UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

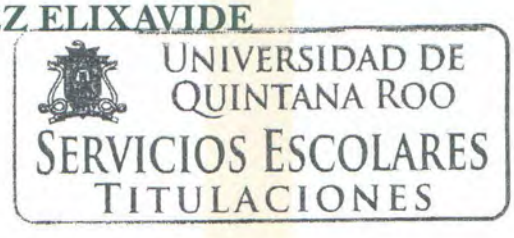
SEGURIDAD PERIMETRAL

TRABAJO MONOGRÁFICO
PARA OBTENER EL GRADO DE

INGENIERO EN REDES

PRESENTA
FEDERICO OSORIO ESCALANTE

ASESORES
M.S.I. LAURA YÉSICA DÁVALOS CASTILLA
M.T.I. VLADIMIR VENIAMIN CABAÑAS VICTORIA
M.S.I. RUBÉN ENRIQUE GONZÁLEZ ELIXAVIDE



CHETUMAL QUINTANA ROO, MÉXICO, OCTUBRE DE 2014

UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

TRABAJO MONOGRÁFICO BAJO LA SUPERVISIÓN DEL COMITÉ DEL PROGRAMA DE LICENCIATURA Y APROBADA COMO REQUISITO PARA OBTENER EL GRADO DE:

INGENIERO EN REDES

COMITÉ DE TRABAJO MONOGRÁFICO

ASESORA: _____
M.S.I. LAURA YESICA DÁVALOS CASTILLA

ASESOR: _____
M.T.I. VLADIMIR VENIAMIN CABAÑAS VICTORIA

ASESOR: _____
M.S.I. RUBÉN ENRIQUE GONZÁLEZ ELIXASUD

UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

UNIVERSIDAD DE QUINTANA ROO
SERVICIOS ESCOLARES
TITULACIONES

CHETUMAL QUINTANA ROO, MÉXICO, OCTUBRE DE 2014

Tabla de contenido

Tabla de ilustraciones

Agradecimientos

A mis padres, hermanos, sobrinos y a Dios
por haberme dado la motivación, inspiración,
fuerza y voluntad para continuar en el camino
del conocimento y la superación.

A mi supervisora de monografía y tutora,
M.S.I. Laura Yésica Dávalos Castilla
por su paciencia y apoyo como guía
durante este interesante viaje.

A mis compañeros, amigos y maestros
de la carrera de Ingeniería en Redes que
fueron mi familia en todo momento
durante este camino.

DEDICATORIA

Dedico este trabajo a todo ser, que, de la nada puede convertirse en un todo a pesar de las líneas marcadas a su paso.

A mis padres que, con este logro quiero devolver algo de lo que ellos me dieron desde que empecé a existir.

1. INTRODUCCIÓN

El espectacular crecimiento de internet y de los servicios telemáticos (comercio electrónico, servicios multimedia de banda ancha, administración electrónica, herramientas de comunicación como el correo electrónico o la videoconferencia, redes sociales, etc.) han contribuido a popularizar aún más el uso de la informática y de las redes de computadoras.

Por otra parte, los servicios críticos para una sociedad moderna, como podrían ser los servicios financieros, el control de la producción y suministro eléctrico (centrales eléctricas, redes de distribución y transformación), los medios de transporte etc. están soportados en su totalidad por sistemas de redes informáticas, hasta el punto de que en muchos de ellos se han eliminado o reducido de forma drástica los procesos manuales.

Por todo lo anterior, se hace evidente que las actividades cotidianas de las empresas, de las administraciones públicas, así como la de los propios ciudadanos, requieren del correcto funcionamiento de los sistemas y redes informáticas que los soportan.

Henry Farol (1919) consideraba la seguridad como una función empresarial, al mismo nivel que otras funciones: producción, comercial, financiera, administrativa…

Estas primeras etapas de seguridad en las empresas se limitaban a las medidas encaminadas a la protección de los activos físicos e instalaciones, ya que ese era el mayor activo de las organizaciones y no se tenía en importante consideración la información o los propios empleados.

En la actualidad el desarrollo de las actividades de los organismos mencionados anteriormente dependen de los datos e información registrados en sus sistemas informáticos, así como del soporte adecuado de las TICs (Tecnologías de información y la comunicación), para facilitar su almacenamiento, procesamiento y distribución, por todo ello es necesario

trasladar a los directivos la importancia de valorar y proteger la información de sus empresas.

La falta de infraestructura tecnológica para respaldar y recuperar datos puede representar pérdidas irrecuperables para las empresas en términos de ingresos y confianza en el mercado.

El director de la división de respaldo y recuperación de EMC para México y Norte de Latinoamérica, Josafath Ramírez, señaló que a nivel mundial, el %57 de las empresas sufrió la pérdida de datos en el último año, derivada de ataques informáticos, fallas físicas de los equipos de almacenamiento y otras causas.

Asimismo el 11 de septiembre de 2001 en los atentados de las torres gemelas en New York, muchas empresas perdieron sus oficinas centrales y, sin embargo, pudieron continuar con la actividad de su negocio a los pocos días, ya que sus datos estaban protegidos y sus sistemas informáticos contaban con los adecuados planes de contingencia y de respuesta a emergencias.

En España el incendio del rascacielos Windsor en Madrid (12 de febrero de 2005), un edificio de 28 plantas dedicado a oficinas, en el que la consultora y auditora DELOITTE & Touche ocupaba 20 plantas, fue un acontecimiento que contribuyó a despertar un mayor interés por la seguridad en los sistemas de información. (Vieites, 2007)

En los últimos años, la tecnología de almacenamiento en la nube ha experimentado un crecimiento considerable en cuanto al número de usuarios finales y empresas que la utilizan. Si antes era común ver que las personas compartían información a través de disquetes, medios ópticos (CD/DVD), dispositivos de almacenamiento extraíbles USB, u otros, en la actualidad es posible observar una clara tendencia hacia el uso masivo de la nube en detrimento de otros medios “tradicionales”. Las ventajas que ofrece la nube son considerables ya que, por ejemplo, facilita el acceso a la información puesto

que los archivos están disponibles desde prácticamente cualquier lugar que cuente con conexión a Internet.

Todas esas ventajas han provocado que la nube sea una tecnología cada vez más popular entre todo tipo de usuarios. En este sentido, Gartner (empresa consultora y de investigación de las tecnologías de la información), aseguró que en 2011 solo un 7% de la información de los usuarios finales fue almacenada en la nube, sin embargo, se espera que para el año 2016 dicho porcentaje aumente a un 36%. Por otro lado, la publicación "Global Cloud Index" de Cisco, estima que en 2017 los usuarios de América Latina habrán almacenado una cantidad de 298 exabytes de información en la nube (1 billón de gigabytes).

Otro estudio que avala el aumento de la preocupación de las personas con respecto a la privacidad en Internet, es la encuesta realizada por ComRes, una consultora de investigación de Gran Bretaña. Esta investigación arrojó que de un total de 10.354 entrevistados que viven en nueve países distintos (Brasil, Gran Bretaña, Alemania, Francia, España, India, Japón, Corea del Sur y Australia), el 79% manifestó estar preocupado por su privacidad en la red. Asimismo, los países que se mostraron más alarmados por este fenómeno son India (94%), Brasil (90%) y España (90%).

De acuerdo a la información recopilada sobre los países que contempló la investigación, Alemania es el menos preocupado por la privacidad en Internet. El resto de las naciones comparten una visión más uniforme sobre la importancia de proteger adecuadamente el ámbito íntimo de las personas en la red. (Latinoamérica, 2014)

El Informe sobre las amenazas para la seguridad en Internet proporciona una descripción general y un análisis anual sobre la actividad de las amenazas de todo el mundo. El informe se basa en los datos de la red Symantec Global Intelligence Network, que los analistas de Symantec utilizan para identificar, analizar y proporcionar comentarios sobre las tendencias emergentes en el escenario de amenazas dinámico.

Puntos destacados del Informe sobre Amenazas a la Seguridad en Internet, 2014

Principales hallazgos

- Aumento de 91% en las campañas de ataques dirigidos en 2013
- En 2013, las fugas de datos aumentaron 62%
- Se expusieron más de 552 millones de identidades como resultado de las fugas de datos en 2013
- Se descubrieron 23 vulnerabilidades de Día Cero (zero-day)
- El 38% de los usuarios móviles fueron víctimas del cibercrimen en los pasados 12 meses
- El volumen de spam disminuyó y representó el 66% de todo el correo electrónico
- 1 de cada 392 correos electrónicos es un mensaje fraudulento o phishing
- Los ataques basados en la web crecieron un 23
- 1 de cada 8 sitios web legítimos tiene vulnerabilidades críticas. (Symantec, www.symantec.com, 2014)

3.1 Antecedentes

Las redes informáticas representan un medio para realizar ataques a los sistemas informáticos de las organizaciones, por lo cual es necesario contar con medidas que disminuyan el impacto de dichos ataques que afectan principalmente el rendimiento y la confiabilidad de los sistemas. Actualmente, existen bandas de crimen organizado que utilizan todos los recursos y tecnologías presentes en Internet para garantizar su anonimato y cometer todo tipo de delitos informáticos: *phishing, pharming* (Ballard, 1982), *scam, clickfraud, worms, zerodayexploits, spam*, ataques de denegación de servicio distribuidos (DDoS) y un largo etcétera de amenazas a las que los sistemas informáticos y los usuarios son susceptibles.

Los sistemas de seguridad en informática y redes han ido evolucionando para dar cada vez una mejor protección a la información de los usuarios y empresas, cada día se descubren nuevos puntos débiles y, por lo general, son pocos los responsables de TI que comprenden en su justa medida la importancia que tiene la seguridad y cómo pueden abordar el grave problema que existe detrás de vulnerabilidades que permiten a un atacante, violar la seguridad de un entorno y cometer delitos en función de los datos robados. (Mieres, 2009)

Sin duda uno de los pioneros en el tema de la seguridad informática fue James P. Anderson, quien allá por 1980 y a pedido de un ente gubernamental produjo uno de los primeros escritos relacionados con el tema, y es allí donde se sientan también las bases de palabras que hoy suenan como naturales, pero que por aquella época parecían ciencia ficción.

El documento se llamó: “Computer Security ThreatMonitoring and Surveillance“, y describe ahí la importancia del comportamiento enfocado hacia la seguridad en materia de informática.

Las siguientes definiciones son usadas en este documento:

Amenaza: la posibilidad de un intento deliberado y no autorizado de:

a) Acceder a información.

b) Manipular información.

c) Convertir un sistema en no confiable o inutilizable.

Riesgo: Exposición accidental e impredecible de información, o violación de la integridad de operaciones debido al malfuncionamiento de hardware o diseño incorrecto o incompleto de software.

Vulnerabilidad: una falla conocida o su sospecha tanto en hardware como en el diseño de software, o la operación de un sistema que se expone a la penetración de su información con exposición accidental.

Ataque: Una formulación especifica o ejecución de un plan para llevar a cabo una amenaza.

Penetración: Un ataque exitoso; la habilidad de obtener acceso no autorizado (indetectable) a archivos y programas o el control de un sistema computarizado."

Un gran número de ataques a los activos informáticos provienen del exterior de la empresa, intrusos y aplicaciones no autorizadas pueden aprovechar los puntos vulnerables de la red local y poner en riesgo la integridad, confidencialidad y disponibilidad de la información.

Aunque los usuarios cuenten con sistemas antivirus y firewall personal, es necesario disponer de una plataforma que evite que los ataques ingresen a la red interna y comprometan su rendimiento y productividad.

1.2 Objetivos

General

Crear un documento que permita representar el funcionamiento de los sistemas de seguridad perimetral en redes corporativas.

Específicos:

- Investigar y crear un esquema sobre la estructuración de un sistema de seguridad perimetral.

- Obtener el conocimiento avanzado en; dispositivos de hardware y software implementados en un sistema de seguridad perimetral.

- Investigar y analizar bibliografía sobre tecnologías de la información

enfocada a seguridad perimetral.

1.3 Alcance

El alcance de este trabajo es el de recopilar información bibliográfica de diferentes autores, sobre el funcionamiento de diferentes tecnologías que pueden utilizarse en un sistema de seguridad perimetral de una red corporativa.

1.4 Metodología.

Se analizarán tecnologías de hardware, software y aplicaciones utilizadas en la protección de datos de una red corporativa. Lo anterior es con la finalidad de crear un documento el cual sirva como herramienta para los administradores de redes en la implementación y adquisición del equipo adecuado.

Tipo de investigación:

- Documental

Método utilizado:

- Análisis

Objeto:

- Tecnologías de seguridad en redes.

Medio:

- Recopilación de información bibliográfica y referencias electrónicas.

Fin:

- Proporcionar las bases necesarias para implementar estrategias que permitan mejorar la seguridad en los sistemas de información.

2. MARCO DE REFERENCIA

2.1 Seguridad Informática

La seguridad informática es la protección de la información y sus características (Confidencialidad, Integridad, disponibilidad) incluyendo los sistemas de hardware y software que se utilicen para almacenar y transmitir la información, mediante la aplicación de políticas. (Mattord, 2010)

Otra definición sería el conjunto de recursos destinados a lograr que la información y activos de una organización o empresa sean confidenciales, íntegros, constantes y que estén disponibles para los usuarios autorizados mediante mecanismos de control de acceso. (Grupo IWI, 2009)

La seguridad informática, o de forma más global, la seguridad en los sistemas de información, representa el conjunto de medios y técnicas implementados para asegurar la integridad y que no se difundan involuntariamente los datos que recorren el sistema de información, entendiendo como tal al conjunto de datos y recursos (Físicos, lógicos y humanos) que permiten almacenar y que circule la información que contiene. (Acissi, 2011)

La seguridad informática es un asunto que preocupa a las empresas y que consiste en poner en práctica una serie de recursos con el fin de lograr confidencialidad, integridad, constancia y disponibilidad de los activos de la empresa.

Obviamente, para lograr una seguridad de los sistemas información realmente efectiva es necesaria una participación real de la dirección de la empresa, ya que ésta es la única figura con poder de decisión (sin el apoyo de la dirección las políticas o los procedimientos de seguridad no tendrán validez, ni serán respetados.) Además, la constante formación e información del personal es igualmente vital. Es necesario que los usuarios que tienen acceso a los sistemas de información estén formados sobre la correcta utilización de los equipos y conozcan los procedimientos de seguridad que deben de aplicar.

Para que un sistema de información sea seguro debe de cumplir varios requisitos:

1. **Integridad:** La información no debe poder ser modificada por alguien que no esté autorizado.
2. **Confidencialidad:** La información solo debe ser legible para las personas autorizadas.
3. **No repudio:** La autoría debe de ser irrefutable, es decir, no debe caber la menor duda de quién ha ocasionado el daño.
4. **Disponibilidad:** La información debe estar siempre disponible.

A pesar de todo lo dicho anteriormente, para la mayoría de los expertos en la materia, no existe un sistema que sea100% seguro. Algunas de las causas por la cuales un sistema es vulnerable son:

- Negligencia de un usuario.
- Error accidental causado por un usuario.
- Desconocimiento o incomprensión de las políticas ó procedimientos de seguridad.

Sin embargo, la seguridad informática es una tarea obligatoria en cualquier empresa que no desee que su información sea robada, modificada o vulnerada de cualquier forma.

Para lograr la máxima seguridad posible hay una frase utilizada por los expertos en la materia: Lo que no está permitido, debe de estar prohibido. Así pues, hay una serie de objetivos que se deben lograr:

1. Restringir el acceso a los programas y archivos que contengan información sobre los datos de carácter personal.
2. Restringir la posibilidad de modificar datos a los usuarios no autorizados.
3. Asegurar que la información que se transmite sea la misma que recibe el destinatario.
4. Asegurar la existencia de sistemas de emergencia alternativos.

5. Organizar al personal a través de claves de acceso distintas y permisos de acceso bien establecidos.
6. Actualizar las contraseñas de acceso a los sistemas periódicamente.

La seguridad informática es muy importante en una empresa, pero nunca debe impedir el trabajo de los usuarios, ésta debe servir para facilitar el trabajo de los usuario y no al contrario, por este motivo, es muy importante diseñar buenos procedimientos y reglas que definan cada servicio o protocolo de la empresa.

También es importante definir una persona encargada de solucionar los problemas como la pérdida de información o el acceso no autorizado a los sistemas de información, y por supuesto, sensibilizar al personal que accede a los sistemas con los posibles problemas que podrían derivarse de un mal uso de los mismos, como siempre, la información y la formación del personal son importantes para evitar posibles errores o pérdidas.

2.2. Zonas de Seguridad.

Zona Internet

Esta zona agrupa la mayoría de los sitio web disponibles en la red que no han sido añadidos a otras zonas, como la zona de sitios de confianza o la zona de sitios restringidos. Esta zona recibe de forma predeterminada una configuración de seguridad Media-alta.

Zona Intranet

Esta zona representa los sitios internos de una organización, es decir, sitios que controlan los administradores de la organización y que por lo tanto son dignos de confianza. Como consecuencia, la configuración de seguridad se sitúa en medio-bajo, autoriza muchas acciones y la ejecución de muchas funcionalidades que podrían suponer riesgos de seguridad si la fuente (sitio web) no es totalmente fiable

Zona de Confianza

La zona de los sitios de confianza contiene los sitios en los que confía plenamente y a los que autoriza a ejecutar cualquier acción en su equipo. La configuración de seguridad está predeterminada en Baja. Los sitios de confianza reciben muy pocas restricciones de seguridad y, además, el modo protegido del navegador no está activado para esta zona.

Antes de añadir un sitio a esta zona, hay que evaluar las consecuencias de hacerlo y de no hacerlo y las eventuales implicaciones de seguridad.

Zona de Equipos Restringidos

Esta zona contiene sitios que pueden causar daño a su equipo y a su empresa. Además de ser bloqueados por el firewall o el proxy de la empresa, conviene añadirlos a esta lista para limitar las consecuencias sobre la seguridad.

No obstante si se añaden muchos sitios web a esta zona se puede ralentizar la navegación.

De forma predeterminada la seguridad en esta zona es Alta.

Zona Máquina Local.

Esta zona oculta representa la máquina donde está instalado el navegador y define los permisos para los archivos almacenados localmente, Esta zona dispone de los privilegios más elevados, sin embargo desde XP SP2 es posible restringir la zona máquina local para evitar que los piratas eleven sus privilegios aprovechándose del nivel de permisos de la zona local. (Elmaleh, 2011)

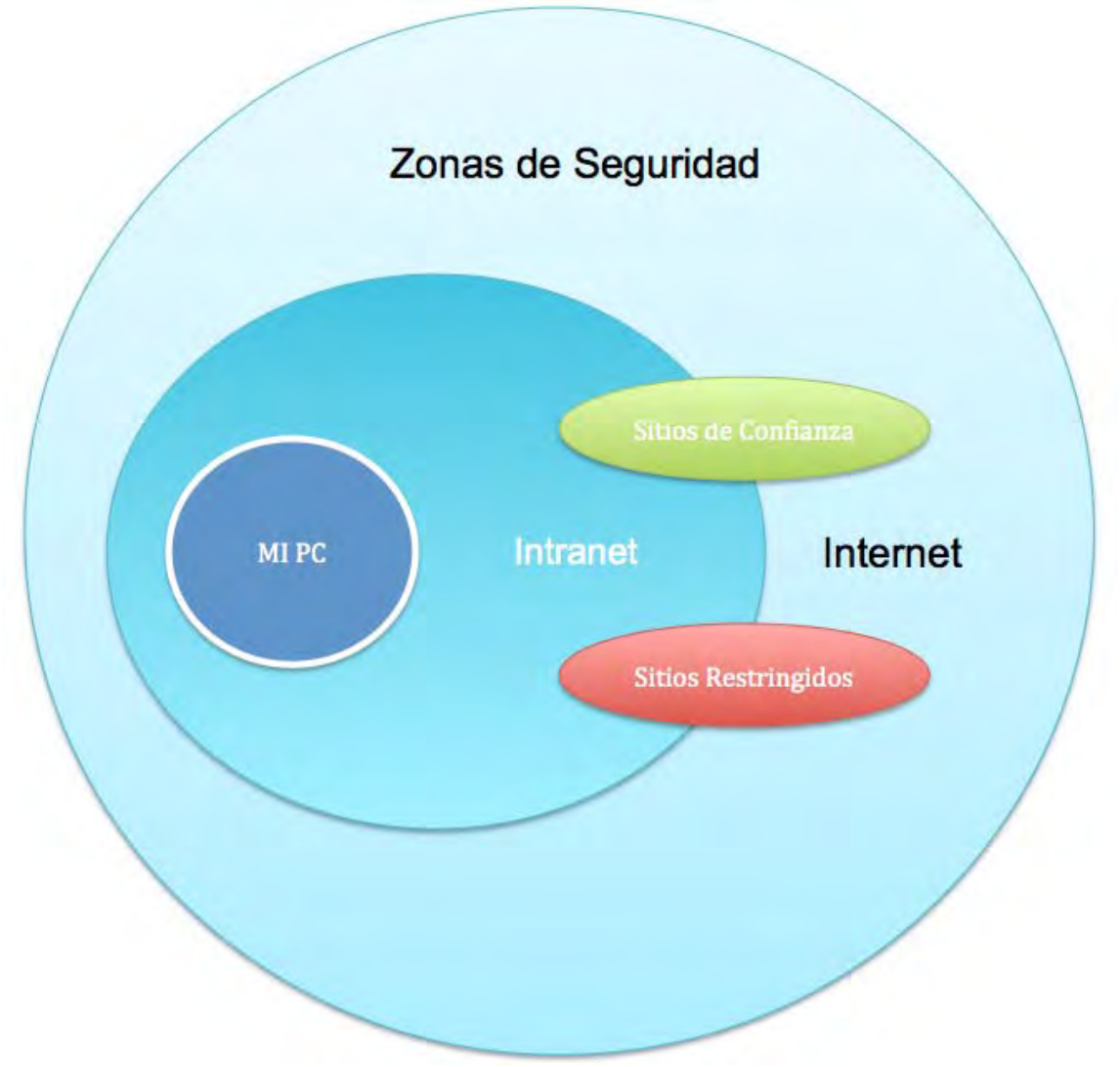


Ilustración 1 - Zonas de Seguridad

2.2.1 Seguridad Física.

La seguridad física consiste en proteger el sistema informático utilizando barreras físicas y mecanismos de control. Se emplea para proteger físicamente el sistema informático. Las amenazas físicas se pueden producir provocadas por el hombre, de forma accidental o voluntaria. O bien por factores naturales. (Alfonso Garcia-Cerevignon Hurtado, 2011)

La seguridad física abarca desde el diseño, implementación, y mantenimiento de las medidas que protegen los recursos físicos de una organización, incluyendo personal, hardware, y elementos que dan soporte al sistema que controla la información en todos sus estados (Transmisión, almacenamiento, y procesamiento). (Michael E. Whitman H. J., 2012)

Es la seguridad física del proceso de datos de la organización. Incluye: condiciones ambientales adecuadas y suministro de energía constante así como actitudes de la administración frente a la seguridad de los sistemas de información, a programas de entrenamiento del personal, a planes de contingencia para desastres o interrupciones del procesamiento, y a la adquisición de pólizas de seguro para cubrir el riesgo de siniestros. (Quiroz, 1996)

Donn B. Parker en su libro “Fighting Computer Crime” enlista las siete principales fuentes de pérdidas físicas en los sistemas TI:

1. **Temperatura extrema**: calor, frío.
2. **Gases**: fugas de tuberías de gas, aire seco o húmedo, partículas suspendidas, vapor comercial.
3. **Líquidos**: Agua, químicos.
4. **Organismos**: virus, bacterias, gente, animales, insectos.
5. **Proyectiles**: objetos en movimiento.
6. **Movimientos**: Terremotos, vibración, deslizamientos, huracanes, tifones, etc.
7. **Energía**: fallas eléctricas, magnetismo, electricidad estática, circuitos viejos, radiación, sonido, luz, radio, microondas, electromagnetismo.

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el sistema de TI.

Las principales amenazas que se prevén en la seguridad física son:

- Desastres naturales, incendios accidentales tormentas e inundaciones.
- Amenazas ocasionadas por el hombre.
- Disturbios, sabotajes internos y externos deliberados.

Además de las fuentes de pérdidas que enlista Donn B. Parker en su libro a continuación analizamos otras mencionadas como acciones hostiles y de control de acceso, este tipo de pérdidas son causadas por el humano.

Acciones Hostiles

- **Robo:** principalmente de información ya sea extraída de una computadora, robo de discos duros, cintas, videos, documentación, etc.
- **Fraude:** Cada año se da este tipo de pérdidas millonarias en las empresas, las computadoras son el instrumento utilizado para cometer este tipo de violación.
- **Sabotaje:** Uno de los peligros más temidos por las empresas, ya que el atacante puede ser tanto una persona de la empresa, como ajena a esta y basta con introducir algún material ya sea químico o imanes como para borrar información de cintas almacenadas o cortar el suministro de energía y causar un daño irreversible a la información resguardada de la empresa.

Control de acceso

El control de acceso no solo consiste en la identificación de los usuarios que tienen acceso autorizado al sistema, también al control de los horarios en los que estos pueden operar, así como las áreas con restricción a las que no les es permitido entrar.

- **Guardias de seguridad privada:** Identificación de los usuarios, revisión de mochilas, bolsas, etc., registro de entrada y salida.
- **Detectores de metales:** detección de algún instrumento de metal (herramientas, armas, imanes).

- **Sistemas biométricos:** Registro por huella digital, verificación de voz, patrones oculares, etc.
- **Seguridad con animales:** Principalmente para sobreproteger el perímetro de la empresa (Terreno)
- **Protección electrónica:** Cámaras de circuito cerrado, infrarrojos, sensores de movimiento, etc.

Llevar un control de evaluación permanente de la seguridad en la se encuentra nuestra organización, es la base principal para mantener en constante crecimiento el aprendizaje de cómo tener el mejor control de la seguridad y que sea una de las funciones principales en nuestra empresa.

2.3 Seguridad Lógica.

La seguridad lógica se encarga de asegurar la parte del software de un sistema informático que se compone de todo lo que no es físico, es decir, los programas y datos.

La seguridad lógica controla que el acceso al sistema informático desde el punto de vista software, se realice correctamente por usuarios autorizados, ya sea desde dentro del sistema como desde fuera, es decir desde una red externa. (Alfonso Garcia-Cerevignon Hurtado, 2011)

La seguridad lógica involucra mecanismos de software para proteger un sistema informático y la información que contiene, como el uso de contraseñas, encriptación de la información, antivirus, cortafuegos, etc. (Ramos, 2010)

La seguridad lógica se refiere principalmente a mantener la integridad de los datos y asegurarse de que la información almacenada en el sistema no sea alterada utilizando aplicaciones de software externas. (Gad, 2009)

Se refiere principalmente a la prevención del acceso no autorizado al equipo físico que conforma la red de trabajo, o a los sistemas conectados a él.

El activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la Seguridad Lógica.

A continuación se plantean algunos objetivos:

1. Restringir el acceso a los programas y archivos.
2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
3. Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.
4. Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
5. Que la información recibida sea la misma que ha sido transmitida.
6. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
7. Que se disponga de pasos alternativos de emergencia para la transmisión de información.

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."

Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no está permitido debe estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica. (Borghello, 2009)

2.3.1 Acceso

El control de acceso se refiere al tipo de autorización que se les concede a los usuarios, o sea, que tanto pueden los usuarios hacer dentro del sistema. La autorización es considerada el siguiente paso de la seguridad lógica inmediatamente después de la autenticación para entrar al sistema de información. La autenticación acredita la identidad del usuario para el sistema, con la adecuada identificación, autorización y control de acceso, un sistema podrá controlar adecuadamente el acceso a los recursos con el fin de prevenir el acceso no autorizado. (Stewart, 2011)

Los tres métodos más comunes en el control de acceso son:

- Control de acceso obligatorio.
- Control de acceso discreto.
- Control de acceso basado en reglas.

Estos son los tres métodos utilizados hoy en día en los sistemas de **TI.**

Así mismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso. Al respecto, el *National Institute for Standars and Technology* (NIST) ha resumido los siguientes estándares de seguridad que se refieren a los requisitos mínimos de seguridad en cualquier sistema:

- **Identificación y Autentificación**
  Se denomina Identificación al momento en que el usuario se da a conocer en el sistema; y Autenticación a la verificación que realiza el sistema sobre esta identificación.

- **Roles**

  El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso. Algunos ejemplos de roles serían los siguientes: programador, líder de proyecto, gerente de un área usuaria, administrador del sistema, etc. En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios.

- **Transacciones**

  También pueden implementarse controles a través de las transacciones, por ejemplo solicitando una clave al requerir el procesamiento de una transacción determinada.

- **Limitaciones a los Servicios.**

  Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema. Podría ser que en la organización se disponga de licencias para la utilización simultánea de un determinado producto de software para cinco personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario.

- **Modalidad de Acceso.**

  Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información. Esta modalidad puede ser: lectura, escritura, ejecución, borrado, creación y búsqueda.

- **Ubicación y Horario.**

  El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas.
  En cuanto a los horarios, este tipo de controles permite limitar el acceso de los usuarios a determinadas horas de día o a determinados días de la semana.

- **Control de Acceso Interno**. El control de acceso interno generalmente es para la autenticación del usuario por medio de passwords, listas de control de acceso, etiquetas de seguridad, etc…
- **Control de Acceso Externo**.

  Una vez establecidos los controles de acceso sobre los sistemas y la aplicación, es necesario realizar una eficiente administración de estas medidas de seguridad lógica, lo que involucra la implementación, seguimientos, pruebas y modificaciones sobre los accesos de los usuarios de los sistemas. (Borghello, 2009)

2.3.2 Canal

VPN

Las redes privadas virtuales son conocidas como VPN (Virtual Private Network), los datos que viajan a través de una VPN son datos encriptados y solo pueden ser descifrados por el destinatario y por supuesto el emisor, de este modo no quedan a la expuestos a la captación fraudulenta durante la transmisión.

La tecnología VPN permite la conexión a una red local desde una localización remota, a través de otro tipo de red, como el internet.

Una aplicación muy usada en las instituciones en donde solo son accesibles algunos recursos dese equipos que se encuentran en su propia red local por motivos de seguridad. Para permitir el acceso desde afuera se necesita una VPN, lo que registrará nuestro equipo como perteneciente a una red local y permitirá su acceso

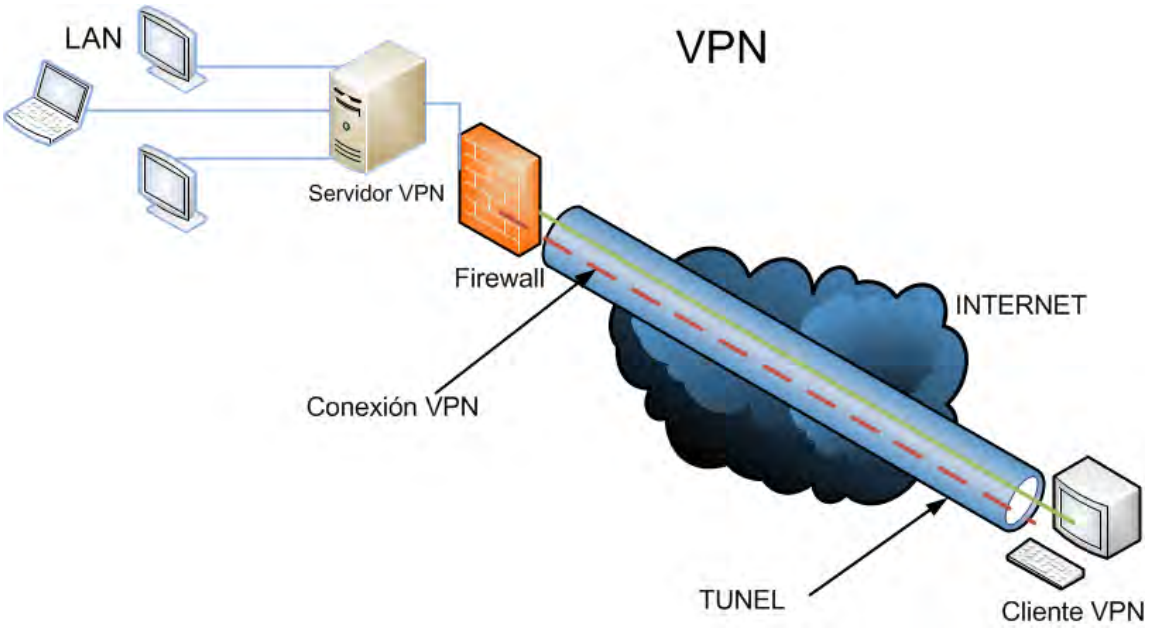


Ilustración 2 - VPN

2.3.3 Perímetro

El perímetro de la red es la línea que separa todo lo que está dentro de la red tanto físico como lógico de lo que se encuentra fuera de la red.

A pesar de que las organizaciones poseen grandes barreras físicas para proteger su perímetro, con la implementación del internet en sus sistemas de información han tenido que enfrentarse a otro tipo de protección perimetral con la entrada y salida de información hacia el ciberespacio, por lo que ahora en vez de utilizar cercas electrificadas, sensores de movimiento, cámara de circuito cerrado, etc. Es necesario implementar dispositivos de protección perimetral de la red tales como routers, firewalls, servidores proxies, ya que estos permiten establecer controles de seguridad así como políticas con la finalidad de proteger tanto física como lógica la red interna de una organización.

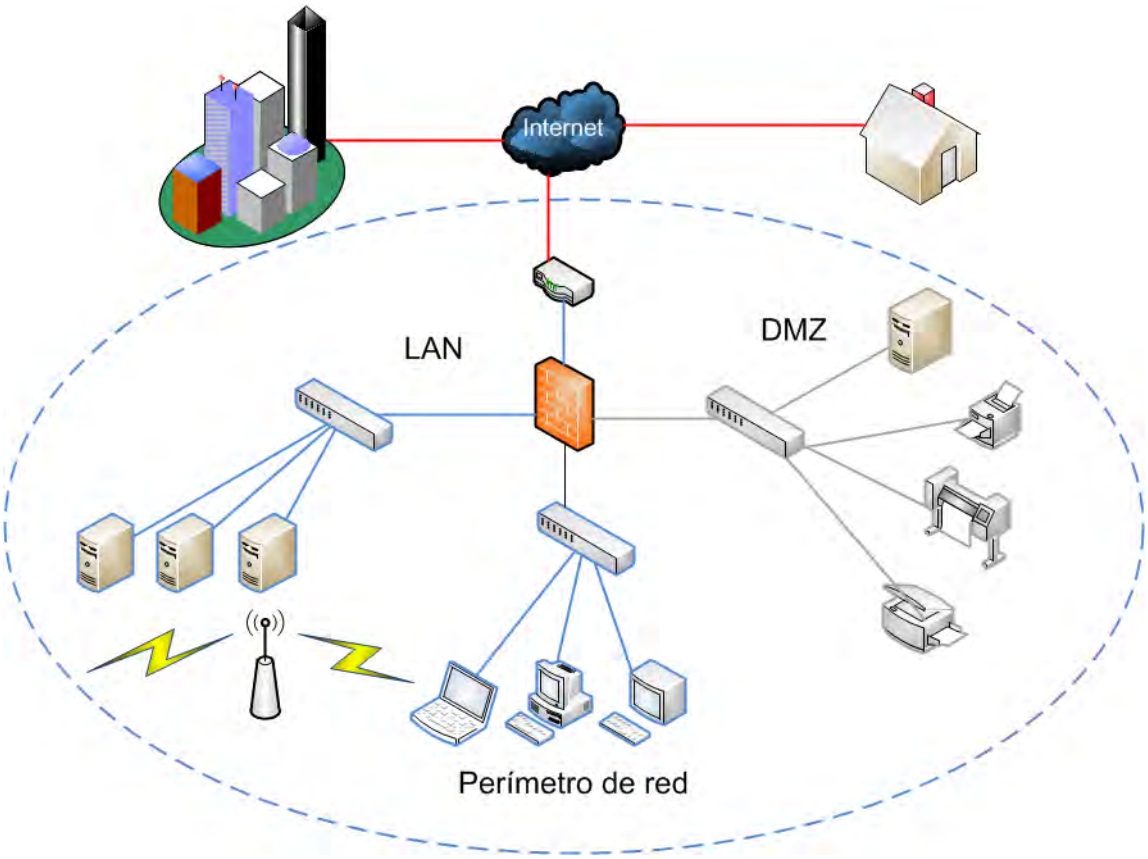


Ilustración 3 - Perímetro

2.3.3.1 DMZ (Zona Desmilitarizada).

En redes de computadoras una DMZ o Zona Desmilitarizada es un equipo host o una pequeña red de trabajo insertada como una “zona neutral”, entre la red privada de una empresa y la red pública, la DMZ evita que los usuarios externos tengan acceso directo a un servidor que tiene datos de la empresa.

La DMZ puede ser utilizada para los servidores que tienen que ser accesibles desde Internet o alguna otra red externa. La DMZ puede ser establecida entre dos routers, con un router interno conectado a la red protegida y un router externo conectado a la red no protegida, o ser simplemente un puerto adicional de un solo router. El firewall, ubicado entre las redes protegida y no protegida, se instala para permitir las conexiones requeridas (por ejemplo, HTTP) de las

redes externas (no confiables) a los servidores públicos en la DMZ. EL firewall sirve como protección primaria para todos los dispositivos en la DMZ. En el enfoque DMZ, el router provee protección filtrando algún tráfico, pero deja la mayoría de la protección a cargo del firewall. (Cisco networking Academy)

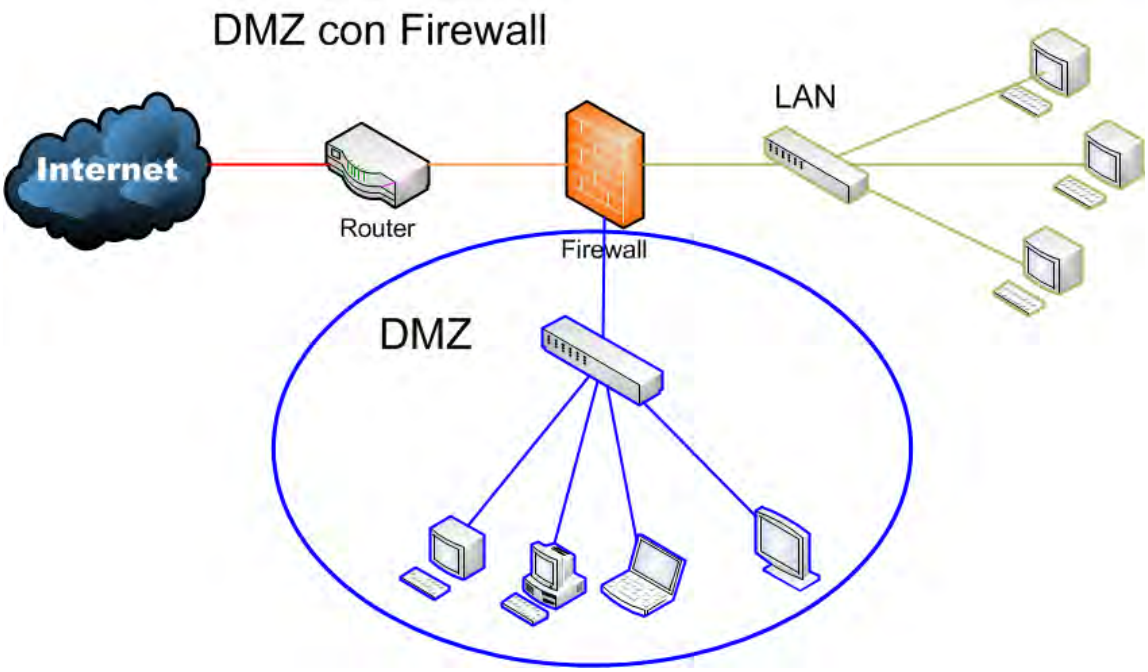


Ilustración 4 - DMZ

2.3.3.2 ACL (listas de Control de Acceso)

Una ACL es una lista secuencial de sentencias de permiso o denegación que se aplican a direcciones o protocolos de capa superior. Las ACL brindan una manera poderosa de controlar el tráfico de entrada o de salida de la red. Se puede configurar las ACL para todos los protocolos de red enrutados. El motivo más importante para configurar las ACL es brindar seguridad a la red.

La ACL es una configuración de router que controla si un router permite o deniega paquetes según el criterio encontrado en el encabezado del paquete. Las ACL también se utilizan para seleccionar los tipos de tráfico por analizar, reenviar o procesar.

USO DE LAS ACL

- Utilice las ACL en router firewalls entre su red interna y su re externa, como internet.
- En un router situado entre dos partes de la red a fin de controlar el tráfico que entra a sale de una parte específica de su red interna.
- Configure las ACL en routers de borde situados en los extremos de la red.
- Configure las ACL para cada protocolo de red configurado en las interfaces del router del borde.

Se puede configurar una ACL por protocolo, por dirección y por interfaz.

ACL por protocolo: Para controlar el tráfico de una interfaz, se debe definir una ACL para cada protocolo habilitado en la interfaz

ACL por dirección: Las ACL controlan el tráfico en una dirección a la vez de un interfaz. Deben crearse dos ACL por separado para controlar el tráfico entrante y saliente.

ACL por interfaz: las ACL controlan el tráfico de una interfaz, por ejemplo, FastEthernet0/0.

Las ACL realizan las siguientes tareas:

- Limitar el tráfico de red para mejorar el rendimiento de ésta.
- Brindar control de flujo de tráfico.
- Proporcionar un nivel básico de seguridad para el acceso a la red.
- Se debe decidir qué tipos de tráfico enviar o bloquear en las interfaces del router.
- Controlar las áreas de la red a las que puede acceder un cliente.
- Analizar los hosts para permitir o denegar su acceso a los servicios de red.

Tipos de ACLs.

Las ACLs se clasifican según el número utilizado en access-list (número) y que están definidos en:

Protocolo	Intervalo
Estandar IP	1-99
Extended IP	100-199
AppleTalk	600-699
IPX	800-899
Extended IPX	900-999
IPX Service Advertising Protocol	1000-1099

Tabla 1 - Tipos de ACLs

Al asignar un ACL a una interfaz, se debe especificar la ubicación entrante o saliente. Un alista de acceso entrante filtra el tráfico que entra por una interfaz y la lista de acceso saliente filtra el tráfico que sale por una interfaz.

Una lista de acose no puede ser modificada, se debe borrar mediante un comando y entonces proceder a recrearla.

Finalmente, también muy importante, la última línea de una lista de acceso nunca aparece, es decir existe de forma implícita y siempre denegará todo.

En la tabla siguiente se muestra un ejemplo de una lista de acceso

```
Router(config)# Access-list 4 deny 192.168.1.4
Router(config)# Access-list 4 permit 192.168.1.0
0.0.0.255
Router(config)# interface e1
Router(config)# ip access-group41in
```

Tabla 2 - Lista de acceso

ACLs dinámicas

Las ACLs dinámicas, también denominadas “Lock and Key Security” (Seguridad bloqueo y clave), tratan la ACL como un proceso de autenticación de usuarios. En lugar de comenzar tratando de conectar con el servidor, el usuario debe hacer primero telnet a un router. El router le pregunta la combinación nombre de usuario y contraseña. Si es auténtico, el router cambia dinámicamente su ACL, permitiendo tráfico desde la dirección IP del host que acaba de enviar los

paquetes de autenticación. Después de un periodo de inactividad, el router borra la entrada dinámica en la ACL, cerrando el potencial agujero de seguridad.

ACL dinámica	
Paso 1	El usuario se conecta con el router por medio de telnet.
Paso 2	El usuario proporciona un nombre de usuario y contraseña que el router compara con una lista, autenticando al usuario.
Paso 3	Después de la autenticación, el router añade dinámicamente una entrada al comienzo de la ACL, permitiendo tráfico originado en el host autenticado.
Paso 4	Los paquetes enviados por el host permitido pasan a través del router hacia el servidor.

Tabla 3 - ACL Dinámica

Diagrama del funcionamiento de la ACL dinámica.

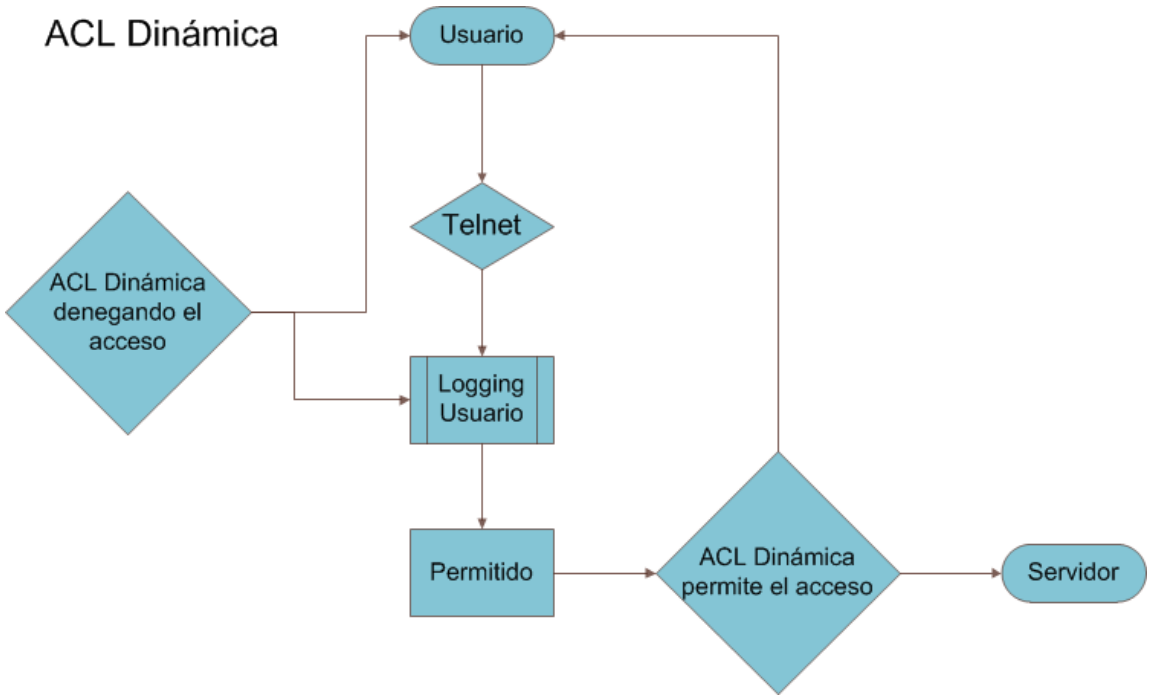


Ilustración 5 - Acl Dinámica

2.3.3.3 Firewall (Cortafuegos)

Un firewall es un guardia de seguridad situado entre el punto de entrada de una red privada e internet, por lo que todos los paquetes de entrada y salida tienen que pasar a través de él. (Liu, 2011)

En general un Firewall es cualquier hardware, software o la combinación de ambos que puede filtrar la transmisión de información digital en su intento de pasar a través de una interfaz entre dos redes. (Michael E. Whitman H. J., 2012)

Los firewalls realizar dos funciones básicas de seguridad:

- **Filtrado de paquetes** Determina si permite a deniega el paso de información digital, basado en las políticas de seguridad establecidas.
- **Aplicación Proxy,** proporciona servicios de red a usuarios mientras que protege a los host individuales, esto lo hace dividiendo el tráfico en las IP.

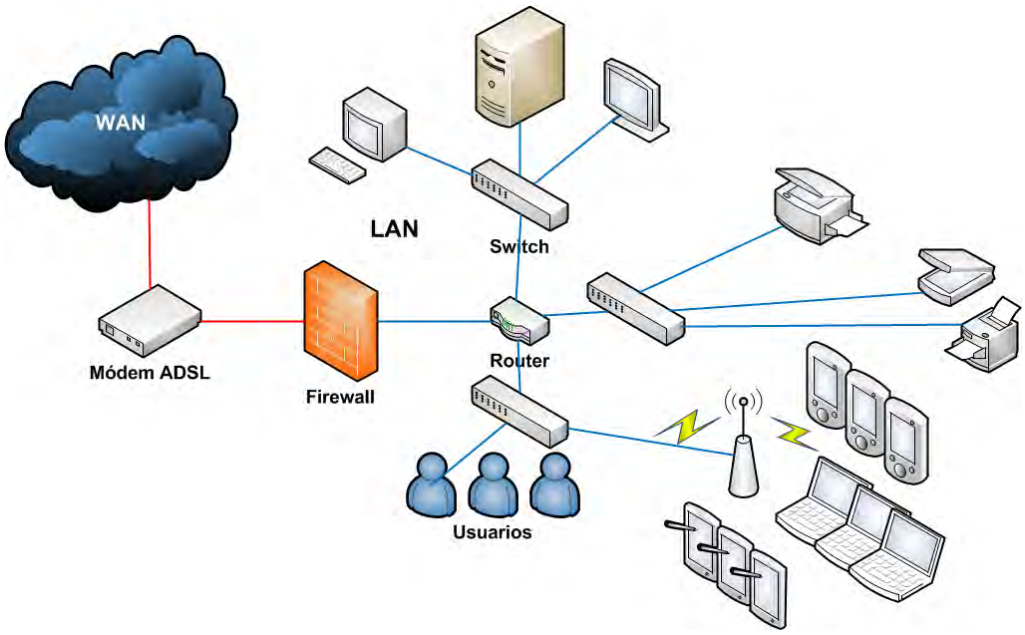


Ilustración 6 - Firewall

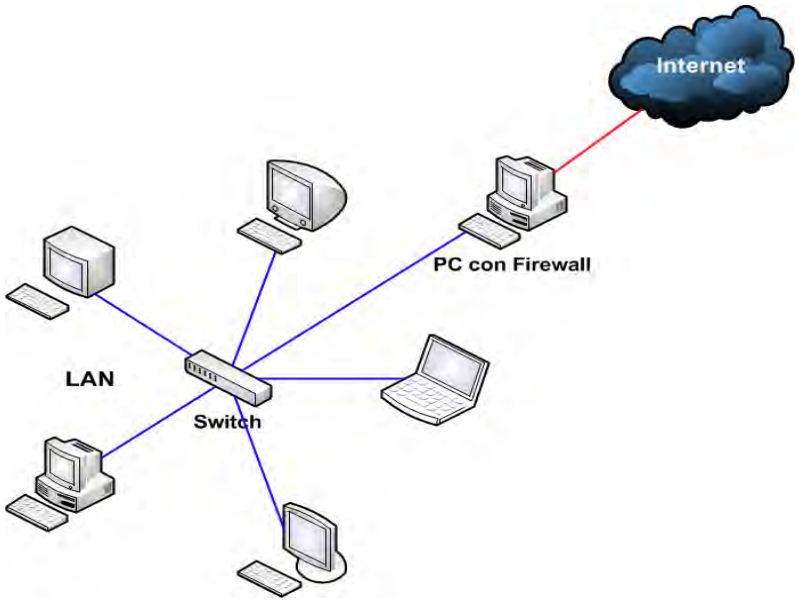


Ilustración 7 - Ilustración de un esquema con Firewall de Software.

Tipos de Firewall

Por su arquitectura o manera de implementación los firewalls se pueden clasificar de la siguiente manera:

Tipo de Firewall	Descripción
Filtrado de paquetes, Screening Router o de capa de red.	Trabaja a nivel de capa de transporte y de red del modelo OSI y se encuentran conectados en ambos perímetros de las red
Proxy-Gateway o de capa de aplicación	Trabaja a nivel de capa de aplicación del modelo OSI, puede implementar filtrados específicos aprovechando las características del protocolo de este nivel
Dual Homed Host	Consiste en un único equipo que implementa filtrado tanto a nivel de red como de aplicación, mediante el

	uso de dos interfaces conectadas lógica y físicamente a ambos segmentos de red distintos (la red interna o privada y la re externa).
Screened host	Es la combinación de los dos anteriores. Primero se filtran paquetes mediante el router y en la segunda se sitúa el host bastión un reducido número de servicios publicados hacia el exterior.
Screened Subnet	Más conocida como DMZ (zona desmilitarizada) es la más utilizada ya que incrementa el nivel de seguridad, agregando una subred intermedia entre las redes externa e interna.
Personal	Se instala como software en computadora, donde se filtran las comunicaciones entre dicha computadora y el resto de la red.

Tabla 4 - Tipos de firewall

2.3.3.4 Proxy

Un servidor proxy es un equipo intermediario situado entre el sistema del usuario e Internet. Puede utilizarse para registrar el uso de Internet y también para bloquear el acceso a una sede Web. El servidor de seguridad del servidor proxy bloquea algunas sedes o páginas Web por diversas razones. (Oracle)

El servidor Proxy, se utiliza especialmente en el ámbito del tráfico HTTP, o incluso con FTP en la red LAN (Red de área local) e internet. Se considera un complemento del firewall (cortafuegos). (DORDOIGNE, 2011)

Cuando intercepta una petición hacia el exterior, el proxy la dirige como si fuera suya y a continuación almacena los datos recibidos. Seguidamente los envía al solicitante inicial. En primer lugar, camufla las direcciones IP internas, puesto que la petición no llega a internet. Y luego permite filtrar para, por ejemplo, prohibir el acceso a algunos sitios web.

Otra de las funciones del servidor proxy es administrar la memoria caché. Así es posible volver a pedir un archivo o sitio de internet, a nivel de web.

Tipos de Servidores proxy:

Proxy	Descripción
Proxy transparente	Un proxy transparente combina un servidor proxy con NAT (Network Address Translation) de manera que las conexiones son enrutadas dentro del proxy sin configuración por parte del cliente, y habitualmente sin que el propio cliente conozca de su existencia. Es utilizado por proveedores de servicios de internet (ISP).
Reverse Proxy	Un reverse proxy es un servidor proxy instalado en el domicilio de uno o más servidores web. Todo el tráfico entrante de Internet y con el destino de uno de estos servidores web pasa a través del servidor proxy.
Proxy NAT	Traducción de direcciones de red (NAT, Network Address Translation) también es conocida como enmascaramiento de IPs. Es una

	técnica mediante la cual las direcciones fuente o destino de los paquetes IP son reescritas, sustituidas por otras (de ahí el "enmascaramiento").
Proxy Abierto	Este tipo de proxy acepta peticiones desde cualquier ordenador, esté o no conectado a su red.
Cross-Domain Proxy	Típicamente usado para Tecnologías Web asíncronas (flash, ajax, comete, etc) que tienen restricciones para establecer una comunicación entre elementos localizados en diferentes dominios.

Tabla 5 - Servidores Proxy

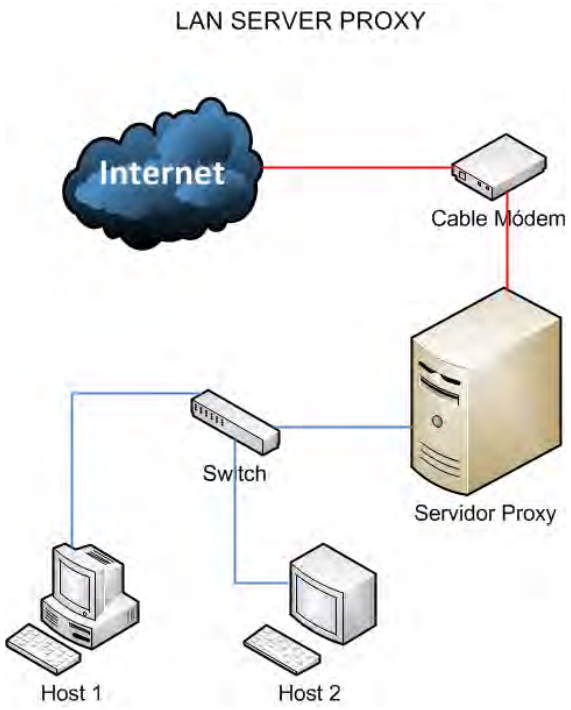


Ilustración 8 - Entorno de Rede con Servidor Proxy

2.3.3.5 Honeypot

Los Honeypots son sistemas llamados trampas diseñados para atraer atacantes potenciales y poder aislarlos del sistema de información. (Michael E. Whitman H. J., 2012)

En la industria son conocidos como señuelos, trampas atrayentes o trampas para moscas, de ahí el nombre "tarro de miel". Cuando una colección de honeypots está conectada a varios sistemas de honeypot o a una subred, esto el llamado "**honeynet".** Un honeypot contiene servicios que emulan a otros servicios muy comunes en los sistemas de información, pero que están configurados de tal manera que hacen ver vulnerable al sistema ante los atacantes potenciales. Esto con la finalidad de atraer a los atacantes potenciales a cometer un ataque al sistema y así poder defender mejor el sistema de posibles ataques en el futuro.

Ventajas de los Honeypots

Los Honeypots tienen varios beneficios debido a su simplicidad:

• Los honeypots pueden recoger pequeñas cantidades de datos, pero los datos recogidos son de gran valor informativo. Por lo tanto, estas pequeñas cantidades de datos son más fáciles de ser analizadas.

• Están diseñados de tal manera que pueden atrapar todo tipo de tácticas y herramientas lanzadas en contra de ellos.

• Los Honeypots funcionas bien en todas las redes encriptadas e IPv6 a diferencia de la mayoría de las otras tecnologías de seguridad.

• Son un concepto simple que contribuye a un menor número de errores de configuración en la tecnología.

Desventajas de los Honeypots

Todos los tipos de tecnologías tienen debilidades; Honeypot no es una excepción a este simple hecho, así que aquí están algunos de sus inconvenientes:

• El uso de Honeypot se limita sólo a las amenazas que interactúan directamente con él y no atrapar a los ataques contra otros sistemas.

• Tiene el riesgo de ser tomado por el atacante de dañar otros sistemas. El nivel de riesgo puede ser demasiado bajo o demasiado alto, dependiendo sobre la especie de trampa utilizada.

Tipos de Honeypots.

	Honeypots	**Descripción**
Honeypots de baja interacción	Specter “Intrusion Detection System”	honeypot inteligente basado en sistemas de detección de intrusos, vulnerables y atractivos a los atacantes, este sistema proporciona servicios como PHP,SMTP,FTP, POP3, HTTP, y TELNET que atraen fácilmente a los atacantes, pero en realidad son trampas que pretenden recolectar información.
	Honeyd	Crea host virtuales en la Red. Los anfitriones pueden ser configurados para ejecutar servicios arbitrarios y su personalidad puede ser adaptada de modo que parezcan estar ejecutando ciertos sistemas operativos.

	KFSensor	honeypot de windows basado en sistema de detección de intrusos (IDS), actúa para atraer y detectar piratas informáticos y gusanos, vulnerables mediante la situación de los servicios del sistema y troyanos.
	PatriotBox	Usa como señuelo el sistema de detección de intrusos (IDS), en entornos de red empresarial de forma efectiva la detección temprana de las amenazas de intrusos.
Honeypots de alta interacción	HoneyNet :	Proporciona un medio real de los sistemas, aplicaciones y servicios para interactuar con los atacantes, en otras palabras un HoneyNet es un conjunto de Honeypots.
	ManTrap	Puede crear “sotfware jaula” y similar una red virtual de una máquina. para ello emula una variedad de diferentes maquinas (FTP,HTTP,SMTP,ODBC) en una sola ManTrap de acogida.

Tabla 6 - Honeypots

En las instituciones y las universidades los investigadores especializados en Honeypots han identificado tres zonas referentes para implementar los sistemas trampa.

1. Delante el Firewall

Al colocarlo delante del Firewall, hace que la seguridad de nuestra red interna no se vea comprometida en ningún momento ya que nuestro Firewall evitará que el ataque vaya a nuestra red interna.

Las dificultades al usar este método son:

- El ancho de banda que se consumiría, ya que al estar en el exterior del Firewall no habrá dificultad en acceder a él.

A él estar fuera de nuestro Firewall, no podremos controlar los ataques internos.

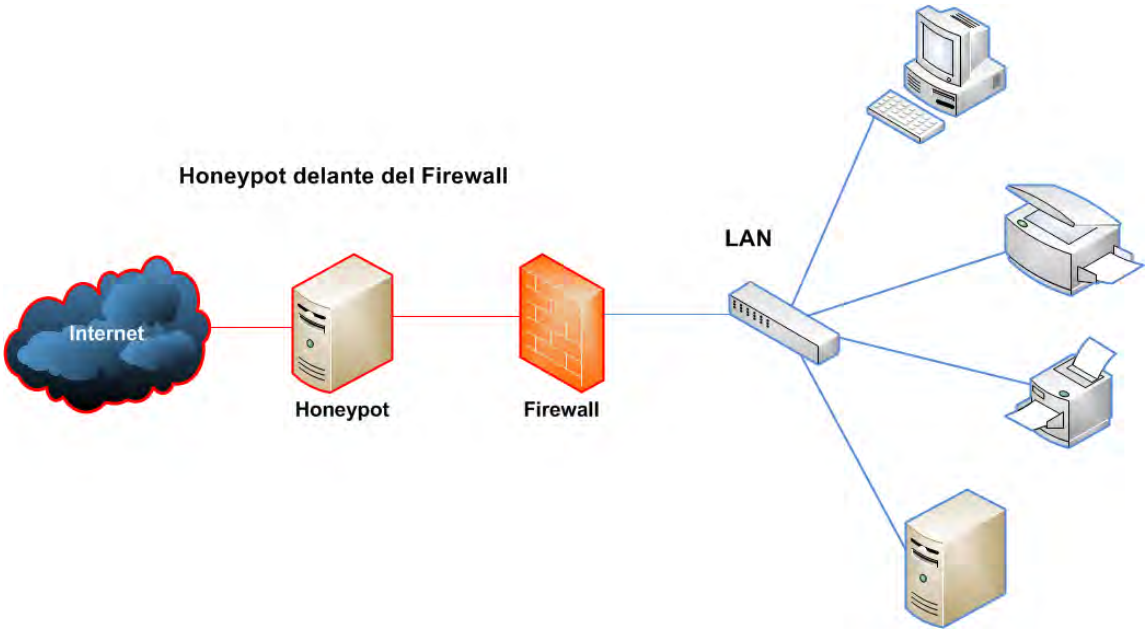


Ilustración 9 - Honeypot Delante del Firewall

2. Detrás del Firewall

Esta opción nos permite el control de los ataques internos y externos de cualquier tipo, el principal problema que presenta este método es que requiere una configuración específica para dejar el acceso al Honeypot pero no a nuestra red. Lo cual provoca posibles fallos de seguridad en la filtración de tráfico.

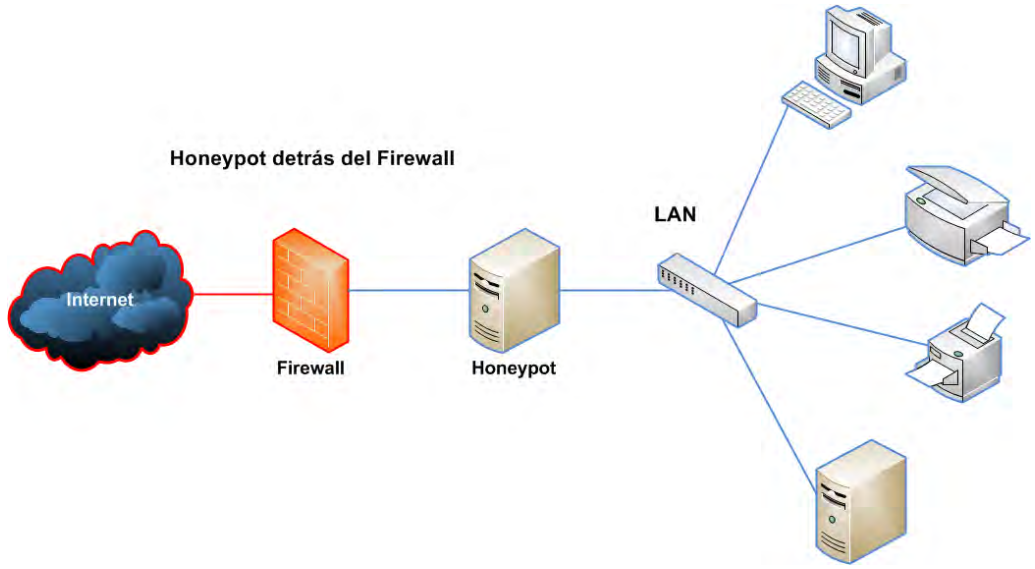


Ilustración 10 - Honeypot detrás del Firewall

3. En una zona desmilitarizada

Al posicionarlo aquí se hace posible la separación del Honeypot de la red interna y la unión con los servidores, esta posibilidad nos permite detectar tanto ataques internos como externos con una pequeña modificación del Firewall.

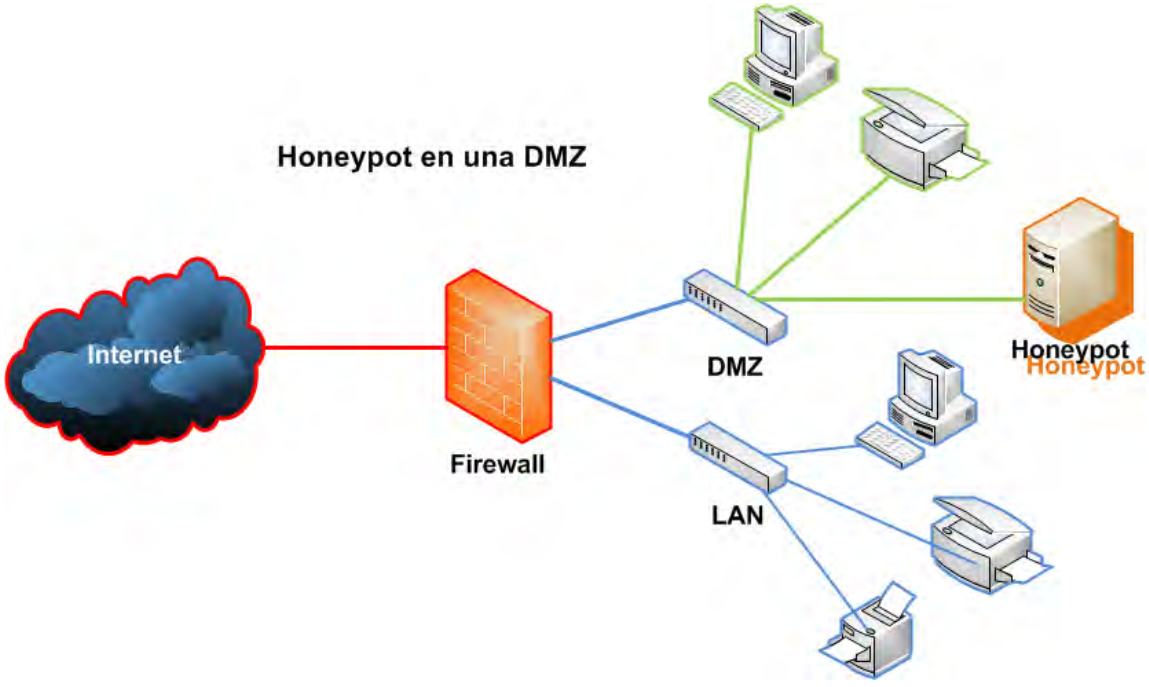


Ilustración 11 - Honeypot en una DMZ

Los honeypots no sustituyen a las tecnologías actuales, sino más bien trabajan en conjunto para el apoyo a las tecnologías existentes.

2.4 Tipos de ataques

Un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización.

Para minimizar el impacto negativo provocado por ataques, existen procedimientos y mejores prácticas que facilitan la lucha contra las actividades delictivas y reducen notablemente el campo de acción de los ataques.

Uno de los pasos más importantes en seguridad, es la educación. Comprender cuáles son riesgos asociados, permitirá conocer de qué manera se ataca un sistema informático ayudando a estrategias de seguridad efectivas.

Conocer las diferentes etapas que conforman un ataque informático brinda la ventaja de aprender a pensar como los atacantes y a jamás subestimar su mentalidad. Desde la perspectiva del profesional de seguridad, se debe aprovechar esas habilidades para comprender y analizar la forma en que los atacantes llevan a cabo un ataque.

La siguiente imagen muestra las cinco etapas por las cuales suele pasar un ataque informático al momento de ser ejecutado:

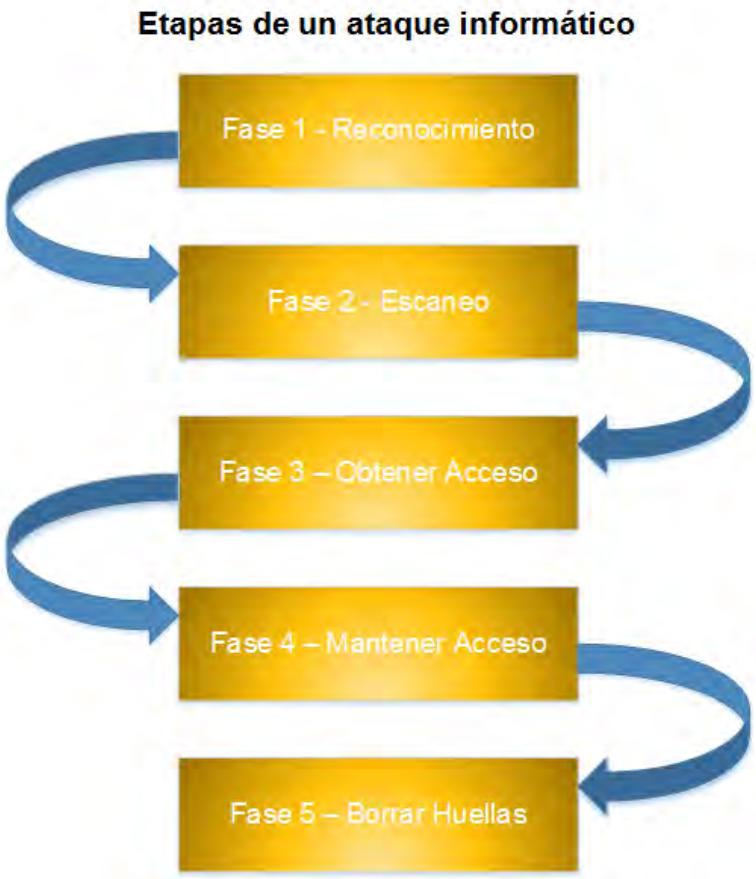


Ilustración 12 - Etapas de un ataque

Fase 1: Reconocimiento.

Esta etapa involucra la obtención de información con respecto a una víctima potencial que puede ser una persona u organización.

Por lo general, durante esta fase se recurre a diferentes recursos de Internet como Google, entre tantos otros, para recolectar datos del objetivo. Algunas de las técnicas utilizadas en este primer paso son la Ingeniería Social, el Dumpster Diving, el sniffing.

Fase 2: Exploración.

En esta segunda etapa se utiliza la información obtenida en la fase 1 para sondear el blanco y tratar de obtener información sobre la víctima como direcciones IP, nombres de host, datos de autenticación, entre otros.

Fase 3: Obtener acceso.

En esta instancia comienza a materializarse el ataque a través de la explotación de las vulnerabilidades y defectos del sistema (Flaw exploitation) descubiertos durante las fases de reconocimiento y exploración.

Algunas de las técnicas que el atacante puede utilizar son ataques de Buffer Overflow, de Denial of Service (DoS), Distributed Denial of Service (DDos), Password filtering y Session hijacking.

Fase 4: Mantener el acceso.

Una vez que el atacante ha conseguido acceder al sistema, buscará implantar herramientas que le permitan volver a acceder en el futuro desde cualquier lugar donde tenga acceso a Internet. Para ello, suelen recurrir a utilidades backdoors, rootkits y troyanos.

Fase 5: Borrar huellas.

Una vez que el atacante logró obtener y mantener el acceso al sistema, intentará borrar todas las huellas que fue dejando durante la intrusión para evitar ser detectado por el profesional de seguridad o los administradores de la red. En consecuencia, buscará eliminar los archivos de registro (log) o alarmas del Sistema de Detección de Intrusos (IDS).

Entre las herramientas que un atacante puede emplear durante la exploración se encuentra el network mappers, port mappers, network scanners, port scanners, y vulnerability scanners.

A continuación se enlistan algunos de los ataques informáticos más comunes:

Ingeniería Social

Es la práctica para obtener datos confidenciales a través de la manipulación psicológica de usuarios legítimos. La técnica se puede utilizar para conseguir información, acceso o privilegios en sistemas, que permitan realizar algún acto

que perjudique o exponga a una persona o empresa a riesgos y abusos. En la práctica se utiliza teléfono o internet para engañar a la gente simulando, por ejemplo, ser el empleado de un banco de una empresa, un compañero de trabajo, un técnico o un cliente y , así obtener información. A través de internet suele enviarse solicitudes para renovar credenciales de acceso a sitios, e-mails falsos que piden respuestas e, incluso, las famosas cadenas, que llevan a revelar información sensible o a violar políticas de seguridad.

Phishing

Denota un uso de la ingeniería social para intentar adquirir información confidencial, por ejemplo, contraseñas, cuentas bancarias, datos de tarjetas, etcétera, de manera fraudulenta. El accionar del phishing es simple, ya que se hace pasar por una persona o identidad de confianza (por e-mail, SMS, mensajería instantánea o páginas web) imitando el formato, el lenguaje y la imagen de entidades bancarias o también corporaciones financieras.

En un leguaje más coloquial, el término deriva de la palabra inglesa fishing (pesca), haciendo referencia al hecho de pescar contraseña e información de los usuarios. (Jara, 2009)

Trashing (Cartoneo)

Generalmente, un usuario anota su login y password en un papelito y luego, cuando lo recuerda, lo arroja a la basura. Este procedimiento por más inocente que parezca es el que puede aprovechar un atacante para hacerse de una llave para entrar el sistema..."nada se destruye, todo se transforma".

El Trashing puede ser físico como el caso descrito o lógico, como analizar buffers de impresora y memoria, bloques de discos, etc.

El Trashing físico suele ser común en organizaciones que no disponen de alta confidencialidad, como colegios y universidades

Ataques de Monitorización

Este tipo de ataque se realiza para observar a la victima y su sistema, con el objetivo de establecer sus vulnerabilidades y posibles formas de acceso futuro.

- **Shoulder Surfing**

  Consiste en espiar físicamente a los usuarios para obtener el login y su password correspondiente. El Surfing explota el error de los usuarios de dejar su login y password anotadas cerca de la computadora (generalmente en post–it adheridos al monitor o teclado).

- **Decoy (Señuelos)**

  Los Decoy son programas diseñados con la misma interface que otro original. En ellos se imita la solicitud de un logeo y el usuario desprevenido lo hace, luego el programa guardará esta información y dará paso a las actividades normales del sistema.

- **Scanning (Búsqueda)**

  El Scaneo, como método de descubrir canales de comunicación susceptibles de ser explotados, lleva en uso mucho tiempo. La idea es recorrer (scanear) tantos puertos de escucha como sea posible, y guardar información de aquellos que sean receptivos o de utilidad para cada necesidad en particular.

Ataques de Autenticación

Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y password.

- **Spoofing-Looping**

Puede traducirse como "hacerse pasar por otro" y el objetivo de esta técnica, justamente, es actuar en nombre de otros usuarios, usualmente para realizar tareas de Snooping o Tampering.

- **Spoofing**

  Este tipo de ataques (sobre protolocos) suele implicar un buen conocimiento del protocolo en el que se va a basar el ataque. Los ataques tipo Spoofing bastante conocidos son el IP Spoofing, el DNS Spoofing y el Web Spoofing.

- **Uso de Diccionarios**

  Los Diccionarios son archivos con millones de palabras, las cuales pueden ser posibles passwords de los usuarios. Este archivo es utilizado para descubrir dicha password en pruebas de fuerza bruta.

Denial of Service (DoS)

- **Por inundación**

  Se basan en consumir total o parcialmente el ancho de banda de l entorno de la víctima. Es quizás, la técnica **DoS** más simple.

  Si el atacante tiene una línea de conexión a internet que le permite enviar datos a 2Mbps, el atacante podrá, fácilmente enviar un flujo continuo de datos basura a la víctima, llenando su caudal de la recepción de 1 Mbps. Mientras dure la inundación, la víctima no será capaz de recibir ni responder a las peticiones de servicio de sus clientes.

- **Ataques por inundación de segmentos SYN**

  Son una forma evolucionada del ataque de inundación. En este caso, el flujo de datos enviados por el atacante tiene la finalidad de consumir la memoria del servidor, además de su ancho de banda.

Ataques Smurf.

Consiste en utilizar determinados recursos dentro de internet para amplificar la inundación original hacia la víctima. El Smurf no es más que un ataque de inundación por consumición de ancho de banda de la máquina de la víctima, pero ampliado. (AREITIO J, 2008)

“El principal engaño empieza por las propias tropas, para hacer que le sigan a uno sin saber a dónde van.”

Sun Tsu, El arte de la guerra. Siglo V a. C.

3. CONCLUSIONES

La realización de este trabajo de investigación sobre la estructura de un sistema de seguridad en redes corporativas, es con la finalidad de ayudar a conocer de manera básica la estructura y el funcionamiento del sistema de seguridad, ya que para que un administrador de red pueda implementar un sistema de que realmente le funcione a un porcentaje alto, es necesario que tenga el conocimiento de las distintas partes que lo conforman (dispositivos, software, hardware etc.).

Es importante mencionar que, cualquiera que sea la capacidad y el presupuesto que se tenga en la empresa ó lugar donde esté protegiendo la información, siempre será blanco de ataques por parte de externos, usuarios, administrativos etc. por lo que una de las mejores herramientas para la seguridad de nuestra información, siempre será la educación, cultura y sobre todo el conocimiento que se tenga del personal que tiene acceso a nuestra red en la empresa o de manera remota ya que los atacante buscan vulnerabilidades para sacar provecho a su favor.

En México y sobre todo en nuestra ciudad, en la mayoría de las empresas y dependencias gubernamentales, se carece de departamentos de recursos humanos especializados en Seguridad informática y en muchos casos hasta de administradores de red que cuenten con el conocimiento necesario para el entendimiento de la seguridad, por lo que es necesario crear herramientas de apoyo como el caso de este documento para ayudar a crear una cultura sólida en la cuestión de seguridad informática.

El principal problema de la deficiencia en los departamentos de informática en todos los casos (seguridad, conexión, ancho de banda etc.) viene del departamento de administración de las empresas, ya que no consideran los recursos necesarios para la compra del equipo adecuado y sobre todo actualizado, así como la contratación del personal calificado para operarlo, por lo que sería de suma importancia que las empresas les proporcionaran este tipo

de información y le puedan dar la importancia que se le debe de dar a la protección de la información de la cual depende la empresa.

4. BIBLIOGRAFÍA

Latinoamérica, E. (2014). *www.eset-la.com .* Retrieved 16 de 07 de 2014 from http://www.eset-la.com/centro-prensa/articulo/2014/codigos-maliciosos-secuestran-informacion-tambien-android/3537

Carroll, L. (n.d.). *Alice's Adventures in Wonderland.* Retrieved 1995 йил 10-febrero from http://www.germany.eu.net/books/carroll/alice.html

Cisco networking Academy. (n.d.). *Implementing Network Security.* Retrieved 28 de Julio de 2012 from http://www.cisco.com/web/learning/netacad/index.html

Liu, A. X. (2011). *Firewall Design and Analysis.* USA: World Scientific.

Stewart, J. M. (2011). *CompTIA Security+ Review Guide.* Indianapolis: Wiley.

Symantec. (2014). *www.symantec.com.* Retrieved 2014 from http://www.symantec.com/es/mx/security_response/publications/threatreport.jsp

Symantec. (2014). *www.symantec.com.* Retrieved 2014 from http://www.symantec.com/es/mx/security_response/publications/threatreport.jsp

Solomos, K., & Avouris, N. (1999). Learning From Multiple Collaborating Intelligent Tutors: An Agent-Based Approach. *10* (3.4).

Vieites, Á. G. (2007). *Enciclopedia de la Seguridad Informática.* México D.F.: Alfaomega.

Alfonso Garcia-Cerevignon Hurtado, M. d. (2011). *Seguridad informática.* Madrid España: PARANINFO.

Acissi. (2011). *SEGURIDAD INFORMATICA. ETHICAL HACKING. CONOCER EL ATAQUE SI.* Barcelona: Arnau oncins rodríguez.

Ballard, D. a. (1982). *Computer vision.* Englewood Cliffs. : Prentice-Hall Inc. .

Borghello, C. (2009). *Segu-info.* Retrieved 28 de julio de 2012 from http://www.segu-info.com.ar/logica/seguridadlogica.htm

DORDOIGNE, J. (2011). *REDES INFORMATICAS. NOCIONES FUNDAMENTALES.* Barcelona: ENI.

Elmaleh, F. (2011). *Expert IT La seguridad en Windows 7.* Barcelona: ENI.

Harwood, M. (2009). *CompTIA Network+ N10-004 Exam Prep.* United States of America: Pearson Education.

Gad, S. C. (2009). *Clinical Trials Handbook.* new Yersey: Wiley.

Grupo IWI. (2009). *Implantación de LOPD en la empresa. Medidas de seguridad.* Málaga: Vértice.

Mattord, M. E. (2010). *Management of Information Security.* Boston: Cengage Learning.

Michael E. Whitman, H. J. (2012). *Guide to Firewalls & VPNs.* Boston MA.: Cengage Learning.

Michael E. Whitman, H. J. (2012). *Principles of Information Security.* Boston, MA: CENGAGE, Learning.

Mieres, J. (Enero de 2009). *www.evilfingers.com.* Retrieved 26 de Julio de 2012 from https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf

Oracle. (n.d.). *Java - Faq.* Retrieved 29 de Julio de 2012 from http://www.java.com/es/download/help/proxy_server.xml

Quiroz, L. G. (1996). *Informática y auditoría para las ciencias empresariales.* Bogotá: UNAB.

Ramos, M. d. (2010). *SISTEMAS OPERATIVOS MONOPUESTO.* Madrid: Paraninfo.