# CAPITULO 1

## 1. INTRODUCCIÓN

Desde la consolidación de Internet como medio de interconexión global, los incidentes de seguridad relacionados con sistemas informáticos vienen incrementándose de manera alarmante. Este hecho, unido a la progresiva dependencia de la mayoría de organizaciones hacia sus sistemas de información, viene provocando una creciente necesidad de implantar mecanismos de protección que reduzcan al mínimo los riesgos asociados a los incidentes de seguridad.

Para ello destacaremos la conveniencia de afrontar su análisis mediante una aproximación de gestión, concretamente con un enfoque de gestión del riesgo. Para completar esta visión introductoria a la seguridad informática, mencionaremos las amenazas y las contramedidas más frecuentes que deberían considerarse en toda organización.

La seguridad informática, de igual forma como sucede con la seguridad aplicada a otros entornos, trata de minimizar los riesgos asociados al acceso y utilización de determinado sistema de forma no autorizada y en general malintencionada. Esta visión de la seguridad informática implica la necesidad de gestión, fundamentalmente gestión del riesgo.

Para ello, se deben evaluar y cuantificar los bienes a proteger, y en función de estos análisis, implantar medidas preventivas y correctivas que eliminen los riegos asociados o que los reduzcan hasta niveles manejables.

En la actualidad se denomina hackers de una forma corriente para referirse mayormente a los piratas informáticos, los criminales se le pueden sumar los llamados *"script kiddies"*, gente que invade computadoras, usando programas escritos por otros, y que tiene muy poco conocimiento sobre cómo funcionan.

Mientras que los hackers aficionados reconocen los tres tipos de hackers y los hackers de la seguridad informática aceptan todos los usos del término, los hackers del software libre consideran la referencia a intrusión informática como un uso incorrecto de la palabra, y se refieren a los que rompen los sistemas de seguridad como *"crackers"*.

En el presente desarrollo abordaremos la metodología de la investigación, seguridad informática y los hackers, métodos comunes de ataques y manual de procedimientos. Donde se da a conocer todo los temas relevantes y necesarios para el proceso de análisis de la seguridad informática.

El criterio personal sobre el tema lo expondré en las conclusiones y recomendaciones.

## 1.1. Tema de investigación (resultado de la problematización)

Análisis de la seguridad informática, sobre los ataques de hackers y como protegerse ante los mismos dentro de una empresa u organización.

## 1.2. Planteamiento del problema

¿El estudio de seguridad informática hackers permitirá implementar seguridad para los sistemas, porque dentro del mundo empresarial diversas

empresas sufren de ataques de Hackers, los cuales son perjudiciales para la economía de la misma?

## 1.3. Antecedentes

Desde que se usó por primera vez la palabra Hacker, más o menos hace 13 años, ésta ha sido mal utilizada, mal interpretada y encasillada en un contexto errado, antes que nada, aclaremos que el termino Hacker no tiene nada que ver con actividades delictivas, si bien muchos Hackers cometen errores, la definición no tiene nada que ver con ello.

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 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.

Los protocolos de comunicación utilizados carecen (en su mayoría) de seguridad o esta ha sido implementada en forma de "parche" tiempo después de su creación.

- Existen agujeros de seguridad en los sistemas operativos.
- Existen agujeros de seguridad en las aplicaciones.
- Existen errores en las configuraciones de los sistemas.
- Los usuarios carecen de información respecto al tema.

Esta lista podría seguir extendiéndose a medida que se evalúen mayor cantidad de elementos de un Sistema Informático.

Las empresas u organizaciones no se pueden permitir el lujo de denunciar ataques a sus sistemas, pues el nivel de confianza de los clientes (ciudadanos) bajaría enormemente.

Los Administradores tienen cada vez mayor conciencia respecto de la seguridad de sus sistemas y arreglan por sí mismos las deficiencias detectadas. A esto hay que añadir las nuevas herramientas de seguridad disponibles en el mercado.

## 1.4. Diagnóstico o planteamiento de la problemática general

### 1.4.1. Causa - Efectos

Los empresarios no poseen de conocimiento de métodos y herramientas más comunes que se utilizan hoy para perpetrar ataques a la seguridad informática.

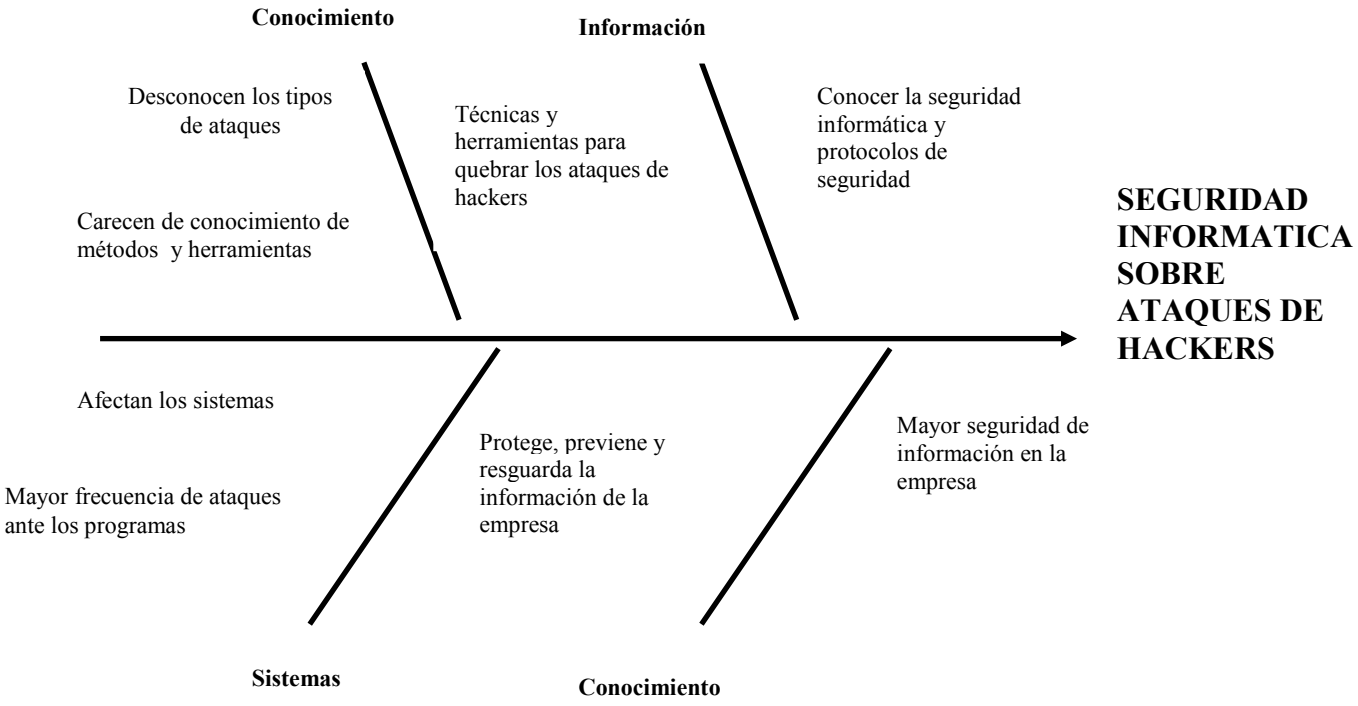


**Imagen nro 1 espina de Pescado**

Dentro del mundo empresarial desconocen los tipos de ataques de hackers de igual manera carecen de conocimiento de métodos y técnicas lo cual afecta la seguridad de los sistemas además son más susceptibles a robo, ataques, perdida o daño. Lo referente a conocimiento de técnicas y herramientas para quebrar los ataques de hackers protegen, previene y resguarda la información de la empresa. Todo lo concerniente a conocimiento

de seguridad informática y protocolos brinda seguridad de información a la empresa

## 1.5. Pronóstico y Control del Pronóstico

### Pronóstico

Los hackers tienen acceso a la red empresarial para modificar, sustraer o borrar datos y cuya pérdida puede afectar el buen funcionamiento de la empresa u organización

### Control del Pronóstico

Se pretende dar a conocer a la sociedad (empresas) las diversas maneras de protegerse ante los hackers. Conocer cómo protegerse de dichos ataques perjudiciales de los hackers. La manera de evitar seria informarse y saber cómo atacan los hackers. Es decir, conocer los métodos, estrategias y herramientas que utilizan para introducirse a nuestros sitios web de información.

## 1.6. Formulación de la Problemática Específica

### 1.6.1. Problema principal

¿El estudio de seguridad informática hackers permitirá implementar seguridad para los sistemas, porque dentro del mundo empresarial diversas empresas sufren de ataques de Hackers, los cuales son perjudiciales para la economía de la misma?

### 1.6.2. Problemas secundarios

- Las empresas u organizaciones desconocen los diferentes tipos de ataques de hackers que afectan a los sistemas.

- Los empresarios no poseen de conocimiento de métodos y herramientas más comunes que se utilizan hoy para perpetrar ataques a la seguridad informática.

- Desconocen las diversas técnicas para quebrar los ataques de hackers y cómo proteger la información ante los mismos.

## 1.7. Objetivos

### 1.7.1. Objetivo General

Análisis de la seguridad informática, sobre los ataques de hackers y como protegerse ante los mismos dentro de una empresa u organización.

### 1.7.2. Objetivos Específicos

1. Identificar los diferentes tipos de ataques de hackers que afectan a las empresas u organizaciones.

2. Recopilar información de métodos y herramientas que utilizan para los ataques de los hackers.

3. Averiguar diversas técnicas para quebrar los ataques de hackers.

4. Valorar cuales son los métodos más comunes que se utilizan hoy para perpetrar ataques a la seguridad informática.

**5.** Elaborar un manual de procedimientos para proteger la información ante los hackers.

## 1.8. Justificación

### 1.8.1. Teórica

Proteger la información para no ser presa de esta nueva ola de ataques más sutiles, por lo tanto se recomienda mantener las soluciones activadas y actualizadas, evitar realizar operaciones comerciales en computadoras de uso público. Y verificar los archivos adjuntos de mensajes sospechosos y evitar su descarga en caso de duda de datos dentro de la empresa u organización.

### 1.8.2. Metodológica

La seguridad informática indispensable dentro del ámbito laboral. Se ha convertido en uno de los elementos más importantes. La seguridad informática debe ser administrada según los criterios establecidos por los administradores y supervisores, evitando que usuarios externos y no autorizados puedan acceder a ella sin autorización.

### 1.8.3. Práctica

Conocer diversas técnicas para quebrar los ataques de hackers. El grado de ansiedad de las empresas y el importe que deben invertir en seguridad informática son objeto de un acalorado debate. Y ese debate refleja en parte una división en la cultura de Internet entre el genio pirata del pasado, cuando el estado subvencionaba la Red y la información se intercambiaba libremente, y el genio comercial de la Internet de hoy.

# CAPÍTULO 2

# 2. Marco de Referencia

## 2.1. Marco Teórico o conceptual

### 2.1.1. Seguridad informática

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

Consecuentemente, muchas organizaciones gubernamentales y no gubernamentales internacionales han desarrollado documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones con el objeto de obtener el mayor provecho de estas ventajas, y evitar el uso indebido de la mismas. Esto puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

En este sentido, las políticas de seguridad informática (PSI) surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información y servicios críticos que favorecen el desarrollo de la organización y su buen funcionamiento.

Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas.

### 2.1.2. ¿ Por qué es tan importante la seguridad?

Por la existencia de personas ajenas a la información, conocidas como piratas informáticos o hackers, que buscan tener acceso a la red empresarial para modificar, sustraer o borrar datos.

Tales personajes pueden, incluso, formar parte del personal administrativo o de sistemas, de cualquier compañía; de acuerdo con expertos en el área, más de 70 por ciento de las violaciones e intrusiones a los recursos informáticos se realiza por el personal interno, debido a que éste conoce los procesos, metodologías y tiene acceso a la información sensible de su empresa, es decir, a todos aquellos datos cuya pérdida puede afectar el buen funcionamiento de la organización.

Recuperado de:http://www.ciberhabitat.gob.mx/museo/cerquita/redes/seguridad/intro.htm

### 2.1.3. Errores y omisiones

Los errores de los empleados al utilizar los sistemas pueden comprometer la integridad de la información que maneja la organización. Ni siquiera las aplicaciones más sofisticadas están libres de este tipo de problemas, que pueden reducirse con refuerzos en controles de integridad de los datos y con un adiestramiento adecuado del personal.

Muchas veces, simples errores pueden comprometer no únicamente la integridad de los datos, sino incluso puede que causen la aparición de nuevas vulnerabilidades en los sistemas.

Este tipo de amenazas es si cabe más relevante en las empresas que se dedican al sector de las nuevas tecnologías, desarrollando e implantando sistemas, muchas veces interconectados entre diversas organizaciones.

Un simple error de programación, en la administración, o la carencia de la formación necesaria para evaluar las implicaciones de seguridad de determinada aproximación de desarrollo, pueden causar vulnerabilidades que afecten no únicamente a las organizaciones usuarias de los sistemas.

Recuperado de; http://web.iti.upv.es/actualidadtic/2003/07/2003-07-seguridad.pdf

**2.1.4. Tipos de hackers:**

### *2.1.4.1. Black hats o hackers negros*

El Hacker negro muestra sus habilidades en informática rompiendo computadoras, colapsando servidores, entrando a zonas restringidas, infectando redes o apoderándose de ellas, entre otras muchas cosas utilizando sus destrezas en métodos Hacking.

### *2.1.4.2. White hats o hackers blancos*

El Hacker Blanco es una persona que busca los bugs de los sistemas informáticos, por decir así de una manera genérica, dando a conocer a las compañías desarrolladoras de software o empresas sus vulnerabilidades, claro sin ánimo de perjudicar. Sin embargo hay algunos de ellos que si buscan el interés personal, queriendo entrar a sitios restringidos, estafando... etc.

### *2.1.4.3. Lammer o Script-Kiddies*

Es un término coloquial inglés aplicado a una persona falta de madurez, sociabilidad y habilidades técnicas o inteligencia, un incompetente, que por lo general pretenden hacer hacking sin tener conocimientos de informática. Solo se dedican a buscar y descargar programas de hacking para luego ejecutarlos, como resultado de la ejecución de los programas descargados estos pueden terminar colapsando sus sistemas por lo potaje general destrozando su plataforma en la que trabajan.

### *2.1.4.4. Luser (looser + user)*

Es un término utilizado por hackers para referirse a los usuarios comunes, de manera despectiva y como burla. "Luser", que generalmente se encuentra en desventaja frente a los usuarios expertos (hackers), quienes pueden controlar todos los aspectos de un sistema.

#### *2.1.4.5. Phreaker*

De phone freak ("monstruo telefónico. Son personas con conocimientos tanto en teléfonos modulares (TM) como en teléfonos móviles, se encuentran sumergidos en entendimientos de telecomunicaciones bastante amplios. Por lo general trabajan en el mercado negro de celulares, desbloqueando, clonando o programando nuevamente los celulares robados.

#### *2.1.4.6. Newbie*

La palabra es una probable corrupción de new boy, arquetipo del "niño nuevo", que debido a la falta de interacciones socioculturales, queda vulnerable a varios tipos de abusos por parte de los otros. Son los hacker novatos, se introducen en sistemas de fácil acceso y fracasan en muchos intentos, sólo con el objetivo de aprender las técnicas que puedan hacer de él, un hacker reconocido, se dedica a leer, escuchar, ver y probar las distintas técnicas que va aprendiendo.

### *2.1.4.7. Pirata Informático / "Delincuente informático"*

Este personaje dedicado a la copia y distribución de software ilegal, tanto software comercial crackeado, como shareware registrado, etc, de una manera consciente o inconsciente uno se convierte en un pirata informático descargando programas, juegos, música,

### *2.1.4.8. Samurai*

Son lo más parecido a una amenaza pura. Sabe lo que busca, donde encontrarlo y cómo lograrlo. Hace su trabajo por encargo y a cambio de dinero, no tienen conciencia de comunidad y no forman parte de los clanes reconocidos por los hackers.

### *2.1.4.8. Trashing ("Basurero")*

Obtienen información en cubos de basura, tal como números de tarjetas de crédito, contraseñas, directorios o recibos.

#### *2.1.4.9. Wannaber*

Desea ser hacker pero estos consideran que su coeficiente no da para tal fin. A pesar de su actitud positiva difícilmente consiga avanzar en sus propósitos.

Recuperado de: http://www.taringa.net/posts/info/1852601/Tipos-de-Hacker.html

### 2.1.5. Programas para protegerse contra los hackers

#### *2.1.5.1. Programas de Antivirus*

Si usted ha utilizado computadoras por varios años, puede ser que haya sido testigo de las consecuencias de lo que significa tener un “virus” informático en la computadora. Un virus es un programa diseñado especialmente para propagarse de computadora en computadoras “infectándolas” a todas en su paso.

Regularmente los virus vienen adjuntos a archivos que han sido infectados y se propagan causando daños que en la mayoría de los casos son catastróficos (por ejemplo: borrando información en el disco duro, paralizando

la ejecución de la computadora y provocando la pérdida de mucho dinero invertido en la restauración de servicios y en la productividad).

#### *2.1.5.2. Programas Antiespías*

Los programas espías (spyware) son aquellos que una vez instalados pueden recopilar y mandar información (archivos, claves, información personal acerca del usuario, etc.) a otras computadoras sin el conocimiento o permiso del usuario o sistema en el cual residen.

Muchos de estos programas son famosos por causar que el computador trabaje de forma lenta y disparatada; así como la aparición de incómodas “ventanas emergentes” (pop-up windows) las cuales suelen ser utilizadas con el objetivo de mostrar avisos de manera intrusiva.

### *2.1.5.3. Programas Cortafuegos Personales*

La función de los programas cortafuegos personales (personal firewalls o desktop firewalls) es limitar, controlar o parar el tránsito de información entre la computadora en el cual residen y todos aquellas computadoras o equipos que se comunican con ella.

### *2.1.5.4. Medidas de Seguridad en General*

Es un constante trabajo mantenerse libre de las amenazas de los programas e individuos maliciosos que constantemente azotan la Internet; nosotros mismos debemos de desarrollar y ejercer buen sentido común para prevenir y detectar el peligro. Dos de los mejores consejos que uno puede seguir para evitar estas amenazas son:

- Nunca habrá un correo electrónico con enlaces a sitios en la Internet o archivo adjunto que provenga de personas que no conozca, lo que tiene que hacer es eliminarlo inmediatamente. Si conoce a la persona pero no esperaba el mensaje o duda de su contenido, verifique la veracidad del mensaje contactando a la persona que se lo envió; más vale prevenir que tener que lamentarse.

- Mantenga al día su computadora con todos los parches (patches) nuevos tanto como para el sistema operativo así como para los otros programas que residen en la computadora.

### *2.1.5.5. Como proteger la información personal*

Los **hackers** tienen la capacidad de provocar el caos mediante el **robo** de **datos personales**. Pero el **robo** se puede prevenir si la gente tiene cuidado con su información.

La primera línea de defensa son siempre sus contraseñas y la información de su computadora. Asegúrense de que su equipo esté perfectamente seguro, primero un buen antivirus como Kaspersky por ejemplo hará que su PC sea más segura, cambiar la información de registro y las contraseñas en todo, desde sus cuentas de tarjetas de crédito hasta su correo electrónico.

Los **hackers** están llegando de todas partes. Traten de no usar las mismas contraseñas para todo, más bien todas deben de ser diferentes.

Traten de usar solo una computadora para realizar sus transacciones bancarias. Sé que es difícil, especialmente los que usan dispositivos diferentes. Pero traten de hacerlo todo en un solo equipo.

Recuperado de: http://tecnologia21.com/proteger-su-informacion-personal-hackers

### 2.1.6. Programas utilizados por hackers

#### *2.1.6.1. Trojan horse programs*

Es la forma más común para engañarte en instalar programas “back door”. Permiten acceso a tu computadora sin tu conocimiento. Puede cambiar la configuración de esta o infectar el sistema con un virus.

#### *2.1.6.2. Back door y Programas de administración*

En computadoras que utilizan Windows, las tres herramientas mayormente utilizados por intrusos para entrar a los sistemas son: BackOrifice, Netbus, and SubSeven. Una vez instalados permiten acceder y controlar la computadora.

#### *2.1.6.3. Negar el servicio*

Otra forma de atacar se conoce como el ataque DOS (denial-of-service). Este ataque causa que la computadora este tan ocupada procesando data que no la puedas utilizar. Además de atacar su sistema también es posible que sea participante en el ataque a otro sistema.

#### *2.1.6.4. Intermediario para otro ataque*

Los intrusos frecuentemente utilizan una computadora como intermediario para atacar varias computadoras a la vez.

#### *2.1.6.5. Código Móvil (Java/JavaScript/ActiveX)*

Se han reportado problemas con lo que se conoce como código móvil. Estos son los lenguajes que permiten a los desarrolladores de páginas crear códigos que serán ejecutados en el navegador. Los códigos son bien útiles, sin embargo pueden ser utilizados por los intrusos para recopilar información.

#### *2.1.6.6. Cross-site scripting*

Un desarrollador malicioso de redes puede adjuntar un código a una página de red, puede ser un URL, cuando esa pagina abra ese código malicioso es transferido al navegador.

#### *2.1.6.7. Packetsniffing*

Es un programa que obtiene data de mientras viaja por la red. Esa data puede incluir nombres de usuarios, contraseñas, etc. Con cientos o miles de contraseñas en manos del intruso este puede lanzar ataques en los sistemas.

Recuperado de: http://www.sg.inter.edu/acc/prMIS104/bravof/pag-05.htm

Recuperado de: http://www.portalhacker.net/hacker/programas-hacker.php

## 2.2. Marco Conceptual

### 2.2.1. Seguridad informática

La seguridad informática se ha convertido en un aspecto muy importante dentro de una empresa u organización, dada por las nuevas plataformas de computación disponibles. Es por ello que existen nuevas amenazas en los sistemas computarizados.

La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. También garantiza los recursos informáticos de una empresa para que estén disponibles para cumplir sus propósitos, es decir, que no estén dañados o alterados por circunstancias o factores externos.

### 2.2.2. ¿ Por qué es tan importante la seguridad?

Es importante la seguridad porque existen piratas informáticos los cuales buscan el acceso a la red ya sea para modificar, sustraer o borrar datos. Las violaciones a los recursos informáticos en la mayoría de los casos se realizan por el personal interno, por lo que conoce la información de la empresa y la

pérdida de información puede afectar el buen funcionamiento de la organización.

#### 2.2.3. Errores y omisiones

Los errores no pueden afectar solo a la información sino directamente a los sistemas. Por lo que un simple error de programación, puede causar vulnerabilidades que afecten no única solo a las organizaciones usuarias de los sistemas, sino también a las propias empresas que los desarrollan que se podrían ver muy perjudicadas en su imagen corporativa.

#### 2.2.4. Tipos de hackers:

***Black hats o hackers negros***

El Hacker negro colapsa servidores, entra a zonas restringidas, infecta redes y utiliza sus destrezas en métodos Hacking.

**White hats o hackers blancos**

El Hacker Blanco busca bugs de los sistemas, dando a conocer a las compañías desarrolladoras de software, quieren entrar a sitios restringidos, estafando... etc.

**Lammer o Script-Kiddies**

Hace hacking sin tener conocimiento de informática. Solo se dedican a buscar y descargar programas de hacking para luego ejecutarlos.

**Luser (looser + user)**

Son usuarios comunes, se encuentra en desventaja frente a los usuarios expertos (hackers), quienes controlan todos los aspectos de un sistema.

**Phreaker**

Tienen conocimientos tanto en teléfonos modulares y teléfonos móviles, también trabajan en el mercado negro programando celulares robados.

**Newbie**

También conocido como new boy, son los hacker novatos, se introducen en sistemas de fácil acceso y fracasan en muchos intentos.

**Pirata Informático / "Delincuente informático"**

Se dedica a la copia y distribución de software ilegal, así como software comercial crackeado, como shareware registrado, etc. Uno se convierte en un pirata informático de una manera consciente o inconsciente.

**Samurai**

Son igual a una amenaza pura porque saben lo que busca, donde encontrarlo y cómo lograrlo. Hace su trabajo por encargo y dinero, no tienen conciencia con la sociedad.

**Trashing ("Basurero")**

Sacan información en cubos de basura, tal como números de tarjetas de crédito, contraseñas, directorios o recibos.

**Wannaber**

Desea ser hacker pero estos consideran que su coeficiente no da para tal fin. A pesar de su actitud positiva difícilmente consiga avanzar en sus propósitos.

### 2.2.5. Programas para protegerse contra los hackers

**Programas de Antivirus**

Un virus es un programa que se propaga de computadora en computadoras “infectándolas” a todas en su paso y que generalmente vienen adjuntos a archivos que han sido infectados.

**Programas Antiespías**

Los programas (spyware) pueden recopilar y mandar información (archivos, claves, información personal acerca del usuario, etc.) a otras computadoras sin el conocimiento o permiso del usuario o sistema.

**Programas Cortafuegos Personales**

La función de los programas cortafuegos personales es limitar, controlar o parar el tránsito de información.

### 2.2.6. Programas utilizados por hackers

**Trojan horse programs**

El programa “back door” permite acceso a tu computadora sin tu conocimiento.

**Back door y Programas de administración**

En Windows, utilizan estas herramientas para entrar a los sistemas BackOrifice, Netbus, and SubSeven.

**Negar el servicio**

Este ataque causa que la computadora este tan ocupada procesando data que no la puedas utilizar.

**Intermediario para otro ataque**

Los intrusos utilizan una computadora como intermediario para atacar varias computadoras a la vez.

**Código Móvil (Java/JavaScript/ActiveX)**

Lenguaje que permiten a los desarrolladores de páginas crear códigos que serán bien útiles, estos pueden ser utilizados por los intrusos para recopilar información.

**Cross-site scripting**

Desarrollador malicioso puede adjuntar un código a una página de red, puede ser un URL.

**Packetsniffing**

Obtiene data mientras viaja por la red. Esa data puede incluir nombres de usuarios, contraseñas, etc.

## 2.3. Marco Espacial

Estudio de seguridad informática hackers permitirá implementar seguridad para los sistemas, porque dentro del mundo empresarial diversas empresas sufren de ataques de Hackers, los cuales son perjudiciales para la economía de la misma, también es de vital importancia conocer un manual de procedimientos para tener en cuenta las precauciones al momento de utilizar un correo electrónico, el internet, al realizar una operación, etc.

# CAPÍTULO 3

## 3. Metodología de investigación

### 3.1. Unidad de análisis

La seguridad informática indispensable dentro del ámbito laboral se ha convertido en uno de los elementos más importantes, por lo que debe ser administrada según los criterios establecidos por los administradores y supervisores, evitando que usuarios externos y no autorizados puedan acceder a ella sin autorización.

Dentro del mundo empresarial desconocen las tipos de ataques de hackers de igual manera carecen de conocimiento de métodos y técnicas lo cual afectan la seguridad de los sistemas además son más susceptible a robo, ataques, perdida o daño. Lo referente a conocimiento de técnicas y herramientas para quebrar los ataques de hackers protege, previene y resguarda la información de la empresa. Todo lo concerniente a conocimiento de seguridad informática y protocolos brinda seguridad de información en la empresa.

## 3.2. Tipo de Investigación

En el desarrollo del análisis se aplicara la metodología analítica y descriptiva, porque me permite investigar, definir y analizar sobre hackers y seguridad informática. Porque dentro de la investigación descriptiva consiste en llegar a conocer las situaciones, costumbres y actitudes de las actividades, objetos, procesos y personas. Y también porque tiene como objetivo analizar un evento y comprenderlo en término de sus aspectos menos evidentes.

**En la etapa de análisis aplicaremos la metodología analítica.-** Porque tiene como objetivo analizar un evento y comprenderlo en término de sus aspectos menos evidentes.

Es un procedimiento más complejo con respecto a investigación descriptiva, que consiste fundamentalmente en establecer la comparación de variables entre grupos de estudio y el control sin aplicar o manipular las variables, estudiando estas según se dan naturalmente en los grupos.

**En la etapa de análisis aplicaremos la metodología descriptiva.-** Porque tiene como objetivo central lograr la descripción o caracterización de un evento de estudio dentro de un contexto.

Se refiere a la etapa preparatoria del trabajo científico que permite ordenar el resultado de las observaciones de las conductas, las características, los factores, los procedimientos y otras variables de fenómenos y hechos.

**Objetivo de la metodología descriptiva**

El objetivo de la investigación descriptiva consiste en llegar a conocer las situaciones, costumbres y actitudes predominantes a través de la descripción exacta de las actividades, objetos, procesos y personas. Su meta no se limita a la recolección de datos, sino a la predicción e identificación de las relaciones que existen entre dos o más variables. Los investigadores no son meros tabuladores, sino que recogen los datos sobre la base de una hipótesis o teoría, exponen y resumen la información de manera cuidadosa y luego analizan minuciosamente los resultados.

Estas metodologías son utilizadas dentro de la investigación con respecto a la marco de referencia y especialmente en la metodología, porque tienen el fin de extraer generalizaciones significativas que contribuyan al conocimiento.

## 3.3. Métodos

La metodología que voy a utilizar para el desarrollo del análisis es la Metodología Propositiva y Descriptiva.

### 3.3.1. Metodología Descriptiva.

Es descriptiva porque voy a recopilar información, realizar investigaciones bibliográficas, para el desarrollo del análisis.

### 3.3.2. Metodología Propositiva.

Porque luego de un proceso de descripción, se realizará un manual de procedimientos para proteger la información ante los hackers.

## 3.4. Técnicas de investigación

### 3.4.1. Observación

Esta técnica me ayudará a determinar la información, observar la misma, interpretarla y registrarla la información mas relevante e importante para el desarrollo del presente análisis.

### 3.4.2. Investigación bibliográfica.

Se utilizará esta técnica por lo que está destinado a obtener información de la web, textos, libros en donde se tendrá que analizar los documentos encontrados.

#### 3.4.3. Instrumentos

- Fichas textuales.
- Fichas de observación
- Internet.
- Software

| Autor | Editorial |
|---|---|

| | |
|---|---|
| Titulo.<br>Autor | Ciudad |
| Tema. …… | |
| 1er edición | Ficha nro. 1 |

**Imagen. Nro 2 Fichas Textuales**

| |
|---|
| FICHA DE OBSERVACIÓN |
| Nombre:<br>Dirección:<br>Editorial |
| Tema. …… |
| Edición Ficha nro. 1 |

**Imagen nro 3 ficha de observación**

# CAPÍTULO 4

# 4. DESARROLLO

## 4.1. Seguridad informática y los hackers

### 4.1.1. Definición de la seguridad informática

La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) sean utilizados de la manera más apropiada y que el acceso a la información allí contenida así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

La seguridad informática garantiza que los recursos informáticos de una compañía estén disponibles para cumplir sus propósitos, es decir aquellas reglas técnicas y 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.

### 4.1.2. Importancia de la seguridad informática

La seguridad informática es importante por la existencia de personas ajenas a la información, conocidas como piratas informáticos o hackers, que buscan el acceso a la red empresarial para modificar, sustraer o borrar datos.

Más del 70 por ciento de las violaciones e intrusiones a los recursos informáticos se realiza por el personal interno, administrativo o de sistemas, debido a que éste conoce los procesos, metodologías y tiene acceso a la información sensible de su empresa, es decir, a todos aquellos datos cuya pérdida puede afectar el buen funcionamiento de la empresa.

El resultado es la violación de los sistemas, provocando la pérdida o modificación de los datos sensibles de la organización, lo que puede representar un daño con valor de miles o millones de dólares.

### 4.1.3. Características de seguridad.

- **Integridad:** La información producida es de calidad porque no puede ser modificada por quien no está autorizado.

- **Confidencialidad:** La información solo debe ser legible para los autorizados, la misma debe llegar a destino con la cantidad y calidad con que fue prevista.

- **Disponibilidad:** la información debe estar disponible cuando se la necesita.

- **Irrefutabilidad:** (No-Rechazo o No Repudio) Que no se pueda negar la autoría de quien provee de dicha información.

### 4.1.4. Objetivo de la seguridad informática.

El objetivo de la seguridad informática es proteger los recursos informáticos valiosos de la organización, tales como la información, el hardware o el software. A través de la adopción de las medidas adecuadas, la seguridad informática ayuda a la organización cumplir sus objetivos, protegiendo sus recursos financieros, sus

sistemas, su reputación, su situación legal, y otros bienes tanto tangibles como inmateriales.

Desafortunadamente, en ocasiones se ve a la seguridad informática como algo que dificulta la consecución de los propios objetivos de la organización, imponiendo normas y procedimientos rígidos a los usuarios, a los sistemas y a los gestores. Sin embargo debe verse a la seguridad informática, no como un objetivo en sí mismo, sino como un medio de apoyo a la consecución de los objetivos de la organización.

En general el principal objetivo de las empresas, es obtener beneficios y el de las organizaciones públicas, ofrecer un servicio eficiente y de calidad a los usuarios. En las empresas privadas, la seguridad informática debería apoyar la consecución de beneficios.

Para ello se deben proteger los sistemas para evitar las potenciales pérdidas que podrían ocasionar la degradación de su funcionalidad o el acceso a los sistemas por parte de personas no autorizadas.

De igual forma, las organizaciones públicas deben proteger sus sistemas para garantizar la oferta de sus servicios de forma eficiente y correcta.

En cualquier caso, los gestores de las diferentes organizaciones deberían considerar los objetivos de la propia organización e incorporar la seguridad de los sistemas desde un punto de vista amplio, como un medio con el que gestionar los riesgos que puede comprometer la consecución de los propios objetivos, donde la cuantificación de los diferentes aspectos, muchas veces económica, debe ser central.

### 4.1.5. Definición de hackers.

Un hacker es una persona con intenso amor por algo, sean las computadoras, la escritura, la naturaleza o los deportes. Un hacker debido a que tiene ese amor, tiene también una curiosidad profunda sobre el tema en cuestión por ende trata de conseguir por cualquier medio las llaves de la información, que esconde algún sistema.

Hacker es el neologismo utilizado para referirse a un experto, en varias o alguna rama técnica relacionada con la informática: programación, redes de computadoras, sistemas operativos, hardware de red/voz, etc.

El término "hackers" trasciende a los expertos relacionados con la informática, para también referirse a cualquier profesional que está en la cúspide de la excelencia en su profesión, ya que en la descripción más pura, un hacker es aquella persona que le apasiona el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas.

Hacker es usuario de ordenadores especializado en penetrar en las bases de datos de sistemas informáticos estatales con el Fin de obtener información secreta. En la actualidad, el término se identifica con el de delincuente informático, e incluye a los cibernautas que realizan operaciones delictivas a través de las redes de ordenadores existentes.

Tradicionalmente se considera Hacker al aficionado a la informática cuya afición es buscar defectos y puertas traseras para entrar en los sistemas. Para los especialistas, la definición correcta sería: experto que puede conseguir de un sistema informático cosas que sus creadores no imaginan.

## 4.1.6. TIPOS DE HACKERS

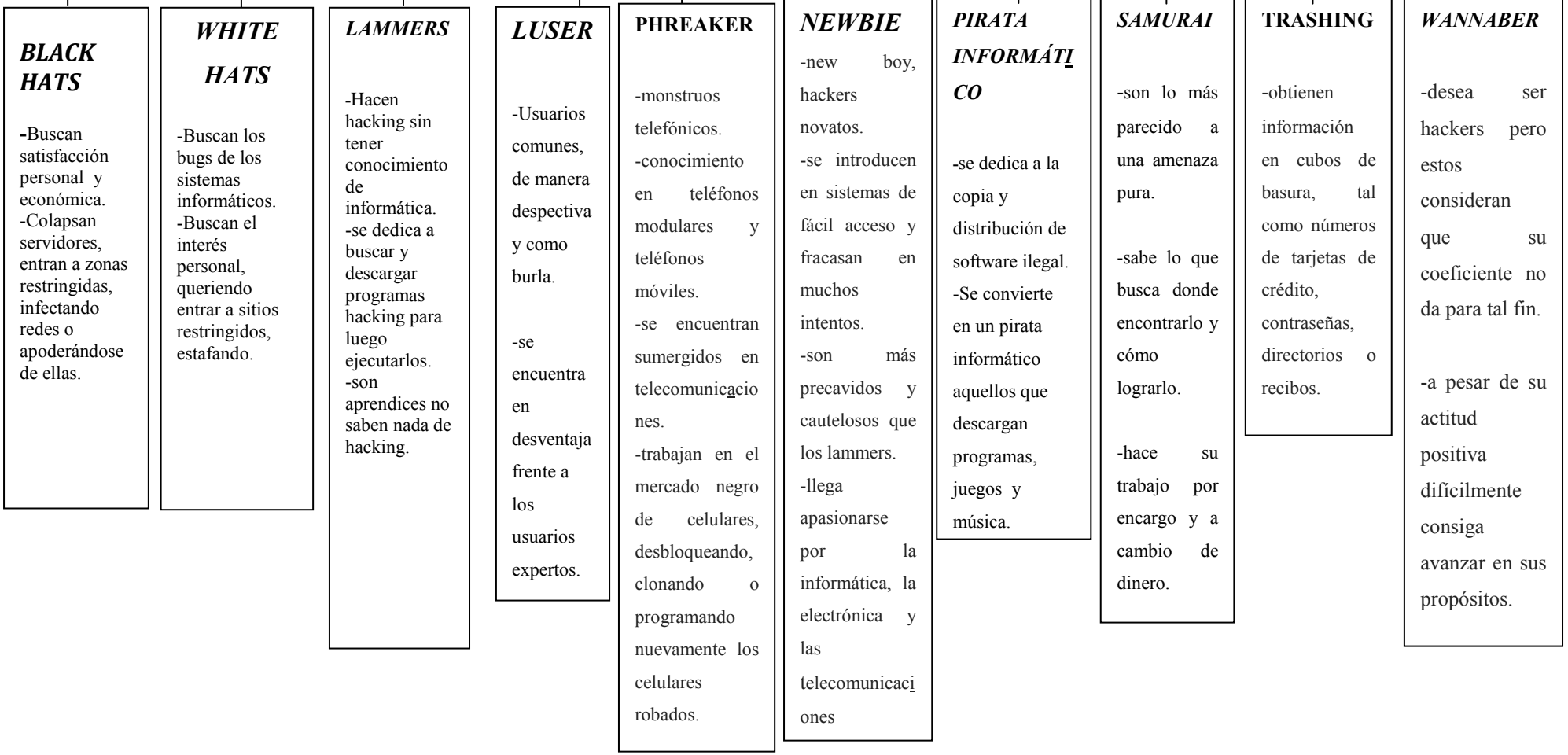


**Imagen No. 4 Tipos de hackers**

### 4.1.7. Programas que utilizan los hackers

**Scanners, IPs, Webs**

| PROGRAMA | BREVE DESCRIPCIÓN |
|---|---|
| **Security Scanner** | Scanner muy bueno y útil para nuestra PC, es de Seguridad, checas: el ftp, telnet, POP3, D.o.S (Denial Of Service) y vulnerabilidades en CGI. |
| **N-Stealth** | Scanner de seguridad muy bueno, lanza exploits y cuenta con una infinita variedad de opciones, todas están a elegir los modos de Gratuito o de Pago. |
| **Angry IP** | Analiza las IPs, resuelve nombre de host e intenta conectar con ellos. Muestra información sobre el PC (nombre de la máquina, grupo de trabajo, nombre del usuario conectado...) |
| **Range Scanner** | Buen scanner con utilidades, de seguridad. Escanea en busca de troyanos |
| **XnsScan** | XNSSCAN es un programa que prueba combinaciones de login's y password's vía ftp o pop3 de forma remota. Las combinaciones se leen de dos ficheros que el usuario debe escoger, y si encuentra alguna combinación correcta guarda la información en un fichero de log (xnsscan.log). La velocidad de escaneo es directamente proporcional a la de nuestra |

| | |
|---|---|
| | conexión. Tiene la típica opción 'single', que genera 32 password's derivados de login. También permite el uso de socks, con lo que el escaneo se realiza de forma anónima. |
| **SockScan** | Pequeño escaner ultra-rápido, que busca en redes B, C y D maquinas con el servicio de Socks5 anónimo disponible. La principal característica es su rapidez: monitoriza una red X.X.*.* en menos de 5 minutos. Se le puede especificar el timeout (para uso en redes lentas) y el número de procesos hijos en cada escaneo. |
| **WebSleuth** | WebSleuth (seguridad web-servers) |
| **WebScan** | WebScan+ (PLUS) es un escaneador de cgi's, hidden paths, asp's... que basa sus principales ventajas en lo facil de la actualizacion de sus ficheros de datos, la posibilidad multiplataforma del TCL y su capacidad modulable para los escaneos. |
| **Irs** | Services Scanner |
| **Webdav** | IIS WebDav vulnerability testing tool |

| **Nukers (Fuerza Bruta) (brute force)** | |
|---|---|
| **NsNuke** | NSNUKE utiliza una vulnerabilidad del protocolo Netbios para colgar ciertos Windows de forma remota. S.O's vulnerables: Windows 98, Windows 98 SE, Windows Me. |

| | |
|---|---|
| **Brute Forcer** | Munga Bunga's HTTP Brute Forcer. Programa para entrar en cuentas como las de Hotmail, Yahoo!, Excite mediante "fuerza bruta". Es muy configurable e incluye ejemplos. Prtocolo HTTP, es usado para poder introducirse en servidores sin que el usuario tenga que estar probando con cientos de listas de passwords |
| **NukeIT** | Buen Nuker, dentro de él trae un buen manual.. lo que sí les puedo decir, es que es muy bueno e útil, con buenas opciones y lo mejor de todo, con un tamaño muy pequeño. Pesa muy poco, para lo bueno que es!! :D |
| **Brutus AET2** | Buen Nuker, para nukear password. Tiene tres métodos:<br>1) Fuerza Bruta "la mejor xD"<br>2) Lista de palabras para descubrir password<br>3) Mezcla con diccionario de palabras |

Sss

| | |
|---|---|
| **Net Lab** | Una multitud de utilidades, es obligatorio tenerlo. Tiene diversas utilidades, como Ping, Trace, Scanner DNS, uno de los mejores escaneadores de Puertos, el Port Scan incluído, Quote, Finger, Whols, etc.. Indispensable!! |
| **CygWin** | Instalador de un sin fin de utilidades, entre ellas el upx, netcat, ping, todo para convertir tu windows en una maquina lista para la guerra |

| | |
|---|---|
| **eXe Scope** | Para ver el interior de los ejecutables (exe´s), permite editarlos. Permite modificar del .exe, los iconos que se usarán, los Copyright, etc. Se utiliza sobre todo, para traducir programas, ya que permite modificar menús. |
| **FlashIT** | Utilidad para desproteger archivos o animaciones .swf Es algo simple esta utilidad, sólo lo abres y buscas el archivo .swf que deseas desproteger, tiene una buena interfaz. Los .swf son archivos de animaciones "flash". |
| **H-Edit** | Buen editor Hexadecimal, con buenas utilidades y buenas opciones. Tiene un buscador incluido, para buscar líneas de comandos y así se nos haga más fácil el trabajo. Edita todo tipo de archivos, recomendado!! |

**Imagen No. 5 Programas que utilizan los hackers**

### 4.1.8. Ataques de hackers.

La mayoría de las vulnerabilidades de ordenadores pueden ser aprovechadas de varias formas. Los ataques Hacker pueden utilizar un simple exploit específico, o varios exploits al mismo tiempo, una configuración deficiente en uno de los componentes del sistema o inclusive un backdoor instalado en un ataque anterior.

Debido a esto, detectar los ataques hacker no es una tarea fácil, sobre todo para un usuario inexperto.

### 4.1.9.Algunos típicos ataques son:

#### *4.1.9.1. Ataques de intromisión*

Este tipo de ataque es cuando alguien abre archivos, uno tras otro, en nuestra computadora hasta encontrar algo que le sea de su interés. Puede ser alguien externo o inclusive alguien que convive todos los días con nosotros. Cabe mencionar que muchos de los ataque registrados a nivel mundial, se dan internamente dentro de la organización y/o empresa.

#### *4.1.9.2. Ataque de espionaje en líneas*

Se da cuando alguien escucha la conversación y en la cual, él no es un invitado. Este tipo de ataque, es muy común en las redes inalámbricas y no se requiere, como ya lo sabemos, de un dispositivo físico conectado a algún cable que entre o salga del edificio. Basta con estar en un rango donde la señal de la red inalámbrica llegue, a bordo de un automóvil o en un edificio cercano, para que alguien esté espiando nuestro flujo de información.

#### *4.1.9.3. Ataque de intercepción*

Este tipo de ataque se dedica a desviar la información a otro punto que no sea la del destinatario, y así poder revisar archivos, información y contenidos de cualquier flujo en una red.

#### *4.1.9.4. Ataque de modificación*

Este tipo de ataque se dedica a alterar la información que se encuentra, de alguna forma ya validada, en computadoras y bases de datos. Es muy común este tipo de ataque en bancos y casas de bolsa. Principalmente los intrusos se dedican a cambiar, insertar, o eliminar información y/o archivos, utilizando la vulnerabilidad del los sistemas operativos y sistemas de seguridad (atributos, claves de accesos, etc.).

#### *4.1.9.5. Ataque de denegación de servicio*

Son ataques que se dedican a negarles el uso de los recursos a los usuarios legítimos del sistema, de la información o inclusive de algunas capacidades del sistema. Cuando se trata de la información, esta, se es escondida, destruida o ilegible. Respecto a las aplicaciones, no se pueden usar los sistemas que llevan el control de la empresa, deteniendo

su administración o inclusive su producción, causando demoras y posiblemente pérdidas millonarias. Cuando es a los sistemas, los dos descritos anteriormente son inutilizados. Si hablamos de comunicaciones, se puede inutilizar dispositivos de comunicación (tan sencillo como cortar un simple cable), como saturar e inundar con tráfico excesivo las redes para que estas colisionen.

#### *4.1.9.6. Ataque de suplantación*

Este tipo de ataque se dedica a dar información falsa, a negar una transacción y/o a hacerse pasar por un usuario conocido. Se ha puesto de moda este tipo de ataques; los "nuevos ladrones" ha hecho portales similares a los bancarios, donde las personas han descargado sus datos de tarjetas de crédito sin encontrar respuesta; posteriormente sus tarjetas de crédito son vaciadas.

Es importante mencionar, que así como se llevan estos tipos de ataques en medios electrónicos, muchas veces se llevan a cabo en archivos físicos (expedientes, archiveros con información en papel, y en otro tipo de medios con los que las personas están familiarizadas a trabajar todos los días (como teléfonos convencionales, celulares, cajeros automáticos, etc.); inclusive los ataques a computadoras, muchas veces, comienzan precisamente con información obtenida de una fuente física (papeles, basura, intervención de

correo, cartas, estados de cuenta que llegan a los domicilios; o simplemente de alguien que vigila lo que hacemos).

## 4.2. MÉTODOS COMUNES DE ATAQUES

### 4.2.1. Definición de ataques

El ataque por diccionario (dictionary attack) es un tipo de ataque informático relacionado al hacking que utiliza un diccionario de palabras para llevar a cabo su cometido.

Por ejemplo, para ingresar a un sistema con contraseña, se puede utilizar un diccionario con palabras frecuentes y un programa automáticamente irá probando una a una para descifrarla. También suele usarse en el envío de spam1, probando direcciones de correo electrónico usando un diccionario.

Contrasta con el ataque por fuerza bruta, en donde las claves son buscadas sistemáticamente. En el ataque por diccionario, sólo se prueban las posibilidades de una lista de palabras. Este tipo de ataque tiende a funcionar

[11] El ataque por diccionario es un tipo de ataque informático relacionado al hacking que utiliza un diccionario de palabras para llevar a cabo su cometido.

debido a que muchas personas emplean claves sencillas, incluso palabras del diccionario, tal vez apenas combinadas con uno o dos números.

### 4.2.2. Tipos de ataques

| *TIPO* | *QUE ES* | *COMO ACTUA* | *CONSECUENCIAS* |
|---|---|---|---|
| ***1.ATAQUES DE INTROMISIÓN*** | El ataque de intromisión se efectúa cuando generalmente abren archivos. | Este tipo de ataque es cuando alguien abre archivos, uno tras otro, en nuestra computadora hasta encontrar algo que le sea de su interés. | Cabe mencionar que muchos de los ataque registrados a nivel mundial, se dan internamente dentro de la organización y/o empresa. |
| ***2.ATAQUE DE ESPIONAJE EN LÍNEAS*** | Este tipo de ataque, es muy común en las redes inalámbricas | Se da cuando alguien escucha la conversación y en la cual, él no es un invitado. | Basta con estar en un rango donde la señal de la red inalámbrica llegue, a bordo de un automóvil o en un edificio cercano, para que alguien esté espiando nuestro flujo de información. |
| ***3.ATAQUE DE INTERCEPCIÓN*** | Este tipo de ataque se caracteriza por desviar información. | Actúa desviando la información a otro punto que no sea la del destinatario, y así poder revisar archivos, información y contenidos de cualquier flujo en una | Desvía la información a otro punto que no sea la del destinatario, |

| | | | |
|---|---|---|---|
| | | red. | |
| ***4.ATAQUE DE MODIFICACIÓN*** | El ataque de modificación cambia la información de la base de datos. | Este tipo de ataque se dedica a alterar la información que se encuentra, de alguna forma ya validada, en computadoras y bases de datos. | Información alterada de la base de datos |
| ***5.ATAQUE DE DENEGACIÓN DE SERVICIO*** | También llamado *ataque DoS* (*Denial of Service*), es un ataque a un sistema de computadoras o red. | que causa que un servicio o recurso sea inaccesible a los usuarios legítimos, | Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima. |
| ***6.ATAQUE DE SUPLANTACIÓN*** | Este tipo de ataque entrega una información falsa, a negar una transacción y/o a hacerse pasar por un usuario conocido | Se ha puesto de moda este tipo de ataques; los "nuevos ladrones" ha hecho portales similares a los bancarios, donde las personas han descargado sus datos de tarjetas de créditos en encontrar respuesta; | Muchas veces se llevan a cabo en archivos físicos (expedientes, archiveros con información en papel, y en otro tipo de medios con los que las personas están familiarizadas a trabajar todos los días, inclusive los ataques a computadoras, muchas veces, |

| | | | |
|---|---|---|---|
| | | posteriormente sus tarjetas de crédito son vaciadas. | comienzan precisamente con información obtenida de una fuente física. |

**Imagen No. 6 Tipos de Ataques**

### 4.2.3. Amenazas y consecuencias

#### *4.2.3.1. Amenazas Lógicas*

Los protocolos de comunicación utilizados carecen (en su mayoría) de seguridad o esta ha sido implementada en forma de "parche" tiempo después de su creación.

- Existen agujeros de seguridad en los sistemas operativos.
- Existen agujeros de seguridad en las aplicaciones.
- Existen errores en las configuraciones de los sistemas.
- Los usuarios carecen de información respecto al tema.

Esta lista podría seguir extendiéndose a medida que se evalúen mayor cantidad de elementos de un Sistema Informático.

Las empresas u organizaciones no se pueden permitir el lujo de denunciar ataques a sus sistemas, pues el nivel de confianza de los clientes (ciudadanos) bajaría enormemente.

Los Administradores tienen cada vez mayor conciencia respecto de la seguridad de sus sistemas y arreglan por sí mismos las deficiencias detectadas. A esto hay que añadir las nuevas herramientas de seguridad disponibles en el mercado.

Los "advisories" (documentos explicativos) sobre los nuevos agujeros de seguridad detectados y la forma de solucionarlos, lanzados por el CERT, han dado sus frutos.

#### *4.2.3.2. Las consecuencias de los ataques se podrían clasificar en:*

- **Data Corruption**: la información que no contenía defectos pasa a tenerlos. Estado de deterioro de la Información.

- **Denial of Service (DoS)**: servicios que deberían estar disponibles no lo están.

En seguridad informática, un **ataque de denegación de servicio**, también llamado ataque **DoS** (de las siglas en inglés ***D**enial **o**f **S**ervice*), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le denomina "denegación", pues hace que el servidor no dé abasto a la cantidad de solicitudes. Esta técnica es usada por los llamados Crackers para dejar fuera de servicio a servidores objetivo.

Una ampliación del ataque Dos es el llamado **ataque distribuido de denegación de servicio**, también llamado ataque **DDoS** (de las siglas en inglés***D**istributed **D**enial **o**f **S**ervice*) el cual lleva a cabo generando un gran flujo de información desde varios puntos de conexión.

La forma más común de realizar un DDoS es a través de una botnet, siendo esta técnica el ciber ataque más usual y eficaz por su sencillez tecnológica.

En ocasiones, esta herramienta ha sido utilizada como un buen método para comprobar la capacidad de tráfico que un ordenador puede soportar sin volverse inestable y afectar a los servicios que presta.

- **Leakage**: los datos llegan a destinos a los que no deberían llegar.

## 4.3. MANUAL DE PROCEDIMIENTOS

El manual de procedimientos desarrollado va dirigido a los usuarios que generalmente están relacionados con el ámbito informático dentro de una empresa u organización, para que tomen en cuenta las siguientes recomendaciones de seguridad.

**ORGANIGRAMA**

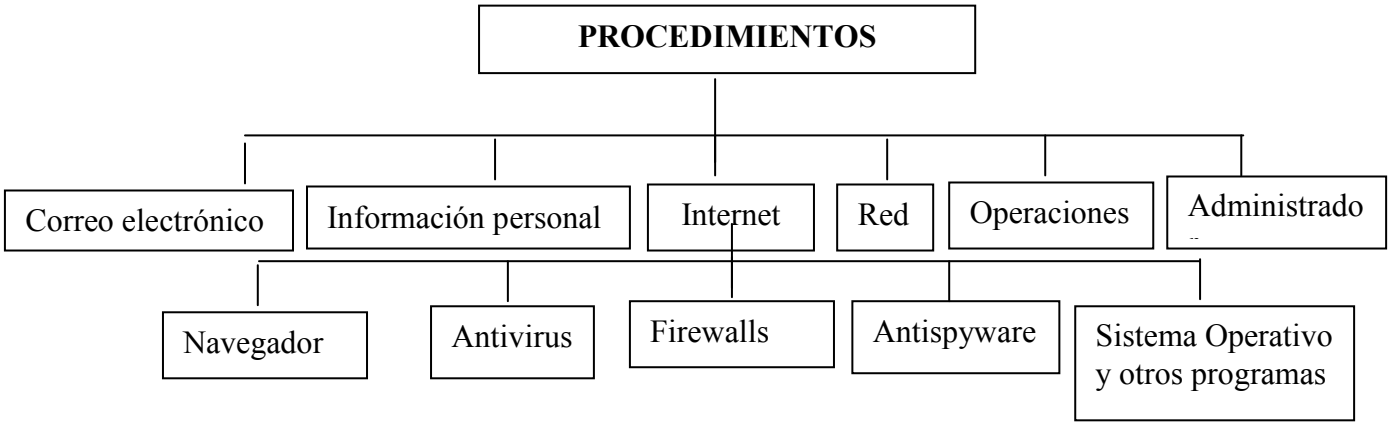


**Imagen No. 7 Organigrama**

### 4.3.1. CORREO ELECTRÓNICO

1. Nunca abra un correo electrónico con enlaces a sitios en la Internet o archivo adjunto que provenga de personas que no conozca.

2. Si eso sucede, tiene que eliminarlo inmediatamente.

3. Si conoce a la persona pero no esperaba el mensaje o duda de su contenido, verifique la veracidad del mensaje contactando a la persona que se lo envió; más vale prevenir que tener que lamentarse.

4. - Usa dos direcciones de correo electrónico, una con tus datos reales y otra con tus datos falsos. Emplea esta última cuando te sea necesario poner la dirección en un sitio del cual dudas de su fiabilidad.

5. -No dejes tu dirección en sitios visibles al público, como foros, comentarios en blogs, etc. Si lo haces, escríbela sustituyendo la arroba por una palabra. NO: usuario@servicio.com. SÍ: usuario_arroba_servicio_punto_com, por ejemplo entre otras variaciones.

6. - Nunca descargues archivos adjuntos de direcciones desconocidas. Así se contraen la mayoría de virus.

7. - No envíes NUNCA correos a múltiples direcciones poniéndolas en el campo de la dirección ni en el de CC (Con Copia). Emplea el campo CCO (Con Copia Oculta). De esta manera, nadie podrá ver las direcciones de las otras personas y contribuirás a que se reciba menos Spam.

8. - El spam es el correo no deseado, ese que recibes con publicidad o con propuestas de negocios que te harán ganar dinero fácil y rápido. Nunca contestes a esos mensajes.

9. - De verdad, las cadenas no funcionan. No se te cumplirá el deseo si le envías ese texto a 50 personas más, ni siquiera a 5. Y si no lo envías, no te pasará nada.

10. - Si un sitio web te muestra un mensaje indicando que tienes un problema en tu computadora, o es falso, o se ha metido en tu equipo sin obtener tu permiso. Por lo tanto, no le hagas caso y sal de ahí.

11. Lee todo cuadro de diálogo que aparezca en el navegador mientras navegas. Si no entiendes lo que pone, simplemente dale al botón "Cancelar". Nunca le des al botón "Aceptar" sin comprender que es lo que estás haciendo.

### 4.3.2. INFORMACIÓN PERSONAL

1. La primera línea de defensa son siempre sus contraseñas y la información de su computadora.

2. Asegúrense de que su equipo esté perfectamente seguro, primero un buen antivirus como Kaspersky, norton, nod32, etc.

3. Cambiar la información de registro y las contraseñas en todo, desde sus cuentas de tarjetas de crédito hasta su correo electrónico.

4. Los **hackers** están llegando de todas partes. Traten de no usar las mismas contraseñas para todo, más bien todas deben de ser diferentes.

5. Traten de usar solo una computadora para realizar sus transacciones bancarias. Sé que es difícil, especialmente los que usan dispositivos diferentes. Pero traten de hacerlo todo en un solo equipo.

6. Mantenga al día su computadora con todos los parches (patches) nuevos tanto como para el sistema operativo así como para los otros programas que residen en la computadora.

### 4.3.3. ADMINISTRADOR

1. Mantener las máquinas actualizadas y seguras físicamente.

2. Mantener personal especializado en cuestiones de seguridad (o subcontratarlo).

3. Aunque una máquina no contenga información valiosa, hay que tener en cuenta que puede resultar útil para un atacante, a la hora de ser empleada en un DoS coordinado o para ocultar su verdadera dirección.

4. No permitir el tráfico "broadcast" desde fuera de nuestra red. De esta forma evitamos ser empleados como "multiplicadores" durante un ataque Smurf.

5. Filtrar el tráfico IP Spoof.

6. Auditorías de seguridad y sistemas de detección.

7. Mantenerse informado constantemente sobre cada unas de las vulnerabilidades encontradas y parches lanzados. Para esto es recomendable estar suscripto a listas que brinden este servicio de información.

8. Por último, pero quizás lo más importante, la capacitación continua del usuario.

### 4.3.4. RED

1. Mantener la integridad en una base de datos. Se refiere al estado de corrección y completitud de los datos ingresados en una base de datos.

2. Realizar sistemas de respaldos, mediante Tecnologías: óptica y magnéticay dispositivos de almacenamiento.

3. Monitorear la red a través de TCPDump / WinDump, DSniff, IpTraf, snoop, etc.

4. Contar con un generador de energía de respaldo mediante UPS.

5. Contar con antivirus actualizados

6. Chequear las conexiones físicas y lógicas periódicamente.

### 4.3.5. OPERACIONES

1. Realice sus operaciones por Internet sólo desde el computador personal de su casa u oficina.

2. Por ningún motivo y bajo ninguna circunstancia la Aseguradora solicitará su clave secreta a través de correos electrónicos, ni por ningún otro medio.

3. Nunca haga click en correos electrónicos que contengan links hacia la página de la Aseguradora. Ingrese siempre en forma directa.

4. Por seguridad, nunca suministre información personal (Usuario, clave secreta, o documento de identidad) a personas que lo soliciten bajo el argumento de participar en concursos, premios o cualquier tipo de oferta.

5. No acepte ayuda de ninguna persona que se ofrezca a colaborarle en caso de que su clave presente fallas. Si esto sucede, anule la operación y antes de retirarse haga click en la opción SALIR.

6. Su usuario y clave secreta son personales e intransferibles. Manténgalos en absoluta reserva.

7. Nunca porte y escriba su usuario y clave secreta, memorícelos!

8. Cuando digite su clave secreta asegúrese que nadie lo observe.

9. Si sospecha que alguien conoce su clave secreta, cámbiela inmediatamente.

10. Nunca utilice a terceras personas para realizar sus operaciones, hágalas siempre personalmente.

11. Antes de arrojar a la basura, destruya las impresiones que por cualquier concepto no esté interesado en conservar.

12. No construyas su clave secreta con nombre de familiares, fechas de nacimiento o aniversarios, número de documento de identidad o números de dirección y teléfono.

## 4.3.6. INTERNET

### *4.3.6.1. NAVEGADOR*

**Navegadores recomendados**

1.- Firefox

2.- Opera

3.- Google Chrome

4.- Internet Explorer 7 o superior (aunque sigue fallando en seguridad)

**Última versión**

Emplea siempre la última versión de tu navegador favorito. Todos los días surgen nuevas amenazas en la red y por eso los navegadores se actualizan con bastante regularidad o frecuencia.

**Plugins**

Los plugins son pequeños programas que funcionan dentro de un programa más grande o principal. Los navegadores hacen mucho de los plugins. Especialmente de los de Flash (para ver videos)

Y los de Java (para ejecutar programas). Procura siempre utilizar la última versión de estos, actualizada desde un sitio web original.

**Extensiones**

Las extensiones son muy similares a los plugins: pequeños programas que funcionan sólo dentro de uno más grande. Firefox cuenta con muchas extensiones y las actualiza automáticamente cuando es necesario. Siempre ten las extensiones actualizadas a la última versión.

**Datos**

En los navegadores se almacenan gran cantidad de datos que pueden ser susceptibles robados o incluso de provocar problemas en el funcionamiento del programa. Cada cierto tiempo, borra el cache del navegador, el historial y las cookies (pequeños archivos que se colocan en nuestro equipo para almacenar información relativa a sitios web).

### *4.3.6.2. ANTIVIRUS*

**LEGAL**

Hay numerosas opciones gratuitas de antivirus que en realidad no hay razón para usar uno"pirata". Dado que un antivirus necesita de una actualización regular vía Internet para su correcto funcionamiento, si empleas un antivirus ilegal es posible que tarde o temprano seas detectado y el programa deje de funcionar o deje de actualizar sus definiciones. Algunos antivirus gratuitos son:

- Avast antivirus.
- Avira antivir.
- AVG

**Actualizado**

En materia de antivirus, no solamente hay que estar actualizado siempre a la última versión para que funcione correctamente, sino que es necesario haber descargado las últimas definiciones de virus. Las definiciones sirven

para que el antivirus pueda detectar el virus y, si no puede eliminarlo, al menos que impida que se ponga en funcionamiento.

Algunos antivirus permiten descargar sus definiciones aparte, de manera que puedas instalarlas más tarde en un computador que no cuente con conexión a Internet y contar así con el máximo de protección.

#### *4.3.6.3. FIREWALL*

**Legal**

Un firewall nos protege de intrusiones un nuestra computadora, las cuales son más comunes de lo que nos pueda parecer. Estas intrusiones pueden limitarse al robo de datos (como el historial) o ir hasta el uso de nuestro equipo como un zombie que es usado para realizar ataques a webs.

Cualquier programa “pirata” de seguridad corre el riesgo de no poder actualizarse debidamente. Hay muchas alternativas gratuitas en materia de

firewalls como para arriesgarse a usar uno ilegal. Entre ellas destaca el Comodo Firewall.

**Actualizado**

Las actualizaciones ofrecen soluciones a fallos de seguridad, detección de sitios web peligrosos y técnicas varias de infiltración en nuestro equipo. Además, en el caso de actualizaciones mayores, se incorporan nuevas funciones.

### *4.3.6.4.ANTISPYWARE*

**Legal**

El antispyware detecta y elimina spyware instalado en nuestra computadora. El uso de un programa "pirata" de este tipo puede hacer que no se actualice regularmente, lo cual hará que nuestros datos corran el riesgo de ser robados.

Para evitar este programa, podemos utilizar muchas de las opciones gratuitas que existen, entre las que destaca Spybot Search & Destroy.

**Actualizado**

Es vital que un antispyware esté siempre actualizado para añadir las nuevas amenazas que van surgiendo. Hay que considerar que el spyware es una de las principales amenazas que nos podemos encontrar al navegar por la web debido a la facilidad con que se puede infiltrar en nuestro sistema sin que nos demos cuenta.

### *4.3.6.5. SISTEMA OPERATIVO Y OTROS PROGRAMAS*

**Legales**

Todo sistema operativo recibe actualizaciones regulares no sólo para cubrir fallos de seguridad sino para mejorar su rendimiento. Igualmente sucede con muchos programas, por no decir todos (siempre y

cuando aún continúen siendo desarrollados, que muchos que no). Al utilizar programas "piratas" o ilegales se corre el riesgo de no poder actualizar cuando aparezca una nueva versión o de no recibir las actualizaciones menores (pero importantes) cuando salgan. Emplear software "pirata" hace nuestro sistema mucho más vulnerable a todo tipo de ataques.

**Actualizados**

Las actualizaciones de los sistemas operativos y los programas corrigen fallos de seguridad y problemas de rendimiento. En el caso de las actualizaciones mayores (como el paso de versión: de 2.0 a 3.0. por ejemplo) traen además nuevas funciones y características.

# CAPITULO 5

## 5.1. Conclusiones

1. Computadoras, equipos y sistemas, se han convertido en algo cotidiano dentro de los procesos de las empresas.

2. Es de vital importancia disponer de políticas de seguridad.

3. Es necesario tener conocimiento de todas las medidas pertinentes para evitar fallas, ataques y fraudes.

4. La falta de información sobre seguridad informática puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

5. Es importante revisar un manual de procedimientos para proteger la información ante los hackers.

6. Es interesante analizar los diferentes tipos de ataques de hackers que afectan a las empresas u organizaciones.

## 5.2. Recomendaciones

1. Disponer de medidas preventivas para así evitar perdida de información, ataques y fallas en los sistemas.

2. Utilizar técnicas de seguridad, también debe tener conocimiento de ataques de hackers y las consecuencias de los mismos.

3. Tener en cuenta las técnicas y medidas preventivas al momento de utilizar el internet para evitar posibles ataques de hackers.

4. Conocer la importancia de la seguridad informática dentro de una empresa u organización.

## BIBLIOGRAFÍA

http://tecnologia21.com/proteger-su-informacion-personal-hackers

http://web.iti.upv.es/actualidadtic/2003/07/2003-07-seguridad.pdf

http://www.viruslist.com/sp/hackers/info?chapter=153349899

http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf

http://www.sg.inter.edu/acc/prMIS104/bravof/pag-05.htm

http://www.portalhacker.net/hacker/programas-hacker.php

http://www.taringa.net/posts/info/1852601/Tipos-de-Hacker.html

http://www.segu-info.com.ar/ataques/ataques.htm

http://www.seguridadinformatica.es/

http://www.seguridadpc.net/hackers.htm

http://www.uribe100.com/computadora_seguridad.pdf

# UNIVERSIDAD TECNOLÓGICA ISRAEL
## DIRECCIÓN DE POSGRADOS
## AUTORIZACIÓN DE EMPASTADO

**DE: Pablo Ochoa**
MIEMBRO DEL TRIBUNAL

**PARA:** Msc. Luis Andrés Chávez Ing.
DIRECTOR DEL SINED DE LA UNIVERSIDAD ISRAEL

**ASUNTO:** Autorización de Empastado

**FECHA** Quito, 01 de Diciembre del 2011

Por medio de la presente certifico que el pregradista Digna Isabel Serrano Bonilla con CI No.010500057-4 han realizado las modificaciones solicitadas de acuerdo a la última revisión realizada en mi tutoría, al documento de tesis titulada **Análisis de la seguridad informática, sobre los ataques de hackers y como protegerse ante los mismos dentro de una empresa u organización,** del título de ingenieros en sistemas informáticos

**Atentamente**

_____
**Ing. Pablo Ochoa**

# UNIVERSIDAD TECNOLÓGICA ISRAEL
## DIRECCIÓN DE POSGRADOS
## AUTORIZACIÓN DE EMPASTADO

**DE: Juan Pérez**
MIEMBRO DEL TRIBUNAL

**PARA:** Msc. Luis Andrés Chávez Ing.
DIRECTOR DEL SINED DE LA UNIVERSIDAD ISRAEL

**ASUNTO:** Autorización de Empastado

**FECHA** Quito, 01 de Diciembre del 2011

Por medio de la presente certifico que el pregradista Digna Isabel Serrano Bonilla con CI No.010500057-4 han realizado las modificaciones solicitadas de acuerdo a la última revisión realizada en mi tutoría, al documento de tesis titulada **Análisis de la seguridad informática, sobre los ataques de hackers y como protegerse ante los mismos dentro de una empresa u organización,** del título de ingenieros en sistemas informáticos

**Atentamente**

_____
**Ing. Juan Pérez**

# UNIVERSIDAD TECNOLÓGICA ISRAEL
## DIRECCIÓN DE POSGRADOS
## AUTORIZACIÓN DE EMPASTADO

**DE: Ing. Tannia Mayorga**
MIEMBRE DEL TRIBUNAL

**PARA:** Msc. Luis Andrés Chávez Ing.
DIRECTOR DEL SINED DE LA UNIVERSIDAD ISRAEL

**ASUNTO:** Autorización de Empastado

**FECHA** Quito, 01 de Diciembre del 2011

Por medio de la presente certifico que el pregradista Digna Isabel Serrano Bonilla con CI No.010500057-4 han realizado las modificaciones solicitadas de acuerdo a la última revisión realizada en mi tutoría, al documento de tesis titulada **Análisis de la seguridad informática, sobre los ataques de hackers y como protegerse ante los mismos dentro de una empresa u organización,** del título de ingenieros en sistemas informáticos

**Atentamente**

_____
**Ing. Tannia Mayorga**