UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

"ANALISIS DE LA TECNICA TAMPERING O DATA DIDDLING PARA LA EMPRESA COMPUSOLUTIONS"

Estudiante

Marco Antonio Marín D.

Tutor

Ing. Marco Lituma

Quito – Ecuador

2011

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

CERTIFICADO DE RESPONSABILIDAD

Yo, Ing. Marco Lituma, certifico que el señor Marco Marín D. con C.C, N° 010529403-7 realizo la presente tesis con el título “Análisis de la Técnica Tampering o Data Diddling para la empresa CompuSolutions”, y que es autor intelectual del mismo, que es original, auténtico y personal.

_____

Ing. Marco Lituma

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

ACTA DE CESION DE DERECHOS

Yo, Marco Antonio Marín Duchi, declaro conocer y aceptar la disposición de la Normativa de la Universidad Tecnológica Israel que en su parte pertinente textualmente dice: “Forma parte del Patrimonio de la Universidad la propiedad intelectual de las investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través, o con el apoyo financiero, académico o institucional (operativo) de la Universidad”.

Cuenca, Noviembre del 2011

_____

Marco Antonio Marín Duchi

C.I: 010529403-7

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

CERTIFICADO DE AUTORÍA

El documento del Trabajo de Titulación con título “Análisis de la Técnica Tampering o Data Diddling para la empresa CompuSolutions”, ha sido desarrollado por Marco Marín D con C.C. N° 010529403-7 persona que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de cada uno de los productos de este Trabajo sin previa autorización.

_____

Marco Antonio Marín Duchi

0105294037

DEDICATORIA

El siguiente trabajo está dedicado principalmente a mi Señor, Jesús, quien me dio la fe, la fortaleza, la salud y la esperanza para terminar este trabajo, a mi familia en especial a mi madre y padre que con esfuerzo, tolerancia, sacrificio, amor y dedicación, me han apoyado día a día para que este trabajo llegue a su fin. Y también lo dedico de forma muy especial a mis compañeros y profesores que compartieron todos estos años brindándome sus conocimientos y más aun su inmensa amistad.

AGRADECIMIENTO

A mis padres, Cecilia Duchi y Marco Marín, que siempre me han dado su apoyo incondicional y a quienes debo este triunfo profesional, por todo su trabajo y dedicación para darme una formación académica y sobre todo humanista y espiritual. De ellos es este triunfo y para ellos es todo mi agradecimiento.

También al docente tutor: Ing. Marco Lituma, por ayudarme en el desarrollo de mi trabajo que con sus conocimientos asieron posible todo esto y además a los profesores de la Universidad Israel quienes me brindaron sus conocimientos, amistad y apoyo durante todo mi proceso académico.

RESUMEN

Debido a que el uso de Internet se encuentra en aumento, cada vez más empresas u hogares permiten a sus proveedores, empleados, o personas acceder a sus sistemas de información. Por lo tanto, es fundamental saber qué recursos necesitan protección para así controlar el acceso al sistema y los derechos de los usuarios del sistema de información. Los mismos procedimientos se aplican cuando se permite el acceso a través de Internet. Entonces el objetivo principal de este trabajo es a ser un Análisis de la Técnica Tampering o Data Diddling para la empresa CompuSolutions, la cual ayude a estar informada de los diferentes medios o ataques que podrían pasar, por lo que una amenaza representa el tipo de acción que tiende a ser dañina, mientras que la vulnerabilidad (conocida a veces como falencias o brechas representa el grado de exposición a las amenazas en un contexto particular.

Para que un sistema sea seguro, deben identificarse las posibles amenazas y por lo tanto, conocer y prever el curso de acción del enemigo. Por lo tanto, el objetivo es realizar un Análisis y así brindar una perspectiva general de los posibles ataques en sí de la técnica Tampering o Data Diddling otras utilizadas por Hackers o personas internas o externas categorizarlas, y dar una idea de cómo funciona para conocer la mejor forma de reducir el riesgo de intrusiones.

SUMARY

Because Internet use is increasing, more and more businesses or households allow their suppliers, employees, or individuals to access their information systems. Therefore, it is essential to know what resources need protection in order to control system access and rights of users of information system. The same procedures apply when access is allowed via the Internet.

The threat is the type of action tends to be harmful, while vulnerability (sometimes known as flaws or gaps represent the degree of exposure to threats in a particular context.

Finally, the counter represents all actions that are implemented to prevent the threat.

The countermeasures to be implemented not only technical solutions but also reflect the training and awareness by the user, and clearly defined rules.

For a system is safe, identify potential threats and therefore, understand and predict the course of enemy action. Therefore, the objective is to analyze and thus provide an overview of the possible attacks of the technique itself Tampering or Data diddling used by hackers or other internal or external people categorize, and give an idea of how to determine the best way to reduce the risk of intrusion**.**

TABLA DE CONTENIDOS

LISTA DE CUADROS Y GRAFICOS

CAPITULO I

1. INTRODUCCIÓN

1.1 Planteamiento del problema

"Análisis de la Técnica TAMPERING O DATA DIDDLING para la empresa CompuSolutions"

1.1.1 Antecedentes

Sabemos que las Redes y Sistemas de información, son bienes muy preciados en las empresas actuales, en los comienzos, los ataques involucraban poca sofisticación técnica para dicha penetración.

- Los insiders (empleados disconformes o personas externas con acceso al sistema dentro de la empresa) utilizaban sus permisos para alterar archivos o registros.
- Los outsiders (personas que atacan desde fuera de la organización) ingresaban a la red simplemente averiguando una contraseña válida.

A través de los años se han desarrollado formas cada vez más sofisticadas de ataque utilizando los "agujeros" en el diseño, configuración y operación de los sistemas.

Esto permitió a los intrusos tomar control de sistemas completos, produciendo verdaderos desastres.

Por ejemplo:
Después de crackear una contraseña, un intruso realiza un login como usuario legítimo para navegar entre los archivos y usar las vulnerabilidades del sistema.

Eventualmente también, el atacante puede adquirir derechos a lugares que le permitan dejar un virus u otras bombas lógicas para paralizar todo un sistema antes de huir.

1.2 Sistematización

1.2.1 Diagnostico o planteamiento de la problemática general

1.2.1.1 Causa – Efecto

CAUSA	EFECTO
Método Tampering o Data Diddling	Modificación desautorizada de los datos o el software instalado en el sistema víctima (incluyendo borrado de archivos).
Acceso o ataques a nuestra red	Son particularmente serios cuando el que lo realiza ha obtenido derechos de Administrador o Supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema.
Empleados internos o atacantes externos	Abusan de sus permisos de acceso, acceden remotamente o interceptan el tráfico de red.
Los Insiders o Outsiders	Propósito de fraude o de dejar fuera de servicio a un competidor.

Tabla 1: Causa – Efecto

1.2.1.2 Pronóstico y control de pronóstico

- **Pronostico**

La mayoría de personas o empresas están expuestas a que su información o sistemas sean fácilmente manipulados cosa que ellos desconocen por falta de información por lo que se recomienda es que

todos los afectados hagan un gasto moderado y un control mucho más estricto al momento de dar cierto privilegios a sus trabajadores, los cuales ayudara a proteger su información, por lo que se recomienda instalar en sus equipos los diferentes programas para prevenir acceso a sus quipos y así no estar vulnerables a los diferentes tipo de ataques.

- **Control de pronóstico**

Al estar expuestos a este tipo de ataques mediante los Tampering o Data Diddling, el presente trabajo explicara qué consecuencias traerá si los Insiders o Outsiders ingresan a sus equipos por lo que daremos ciertas recomendaciones para que esto no suceda y así las personas o empresas podrán tener un concepto más claro sobre el tema y estén preparados para tomar las medidas correctivas a tiempo para proteger su información.

1.3 Objetivos

1.3.1 Objetivo general

Realizar el análisis de la Técnica Tampering o Data Diddling para la empresa CompuSolutions, para dar a conocer a dicha empresa los posibles daños que estos pueden generar al momento que logran ingresar a sus equipos y más aun a su infamación.

1.3.1.2 Objetivos específicos

- ✓ Fundamentar teóricamente la técnica Tampering o Data Diddling.
- ✓ Determinar los posibles riesgos e impactos.
- ✓ Alternativas de solución para contrarrestar los ataques y minimizar el riesgo**.**
- ✓ Brindar recomendaciones para evitar dichos ataques Tampering o Data Diddling.
- ✓ Proceso de implementación para las alternativas de solución.

1.4 Justificación

1.4.1 Justificación Teórica

Esta técnica 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 disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema en forma deliberada.

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 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 home page 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 esta 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 Oríffice y Net Bus.

1.4.1.2 Justificación Metodológica

E escogido este tema porque es de suma importancia y que conozco, además es un tema muy interesante ya que como se ha expuesto anteriormente la Técnica Tampering o Data Diddling es usado en si para perjudicar a personas, empresas u organizaciones, por lo que es de suma importancia saberlo.

1.4.1.3 Justificación Práctica

Este tema podrá aportar de manera clara y precisa asía las múltiples consecuencias que esta técnica conlleva por lo que daremos muchas alternativas para prevenir este y todos los tipos de ataques que existen y de esta manera proteger lo que es más preciado para todos la información.

1.5 Alcance y limitaciones

1.5.1 Alcance

El siguiente proyecto consta en averiguar cómo esta técnica Tampering o Data Diddling hace daño dentro de esta empresa, en si quienes los realizan y como asen posible el acceso a diferentes ares de trabajo o a todo para luego perjudicar a dicha empresa.

1.5.2 Limitaciones

Este proyecto consiste en si aun análisis de esta técnica la cual no se realizara una práctica comparativa de de esta técnica puesto que

es solamente un análisis, el cual ayudara a la Empresa CompuSolutions a tomar ciertas recomendaciones o seguridades para de esta forma mantener segura su información.

1.6 Marco de Referencia

1.6.1 Marco Espacial

En si el presente trabajo es de suma importancia puesto que esto sucede en todo el mundo, por lo que se requiere un análisis profundo acerca del tema el cual ayude a las personas, empresas o organizaciones a tomar las dividas precauciones y de esta manera tener una mayor solvencia en cuanto a su información.

1.6.2 Marco Temporal

El tiempo estimado que se espera lograr esta investigación será alrededor de unos 2 a 3 meses exactamente.

CAPITULO II

2. MARCO DE REFERENCIA

2.1 Marco Teórico

2.1.1 Introducción

Cuando hablamos de Seguridad Informática hacemos referencia a la protección de nuestra Información a través de medios Informáticos, divididos entre Hardware y Software que complementados son una excelente defensa contra delitos informáticos ataques informáticos.

Durante 1997, el 54 por ciento de las empresas norteamericanas sufrieron ataques en sus sistemas. Las incursiones de los piratas informáticos, ocasionaron pérdidas totales de 137 millones de dólares en ese mismo año.

El Pentágono, la CIA, UNICEF, la ONU y demás organismos mundiales han sido víctimas de intromisiones por parte de estas personas que tienen o no muchos conocimientos en la materia y también una gran capacidad para resolver los obstáculos que se les presentan.

Un hacker puede tardar meses en vulnerar un sistema ya que son cada vez más sofisticados. Pero el lema es: hecha la ley, hecha la trampa. (Netzweb, 2011)

2.1.1.1 Seguridad Física

Es uno de los aspectos más olvidados a la hora del diseño de un sistema informático.

Si bien algunos de los aspectos tratados a continuación se prevén, otros, como la detección de un atacante interno a la empresa que intenta a acceder físicamente a una sala de operaciones de la misma, no.

Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de la sala, que intentar acceder vía lógica a la misma.

Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

- **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.

Evaluar y controlar permanentemente la seguridad física del edificio es la base para o comenzar a integrar la seguridad como una función primordial dentro de cualquier organismo.

- **Tener controlado el ambiente y acceso físico permite:**
  - ✓ Disminuir siniestros
  - ✓ Trabajar mejor manteniendo la sensación de seguridad
  - ✓ Descartar falsas hipótesis si se produjeran incidentes
  - ✓ Tener los medios para luchar contra accidentes

2.1.1.2 Seguridad Lógica

Una vez que se haya planteada la estructura de nuestra Seguridad Física podemos complementar con 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."

- **Las recomendaciones que se plantean para crear Seguridad Lógica son:**
  - Restringir el acceso a los programas y archivos
  - Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
  - Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.
  - Que la información transmitida sea recibida por el destinatario al cual ha sido enviada y no a otro.

2.1.1.3 Ataque Informatico

Un ataque informático consiste en aprovechar alguna debilidad o falla tanto en el software, hardware, o incluso en las personas que forman parte de un ambiente informático; con el fin de obtener un beneficio por lo general económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización. (Global Knowledge, 2008)

2.1.1.4 Delitos Informáticos

Cuando hablamos de delitos informáticos, hacemos referencia a aquellos delincuentes que sin contar con muchas armas físicas, usan su arma más elemental, su extraordinario conocimiento sobre los métodos Informáticos para extraer información ajena de personas e inclusive Empresas, Organizaciones, Bancos u otros lugares de importancia.

El avance de la era informática ha introducido nuevos términos en el vocabulario de cada día. Una de estas palabras, hacker, tiene que ver con los delitos informáticos.

A veces escuchamos historias acerca de desapariciones de Información en instituciones de prestigio, dinero desaparecido de Bancos o quizá transacciones financieras de personas que ni siquiera tienen idea de cómo sucedió, pero esto se apega demasiado a la realidad, en especial en el año 1997 en estados Unidos ocasionando pérdidas millonarias y en

el 2000 cuando este tipo de delincuencia informática se propago a un nivel más avanzados, refiriéndonos a las estrategias de manipulación de sistemas e incluso de personas ingenuas que han sido víctimas de este tipo de actividades ilegales.

Una forma de combatir este tipo de delitos, no es tan difícil o inimaginable como parece, es mucho más sencillo, simplemente hay que conocer los procedimientos que este tipo de delincuentes usan, como por ejemplo, saber acerca de seguridades financieras, desconfianza a personas desconocidas, y sobre todo un conocimiento mediano sobre informática. Al estar preparado y prevenido sobre estos delitos, será muy difícil que este tipo de delincuencia nos afecte.

2.1.1.5 Sistema Informatico

Un sistema Informático es el conjunto que resulta de la integración de cuatro elementos: Hardware, software, datos, usuarios y su objetivo principal es el de integrar estos 4 componentes para hacer posible el procesamiento automático de los datos mediante el uso de computadoras. (Deleitos, 2008)

2.1.1.6 Que es la información

"Es un conjunto de datos con un significado, o sea, que reduce la incertidumbre o que aumenta el conocimiento de algo, y que nos ayuda a la toma de decisiones" [CHIAVETANO IDALBERTO, Año 2006].

Para Ferrell y Hirt, la información "comprende los datos y conocimientos que se usan en la toma de decisiones". [FARREY O. C. y HIRT GEOFFREY, Año 2004] Según Czinkota y Kotabe la información "consiste en datos seleccionados y ordenados con un propósito específico". [CZINKOTA MICHAEL y COBATE].

2.1.1.7 Ataques a nuestra información

2.1.1.7.1 Quienes los realizan:

Por empleados internos que abusan de sus permisos de acceso, o por atacantes externos que acceden remotamente o interceptan el tráfico de red, y de esta forma tratar de perpetrar en si a la seguridad informática como son: Confidencialidad, Integridad, Disponibilidad.

Y dichas amenazas o ataques dentro de una organización tratan básicamente perpetrar a una organización o empresa de una u otra forma con el fin de: Fraude (está asociado al de estafa, que es un delito contra el patrimonio o la propiedad.).

Extorsión (es un delito que significa obligar a una persona, a través de la utilización de violencia o intimidación y de esta forma obtener lo propuesto), Robo de información, Venganza, Simplemente el desafío de penetrar un sistema.

(http://carlosadlrs.wordpress.com/hacking/hacking/)

Sujeto Activo:

En este tipo de delitos, el sujeto activo debe tener conocimientos técnicos de informática, es decir, en cierto modo, una persona con nivel de instrucción elevado, para poder manipular información o sistemas de computación. (**http://www.derechoecuador.com**).

Sujeto Pasivo:

En el caso del delito informático pueden ser: individuos, instituciones de crédito, gobiernos, en fin entidades que usan sistemas automatizados de información. (http://www.derechoecuador.com).

2.2 La técnica Tampering y Data Diddling:

Esta categoría se refiere a la modificación desautorizada de los datos o el software instalado en el sistema víctima (incluyendo borrado de archivos).

Son particularmente serios cuando el que lo realiza ha obtenido derechos de Administrador o Supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema. (http://www.todoecommerce.com)

2.3 Marco Conceptual

El Proyecto estará enfocado en el Análisis de la Técnica Tampering o Data Diddling, para ayudar, proteger, combatir, para que de esta forma las personas, o la empresa llamada CompuSolutions o más, logrando con esto, segmentar el análisis y tener una apreciación viable para la justificación del Proyecto.

2.4 Marco Espacial

El Proyecto a desarrollarse estará planteado en una duración de 2 o 3 meses exactamente.

2.5 Marco Legal

CompuSolutions es una empresa que se formó hace años, la misma se está constituida con número de ruc0101994671 001 con su respectiva actividad profesional en servicios y venta de equipos informáticos.

CAPITULO III

3. METODOLOGÍA Y ANÁLISIS

3.1 Análisis de la Problemática

Nos basaremos en el uso de técnicas y métodos de Investigación para recopilar la mayor cantidad de información y sobre todo opiniones que ayuden a fundamentar nuestros objetivos.

Mediante las herramientas de investigación se podrá identificar de una manera más certera los problemas que tanto la empresa ya dicha o personas que tienes este tipo de dificultades y con esto ayudando a prevenir y corregir las mismas.

3.2 Metodología Investigativa

3.2.1 Método

3.2.1.1 Cualitativo – Cuantitativo

Mediante estos métodos se busca conocer de manera más segura cuales son los conocimientos, evidencias, sucesos, casos, o experiencias sobre temas como seguridad informática, ataques informáticos, etc.

Basándonos en porcentajes, todo esto con el fin de lograr los objetivos propuestos.

3.2.2 Técnica

3.2.2.1 Encuestas

Esta técnica a utilizar es aquella destinada a obtener datos de varias personas que en este caso son de estudiantes del Colegio Particular Técnico Cesar Andrade y Cordero del curso 6 de Administración de Sistemas y de ciertos locales o empresas de informática, cuyas opiniones impersonales son de gran importancia para el análisis de este proyecto o de algún otro.

Después de a ver recopilado la información de las personas en general encuestadas se procederá a realizar un Análisis basado en porcentajes para identificar cual es el conocimiento real sobre los temas planteados y de esta forma obtener una conclusión global que nos permitirá saber si esta técnica es o fue entendida y ala ves como protegerse de ella.

3.3 Población Involucrada

Para este proceso de estudio se ha tomado como referencia las opiniones de 35 encuestados, que representan a estudiantes del Colegio Particular Técnico Cesar Andrade y Cordero del curso 6 de Administración de Sistemas y de ciertos locales o empresas de informática.

3.4 Formato de la Encuesta

- **Hoja 1**

Formato de la Encuesta

Encuesta para determinar el grado de conocimiento acerca del robo, alteración de información en su computador mediante el internet o por personas internas o externas.

Marque con una “x” lo falso o encierre con un circulo“0” lo verdadero la respuesta que elija:

1. **¿En su casa o empresa el uso de internet es fundamental?**
   - Si
   - No

2. **¿Cree usted que el robo, alteración, violación de información y acceso a datos a través de Internet sucede en nuestra vida?**
   - Si
   - No

3. **¿Ha pensado usted que abría la posibilidad de perder, robar, copiar, o eliminar información total de su computador a través de algún delito informático o por personas de su mismo entorno?**
   - Si
   - No

4. **¿Ha pasado usted por algún tipo de estafas económicas o robo de información?**
   - **SI**
   - **NO**

5. **¿Tiene usted algún conocimiento sobre Hackers y como evitarlos?**
   - SI
   - NO
   - REGULAR

- **Hoja 2**

6. ¿Qué tipos de amenazas o ataques Informáticas conoce?

- Tampering o Data Diddling
- Spoofing
- Eavesdropping y Packet Sniffing
- Snooping y Downloading:
- Virus
- Gusano
- Phishing
- Spyware
- Spam
- Ninguna
- Otras

7. ¿Actualmente en su hogar o empresa o institución cuál de estas opciones usa como medida de Seguridad Informática?

- Contraseñas de Acceso para Usuarios
- Seguridades Biométricas(como lector de huellas, rostro facial)
- Firmas/Certificados Digitales
- Monitores de Trafico de Red
- Copias de Seguridad de Datos Periódicas
- Ninguna
- Otros

8. ¿Le gustaría conocer o aprender medidas de seguridad para contrarrestar estos ataques?

- Si
- No

3.5 Análisis y Resultados de la Encuesta

1. **¿En su casa o empresa el uso de internet es fundamental?**

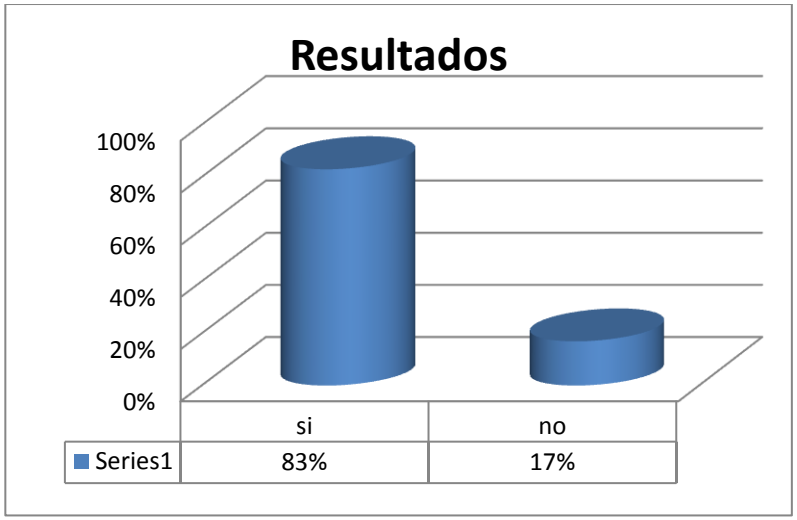


Grafico 1: Resultados de la pregunta 1 de la encuesta.

(Marin, 2011)

	SI	NO
N° de Encuestados 35	28	7
Resultados de los Encuestados %	83	17

Tabla 2: Respuesta de la pregunta 1

(Marin, 2011)

Se puede observar claramente que existe un porcentaje muy elevado en cuanto a esta pregunta, las opiniones apuntaron un 83% por la respuesta “SI”, de esta manera se entiende que la mayoría de Encuestados usan el internet para sus labores matutinas u otras actividades.

2. **¿Cree usted que el robo, alteración, violación de información y acceso a datos a través de Internet sucede en nuestra vida?**

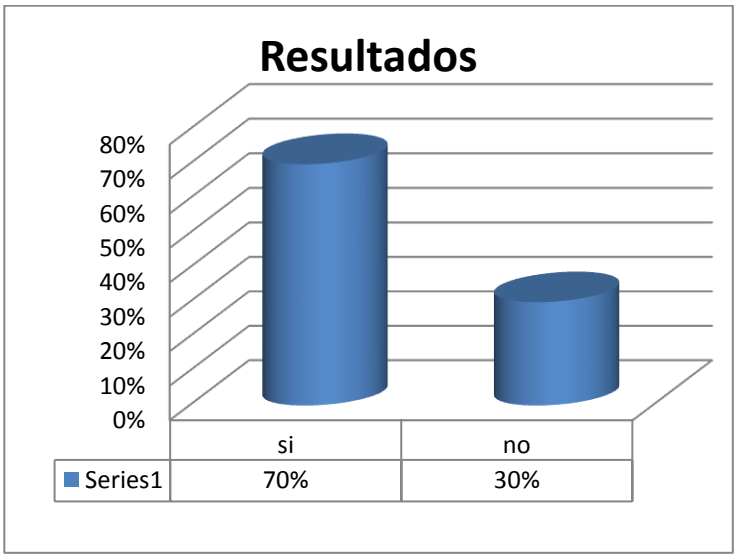


Grafico 2: Resultados de la pregunta 2 de la encuesta.

(Marin, 2011)

	SI	NO
N° de Encuestados 35	25	10
Resultados de los Encuestados %	70	30

Tabla 3: Respuesta de la pregunta 2

(Marin, 2011)

Los resultados que mostro nuestra encuesta apunto claramente un 70% para un “SI”, lo cual nos indica que la gente de hoy en día y aún más aquellas personas que está ligadas al trabajo en Internet consideran que el robo de Información es algo Real, y por supuesto algo que no se debe tomar a la ligera, debido a las constantes evidencias de acceso no autorizado, suplantación de Identidad, instalación de software maligno, robo de contraseñas y robos a través de internet que se han dado hoy en día.

3. **¿Ha pensado usted que abría la posibilidad de perder, robar, copiar, o eliminar información total de su computador a través de algún delito informático o por personas de su mismo entorno?**

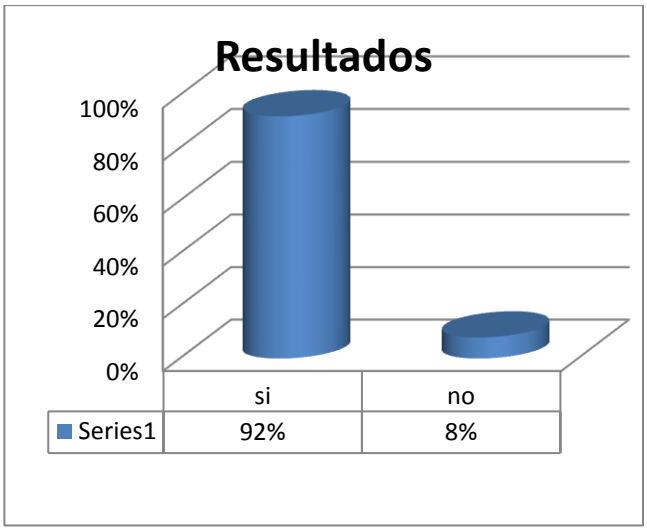


Grafico 3: Resultados de la pregunta 3 de la encuesta.
(Marin, 2011)

	SI	NO
N° de Encuestados 35	30	5
Resultados de los Encuestados %	92	8

Tabla 4: Respuesta de la pregunta 3
(Marin, 2011)

En base a la respuesta dada en la pregunta anterior por la gente, se complementa lógicamente con esta debido a que el 92% de encuestados consideran que “SI” han tenido en cuenta perder información, y un “NO” representado por un 8% que no consideran peligroso el de robar información.

Lo que se puede observar entonces es que entre los encuestados si hay una cultura de seguridad informática, y esto lógicamente ayuda a que las

personas opten por mejorar las seguridades de su PC o simplemente buscar información por curiosidad sobre estas.

4. **¿Ha pasado usted por algún tipo de estafas económicas o robo de información?**

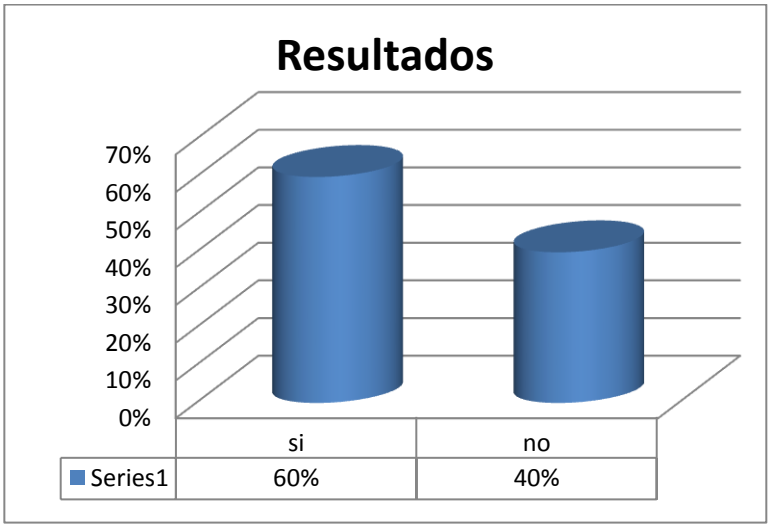


Grafico 4: Resultados de la pregunta 4 de la encuesta. (Marin, 2011)

	SI	NO
N° de Encuestados 35	22	13
Resultados de los Encuestados %	60	40

Tabla 5: Respuesta de la pregunta 4
(Marin, 2011)

Los resultados que mostro nuestra encuesta muestra claramente un 60% para un “SI”, lo cual nos indica que la gente, empresas de hoy en día y aún más aquellas personas que está ligadas al trabajo en Internet aseguran a ver pasado por alguna estafa Real, y un 40% el cual es un porcentaje alto cual opinan que si caen en alguno de ese tipo de estafas son por qué no entran a paginas conocidas o seguras,

y en cuanto a la información por no contar con la medidas de seguridad apropiada.

5. ¿Tiene usted algún conocimiento sobre Hackers y como evitarlos?

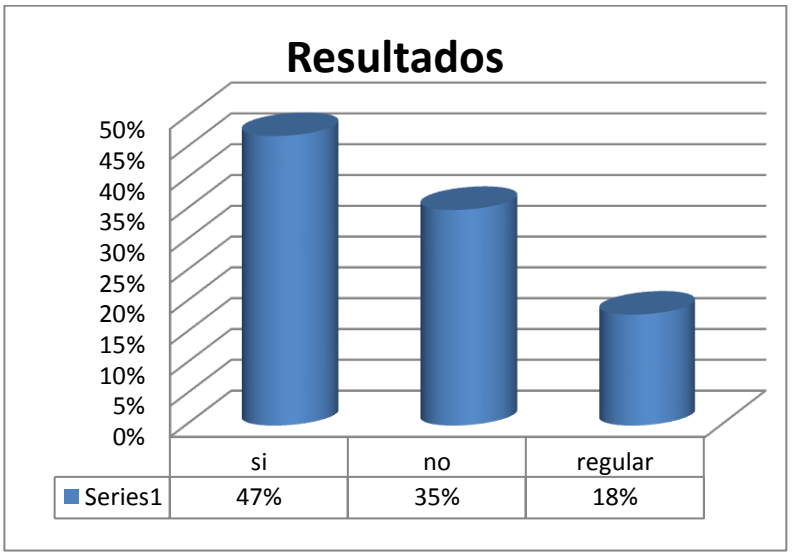


Grafico 5: Resultados de la pregunta 5 de la encuesta.

(Marin, 2011)

	SI	**NO**	**Regular**
N° de Encuestados 35	15	10	5
Resultados de los Encuestados %	47	35	18

Tabla 6: Respuesta de la pregunta 5

(Marin, 2011)

Los resultados que mostro nuestra encuesta son los siguientes un 47% por un “SI”, lo cual nos indica que la gente de hoy en día y aún más aquellas personas que está ligadas al trabajo en Internet consideran que han escuchado sobre este tipo de personas de lo que son capaces, pero que no saben cómo evitarlos, el 35% concluyo con que no conocen nada

acerca de este tema y un Regular el cual se dedujo que tienen cierto grado de conocimiento de este tema, pero que quisieran saberlo.

6. ¿Qué tipos de amenazas o ataques Informáticas conoce?

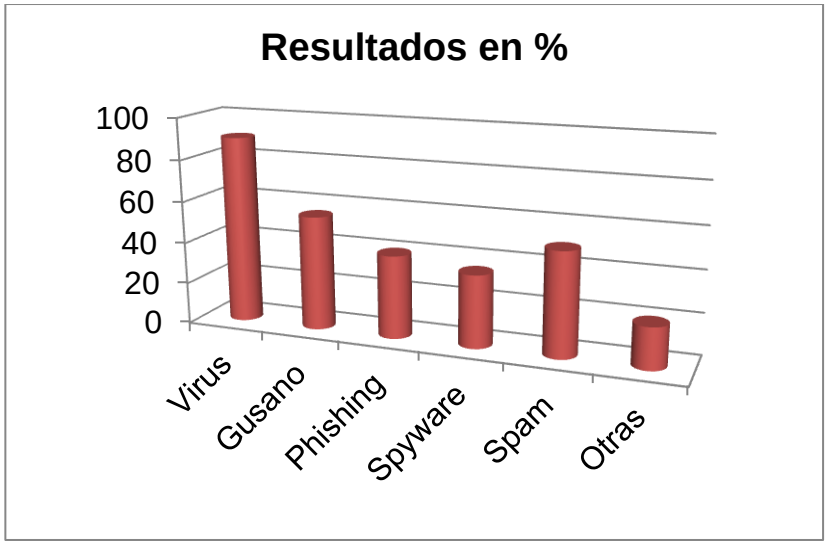


Grafico 6: Resultados de la pregunta 6 de la encuesta.
(Marin, 2011)

Los resultados fueron:

	Virus	Gusano	Tampering	Phishing	Spam	Total Encuestados
Resultados	**90%**	**55%**	**1%**	**35%**	**50%**	**35**

Tabla 7: Respuesta de la pregunta 6
(Marin, 2011)

Los resultados que se expresaron con mayor porcentaje son por parte de los virus, Spam, gusanos y un poco de los Phishing este y los demás aquellos que son tan molestosos e inclusive destructivos, que ya se encuentran en la mente de las personas por causa de su constante desarrollo y ataques a través de las redes informáticas, y en

cuanto a Tampering apenas un 1% eso quiere decir que casi nunca ha escuchado o pasado por este tipos de ataques.

7. **¿Actualmente en su hogar o empresa o institución cuál de estas opciones usa como medida de Seguridad Informática?**

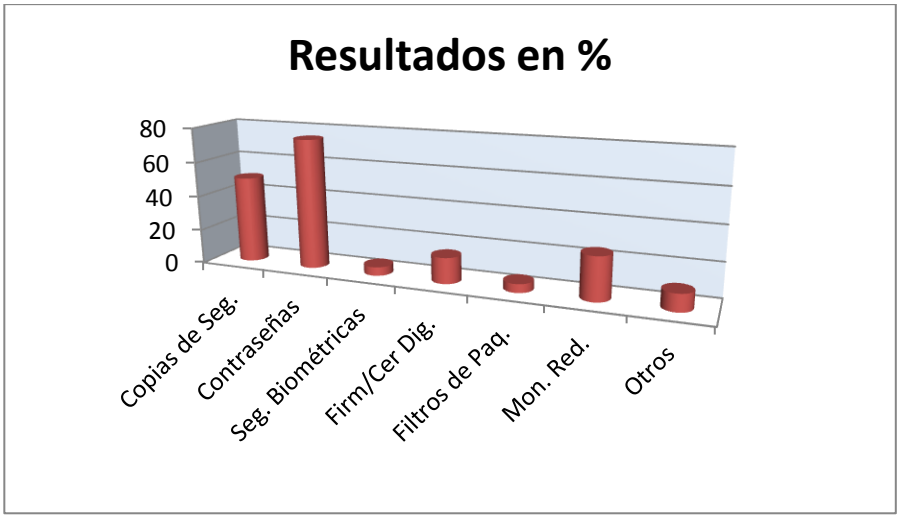


Grafico 7: Resultados de la pregunta 7 de la encuesta.
(Marin, 2011)

	C.Seguridad	Contraseñas	F.digitales	Filtros	Mon.Red	Seg. Biométricos	Otros
Total de encuestados	**35**	**35**	**35**	**35**	**35**	**35**	**35**
Resultados	**50**	**75**	**15**	**5**	**25**	**5**	**10**

Tabla 8: Respuesta de la pregunta 7
(Marin, 2011)

Se planteó varias opciones de respuesta, sobre medidas de seguridad, los Resultados reflejaron que claramente cuál es la respuesta que comúnmente es utilizada como una medida de seguridad, apuntaron al

uso de “Contraseñas”, pues es la forma más común de proteger datos y restringir accesos a personas o intrusos inadecuados.

8. **¿Le gustaría conocer o aprender medidas de seguridad para contrarrestar estos ataques?**

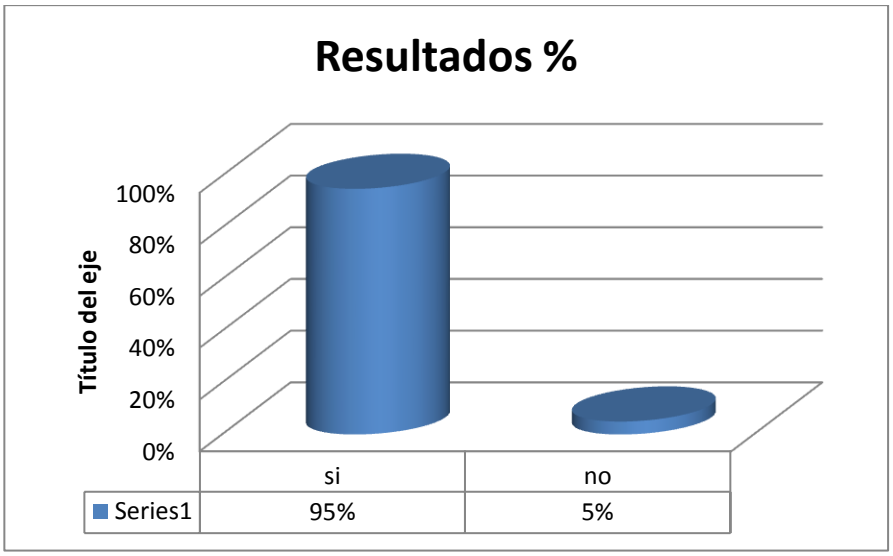


Grafico 8: Resultados de la pregunta 8 de la encuesta.

(Marin, 2011)

	SI	NO
N° de Encuestados 35	32	3
Resultados de los Encuestados %	95	5

Tabla 9: Respuesta de la pregunta 8

(Marin, 2011)

De forma mayoritaria se pudo observar un notable interés con un 95% de agrado hacia esta pregunta, el cual estarían dispuestas a aprender medida de seguridad para contrarrestar este tipo de ataques.

CAPITULO IV

4. DESARROLLO

4.1 Fundamentar teóricamente la técnica Tampering o Data Diddling

4.1.1 Ataques de Modificación o Daño

- **Que es la técnica 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 disparar 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 chequear y tratar de recuperar aquella información que ha sido alterada o borrada.

Como siempre, esto puede ser realizado por insiders o 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 home page 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 está 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.
(canal-ayuda, 2010)

- **Quienes los realizan:**

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 home page 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 esta 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 Orífice y NetBus.

- **Algunos conceptos que involucran esta Técnica**

9. Seguridad Informática

La seguridad informática puede entenderse como aquellas reglas técnicas o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial.

En este sentido, es la información el elemento principal a proteger, resguardar y recuperar la información que nosotros consideramos

importantes. Esta información puede estar susceptible tanto como a virus, daños técnicos, mal manejo de la computadora, etc.

En el área de informática, existen varios riesgos tales como: ataque de virus, códigos maliciosos, gusanos, caballos de Troya y hackers; no obstante, con la adopción de Internet como instrumento de comunicación y colaboración, los riesgos han evolucionado y, ahora, las empresas deben enfrentar ataques de negación de servicio y amenazas combinadas; es decir, la integración de herramientas automáticas de "hackeo", accesos no autorizados a los sistemas y capacidad de identificar y explotar las vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos.

Es importante que para tener nuestra información se encuentre bien resguardada, tener un buen antivirus instalado, para que elimine y localice cualquier virus que se haya instalado en nuestra computadora.

El objetivo primordial de cualquier antivirus actual es detectar la mayor cantidad de amenazas informáticas que puedan afectar un ordenador y bloquearlas antes de que la misma pueda infectar un equipo, o poder eliminarla tras la infección.

(eumed, 2009)

Imagen 1: Seguridad Informática

- **Riesgos de Seguridad:**

  En la Actualidad existen muchos riesgos que surgen de no asegurar una red inalámbrica de manera adecuada: La intercepción de datos es la práctica que consiste en escuchar las transmisiones de varios usuarios de una red inalámbrica.

  El crackear es un intento de acceder a la red local o a Internet. La interferencia de transmisión significa enviar señales radiales para interferir con tráfico. Los ataques de denegación de servicio inutilizan la red al enviar solicitudes falsas.

- **Ataques a nuestra Información:**

  ¿Cuáles son las amenazas?

  Los ataques pueden servir a varios objetivos incluyendo fraude, extorsión, robo de información, venganza o simplemente el desafío de penetrar un sistema.

Esto puede ser realizado por empleados internos que abusan de sus permisos de acceso, o por atacantes externos que acceden remotamente o interceptan el tráfico de red.

A esta altura del desarrollo de la "sociedad de la información" y de las tecnologías computacionales, los piratas informáticos ya no son novedad.

Los hay prácticamente desde que surgieron las redes digitales, hace ya unos buenos años.

Sin duda a medida que el acceso a las redes de comunicación electrónica se fue generalizando, también se fue multiplicando el número de quienes ingresan "ilegalmente" a ellas, con distintos fines.

Los piratas de la era cibernética que se consideran como una suerte de Robin Hood modernos y reclaman un acceso libre e irrestricto a los medios de comunicación electrónicos. (ataques, 2011)

Imagen 2: Ataques a nuestra Información

- **Existe una clasificación sobre los atacantes:**

Según el tipo de persona:	Según el tipo de Ataque:	Según el objetivo del Ataque:
10. Personal Interno 11. Ex-empleados 12. Timadores 13. Vándalos 14. Mercenarios 15. Curiosos	16. Hacker 17. Cracker 18. Crasher 19. Pheacker 20. Phishers 21. Sniffers	22. Según el objetivo del ataque: 23. Dinero 24. Información confidencial 25. Beneficios personales 26. DañoAccidente

Cuadro 1: Clasificación sobre los Atacantes

- **Software utilizado por atacantes:**

Utilizan software llamado “malware” (malicious software): termino para designar un programa informático que provoca de forma intencionada una acción dañina para el sistema y/o usuario.

Tipos de malware:

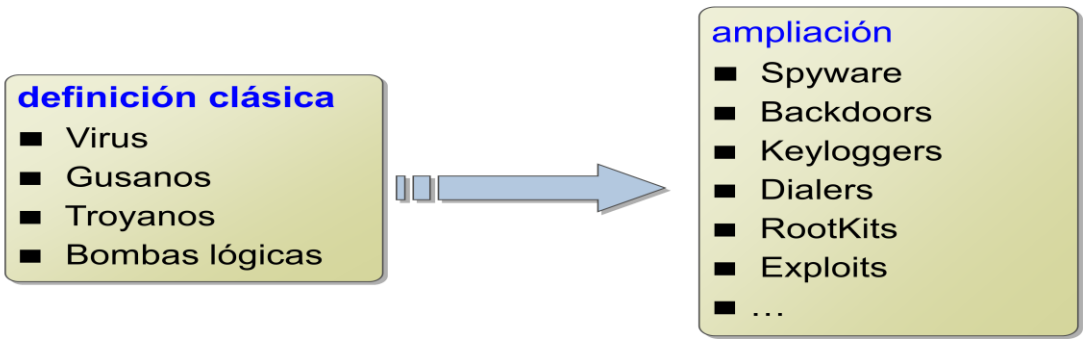


Imagen 3: Los Virus y sus Aplicaciones

Spyware:	Recolecta y envía información privada sin el consentimiento y/o conocimiento del usuario.
Dialer:	Realiza una llamada a través de módem o RDSI para conectar a Internet utilizando números de tarificación adicional sin conocimiento del usuario
Keylogger:	Captura las teclas pulsadas por el usuario, permitiendo obtener datos sensibles como contraseñas.
Adware:	Muestra anuncios o abre páginas webs no solicitadas.
Backdoor:	Llamada puerta trasera, permite acceso y control remoto del sistema sin una autentificación legítima.
Exploit:	Sirve básicamente para ejecutar código casero en la consola, es decir, programas NO oficiales como emuladores, reproductores multimedia, navegadores, juegos de importación y todo lo que pueda programarse.
Rootkit:	Es un clásico ejemplo de un software tipo Caballo de Troya, que permiten a un hacker crear backdoors en un sistema, recolectando información sobre otros sistemas en la red.

Cuadro 2: Definiciones de cada Virus

- **Métodos y herramientas de ataque**

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 numerosos "hacker" bulletin boards y web sites, donde

además encuentra todas las instrucciones para ejecutar ataques con las herramientas disponibles.

Los métodos de ataque listados a continuación 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.

- **Estos pueden ser:**
    - Eavesdropping y Packet Sniffing
    - Snooping y Downloading
    - Tampering o Data Diddling
    - Spoofing
    - Jamming o Flooding

- **Los Ataques a la Wi-Fi:**

El medio más común en este tiempo para atacar son las redes Wireless que se ha convertido desde hace tiempo en un deporte, una diversión o un hobby.

En casi todos los medios de comunicación se han escrito artículos sobre como hackear redes Inalámbricas. Existen diferentes maneras de atacar a las seguridades de una red Wi-Fi. (Wifi, 2011)

Imagen 4: Ataques WiFi

Una alternativa consiste en que el intruso intente conectarse a un Access point de la red inalámbrica para luego ganar acceso a la red corporativa.

La otra alternativa consiste en implantar un Access point "pirata" para atraer a los usuarios desprevenidos o muy curiosos a una red de hackers o red pirata.

Es muy importante conocer que en las redes Inalámbricas la información se transmite por medio de ondas de radio frecuencia, debido a que estas ondas viajan por el aire es imposible evitar que esta sea observada o accedida sino se tiene restricciones, por cualquier persona que se encuentre en un radio aproximado de 100 metros.

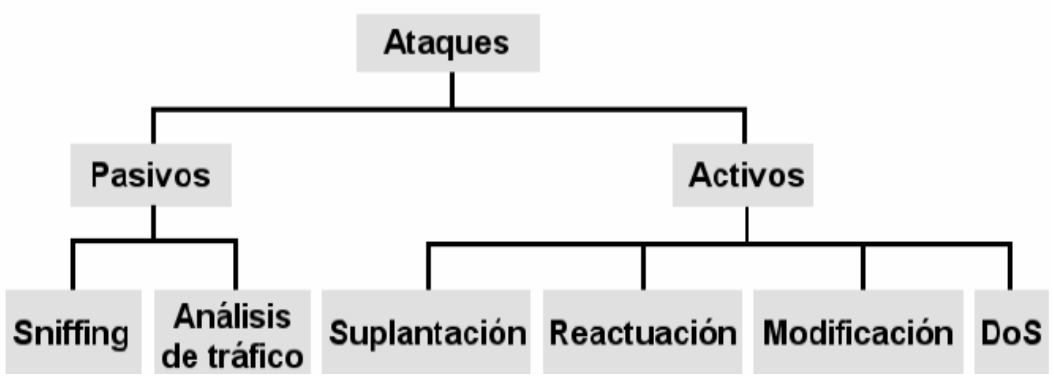


Imagen 5: Ataques Pasivos y Activos

- **Explicación:**

Ataques pasivos	
Sniffing	El tráfico de redes inalámbricas puede espiarse con mucha más facilidad que en una LAN Basta con disponer de un portátil con una tarjeta inalámbrica El tráfico que no haya sido cifrado, será accesible para el atacante y el cifrado con WEP también
Análisis de tráfico	El atacante obtiene información por el mero hecho de examinar el tráfico y sus patrones: a qué hora se encienden ciertos equipos, cuánto tráfico envían, durante cuánto tiempo, etc.
Ataques activos	
Suplantación	Mediante un sniffer para hacerse con varias direcciones MAC válidas El análisis de tráfico le ayudará a saber a qué horas debe conectarse suplantando a un usuario u otro Otra forma consiste en instalar puntos de acceso ilegítimos para engañar a usuarios legítimos para que se conecten a este AP en lugar del autorizado
Modificación	El atacante borra, manipula, añade o reordena los mensajes transmitidos

Cuadro 3: Ataques Pasivos y Activos

- **Ventajas y Desventajas de DE WI-FI**

Ahora bien, el hecho de tener una conexión Wi-Fi en nuestro equipo para muchos nos representan muchas ventajas, tales como:

- ✓ Conectividad inalámbrica
- ✓ Cero cables
- ✓ Poder conectarse en cualquier lugar
- ✓ Elección de entre varias señales libres o con seguridad

Pero como se dice comúnmente, no todo lo que brilla es oro, así que siempre cada situación de ventajas puede ofrecernos determinadas desventajas, de las cuales podríamos llegar a mencionar algunas:

- ✓ Falla en la conexión
- ✓ Distancia limitada para la recepción de la señal
- ✓ Facilidad de hackeo de las seguridades.

Como se puede observar, tenemos varias ventajas así como desventajas, mismas que deberíamos de evaluarlas y analizarlas detenidamente y ver si nos conviene en alguna medida o no el tener que usar una conexión inalámbrica.

4.2 Posibles riesgos e impactos:

A continuación describiremos algunos procesos que se manejan dentro de la empresa, para que mediante estos pode determinar que riesgos e impactos tendrían sobre cada uno de estos procesos, además para el desarrollo de individual realizaremos varias matrices, las cuales nos ayudaran o facilitaran ver los riesgos e impactos ocurridos, y así visualizar que proceso hay que tomarlo mas en consideración para un futuro y solucionarlo.

Los siguientes riesgos son:

1. La información
2. Los equipos
3. La tecnología
4. El personal
5. Las ventas de productos
6. Ambientales

4.2.1 Riesgo 1

Venta de productos:

Para el proceso de ventas por internet los clientes se registran en un portal de Internet, seleccionan los productos que requieren según su necesidad, de ahí los datos de su tarjeta de crédito para pagar.

Si la venta es directamente con un vendedor de la empresa, este vendedor ofrecería todos los productos que tiene, de ahí el cliente podrá

escoger según su necesidad y comprarlo enseguida y también podrá realizar los pagos a contado, crédito o con tarjeta de crédito.

Luego de todo esto se prosigue a la obtención de toda la información para generar la respectiva matriz la cual ayudara a ver de una mejor manera si algún cambio dentro de este proceso sería catastrófico.

En si al no contar con un sistema adecuado el cual valide la tarjeta y a su vez genere un reporte diario de ingresos el cual ayude a constatar si la venta fue satisfactoria o no, igual para el cliente verificar su compra.
Para la cual contamos con la siguiente información que nos ayudara a realizar la matriz correspondiente:

- **Entradas / insumos del proceso:**
  - computadoras
  - Lista de precios
  - Lista de ofertas
  - Proveedores
  - Solicitudes de compra de clientes
  - Datos de instrumentos de pago (tarjeta de crédito)
  - Información de clientes
  - Credenciales de entrada al sistema

- **Activos / Infraestructura del proceso:**
  - infraestructura de telecomunicaciones (Internet)
  - Portal de ventas en línea (aplicativo)
  - Sistema de transferencia de dinero (aplicativo)
  - Sistema de recepción de pagos con tarjeta (aplicativo)
  - Información del proceso de ventas y de clientes (bases de datos)

- **Salidas / productos del proceso:**
    - Ingresos por ventas
    - Reporte de ventas
    - Productos comprados por clientes
    - Cuentas en el sistema de ventas

Para cada proceso de negocio, se recomienda preguntar lo siguiente:

- **Confidencialidad:**

¿Qué afectación sufriría el negocio si su información sensible del proceso se filtra por un error, es robada, hurtada, manipulada, copiada, eliminada de manera intencional?

- **Integridad:**

¿Qué afectación sufriría el negocio si el proceso se realiza de forma incorrecta, sea por un error o por un cambio intencional? (ej. qué pasa si hay un error en la forma en que se lleva a cabo la venta del producto).

- **Disponibilidad:**

¿Qué afectación sufriría el negocio si el proceso se detiene por un error o por una acción deliberada? (ej. qué pasa si fallan los medios por los cuales se lleva a cabo el proceso de venta del producto).

- **Autenticidad:**

¿Qué afectación sufriría el negocio si en el proceso interviene alguien que no está autorizado para hacerlo? (ej. qué pasa si alguien no

autorizado modifica precios de productos, o si la información de pago es falsa.

En base a estos 4 puntos podremos ya generar la matriz correspondiente a los posibles riesgos e impactos que tendría.

Significado de:

- **Alta:** quiere decir que las posibilidades de un ataque están entre un 75% a un 100%.
- **Medio:** quiere decir que las posibilidades de un ataque están entre un 50% a un 75%.
- **Bajo:** quiere decir que las posibilidades de un ataque están entre un 0% a un 50%.

Tabla:

Proceso: Venta de productos	PROBABILIDAD	IMPACTO
Entradas / insumos del proceso.	ALTA	ALTA
Activos / Infraestructura del proceso	MEDIO	MEDIO
Salidas / productos del proceso.	MEDIO	MEDIO

Tabla 10: Riesgos Venta de Productos

4.2.2 Riesgo 2

La Información:

Tabla

Proceso: La información	PROBABILIDAD	IMPACTO
Perdida	ALTA	ALTA
Robo	ALTA	ALTA
Modificación	MEDIO	ALTA
Eliminación	MEDIO	MEDIO

Tabla 11: Riesgos Información

Puede haber mucha información perdida, al no tener un buen respaldo en un sistema de basa de datos o un control seguro o controlado.

4.2.3 Riesgo 3

Los Equipos:

Tabla

Proceso: Equipos	PROBABILIDAD	IMPACTO
Malos	ALTA	ALTA
Viejos	ALTA	ALTA
Desactualizados	MEDIO	ALTA

Tabla 12: Riesgos Equipos

Los equipos actuales con los que trabaja la empresa sufren desperfectos muy seguidos, por lo que puede ocasionar retrasos en el manejo del sistema con el que trabajan.

4.2.4 Riesgo 4

La Tecnología:

Tabla

Proceso: La Tecnología	PROBABILIDAD	IMPACTO
Falta de equipos informáticos	ALTA	ALTA
No cuentan con el suficiente capital	ALTA	ALTA

Tabla 13: Riesgo Tecnología

La falta de equipos informáticos con el que cuenta la empresa son muy pocos, y aun así ellos manejan todos sus procesos, por lo que el riesgo ante un ataque es muy ALTA.

4.2.5 Riesgo 5

Humano:

Tabla

Proceso: Humano	PROBABILIDAD	IMPACTO
Poco personal	ALTA	ALTA
Falta de preparación	ALTA	ALTA
Los insiders (empleados disconformes o personas externas con acceso al sistema dentro de la empresa	MEDIO	ALTA
Los outsiders (personas que atacan desde fuera de la organización)	MEDIO	ALTA
Hurto, adulteración, fraude, modificación, revelación, perdida, sabotaje, vandalismo, crackers, hackers, falsificación, robo de contraseñas, intrusión, alteración, etc.	ALTA	ALTA

Tabla 14: Riesgo Humano

Al no haber existido un sistema Informático anteriormente eficiente, la empresa está en clara inseguridad por lo que el personal tanto interno o personas externas pueden ocasionar daños terribles a la empresa, con o sin intensiones, se recomienda que el dueño de la empresa asigne ciertos permisos y las debidas contraseñas al personal, para que de esta manera pueda prevenir todos estos posibles riesgos humanos, y así asegurar su información.

4.2.6 Riesgo 6

Ambientales:

Tabla

Proceso: Ambientales	PROBABILIDAD	IMPACTO
Factores externos: lluvias, inundaciones, terremotos, tormentas, rayos, suciedad, humedad, calor.	ALTA	ALTA

Tabla 15: Riesgo Ambientales

Con respecto a este riesgo a este se le considera en sí el más importante por lo que cualquiera de este tipo de riesgos que sucedieran las consecuencias sería muy alta puesto que podrían suceder en cualquier momento puesto que son impredecibles.

4.3 Alternativas de solución para contrarrestar los ataques y minimizar el riesgo.

A continuación brindaremos algunas soluciones para contrarrestar y minimizar el riesgo que existe ante estos ataques y así poder controlar a los intrusos que existen internamente y externamente, para de esta forma disminuir el riesgo.

- **Firewalls (Cortafuegos):**

Un cortafuego (firewalls en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos.

Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets.

Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuego, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.

También es frecuente conectar a los cortafuegos a una tercera red, llamada Zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un cortafuego correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente.

- **Ventajas de un cortafuegos:**

  Bloquea el acceso a personas no autorizadas a redes privadas

- **Limitaciones de un cortafuego:**

  Las limitaciones se desprenden de la misma definición del cortafuego:

  Filtro de tráfico. Cualquier tipo de ataque informático que use tráfico aceptado por el cortafuego (por usar puertos TCP abiertos expresamente, por ejemplo) o que sencillamente no use la red,

seguirá constituyendo una amenaza. La siguiente lista muestra algunos de estos riesgos:

- ✓ Un cortafuego no puede proteger contra aquellos ataques cuyo tráfico no pase a través de él.
- ✓ El cortafuego no puede proteger de las amenazas a las que está sometido por ataques internos o usuarios negligentes.
- ✓ El cortafuego no puede prohibir a espías corporativos copiar datos sensibles en medios físicos de almacenamiento (discos, memorias, etc.) y sustraerlas del edificio.
- ✓ El cortafuego no puede proteger contra los ataques de ingeniería social.
- ✓ El cortafuego no puede proteger contra los ataques posibles a la red interna por virus informáticos a través de archivos y software.
- ✓ La solución real está en que la organización debe ser consciente en instalar software antivirus en cada máquina para protegerse de los virus que llegan por cualquier medio de almacenamiento u otra fuente.
- ✓ El cortafuego no protege de los fallos de seguridad de los servicios y protocolos cuyo tráfico esté permitido. Hay que configurar correctamente y cuidar la seguridad de los servicios que se publiquen en Internet.

(firewall1, 2004)

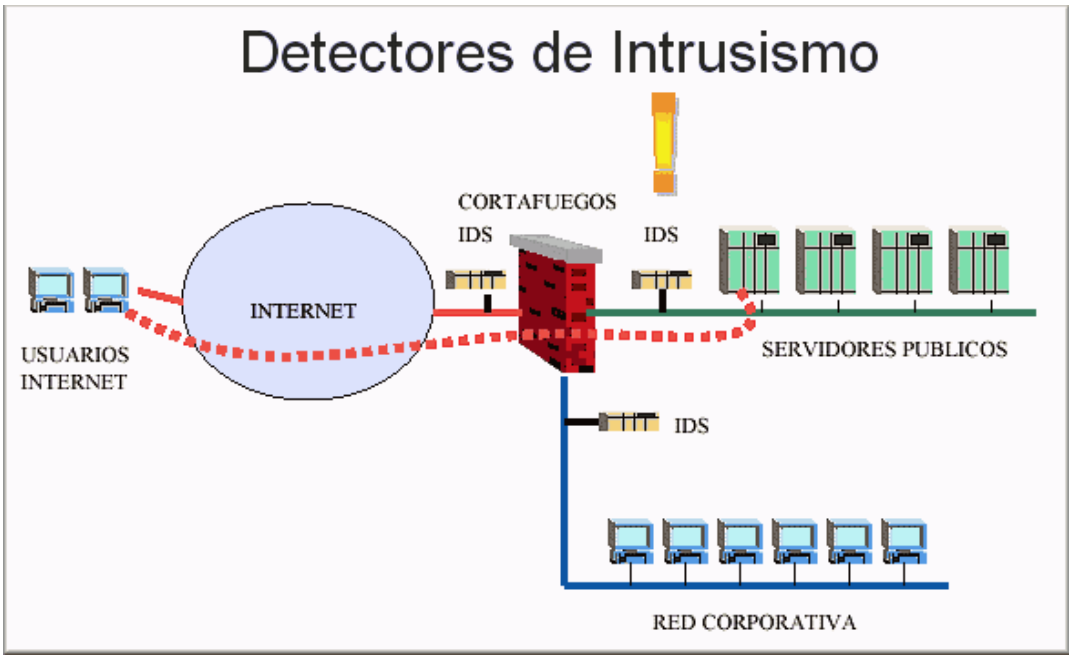


Imagen 6: Firewall / Cortafuegos

Si colocamos el IDS antes del cortafuego capturaremos todo el tráfico de entrada y salida de nuestra red. La posibilidad de falsas alarmas es grande.

La colocación detrás de los cortafuegos monitorizará todo el tráfico que no sea detectado y parado por el firewall o cortafuegos, por lo que será considerado como malicioso en un alto porcentaje de los casos.
La posibilidad de falsas alarmas muy inferior.

Algunos administradores de sistemas colocan dos IDS, uno delante y otro detrás del cortafuegos para obtener información exacta de los tipos de ataques que recibe nuestra red ya que si el cortafuegos está bien configurado puede parar o filtras muchos ataques.

En ambientes domésticos, que es el propósito de este taller sobre IDS y Snort, podemos colocar el IDS en la misma máquina que el cortafuego.

En este caso actúan en paralelo, es decir, el firewall detecta los paquetes y el IDS los analizaría. (Sistema de deteccion, 2011)

- **Proxies (o pasarelas):**

Es un ordenador que sirve de intermediario entre un navegador Web en Internet, el Proxy contribuye a la seguridad de la red**.**

Permiten dar seguridad y mejorar el acceso a páginas Web, conservándolas en la caché.

De este modo, cuando un usuario envía una petición para acceder a una página Web que está almacenada en la caché, la respuesta y el tiempo de visualización es más rápido.

Los servidores Proxy aumentan también la seguridad ya que pueden filtrar cierto contenido Web y programas maliciosos.

(kioskea, 2003)

Además de ocultar la dirección IP, un Proxy anónimo puede eliminar lo siguiente:

- Cookies
- Pop-ups
- Banners
- Scripts

- Información confidencial en los campos de texto (nombre de usuario y contraseña)

Imagen 7: El Proxy

- **Ventajas:**

  En general (no sólo en informática), los proxies hacen posibles varias cosas nuevas:

Control:	Sólo el intermediario hace el trabajo real, por tanto se pueden limitar y restringir los derechos de los usuarios, y dar permisos sólo al proxy.
Ahorro.	Por tanto, sólo *uno* de los usuarios (el proxy) ha de estar equipado para hacer el trabajo real.
Velocidad	Si varios clientes van a pedir el mismo recurso, el proxy puede hacer caché: guardar la respuesta de una petición para darla directamente cuando otro usuario la pida. Así no tiene que volver a contactar con el destino, y acaba más rápido.
Filtrado	El proxy puede negarse a responder algunas peticiones si detecta que están prohibidas.

Modificación	Como intermediario que es, un proxy puede falsificar información, o modificarla siguiendo un algoritmo.
Modificación	Anonimato. Si todos lo usuarios se identifican como uno sólo, es difícil que el recurso accedido pueda diferenciarlos. Pero esto puede ser malo, por ejemplo cuando hay que hacer necesariamente la identificación.

Cuadro 4: Ventajas de Proxy

(servidor-proxy, 2005)

- **Control de Acceso:**

Se utilizan para realizar la autenticación del usuario y sirven para proteger los datos y aplicaciones.

Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo.

Sin embargo cuando el usuario se ve en la necesidad de utilizar varias palabras clave para acceder a diversos sistemas encuentra dificultoso recordarlas y probablemente las escriba o elija palabras fácilmente deducibles, con lo que se ve disminuida la utilidad de esta técnica.

Se podrá, por años, seguir creando sistemas altamente seguros, pero en última instancia cada uno de ellos se romperá por este eslabón: la elección de passwords débiles.

Es mi deseo que después de la lectura del presente quede la idea útil de usar passwords seguras ya que aquí radican entre el 90% y 99% de los problemas de seguridad planteados.

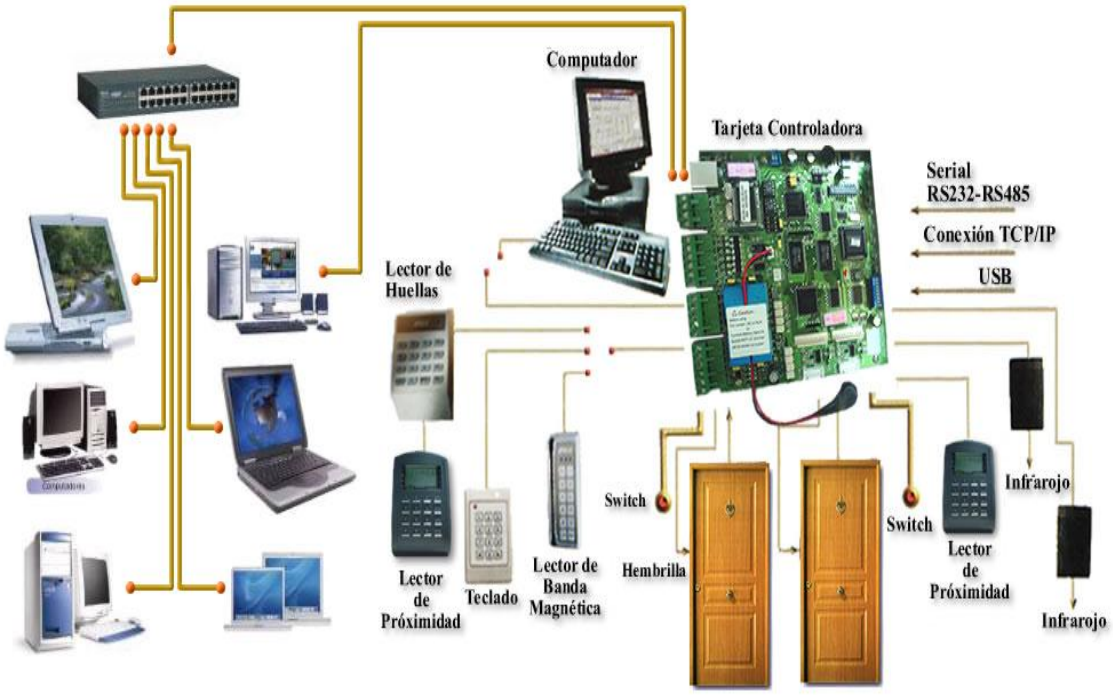


Imagen 8: Control de Acceso

También se puede utilizar lo siguiente:

- ✓ Utilización de Guardias
- ✓ Utilización de Detectores de Metales
- ✓ Utilización de Sistemas Biométricos
- ✓ Verificación Automática de Firmas (VAF)
- ✓ Seguridad con Animales
- ✓ Protección Electrónica

Imagen 9: Opciones de Control de Acceso

- **Router:**

Este dispositivo es de propósito General está diseñado para segmentar la red, con la función de limitar el tráfico de Brodcast y proporcionar más seguridad y control entre los dominios individuales de Brodcast, también para proporcionar servicio de firewall y un acceso a un servicio económico de WAN. (networking, 2010)

EL Router trabaja en la capa 3 del modelo OSI, el tuteador tiene dos funciones básicas:

- El Router lo q hace es escoger el mejor “camino” para empezar el envío, lo q se hace es mirar los siguientes factores:
  - velocidad de transmisión
  - trafico de la transmisión
  - seguridad de la transmisión
  - procedencia de transmisión
  - recepción de la transmisión
  - entre otros factores

- **Clasificación:**

Podemos clasificar a los routers en dos grandes grupos según su conectividad.

- **Según su conectividad**
  - Routers simples: sólo permiten un sistema MAC y un protocolo de red.
  - Router múltiple MAC: tienen puertos para distintos tipos de red. El funcionamiento de conectividad es el mismo ya que los Routers no utilizan el protocolo MAC.
  - Routers multiprotocolo: permiten enrutar diferentes protocolos (IP, IPX, etc.) de paquetes que llegan por cualquier puerto.
  - Routers multiprotocolo y múltiple MAC: combina los dos anteriores.

Imagen 10: Router

Consejos para evitar ataques
• Ser precavido con los mensajes de correo electronico en los que se te pide que idiques tus datos personales. • Lee con atencion los mensajes de correo electronico que parezcan sospechosos. • Protega la contraseña de su correo. • Tomar medidas • Ayude a identificar nuevos fraudes.

Cuadro 5: Consejos para evitar Ataques

Politicas, procedimientos y conciencia para prevenir ataques
Educar / Formar al usuario:
• Saber un poco de cultura de seguridad • Formatos potencialmente peligrosos • No abrir archivos no solicitados • Navegacion segura • Politicas de passwords • Copias de seguridad

Cuadro 6: Políticas, Procedimientos y conciencia para prevenir Ataques

4.4 Recomendaciones para evitar dichos ataques Tampering o Data Diddling:

A continuación brindaremos algunas recomendaciones para evitar ataques de la técnica Tampering o Data Diddling.

- **Instalación de antivirus**

➢ **Antivirus**:

Un antivirus es un programa que detecta, bloquea y elimina malware. Aunque se sigue utilizando la palabra antivirus, estos programas han evolucionado y son capaces de detectar y eliminar, no solo virus, sino también otros tipos de códigos maliciosos, mediante este tipo de codigos maliciosos pueden ingras a su computador.

Se recomienda tener siempre actualizado su Antivirus, porque de esa forma usted podra detectar algun daño malicioso dentro de sus equipos.

Ejemplos de antivirus:

Imagen 11: Los Antivirus

- **Limpiar mi ordenador de virus se recomienda:**

Cualquier PC puede infectarse de un virus informático si no se usa un buen programa de protección antivirus que vigile el sistema y las posibles entradas de estos programas indeseados.

Los antivirus harán un barrido de todos los ficheros de tu ordenador para ver indicaciones de posibles infecciones.

Cuando encuentra un virus, el software intentará limpiar el archivo o si no puede hacerlo, eliminarlo.

Es importante mantener actualizado tu antivirus. Se debería actualizar frecuentemente, es interesante que el fabricante de tu software, te envíe noticias sobre este tipo de actualizaciones, y si no es así, visitar su página Web para verlo nosotros.

No está de más instalarse un corta fuegos llamado en inglés “firewall”.

Con esto impediremos ataques externos mientras estemos conectados a Internet y sabremos qué es lo que accede a nuestro ordenador.

Un "firewall" gratuito bastante aconsejable es Zone labs**,** aunque también tiene una versión profesional de pago.

También tenemos que estar pendientes del llamado spyware, que son pequeños programas que se instalan sin nuestro consentimiento y que suelen vigilar nuestras rutinas de navegación por Internet.

Aconsejamos para esto, un programa gratuito y muy popular llamado ad-aware**.**

- **Cortafuegos:**
  - Es un programa para controlar las comunicaciones e impedir accesos no autorizados.
  - Instalar un cortafuegos correctamente es una de las medidas mas efectivas que podemos usar para protegernos.
  - Windows incluye un cortafuego muy sencillo pero efectivo pero se puede utilizar otros

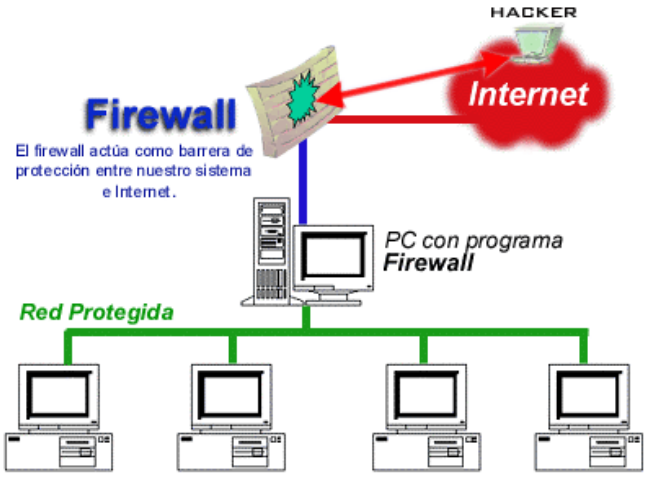


Imagen 12: Recomendaciones el Firewall / Cortafuegos

(firewall, 2008)

- **Copias de seguridad:**

  Los virus pueden dañar nuestros datos o incluso borrarlos. Las copias de seguridad son copias de todos los datos que permiten recuperar la información original.

  Una copia de seguridad consiste en copiar un archivo o un conjunto de archivos en un disco extraíble, por si los archivos en el ordenador son dañados.

  Para realizar copias de seguridad se pueden utilizar herramientas que traen los mismos sistemas operativos, programas específicos para esta función.

  - **Planificación:**

    La forma mas sencilla y barata de evitar la pérdida de los datos es llevar a cabo una planificacion periódica de copias de seguridad.

    - ✓ Por lo general se debería realizar:
    - ✓ Una copia de seguridad de los archivos nuevos.
    - ✓ Una copia mensual de toda la información del equipo.

    Existen diferentes formas de copiar la seguridad ya sea con herramientas del sistema o con DVD o discos externos.

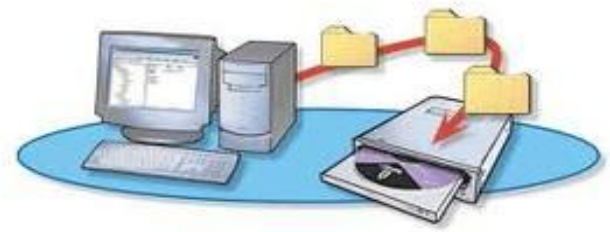


Imagen 13: Copias de Seguridad

- **Seguridad en internet**

  - **Cuidado con el E-mail**

El e-mail es una de las mayores fuentes de virus para el ordenador. Si no se conoce al remitente no se deben abrir los ficheros ya que muchos son malignos y se ocultan con la apriencia de ficheros graciosos.

Algunos ejemplos de e-mail peligroso son:

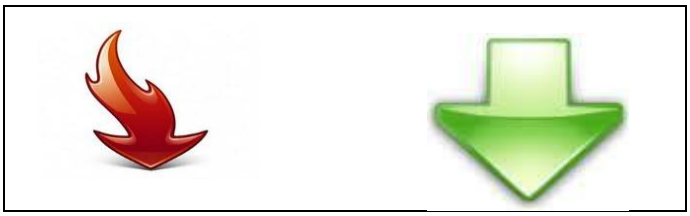
- ✓ Mensajes simulando ser entidades bancarias que solicitan claves al usuario.
- ✓ E-mail que contienen cadenas solidarias de ayuda o denuncia y acumulan direcciones de cientos de personas.
- ✓ Mensajes con archivos de usuarios desconocidos.
- ✓ Premios, bonos descuentos, viajes regalados, etc.

Imagen 14: Cuidado con los E- Mail

- **El riesgo de las descargas**

  Un ordenador queda infectado cuando se ejecuta algún archivo que tiene un virus, por lo tanto debemos usar las páginas webs oficiales para descargar.

  Programas como el Emule y demás son muy arriesgados ya que cualquiera puede renombrar un archivo con un virus y si no tienes un antivirus capaz de detenerlo el virus se instalará.



¿Descarga insegura **Descarga segura?**

Imagen 15: Las Descargas

- **Uso de criptografía.**

  La criptografía se utiliza para proteger la información enviada a través de Internet. La criptografía transforma la información del modo que sea incomprensible para receptores externos no autorizados.

Imagen 16: Uso de Criptografía

- **Proteger la conexión inalámbrica.**

  Si las conexiones inalámbricas no están protegidas cualquiera puede aprovechar para conectarse a Internet.

  Para evitarlo hay que tomar medidas como:

  - ✓ Cambiar la contraseña por defecto.
  - ✓ Usar encriptaciones WEP/WPA.
  - ✓ Usar filtrados de direcciones MAC.
  - ✓ Desactivar el DHCP.

Imagen 17: Proteger la conexión Inalámbrica

4.5 Implementar Herramientas de seguridad

4.5.1 Programas para la detención de intrusos:

En este punto del desarrollo realizaremos los paso a paso para la instalación y configuración de algunas recomendaciones que de dan para prevenir ataques de la Técnica Tampering o Data Diddling.

1. Multi Random Data Generator 1.0.0.0

Generador de múltiples datos aleatorios (MRDGen):

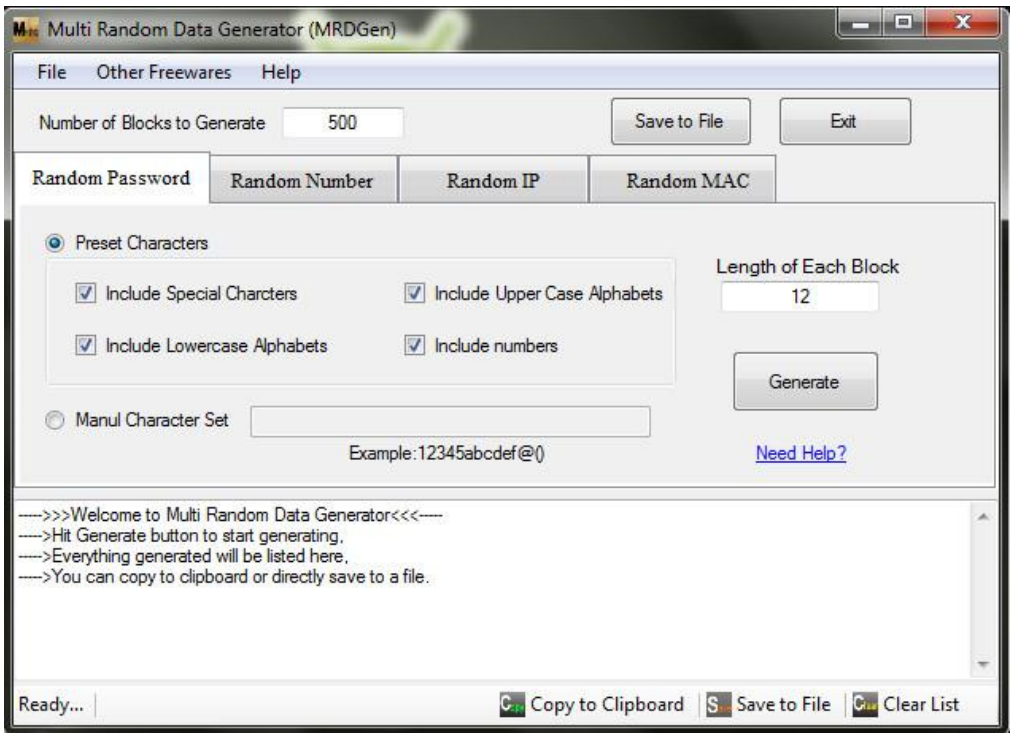


Imagen 18: Multi Random Data Generator (MRDGen)

Es una utilidad gratuita de Windows para generar datos aleatorios a gran velocidad.

Utilizando MRDGen puede generar datos tales como contraseñas, números, direcciones IP, direcciones MAC.

Muchos tipos de datos aleatorios se pueden generar utilizando MDRGen.

Link de descarga: (http://gratis.portalprogramas.com/Multi-Random-Data-Generator.html)

Tipos soportados actualmente son:

- Generador de contraseñas aleatorias con opción de seleccionar el conjunto de caracteres predefinidos o manual.
- Generador de números aleatorios con soporte para binarios, octales, la generación de números hexadecimales y decimales.
- IP al azar (Internet Protocol) del generador de direcciones con opciones para configurar cualquier octante de modo que se mantendrá constante en todos los bloques generados.
- Al azar MAC (Media Access Control) del generador de direcciones con opciones para configurar cualquier octante de modo que se mantendrá constante en todos los bloques generados.

Requisitos del sistema:

- Windows XP, Vista, 7 o superior, Linux,
- . Net Framework 3.5 o superior,

2. El Zone Alarm Free Firewall:

Es uno de los firewall más conocidos, además de firewall actúa como limpiador de spyware, de la página oficial te puedes bajar una versión gratuita y otra profesional por la que has de pagar, aquí tienes el enlace la versión gratuita

Este es link de descarga:

(**http://www.zonealarm.com/security/en/trialpay-za-signup.htm**)

- **Instalación:**

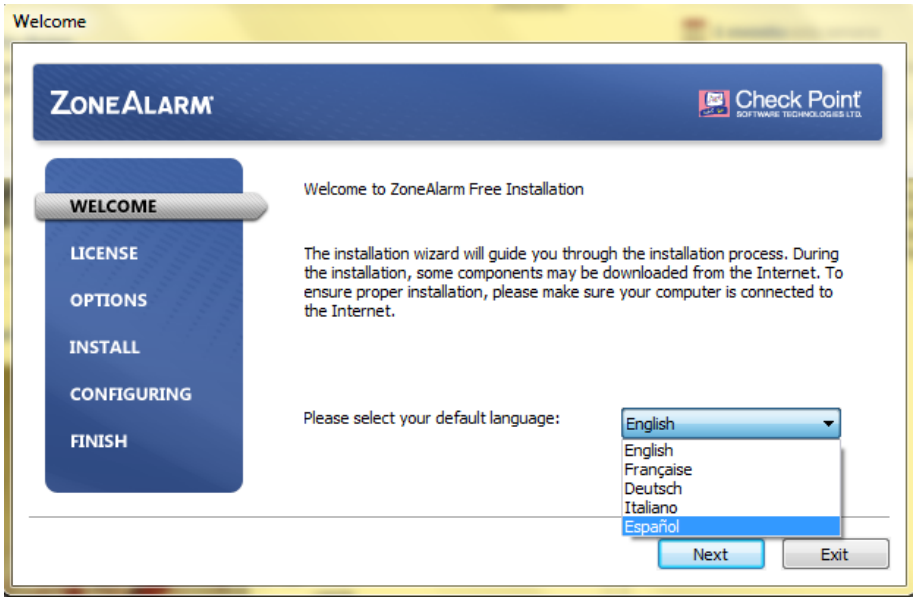


Imagen 19: Instalación de ZoneAlarm Bienvenida

Esta es la pantalla de inicio de la instalación en donde escogemos el idioma a instalar: Seleccionamos en español y luego Next.

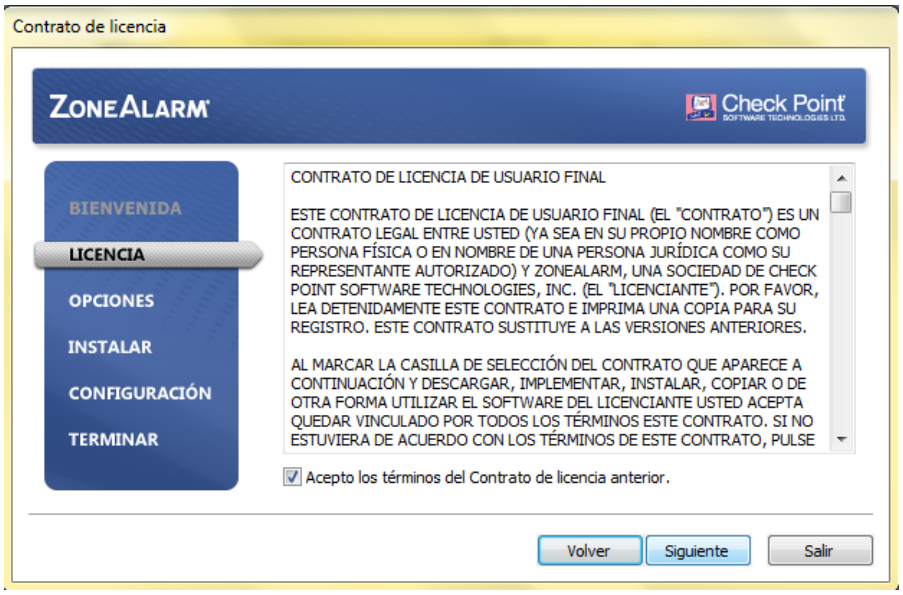


Imagen 20: Instalación de ZoneAlarm Licencia

Aceptamos los Términos d la licencia para que el programa funciono luego damos un clik en Siguiente

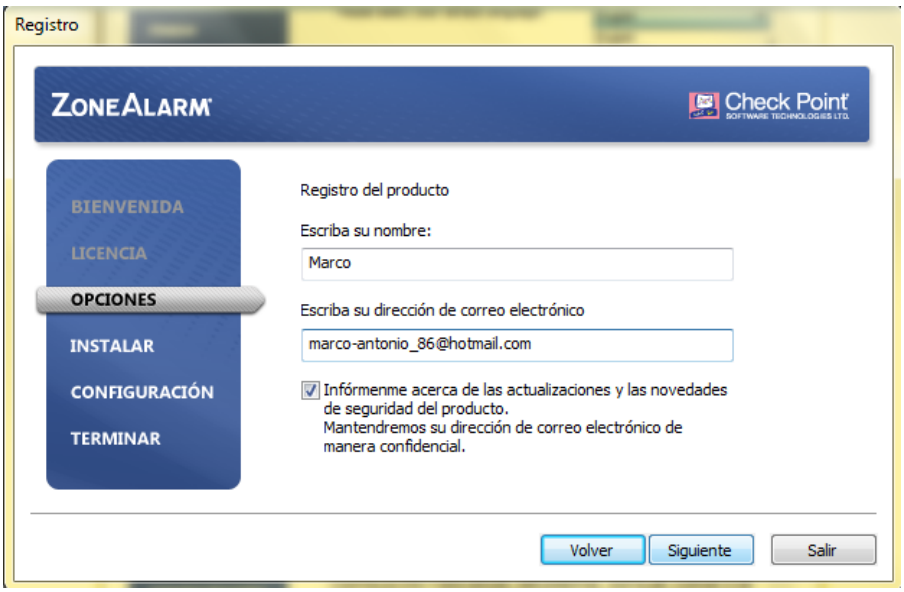


Imagen 21: Instalación de ZoneAlarm Opciones e ingreso de nombre y e-mail

Pantalla de registro debe introducir un nombre cualquiera y un mail verídico para seguir con la instalación.

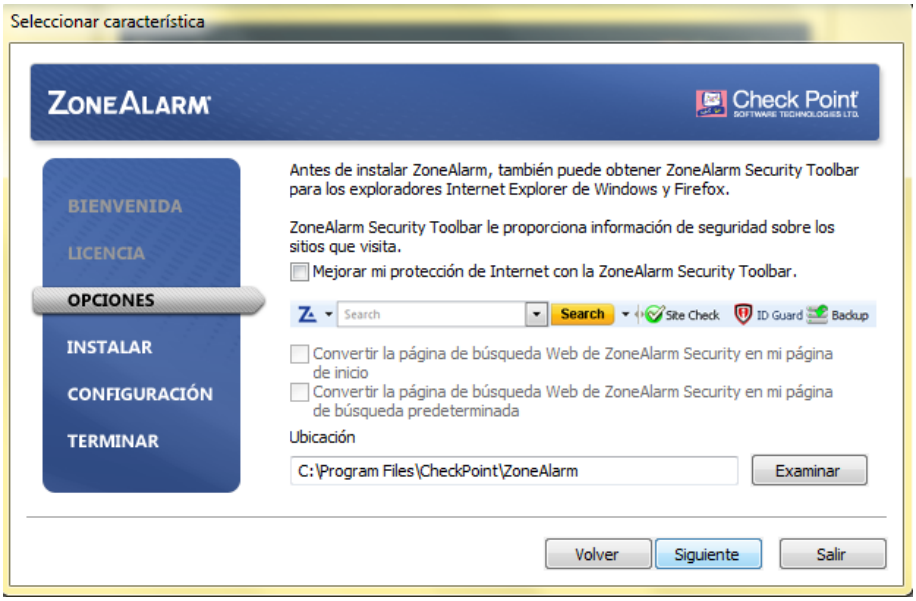


Imagen 22: Instalación de ZoneAlarm Ubicación de Instalación

Desactivamos las cajas de texto, revise bien la ubicación de donde se va a instalar el programa, y después damos click en siguiente.

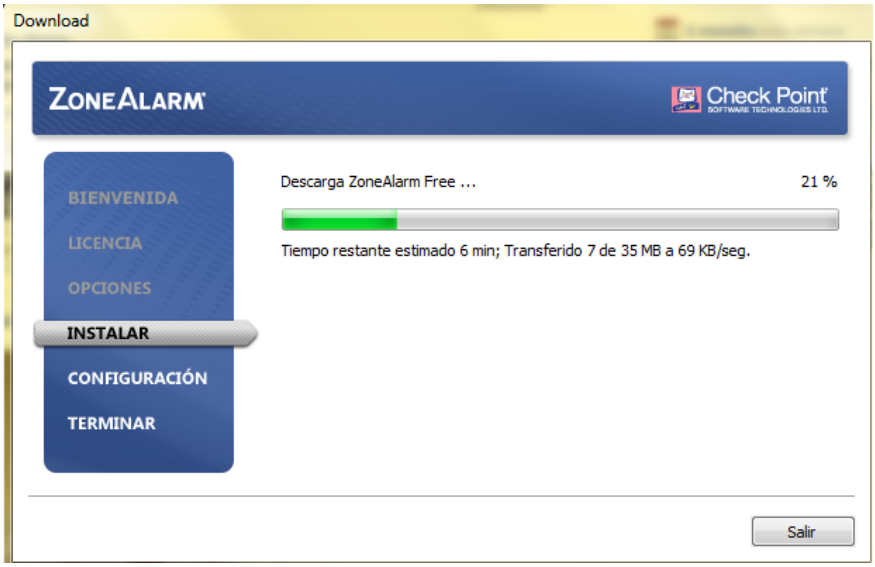


Imagen 23: Instalación de ZoneAlarm

Pantalla de instalación aquí se tardara varios minutos para su instalación respectiva, luego:

Imagen 24: Configuración de ZoneAlarm Licencia

A la pantalla de configuración de ZoneAlarm debe esperar que termine y casi culminaría con la instalación

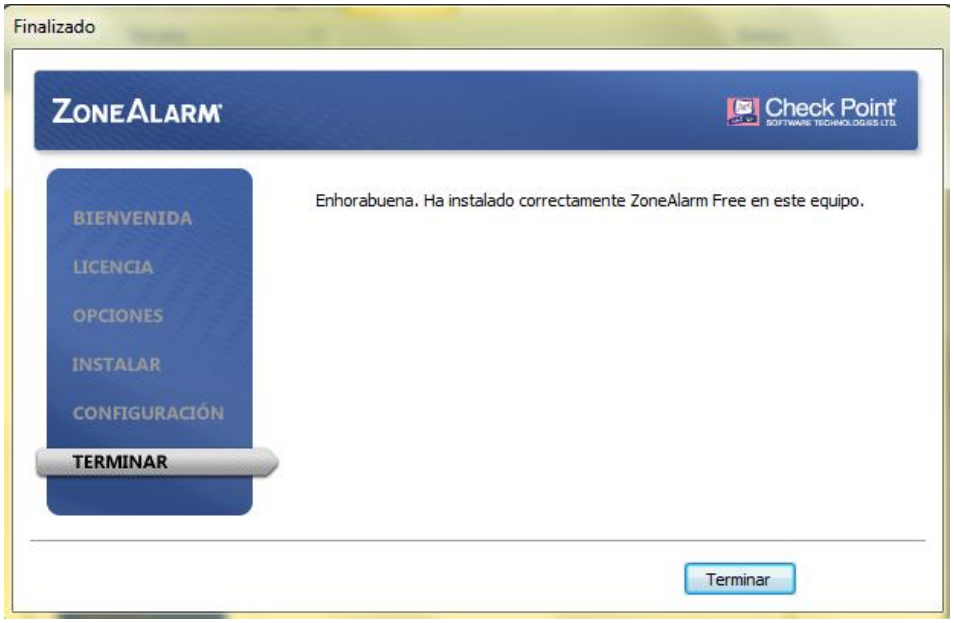


Imagen 25: Terminar ZoneAlarm

Fin de la instalación y automáticamente su equipo está YA protegido contra este tipo de ataques.

3. Cortafuegos o Firewall como mediadas de seguridad.

Opciones de configuración del firewall de Windows 7:

El firewall de Windows 7 tiene 3 configuraciones distintas para los 3 tipos de red:

- ✓ Red Dominio
- ✓ Red Pública
- ✓ Red doméstica o de trabajo (red privada)

Para acceder al firewall de Windows 7, podremos hacerlo desde:

- Inicio> Panel de Control > Sistema de Seguridad > Firewall de Windows

  Una vez dentro, veremos las opciones básicas para activar el firewall de Windows 7 o desactivarlo. El sistema nos permite modificar las opciones por defecto para cada tipo de conexión por separado, pudiendo bloquear todas las conexiones entrantes, desactivar el firewall de Windows 7, que nos notifique cuando bloquee una conexión.
- Cuando nos vallamos a conectar a una red con Windows 7, será cuando seleccionemos el tipo de red y la protección del Firewall.

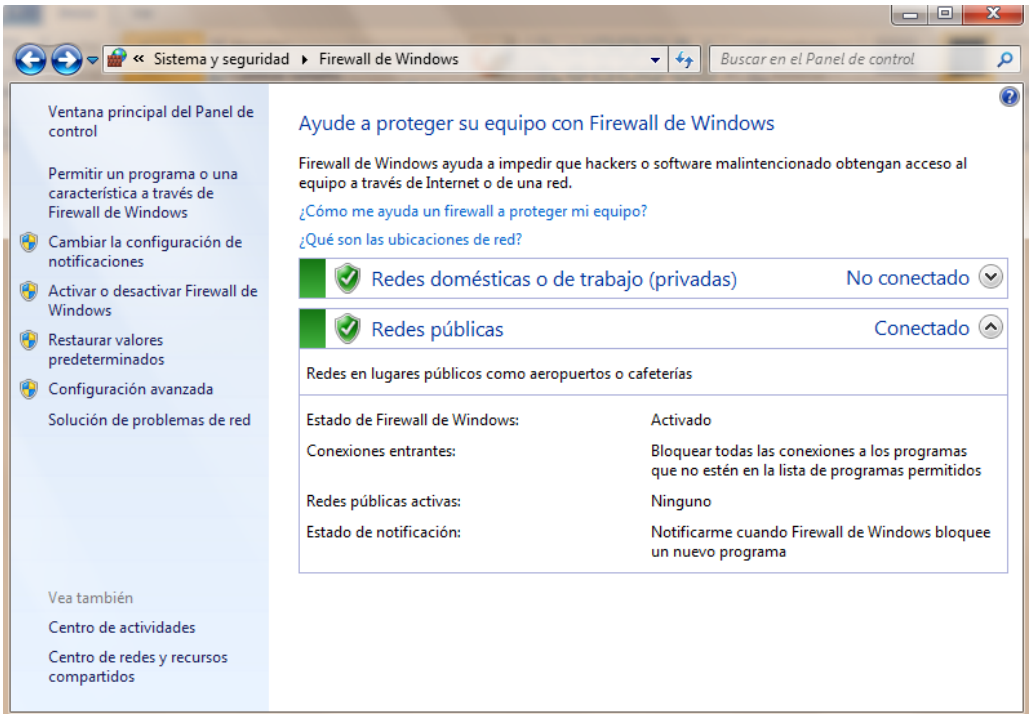


Imagen 26: Configuración del Cortafuegos Primero

- Las limitaciones de conectividad para los 3 tipos de redes en Windows 7, contemplan distintas condiciones de seguridad:
    - Red pública en Windows 7:
      Para este tipo de red, Windows 7 no permite que otros ordenadores puedan localizarnos para compartir recursos.
      Red doméstica en Windows 7:
    - Para este tipo de red, Windows 7:
      Permite que nos podamos conectar a redes del tipo "grupo en el hogar", pudiendo compartir recursos en Windows 7 y que serán públicos para el resto de la red.
      Red de trabajo en Windows 7:
    - En esta última situación, el firewall de Windows 7 no permite conectar a un grupo hogar, aunque si se puede compartir recursos con otros componentes de la red.

En las redes de trabajo, el firewall de Windows 7 permite acceder a la red mediante un dominio que podremos establecer en:

- Inicio > Panel de Control > Sistema de seguridad > Sistema > Configuración avanzada del sistema > Nombre del Equipo

Una vez estemos aquí, pulsaremos cambiar, y el controlador de dominio del Firewall reconocerá el modo de conexión de red dentro de un dominio.

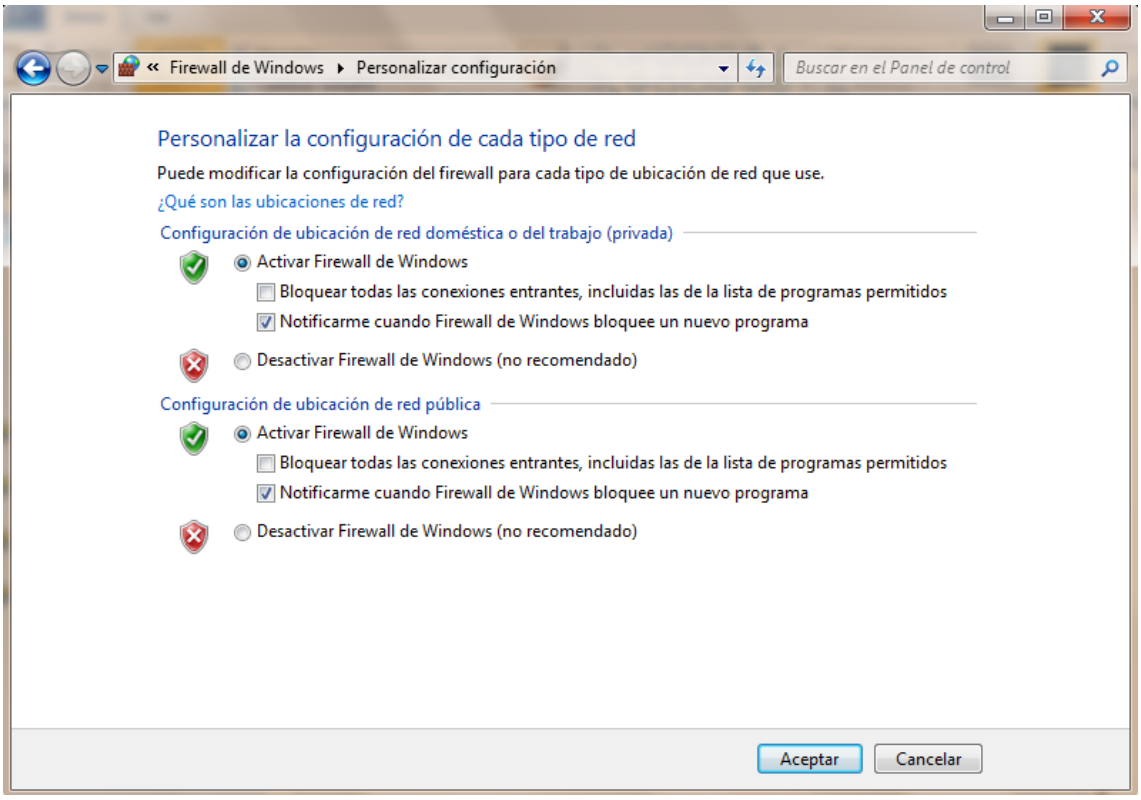


Imagen 27: Configuración del Cortafuegos Segundo

Una de las cosas que el firewall de Windows 7 ofrece, es la posibilidad de proteger 2 tipos de red al mismo tiempo, es decir, podemos crear dos redes distintas en Windows 7 y que la protección del firewall actúe por separado con respecto a cada red.

✓ Crear reglas de conexión en el firewall de Windows 7

- Otra de las funciones que encontraremos al configurar el firewall de Windows 7, es que podemos crear y acceder a las reglas de conexión para cada tipo de red.

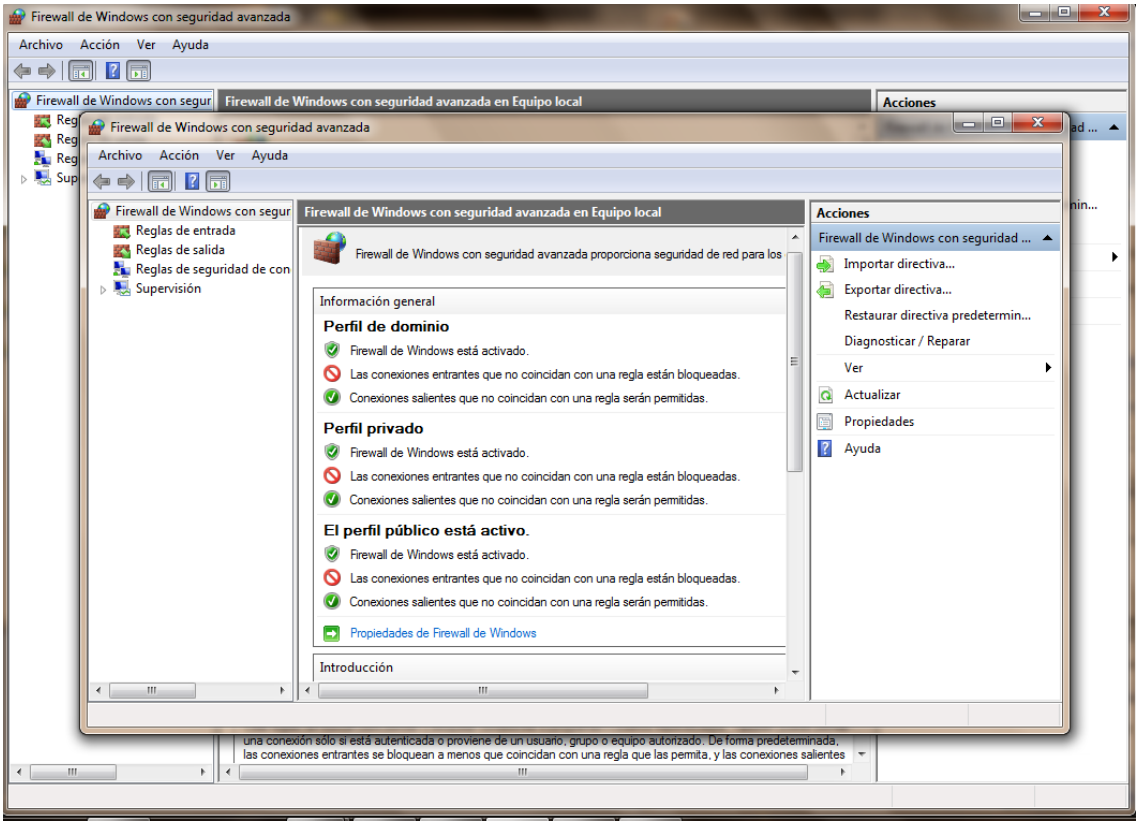


Imagen 28: Configuración del Cortafuegos Tercero

Podemos acceder a esta función desde la sección de Firewall de Panel de Control, y pulsando sobre Configuración Avanzada. Una vez dentro, podremos crear una regla de conexión como lo haríamos en el firewall de Vista.

En el centro de la ventana, pulsaremos sobre Ver y Crear reglas de firewall. Seguidamente sólo tendremos que seleccionar en Reglas de Entrada o Reglas de salida y especificar las características y parámetros para cada una de ellas.

El firewall de Windows 7 también ofrece una nueva función, y es que podemos definir un rango de puertos para las conexiones entrantes desde la misma consola con el que las conexiones entrantes deben de cumplir.

Registro de Eventos del firewall en Windows 7

- Cuando se produce una incidencia en el firewall de Windows 7, se crea un log o registro donde se almacena la actividad y bloqueos de conexiones entrantes por parte del firewall.

Para acceder al archivo de incidencias abriendo el Visor de eventos, sólo tenemos que ir a:

- Menú Inicio > Registro de aplicaciones y servicios > Microsoft > Windows > Windows Firewall Advanced Security

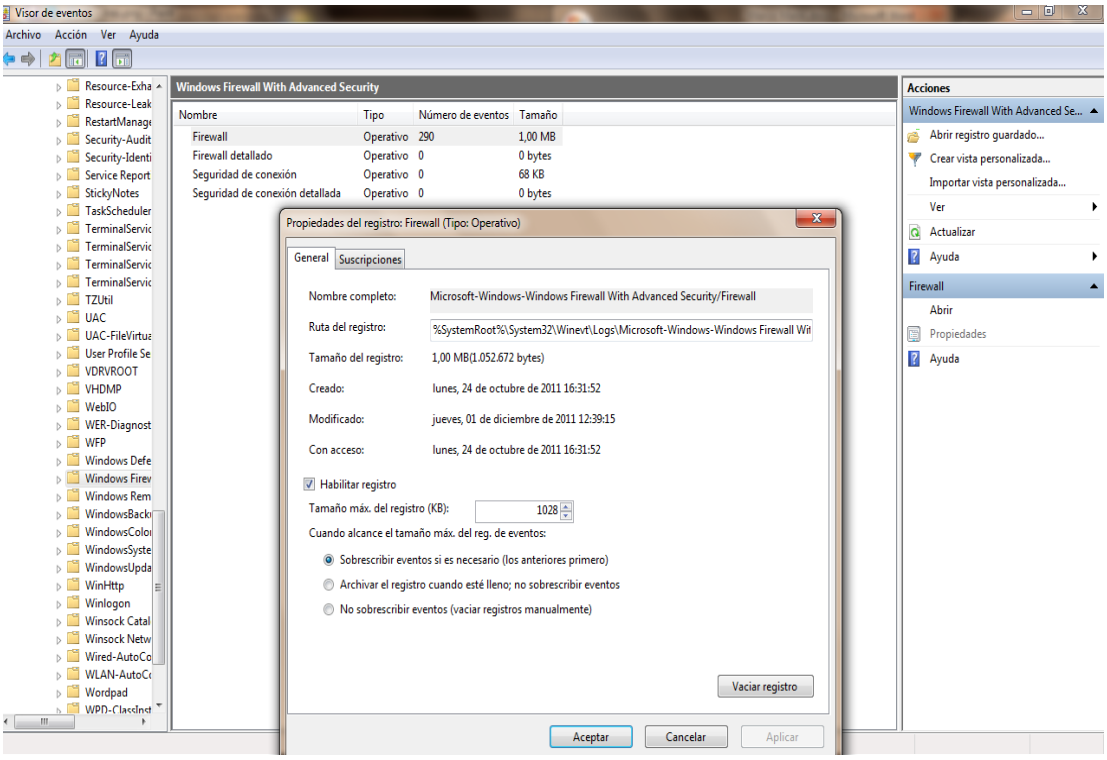


Imagen 29: Configuración del Cortafuegos Cuatro

- Una vez que logramos acceder a la entrada, podremos ver los eventos del firewall, filtrarlos, exportar el archivo, consultar los datos de cada evento, en si un mejor control de acceso a su computador, etc.

4. Como instalar Kaspersky Internet Security 2012:

Si ya instaló Kaspersky Internet Security 2012 y necesita activarlo, consulte nuestra página de activación de Kaspersky 2012.

Antes de comenzar:

Antes de instalar Kaspersky Internet Security 2012, asegúrese de haber quitado el software de seguridad anterior (incluidas las versiones anteriores de Kaspersky) en el Panel de control.

Si necesita ayuda para quitar los programas de seguridad instalados previamente, consulte nuestra lista de herramientas de eliminación de software conflictivo.

Si está realizando la instalación con el CD de Kaspersky Internet Security 2012, vaya al **Paso 2**.Si realizó una adquisición en línea, siga el **Paso 1** para descargar el software.

Paso 1: Guarde el archivo de instalación:

Si tiene una conexión de acceso telefónico a Internet, le sugerimos esperar a recibir el CD de copia de seguridad para realizar la instalación.

Para comenzar, haga clic en el vínculo de descarga proporcionado en el mensaje de correo electrónico de solicitud. Si el vínculo caducó, puede realizar la descarga desde nuestra página Actualizaciones del producto Kaspersky Internet Security.

Se le solicitará que ejecute, guarde o cancele la descarga. Haga clic en Guardar.

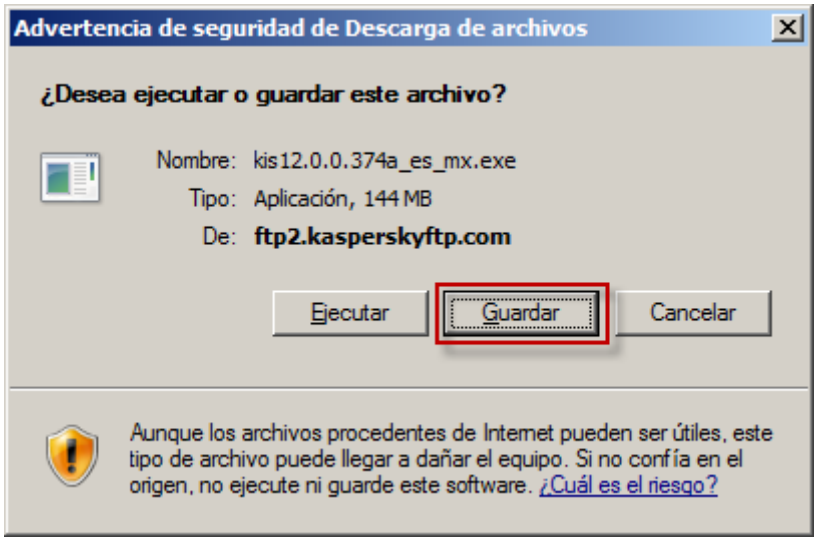


Imagen 30: Instalación de Kaspersky

A continuación, el navegador web le preguntará dónde guardar el archivo. Utilice el menú desplegable para seleccionar el Escritorio y, a continuación, haga clic en Guardar.

Comenzará el proceso de descarga. La velocidad de descarga varía según la conexión a Internet, pero puede tomar desde unos minutos hasta una hora.

Una vez completada la descarga, haga clic en Cerrar.

Cierre todas las ventanas abiertas excepto esta página web. Luego, ubique el archivo en el Escritorio y haga doble clic sobre él para iniciar el proceso de instalación.

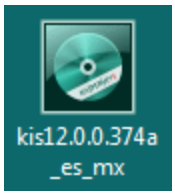


Imagen 31: Instalación de Kaspersky_ Logo

Si se le solicita que ejecute el archivo, haga clic en Ejecutar.

Imagen 32: Instalación de Kaspersky_ Ejecutar

Pasó 2: Proceso de instalación:

El proceso de instalación copiará rápidamente los archivos de instalación a su equipo.

El proceso de instalación comprobará si existe una versión nueva en línea y, si es necesario, le solicitará que la descargue.

Se abrirá el Asistente de instalación. Haga clic en Siguiente para iniciar la Instalación rápida..

Imagen 33: Instalación de Kaspersky_ Bienvenidos

Lea el Acuerdo de licencia de usuario final y haga clic en Acepto.

Lea la Declaración de recopilación de datos de Kaspersky Security Network. Esto nos permite detectar y recopilar virus nuevos según su comportamiento y datos no personales acerca de cómo usted utiliza el software. El Kaspersky Security Network no recopila ni procesa información personal. Haga clic en Instalar.

Al término de este paso, el firewall de Windows quedará deshabilitado. Kaspersky Internet Security 2012 incluye un firewall completo.

Es posible que, mientras Kaspersky está en proceso de instalación, aparezca una notificación del Centro de seguridad de Windows que indique que se produjo un problema. Esto es normal y se resolverá automáticamente una vez que el proceso haya finalizado.

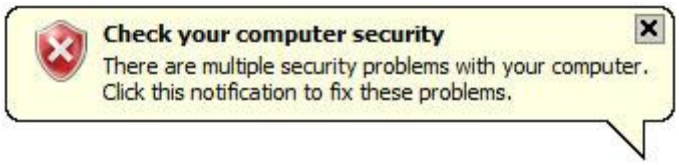


Imagen 34: Error normal de Windows para la Instalación de Kaspersky

Pasó 3: Asistente de configuración:

Si Kaspersky no estaba instalado en su equipo o si su licencia anterior caducó, se le solicitará que active una licencia comercial. Escriba el código de activación de 20 caracteres, que está compuesto por cuatro grupos de cinco caracteres, es decir: XXXXX-XXXXX-XXXXX-XXXXX.

El asistente pondrá las letras y los guiones en mayúsculas de manera automática. Haga clic en Siguiente.

Puede encontrar el código de activación en el mensaje de correo electrónico de solicitud, en el envoltorio del CD o en la tarjeta de activación que se incluye en el estuche del DVD.Si el asistente detecta una licencia válida, no se le solicita la activación.

Si debe realizar la activación una vez que la instalación haya finalizado, siga estos pasos para activar Kaspersky Internet Security 2012.

Espere mientras el asistente activa Kaspersky Internet Security 2011.

Una vez que la licencia esté activada, verá el tipo de licencia y su fecha de caducidad. Haga clic en Siguiente.

Imagen 35: Instalación de Kaspersky_ Método de Activación

A continuación, el asistente comprobará los archivos de Windows y establecerá niveles para cada aplicación para la función Control de aplicaciones.

Haga clic en Finalizar para comenzar a utilizar Kaspersky Internet Security 2012.

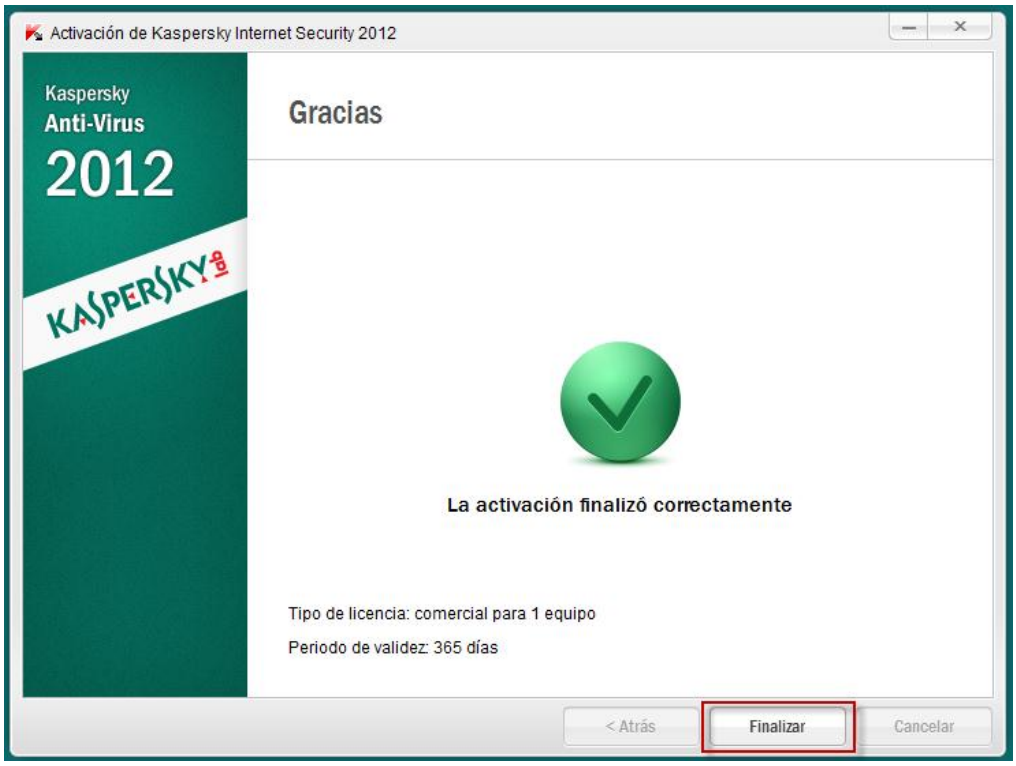


Imagen 36: Instalación de Kaspersky_ Finalizar

Una vez que el programa esté instalado y se haya iniciado, le recomendamos realizar las siguientes operaciones:

- **Actualizar las bases de datos.**

Para esto, haga clic en Actualizar, a la izquierda y, luego, en Ejecutar actualización, a la derecha de la ventana principal.

- **Comprobar que el equipo esté protegido.**

El color de la barra horizontal y la luz ubicada en la parte superior de la ventana principal del programa indican el estado de protección del equipo:

- **Verde:**

  El equipo está protegido.

- **Amarillo y rojo:**

  El equipo está en riesgo.

Analizar el equipo en busca de virus.

Kaspersky le recomienda realizar un análisis completo del equipo.

Haga clic en Analizar, a la izquierda de la ventana principal y, a continuación, en Ejecutar análisis completo, a la derecha.

5. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES:

Durante el desarrollo de este trabajo se puedo conocer algunos puntos entre ellos cual es el grado de conocimientos de personas y de empresas sobre delitos informáticos, seguridad informática, en donde la seguridad y prevenciones son las que sobresalen en este trabajo. Donde tanto internos o externos informáticos se concluye que: la información obtenida por estas personas con o sin conocimiento utilizan sus habilidades para acceder y provocar enormes problemas económicos dentro de la empresa o a personas comunes, estos ataques son para alterar, destruir y apropiarse de la información de las empresas.

Se concluyó también que los antivirus, cortafuegos, y copias de seguridad representan la principal forma de protección ante ataques.

El promedio mensual de ataques recibidos es elevado, ocasionando en la mayoría casos daños leves.

La mayoría de los administradores de la red no logran reconocer los ataques proporcionados por intrusos informáticos debido a lo difícil que resulta rastrear sus huellas, resultando el diagnóstico de un antivirus o software experto la principal forma de detección de virus y de ataques, a pesar de esto la mayoría de los ataques se detecta cuando ya se ha causado un daño.

5.2 RECOMENDACIONES:

Las siguientes sugerencias surgen de las necesidades observadas en el proceso de análisis de resultados de esta investigación, están dirigidas a los dueños de empresas y a personas normales.

Las recomendaciones propuestas consisten en crear políticas de seguridad de información basadas en:

Mantener vigentes los conocimientos sobre nuevos riesgos y amenazas que afectan la información de la empresa, a través de talleres de capacitación. Los mismos deben incluir las últimas vulnerabilidades encontradas en los sistemas operativos y diferentes las aplicaciones Microsoft.

Mantener actualizada las versiones de los antivirus así como las definiciones de los virus.

Instalar los Service Packs necesarios a las aplicaciones y sistemas señalados por la Corporación Microsoft.

Mantener respaldos de información periódicos y actualizados de diferentes tipos, para minimizar el impacto de la empresa al enfrentar desastres informáticos.

Preparar y realizar talleres de capacitación sobre las amenazas y riesgos utilizando lenguaje sencillo a los trabajadores de empresas, a fin de minimizar puntos débiles en las redes.

GLOSARIO

- **Ataque:** Cualquier acción deliberada con el objetivo de violar los mecanismos de seguridad de un sistema de información.
- **Autenticidad:** Aseguramiento de la identidad u origen.
- **Certificación:** Confirmación del resultado de una evaluación y de que los criterios de la evaluación utilizados fueron correctamente aplicados.
- **Confidencialidad:** Aseguramiento de que la información es accesible sólo por aquellos autorizados a tener acceso.
- **Degradación:** Pérdida de valor de un activo como consecuencia de la materialización de una amenaza.
- **Disponibilidad:** Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y a sus activos asociados.
- **Evento de seguridad:** Momento en que la amenaza existe y pone en riesgo activos, procedimientos o información.
- **Evaluación de Medidas de Seguridad:** Evaluación de las medidas de seguridad existentes con relación al riesgo que enfrentan.
- **Frecuencia:** Tasa de ocurrencia de una amenaza
- **Impacto:** Consecuencia que sobre un activo tiene la materialización de una amenaza.
- **Insiders:** Empleado desleal quien por motivos de desinterés, falta de capacidad intelectual y/o analítica, problemas psicológicos o psiquiátricos, corrupción, colusión u otros provoca daños en forma deliberada en la empresa en que trabaja, incumpliendo conscientemente con normas y procedimientos establecidos, robando o hurtando activos (físicos o información) con objetivos económicos o simplemente de daño deliberado.

- **Integridad:** Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.
- **Mapa de riesgos:** Relación de las amenazas a que están expuestos los activos.
- **Plan de seguridad:** Conjunto de programas de seguridad que permiten materializar las decisiones de gestión de riesgos.
- **Riesgo:** Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños y / o perjuicios a la Organización.
- **Seguridad:** Capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.
- **Sistema de información:** Computadoras y redes de comunicaciones electrónicas, datos electrónicos almacenados, procesados, recuperados o transmitidos por los mismos para su operación, uso, protección y mantenimiento.
    - Conjunto de elementos físicos, lógicos, elementos de comunicación, datos y personal que permiten el almacenamiento, transmisión y proceso de la información.
- **Vulnerabilidad**: Cálculo o estimación de la exposición efectiva de un activo a una amenaza. Se determina por dos medidas: frecuencia de ocurrencia y degradación causada.

- **Robo:** Delito que se comete apoderándose con ánimo de lucro de una cosa mueble ajena, empleándose violencia o intimidación sobre las personas, o fuerza en las cosas
- **Fraude:** Acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete
- **Fraude informático:** Cualquier cambio no autorizado y malicioso de datos o informaciones contenidos en un sistema informático
- **Robo informático:** Delito contra el patrimonio, consistente en el apoderamiento de bienes ajenos usando sistemas informáticos
- **Red**: Posiblemente oiremos la expresión anglosajona “network”, la cual es un grupo de ordenadores conectados entre si que permite que la información sea intercambiada entre ellos.
- **Nodo**: Podemos entender un nodo como cualquier cosa que esté conectado a la red. Aunque normalmente se entiende un nodo como un ordenador o un Router, puede ser también una **impresora** u otro elemento que se puede compartir en una red.
- **Segmento:** Un segmento es una porción de la red que está separada por un switch, un bridge o un router, de otras partes de la red.
- **Delito Informático:** Delito cometido utilizando un PC; también se entiende por delito informático cualquier ataque contra un sistema de PC's.
- **Phishing:** Tipo de delito encuadrado dentro del ámbito de las estafas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial.

- **Spam:** Se llama Spam, correo basura o SMS basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming.
- **Spyware:** Software que se instala en una computadora para recopilar información sobre las actividades realizadas en ella.
- **Firewall:** Elemento utilizado en redes de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas.
- **Paquete:** Un paquete es un pequeño bloque de datos transmitido en una red de conmutación de paquetes.
- **Criptología:** Ciencia que estudia el arte de crear y utilizar sistemas de encriptación.
- **Firma Digital:** Información añadida o transformación cifrada de los datos que permite al receptor de los mismos comprobar su fuente e integridad y protegerse así de la suplantación o falsificación.

BIBLIOGRAFIA

ataques. (22 de 1 de 2011). Obtenido de http://business.ftc.gov/documents/sbus69-como-proteger-la-informacion-personal-una-gui-para-negocios
canal-ayuda. (05 de 1 de 2010). Recuperado el 20 de 11 de 2011, de http://www.canal-ayuda.org/a-seguridad/seguridadin.htm
Chiavenato. (2006). Teoria General. [1]: «Introducción a la Teoría General de la Administración», Séptima Edición, de Chiavenato Idalberto, McGraw-Hill Interamericana, 2006, Pág. 110.
Deleitos. (9 de 5 de 2008). Recuperado el 4 de 9 de 2011, de www.slideshare.net
eumed. (15 de 2 de 2009). Recuperado el 22 de 10 de 2011, de http://www.eumed.net/grumetes/evitarvirus.htm
firewall. (22 de 01 de 2008). Recuperado el 15 de 11 de 2011, de http://www.segu-info.com.ar/firewall/firewall.htm
firewall1. (19 de 1 de 2004). Recuperado el 22 de 9 de 2011, de http://www.zonagratuita.com/servicios/seguridad/firewall.html
Geoffery, F. O. (2004). Negocios. [1]: «Introducción a la Teoría General de la Administración», Séptima Edición, de Chiavenato Idalberto, McGraw-Hill Interamericana, 2006, Pág. 110.
Global Knowledge. (2008).
kioskea. (27 de 2 de 2003). Recuperado el 11 de 9 de 2011, de http://es.kioskea.net/faq/2755-que-es-un-proxy
Marin, M. (2011). Patente nº 001. Ecudor.
modificacion. (3 de 11 de 2011). Obtenido de http://www.segu-info.com.ar/ataques/ataques_modificacion.htm
networking. (04 de 6 de 2010). Recuperado el 17 de 08 de 2011, de http: //kimleymajim.blogspot.com/2010/que-es-networking.html
Netzweb. (24 de 5 de 2011). Recuperado el Septiembre de 2011, de http://www.netzweb.net/html/text/segurid/intro.php
seguridad informatica. (1 de 11 de 2011). Obtenido de http://www.monografias.com/trabajos16/seguridad-informatica/seguridad-informatica.shtml
servidor-proxy. (9 de 8 de 2005). Recuperado el 24 de 11 de 2011, de http://es.kioskea.net/faq/2755-que-es-un-proxy
Sistema de deteccion. (29 de 11 de 2011). Obtenido de http://www.wikilearning.com/tutorial/taller_de_sistemas_de_deteccion_de_intrusiones_snort/4735-6
tampering. (10 de 03 de 2004). Recuperado el 15 de 11 de 2011, de http://es.scribd.com/doc/49893078/49/TAMPERING O DATA DIDDLING
Wifi. (2 de 11 de 2011). Obtenido de http://culturacion.com/2009/11/ventajas-y-desventajas-del-wifi/
http://www.slideshare.net/marinoi/seguridad-informtica-1125964
http://www.derechoecuador.com/index.php?option=com_content&task=view&id=3091&Itemid=426
http://www.netzweb.net/html/print/segurid/met_ata.pdf
http://culturacion.com/2009/11/ventajas-y-desventajas-del-wifi/
http://www.cabinas.net/informatica/analisis_riesgos_informaticos.asp

RAMIREZ, TULIO (1.999). Como hacer un proyecto de Investigación.
Mc Graw, Gill (2000). Los Hackers.
II Congreso Mundial De La Informática.
http://www.segu-info.com.ar/firewall/firewall.htm
http://es.kioskea.net/faq/2755-que-es-un-proxy
http://www.ibiblio.org/pub/linux/docs/LuCaS/Manuales-LuCAS/doc-como-seguridad-fisica/html_out/eledifici.html
http://comunidad.dragonjar.org/f182/intro-routers-y-switches-7996/