. Un ruteador selectivo puede ser un ruteador comercial con capacidad de filtración de paquetes. Bloquea el tráfico entre dos redes o servidores específicos. El bastión-host contiene la mayor parte del software del firewall. En general se cuenta con dos tipos de configuración, dual-homed gateway, Figura 5.1, y screened-host gateway, Figura 5.2.

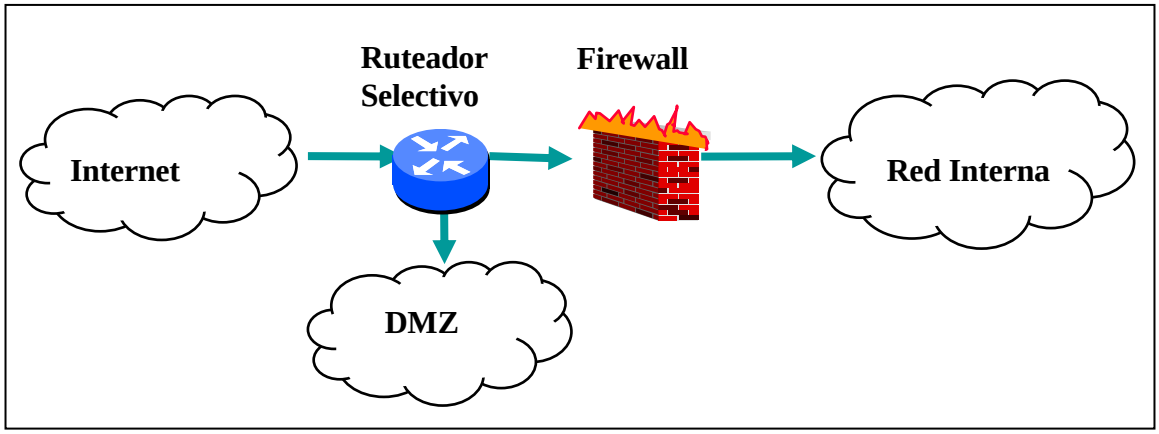


Figura 5.2 Screened-host gateway

Los tipos de firewalls que existen se han tratado de forma independiente, no como sistema. Cuando se realiza un sistema de firewalls, suelen emplearse varios o todos los tipos. Se hace así porque, cada uno de ellos trata la protección a un nivel distinto, desde los paquetes de red, pasando por los puertos de conexión, hasta el servicio propiamente dicho.

Existen múltiples variaciones sobre los esquemas de configuración. Algunos de ellos aportan un nivel mayor de seguridad, pero requieren la dedicación de un número mayor de recursos del sistema, con el consiguiente costo, mientras que otras reducen gastos a costa de la seguridad, pero siendo aún plenamente funcionales.

Se ha de encontrar la configuración adecuada a cada sistema, en función del nivel de seguridad que requiera la política de seguridad del sistema y el trabajo y los recursos que se quieran invertir en dicha seguridad. Esta configuración se conseguirá equilibrando esos dos factores de forma coherente.

5.1.4. Host de base dual

En las redes de TCP/IP, el término host de base múltiple (multi homed host) describe a un host que tiene varias tarjetas de interfaz de red.

Por lo general, cada tarjeta de interfaz de red se conecta a una red. Históricamente, este host de base múltiple también puede enrutar el tráfico entre los segmentos de la red. El término gateway se utilizó para describir la función de enrutamiento desarrollada por estos host de base múltiple.

Hoy en día, el término ruteador se utiliza para describir esta función de enrutamiento, mientras que el término gateway se reserva para aquellas funciones que corresponden a las capas superiores del modelo OSI.

Si la función de enrutamiento en el host de base múltiple está inhabilitada, el host puede proporcionar aislamiento del tráfico de red entre las redes a las que está conectado, y cada red todavía podrá procesar aplicaciones en los hosts de base múltiple. Es más, si las aplicaciones lo permiten, las redes también pueden compartir datos.

Un host de base dual (dual-homed host) es un ejemplo, especial de host de base múltiple que cuenta con dos interfaces de red y tiene inhabilitadas las funciones de enrutamiento.

En la Figura 5.3 se muestra un ejemplo de un host de base dual con las funciones de enrutamiento inhabilitadas. El host A de la red 1 puede tener acceso a la aplicación A del host de base dual. De igual manera, el host B puede tener acceso a la aplicación B del host de base dual. Incluso, las dos aplicaciones de los hosts de base dual pueden compartir datos.

Es posible que los hosts A y B intercambien información a través de los datos compartidos en los hosts de base dual, y aún así no hay intercambio de tronco de red entre los dos segmentos de red conectados al host de base dual.

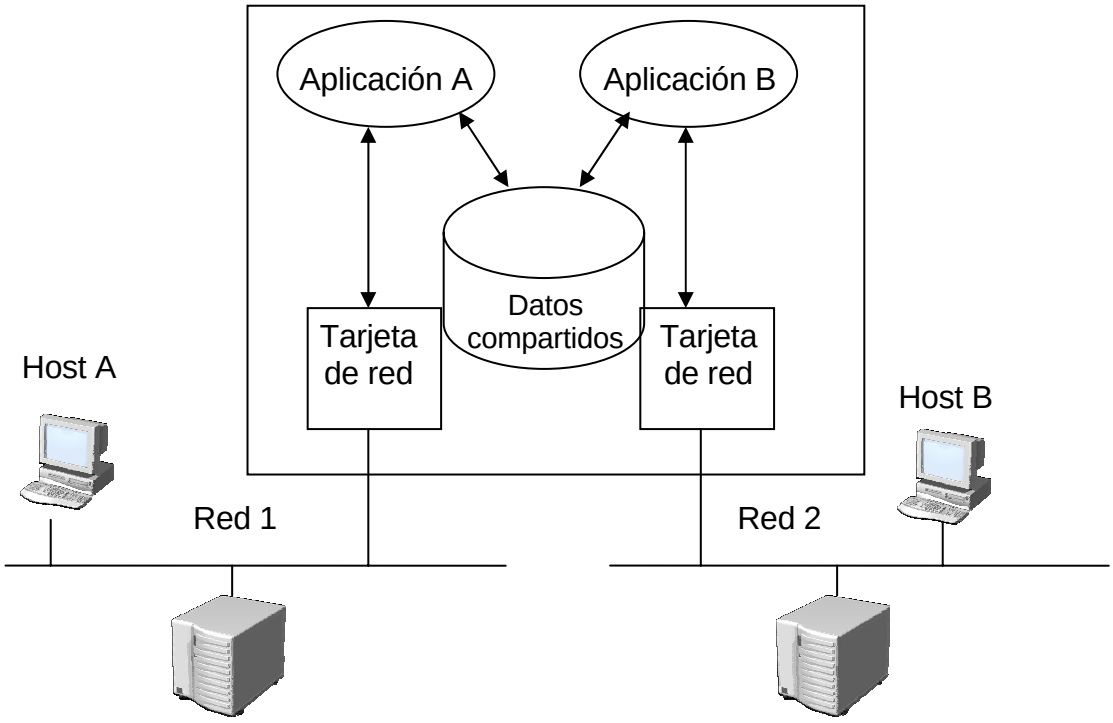


Figura 5.3 Host de base dual

Host de base dual como firewall

El host de base dual puede utilizarse para aislar una red interna de una red externa no confiable, Figura 5.4. Debido a que el host de base dual no envía ningún tráfico de TCP/IP, bloquea completamente cualquier tráfico de IP entre la red interna y la red externa no confiable.

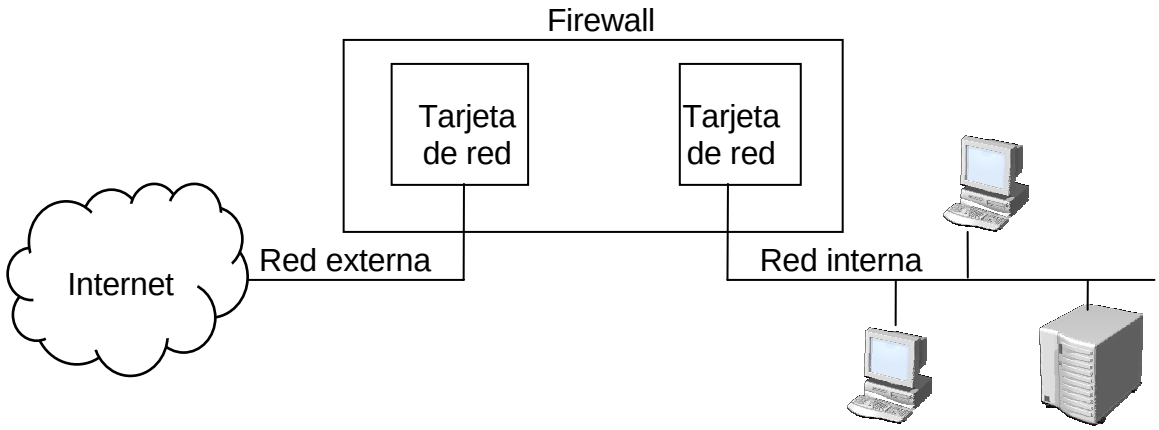


Figura 5.4 Un host de base dual como firewall

Los servicios de Internet, como correo y noticias, son esencialmente servicios de almacenamiento y envío. World Wide Web también puede considerarse como de almacenamiento y envío, pero los términos "cacheo" y "proxy' se utilizan de manera más común en el vocabulario de web. Si estos servicios se ejecutan en un host de base dual, pueden configurarse para transmitir servicios de aplicación de una red a otra. Si los datos de la aplicación deben cruzar el firewall, pueden configurarse los agentes emisores de aplicación para ejecutarse en el host de base dual, Figura 5.5.

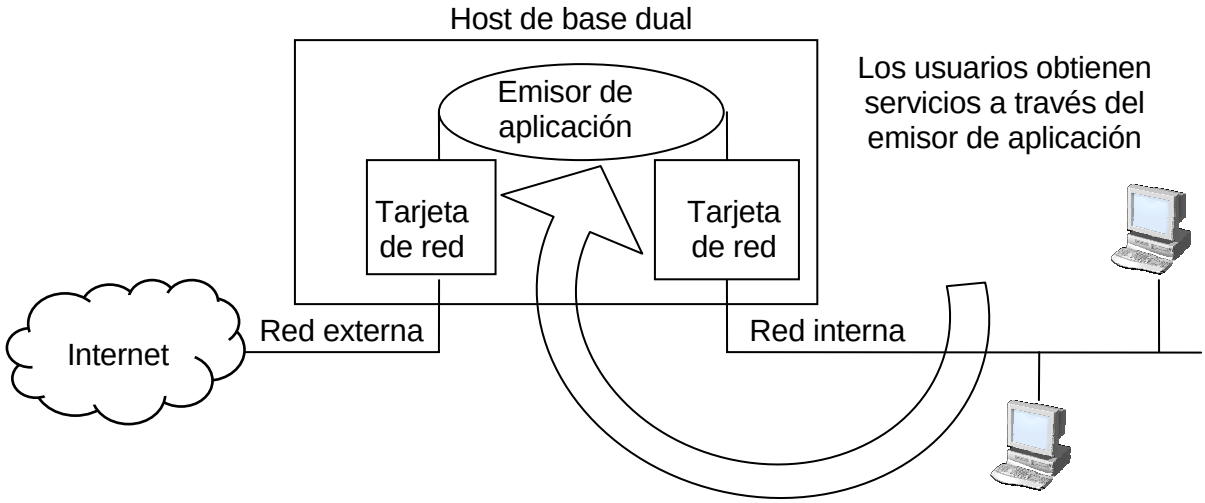


Figura 5.5 Host de base dual con emisores de aplicación

Los agentes emisores de aplicación son un software especial utilizado para enviar las solicitudes de la aplicación entre dos redes conectadas. Otro método consiste en permitir que los usuarios se conecten al host de base dual, y luego acceder a los servicios externos desde la interfaz de red externa del host de base dual, Figura 5.6.

Si se utilizan emisores de aplicación, el tráfico de la aplicación no puede cruzar el firewall de base dual, a menos que el emisor de aplicación esté ejecutándose y que se haya configurado en la máquina del firewall.

Se trata de una implementación de la política "lo que no está permitido expresamente, está prohibido". Si se les permite a los usuarios conectarse directamente con el firewall, Figura 5.6, puede comprometerse la seguridad del firewall. Esto se debe a que el firewall de base dual es un punto central de conexión entre la red externa y la red interna. Por definición, el firewall de base dual es la zona de riesgo.

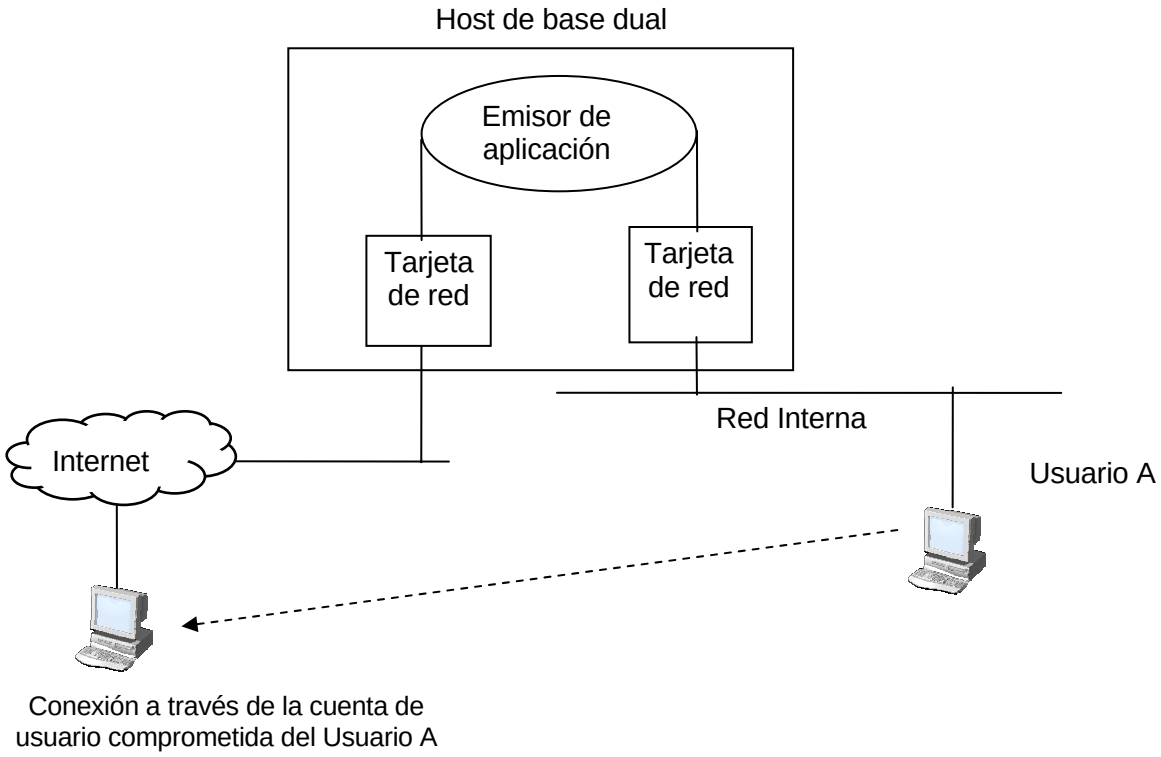


Figura 5.6 Inseguridad introducida con la conexión de usuario estándar a un host de base dual

Si el usuario selecciona una contraseña débil o permite que su cuenta de usuario se comprometa, la zona de riesgo puede extenderse a la red interna, frustrando así el propósito del firewall de base dual.

El administrador de seguridad prohibirá la creación de cuentas de usuario para tener acceso al firewall. El firewall sólo debe utilizarse para autenticar usuarios para permitir que sus sesiones pasen a través del firewall.

Si se conserva un registro apropiado de las conexiones de usuarios, es posible rastrear conexiones no autorizadas al firewall cuando se ha descubierto una brecha de seguridad. Sin embargo, si los usuarios no tienen permitido conectarse directamente al firewall de base dual, cualquier intento de conexión directa de usuario se registrará como un evento digno de atención y una potencial brecha de seguridad.

Ejemplos de servicios de almacenamiento y envío son SMTP (correo) y NNTP (noticias). En la Figura 5.7 se muestra una situación donde el host de base dual está configurado para proporcionar envío discrecional de mensajes de correo entre una red externa no confiable y una red interna.

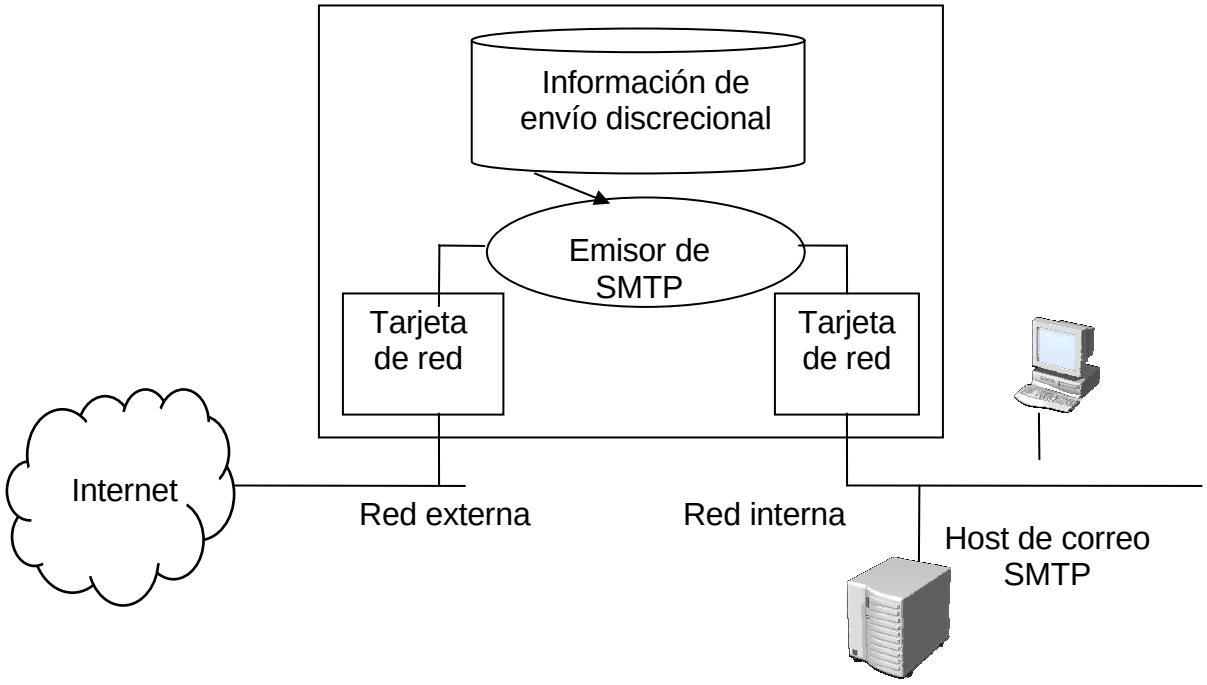


Figura 5.7 Host de base dual como emisor de correo

En la Figura 5.8 se muestra una situación donde el host de base dual está configurado para proporcionar envío discrecional de mensajes de noticias entre servidores de una red externa no confiable y una red interna.

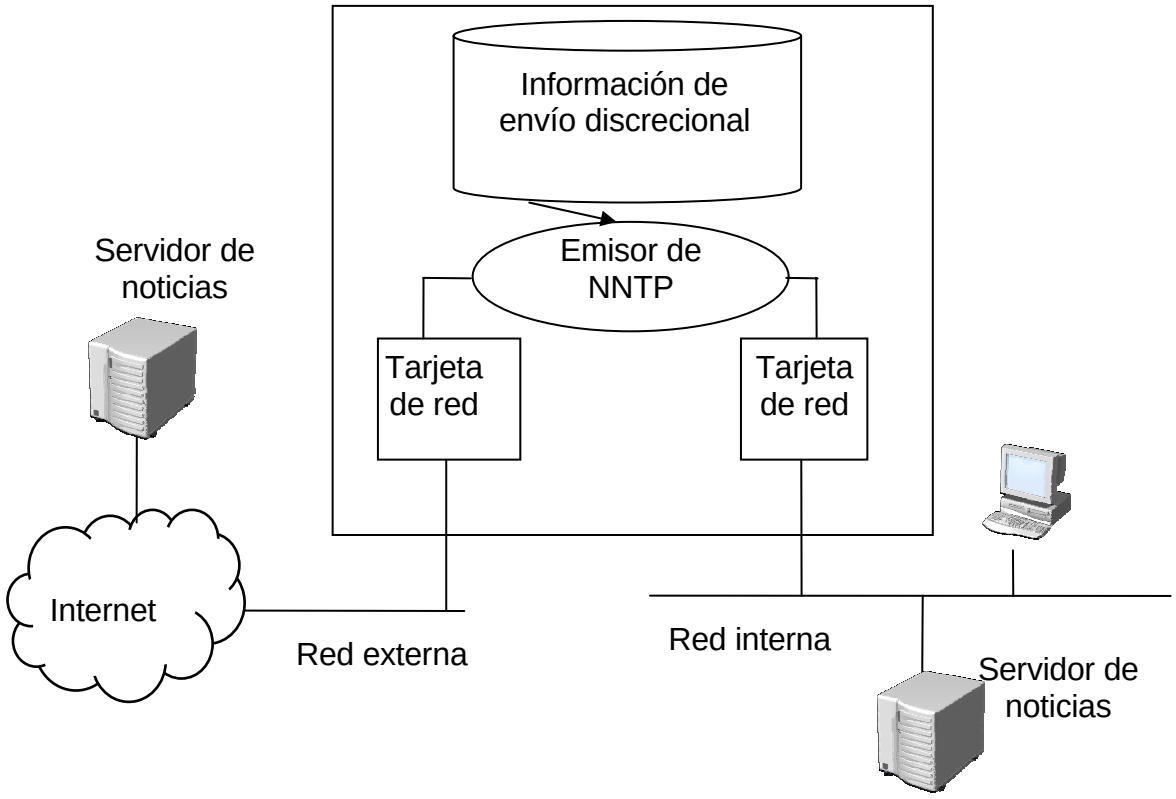


Figura 5.8 Host de base dual como emisor de noticias

El host de base dual es la configuración básica utilizada en firewalls. El aspecto importante de los hosts de firewall de base dual es que se inhabilita el enrutamiento y que la única ruta entre los segmentos de red es a través de una función de capa de aplicación.

Si el enrutamiento se configura mal por accidente (o por diseño) de modo que se habilite el envío IP, es posible que se ignoren las funciones de la capa de aplicación de los firewalls de base dual, Figura 5.9.

La mayoría de los firewalls se construyen con base en máquinas Unix. En algunas implementaciones de Unix, las funciones de enrutamiento están permitidas de manera predeterminada. Por lo tanto, es importante verificar que las funciones de enrutamiento del firewall de base dual estén inhabilitadas o, si no lo están, el encargado de seguridad debe saber cómo inhabilitarlas.

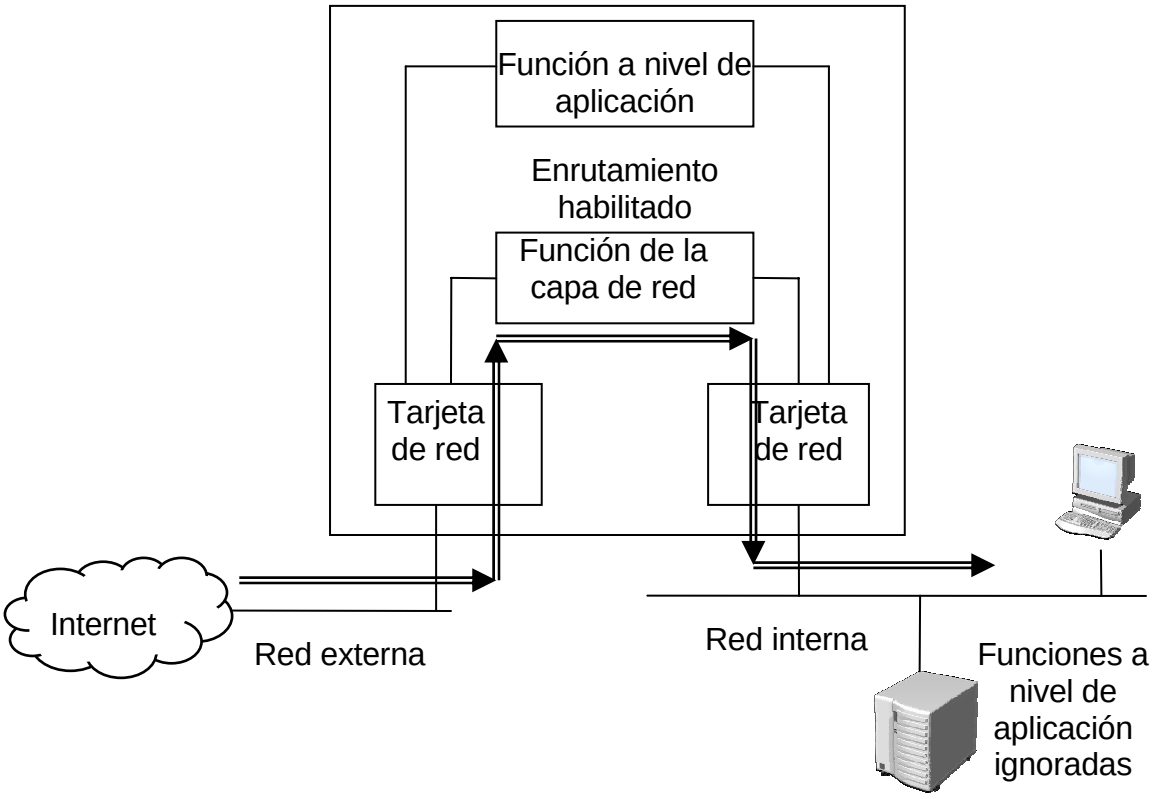


Figura 5.9 Firewall de base dual mal configurada

Cómo comprometer la seguridad de un firewall de base dual

Se deben conocer las acciones que pueden comprometer la integridad de un firewall de base dual. Con este conocimiento se pueden tomar las medidas para evitar que esto ocurra.

La amenaza más grande es que un intruso obtenga acceso directo al host de base dual. La conexión siempre debe establecerse a través de un proxy de aplicación en el host de base dual. Las conexiones desde redes externas no contables deben sujetarse a una autenticación estricta.

El único acceso al firewall mismo debe ser a través de la consola de operación.

Si el usuario obtiene acceso directo al host de base dual, la red interna estará sujeta a intrusiones.

Estas intrusiones pueden provenir de cualquiera de las siguientes fuentes:

Permisos débiles en el sistema de archivos.

Red interna con volúmenes montados en NFS.

Permisos otorgados a utilerías "r"[2] de Berkeley a través de archivos equivalentes de host, como rhosts, en directorios base de usuarios para cuentas de usuarios que han sido comprometidos.

[2] Bello, Claudia. *Manual de seguridad en redes*. Secretaría de la Función Pública. Argentina. 2002. Página 19.

Los comandos “r” provienen del sistema de autenticación del UNIX BSD. Un usuario puede realizar un rlogin a una máquina remota sin ingresar password si el criterio de autenticación es el correcto. Estos criterios consisten en:

La conexión debe originarse desde un puerto TCP privilegiado. En sistemas como pc’s con Windows 95, por ejemplo, estas restricciones no existen con lo cual no tienen mucho sentido. Como corolario, rlogin y rsh deben ser permitidos sólo desde máquinas donde esta restricción exista.

El usuario y la máquina cliente deben estar listados en la máquina server, como socios autenticados, típicamente /etc/hosts.equiv o en el directorio home del usuario, en el archivo .rhosts.

Desde el punto de vista del usuario, este esquema es muy interesante. El usuario no es molestado con prompts de passwords en logins que utiliza frecuentemente. Pero desde el punto de vista del hacker, los comandos “r” ofrecen dos ventajas: una manera de entrar a un sistema, y una vez dentro, una forma de ganar acceso a máquinas de confianza de la primera máquina hackeada.

El principal objetivo del hacker es colocar una entrada apropiada en /etc/hosts.equiv o .rhosts. Para ello utilizan FTP, UUCP, TFTP u otros medios. Por ejemplo, pueden utilizar FTP para dejar .rhosts en /usr/ftp o UUCP, para dejarlo en /usr/spool/uucppublic. Obviamente, uno debe verificar la estructura de permisos de la máquina server para prohibir eso.

Una vez adquirido el acceso no autorizado, muchas otras computadoras son accesibles. El hacker accede a /etc/hosts.equiv de la máquina atacada, y de ahí puede seguir su cadena de accesos, obteniendo más archivos /etc/passwd.

La implementación de comandos “r” presenta un problema adicional:

Parte de la seguridad del sistema puede residir en decisiones del usuario y no del administrador. En efecto, el usuario puede hacer que su archivo .rhosts sea de lectura y escritura para todos los otros usuarios. Algunas implementaciones de rlogin y rsh solucionan esto: si el usuario no lo hace, un cron se ocupa que los archivos .rhosts estén con sus permisos en orden.

Dado las debilidades del sistema de autenticación de los comandos “r” que se han visto, no se recomienda que estos servicios estén disponibles en sistemas accesibles directamente en Internet.

La alternativa usual a emplear rlogin es usar telnet, que transmite por la red un password, mientras que rlogin no lo hace.

Programas de respaldo de red que pueden restaurar permisos excesivos.

Uso de scripts de shell administrativos que no han sido asegurados apropiadamente.

Instalación de kernels antiguos de sistema operativo que tienen habilitado el envío IP, o instalación de versiones de kernels antiguos de sistemas operativos con problemas de seguridad conocidos.

El uso de programas de rastreo como tcpdump o etherfind para "rastrear" la red interna que busca la información del nombre de usuario y de la contraseña.

Si falla el host de base dual, la red interna está abierta de par en par para intrusos futuros, a menos que se detecte el problema y se corrija rápidamente.

La variable ipforwarding del kernel de Unix controla el desarrollo del enrutamiento IP. Si el intruso obtiene suficientes privilegios de sistema, puede cambiar el valor de esta variable del kernel y habilitar el envío IP. Con el envío IP permitido, se ignora el mecanismo de firewall.

Servicios en un firewall de base dual

Además de inhabilitar el envío IP, se deben eliminar todos los programas, utilerías y servicios del firewall de base dual que pueden resultar peligrosos en manos de un intruso. La siguiente es una lista parcial de algunos puntos de verificación útiles para firewalls de base dual de Unix:

- Hay que eliminar las herramientas de programación: compiladores, ruteadores, etc.
- Eliminar los programas con permisos SUID y SGID que no se necesiten. Si las cosas no funcionan, siempre es factible restaurar los programas esenciales. Si se tiene experiencia, hay que construir un monitor de espacio de disco que apague el host de base dual en caso de que se llene una partición crítica del disco.
- Utilizar particiones de disco para que una intrusión que intente llenar todo el espacio de disco de la partición sea confinada únicamente a esa partición.
- Eliminar las cuentas especiales y de sistema innecesarias.
- Eliminar servicios de red que no sean necesarios. Utilizar el comando netstat para verificar que sólo tenga los servicios de red que necesita. Editar los archivos /etc/inetd.conf y /etc/services y eliminar definiciones innecesarias de servicios.
- Modificar los scripts de inicio del sistema para evitar la inicialización de programas innecesarios como routed/gated y cualquier programa de soporte de enrutamiento.

5.1.5. Hosts de bastión

Un host de bastión es cualquier host de firewall que resulta determinante para la seguridad de la red. El host de bastión es el host central en la seguridad de red de una organización.

Debido a que el host de bastión es determinante para la seguridad de la red, debe estar bien fortificado. Esto significa que los administradores de red deben monitorear de cerca el host de bastión. El software de host de bastión y la seguridad del sistema deben auditarse con regularidad. Los registros de acceso deben examinarse en busca de cualquier brecha potencial de seguridad y cualquier intento de asalto al host de bastión.

El host de base dual analizado antes es un ejemplo de un host de bastión, ya que resulta crítico para la seguridad de la red.

El despliegue más simple de un host de bastión

Debido a que los hosts de bastión actúan como punto de interfaz a una red externa no confiable, a menudo son sujetos de intrusión. El despliegue más simple de un host de bastión es como el primero y único punto de entrada para el tráfico de la red externa, Figura 5.10.

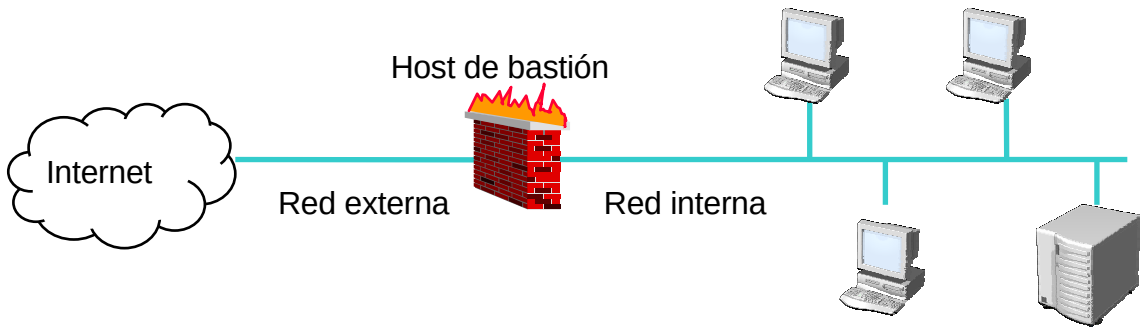


Figura 5.10 Despliegue de un host de bastión

La red de la Figura 5.10 es una configuración en la que se puede seguir la ruta del tráfico de red desde la red externa a la interna y consta de un host de bastión con dos conexiones de red.

5.1.6. Gateway de host seleccionado

Debido a que el host de bastión es crucial para la seguridad de la red interna, a menudo se introduce otra primera línea de defensa entre la red externa no confiable y la red interna. La primera línea de defensa es proporcionada generalmente por un ruteador de selección.

En la Figura 5.11 se muestra el uso de un host de bastión con un ruteador de selección como primera línea de defensa. En este ejemplo sólo está configurada la interfaz de red el host de

bastión, la cual se encuentra conectada a la red interna. Uno de los puertos del ruteador de selección está conectado a la red interna y el otro a Internet. A este tipo de configuración se le llama gateway de host seleccionado.

Utilizando la notación definida en este capítulo, la configuración del gateway de host seleccionado, mostrada en la Figura 5.11, puede describirse como configuración S-B 1 o sólo "SB1".

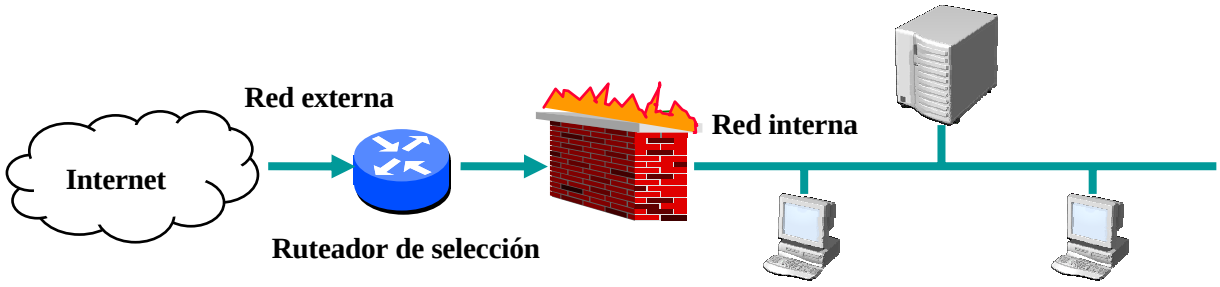


Figura 5.11 Host de bastión con un ruteador de selección (configuración SB1)

Se debe configurar el ruteador de selección para que éste le envíe primero al host de bastión todo el tráfico que la red interna recibe de las redes externas. Antes de enviarle el tráfico al host de bastión, el ruteador de selección aplicará sus reglas de filtración al tráfico de paquetes. Sólo tráfico de red que pasa las reglas de filtración se desvía al host de bastión; el resto del tráfico de red es rechazado. Esta arquitectura da un nivel de confianza a la seguridad de la red que no se ve en la Figura 5.10. Un intruso debe entrar primero al ruteador de selección y después, si consigue, debe enfrentarse con el host de bastión.

El host de bastión utiliza funciones a nivel de aplicación para determinar si se permiten o niegan las solicitudes que van y vienen de la red externa. Si la solicitud pasa la investigación del host de bastión, se envía a la red interna para el tráfico entrante. Para el tráfico saliente, (tráfico a la red externa), las solicitudes se envían al ruteador de selección.

5.1.7. Cómo descargar la filtración de paquetes al IAP

Algunas organizaciones prefieren que su proveedor de acceso a Internet (IAP, Internet Acces Provider) proporcione reglas de filtración de paquetes para el tráfico que llega a su red. El filtro de paquetes todavía actúa como primera línea de defensa, pero se tiene que apoyar en el IAP para el correcto mantenimiento de las reglas de filtración de paquetes.

5.1.8. Limitaciones del firewall

La limitación más grande que tiene un firewall sencillamente es el hueco que no se tapa y que coincidencialmente o no, es descubierto por un hacker. Los firewalls no son sistemas inteligentes, ellos actúan de acuerdo a parámetros introducidos por el diseñador. Por lo tanto, si un paquete de información no se encuentra dentro de estos parámetros como una amenaza de peligro, simplemente lo dejará pasar. Pero esto no es lo más peligroso, lo verdaderamente peligroso es que ese hacker deje "back doors" es decir abra un hueco diferente y borre las pruebas o indicios del ataque original.

Otra limitación es que el firewall "no es contra humanos", es decir que si un hacker logra entrar a la organización y descubrir passwords o se entera de los huecos del firewall y difunde la información, el firewall no se dará cuenta.

Es claro que el firewall tampoco provee de herramientas contra la filtración de software o archivos infectados con virus.

5.2. Proxies

Con los "Packet Filtering Firewalls" sólo es posible realizar filtrajes cuando los criterios están limitados a las direcciones y a los puertos. Una de las técnicas más usadas para resolver este problema son los proxies.

5.2.1. Introducción a los servidores proxy

Los servidores proxy, Figura 5.12 (el término proxy significa representante), proporcionan el acceso a una red insegura para determinados protocolos de aplicación a través de un host con doble acceso. El programa del cliente se comunica con el servidor proxy en lugar de hacerlo directamente con el servidor real situado en la red insegura. El servidor proxy es el encargado de evaluar las solicitudes del cliente y decide cuáles deja pasar y cuáles no. Si una petición es aceptada, el proxy se comunica con el servidor real en nombre del cliente y lleva a cabo las peticiones de servicio del cliente al verdadero servidor y transmite las respuestas de éste de nuevo al cliente.

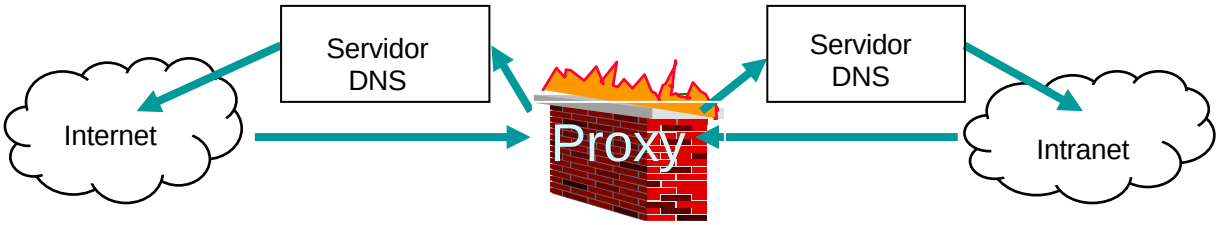


Figura 5.12 Servidor proxy

Es importante realizar las conexiones a través de un proxy junto con algún método de restricción de tráfico IP entre los clientes y los servidores en la red insegura, como un ruteador con filtrado de paquetes o un host con doble acceso que no enrute paquetes. Si hay conectividad a nivel IP entre clientes y servidores de la red insegura, los clientes pueden saltarse el servidor proxy y producirse ataques desde el exterior.

5.2.2. Ventajas y desventajas de los servidores proxy

Ventajas de los servidores proxy

Acceso directo a la red externa

Si se utiliza la arquitectura de host con doble acceso, un usuario debe iniciar una sesión con el host antes de utilizar cualquier servicio de la red exterior, algo que resulta molesto para la mayoría de usuarios.

Al utilizar un servidor proxy, los usuarios pueden conectarse de una forma más o menos transparente a un servidor de la red externa de forma directa sin que se den cuenta que están pasando por una máquina intermedia, el servidor proxy. No obstante, esto requiere reconfiguraciones en los programas cliente (navegador HTTP, cliente FTP, etc.).

Gracias a que los servidores proxy trabajan a nivel aplicación resulta fácil generar archivos de registro o monitorear las conexiones de los usuarios a cada tipo de servicio de forma cómoda sin tener que profundizar a nivel IP.

Desventajas de los servidores proxy

Disponibilidad de servidores para nuevos servicios

Debido a que es necesario un servidor proxy específico para cada tipo de servicio esto resulta bastante problemático a la hora de utilizar servicios de reciente aparición. Aunque existen servidores proxy para la gran mayoría de servicios (HTTP, Telnet, FTP, SMTP, etc.) el

administrador de red puede encontrarse en la necesidad de utilizar un nuevo servicio para el cual todavía no se ha creado ningún proxy.

Dependencia del servicio

Puede ser necesario utilizar un servidor proxy exclusivo para cada protocolo. La instalación, configuración y administración de varios servidores puede requerir mucho trabajo.

También existen servicios para los cuales difícilmente existirá alguna vez un servidor proxy. Son servicios como talk es decir el servicio de mensajería comúnmente conocido como chat, con interacciones complicadas y desordenadas entre cliente y servidor.

Modificaciones en los clientes:

La utilización de un servidor proxy requiere la modificación o configuración de los clientes. Esto requiere tiempo y trabajo. Los navegadores HTTP de última generación incluyen la opción centralizada de configuraciones para proxy.

Desde un puesto de trabajo, el administrador pueda cambiar la configuración en lo que respecta a servidores proxy de todos los clientes de forma automatizada.

5.2.3. Tipos de servidores proxies

Servidores proxy a nivel de aplicación y a nivel de circuito.

Un proxy a nivel de aplicación conoce la aplicación o servicio específico para el cual está proporcionando los servicios de proxy, es decir, comprende e interpreta los comandos en el protocolo de aplicación.

Un proxy a nivel de circuito crea un circuito entre el cliente y el servidor sin interpretar el protocolo de aplicación. Normalmente se utiliza con aplicaciones como SMTP, que implementa un protocolo de guardar y enviar. La versión más avanzada de un proxy a nivel de circuito actúa como proxy para el exterior, pero como ruteador con filtrado para el interior.

En general, los proxy a nivel de aplicación emplean procedimientos modificados y los proxy a nivel de circuito clientes modificados. Esto se relaciona con los aspectos prácticos del proxy.

Un proxy a nivel de aplicación obtiene la información necesaria para conectarse al servidor exterior del protocolo de aplicación. Un proxy a nivel de circuito no puede interpretar el protocolo de aplicación y necesita que le proporcione la información a través de otros medios (por ejemplo, mediante un cliente modificado que le dé al servidor la dirección de destino).

La ventaja de un proxy a nivel de circuito es que proporciona servicios para una amplia gama de protocolos. La mayoría de los servidores proxy a nivel circuito también son servidores proxy genéricos; pueden adaptarse para servir casi a cualquier protocolo.

No todos los protocolos pueden manejarse fácilmente por un proxy a nivel de circuito. Los protocolos como FTP, que comunican datos del puerto cliente al servidor, necesitan cierta intervención a nivel de protocolo y, por lo tanto, ciertos conocimientos a nivel de aplicación.

La desventaja de un servidor proxy a nivel circuito es que proporciona muy poco control sobre lo que circula a través del proxy.

Al igual que el firwall de filtro de paquetes, controla las conexiones con base en su fuente y destino y no puede determinar fácilmente si los comandos que están pasando a través de él son seguros o están en el protocolo esperado.

Servidores proxy genéricos y dedicados

Un servidor proxy dedicado funciona para un único protocolo, mientras que uno genérico sirve para varios protocolos. En la práctica los servidores proxy dedicados son a nivel de aplicación y los genéricos son a nivel de circuito.

5.2.4. Servidores proxy inteligentes

Se denomina servidor proxy inteligente a aquellos que son capaces de hacer algo más que transmitir peticiones, como por ejemplo funciones de cache de datos (páginas web, archivos de FTP). A medida que se consoliden los servidores proxy sus habilidades se irán incrementando de forma rápida.

Generalmente los servidores proxy inteligentes son dedicados a aplicación. Un servidor proxy a nivel de circuito tiene habilidades limitadas.

Esquema del funcionamiento de un proxy

Paso 1. El usuario pide una URL cualquiera, Figura 5.13.

Paso 2. El requerimiento del usuario está en el servidor de la red, y el proxy comprueba si tiene esta URL en su memoria caché, Figura 5.14.

Paso 3. Si el proxy no cuenta con esa página en su caché la solicita al exterior, Figura 5.15.

Paso 4. Desde el exterior llegan los datos solicitados al servidor de la red, Figura 5.16.

Paso 5. El proxy incluye los datos en su caché y los transmite al usuario, Figura 5.17.

Paso 6. El usuario obtiene los datos en su pc, Figura 5.18.

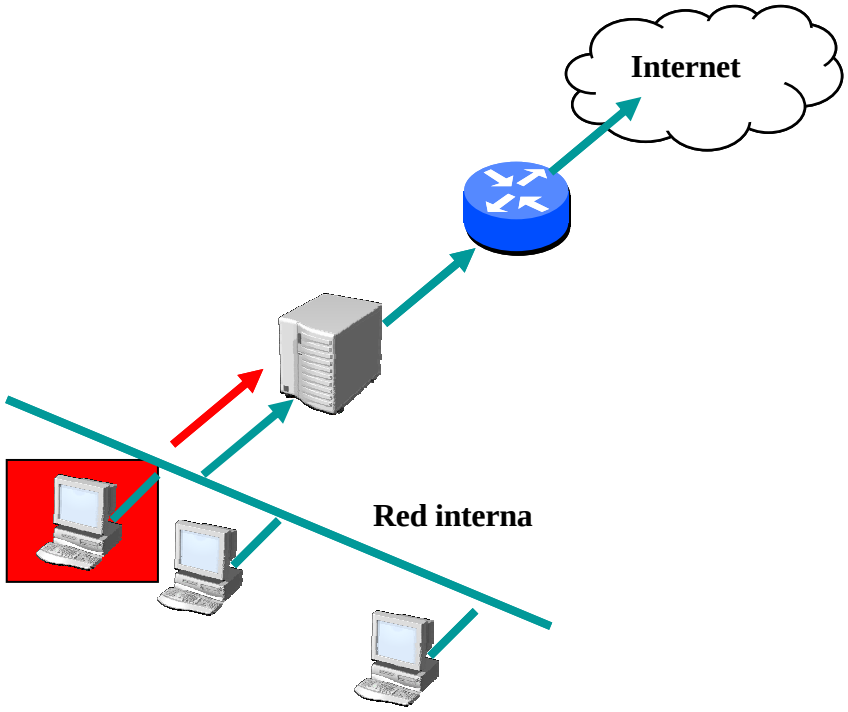


Figura 5.13 Paso 1 del funcionamiento de un servidor proxy

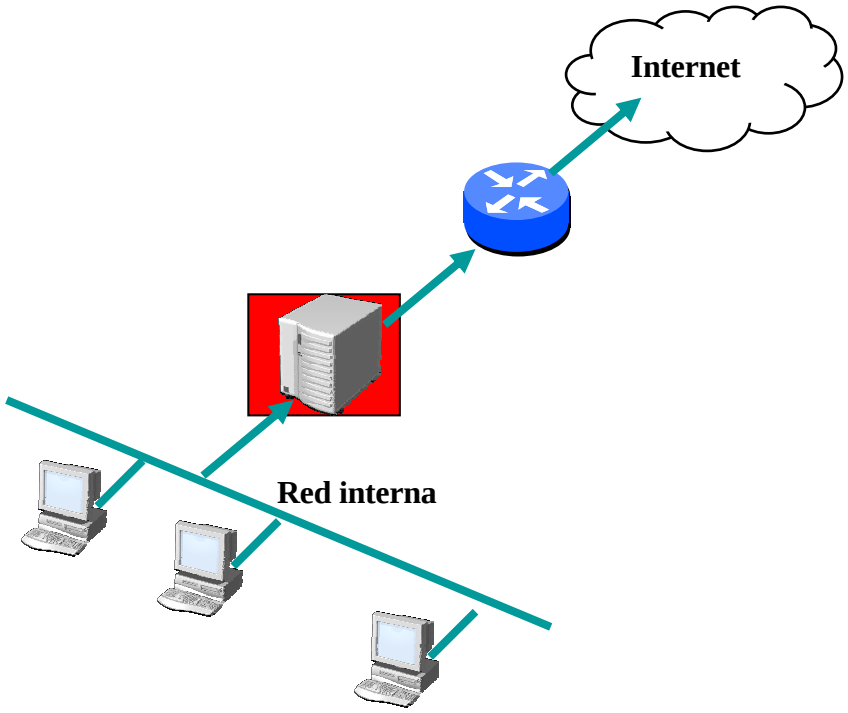


Figura 5.14 Paso 2 del funcionamiento de un servidor proxy

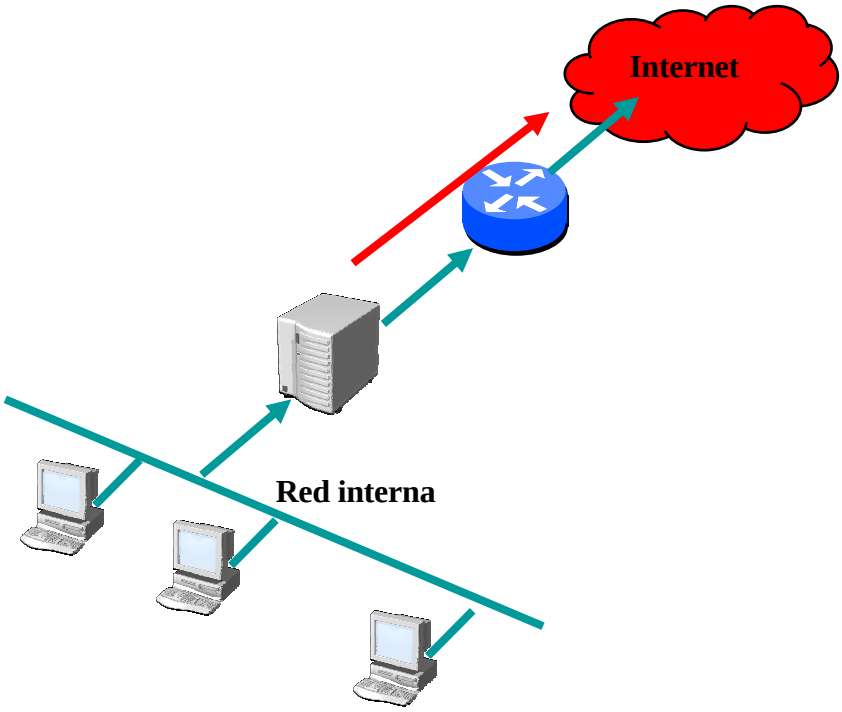


Figura 5.15 Paso 3 del funcionamiento de un servidor proxy

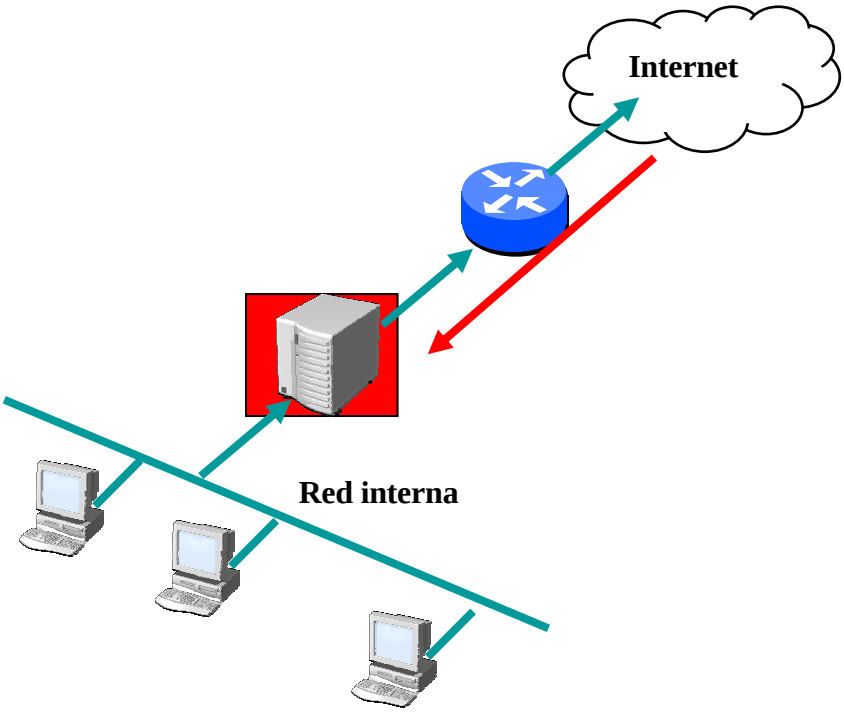


Figura 5.16 Paso 4 del funcionamiento de un servidor proxy

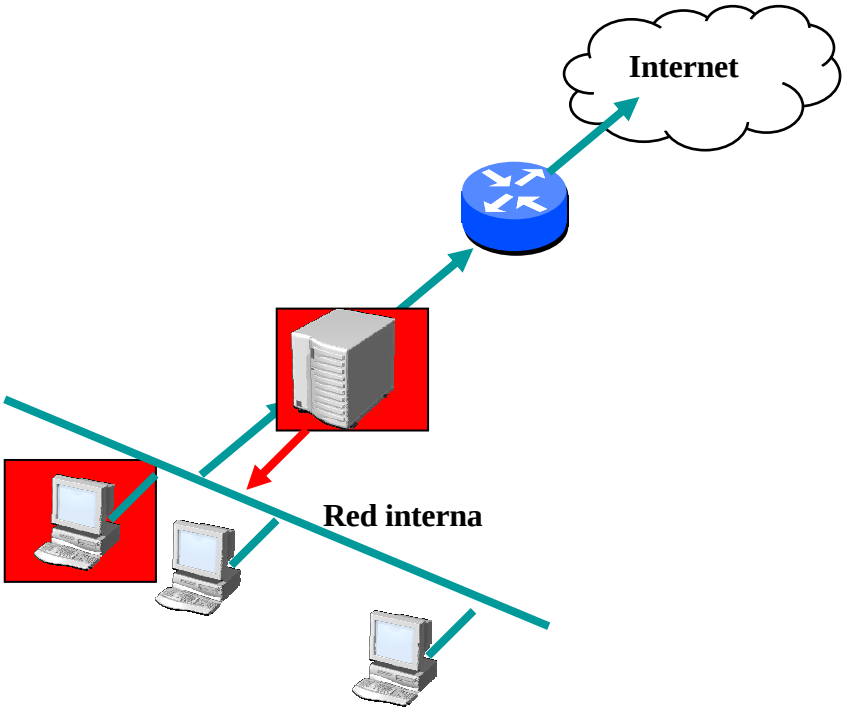


Figura 5.17 Paso 5 del funcionamiento de un servidor proxy

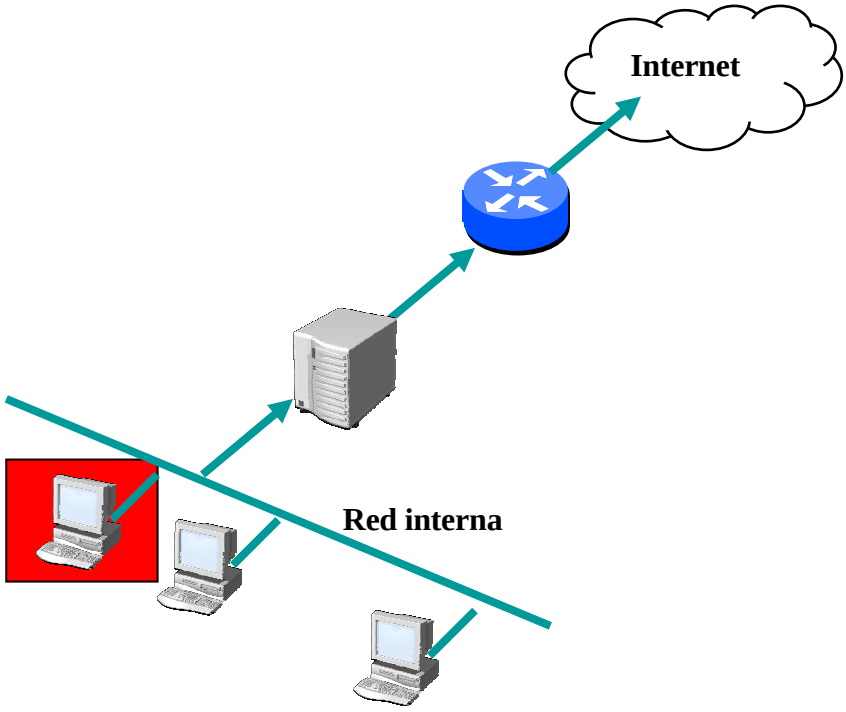


Figura 5.18 Paso 6 del funcionamiento de un servidor proxy

5.3. Sistemas detectores de intrusos IDS

Un sistema de detección de intrusos (IDS) es un sistema que permite identificar las amenazas dirigidas hacia una empresa o usuario y establecer un método de evitar que esa amenaza tenga el efecto deseado por el atacante.

Existen varios tipos de sistemas detectores de intrusos, los más comunes son los basados en red NIDS, los basados en Host HIDS en el apartado máquinas y sistemas de detección de intrusos de máquina en este capítulo y por último lo que se conoce como honeypots y honeynets, capítulo 5.4**.**

5.3.1. Sistema de detección de intrusos de una capa

Instalar un sistema de detección de intrusos, un componente cada vez más común de la seguridad en capas, "elevará el obstáculo aún más" para que el pirata informático tenga la determinación de efectivamente penetrar la red. Un IDS podrá:

- Aumentar los sistemas de control de acceso, como los firewalls, al alertar a los administradores de sistemas sobre intrusos reales o tentativas de ataques.
- Reconocer los ataques a la red que con frecuencia los firewalls no pueden ver; aquellos ataques que provienen del interior de la organización.
- Suministrar información que ayude a controlar o mitigar los daños después de una tentativa de ataques.

Así como un sistema de detección de intrusos es reconocido ampliamente como herramientas efectivas de seguridad, es importante recordar que un IDS no debe operar solo.

5.3.2. Otros elementos de la seguridad en capas

Incluso si el IDS de la red falla, los firewalls, la evaluación de vulnerabilidades y el software antivirus siguen siendo eficaces. Un firewall debidamente configurado puede bloquear los ataques más comunes antes de que un IDS de redes los detecte. La evaluación de vulnerabilidades puede identificar las debilidades y ayudar a eliminarlas. Si el sistema no tiene vulnerabilidades, los ataques reales fracasan incluso si no son detectados. Además, si el IDS no detecta la producción de virus conocidos, el firewall no bloquea la producción y la evaluación de vulnerabilidades no elimina los medios de infección, el software antivirus puede seguir detectando los virus conocidos.

5.3.3. Compromiso con la seguridad

Mantener la protección de la empresa exige un compromiso firme. Puesto que las amenazas, las vulnerabilidades y los requerimientos de la empresa cambian, las políticas de seguridad y los mecanismos adoptados deben ser reevaluados periódica y habitualmente para brindar protección total

Casos recientes de intrusos con un historial preponderante han demostrado que existe una desigualdad fundamental en la guerra informática, que consiste en que un atacante con poca experiencia e incluso una conexión a Internet por acceso telefónico pueden en un momento dado costarle a una organización millones de dólares y comprometer su reputación y destreza para hacer negocios. Si un pirata informático tiene la intención de causar daños a una empresa, probablemente lo logrará. El sistema de seguridad de multiniveles implementado aumentará los costos de penetración a la red por parte de los intrusos y requerirá más recursos que la mayoría de intrusos potenciales estaría dispuesto a invertir o en condiciones de hacerlo. La seguridad por niveles aumenta las posibilidades de que un intruso vaya en busca de sistemas menos protegidos.

Varias cualidades importantes de los IDS los ubican bastante más allá de los sistemas de administración de redes, los ruteadores, los firewalls y otros medios de protección de redes.

A diferencia de los productos de monitoreo remoto (RMON), los IDS no usan SNMP (que en estos momentos carece de rasgos de seguridad claves) para transmitir información del monitor al gerente. En lugar de ello, los IDS utilizan diversos medios de autenticación y codificado.

Algunos productos IDS incluyen también rutinas predefinidas para detectar ataques específicos, y permiten a vendedores y a usuarios agregar rutinas que detectan ataques nuevos apenas se los descubre. De todas maneras, existen grandes diferencias en cuanto a qué tipo de definiciones están disponibles para los usuarios.

Los agentes de un IDS basado en red monitorean el tráfico de red para enviar los datos al motor de análisis. Estos elementos de monitoreo pueden colocarse en distintos puntos de la arquitectura.

Uno de los objetivos de los agentes es el de no ser reconocido por atacantes, así como no interferir en el rendimiento de la red. Para ello, se suelen conectar al medio utilizando dispositivos de escucha. La interfaz de red dedicada al monitoreo se configura de forma que no tenga dirección IP. En algunas ocasiones, estos dispositivos se conectan a la red mediante un cable de sólo recepción o un "network tap" (dispositivo de escucha de red).

A continuación se describirán las localizaciones más comunes en las que se puede implementar un NIDS. Cada una tiene sus propias ventajas e inconvenientes.

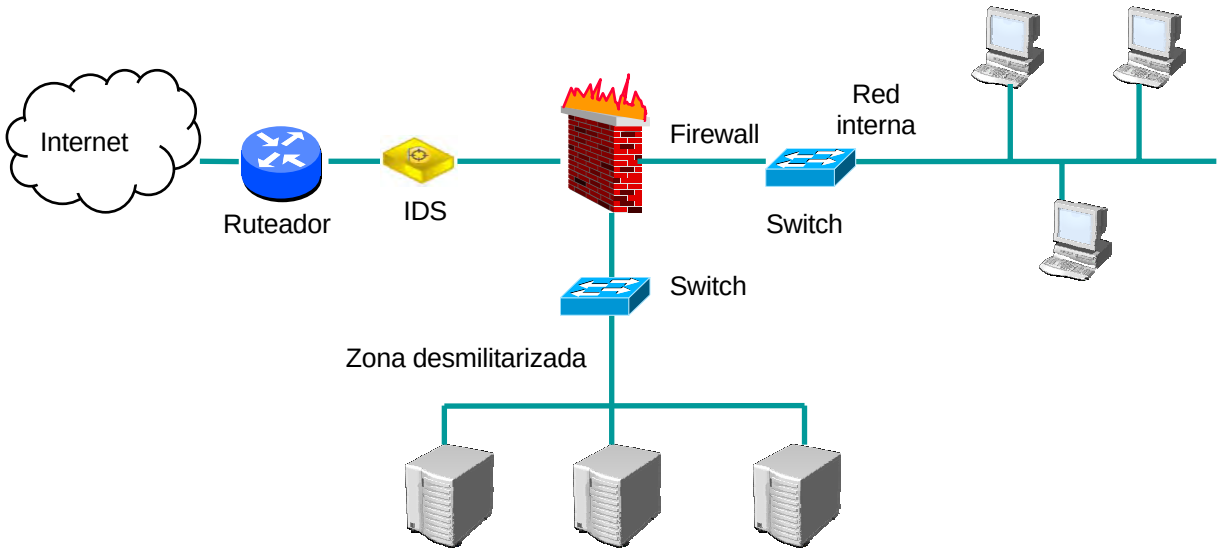


Figura 5.19 IDS colocado delante del firewall

Delante del firewall externo

Colocar los agentes delante del firewall externo, Figura 5.19, permite:

- Monitorear el número y tipo de ataques dirigidos contra la infraestructura de la organización.
- Detectar ataques cuyo objetivo es el firewall principal.

Por otra parte, esta posición también presenta algunos inconvenientes:

- No permite detectar ataques que utilicen en sus comunicaciones algún método para ocultar la información, como algoritmos de cifrado.
- En esta localización suele haber gran cantidad de tráfico de red. Un detector de intrusiones mal diseñado puede saturarse, descartando parte de la información que percibe, si no ha sido bien diseñado.
- Una situación como ésta no ofrece ninguna protección. El NIDS puede convertirse en un blanco fácil si algún atacante logra identificarlo.

Detrás del firewall externo

Esta localización situada entre Internet y la red interna, se denomina DMZ. Se utiliza para proporcionar servicios públicos sin tener que permitir acceso a la red privada de la organización. En esta subred se suelen ubicar los servicios principales de la infraestructura (servidores HTTP, FTP, SMTP, DNS, etc.). Normalmente está protegida por el firewall y otros elementos de seguridad.

Algunas de las ventajas de este caso son:

- Se monitorean intrusiones que logran atravesar el firewall principal.
- Se pueden detectar ataques dirigidos contra los servidores que ofrecen servicios públicos situados en esta subred.
- En caso de no detectar ataques con éxito, pueden reconocer algunas consecuencias de los mismos, como intentos de conexiones salientes, realizadas desde los servidores comprometidos.
- La identificación de los ataques y escaneos más comunes permite mejorar la configuración del firewall principal.

A continuación se indican algunas de las desventajas de esta localización:

- No permite identificar ataques que utilicen métodos para ocultar la información contenida en sus comunicaciones, como algoritmos de cifrado.
- La cantidad de tráfico existente normalmente en este segmento de red, puede hacer que el NIDS no pueda analizarla toda, descartando datos. Es importante diseñar un sistema capaz de responder ante situaciones críticas.

La seguridad del NIDS mejora con la inclusión del firewall que lo separa de la red exterior. Sin embargo, esto no excluye de tomar medidas adicionales para evitar que pueda ser comprometido por atacantes.

Redes principales

Cuando se monitorea el tráfico de red en las redes con mayor actividad, se obtienen estas ventajas:

Al haber más cantidad de tráfico, hay también más posibilidades de encontrar posibles ataques. Este hecho se cumple siempre que la cantidad de tráfico no supere la capacidad del NIDS.

Se pueden detectar ataques producidos desde dentro de la propia red, como los realizados por personal interno.

Las desventajas relacionadas con esta posición son, entre otras:

Al igual que en los casos anteriores, esta localización no permite detectar ataques que utilicen algoritmos de cifrado en sus comunicaciones.

No pueden evitar problemas asociados al uso de conmutadores en la red. Las características de estos dispositivos podrían impedir el monitoreo de los miembros de la red.

Esta situación hace que estos sistemas sean especialmente vulnerables ante ataques provenientes, no ya del exterior, sino del interior de la propia infraestructura. Es vital tener este aspecto en cuenta a la hora de implementar un detector de intrusiones en esta localización.

Subredes de valor crítico

A veces, los servidores y recursos más importantes de una red están situados en una subred, separada de la red principal mediante dispositivos como firewall. Para protegerlos debidamente, es necesario implementar detectores de intrusos basados en red en estas subredes privadas.

Algunas de las ventajas de tener separada de la red principal los servidores más importantes de una organización son:

- Detectar ataques realizados contra elementos críticos de la red.
- Dedicar especial atención a los recursos más valiosos de la infraestructura.

A continuación se mencionan algunas desventajas del uso de esta opción:

- Como ya se comentó en las situaciones anteriores, este caso no permite detectar ataques que utilicen algoritmos de cifrado en sus comunicaciones.
- No evitan problemas de monitoreo relacionados con el uso de conmutadores.
- No están estratégicamente bien situados ante ataques de origen interno.

Máquinas

Otra de las posibles formas de instalar este tipo de sistemas es en las propias máquinas, convirtiéndolas rastreadores de red. Los IDSs basados en red implementados de esta forma se denominan IDS de nodo de red (NNIDS) (Network Node IDS).

La mayoría de los productos de detección basados en red nombrados antes se pueden implementar de esta forma. Cualquier detector basado en red, que permita la instalación de uno de sus agentes en una máquina, puede ser utilizado de esta forma.

Esta localización proporciona ventajas únicas:

- Se evitan los inconvenientes de cifrado de las comunicaciones, presentes en las localizaciones anteriores. El NNIDS deja de recibir cifrado el tráfico originado o destinado a

la máquina en la que está instalado. No obstante, seguirá percibiendo cifradas el resto de las comunicaciones.

- Es una forma de solventar problemas derivados del uso de conmutadores, este tipo de dispositivos dificultan el monitoreo del tráfico red, realizando tareas de encaminamiento, cosa que no hacen los concentradores. Situar un detector en una máquina permite al menos, examinar sus propias comunicaciones.

Por otra parte, este enfoque también tiene inconvenientes:

- La visión del sistema de detección está claramente limitada tanto por la situación de la máquina, como por la arquitectura de la red. Por ejemplo, si se utilizan conmutadores, sólo puede analizar el tráfico relacionado con la máquina anfitriona. No obstante, si se hace uso de concentradores, analizaría además el tráfico del resto de los miembros de la red, actuando como un rastreador.

El NIDS está compartiendo los mismos recursos que la máquina que monitorea. Esto reduce los recursos de la misma, afectando evidentemente a su rendimiento final.

Que la máquina anfitriona sea comprometida puede tener graves consecuencias. El detector no sólo perdería toda eficacia, sino que además, podría ser controlado por el atacante para llevar a cabo sus fines. Obtener información sobre la infraestructura de la organización, o enviar falsas alarmas que distrajeran la atención del responsable de seguridad, son sólo algunos ejemplos de lo que un intruso podría hacer en dicha situación.

Sistemas de detección de intrusos de máquina

En una estrategia de implementación general, los detectores de intrusos basados en máquina (host) se suelen instalar después de los basados en red. Esto se hace así ya que, dadas sus características, son más complicados de instalar, Figura 5.20.

Este tipo de sistemas necesita ser configurado de forma individual en cada máquina, y utiliza como fuente de datos la información obtenida del sistema.

La mayoría de los detectores de intrusos incluyen, entre otras funciones, mecanismos de verificación de integridad de archivos. Esto les permite, mediante el uso de algoritmos de cifrado como funciones resumen, reconocer cambios en los archivos más importantes del sistema.

Aunque la situación ideal es la de contar con uno de estos sistemas en cada una de las máquinas de la red, lo cierto es que el procedimiento más extendido a seguir es el de instalarlos primero en los servidores más importantes. Una vez que los responsables se han acostumbrado a esta situación, se pueden ir implementando en el resto de los equipos.

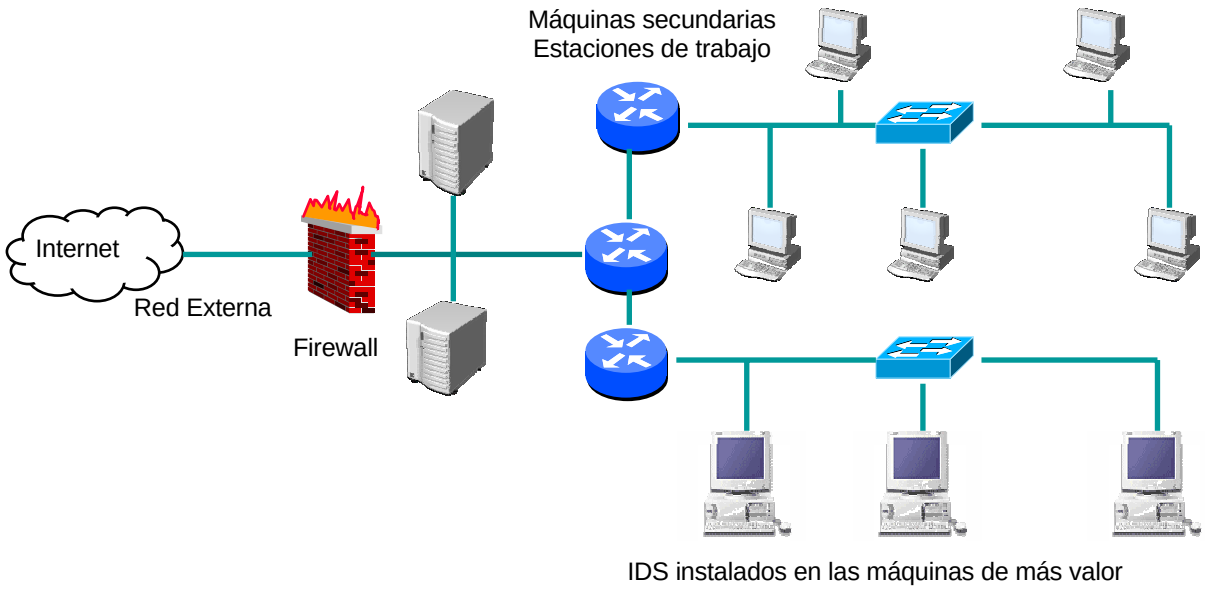


Figura 5.20 Implementación progresiva de HIDS

Es muy importante que los administradores de los detectores de intrusos se acostumbren a la forma de trabajar de estos sistemas, afinando la configuración para adaptarla a su situación particular, y aprendiendo a distinguir entre las falsas alarmas y los verdaderos problemas de seguridad.

Los informes emitidos por los detectores basados en máquina deben ser revisados de forma periódica. No siempre es posible ir examinando individualmente cada detector. Por ello, muchos productos facilitan mecanismos de centralización de registros, que permiten gestionar las alarmas de una forma más cómoda, rápida y eficiente.

Algunas de las ventajas del uso de estos sistemas son:

Trabajan con el sistema de archivos, y con registros de sistema operativo locales, por lo que pueden detectar ataques que no identifican los detectores basados en red.

Su especialización les otorga ventaja a la hora de detectar ataques específicos de los sistemas que monitorean.

Su posición privilegiada les permite identificar con precisión los elementos involucrados en un ataque, tales como procesos de sistema, archivos o nombres de usuario.

Dada su naturaleza, este tipo de sistemas no se ve afectado por un entorno de red con conmutadores.

5.3.4. Aspectos a tener en cuenta a evaluar un IDS

Cuando la empresa ha decidido comprar e instalar una solución de detector de intrusos, es necesario tomar varios factores en cuenta para realizar la mejor compra, entre los que se encuentran los siguientes:

- Costo/beneficio.
- Cantidad de protocolos que puede analizar.
- Cantidad de firmas que puede detectar.
- ¿Qué respuestas puede ejercer?.
- Actualización de nuevas firmas de ataque.
- Desempeño en redes de alto tráfico.
- ¿Qué tan fácil es de evadir?
- ¿Qué tan vulnerable es?
- ¿Qué tan escalable es?
- ¿Cómo disminuye los falsos positivos?

5.4. Honeypots y honeynets

Los sistemas descritos a continuación presentan un enfoque innovador con respecto a los sistemas de seguridad tradicionales. En vez de repeler las acciones de los atacantes, utilizan técnicas para monitorearlas y registrarlas, para así aprender de ellos. A pesar de que en algunos países no están claramente definidos los aspectos legales de estos sistemas, lo cierto es que cada vez son más utilizados.

Honeypot

Un honeypot, Figura 5.21, no es un sistema de detección de intrusiones, pero puede ayudar a mejorar sus métodos de detección y aportar nuevos patrones de ataque. Es un sistema diseñado para engañar a los intrusos, poder estudiar sus actividades, y así aprender de sus métodos. Se basa en la idea de conocer al enemigo para poder combatirlo; el valor de este dispositivo en el uso no autorizado o ilícito de dichos recursos.

Los sistemas trampa están diseñados para imitar el comportamiento de aquellos sistemas que puedan ser de interés para un intruso. Suelen contar con mecanismos de protección para que un atacante con éxito no pueda acceder a la totalidad de la red.

Naturalmente, si un intruso consigue entrar en un sistema trampa, no debe percatarse de que está siendo monitoreado o engañado.

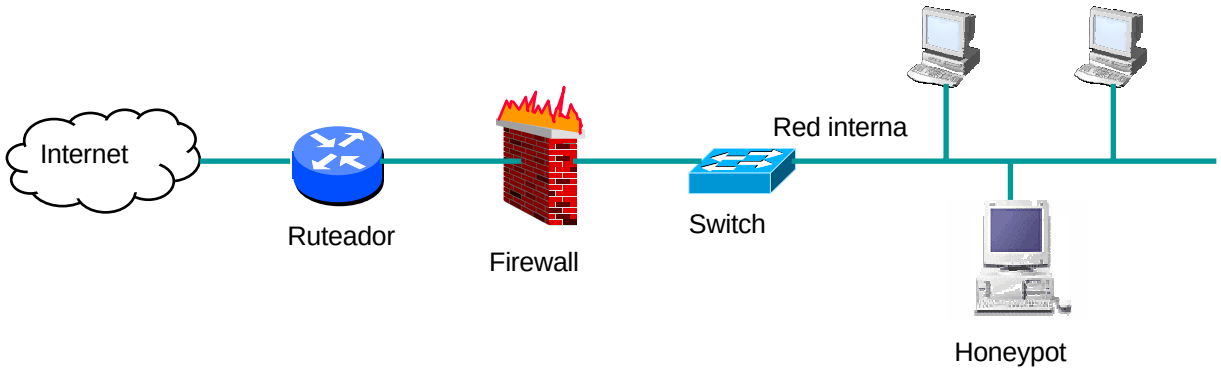


Figura 5.21 Ejemplo de un honeypot, sistema trampa

La mayoría de los sistemas trampa están instalados detrás de un firewall, aunque también es posible situarlos delante de ellos. El firewall responsable del tráfico de un sistema trampa suele programarse para permitir las conexiones entrantes al sistema, y limitar las conexiones salientes.

Ventajas e inconvenientes

Los sistemas trampa poseen una serie de características que los distinguen claramente de otras soluciones de seguridad. A continuación se describen algunas de las ventajas e inconvenientes asociadas a los mismos.

Ventajas

Pocos y valiosos datos. Los sistemas trampa registran poco volumen de datos, pero de mucho valor. Un sistema trampa no se utiliza como sistema de producción, sino únicamente como objeto de ataques. Por lo tanto, no suele registrar cantidades importantes de información. Sin embargo, toda esta información es útil, porque está relacionada con actividades hostiles. Esto hace, además, que los datos obtenidos sean claros y fácilmente analizables.

Falsas alarmas

La filosofía de los sistemas trampa elimina la existencia de actividad normal o de producción en los mismos. Estas herramientas de seguridad sólo deben recibir únicamente actividades sospechosas. Esto reduce significativamente el número de falsos positivos (alarma cuando no existe ataque) y falsos negativos (omisión de alarma cuando hay verdaderamente un ataque).

Recursos

Este tipo de herramientas no hace análisis de las actividades que registran. Por tanto, los recursos que consumen son reducidos, al contrario que muchos IDSs, que pueden llegar a descartar información por esta razón. Los sistemas trampa centran sus necesidades en la infraestructura necesaria para poder registrar toda la actividad que tenga lugar en ellos.

Simplicidad

Uno de los puntos más importantes a favor de los sistemas trampa es su sencillez. No utilizan complicados algoritmos de análisis, ni rebuscados métodos para registrar la actividad de los intrusos. Por el contrario, sólo hay que instalarlos y esperar. Algunos sistemas trampa de desarrollo pueden poseer mayor nivel de complejidad, pero no comparable a otros enfoques. Cuanto más sencillo es un método, más posibilidades tiene de funcionar.

Cifrado

Los problemas de monitoreo relacionados con protocolos de cifrado (SSH, SSL, IPSec, etc.) aparecen cuando se intercepta una comunicación entre dos entidades, protegida mediante cifrado. Los sistemas trampa suelen ser uno de los extremos de la comunicación cifrada durante una intrusión o ataque. Además, registran en todo momento la actividad ocurrida.

Reutilización

La mayoría de los productos de seguridad necesitan mantener al día sus mecanismos de detección y defensa para mantener su efectividad. Si no se renuevan, dejan de ser útiles. No obstante, los sistemas trampa, debido a su propia naturaleza, siempre serán de ayuda. Independientemente del tiempo que pase, siempre habrá atacantes dispuestos a comprometer estos sistemas de una u otra forma, mostrando el nivel de actividad de este sector y los métodos que utilizan.

IPv6

Uno de los problemas que presentan algunas herramientas de seguridad es que no soportan el protocolo IPv6, sucesor del actual IPv4 ampliamente utilizado en Internet. Este protocolo está siendo principalmente utilizado en países asiáticos como Japón. Utilizar IPv6 utilizando túneles sobre IPv4, como hacen algunos atacantes, puede imposibilitar la detección por parte de muchos sistemas de detección. No obstante, los sistemas trampa registran toda la actividad

ocurrida, por lo que se pueden identificar este tipo de ataques. Como ya se comentó, los sistemas trampa no registran grandes volúmenes de datos.

Desventajas

- Punto de vista limitado
- Riesgo

Punto de vista limitado

Los sistemas trampa carecen de valor si no reciben ataques. Si un atacante logra identificar uno de estos sistemas, puede anular toda su efectividad evitándolos. Los sistemas trampa pueden no ser atacados, aún estando situados en la misma red que otros sistemas de producción que sí pueden ser objeto de ataques.

Riesgo

Si un sistema trampa es atacado con éxito puede ser utilizado por el intruso para acceder al resto de sistemas de la red en que está instalado. El riesgo varia según el grado de complejidad del sistema trampa; cuanto más sencillo es, menores riesgos implica. Este aspecto es crítico a la hora de implementar este tipo de sistemas. Y siempre se toman medidas para minimizar este factor.

Finger print (huella dactilar)

Fingerprinting consiste básicamente en la identificación, local o remota, de un sistema o servicio. Esto se hace a través de diversos métodos, como por ejemplo realizando un escaneo de puertos, o enviando peticiones de solicitud de versión, u observando las respuestas del sistema ante determinados comandos. Es posible que la deficiente implementación de un sistema trampa lo delate, haciéndolo reconocible ante un intruso. Por ejemplo, si un sistema trampa que emula un servidor FTP, no implementa bien un comando como prompt, y sí reconoce prompt, esto se convierte en un patrón que lo hace identificable a los ojos de un atacante. Un sistema trampa, como ya se comentó, pierde eficacia cuando es reconocido por un atacante, convirtiéndose incluso en una herramienta que puede ser utilizada por éste para desviar la atención de un administrador de seguridad. No obstante, en ocasiones, un atacante puede cesar en sus actividades al percatarse de la existencia de un sistema de estas características.

Honeynet

La idea de honeypot es desarrollada con el término honeynet, red trampa. Esta expresión fue adoptada por "The Honeynet Project"; una organización no lucrativa, fundada por Lance Spitzner. Este grupo está compuesto por expertos en seguridad, cuyo objetivo es aprender las herramientas, tácticas y motivos de los atacantes.

Una honeynet es una herramienta de investigación. Es un tipo de honeypot que consiste en una red diseñada para ser comprometida por intrusos. Sirve para estudiar las técnicas utilizados por los intrusos que la han comprometido.

Una honeynet no es lo mismo que un sistema trampa tradicional. A continuación se describen las diferencias más significativas:

- Una honeynet no es un sistema en solitario, sino una red. Esta red puede estar compuesta por distintos sistemas trampa, tales como Linux, Windows, Solaris, ruteadores, conmutadores, etc. El hecho de proporcionar un entorno de red aporta un ambiente más creíble desde el punto de vista del atacante. Un entorno de sistemas heterogéneo permite además, captar la atención de más intrusos, algunos de los cuales están especializados en atacar determinados sistemas operativos o servicios. Por otra parte, permite aprender un mayor y variado número de tácticas de ataque.
- Los sistemas utilizados en una honeynet son sistemas de producción.

Son sistemas reales, aunque no se utilicen con otro propósito que el de monitorear su actividad. Ningún sistema o servicio es emulado. No se hace intento alguno de disminuir su seguridad.

Normalmente se instalan los sistemas trampa más conocidos, con la configuración que traen por defecto, como Linux Red Hat, servidores Windows o servidores Solaris.

Las honeynets son herramientas de seguridad con un punto de vista diferente al tradicional defensivo, presente en firewalls, cifrado o sistemas de detección de intrusiones. Son herramientas diseñadas básicamente para aprender y adquirir experiencia en el área de seguridad.

El proyecto honeynet ha definido dos tipos de arquitecturas básicas para sus honeynets: **GenI,** Figura 5.22, y **GenII,** Figura 5.23. Ambas arquitecturas son descritas a continuación, seguidas de varios métodos para implementar honeynets virtuales.

GenI. Esta arquitectura simple fue en 1999 la primera en desarrollarse. Una red es situada detrás de un dispositivo de control de acceso, generalmente un firewall, como se muestra a continuación.

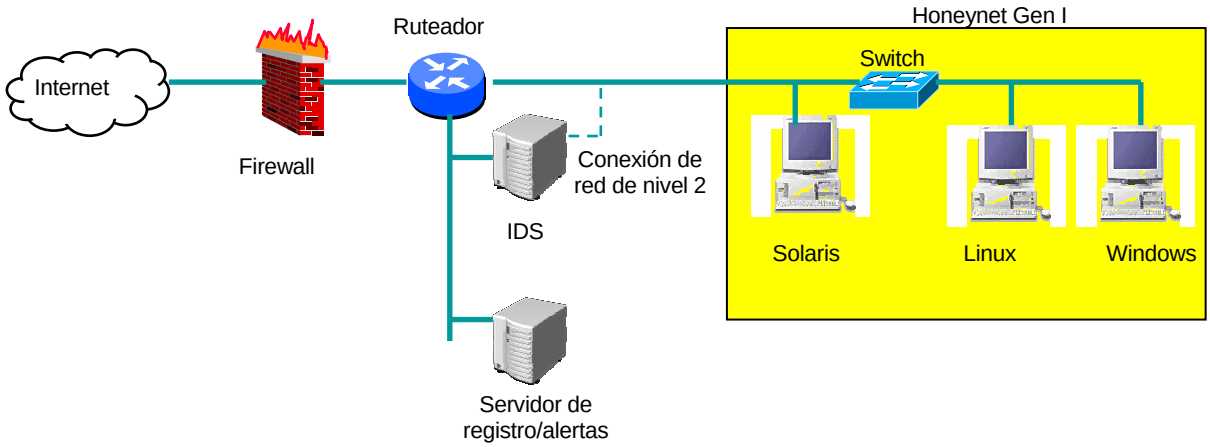


Figura 5.22 Arquitectura honeynet GenI

En la Figura 5.22, se puede ver un firewall de nivel tres separando la honeynet en tres redes diferentes: la honeynet, Internet y la red de producción. Cualquier paquete que entre o salga de la honeynet tiene que pasar a través del firewall y del ruteador.

El firewall filtra las conexiones entrantes y salientes. El ruteador complementa este filtrado. El firewall está diseñado para permitir cualquier conexión entrante, pero controla las conexiones salientes.

Este tipo de arquitectura es eficaz contra ataques automatizados o contra atacantes de nivel básico. Pero no son de gran utilidad contra atacantes avanzados. El entorno proporcionado por las honeynets GenI suele ser poco atractivo, consistiendo básicamente en instalaciones por defecto de sistemas operativos.

GenII. Esta arquitectura de honeynets se desarrolló en 2002 y fue pensada para solventar muchos de los problemas existentes en el modelo anterior. Con respecto a las tecnologías GenI, esta arquitectura es más fácil de implementar, difícil de detectar y de mantenimiento más seguro.

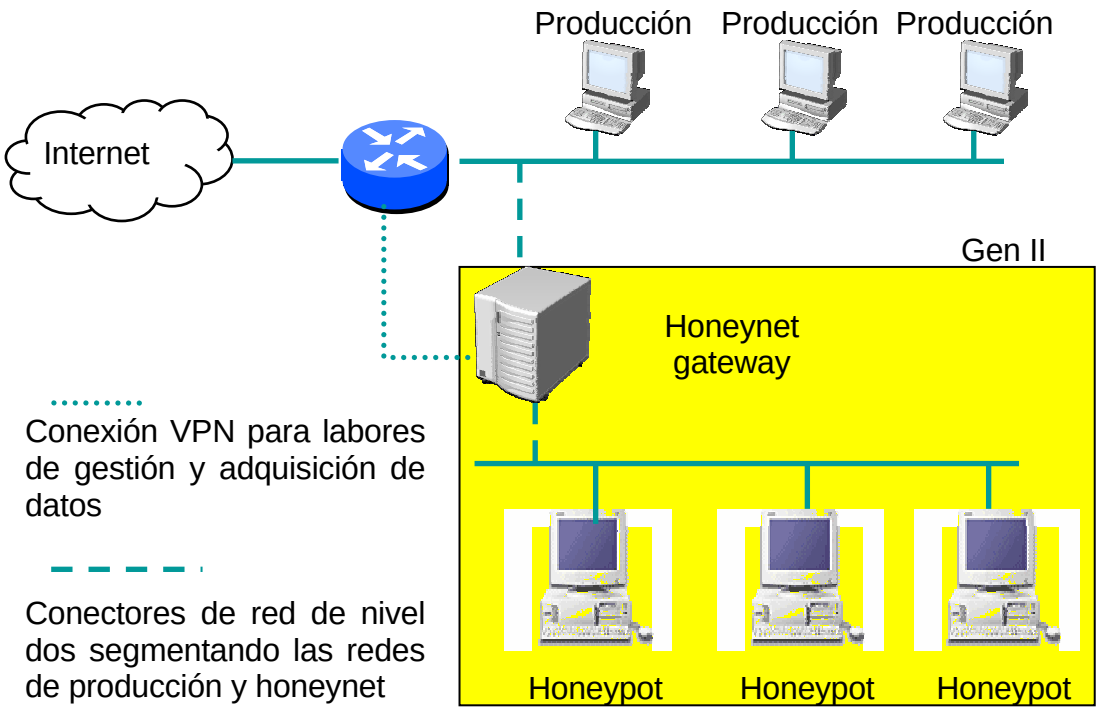


Figura 5.23 Arquitectura honeynet GenII

Como se puede ver en la Figura 5.23, la primera diferencia con respecto a la arquitectura GenI es que se utiliza un honeynet gateway, puerta de enlace de la red trampa que combina los elementos de IDS y firewall aparecidos por separado en el modelo GenI. Esto simplifica su administración. La segunda diferencia radica en el propio gateway, que trabaja a nivel dos, de forma similar a un puente. Este método, muy común en este tipo de mecanismos, permite prescindir de dirección IP, reduciendo las posibilidades de detección por parte de los atacantes.

Además, el gateway no encamina paquetes. En vez de bloquear las conexiones de salida, se limita el ancho de banda del atacante, haciendo más realista y flexible el entorno.

Los sistemas trampa, introducidos dentro de la honeynet consisten normalmente en instalaciones básicas de los sistemas operativos más comunes, a veces con algunos servicios de red activados para hacerlos más atractivos como objetivo de ataque.

Honeynet virtual

La aparición de herramientas de emulación o soporte virtual, han hecho posible este modelo de implementación de honeynets. Este enfoque consiste en crear una honeynet completa en un solo equipo físico. Una honeynet virtual no es una arquitectura, sino una forma de implementarlas; de esta manera, se puede utilizar para crear tanto arquitecturas tipo GenI, como GenII.

Entre las opciones existentes para crear una honeynet virtual destacan el producto comercial VMware, y User Mode Linux (UML).

Consiste en un módulo especial del núcleo de sistema que permite ejecutar muchas versiones virtuales de Linux en el mismo sistema simultáneamente. A continuación se describen brevemente las ventajas e inconvenientes de ambos productos:

- VMware es de pago y de código cerrado, mientras que UML es de libre distribución.
- VMware permite tres modos de instalación: Workstation, GSX, o ESX. Cada uno con diferentes capacidades, según las necesidades del usuario.
- UML necesita significativamente menos recursos que VMware.
- VMware soporta más sistemas operativos que UML, el cual, está limitado a sistemas Linux; aunque se está desarrollando una aplicación para Windows.

Una de las mejores características con las que cuenta VMware, es que tiene una consola de administración remota que presenta al sistema invitado como si se estuviera sentado delante, permitiendo su gestión remota sin generar tráfico de red. UML no posee interfaz gráfica, sino realiza la gestión a través de la línea de comandos.

Al ser UML un producto de código abierto, no proporciona soporte oficial ni comercial.

Una honeynet virtual puede ser autocontenida o híbrida.

La honeynet virtual autocontenida, Figura 5.24, engloba una honeynet en un sistema físico único.

Ventajas

- Fácilmente transportable, especialmente si se instala en una computadora portátil.
- Rápida puesta en funcionamiento. Una vez instalada, sólo hay que conectarla a la red y configurarla en pocos minutos.
- Es barata y ocupa poco espacio. Sólo hace falta una computadora.

Desventajas

Si falla el hardware, la honeynet entera podría dejar de funcionar.

Computadora de altas prestaciones. Aunque sólo requiere una computadora, es necesario que tenga suficiente memoria y procesador.

Seguridad. Como todos los sistemas comparten el mismo hardware, es posible que un atacante acceda a otras partes del sistema. Mucho depende del software virtual.

Limitación por software. Como todo tiene que ejecutarse en una sola máquina, hay software que no se podrá utilizar por problemas de incompatibilidad. Por ejemplo, una IOS Cisco en un procesador Intel.

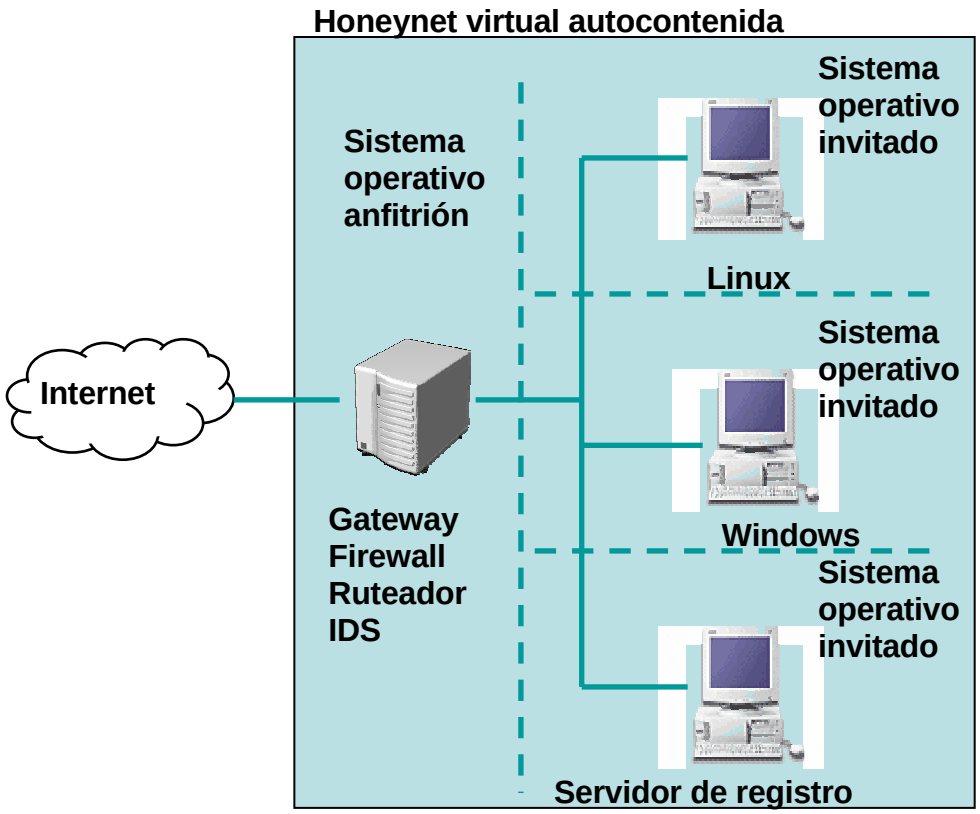


Figura 5.24 Honeynet virtual autocontenida

Honeynet virtual híbrida

Una honeynet virtual híbrida, Figura 5.25, es una combinación de una honeynet y del software virtual. Es decir, los sensores de IDS y el almacenamiento de registros, están en un sistema separado y aislado, para reducir el riesgo de compromiso. Sin embargo, todos los honeypots son ejecutados virtualmente en una única máquina.

Ventajas

- Seguridad. El único peligro sería que el atacante accediera a otros honeypots.
- Hay mayor flexibilidad a la hora de utilizar software para el control y captura de los datos de red.

Desventajas

- Al implicar a más de una máquina, la movilidad es más reducida.
- Es más cara y ocupa más espacio que la autocontenida.

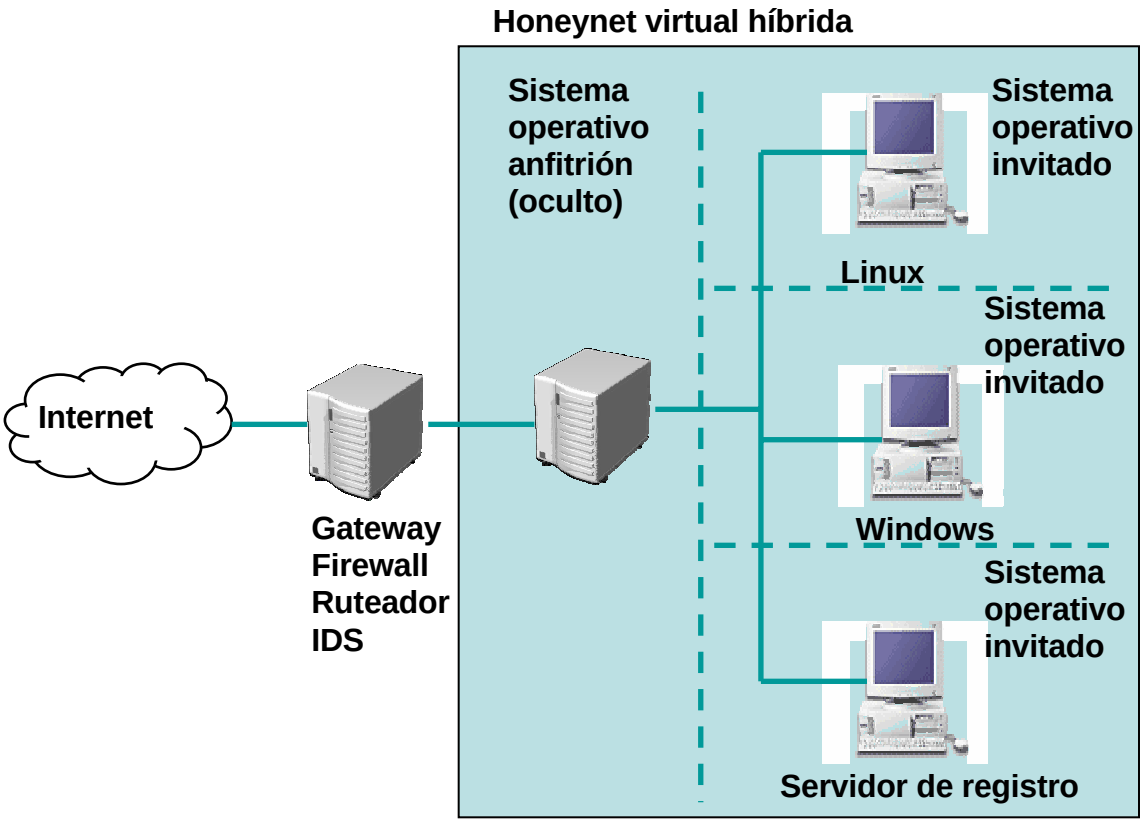


Figura 5.25 Honeynet virtual híbrida

Ventajas e inconvenientes

Los sistemas comentados en este capítulo permiten estudiar, con lujo de detalle, las tácticas, métodos y motivos de los intrusos, aspecto que los diferencia del resto de los productos y soluciones de seguridad. Su enfoque no está basado en la tradicional posición defensiva (firewalls, cifrado, etc.). Lejos de bloquear los ataques, su metodología se basa en el seguimiento en detalle de los procesos de intrusiones.

No obstante, hay que conocer los aspectos legales que puede suponer la implantación de uno de estos sistemas antes de decidir hacerlo.

Ventajas

- Ayudan a descubrir nuevos ataques, en ocasiones no publicados por las autoridades de seguridad. Esto permite mejorar los motores de detección de los sistemas de detección de intrusiones, así como la creación de nuevos patrones de ataque.
- Los atacantes no dañan sistemas reales.
- Utilizar sistemas trampa, similares a los de producción permite identificar fallas de seguridad existentes en el entorno real.
- Ayudan a perfeccionar los mecanismos de respuesta ante incidentes.
- Aportan mucha experiencia en el campo de la seguridad.

Inconvenientes

- Este tipo de sistemas siempre ha presentado dudas en cuanto a su verdadera efectividad a la hora de mejorar la seguridad. No obstante, cada vez está recibiendo más aceptación entre los miembros de la comunidad de seguridad.
- Es necesario un alto nivel de conocimientos y experiencia en materia de redes y seguridad para poder instalar eficazmente un sistema de estas características. Para poder cumplir con el objetivo de rastrear las operaciones de un intruso, sin que éste se de cuenta.

El control de accesos es uno de los puntos principales en donde existe una amplia gama de productos en el mercado, que ofrecen una adecuada protección a las redes de computadoras, estos productos incluyen sistemas detectores de intrusos, firewalls y controles de acceso físico utilizando sistemas biométricos en su fabricación.

Para poder hacer una implementación de los mismos, es necesario que el personal que va a configurarlos se capacite en el uso y mejor forma de manipularlos.

CAPÍTULO 6

METODOLOGÍA DE SEGURIDAD EN REDES DE COMPUTADORAS

A manera de definición, una metodología es un modo ordenado de proceder para llegar a un resultado o fin determinado, también es considerada como una especialización para descubrir la verdad y sistematizar los conocimientos. Por proceder debe entenderse a la acción de ejecutar ciertos pasos, unos tras otros, guardando un orden determinado; es por ello que en este capítulo se dan a conocer los pasos necesarios para establecer una metodología de seguridad en redes de computadoras en un sistema informático en general. Para lograr los objetivos hay que considerar que la seguridad no es un fin en sí, sino un proceso dinámico que requiere de atención periódica, debido principalmente a que los sistemas de información están en constante actualización y cambio.

Aunque una estrategia de seguridad puede ahorrar mucho tiempo a la organización y proporcionar importantes recomendaciones de lo que se debe hacer, la seguridad es una actividad, que requiere de actualizaciones y revisiones periódicas. Estos cambios se realizan cuando las configuraciones y otras condiciones y circunstancias cambian o cuando hay que modificar las leyes y normas organizativas. Es por ello que la seguridad en las redes informáticas, se considera como un proceso iterativo, ya que nunca termina y debe revisarse y probarse cíclicamente.

En cada método, el plan de seguridad debe incluir una estrategia preactiva y otra reactiva, ya que de una nace la otra.

La estrategia preactiva o de prevención de ataques es un conjunto de pasos predefinidos que deben seguirse para evitar ataques antes de que ocurran y que ayuda a reducir al mínimo la cantidad de puntos vulnerables existentes en las políticas de seguridad y a desarrollar planes de contingencia.

Entre estos pasos se incluye observar cómo podría afectar o dañar el sistema, y los puntos vulnerables que explota. Los conocimientos adquiridos en estas evaluaciones pueden ayudar a implementar las políticas de seguridad que controlarán o aminorarán los ataques.

La estrategia reactiva o estrategia posterior al ataque ayuda al personal de seguridad a evaluar el daño que ha causado el ataque, a repararlo o implementar el plan de contingencia desarrollado en la estrategia preactiva, a documentar y aprender de la experiencia, y conseguir que las funciones críticas y principales se normalicen lo antes posible.

La metodología de seguridad que se describe en este capítulo, Tabla 6.1 está diseñada para auxiliar a todos aquellos responsables de redes de computadoras encargados de proteger la confidencialidad, integridad y disponibilidad de los datos de los sistemas informáticos.

Como se ha mencionado a lo largo de este trabajo, los datos de los sistemas informáticos están en constante peligro por varias causas, tales como riesgos, amenazas y ataques; las cuales pueden interrumpir los servicios, inutilizar los sistemas o alterar, suprimir o robar información.

Para poder fortalecer la seguridad en redes dentro de una organización, además del desarrollo de una metodología, se tiene que considerar otros elementos tales como el tiempo, dinero y esfuerzo que se necesite para poder establecer los controles de seguridad apropiados. Cada organización debe analizar sus necesidades específicas y determinar sus requisitos y limitaciones en cuanto a recursos y programación.

Cada sistema informático, entorno y directiva organizativa es distinta, lo que hace que cada servicio y cada estrategia de seguridad sean únicos. Sin embargo, los fundamentos de una buena seguridad deben ser los mismos y este trabajo se centra en tales principios.

La seguridad informática es algo que ha estado evolucionando y una vez que es tomada en serio por las organizaciones, debe tener el apoyo de la alta dirección, la cual se obliga a crear un Comité de Seguridad Informática, así como la figura de un responsable o administrador de seguridad, comúnmente conocido como Oficial de Seguridad Informática (CSO, por sus siglas en inglés).

La metodología propuesta la deberá poner en práctica el CSO y se basa en una serie de pasos que se indican a continuación:

I. Políticas de seguridad	
II. Análisis de riesgos	Etapa 1. Determinar el daño posible que puede causar un ataque
	Etapa 2. Determinar los puntos vulnerables y las debilidades que explotará el ataque
	Etapa 3. Reducir los puntos vulnerables y las debilidades para ese tipo de ataque específico
III. Identificación de soluciones	Tácticas
	Operativas
	Técnicas
IV. Implantación y capacitación en las soluciones	
V. Auditoría y monitoreo de seguridad	
VI. Elaborar y actualizar planes de continuidad de negocio	Etapa 1. Análisis de impacto al negocio
	Etapa 2. Protección de la instalación
	Etapa 3. Almacenamiento fuera del site
	Etapa 4. Estrategia de respaldo de sistemas
	Etapa 5. Estrategia de respaldo de redes
	Etapa 6. Toma de decisiones en caso de emergencia
	Etapa 7. Mantenimiento y pruebas del plan

Tabla 6.1 Metodología de seguridad informática en redes de computadoras

6.1. Políticas de seguridad

El establecimiento de un conjunto eficaz de políticas y controles de seguridad requiere el uso de un método para determinar los puntos vulnerables que existen en los sistemas informáticos, en las mismas políticas y en los controles de seguridad que protegen a dichos sistemas.

El estado actual de las políticas de seguridad informática se determina mediante la revisión de una serie de documentos que son esenciales en lo que a seguridad informática se refiere. En la revisión, deben darse a notar las áreas en las que las políticas de seguridad no han logrado desarrollarse, de acuerdo a las metas establecidas. Tal documentación debe considerar principalmente cuatro elementos para su definición: objetivos, alcances, políticas y sanciones, deben estar constituidas entre otras por:

- Las funciones del responsable o administrador de seguridad.
- Las funciones del comité de seguridad.
- Uso de equipo de cómputo.
- La directiva de seguridad informática referente al acceso físico.
- Las políticas de correo electrónico.
- Las políticas de acceso a Internet.
- Escritorio limpio.
- Los planes, pruebas de contingencias y de recuperación de desastres.
- Las políticas de contraseñas de acceso a los equipos.

A continuación se presentarán ejemplos de políticas referentes a funciones del responsable o administrador de seguridad, funciones del comité de seguridad y uso de equipo de cómputo.

6.1.1. Funciones del responsable o administrador de seguridad

- Dirigir y coordinar los distintos procesos relacionados con la seguridad de la aplicación.
- Diseñar, probar e implantar el plan de continuidad del negocio.
- Informar al responsable de las aplicaciones y, en su caso, a la alta dirección o al comité de seguridad informática, sobre los niveles de seguridad alcanzados en las aplicaciones.
- Garantizar la buena comunicación con el resto de actores participantes en la seguridad.
- Dirigir las actividades de auditoría y control de la seguridad.
- Preparar los planes de implantación de distintos tipos de controles.
- Identificar, analizar los distintos incidentes de seguridad e informar al responsable de las aplicaciones de cualquier incidencia detectada.

6.1.2. Funciones del comité de seguridad

- Identificar objetivos y estrategias relacionados con la seguridad.
- Revisar la implantación de la política de seguridad.
- Iniciar, dirigir y controlar los procesos de seguridad.
- Aprobar los distintos planes de implantación y asignar los recursos necesarios.
- Vigilar que las medidas de la política planificadas son implantadas tal como se había previsto y dan los resultados esperados.
- Preparar el programa de seguridad así como el plan de formación y concientización.
- Estar en contacto con los distintos equipos de sistemas.

6.1.3. Uso de equipo de cómputo

- El empleado es custodio de la información que procesa y almacena en el equipo que le ha asignado la institución.
- Todos los empleados están obligados a firmar su resguardo de equipo de cómputo y telecomunicaciones que tienen en custodia.
- El código o contraseña (password) de cada equipo es personal y confidencial, por lo que únicamente es conocido por la persona que lo tiene asignado. En caso de que éste sea extraviado u olvidado, la persona responsable del equipo deberá solicitar a soporte a usuarios que se coloque un código temporal, para que el empleado tenga acceso y pueda asignarse uno nuevo.
- El propietario de la cuenta es el responsable único de la privacidad de su clave y cualquier acción efectuada con ésta será atribuida a dicho propietario.
- Está prohibido instalar programas ajenos a los que la institución proporciona a sus empleados para realizar sus funciones.
- La información contenida en cada equipo de cómputo es considerada confidencial y ninguna persona ajena a dicho equipo, incluyendo a los administradores, tendrá acceso sin autorización expresa del usuario.
- Está estrictamente prohibido conectar cualquier equipo periférico (impresoras, pda’s, memorias, cámaras fotográficas o de video, unidades externas de almacenamiento, puertos infrarrojos, etc.) a los equipos de cómputo.
- Todos los equipos de cómputo deben tener protectores de pantalla protegidos con contraseñas, que deben activarse cuando han transcurrido quince minutos y no se detecta actividad en la pc.

• Los equipos deben ser apagados cuando no vayan a ser utilizados por periodos prolongados, por las noches y fines de semana. Cuando un usuario tenga la necesidad de abandonar su lugar sin apagar su equipo, deberá activar el protector de pantalla y apagar el monitor. Al finalizar su jornada deberá salirse de la sesión de trabajo.

• El usuario que tiene asignado el equipo de cómputo es el responsable de su uso y cuidado. Si se presentara alguna falla, deberá reportarla a help desk para que se efectúe el mantenimiento que corresponda.

6.2. Análisis de riesgos

Este paso es el más importante, ya que permite identificar claramente los problemas de seguridad a los que una organización se puede enfrentar, tomando como base la infraestructura tecnológica con la que cuenta.

El análisis de riesgos permite identificar y conocer las vulnerabilidades existentes en los sistemas de información y el impacto que éstas le pueden ocasionar a la organización.

Esta actividad tiene como finalidad identificar y priorizar los requerimientos de seguridad de la organización.

Como se mencionó en el capítulo tres, se utiliza la matriz de análisis de riesgo cualitativo, Figura 6.1, propuesta en el estándar australiano-neozelandés AS/NZS 4360.

	IMPACTO				
PROBABILIDAD	INSIGNIFICANTE 1	MENOR 2	MODERADO 3	MAYOR 4	CATASTRÓFICO 5
5 CASI CERTEZA	A	A	E	E	E
4 PROBABLE	M	A	A	E	E
3 POSIBLE	B	M	A	E	E
2 IMPROBABLE	B	B	M	A	E
1 RARO	B	B	M	A	A

Figura 6.1 Matriz de análisis de riesgo cualitativo

En esta matriz el significado de las letras es el siguiente:

E: Riesgo extremo.

A: Riesgo alto.

M: Riesgo moderado.

B: Riesgo bajo.

De acuerdo a esta matriz, Figura 6.1, debe darse especial atención primeramente a todas las amenazas que signifiquen un riesgo extremo.

Las listas de amenazas que puedan ser recopiladas por la organización de manera periódica, ayudan a los administradores de seguridad a identificar los distintos métodos, herramientas y técnicas que se consiguen utilizar en los ataques. Los métodos pueden abarcar desde virus y gusanos para adivinar contraseñas, hasta la intercepción de la información que viaja por las redes. Es importante que los administradores actualicen constantemente sus conocimientos en esta área, ya que los nuevos métodos, herramientas y técnicas para sortear las medidas de seguridad evolucionan de forma continua.

Dentro de este paso se estudian las distintas amenazas que ponen en peligro las redes de computadoras, las técnicas correspondientes que se ocupan para comprometer los controles de seguridad. El conocimiento de estos elementos de los ataques ayuda a predecir su aparición e incluso, su duración o ubicación.

La primera etapa de este segundo paso de la metodología, consiste en determinar los ataques que se pueden esperar y las formas de defenderse contra ellos. Es imposible estar prevenido contra todos los ataques; por lo tanto, hay que prepararse para los que tiene más probabilidad de sufrir la organización.

Para iniciar un ataque, se necesita un método, una herramienta o una técnica para explotar los distintos puntos vulnerables de los sistemas, de las políticas de seguridad y de los controles.

Los agresores utilizan un método para iniciar un ataque o incluso, aplican varios métodos para iniciar el mismo ataque. Por lo tanto, la estrategia defensiva debe personalizarse para cada tipo de método manejado en cada clase de amenaza. De nuevo, es importante que se esté al día en los diferentes métodos, herramientas y técnicas que ocupan los agresores. Las amenazas como empleados ignorantes o negligentes, y los desastres naturales no implican motivos u objetivos; por lo tanto, no se aplican métodos, herramientas o técnicas predeterminadas para iniciar los ataques. Casi todos estos ataques o infiltraciones en la seguridad se generan internamente; raras veces los va a iniciar alguien ajeno a la organización.

Por otro lado, en esta fase también se deben desarrollar y establecer las estrategias preactivas y reactivas.

También es necesario tomar nota del costo que supone la pérdida de los datos frente al de la implementación de controles de seguridad. La ponderación de los riesgos y los costos forma parte de un análisis de riesgos del sistema.

Estas son las tres etapas que forman una estrategia preactiva y que están incluidas en el análisis de riesgos:

- Determinar el daño posible que puede causar un ataque.
- Determinar los puntos vulnerables y las debilidades que explotará el ataque.
- Reducir los puntos vulnerables y las debilidades para ese tipo de ataque específico.

6.2.1. Determinar el daño posible que puede causar un ataque

Los daños posibles pueden ir desde pequeñas fallas del equipo hasta la pérdida de los datos. El daño causado al sistema dependerá del tipo de ataque. Es por ello que hay que utilizar un entorno de prueba para clarificar los daños que provocan los diferentes tipos de ataques, que realizará el personal de seguridad en este ambiente, así mismo, permitirá ver el daño físico causado. Hay que tener en cuenta que no todos los ataques causan el mismo daño.

6.2.2. Determinar los puntos vulnerables y las debilidades que explotará el ataque

Si se pueden descubrir los puntos vulnerables que explota un ataque específico, se pueden modificar las políticas de seguridad y los controles de seguridad actuales o implementar otras nuevas para reducir estos huecos en la seguridad. La determinación del tipo de ataque, amenaza y método facilita el descubrimiento de las vulnerabilidades existentes.

A continuación se enlistan algunas de las cuestiones que se pueden plantear para ayudar a identificar los posibles puntos vulnerables que existen en la organización. Éstas representan solamente algunas de las muchas que existen, y están clasificadas de acuerdo a los diferentes aspectos de seguridad que conforman una estrategia completa en seguridad informática:

- Vulnerabilidades en la seguridad física.
- Vulnerabilidades en la seguridad de datos.

Vulnerabilidades en la seguridad física

Para conocer cuáles son los riesgos asociados a la seguridad física, el CSO buscará cómo responder adecuadamente a las siguientes preguntas:

¿Hay bloqueos y procedimientos de entrada para obtener acceso a los servidores?

¿Es suficiente el aire acondicionado y se limpian regularmente los filtros?

¿Hay sistemas de alimentación ininterrumpida y generadores, y se comprueban en los procedimientos de mantenimiento?

¿Hay equipo para la extinción de incendios y procedimientos de mantenimiento apropiados para el equipo?

¿Hay protección contra el robo de hardware y software?

¿Se guardan los paquetes y licencias de software y las copias de seguridad en lugares seguros?

¿Hay procedimientos para almacenar los datos, copias de seguridad y software con licencia en las instalaciones y fuera de ellas?

Vulnerabilidades en la seguridad de datos

El responsable de la seguridad de la organización, para reducir las amenazas a los datos se planteará las siguientes preguntas:

¿Qué controles de acceso, controles de integridad y procedimientos de copias de seguridad existen para limitar los ataques?

¿Hay políticas de seguridad de privacidad y procedimientos que deban cumplir los usuarios?

¿Qué controles de acceso a los datos (autorización, autenticación e implementación) hay?

¿Qué responsabilidades tienen los usuarios en la administración de los datos y las aplicaciones?

¿Se han definido técnicas de administración de los dispositivos de almacenamiento con acceso directo?

¿Cuál es su efecto en la integridad de los archivos de los usuarios?

¿Hay procedimientos para controlar los datos importantes?

Vulnerabilidades en la seguridad de la red

Para mitigar las amenazas en la red, las siguientes preguntas darán al responsable de la seguridad de la organización una idea clara, del estatus de la seguridad en esta área:

¿Qué tipos de controles de acceso existen?

¿Hay procedimientos de autenticación?

¿Qué protocolos de autenticación se utilizan en las redes de área local, redes de área extensa y servidores de acceso telefónico?

¿Quién tiene la responsabilidad de la administración de la seguridad?

¿Qué tipo de medios de red, por ejemplo, cables, conmutadores y ruteadores, se utilizan?

¿Qué tipo de seguridad tienen los medios de red?

¿Se ha implementado la seguridad en los servidores de archivos y de impresoras?

¿Hace uso la organización del cifrado y la criptografía, redes privadas virtuales (VPN), sistemas de correo electrónico y acceso remoto?

6.3. Identificación de soluciones

Las soluciones de seguridad tienen como objetivo controlar y/o eliminar los riesgos de seguridad.

La selección de soluciones de seguridad debe mantener un equilibrio entre el costo de la solución y el impacto causado por las violaciones de seguridad.

Las soluciones se pueden clasificar en:

1. Tácticas.
2. Operativas.
3. Técnicas.

1. Tácticas

En esta categoría se encuentran las políticas, estándares y procedimientos, la administración de riesgos y los programas de seguridad.

2. Operativas

Ejemplos de estas soluciones son la administración de usuarios, los planes de contingencia, el manejo de incidentes de seguridad, la concientización y la seguridad física y ambiental.

3. Técnicas

En esta categoría se encuentran todas las herramientas de hardware y software de seguridad incluyendo los firewalls, los IDS (Intrusion Detection Systems), los antivirus, las VPN (Virtual Private Networks), las herramientas de filtrado de contenido, las PKI (Public Key Infrastructure), etc.

6.4. Implantación y capacitación en las soluciones

En caso de que la solución al problema de seguridad analizado sea técnica, debe llevarse a cabo su implementación para disminuir el riesgo por el cual se seleccionó dicha herramienta.

Para hacer un uso adecuado de la herramienta, es conveniente capacitar al personal encargado de la misma para configurar, actualizar y monitorear las alarmas que envíe y así en caso de presentarse un ataque pueda activarse la estrategia reactiva.

Un principio comúnmente aplicado a la seguridad informática es el que dice que "la seguridad, al igual que una cadena, es tan fuerte como su eslabón más débil", y normalmente el eslabón más débil en la cadena son los usuarios e incluso los mismos administradores de la tecnología de información.

La capacitación, el entrenamiento y la educación, en el uso de las herramientas son factores primordiales dentro de la seguridad informática, ya que de su correcta implementación y actualización dependerá el nivel de protección establecido, como por ejemplo si se tiene un antivirus desactualizado, es sólo un poco mejor que no tener ninguno.

6.5. Auditoría y monitoreo de seguridad

En general, la auditoría y el monitoreo tienen como objetivo asegurar que las soluciones de seguridad continúan siendo válidas y cumplen con la finalidad para la cual fueron implantadas.

Por un lado, la auditoría es un evento único o repetitivo que evalúa el ambiente de control de la seguridad. Una auditoría puede variar ampliamente en su alcance, desde la investigación de un incidente hasta la revisión de todo un sistema con el objeto de acreditarlo o recertificarlo.

En cambio, el monitoreo es una actividad constante que puede consistir, por ejemplo, en la revisión de la actividad en un firewall, los accesos a un sistema o el ambiente de red.

En el monitoreo se deben definir los acuerdos de niveles de servicio (SLA por sus siglas en inglés) y los medidores de desempeño para la función de seguridad.

6.6. Elaborar y actualizar planes de continuidad de negocio

Este paso consiste en la preparación de planes de acción en el caso que algún evento produzca una interrupción en el funcionamiento normal de los sistemas de información afectando procesos importantes de la organización.

Ya sea un Business Continuity Plan (BCP), un Disaster Recovery Plan (DRP) o un Contingency Plan (CP) la organización debe contar con procedimientos definidos y probados que la ayuden a restablecer su funcionamiento normal en el menor tiempo posible minimizando el impacto.

El último de los pasos en la estrategia preactiva es la elaboración de un plan de contingencia, el cual es un plan alternativo que debe aplicarse en caso de que alguna amenaza se presente en el sistema y dañe los datos o cualquier otro activo y detenga las operaciones habituales. El plan se sigue si el sistema no se puede restaurar a tiempo. Su objetivo final es mantener la disponibilidad, integridad y confidencialidad de los datos; a este tipo de acción se le puede identificar como el muy conocido Plan B.

Existen varias compañías que se especializan en ofrecer servicios de sitio alterno, que van desde cold site hasta sistemas espejo pasando por el hot site. Sus instalaciones cuentan con varias plantas de generación de energía eléctrica, equipo de aire acondicionado, sensores y equipo contra incendio, contratación de equipo de telecomunicaciones con diferentes proveedores y con diferente central, personal especialista en diferentes plataformas, etc.

Normalmente manejan varios planes de contratación, pero en general el servicio más común es el llamado Business Center, el cual incluye veinte computadoras, teléfonos, fax, escáner y la posibilidad de contratación de servicios financieros, como acceso por una línea especializada ya sea a bancos o a donde el cliente lo indique.

El número de computadoras varía de acuerdo a las necesidades del cliente, pueden contratarse más o menos, según sea el caso.

Ofrecen además el tener ubicado en sus instalaciones los equipos servidores de respaldo, que hagan falta para que, en caso de desastre, se conecten precisamente el número de computadoras contratadas y con esto se continúe con la operación del negocio.

Estos servidores deben tener las bases de datos, los programas de las aplicaciones y la configuración de usuarios, lista para que la reanudación de las operaciones se lleve con el menor tiempo posible de interrupción.

SUNGARD, KIO Networks, DiVEO, Xertix, GEDAS, Triara, IBM, HP son algunas empresas en México que ofrecen estos servicios.

6.6.1. Objetivos del plan de continuidad del negocio

1. Desarrollar un método formal de respuesta a las emergencias que permita a la institución enfrentarse a un desastre reduciendo sus riesgos y optimizando su recuperación.

2. Contar con una guía que describa paso a paso tanto el qué hacer, quién hace qué, cómo y cuándo, es decir, formar un equipo de respuesta a incidentes (ERI) que lleve el detalle de acciones, procedimientos y recursos que deben utilizarse para que al presentarse un desastre parcial o total estar en condición de restablecer, lo más pronto posible, el procesamiento de aplicaciones críticas para posteriormente restaurar totalmente el procesamiento normal, minimizando las pérdidas y manteniendo a la institución operando.

Para el desarrollo del presente plan de contingencia me he apoyado en la metodología de William Toigo.

6.6.2. Etapas del plan de continuidad del negocio

Esta metodología contempla siete etapas para su instrumentación, las cuales son las siguientes:

Etapa 1. Análisis de impacto al negocio.

Etapa 2. Protección de la instalación.

Etapa 3. Almacenamiento fuera del site.

Etapa 4. Estrategia de respaldo de sistemas.

Etapa 5. Estrategia de respaldo de redes.

Etapa 6. Toma de decisiones en caso de emergencia.

Etapa 7. Mantenimiento y pruebas del plan.

Etapa 1. Análisis de impacto al negocio

Ésta se lleva a cabo mediante un cuestionario a las áreas de la institución, las cuales pueden ser por ejemplo:

1. ¿Podrías enumerar tus procesos de información?
2. ¿Cuáles son tus objetos de información críticos?
3. ¿Qué relación tienen con el área de sistemas?
4. ¿Qué otras áreas tienen relación con tus procesos?
5. Con esos procesos más importantes, ¿levantas el negocio por si esto se cae?
6. ¿Qué equipo y personal será necesario para desarrollar las tareas de alta prioridad? pc's, impresoras, faxes, acceso a Internet, etc. ¿Para qué procesos? Listas de contactos internos y externos.
7. ¿Qué servicios fuera de la organización son necesarios para la operación normal? Por ejemplo, enlaces directos a otras instituciones.
8. Se consulta qué impacto representa que la información sea divulgada y/o modificada.
9. Si un desastre ocurre, por cuánto tiempo puede funcionar el departamento sin el equipo existente.
10. ¿Cuál es la hora crítica durante el día?
11. ¿Cuál es el día más crítico de la semana?
12. ¿Cuál es la semana más crítica del mes?
13. ¿Cuál es el mes más crítico del año?
14. ¿Cuáles son los periodos más críticos del año?

Mediante este cuestionario se efectúa una matriz de requerimientos mínimos para que la institución siga operando en caso de presentarse un desastre.

Etapa 2. Protección de la instalación

Control de acceso físico

Se debe controlar el acceso a las instalaciones en todo momento, los siguientes son ejemplos de las formas de implementar los controles; por medio de credenciales, torniquetes, arcos de seguridad y enrejados, además se debe contar con circuito cerrado de televisión en donde se registren todos los movimientos desde la calle hasta los pasillos de cada piso. Las personas podrán tener acceso sólo a los pisos a los que tenga la autorización correspondiente.

Protección contra fuego

La institución debe contar con un sistema de control de accesos, detección de humo e incendio en todo el edificio y de extinción de incendios en el centro de cómputo. También se compromete a tener instalados extintores manuales en varias zonas de cada piso.

Etapa 3. Almacenamiento fuera del site

Los programas y sistemas deben ser respaldados en cintas o discos mediante un proceso programado idealmente de manera diaria. Es conveniente contratar servicios de caja fuerte en algún banco o en alguna otra institución que su giro de negocio sea éste. En la actualidad existen varias compañías que ofrecen el servicio. Por mencionar alguna, Fortinet.

Es recomendable tener copias de seguridad del software necesario para configurar tanto pc’s como servidores, así como una copia de los programas fuentes, ejecutables y librerías

Conviene respaldar también toda la documentación necesaria para restaurar los sistemas de información que debe estar contenida en los manuales y procedimientos operativos de sistemas.

Etapa 4. Estrategia de respaldo de sistemas

Toda la información crítica y vital, de la cual depende la institución para seguir operando debe ser respaldada, ya sea en cintas o en discos. Todo está en función de qué tanto depende la organización del tiempo para tener disponible dicha información.

Así, en caso de ser necesario, tener contratado el servicio de un sitio alterno, el cual tenga en sus instalaciones el equipo de cómputo suficiente para que la operación del negocio no se detenga y siga su operación crítica.

Como ejemplo se tiene el caso de empresas petroleras, las cuales no pueden detener sus procesos de producción y en tal situación se justifica una inversión de este tipo.

Etapa 5. Estrategia de respaldo de redes

Para sistemas de comunicación interna

Adquirir software apropiado para diagnóstico y reparación de problemas de redes.

En caso de problemas con el conmutador:

- Instalar suficientes líneas directas para las funciones dependientes de las telecomunicaciones.
- Tener hardware redundante almacenado para reemplazo inmediato cuando falla un dispositivo crítico.

Para redes de área local

Usar software para crear y controlar la red para protegerla contra pérdidas de integridad de los medios de comunicación, por fallas de nodos o factores relacionados por el software.

Etapa 6. Toma de decisiones en caso de emergencia

Nos dice que, en caso de presentarse una emergencia la cual ya es parte de una estrategia reactiva, se implementan los siguientes pasos:

1. Evaluar el daño.
2. Determinar las causas del daño.
3. Reparar los daños causados por el ataque.
4. Documentar y aprender.
5. Actualizar el plan de contingencia.

1. Evaluar el daño

Se recomienda determinar el daño causado durante el ataque. Esto conviene hacerlo lo antes posible para que puedan comenzar las operaciones de restauración. Si no se puede evaluar el daño a tiempo, debe implementarse un plan de contingencia para que logren continuar las operaciones y la productividad normales de la organización.

2. Determinar la causa del daño

Para determinar la causa del daño, se necesita saber a qué recursos iba dirigido el ataque y qué puntos vulnerables se explotaron para obtener acceso o perturbar los servicios. Hay que revisar los registros del sistema y de auditoría; estas revisiones suelen ayudar a descubrir el lugar del sistema en el que se originó el ataque y qué otros recursos resultaron afectados.

3. Reparar los daños causados por el ataque

Es muy importante que el daño se repare lo antes posible para restaurar las operaciones normales y todos los datos perdidos durante el ataque. Los planes y procedimientos para la recuperación de desastres de la organización deben cubrir la estrategia de restauración. El equipo de respuesta a incidentes es el responsable de controlar y ayudar en los procesos de restauración y recuperación.

4. Documentar y aprender

Es importante documentar el ataque una vez que se ha producido; la documentación debe abarcar todos los aspectos que se conozcan y que van descubriéndose, entre los que se incluyen el daño que ha causado, los puntos vulnerables y las debilidades que se explotaron durante el ataque, la cantidad de tiempo de producción perdido y los procedimientos tomados para reparar el daño. La documentación ayudará a modificar las estrategias preactivas para evitar ataques futuros o mitigar los daños.

5. Actualizar el plan de contingencia

Si ya existe un plan de contingencia, se puede implementar para ahorrar tiempo y mantener el buen funcionamiento de las operaciones. Si no hay ningún plan de contingencia, hay que desarrollar un plan apropiado basado en la documentación del paso anterior.

Equipos o grupos, de respuesta a incidentes

Es aconsejable formar un equipo o grupo de respuesta a incidentes (IRT por sus siglas en inglés). Este equipo estará implicado en los trabajos preactivos de la estrategia de seguridad. Entre éstos se incluyen:

1. El desarrollo de instrucciones para controlar incidentes.
2. La identificación de las herramientas de software para responder a incidentes.
3. La investigación y desarrollo de otras herramientas de seguridad informática.
4. La realización de actividades formativas y de motivación.
5. La realización de investigaciones acerca de virus.
6. La ejecución de estudios relativos a ataques al sistema.

Estos trabajos proporcionarán los conocimientos que la organización puede utilizar y la información que hay que distribuir antes y durante los incidentes.

Una vez que el administrador de seguridad y el IRT han realizado estas funciones preactivas, el administrador delegará la responsabilidad del control de incidentes al IRT. Esto no significa que el administrador no se comprometa a seguir implicado o formar parte del IRT, sino que no tenga que estar siempre disponible, necesariamente, y que el IRT debe ser capaz de controlar los incidentes por sí mismo. El equipo de respuesta a incidentes será el responsable de responder a incidentes como virus, gusanos o cualquier otro código dañino, invasión, engaños, desastres naturales y ataques del personal interno. El IRT también se obliga a participar en el análisis de cualquier evento inusual que pueda estar implicado en la seguridad de los equipos de cómputo o de la red.

Etapa 7. Mantenimiento y pruebas del plan

El último elemento de las estrategias de seguridad, las pruebas y el estudio de sus resultados, se lleva a cabo después de que se han puesto en marcha las estrategias preactiva y reactiva. La realización de ataques simulados en sistemas de pruebas o en laboratorios, permiten evaluar los lugares en los que hay puntos vulnerables y ajustar las políticas de seguridad y los controles de seguridad en consecuencia.

Estas pruebas no se deben llevar a cabo en los sistemas de producción real, ya que el resultado puede ser desastroso. La carencia de laboratorios y equipos de pruebas a causa de restricciones presupuestarias puede hacer imposible la realización de ataques simulados. Para asegurar los fondos necesarios para las pruebas, es importante que los directivos estén conscientes de los riesgos y consecuencias de los ataques, así como de las medidas de seguridad que se pueden adoptar para proteger al sistema, incluidos los procedimientos de las pruebas. Si es posible, es recomendable probar físicamente y documentar todos los casos de ataque para determinar las mejores políticas de seguridad y controles de seguridad posibles que se van a implementar.

Determinados ataques, por ejemplo desastres naturales como inundaciones y rayos, no se pueden probar, aunque una simulación servirá de gran ayuda. Por ejemplo, se puede simular un incendio en la sala de servidores en el que todos los servidores hayan resultado dañados y hayan quedado inutilizables. Este caso puede ser útil para probar la respuesta de los administradores y del personal de seguridad, y para determinar el tiempo que se tardará en volver a poner la organización en funcionamiento.

La realización de pruebas y de ajustes en las políticas y controles de seguridad en función de los resultados de las pruebas es un proceso iterativo, ya que debe evaluarse y revisarse de forma periódica para poder implementar mejoras.

6.7. Ejemplos prácticos

Para mostrar la utilidad de la metodología de seguridad en redes de computadoras, se explicará su uso en tres tipos de amenazas:

1. Fallas de energía.
2. Hackers.
3. Auditoría.

6.7.1. Fallas de energía

En este primer ejemplo, se considerará un caso de amenaza natural ejemplificado por la situación de que se presente una falla en el suministro de energía eléctrica.

1. Políticas de seguridad

De acuerdo a la metodología, conviene estar incluido en las políticas de seguridad las funciones del responsable o administrador de seguridad, y una de ellas es evaluar los distintos tipos de riesgos a los que está expuesta la información de la organización, así como preparar los planes de implantación de distintos tipos de controles que reduzcan los impactos asociados a estos riesgos.

2. Análisis de riesgos

Como lo indica la metodología una vez que se verifica que la política existe, lo siguiente a realizar es un análisis de riesgo. Para este caso particular, la probabilidad de que ocurra un incidente de este tipo puede considerarse como alta, ya que se pueden presentar en el mes varios incidentes, la vulnerabilidad de los sistemas de cómputo es muy grande debido a que sin energía eléctrica estos dispositivos no pueden funcionar, el riesgo asociado es mayor y el costo que esta falla representa para la organización es muy alto, ya que implica que todos los equipos de cómputo se apaguen y se detenga de forma repentina toda la operación.

Por lo tanto, en la matriz de análisis de riesgo cualitativo mostrada en la Figura 6.2 queda con medida de probabilidad nivel cuatro e impacto mayor, grado cuatro, lo que significa que es un riesgo extremo.

De manera práctica, se resalta la casilla en la que cae esta amenaza, ya que visualmente se puede tener una idea más clara del impacto que representa, que sólo indicar con números los resultados del análisis.

	IMPACTO				
PROBABILIDAD	**INSIGNIFICANTE 1**	**MENOR 2**	**MODERADO 3**	**MAYOR 4**	**CATASTRÓFICO 5**
CASI CERTEZA 5	**A**	**A**	**E**	**E**	**E**
PROBABLE 4	**M**	**A**	**A**	**E**	**E**
POSIBLE 3	**B**	**M**	**A**	**E**	**E**
IMPROBABLE 2	**B**	**B**	**M**	**A**	**E**
RARO 1	**B**	**B**	**M**	**A**	**A**

Figura 6.2 Matriz de análisis de riesgo cualitativo, situación fallas en el suministro de energía eléctrica

En esta matriz el significado de las letras es el siguiente:

E: Riesgo extremo.

A: Riesgo alto.

M: Riesgo moderado.

B: Riesgo bajo.

3. Identificación de soluciones

Debido a que una falla en el suministro de energía eléctrica representa un riesgo extremo, el siguiente paso es la identificación de soluciones que reduzcan este riesgo.

Las soluciones a evaluar implican en este caso particular, una solución técnica que implica la compra de tecnología, la cual incluye:

1. Equipos no-breaks para computadoras y servidores.

2. Banco de baterías de mayor capacidad para no sólo un equipo servidor sino todo un grupo de servidores.

3. Planta de emergencia generadora de energía eléctrica.

Para seleccionar la mejor solución para este tipo de amenaza, es recomendable hacer un estudio de consumo de energía eléctrica, tanto de servidores, como de las computadoras, críticos para la organización.

Ya que existen equipos de diferentes capacidades así como precios, conviene seleccionar el producto que solucione el problema de la manera más productiva y económica.

4. Implantación y capacitación en las soluciones

Una vez que se ha tomado la decisión de adquirir el equipo, en este caso se supondrá que incluyó la compra de la planta generadora de energía eléctrica y el banco de baterías, que además entrega energía regulada a los equipos.

Una vez que se instalen los equipos, la empresa proveedora de los mismos entrega a la organización, además de la garantía, el manual de operación y el plan de mantenimiento que ha de llevarse a cabo para el buen funcionamiento del mismo.

El manual de operación incluirá una guía de operación normal del equipo, así como también una sección de procedimientos, para saber qué hacer en caso de presentarse alarmas o fallas, incluyendo los números telefónicos de atención a clientes.

Esto es, al momento de implantar las soluciones se recomienda capacitar a personal en el uso de las mismas.

5. Auditoría y monitoreo de seguridad

Una vez que se ha instalado el equipo, debe hacerse un plan de monitoreo para verificar que está operando correctamente y que no presenta ninguna alarma.

Conviene verificar entre otras cosas, niveles de combustible, niveles de temperatura, verificación de buen estado de baterías, calendario de mantenimiento y ha de establecerse también un plan de prueba de funcionamiento, para que en caso de que se vaya la energía eléctrica por un periodo prolongado de tiempo, se tenga la seguridad de que la planta va a operar correctamente, un caso común es que la batería del motor se encuentre descargada o rota, y esto no permitiría que el motor arranque.

6. Elaborar y actualizar planes de continuidad de negocio

Todas las medidas anteriores se puede decir que son medidas preventivas que se han tomado para reducir el impacto que ocasionaría una falla en el suministro de energía eléctrica, pero ¿qué pasa si la interrupción se prolonga por varios días?, ¿tiene la planta de emergencia capacidad para operar este tiempo, de forma continua?

Los planes de continuidad del negocio, se realizan pensando que algo puede fallar y que se deben activar en caso de presentarse un desastre; es decir, el propósito de un plan de

continuidad de negocio es definir la respuesta más efectiva y eficiente a interrupciones de cualquier magnitud que impacten en las operaciones críticas del negocio.

En este caso el CSO, de acuerdo al método de William Toigo se obliga a identificar qué áreas de la institución son las más críticas, para que no detengan su operación en caso de presentarse una falla de esta magnitud.

Para el caso de que se presenten desastres, se evalúa la contratación de los servicios de sitio alterno en el caso de que la organización no pueda proporcionar los mínimos requeridos para que pueda seguir con su operación crítica.

Como se mencionó anteriormente existen varias compañías que ofrecen estos servicios y que sus costos varían entre otras cosas de acuerdo al número de pc's contratadas, renta de servidores, líneas telefónicas, fax, escáners, multifuncionales, etc.

Si la organización proporciona y administra sus propios servidores ubicados en estas instalaciones, el costo es menor ya que no se cobra por renta de equipo; el costo por uso de líneas telefónicas normalmente se cobra por llamadas realizadas utilizando un tarificador.

Etapas para el desarrollo del plan de continuidad del negocio

Etapa 1. Análisis de impacto al negocio.

Etapa 2. Protección de la instalación.

Etapa 3. Almacenamiento fuera del site.

Etapa 4. Estrategia de respaldo de sistemas.

Etapa 5. Estrategia de respaldo de redes.

Etapa 6. Toma de decisiones en caso de emergencia.

Etapa 7. Mantenimiento y pruebas del plan.

Etapa 1. Análisis de impacto al negocio

Éste se lleva a cabo mediante un cuestionario y la idea es identificar qué áreas de la empresa no pueden detener su operación y deben buscarse alternativas para ello.

El cuestionario se efectúa tomando la consideración no sólo de este caso en particular, sino más bien una serie de incidentes que pueden considerarse como desastres.

Este análisis es el que se toma en cuenta para saber con qué compañía se efectúa el contrato de sitio alterno y cuántas pc's son necesarias para continuar con la operación del negocio.

Etapa 2. Protección de la instalación

En el caso de que suceda un desastre desde el punto de vista del negocio, cada área crítica se compromete a tener formado y capacitado un equipo de respuesta a incidentes y son los únicos que tendrán acceso a las instalaciones del sitio alterno contratado para estos casos.

Etapa 3. Almacenamiento fuera del site

Todos los respaldos de programas y sistemas deben estar actualizados a las mismas versiones que se utilizan en producción.

El no tener las mismas versiones es un error muy común, ya que una vez que se hace un respaldo normalmente no se actualiza, si la versión en producción cambia hay que efectuar el respaldo de esta nueva versión.

Por ejemplo, en servidores con sistema operativo Windows, se recomienda el crear discos llamados emergency repair disk, que cuando se está haciendo la instalación en un servidor por lo general se crean estos discos y se guardan.

Posteriormente, se hacen actualizaciones al sistema, se instalan service pack o simplemente hot fixes, pero normalmente no se vuelve a crear los discos de reparación en casos de emergencia y cuando se necesitan no sirven, por no haber efectuado la actualización también a éstos.

Etapa 4. Estrategia de respaldo de sistemas

Esta es la etapa en la cual todos los respaldos de información que se han llevado a cabo de manera preventiva, se utilicen para que se bajen a los servidores del sitio alterno y se continúe con la operación normal del negocio.

Es muy útil una configuración en donde tenga comunicación el servidor de producción con el servidor de respaldo, ya que de esta forma se puede enviar diariamente en un proceso batch todas las actualizaciones que se hayan realizado a los datos durante el transcurso del día.

Otra forma de hacerlo es mediante cintas de respaldo, las cuales son llevadas a una caja fuerte de alguna sucursal bancaria.

Personal del equipo de respuesta a incidentes, previamente especificado acudirá por las cintas y las llevará al sitio alterno.

Etapa 5. Estrategia de respaldo de redes

Normalmente las compañías que ofrecen el servicio de sitio alterno tienen contratados a su vez los servicios de comunicación con diferentes compañías, los cuales vienen de centrales distintas y de esta forma ofrecen continuidad en los servicios de telecomunicaciones que se requieren, ya sea que se necesite enviar correos, o que se ofrezca algún servicio mediante Internet, o se requiera tener una conexión directa a algún banco, etc.

La necesidad de continuidad en las redes de telecomunicaciones, la determinan las áreas operativas del negocio.

El CSO debe verificar que lo que se promete y está especificado en el contrato, realmente se tenga la capacidad de cumplirlo.

Etapa 6. Toma de decisiones en caso de emergencia

Esta etapa se subdivide a su vez en cinco pasos para su implementación.

1. Evaluar el daño.
2. Determinar las causas del daño.
3. Reparar los daños causados por el ataque.
4. Documentar y aprender.
5. Actualizar el plan de contingencia.

1. Evaluar el daño

Al ser ésta una falla que afecta directamente al funcionamiento de la institución, se evalúa el tiempo que va a tardar en arreglarse la falla que originó la falta de suministro de energía eléctrica por parte de la compañía de luz, si es por una falla que se considere grave como por ejemplo un transformador, de inmediato se activa el plan de contingencia, ya que el cambiarlo requiere de un tiempo considerable.

Una vez activado el plan de contingencia, el CSO es uno de los responsables de comunicarse con la empresa del sitio alterno y declarar la contingencia, es recomendable tener un árbol de llamadas para respuesta a incidentes y seguirlo, de esta manera se evita que se realicen llamadas duplicadas.

Ya sea que los integrantes del equipo de respuesta a incidentes de sistemas se comuniquen con el CSO o él se comunique con ellos para definir quiénes acudirán a las instalaciones donde se encuentra el sitio alterno para levantar los servicios requeridos y proporcionar soporte a las áreas operativas que acudirán a trabajar en ese lugar.

Los responsables de las áreas críticas de negocio son los encargados de comunicarse con los miembros del equipo de respuesta a incidentes de su área y definir quiénes son los encargados de acudir al sitio alterno y realizar las operaciones críticas mínimas del día y los subsecuentes hasta que se arregle el problema que forzó acudir a dicho site.

2. Determinar las causas del daño

Es necesario que se determinen las causas que provocaron la falla, ya que de esta forma se puede saber cuánto tiempo se va a tardar en arreglarla, existen muchas causas que pueden provocar que se interrumpa el suministro de energía eléctrica, puede ser desde que se haya botado una pastilla, o una cuchilla, o que un transformador ya no sirva, hasta problemas en subestaciones, o en la generación; cuestiones que van más allá del alcance de este trabajo.

Únicamente se investigará de forma que se pueda establecer de manera aproximada el tiempo que tardará en regresar el abastecimiento de la energía eléctrica.

3. Reparar los daños causados por el ataque

De manera general, si se encuentra la causa del daño se procede a su corrección, en este caso si depende de los proveedores del servicio, de ellos también depende su reparación.

En caso de ser una falla en el equipo de la institución se procede a su reemplazo, para continuar con la operación.

4. Documentar y aprender

Una vez arreglado el problema se procede a documentarlo dentro del mismo plan de contingencias, ¿cuál fue el problema?, ¿cómo se resolvió?, ¿quiénes participaron?, si se presentaron otros problemas, ¿cuáles fueron?, ¿quién los resolvió?, etc.

La idea de documentar los incidentes es evitar que se vuelvan a presentar en caso de ser esto posible y si no, la idea es resolverlos de una manera más rápida y evitar que se presenten otros problemas adicionales al que obligó la declaración de la contingencia.

5. Actualizar el plan de contingencia

Al finalizar la etapa de contingencia y una vez que se vuelve a las condiciones normales de operación, corresponde llevar a cabo la actualización del plan de contingencia con los datos y observaciones de todos los responsables de los equipos de respuesta a incidentes de las áreas que participaron en la contingencia.

Pueden ser actualizaciones de números telefónicos, actualizaciones de listas de contactos de proveedores externos, internos, incluso de procedimientos, forma de acudir al sitio alterno, gastos de transporte, viáticos, etc.

Etapa 7. Mantenimiento y pruebas del plan

Esta etapa indica que se planteen simulacros y operar de acuerdo a la situación supuesta, es importante que se considere que se está en un incidente que puede llegar a ocurrir y debe dársele la seriedad requerida.

Sirven para encontrar fallas en los procesos y documentación y la idea es actualizar el plan de contingencia para evitar las fallas que se presenten en estos simulacros.

6.7.2. Hackers

En este ejemplo se va a considerar la amenaza de los hackers de sombrero negro a una infraestructura de cómputo, en la cual el ambiente es el siguiente:

Se tienen varios servidores de aplicación, realizando las operaciones de negocio de la organización, servidores de correo, servidores de datos y de impresión, servidores de respaldo, servidores de prueba, etc., se tiene contratado un proveedor de servidor de servicios de Internet, y se tiene un servidor web con el que se pretende realizar operaciones de comercio electrónico.

1. Políticas de seguridad

Se verifica que en las políticas de seguridad, estén incluidas las funciones del responsable o administrador de seguridad, donde una de ellas es evaluar los distintos tipos de riesgos a los que está expuesta la información de la organización, así como preparar los planes de implantación de distintos tipos de controles que reduzcan los impactos asociados a estos riesgos.

2. Análisis de riesgos

De acuerdo a las estadísticas mostradas en este trabajo, existe una alta probabilidad de que un hacker quiera atacar la página web de la organización y que el impacto causado por ello varia de moderado a catastrófico, ya que dependiendo de los conocimientos del hacker, el daño provocado puede ser sólo la modificación de la página web, mejor conocido como web defacement, hasta la penetración a la red interna, con derechos de administrador y con la posibilidad de cambiar/borrar información, de dejar puertas traseras, de instalar caballos de Troya, virus, etc.

En la matriz de análisis de riesgo cualitativo, Figura 6.3, esta amenaza significa un riesgo extremo, ya que con la medida cualitativa de probabilidad nivel cinco y el impacto varia de moderado a catastrófico, el riesgo para todos estos casos es extremo.

	IMPACTO				
PROBABILIDAD	**INSIGNIFICANTE 1**	**MENOR 2**	**MODERADO 3**	**MAYOR 4**	**CATASTRÓFICO 5**
CASI CERTEZA 5	**A**	**A**	**E**	**E**	**E**
PROBABLE 4	**M**	**A**	**A**	**E**	**E**
POSIBLE 3	**B**	**M**	**A**	**E**	**E**
IMPROBABLE 2	**B**	**B**	**M**	**A**	**E**
RARO 1	**B**	**B**	**M**	**A**	**A**

Figura 6.3 Matriz de análisis de riesgo cualitativo, amenaza hackers

En esta matriz el significado de las letras es el siguiente:

E: Riesgo extremo.

A: Riesgo alto.

M: Riesgo moderado.

B: Riesgo bajo.

3. Identificación de soluciones

Para proteger a la organización de este tipo de amenaza se necesita la instalación de por lo menos un firewall que reduzca la exposición a Internet de la red interna, se requiere también la compra de un detector de intrusos para que mande una alerta en caso de presentarse una invasión o un acceso no autorizado, y para el servidor web, se demanda la infraestructura de llave pública, todas las soluciones mencionadas caen en la categoría de soluciones técnicas.

Además de lo mencionado anteriormente es necesario contar con soluciones tácticas que fortalezcan la seguridad de los servidores checando constantemente las actualizaciones en seguridad hot fixes y la manera de reducir las vulnerabilidades en ellos, se pueden utilizar herramientas automatizadas, las guías NIST son de mucha utilidad, también es de gran beneficio subscribirse a grupos de noticias, dedicados a publicar vulnerabilidades no sólo de los sistemas operativos sino de programas de aplicación comercial.

4. Implantación y capacitación en las soluciones

Para la selección de firewall, de IDS y de herramientas para detectar vulnerabilidades, el CSO tiene una amplia variedad para escoger.

Uno de los factores que tiene que tomar en cuenta aparte de calidad, precio, facilidad de uso, etc., es el soporte que ofrece el distribuidor de estos productos a sus clientes.

Una vez que se han implantado estas soluciones es recomendable capacitar al personal en el manejo de las mismas, saber cómo configurarlas, cómo indicar que mande las alertas, cómo generar reportes, qué hacer en caso de presentarse alarmas, etc.

5. Auditoría y monitoreo de seguridad

En el caso de las herramientas de firewall y detectores de intrusos, se observa claramente la etapa de monitoreo, ya que son programas que supervisan el uso adecuado de la red y que, de presentarse un comportamiento anormal, generan alarmas que alertan a personal de seguridad de sistemas que está ocurriendo algo raro.

Como se mencionó anteriormente, el personal debe estar capacitado para el manejo de alarmas y tener un adecuado conocimiento para descartar lo que serían falsas alarmas y activar un proceso de manejo de incidentes en caso de ser necesario.

6. Elaborar y actualizar planes de continuidad de negocio

Este paso consiste en siete etapas para que se lleve de manera correcta, las cuales son las siguientes:

Etapa 1. Análisis de impacto al negocio.

Etapa 2. Protección de la instalación.

Etapa 3. Almacenamiento fuera del site.

Etapa 4. Estrategia de respaldo de sistemas.

Etapa 5. Estrategia de respaldo de redes.

Etapa 6. Toma de decisiones en caso de emergencia.

Etapa 7. Mantenimiento y pruebas del plan.

Etapa 1. Análisis de impacto al negocio

En esta etapa se debe evaluar qué áreas operativas afecta un ataque de este tipo, considerando que puede ser muy variado, incluyendo contaminación por virus, modificación de página web, bloqueo de accesos a la página, que el hacker obtenga permisos de administrador, etc.

Etapa 2. Protección de la instalación

La instalación de los controles de firewall y detector de intrusos son herramientas preventivas que mandan una alerta cuando se presenta un comportamiento extraño en la red, así como el uso de herramientas que detectan vulnerabilidades se utilizan para implantar controles preventivos que minimicen las vulnerabilidades de los sistemas operativos y de los programas de aplicación comercial reduciendo de esta forma el riesgo asociado a ellos.

La infraestructura de llave pública es una herramienta muy utilizada por organizaciones que requieren tener una comunicación muy segura, con clientes o con otras organizaciones, hace uso de las llamadas autoridades certificadoras que son las que proporcionan llave pública, llave privada y un certificado digital a empresas y de esta forma se garantiza que los mensajes intercambiados por ellas, sólo pueden ser descifrados por las partes involucradas, garantizando de esta forma su confidencialidad, integridad y autenticación.

Haciendo uso de la criptografía de llave asimétrica, se evita que algún hacker pueda descifrar el mensaje aunque lo intercepte ya que el mensaje se cifra con la llave pública de a quien se le envía el mensaje y sólo él puede descifrarlo con su llave privada.

Además, el que recibe el mensaje comprueba que el mensaje es realmente de quien dice ser que lo está enviando, porque al descifrarlo obtiene el mismo número de certificado digital que le otorgó la autoridad certificadora y de esta forma se evita el problema de no repudio que podría ocurrir en caso de no utilizar esta infraestructura.

Normalmente en el intercambio de esta información se hace uso del protocolo SSL y se establece la comunicación por medio de una red privada virtual.

Esta infraestructura en línea es prácticamente inquebrantable si se implementa adecuadamente.

Etapa 3. Almacenamiento fuera del site

Todos los respaldos de programas y sistemas deben estar actualizados a las mismas versiones que se utilizan en producción.

Y conviene que estén guardados en un lugar seguro fuera de las instalaciones de la organización, llámese caja fuerte, cajas de seguridad en algún banco, o en instalaciones de empresas que se dedican a ello.

Etapa 4. Estrategia de respaldo de sistemas

Esta etapa indica qué tan importante es que la información sea respaldada, ya sea en cintas o en discos, o incluso en servidores externos, a los de producción que son los que la utilizan normalmente.

Para que, en caso de daño, se tenga la versión más actualizada y de esta forma reducir el riesgo de no disponibilidad de ella.

Etapa 5. Estrategia de respaldo de redes

Como se ha mencionado, es muy importante que se tenga la opción de acceso por otro proveedor de telecomunicaciones, para que en caso de que se presente un problema con un acceso, tener la posibilidad de establecer la comunicación por medio de otro enlace.

En este ejemplo se prevé, que de ser necesario, se configurará otro servidor que ofrezca el acceso a la página de Internet de la organización y que se obliga a cambiar la dirección de acceso a donde se le indique.

Etapa 6. Toma de decisiones en caso de emergencia

Los pasos en esta etapa son:

1. Evaluar el daño.
2. Determinar las causas del daño.
3. Reparar los daños causados por el ataque.
4. Documentar y aprender.
5. Actualizar el plan de contingencia.

1. Evaluar el daño

Es muy importante que se haga una evaluación rápida del daño, para que de esta forma se tengan los elementos necesarios y decidir lo que procede hacer.

Se debe evaluar en caso de que un ataque de hacker, si todavía está ahí, si se puede sacar de sesión, si se corta la conexión, etc.

En este paso es donde se evalúa la opción de acudir al sitio alterno.

2. Determinar las causas del daño

Lo que conviene evaluar es cuál hueco utilizó el hacker para entrar, qué vulnerabilidad aprovechó para poder cambiar la página, si el virus entró por medio de un correo, si ya se tiene la vacuna para este tipo de malware, etc.

En este paso resalta la importancia de tener personal capacitado para enfrentar este tipo de ataques.

3. Reparar los daños causados por el ataque

Normalmente se emplean los controles correctivos, aplicación de services packs, así como de hot fix, aplicación de vacunas, etc.

En caso de ser necesario se utilizan los respaldos de la información que se tienen, por si el ataque dañó, modificó o borró la información en uso.

Se tiene también la opción de llamar a los proveedores de las herramientas para que ayuden en esta labor, debe considerarse como una oferta de este servicio en el acuerdo de nivel de servicio que se defina en el contrato celebrado.

4. Documentar y aprender

Una vez solucionado el problema se recomienda documentar, qué problemas se presentaron y qué pasos se llevaron a cabo para resolverlos.

5. Actualizar el plan de contingencia

Como en todos los casos que se presenta un incidente, es conveniente actualizar todo lo que haga falta incluir en el plan de contingencia, para de esta forma tener la seguridad de que se tienen procedimientos útiles, con la información correcta y en donde se definen los pasos a seguir y quién los debe llevar a cabo.

Etapa 7. Mantenimiento y pruebas del plan

Una de las acciones que se deben planear es la opción de hacer pruebas de penetración, ya sea por algún miembro del equipo de respuesta a incidentes que esté capacitado para ello, o por alguna empresa que se dedique a esto, con todos los acuerdos pertinentes.

La idea es encontrar fallas en el plan, sin tener un ataque y ninguna falla real.

Al final de las pruebas es necesario actualizar la documentación y procesos en el plan de contingencias.

De esta forma se puede verificar que el plan de continuidad existe, está actualizado y es de conocimiento de todas las partes involucradas, los servicios a proveer por los terceros son consistentes con las expectativas y necesidades, se encuentran incluidos en el plan todas las necesidades del negocio, las características del sitio de procesamiento alternativo y su equipo son suficientes para los requerimientos de las áreas críticas de operación de la organización.

6.7.3. Auditoría

En este ejemplo se va a utilizar la metodología como proceso de auditoría de seguridad informática para alguna empresa, con el objeto de validar su aplicabilidad en este aspecto.

1. Políticas de seguridad

Como lo indica la metodología, el primer paso es evaluar si la empresa tiene un documento de políticas de seguridad, en donde se indiquen las normas y procesos de seguridad informática.

2. Análisis de riesgos

El siguiente paso es pedir al área de sistemas que muestre todos los análisis de riesgos que se hayan implementado para evaluar su impacto en la organización.

Debe incluir las amenazas que se mencionaron en el capítulo tres, riesgos, amenazas y ataques, las cuales son clasificadas en externas e internas.

En externas se tiene, naturales, humanas y materiales.

Dentro de las naturales pertenecen temblores, incendios, inundaciones y tormentas.

En humanas, robo, sabotaje, fraude y motines sociales.

En materiales, daño del equipo y fallas de energía.

En internas se tiene robo, sabotaje, destrucción, fraude.

Dentro de sabotaje corresponden material, recursos e información (datos y programas).

En destrucción recursos, datos voluntaria e involuntariamente.

Si la organización ha efectuado un análisis con los riesgos mencionados, tendrá una mejor puntuación al evaluar su sistema de seguridad informática que si sólo ha hecho un análisis parcial de estas amenazas.

3. Identificación de soluciones

Con la tarea realizada en el paso anterior se recomienda identificar las soluciones que le permitan a la empresa mitigar las amenazas analizada una por una, ya sea que sólo se tomen medidas tácticas u operativas, siendo no necesario que se efectúen soluciones técnicas, pero de ser así, necesita el apoyo de las dos anteriores.

En el documento donde se realiza el análisis de riesgos al final corresponde indicar qué tipo de solución se deberá implementar.

4. Implantación y capacitación en las soluciones

Una vez que se ha identificado la solución que ha de implantarse, la empresa ha de comprometerse a capacitar a sus empleados en el procedimiento o uso de la herramienta seleccionada.

La empresa deberá mostrar dónde se han implantado las soluciones seleccionadas en el análisis de riesgos.

5. Auditoría y monitoreo de seguridad

La organización ha de mostrar los reportes que tenga, de cada una de las herramientas que haya implementado.

Estos reportes se deben generar periódicamente para hacer un seguimiento adecuado, de esta manera se corrobora que se tiene un correcto sistema de seguridad informática.

La periodicidad de los reportes puede ser diaria, semanal o mensual, según sea la criticidad del activo a proteger.

6. Elaborar y actualizar planes de continuidad de negocio

La empresa deberá mostrar el plan de continuidad del negocio. Éste tendrá que incluir como mínimo la lista de responsables, la sección de administración en crisis, quiénes son los que pueden declarar la contingencia, su calendario de pruebas programadas para el año en curso y los resultados de las pruebas efectuadas hasta el momento.

Cada empresa tiene su propio plan de continuidad de negocio, por lo que se pide sólo la documentación anterior debido a que la mayoría de las metodologías coinciden en los puntos mencionados.

Este ejemplo trata de ilustrar que existen tres factores críticos en un sistema de seguridad informática para que sea funcional.

1. Es imprescindible realizar análisis de riesgos.

2. Contar con los respaldos de la información crítica necesaria para que la empresa opere, es una de las soluciones que debe ser vista de manera independiente.

3. Tener un plan de continuidad de negocio, documentado, actualizado y difundido entre todos los involucrados, permite a la organización realizar sus operaciones críticas y de esta forma garantiza su permanencia en el mercado.

Una vez realizados los ejemplos prácticos de riesgos de fallas externas materiales, como la falla en el suministro de energía eléctrica, amenazas de hackers de sombrero negro y en caso de auditoría, con la metodología descrita se puede concluir que:

Las amenazas naturales son poco frecuentes, pero de alto impacto y tener un sistema de seguridad informática que las contemple permite reducir las vulnerabilidades y el riesgo asociado a ellas.

Para las amenazas de hackers y virus se deben tomar medidas que implican el contar con más herramientas para repeler sus ataques, así como contar con gente capacitada en las tecnologías implementadas para monitorear de manera constante y configurar las alarmas pertinentes, para responder de manera rápida y automática en caso de una contingencia.

Para el caso de la auditoría, la metodología permite percibir que también puede ser útil para esta función, demostrando que es un sistema completo y que se adapta a todas las empresas, no importando el giro ni el tamaño de las mismas.

6.8. Resultados de la aplicación de la metodología de seguridad en redes de computadoras en una institución de crédito hipotecario

La metodología de seguridad en redes de computadoras se aplica en una institución de crédito hipotecario para proteger la información, así como los equipos de cómputo y telecomunicaciones. Sirve además para dar cumplimiento al requerimiento regulatorio acordado por la Comisión Nacional Bancaria y de Valores establecido en el inciso II "La Administración de Riesgo Tecnológico" del artículo 23, sección II, referente a los riesgos cuantificables no discrecionales, de las disposiciones de carácter prudencial en materia de administración integral de riesgos aplicables a las instituciones de crédito, publicadas en el Diario Oficial de la Federación, el primero de julio del año 2004 (en el anexo 1 se muestran estas disposiciones).

Para tener una adecuada administración del riesgo operacional de la institución, se deben tener implantados efectivos controles de seguridad informática.

Algunas actividades que indica la circular incluyen evaluar vulnerabilidades, tanto en software como en hardware, diseñar planes de contingencia y mantener políticas y procedimientos que aseguren en todo momento el nivel de calidad del servicio y la seguridad e integridad de la información.

La institución de crédito hipotecario analizada, ya tenía implantadas varias soluciones, antes de la aplicación de esta metodología, se habían establecido de manera puntual, lo cual es incorrecto debido a que no se sigue la logística de una metodología formal y esta circular dio la oportunidad de dar a la seguridad informática una visión más completa.

De acuerdo a los pasos de la metodología de seguridad en redes de computadoras, se procedió de la siguiente manera:

1. Desarrollo de políticas de seguridad informática.
2. Análisis de riesgos.
3. Identificación de soluciones.
4. Implantación y capacitación en las soluciones.
5. Auditoría y monitoreo de seguridad.
6. Planes de continuidad de negocio.

1. Desarrollo de políticas de seguridad informática

En cumplimiento de la metodología, lo primero que se llevó a cabo fue el desarrollo de políticas de seguridad informática, las cuales se presentaron para su autorización y distribución al comité de seguridad informática, debido a que una vez escritas y aprobadas, se deben difundir

a todo el personal de la institución para que las conozcan, comprendan y apliquen sus lineamientos y de esta forma se eviten sanciones por incumplimiento.

Por ser la primera vez que se hacía una propuesta de este tipo, se presentaron únicamente las referentes al uso de equipo de cómputo y las políticas generales de seguridad informática; en estas últimas se hace hincapié de la importancia de la seguridad, se indica quiénes son los responsables de llevar a cabo los controles (soluciones) para mitigar los riesgos, así como qué personas son las autorizadas para declarar contingencias y acudir a los sitios alternos para continuar con las operaciones críticas de la institución.

Las políticas de uso de equipo de cómputo se refieren principalmente a que está prohibido, por ejemplo, bajar software de páginas web y de cd's que incluyen varias revistas, debido al riesgo de contener virus. El software instalado en las computadoras de los empleados de la institución, es original y tiene el objetivo de que el personal cumpla de manera eficiente con las funciones encomendadas.

2. Análisis de riesgos

A continuación se llevó a cabo el análisis de riesgos, utilizando el estándar australiano-neozelandés de administración de riesgos AS/NZS 4360, efectuando para ello análisis de riesgos externos e internos; dentro de los externos sólo se observaron los naturales correspondientes a temblor e incendio, en humanos hackers y motines sociales, y en materiales daño del equipo y fallas de energía; en los internos, los correspondientes a riesgos de sabotaje a la información, así como la destrucción de los recursos y datos; el resumen de los resultados se muestra en la Tabla 6.2.

AMENAZA	RIESGO	PROBABILIDAD	IMPACTO	SOLUCIONES PARA MITIGAR EL RIESGO
Temblor	Extremo	Probable	Catastrófico	Contratación de sitio alterno. Efectuar respaldos de información. Desarrollo y capacitación en los planes de continuidad de negocio.
Incendio	Extremo	Improbable	Catastrófico	Efectuar respaldos de información. Instalación de sistema automático de detección y extinción de incendio en el centro de cómputo. Contratación de sitio alterno.
Hackers	Extremo	Probable	Mayor	Instalación de firewall. Instalación de IDS.
Motines Sociales	Alta	Posible	Moderado	Contratación de sitio alterno. Desarrollo y capacitación en los planes de continuidad de negocio.
Daño del equipo de cómputo	Extremo	Posible	Mayor	Mantenimiento a pc's cada tres meses. Imágenes de las computadoras personales y de los servidores críticos, respaldadas. Imagen de servidores. Configuración de servidores críticos en cluster. Configuración de servidores, de discos duros en RAID 1 (espejo) sistema operativo y RAID 5 información. Instalación de aire acondicionado en el centro de cómputo de tres equipos de ocho toneladas.
Fallas de energía eléctrica	Extremo	Probable	Mayor	Instalación de un UPS para cada servidor. Instalación de dos plantas generadoras de energía.
Sabotaje a la información	Alta	Posible	Moderado	Efectuar respaldos de información. Control de acceso lógico a la red de la institución y control de acceso a las aplicaciones, mediante perfiles de usuario y validadas a través de passwords. Registro de actividades en servidores.
Destrucción de recursos y datos	Extremo	Posible	Mayor	Control de acceso a cada piso mediante tarjeta magnética. Control de acceso a centro de cómputo por tarjeta magnética, control biométrico y clave de acceso. Instalación de circuito cerrado de televisión.

Tabla 6.2. Resumen de análisis de riesgos en la institución de crédito hipotecario

3. Identificación de soluciones

Una vez terminado el análisis de riesgos, se procedió a verificar si las soluciones necesarias para mitigar de manera adecuada estos riesgos eran las que se tenían ya implantadas, sin embargo se detectó que hacía falta la instalación de sistemas detectores de intrusos y la instalación de un sistema automático de detección de humo e incendio y de extinción del mismo, por lo que se realizaron las acciones pertinentes para su compra incluyendo el servicio de actualización.

4. Implantación y capacitación en las soluciones

Con la información obtenida en el paso anterior se llevó a cabo la instalación de un sistema detector de intrusos basado en red y la de un sistema automático de detección y extinción de incendio, lo cual implicó la capacitación en el uso, configuración y mantenimiento de los mismos.

Asimismo se lleva a cabo una capacitación periódica al personal de la dirección de tecnología de información, en las diferentes soluciones de seguridad informática, y de esta forma tener la configuración eficiente y las versiones más actualizadas de las mismas.

5. Auditoría y monitoreo de seguridad

La institución cuenta con un software de monitoreo de los equipos de cómputo, el cual le permite atender cualquier incidente que se presente en los mismos, los problemas que más se presentan son los de falla en discos, los cuales se cambian en un horario que afecte lo menos posible a los usuarios, sin embargo gracias a la tecnología y a la configuración de algunos en RAID 5 esto se puede realizar de manera inmediata si se cuenta con la disponibilidad de la refacción y sin afectar ningún servicio.

Además, efectúa diariamente revisiones visuales de los equipos de cómputo llamados servidores, así como de los equipos de aire acondicionado, plantas generadoras de energía eléctrica y equipos UPS.

Con la integración de los diferentes reportes que genera el software de monitoreo de los equipos de cómputo, el que produce el software antivirus y las revisiones visuales se efectúan reportes diarios del estado de seguridad del equipo de cómputo de la institución, los cuales se consolidan, para que a fin de mes se cree un reporte con todos los incidentes presentados y la solución que se dio a cada evento.

Cada año una empresa externa realiza una auditoría a la dirección general de sistemas y en todas ellas los dominios que corresponden a la seguridad informática son:

1. Acceso a datos y programas.
2. Seguridad física.
3. Seguridad lógica.
4. Continuidad de negocio.

1. El control de acceso a datos y programas se lleva a cabo mediante perfiles de usuario validadas a través de passwords.

2. La seguridad física es la que se refiere a la protección del daño físico de equipo de cómputo y telecomunicaciones, las cuales pueden ser destrucción de las instalaciones por incendio o temblor, incluyendo las causadas por motines sociales y por el acceso de personal ajeno a la institución.

Para prevenir este tipo de riesgos se tiene implantado el control de acceso físico a las instalaciones, al centro de cómputo, detectores de humo en todos los pisos, extintor de incendio en el centro de cómputo, circuito cerrado de televisión, contratación de un sitio alterno para casos de contingencia; personal de sistemas revisa diariamente la operación normal de todos los servidores de la institución.

3. En seguridad lógica se tienen implantados firewalls, detectores de intrusos, software antivirus, control de acceso lógico a la red de la institución, se llevan a cabo periódicamente análisis de vulnerabilidades, así como actualizaciones de seguridad para las diferentes aplicaciones de software que se utilizan.

4. El plan de contingencia cubre la continuidad del negocio, al que se refiere el último dominio, que las empresas externas auditan.

Todo lo anterior debe estar perfectamente documentado y existir pruebas de que las soluciones están realmente implantadas y funcionando como se espera.

En la institución de crédito hipotecario, la subdirección de análisis de riesgo operativo y de regulación, en conjunto con la subdirección de seguridad informática y base de datos, deben presentar mensualmente al comité de riesgos, un informe de los riesgos tecnológicos ocurridos, indicando su origen y solución o tratamiento.

Se muestra un ejemplo de un reporte mensual de riesgos en el anexo 2.

6. Planes de continuidad de negocio.

Una de las medidas más importantes que se deben llevar a cabo es la de diseñar, implementar y probar planes de continuidad del negocio; investigando y evaluando los planes públicos del Disaster Recovery Institute Internacional (DRII), de Business Continuity Institute y el de William Toigo, se seleccionó este último por ser para la Dirección de Tecnología de Información el más completo, debido a que el oficial de seguridad informática reporta sus actividades a ésta.

La primera etapa para elaborar planes de continuidad de negocio, es realizar un análisis de impacto al negocio, por lo que se diseñó un cuestionario de levantamiento de necesidades (ver anexo 3) a todas las áreas de la institución. Esto permitió a la subdirección de seguridad informática y base de datos saber cuáles eran los requerimientos de equipo y servicios más críticos para su operación; este cuestionario es de desarrollo interno.

Finalmente, la metodología de seguridad en redes de computadoras le permite a la institución, cumplir en tiempo y forma a las auditorías que realiza el Banco de México y empresas externas que se dedican a esta actividad.

CAPÍTULO 7

CONCLUSIONES

La seguridad informática no requiere únicamente de tecnología para implementarla, ya que las soluciones técnicas son sólo una parte de la solución total del problema de seguridad, necesita además de gente capacitada y de procesos bien elaborados y documentados. Sólo con la unión de estos tres elementos se puede garantizar una adecuada implementación de un programa efectivo de seguridad informática.

Para que se pueda decir que se tiene una adecuada seguridad de la información, se deben proteger los principios básicos de ésta, los cuales son confidencialidad, integridad y disponibilidad.

Actualmente las organizaciones son cada vez más dependientes de sus recursos informáticos, esto pone de manifiesto la necesidad de contar con sistemas de seguridad informática acordes a su giro y tamaño, teniendo en cuenta que pérdidas de información o de confidencialidad puede llevar aparejado una pérdida de confianza, prestigio e ingresos en la compañía afectada.

La criptografía ha demostrado su eficacia, al evitar que la información considerada como confidencial sea substraída por personas ajenas a la misma, en la transmisión de información garantiza que en el caso de que ésta sea interceptada, el cracker no pueda interpretarla correctamente, y en el campo de la infraestructura de llave pública ayuda a resolver problemas de no repudio que consiste en que alguien niegue haber enviado una determinada información (que efectivamente envió) o lo inverso, que alguien niegue que recibió cierta información que se le mandó.

La criptografía también ayuda a resolver problemas de autenticidad al asegurar que el origen y el destino de la información son los que dicen y deben ser.

El ingreso al sistema tiene que ser únicamente por usuarios debidamente autorizados con los accesos y privilegios respectivos al sistema y es en este aspecto en el que se ha enfocado la mayoría de las soluciones tecnológicas de seguridad.

El mercado en México de empresas, profesionales y desarrollos en seguridad informática es incipiente. Sin embargo, se requerirá en un futuro próximo de expertos en el tema para cumplir de forma adecuada la normatividad propuesta en este campo. Actualmente, los principales participantes son empresas trasnacionales como IBM, KPMG, Price Waterhouse Coopers, Ernest &Young, Delloitte and Touche, y recientemente se han incorporado a este sector empresas mexicanas como Scitum, Cynthus, ConSeti.

En México, la cultura de seguridad informática no está difundida, ya que aún no forma parte importante de la cultura organizacional del país, el desconocimiento en soluciones de seguridad en informática es generalizado en los niveles de mandos medios de las organizaciones y no existen los expertos en seguridad informática necesarios para cumplir con la demanda que se

está generando con la regulación que se exige en empresas del sector público, gobierno, instituciones financieras, etc.

Tener seguridad informática es más económico que no tenerla, ya que el costo de una falla representa varias veces más el costo para repararla, que tener los mecanismos que permitan evitar que esa falla ocurra.

El tema es interdisciplinario ya que involucra a todas las áreas de una empresa, ya sean técnicos, administrativos, contadores, ingenieros, licenciados en derecho, etc.

Los estándares internacionales dicen qué hacer, pero no dicen cómo; la metodología de seguridad en redes de computadoras mostrada se enfoca precisamente en este último aspecto, pretendiendo ser una guía práctica para la implementación de sistemas de seguridad informática en redes de cómputo de cualquier tipo.

Debido al creciente número de riesgos, amenazas y ataques, a los que está expuesta la información, y tomando en cuenta que un sistema de seguridad informática al 100% no es posible, el impacto al negocio se puede reducir de manera significativa si se lleva a cabo de forma sistemática la metodología de seguridad en redes de computadoras propuesta.

Todos los administradores de sistemas deberían conocer las diferentes medidas para mantener a salvo de intrusos a las empresas y a sus sistemas y no sólo preocuparse por configurarlos para que estén en funcionamiento.

Considerando que la seguridad no es un producto sino un proceso, se necesitan expertos que efectúen análisis de riesgos completos, que seleccionen las mejores soluciones tecnológicas, que las configuren, administren y monitoreen; y al final elaboren planes de continuidad del negocio, en caso de que todas las medidas preventivas de protección fallen.

La metodología de seguridad en redes de computadoras está formada por todos estos pasos y garantiza que si se lleva a cabo para los riesgos que amenazan la información, se tendrán excelentes resultados.

ANEXO 1

…

Sección II

De los riesgos cuantificables no discrecionales

Artículo 23.- Las instituciones de banca múltiple para llevar a cabo la administración del riesgo operativo, deberán asegurarse del cumplimiento de las disposiciones prudenciales en materia de control interno para las instituciones de banca múltiple emitidas por esta Comisión.

Por su parte, las instituciones de banca de desarrollo deberán asegurar:

A. La implementación de controles internos que procuren la seguridad en las operaciones, que permitan verificar la existencia de una clara delimitación de funciones y niveles de autorización.

B. El establecimiento de mecanismos para el control en la liquidación de las operaciones.

C. La existencia de sistemas de procesamiento de información para la administración de riesgos, que permitan reestablecer los niveles mínimos de la operación del negocio ante fallas técnicas, eventos fortuitos o de fuerza mayor.

D. El establecimiento de procedimientos relativos a la guarda, custodia, mantenimiento y control de expedientes que contengan lo relativo a los distintos tipos de servicios y operaciones que realiza la institución.

Las funciones anteriores que, en principio, corresponden a la dirección general de las instituciones de banca de desarrollo, podrán ser asignadas a un área específica o, en su caso, a personal distribuido en varias áreas, siempre y cuando la dirección general se asegure de que se trata de personas o unidades independientes.

En adición a lo expuesto, las instituciones de crédito deberán como mínimo desarrollar las funciones siguientes respecto de:

I. La administración del riesgo operativo:

a) Identificar y documentar los procesos que describen el quehacer de cada unidad de la institución.

b) Identificar y documentar los riesgos operativos implícitos a los procesos a que hace referencia el inciso a) anterior.

c) Evaluar e informar por lo menos trimestralmente, las consecuencias que sobre el negocio generaría la materialización de los riesgos identificados e informar los resultados a los responsables de las unidades implicadas, a fin de que se evalúen las diferentes medidas de control de dichos riesgos.

d) Establecer los niveles de tolerancia para cada tipo de riesgo identificado, definiendo sus causas, orígenes o factores de riesgo.

e) Para el registro de eventos de pérdida por riesgo operativo, incluyendo el tecnológico y legal, deberán:

1. Obtener una clasificación detallada de las distintas unidades y líneas de negocio al interior de la institución de crédito.

2. Identificar y clasificar los diferentes tipos de eventos de pérdida conforme al numeral anterior.

3. Mantener una base de datos histórica que contenga el registro sistemático de los diferentes tipos de pérdida y su costo, en correspondencia con su registro contable, debidamente identificados con la línea o unidad de negocio de origen, según las clasificaciones al efecto definidas por los numerales 1 y 2 anteriores.

El desempeño de las funciones descritas en los incisos a), b), c) y d) a que hace referencia la presente fracción serán responsabilidad del comité de riesgos de la institución de crédito de que se trate, pudiendo auxiliarse en el área que se estime conveniente, siempre y cuando con ello no se susciten conflictos de interés.

Por lo que toca a las funciones relativas al riesgo operativo a que hace referencia el inciso e) anterior, su desempeño corresponderá a la unidad de administración integral de riesgos de la institución de crédito correspondiente. Para ello, las instituciones deberán establecer mecanismos que aseguren un adecuado flujo, calidad y oportunidad de la información entre la referida unidad de administración integral de riesgos y el resto de

las unidades al interior de la entidad, a fin de que estas últimas provean a la primera los elementos necesarios para llevar a cabo su función.

II. La administración del riesgo tecnológico:

a) Evaluar la vulnerabilidad en el hardware, software, sistemas, aplicaciones, seguridad, recuperación de información y redes, por errores de procesamiento u operativos, fallas en procedimientos, capacidades inadecuadas, insuficiencias de los controles instalados, entre otros.

b) Considerar en la implementación de controles internos, respecto del hardware, software, sistemas, aplicaciones, seguridad, recuperación de información y redes de la institución, cuando menos, los aspectos siguientes:

1. Mantener políticas y procedimientos que aseguren en todo momento el nivel de calidad del servicio y la seguridad e integridad de la información; lo anterior con especial énfasis cuando las instituciones contraten la prestación de servicios por parte de proveedores externos para el procesamiento y almacenamiento de dicha información.

2. Asegurar que cada operación o actividad realizada por los usuarios deje constancia electrónica que conformen registros de auditoría.

3. Implementar mecanismos que midan y aseguren niveles de disponibilidad y tiempos de respuesta, que garanticen la adecuada ejecución de las operaciones y servicios bancarios realizados.

c) En caso de mantener canales de distribución para operaciones bancarias con clientes realizadas a través de la red electrónica mundial denominada Internet, cajeros automáticos, banca telefónica, sucursales, entre otros, deberán en lo conducente:

1. Establecer medidas y controles necesarios que permitan asegurar confidencialidad en la generación, almacenamiento, transmisión y recepción de las claves de identificación y acceso para los usuarios.

2. Implementar medidas de control que garanticen la protección, seguridad y confidencialidad de la información generada por la realización de operaciones bancarias a través de cualquier medio tecnológico.

3. Contar con esquemas de control y políticas de operación, autorización y acceso a los sistemas, bases de datos y aplicaciones implementadas para la realización de operaciones bancarias a través de cualquier medio tecnológico.

4. Incorporar los medios adecuados para respaldar y, en su caso, recuperar la información que se genere respecto de las operaciones bancarias que se realicen a través de cualquier medio tecnológico.

5. Diseñar planes de contingencia, a fin de asegurar la capacidad y continuidad de los sistemas implementados para la celebración de operaciones bancarias, a través de cualquier medio tecnológico. Dichos planes deberán comprender, además, las medidas necesarias que permitan minimizar y reparar los efectos generados por eventualidades que, en su caso, llegaren a afectar el continuo y permanente funcionamiento de los servicios.

6. Establecer mecanismos para la identificación y resolución de aquellos actos o eventos que puedan generarle a la institución, riesgos derivados de:

i. Comisión de hechos, actos u operaciones fraudulentas a través de medios tecnológicos.

ii. Contingencias generadas en los sistemas relacionados con los servicios bancarios prestados y operaciones celebradas a través de cualquier medio tecnológico.

iii. El uso inadecuado por parte de los usuarios de los canales de distribución antes mencionados, para operar con la institución, a través de los medios citados en el presente artículo.

La institución deberá evaluar las circunstancias que en materia de riesgo tecnológico pudieran influir en su operación ordinaria, las cuales se sujetarán a vigilancia permanente a fin de verificar el desempeño del proceso de administración integral de riesgos.

...

ANEXO 2

REPORTE DE RIESGO TECNOLÓGICO

DIRECCIÓN DE TECNOLOGÍA DE INFORMACIÓN Julio 2004

Clasificación	Grupo	Elemento	Tipo de incidentes	Número de incidentes
Seguridad Física	Eventos externos	Humanos		
		Naturales		
		Materiales	Suministro de energía eléctrica	2
	Hardware	Servidores	Falla en un disco duro del servidor de desarrollo UPS Firewalls	1 1
		Red local (LAN)		
		Enlaces (WAN)		
		Telefonía	Tarificador	1
		UPS		
		Planta de emergencia		
Seguridad Lógica	Software	Sistema operativo		
		Antivirus		
		Firewalls		
		Aplicaciones de servidor[1]	Web interno. Correo interno. Balanced Score Card.	3
		Aplicaciones de operación[2]		
TOTAL				8

Día 4. Se presentó una alarma en los UPS donde están conectados los firewalls. De acuerdo al manual, esto consiste en que la alimentación es 15% más baja de lo que se espera. Este caso quedó cerrado el día 15 reacomodando las conexiones de salida.

Día 7. Se dio de baja la aplicación SQL Remote, la cual corre en el servidor de replicación, ya que no enviaba la información hacia el web Interno, provocando que no se actualizaran las páginas, pero no se suspendió el acceso a ellas. Una vez levantada la aplicación quedó trabajando normalmente.

Día 10. Se efectuaron pruebas al plan de contingencia, participando en ellas las subdirecciones de control de operaciones de tesorería, control operativo de crédito y garantías, tesorería, cartera y cobranza, soporte a usuarios, cómputo y telecomunicaciones, seguridad informática y base de datos.

Día 11. El tarificador dejó de procesar el registro de llamadas telefónicas, por lo que manualmente se ejecutó la instrucción "Procesar". No se pierde información. Quedó operando OK.

Día 14. Caída del servicio de la aplicación SPImact (Balanced Scorecard) se realizó respaldo y se levantó nuevamente el servicio. Se reportó a personal de la subdirección de gestión de calidad para que verificara el funcionamiento correcto de la aplicación.

Día 17. Se presentó una falla en un disco duro del servidor de desarrollo de sistemas, se procedió a la reconstrucción de la información. Este servidor tiene una configuración de espejo de sus discos duros, por lo que no se perdió información ni se afectó el servicio. Quedó funcionando bien.

Nota: El detalle de las pruebas al plan se encuentra en el plan de contingencias de sistemas.

Subdirección de seguridad informática y base de datos

Subdirección de análisis de riesgo operativo y de regulación

[1] Bases de datos, correo, impresión, respaldos, etc.

[2] Módulos de Apesa, Risk Watch son aplicaciones que utiliza la Dirección de Tesorería

ANEXO 3

Formato XXX-XXX

Institución de Crédito Hipotecario

Fecha:

REQUERIMIENTOS ANTE CONTINGENCIAS

OBJETIVO:
Tener una referencia de los requerimientos tecnológicos mínimos que se necesitan para mantener la operación crítica de la institución cuando se presenten contingencias.

ÁREA: _____
Nombre de la Dirección o Subdirección

Consideraciones:

1. Todas las áreas en la institución son responsables de mantener su propio plan de contingencias que les permita soportar las operaciones críticas en caso de contingencia. Este cuestionario tiene la finalidad de identificar los requerimientos tecnológicos que brinden soporte a dichos planes.

2. Enumere en la siguiente tabla los procesos de información que requiere mantener en caso de una contingencia, ordenándolos por grado de criticidad, de forma que el más crítico sea el primero y el menos crítico esté al final.

3. En la columna de la derecha indique con qué otras áreas o entidades tienen relación dichos procesos.

	Procesos prioritarios	Áreas relacionadas
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Proceso:	
Responsables dentro del área:	
Horarios de las ventanas críticas:	
Días claves en la semana, mes y año:	
Tiempo de utilización:	

Recursos tecnológicos indispensables para realizar el proceso:

Equipo	Descripción general	SI / NO	Cantidad
Computadora			
Impresora			
Fax			
Internet			
Grabación de llamadas			

Módulos del sistema y demás software necesario:
Servicios fuera de la organización:
Observaciones:

Lista de contactos externos			
Organización:			
Nombre del contacto:			
Puesto:			
Dirección:			
Teléfonos:	**Extensiones:**	**Fax:**	**Correo electrónico:**
Otros			

Lista de contactos internos

OBJETIVO

Tener una lista de contactos internos para poder mantener la comunicación entre los compañeros de la institución en caso de que se presente una contingencia. La lista debe incluir al director de área, a los subdirectores y a todas las personas que integran el equipo de respuesta a incidentes.

Dirección

Persona No.___ Nombre: _____	Persona No.___ Nombre: _____
Puesto: _____	Puesto: _____
Teléfono: _____	Teléfono: _____
Celular: _____	Celular: _____
Fax: _____	Fax: _____
E-mail: _____	E-mail: _____
Persona No.___ Nombre: _____	Persona No.___ Nombre: _____
Puesto: _____	Puesto: _____
Teléfono: _____	Teléfono: _____
Celular: _____	Celular: _____
Fax: _____	Fax: _____
E-mail: _____	E-mail: _____

EQUIPO DE RESPUESTA A INCIDENTES (ERI)

Nombre	Firma

Responsabilidades	

Nombre y Firma	Nombre y Firma
Vo. Bo. Subdirector	**Vo. Bo. Director**

BIBLIOGRAFÍA

Schneier Bruce
Secrets and Lies: Digital Security in a Networked World
Wiley
U.S.A.
2000

Harris Shon
Cissp All in One Exam Guide
McGraw Hill / Osborne
U.S.A.
2002

Krutz Ronald L., Dean Vines Rusell
The Cissp Prep Guide Gold Edition
Wiley
U.S.A.
2003

Ramió Aguirre, Jorge
Seguridad informática y criptografía
Universidad Politécnica de Madrid
España
2003

Bello, Claudia
Manual de seguridad en redes
Secretaría de la Función Pública
ARGENTINA
2002

Gómez Cárdenas, Roberto
Seguridad computacional
Instituto Tecnológico de Estudios Superiores Monterrey, Campus Estado de México
México
2001

Gómez Cárdenas, Roberto
Apuntes de la maestría en ciencias de la computación
Criptología y otras herramientas de seguridad
Instituto Tecnológico de Estudios Superiores Monterrey, Campus Estado de México
México
2001

REFERENCIAS

https://www.isc2.org/cgi-bin/content.cgi?category=97

https://www.isc2.org/cgi-bin/content.cgi?category=98

http://www.sans.org/top20

http://www.gocsi.com

http://www.cert.org

http://csrc.nist.gov/publications/nistpubs

http://www.drj.com

http://www.bci.com

http://www.hispasec.com