Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

SEGURIDAD INFORMÁTICA ORIENTADA A PARTICULARES

Jorge Lizandro Flores Barco

Asesorado por el Ing. Byron Rodolfo Zepeda Arévalo

Guatemala, noviembre de 2015

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

SEGURIDAD INFORMÁTICA ORIENTADA A PARTICULARES

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

JORGE LIZANDRO FLORES BARCO
ASESORADO POR EL ING. BYRON RODOLFO ZEPEDA ARÉVALO

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, NOVIEMBRE DE 2015

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Pedro Antonio Aguilar Polanco
VOCAL I	Ing. Angel Roberto Sic García
VOCAL II	Ing. Pablo Christian de León Rodríguez
VOCAL III	Inga. Elvia Miriam Ruballos Samayoa
VOCAL IV	Br. Raúl Eduardo Ticún Córdova
VOCAL V	Br. Henry Fernando Duarte García
SECRETARIA	Inga. Lesbia Magalí Herrera López

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Pedro Antonio Aguilar Polanco
EXAMINADOR	Ing. José Ricardo Morales Prado
EXAMINADOR	Ing. Marlon Francisco Orellana López
EXAMINADOR	Ing. Miguel Ángel Cancinos Rendón
SECRETARIA	Inga. Lesbia Magalí Herrera López

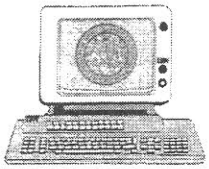
HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

SEGURIDAD INFORMÁTICA ORIENTADA A PARTICULARES

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha octubre de 2014.

Jorge Lizandro Flores Barco



Guatemala 28 de abril de 2015.

Facultad de Ingeniería USAC
Ing. Carlos Azurdia:

Por medio de la presente hago de su conocimiento que el estudiante Jorge Lizandro Flores Barco que se identifica con el número de carné 201114435 de la Facultad de Ingeniería, USAC, de la Carrera de Ingeniería en Ciencias y Sistemas presentó la modalidad de investigación y sus componentes asociados, el trabajo "SEGURIDAD INFORMÁTICA ORIENTADA A PARTICULARES", el cual se encuentra concluido satisfactoriamente y por lo tanto lo doy por aprobado.

F:

Jorge Flores
Universidad de San Carlos de Guatemala,
Facultad de Ingeniería
Jorgelizandro55@gmail.com

BYRON RODOLFO ZEPEDA ARÉVALO
INGENIERO EN CIENCIAS Y SISTEMAS
Colegiado No. 12802

F:

Ingeniero Byron Zepeda
Universidad de San Carlos de Guatemala,
Facultad de Ingeniería
byron.zepeda.usac@gmail.com

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 13 de Mayo de 2015

Ingeniero
Marlon Antonio Pérez Türk
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Pérez:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **JORGE LIZANDRO FLORES BARCO** con carné **2011-14435,** titulado: **"SEGURIDAD INFORMÁTICA ORIENTADA A PARTICULARES",** y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

ESCUELA DE CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÌA
ESCUELA DE CIENCIAS Y SISTEMAS
TEL: 24767644

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, del trabajo de graduación ***"SEGURIDAD INFORMÁTICA ORIENTADA A PARTICULARES"****, realizado por el estudiante JORGE LIZANDRO FLORES BARCO, aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION DE INGENIERIA EN CIENCIAS Y SISTEMAS

Ing. Marlon Antonio Pérez Türk
Director, Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 12 de Noviembre de 2015

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

DTG. 621.2015

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al Trabajo de Graduación titulado: **SEGURIDAD INFORMÁTICA ORIENTADA A PARTICULARES,** presentado por el estudiante universitario: **Jorge Lizandro Flores Barco,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

Ing. Pedro Antonio Aguilar Polanco
Decano

Guatemala, noviembre de 2015

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

/gdech

ACTO QUE DEDICO A:

Dios	Por ser la base de mi desarrollo y por permitirme culminar esta meta en mi vida.
Mis padres	Jorge Flores y Lilian Barco, por no dejarme solo en este camino, por su lucha constante, esfuerzo, tolerancia y perseverancia, que pueden verse reflejados en mi desempeño y desarrollo en general.
Mis hermanos	Por su apoyo, confianza y compañía, dado que influyen en todos los aspectos de mi vida.
A mis amigos	Por ser mi segunda familia, manteniéndose a mi lado en las buenas y las malas, siendo parte también de mi desarrollo profesional.

AGRADECIMIENTOS A:

Mi asesor	Por compartir sus conocimientos y ser guía en mi proyecto.
Universidad de San Carlos de Guatemala	Por ser mi alma máter y formar el profesional que soy hoy en día, a partir de una constante lucha, no solamente en el ámbito académico.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES VII
GLOSARIO IX
RESUMEN XI
OBJETIVOS XIII
INTRODUCCIÓN XV

1. MARCO TEÓRICO 1
1.1. Informática: pasado, presente y futuro 1
1.2. Seguridad 2
1.2.1. Definición de seguridad 3
1.2.2. Valor de la información 4
1.2.3. Ataques 5
1.2.4. Operatividad *versus* seguridad 7
1.2.5. Seguridad informática 9
1.2.5.1. Implicaciones de la seguridad informática 9
1.2.5.2. Principios 11
1.2.5.2.1. Integridad 11
1.2.5.2.2. Confidencialidad 11
1.2.5.2.3. Disponibilidad 12

2. CLASIFICACIÓN Y PLANEACIÓN DE SEGURIDAD 13
2.1. Seguridad 13
2.1.1. Seguridad informática 13
2.1.1.1. Autenticidad 14

2.1.1.2. Control 15
2.1.2. Clasificación 15
2.1.2.1. Seguridad física 15
2.1.2.1.1. Control de acceso 16
2.1.2.1.2. Protección electrónica ... 17
2.1.2.1.3. Sistemas de medición ... 17
2.1.2.1.4. Condiciones ambientales 18
2.1.2.2. Seguridad lógica 19
2.1.2.2.1. Seguridad de accesos .. 19
2.2. Planeación 22
2.2.1. Identificación y análisis de recursos 23
2.2.1.1. Activos 23
2.2.1.1.1. Datos 24
2.2.1.1.2. Hardware 24
2.2.1.1.3. Software 24
2.2.1.1.4. Redes 24
2.2.1.1.5. Instalaciones 25
2.2.1.1.6. Servicios 25
2.2.1.1.7. Recurso humano 25
2.2.2. Análisis de vulnerabilidades y riesgos 25
2.2.2.1. Vulnerabilidades 25
2.2.2.2. Riesgos 26
2.2.3. Políticas de seguridad 28
2.2.3.1. Definición de protección y política de seguridad 28
2.2.3.2. Parámetros para establecer políticas de seguridad 32

3. AMENAZAS 33
3.1. Definición de amenaza informática 33
3.2. Clasificación de amenazas 33
3.2.1. Amenaza humana 34
3.2.1.1. Otras amenazas humanas 36
3.2.1.1.1. *Copyhackers* 36
3.2.1.1.2. Samurai 36
3.2.1.1.3. *Crackers* 36
3.2.1.1.4. *Phreakers* 37
3.2.1.1.5. Creadores de virus 37
3.2.1.1.6. *Wannaber* 37
3.2.1.1.7. *Newbie* 37
3.2.1.1.8. Lammer 37
3.2.2. Amenaza lógica 38
3.2.2.1. Ejemplos 39
3.2.2.1.1. Software incorrecto 39
3.2.2.1.2. Puertas traseras 39
3.2.2.1.3. Gusanos 40
3.2.2.1.4. Virus 40
3.2.2.1.5. Caballo de Troya 40
3.2.3. Amenaza física 40
3.2.3.1. Clasificación de amenazas físicas 41
3.2.3.1.1. Terremotos 41
3.2.3.1.2. Incendios 42
3.2.3.1.3. Instalaciones eléctricas 42
3.2.3.1.4. Inundaciones 42
3.3. Análisis de las amenazas 42
3.3.1. Prevención 43

3.3.2. Detección 43
3.3.3. Recuperación 44
3.4. Tipos de amenaza 44
3.4.1. Por el origen 44
3.4.1.1. Amenazas internas 44
3.4.1.2. Amenazas externas 45
3.4.2. Por el medio 45
3.4.3. Por el efecto 46

4. SEGURIDAD A NIVEL DE USUARIO 47
4.1. Información 47
4.1.1. Tipos de información 47
4.1.1.1. Confidencial o sensible 47
4.1.1.2. Restringida 48
4.1.1.3. Pública 48
4.1.1.4. Privada 48
4.1.1.5. Uso interno 48
4.1.2. Manejo de la información 49
4.2. Plan de aseguramiento 50
4.2.1. Protección física 51
4.2.1.1. Instalaciones 51
4.2.1.2. Equipo 52
4.2.2. Protección lógica 53
4.2.2.1. Información 53
4.2.2.2. Sistema operativo 55
4.2.2.3. Datos 56

5. APORTE 57
5.1. Contexto de la investigación 57

5.2. Evaluación realizada 57
5.3. Discusión de resultados 70

CONCLUSIONES 71
RECOMENDACIONES 73
BIBLIOGRAFÍA 75
ANEXOS 77

ÍNDICE DE ILUSTRACIONES

FIGURAS

1. Operatividad *versus* seguridad 8
2. Inicio de sesión por fuerza bruta 20
3. Cantidad total de vulnerabilidades (global) 26
4. Riesgos de los sectores y encuentros con *malware* web 30
5. Anatomía de una amenaza moderna 34
6. La jerarquía del ciberdelincuente 35
7. Ataques malintencionados generados mediante PDF, *flash* y Java 38
8. Resultados pregunta 1 57
9. Resultados pregunta 2 58
10. Resultados pregunta 3 59
11. Resultados pregunta 4 60
12. Resultados pregunta 5 60
13. Resultados pregunta 6 61
14. Resultados pregunta 7 62
15. Resultados pregunta 8 62
16. Resultados pregunta 9 63
17. Resultados pregunta 10 64
18. Resultados pregunta 11 64
19. Resultados pregunta 12 65
20. Resultados pregunta 13 65
21. Resultados pregunta 14 66
22. Resultados pregunta 15 67
23. Resultados pregunta 16 68

24. Resultados pregunta 17.....68
25. Resultados pregunta 18.....69
26. Resultados pregunta 19.....70

TABLAS

I. Índice de tipo de ataque.....6
II. Tipos de riesgos-factor 29
III. Infecciones por tipo de *malware* 41

GLOSARIO

Ábaco Todo instrumento que sirve para efectuar manualmente cálculos aritméticos mediante marcadores deslizables.

Biometría Estudio estadístico de los fenómenos o procesos biológicos.

Botnet Término que hace referencia a un conjunto o red de robots informáticos o *bots*, que se ejecutan de manera autónoma y automática.

Dato Información dispuesta de manera adecuada para su tratamiento por un ordenador.

Encriptación Proceso para volver ilegible información que se considera importante. La información una vez encriptada puede leerse aplicándole una clave.

Firewall Palabra en inglés referente a una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado: cortafuegos.

Flash Tecnología para crear animaciones gráficas vectoriales independientes del navegador.

Hacker	Persona que descubre las debilidades de una computadora o de una red informática
Información	Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada.
Java	Es un lenguaje de programación y una plataforma informática comercializada por primera vez en 1995, por Sun Microsystems.
Malware	Tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

RESUMEN

En la actualidad, el uso de tecnología se ha vuelto un hábito para la mayoría de personas a nivel mundial, sobre todo tras la aparición de internet en la década de los noventa. Dicha innovación brinda muchas ventajas y por tal razón existen cada vez más aparatos inteligentes que buscan facilitar la realización de las tareas de cualquier ser humano.

Al hacer uso de dispositivos electrónicos con cierto nivel de inteligencia, las personas suelen ignorar un aspecto realmente importante y digno de tomar en cuenta por bien propio, la seguridad. Hacer uso de dispositivos inteligentes significa poner en riesgo información de la persona que lo posee al encontrarse sumergido en una red tan grande; es por eso que es de gran importancia contar con fuerte conocimiento de conceptos, formas de prevención, cuidado de hardware y software, entre otros.

Es importante conocer todos los tipos de amenazas que actualmente existen para poder mantener el cuidado debido de los dispositivos que las personas poseen y qué se debe hacer en caso de que ocurra algún incidente, así no se pierda información importante o caiga en manos de terceros según se trate de amenazas lógicas o físicas. Asimismo, la elaboración de planificaciones de seguridad estructuradas como prevención de ataques.

Tras realizar una encuesta a determinada muestra de personas, se evaluó el nivel de seguridad con el que adaptan sus dispositivos y qué tanto conocimiento poseen sobre las amenazas que existen para prevenirlas o eliminarlas.

OBJETIVOS

General

Realizar una investigación que permita determinar, estudiar y analizar los principales aspectos sobre la seguridad informática, además de amenazas y medidas a considerar, por parte de los usuarios y según experiencias brindadas por estudiantes, buscar problemas comunes y buenas prácticas sobre seguridad.

Específicos

1. Estudiar la importancia del manejo de la información.

2. Establecer los riesgos en los que incurre un estudiante, en sus actividades cotidianas.

3. Identificar las amenazas y vulnerabilidades comunes a las que se enfrenta un sistema informático.

4. Comprender el desarrollo de la seguridad informática y su implicación, además de la importancia de un plan de seguridad para el estudiante/usuario.

5. Explicar los conceptos asociados a las vulnerabilidades de un sistema y su mitigación.

6. Introducir al lector a la realidad de seguridad de la información y de las medidas que puede tomar, de forma preventiva.

INTRODUCCIÓN

La tecnología, como parte de la vida cotidiana es fundamental, dado que cada persona interactúa con ella a cada momento. Generalmente se considera a los dispositivos electrónicos como inofensivos, pero pueden llegar a ocasionar lesiones o daños graves según su forma de uso, pues la tendencia es que todo se vuelva “inteligente”; sin embargo siguen siendo máquinas que en cualquier momento pueden fallar de diversas maneras.

Al requerir la inteligencia de dispositivos la comunicación se vuelve un factor esencial, pero al mismo tiempo podría ser una debilidad, por lo que cada persona debe entender que cualquier objeto en un entorno doméstico puede llegar a verse como un sistema, el cual se divide en diversos componentes que interactúan entre sí.

Entre esos componentes se puede mencionar: teléfono, computadora, televisor, entre otros. La interacción de los componentes incrementa las funcionalidades que proporcionan dichos dispositivos al poder comunicarse entre ellos y en ese proceso pueden presentar fallas, riesgos, vulnerabilidades o pueden existir amenazas que atenten contra cualquier sistema inteligente, es por esto que es necesario tomar medidas de protección.

La apertura de la comunicación e interacción entre dispositivos ha sido una brecha para el avance tecnológico, pero como contraparte también ha abierto el paso a personas con conductas antisociales que con fines maliciosos dañan a otras personas a través del acceso a su información, ocasionando pérdidas, alteración de datos y hasta ataques contra hardware funcional y los

usuarios finales sufren por falta de conocimiento necesario sobre los riesgos a los que se está expuesto cuando alguien se encuentra conectado a la red o tiene acceso a su información o demás recursos importantes de alguna forma.

Gran cantidad de información que se hace pública, comúnmente por internet, puede ser falsa por lo que se busca identificar las principales amenazas que asedian al usuario y a su vez, formas de protegerse ante las mismas.

La mayoría de usuarios pertenecientes al mundo informático no saben la magnitud del problema que se tiene respecto de la seguridad y generalmente no se cuenta con formas que faciliten a las personas el indagar en este aspecto, no se tiene la inversión adecuada de conocimiento para mitigar este mal; por lo que la forma de manejarlo es reactiva, dado que es cuando se produce un daño que se recurre a la búsqueda de la manera de protegerse o proteger sus recursos, sobre todo la información que se maneja, porque es el recurso con más valor y el que se encuentra en mayor riesgo si no se toman medidas de seguridad, necesarias.

1. MARCO TEÓRICO

Es indispensable que toda persona que posee un dispositivo electrónico conozca a profundidad los términos relevantes del tema de seguridad informática para estar al tanto de los beneficios y consecuencias que este brinda.

1.1. Informática: pasado, presente y futuro

La humanidad ha usado una gran variedad de dispositivos mecánicos para ayudarse a realizar cálculos, durante miles de años. Un ejemplo de esto es el ábaco, el cual, probablemente existió en Babilonia. A esto se agregan otros inventos, como el que realizó Blaise Pascal en 1641, que era una sumadora mecánica.

El periodo comprendido de 1900 a 1939, se le conoce como el levantamiento de los matemáticos, esto se debe al trabajo continuo que se realizó para inventar máquinas con las cuales se pueda asistir al cálculo, tal como sucedió en 1919, año en el que se inventó una máquina capaz de factorizar números enteros.

Posteriormente, la Segunda Guerra Mundial estimuló el desarrollo de la computadora electrónica digital, para uso general, la cual fue desarrollada en Harvard con la asistencia de IBM y nombrada como Mark I, en 1944.

En 1947, Jhon Bardeen inventó el transistor, lo que transformó la computadora de aquel entonces y dio paso a la revolución del microprocesador.

A lo largo de los próximos años, desarrollan algoritmos para resolver diversos problemas, tal como el de Dijkstra, para encontrar la ruta más corta, la máquina de Turing, y otros. Se introduce el concepto de “inteligencia artificial”.

La ciencia computación se vuelve una disciplina en los 60, término acuñado por George Forsythe, un analista numérico. Dado esto, en 1962 se forma el primer departamento informático en la Universidad de Purdue. A finales de esta década, se forma ARPAnet, precursora de lo que actualmente se conoce como internet.

En los 70 nace el sistema operativo UNIX y se dan avances en la teoría sobre bases de datos, gracias a Edgar F. Codd, en bases de datos relacionales.

La década de 1980 es conocida por el aumento que tuvieron los ordenadores personales, que se produjo gracias a Steve Wozniak y Steve Jobs, y con ello, surge el primer virus de computadora, cuyo término fue acuñado por Leonard Adleman, en la Universidad del Sur de California.

Los sucesos anteriores dieron paso a lo que se conoce en la actualidad, en conjunto con los dispositivos móviles y la interconexión entre los sistemas. A esto se agrega cosas que se están desarrollando, como las computadoras cuánticas o la computación biológica. Por lo que se denotan grandes avances en distintos campos, pero esto conlleva el manejo de grandes cantidades de información, cuyo manejo debe ser con las medidas adecuadas.

1.2. Seguridad

La seguridad es una necesidad básica. Estando interesada en la protección de la vida y de las posesiones, es tan antigua como ella.

1.2.1. Definición de seguridad

El inicio de la seguridad se remonta a tiempos remotos, desde los orígenes del hombre, junto con el instinto de protección y preservación de la especie. Los primeros conceptos de seguridad, se evidencian en los inicios de la escritura, con los Sumerios (3000 A. C.) o el Código Hammurabi. Escritores como Homero, César y Cicerón denotan prácticas que se implementan en la guerra o en el gobierno. Las pruebas antiguas más importantes, se evidencian en descubrimientos arqueológicos, como las pirámides, palacios, templos, entre otros.

La seguridad es un concepto que ha seguido un proceso evolutivo dentro de las organizaciones sociales y la familia; que en conjunto, surgen técnicas para su protección ante las amenazas que los rodean. A partir de eso, surge lo que es el Estado y su gobierno.

Las primeras evidencias de una cultura, cuya organización de seguridad se considera madura, fue Roma Imperial, de donde nace la “seguridad externa”, que consiste en protección de entes externos a la organización.

La seguridad interna, por otro lado, se refiere a la que se da, dentro de la misma organización. De estos dos conceptos, en conjunto con el concepto de Estado, surgió la seguridad pública y privada.

Por lo que esta viene dada desde los niveles más altos, que pueden ser el gobierno, hasta llegar al ciudadano común, respecto de la importancia y concientización que incluye el manejo de la información, que se involucra en la actualidad.

1.2.2. Valor de la información

La información es cualquier elemento intangible que afecta a la organización, como tal, no tiene un valor establecido, sino que su valor viene dado por quien hace uso de ella. No es como otros recursos como el dinero, la gente o bienes, la información se puede alterar y duplicar fácilmente. Hay ocasiones en que su importancia reside en que esté oculta, dado que de ser expuesta perdería todo su valor.

Una computadora es una herramienta útil que ayuda al manejo de la información, pero depende del usuario, evaluarla y tomar decisiones sobre los datos obtenidos. Existen tres valores que afectan el valor de la información:

- Oportunidad
- Precisión
- Presentación

Mantener en balance estas necesidades crea retos que consisten en que se debe mantener, desechar, encontrar cómo organizarla o quién tiene acceso. Todas estas son interrogantes que deben ser evaluadas, las cuales están asociadas al costo del manejo de la información.

El valor de la información es difícil de establecer; por otra parte, el costo de su administración no, aunque aumenta según qué tan rápido se requiera de la cantidad o qué tan detallada sea.

Consecuentemente, la información para una organización es un factor importante al momento de la toma de decisiones que afecten o no a la rentabilidad de la misma.

1.2.3. Ataques

Delitos cibernéticos están creciendo y para 2017 se espera que el mercado mundial de seguridad cibernética se dispare a $ 120,1 billones. El costo anual estimado sobre la delincuencia cibernética mundial es de $ 100 billones. Entre los datos más relevantes se encuentran:

- Más de 600,000 cuentas de Facebook[1] son comprometidas cada día.
- Uno de cada diez usuarios de redes sociales dice haber caído presa de engaños en redes sociales.
- Los ataques más comunes son: *malware*, robo de información de dispositivos, inyección sql, ataques web, robo de identidad e ingeniería social.
- Las denominadas "*botnets*" tiene alrededor de 120,000 computadoras infectadas, enviando *spam*, cada día.
- Del total por género, 71 % de los hombres y 63 % de las mujeres son cibercriminales.
- Un 59 % de los empleados, admiten haber robado información, antes de dejar su antiguo trabajo.
- Los ciberaques suelen causar el 85 % de costos directamente financiados en EU.
- Los dos países que producen más ataques son Rusia y Estados Unidos.

En la tabla I se muestra el porcentaje en el que es común cada ataque, según su tipo. Esto es importante tomarlo en cuenta para el análisis de los riesgos y evidencia a qué tipo de ataque se está más expuesto de forma generalizada.

[1] Facebook. https://www.facebook.com/. Consulta: 01/11/2014.

Tabla I. **Índice de tipo de ataque**

Tipo de ataque	Porcentaje (%)
Virus, malware, gusanos, troyanos	50
Criminal interno	33
Robo de dispositivos de soporte de datos	28
Inyección SQL	28
Robo de identidad	22
Ataque basado en web	17
Ingeniería social	17
Otros	11

Fuente: *Cyber Crime Statistics and Trends*. http://www.go-gulf.com/blog/cyber-crime/. Consulta: 5 de septiembre de 2014.

Una gran parte de organizaciones consideran que la seguridad informática es un gasto y no una inversión, dado que no se ve directamente reflejado en sus ganancias, únicamente se puede establecer mediante monitoreos, los ataques que han sido evitados. De esta manera se obtienen los análisis y se realizan estadísticas que determinan la situación y los principales ataques a los que se está expuesto. Por lo anterior, es de gran importancia la inversión en seguridad, dado que cuando se percata de alguna anomalía la organización, puede ser demasiado tarde.

En consecuencia, los costos de restauración del sistema pueden ser mucho mayores, a la inversión que se pudo realizar en la seguridad, e incluso, se podría dar la pérdida total de la información como un caso fatal.

1.2.4. Operatividad *versus* seguridad

Elegir las medidas de seguridad que se implementan en un sistema, requiere tomar en cuenta el equilibrio entre los intereses relacionados con la seguridad, los requerimientos operacionales y de qué tan amigable es para el usuario.

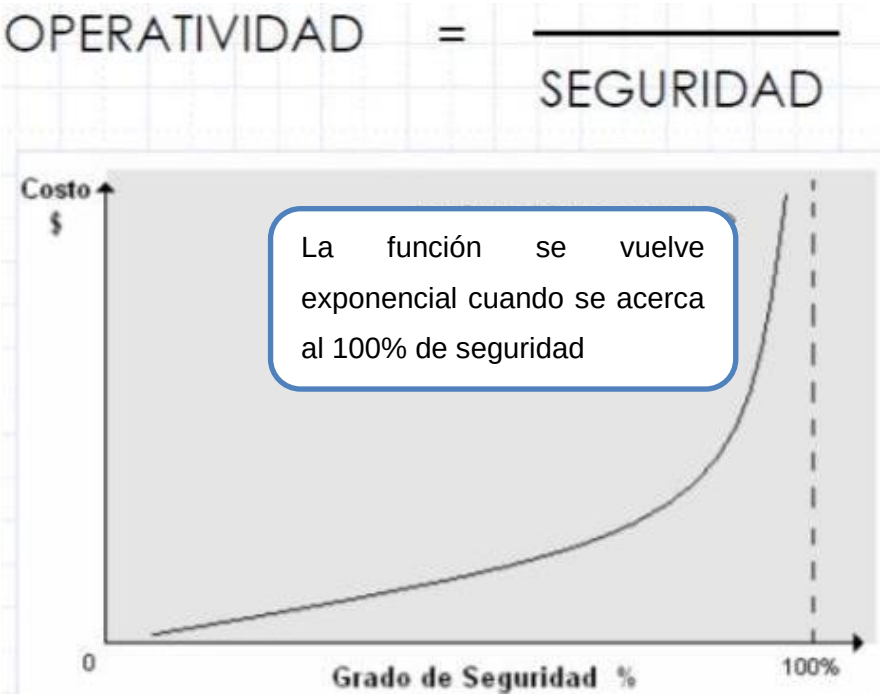
Como ejemplo a lo descrito, se puede imaginar una computadora muy segura:

- Instalada en un refugio subterráneo a gran profundidad
- Sin acceso a redes externas
- Alimentada por un sistema autónomo de energía

Con esto se puede evidenciar que la seguridad y la operatividad, son inversamente proporcionales; es decir, al aumentar la seguridad de un sistema, disminuye su operatividad y viceversa.

Tal como se muestra en la figura 1, el crecimiento del costo, al aumentar la seguridad se vuelve exponencial; todos los procesos son implicados en mantener ese nivel de seguridad.

Figura 1. **Operatividad *versus* seguridad**



Fuente: ALONZO, Sen. *Objetivos de la seguridad informática y posibles riesgos.* http://es.slideshare.net/lucerovaz/objetivos-de-la-seguridad-informatica-y-posibles-riesgos. Consulta: 25 de septiembre de 2014.

Más allá de ello, al ser de índole social, mantendrá siempre un grado de incertidumbre propia de la naturaleza humana, que puede permitir un acceso no autorizado, el cual puede llegar a causar daños.

Se debe tener presente que el concepto de seguridad es relativo; existen niveles mínimos de seguridad que se deben tomar en cuenta, pero esto dependerá de un análisis de riesgos y de si está dispuesto a aceptar sus costos y medidas a aplicar.

1.2.5. Seguridad informática

La seguridad de la información, protege a esta de una amplia gama de amenazas, con el fin de garantizar la continuidad comercial, minimizar el daño al negocio y maximizar el retorno sobre las inversiones y las oportunidades.

1.2.5.1. Implicaciones de la seguridad informática

Los problemas de seguridad informáticos son sucesos que no se espera que ocurran y que en muchos casos se pueden prevenir. Cuando se hace mención de esto, se habla de:

- Alteración de la información
- Invasión a la privacidad
- Pérdida de datos
- Acceso no autorizado

Cada sistema es distinto y maneja diversa información con varios tipos, por lo que su manejo es distinto. En consecuencia, las medidas de seguridad que se toman en cada componente del sistema son diferentes, dependiendo de la tecnología usada en la plataforma y el equipo con el que trabaja. Las funciones y características técnicas de los componentes varían significativamente, según el fabricante, particularmente en el aspecto de seguridad.

En la actualidad, la amenaza más común para los sistemas informáticos se enfoca en la negación del acceso a los servicios, provocando la disminución o eliminación de los recursos o servicios de los que dispone el usuario.

El crecimiento de las telecomunicaciones y la dependencia que existe entre las organizaciones y las tecnologías informáticas, hace de la seguridad un factor crucial, para el manejo de las comunicaciones e información.

Las fallas de seguridad de un sistema son las que se convierten en amenazas susceptibles de ser aprovechadas por usuarios malintencionados para causar daños o algún tipo de invasión a la confidencialidad.

El problema de la seguridad no se resuelve únicamente con solventar las fallas existentes o fortalecer el sistema; este es un problema que va más allá y se convierte en un problema cultural, en el cual el usuario juega un rol fundamental.

La seguridad sobre la información y equipo ya no es responsabilidad solamente del personal técnico designado a la tarea, encargado de resguardar los bienes y servicios brindados por el entorno, sino que además, es el usuario el encargado de velar por la seguridad de los bienes físicos y lógicos tiene a su disposición.

Por esto, es que la seguridad debe estar integrada en todo proceso desde el diseño, para garantizar la evaluación de todos los factores funcionales a tener en consideración para el uso seguro del entorno.

Entonces la seguridad se origina en el diseño formando de manera correcta la estructura de la organización, distribuyendo adecuadamente las tareas, y en contraparte, la información y responsabilidad. Posterior a esto se deben implementar políticas de carácter técnico, con lo que garanticen el uso y disponibilidad, de recursos y servicios, únicamente por usuarios autorizados.

La seguridad ya no es un tema que sea enfocado a expertos o especialistas, sino que se ha llegado a instalar en el escritorio del usuario, en donde nacen los problemas de seguridad.

1.2.5.2. Principios

Cada sistema informático debe contar con una serie de propiedades específicas para poder asegurar que es un sistema seguro y establecer de manera correcta la información pública y privada. Cada una de estas propiedades conlleva la implantación de determinados servicios y mecanismos de seguridad, para su cumplimiento. A continuación se definen dichas características:

1.2.5.2.1. Integridad

Característica de información que se encarga de asegurar que el contenido permanezca sin alteración alguna por parte de personas no autorizadas. Una falla en la integridad puede darse por anomalías en el hardware o software que no fueron previstas, o por personas que lograron ingresar al sistema de forma indebida o con fines maliciosos.

1.2.5.2.2. Confidencialidad

Propiedad que se refiere a la capacidad del sistema de evitar que personas o cualquier tipo de intruso no autorizado pueda acceder al sistema y a la información que allí se almacena. Es una necesidad de que la información sea conocida solo por personas confiables dentro del sistema, con el acceso debido.

1.2.5.2.3. Disponibilidad

Propiedad que se refiere a que el sistema informático está funcionando siempre de manera eficiente y cumpliendo con todas sus funciones; asimismo, es capaz de recuperarse rápidamente si sucediera alguna falla. Esto conlleva a que los equipos de comunicación deben de estar funcionando correctamente y de manera segura; en caso contrario se está expuesto a sufrir cualquier tipo de ataque teniendo como resultado daños a la reputación y consecuencias legales, entre otros.

2. CLASIFICACIÓN Y PLANEACIÓN DE SEGURIDAD

2.1. Seguridad

Propiedad de algo donde no se registran peligros, daños ni riesgos. Una cosa segura es algo firme, cierto e indubitable. La seguridad, por lo tanto, puede considerarse como una certeza.

2.1.1. Seguridad informática

Disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema informático seguro y confiable. Se refiere entonces a las características de sistemas de procesamiento de datos y su forma de almacenamiento y garantizar ciertas propiedades, como: disponibilidad, integridad, confidencialidad y consistencia. En la actualidad, cada vez que se toca el término: información o datos, se hace referencia a la información que está siendo procesada por sistemas electrónico/informático.

Al implementar un sistema de seguridad informática en un sistema de cómputo, como primer punto deberán conocerse las características de lo que se desea proteger; en primer lugar, el conjunto de datos. La información es una colección de datos que tiene significado específico, conciso y general y tiene un determinado fin según cómo o para qué sea procesada. La información tiene un valor relativo pues es un recurso más de los tantos de la organización; sin embargo cuenta con un gran valor, el lugar primordial; generalmente se ignora su valor debido a su propiedad abstracta e intangible.

La seguridad informática implica valores como la confianza y el respeto, dado que siempre que se trabaja con información, cada transacción es muy delicada y debe realizarse con cuidado porque se trabaja con información, muchas veces, ajena. La confianza va del lado del cliente que cree en la organización o la persona detrás del software o hardware, al confiar los datos, por ejemplo en un banco.

El respeto debe ir del lado del usuario del software, pues también existen normas morales para las personas informáticas. La seguridad informática se ha vuelto un factor de gran importancia pues cada vez aumenta más la necesidad de mantener protegida la información que se maneja como transacciones, dispositivos o los usuarios finales.

Entre los principios con los que debe cumplir un sistema informático para determinar que es seguro están: la autenticidad y control, además de disponibilidad, integridad y confidencialidad, que se explican en la sección 1.2.5.2.

2.1.1.1. Autenticidad

Propiedad que se cumple por medio de la implementación de mecanismos para validar accesos al sistema. Permite definir que la información requerida es válida y puede utilizarse; también permite asegurar el origen de la información y validar el origen de la misma.

2.1.1.2. Control

Propiedad con la que debe contar el sistema que permite asegurar que solamente los usuarios autorizados pueden decidir cuándo y cómo permitir el acceso.

2.1.2. Clasificación

Existe una clasificación de la seguridad informática, según el ámbito de trabajo en los que se desempeña el usuario. A continuación se detalla dicha clasificación.

2.1.2.1. Seguridad física

La seguridad física de un sistema informático consiste en la aplicación de barreras físicas y procedimientos de control frente a amenazas físicas al hardware. Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el sistema.

Realizar evaluaciones y controlar permanentemente la seguridad física del sistema es la base para comenzar a integrar la seguridad como función primordial del mismo. Tener controlado el ambiente y acceso físico permite disminuir siniestros y tener los medios para luchar contra accidentes. Es la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. 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.

A continuación se lista un conjunto de desastres que atentan contra la seguridad física de un sistema informático:

- Incendios
- Desastres naturales
- Disturbios internos o externos
- Robos
- Sabotaje

2.1.2.1.1. Control de acceso

El control de acceso se refiere a la acción de identificación de ingreso al inmueble, relacionado con la apertura y cierre de puertas, permitir o negar acceso. Es decir se verificará el nivel de acceso de cada persona mediante aplicación de tecnología con tarjetas o contraseñas de alguna forma. El servicio de vigilancia es el que se encarga del control de acceso de las personas al inmueble, es el encargado de colocar a los guardias en lugares estratégicos para cumplir con sus objetivos y controlar el acceso del personal.

En general se utilizan credenciales de identificación para poder realizar un eficaz control de salida e ingreso del personal de la empresa o personas particulares, en este caso la persona se identifica por algo que posee, por ejemplo una tarjeta de identificación o una tarjeta electrónica. Cada forma de identificación debe tener un único código de identificación que se almacena en una base de datos que tiene el control del servicio de vigilancia. Sin embargo,

como todo, puede tener ciertas desventajas porque es algo físico, por lo tanto puede ser robada, extraviada, entre otros.

2.1.2.1.2. Protección electrónica

Consiste en la detección de robos, asaltos, incendios o cualquier otra situación que pueda ser percibida mediante la utilización de sensores que son conectados a alarmas.

Cuando uno de los elementos sensores detecta una situación de riesgo y transmite inmediatamente el aviso a la central de percepción de anomalías; esta procesa la información recibida. Todos estos elementos poseen un control contra sabotaje de manera que si en algún elemento se produce la rotura de algunos de sus componentes, se enviará una señal de alarma para que esta accione los elementos de señalización correspondiente.

2.1.2.1.3. Sistemas de medición

En este apartado entra el término de biometría; es la parte de la biología que realiza mediciones de forma electrónica, percibe, almacena y compara características únicas para la identificación de personas; se basa en factores genéticos o rasgos físicos. El proceso de identificación consiste en la obtención de características personales que se almacenan en una base de datos, de lo que se obtiene un patrón utilizado para comparar las características físicas de cada persona. Algunos sistemas biométricos son:

- Huellas digitales: identificación de huellas digitales dado que no hay dos huellas idénticas. Es un mecanismo para defender los derechos de autor y erradicar las cosas ilegales.

- Verificación de la voz: se graban frases y se compara la voz, la agudeza, las sílabas percibidas, entre otros. Este sistema es muy sensible a factores externos, como el ruido, el estado de ánimo, enfermedades, entre otros.

- Emisión de calor: se mide la emisión de calor del cuerpo realizando un mapa de valores sobre la forma de cada persona.

- Verificación de patrones oculares: modelos basados en los patrones del iris o la retina y en estos momentos son considerados los más eficaces.

2.1.2.1.4. Condiciones ambientales

Respecto de la ubicación del sistema informático, generalmente se puede saber lo que pasará con aspectos climáticos por avisos de tormentas, sismos, etc. Las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran está documentada. La frecuencia y severidad de su ocurrencia deben ser tomadas en cuenta al decidir la construcción de un edificio.

Algunos factores ambientales que pueden provocar daños son:

- Terremotos
- Incendios
- Inundaciones

2.1.2.2. Seguridad lógica

Es el tipo de seguridad que está relacionado con la protección del software, de los sistemas operativos y con la información en sí. Consiste en la aplicación de barreras y procedimientos que protejan el acceso a los datos y la información. Involucra el control de acceso al sistema. Este tipo de seguridad empezó a tener importancia con el uso de las primeras computadoras; en los 90 la cantidad de ataques a ordenadores, aumentaba y surgen los primeros *malware* sobre todo por el acceso a internet.

El objetivo de implementación de la seguridad lógica es asegurar que los programas no puedan ser alterados por cualquier persona y restringir accesos a estos y a los archivos, para que la información procesada no caiga en manos de personas no autorizadas o destinatarios erróneos y prevalezca la integridad de la misma. Que existan sistemas secundarios para la transmisión de información en dado caso existan fallos en los principales. Todo radica en el cuidado de la información y que no caiga en manos de terceros.

2.1.2.2.1. Seguridad de accesos

Es la seguridad en los ingresos al sistema, a las aplicaciones, sistema operativo, bases de datos, entre otros. Mantener la seguridad en los accesos es muy importante pues de esta manera se tiene control sobre usuarios que se registran para poder acceder a información confidencial de la organización y se protege el sistema de modificaciones o alteraciones no autorizadas y anónimas.

NIST determinó que los requisitos mínimos de seguridad lógica en un sistema informático son los siguientes:

- Autenticación: permite controlar el acceso de las personas al sistema informático, dejando ingresar únicamente a las personas que el sistema de identificación reconozca y pueda autenticar su identidad. Una forma de implementar la identificación única de usuarios es utilizando un servidor de autenticaciones sobre el cual los usuarios se identifican, y este se encarga luego de autenticar al usuario sobre los restantes equipos a los que pueda acceder. En la figura 2 se muestra cómo funcionan los intentos de inicio de sesión por fuerza bruta.

Figura 2. **Inicio de sesión por fuerza bruta**

Fuente: Cisco Systems, Inc. Informe anual de seguridad Cisco (2014). http://www.cisco.com/assets/global/ES/pdfs/executive_security/sc-01casr2014_cte_lig_es_35330.pdf. Consulta: 12 de octubre de 2014. p. 54.

- Roles: los roles son perfiles que permiten agrupar usuarios que cumplen una determinada función y de esta forma se facilita la configuración de seguridad lógica al asignar a cierto grupo de usuarios algunos derechos o restricciones para indagar por el sistema.

- Transacciones: la seguridad también se puede implementar sobre cada transacción; para la ejecución de una determinada transacción será necesario autenticarse o simplemente pedir una clave.

- Limitación de servicios: limitaciones que se asignan a determinados programas o archivos que personas con mayor autoridad de acceso o administradores del sistema, establecen sobre ellos para cuidado de la información y software sensible.

- Forma de acceso: son permisos que los usuarios tienen sobre determinados programas, archivos o información en general.

    - Creación
    - Lectura
    - Escritura
    - Búsqueda
    - Borrado
    - Ejecución
    - Todos los anteriores

- Horario: permite limitar el acceso de los usuarios a determinadas horas del día o a determinados días de la semana y también según ubicación. Con la implementación de este requerimiento se mantiene un control más restringido de los usuarios y zonas de ingreso.

- Control de acceso interno: son formas de seguridad interna, sumergidas en el funcionamiento lógico del sistema, entre ellas cabe mencionar:

    - Encriptación

- Contraseñas
- Listas de control de acceso
- Etiquetas de seguridad

- Control de acceso externo: son formas de seguridad en el ámbito de amenazas externas de tipo lógico, temiendo la intrusión de terceros en el ámbito lógico del sistema informático.

  - *Firewall*
  - Accesos públicos
  - Control de puertos

- Administración: cuando se establecen los controles de acceso, tanto interno como externo, se debe crear y manejar la administración eficiente de estos requerimientos para su correcto funcionamiento y resultados esperados, lo cual involucra medidas de seguridad lógica, implementación, pruebas y modificaciones sobre los accesos de los usuarios de los sistemas.

El establecimiento de los permisos de acceso requiere determinar cuál será el nivel de seguridad necesario sobre los datos, por lo que es imprescindible clasificar la información, determinando el riesgo que produciría una eventual exposición de la misma a usuarios no autorizados.

2.2. Planeación

Es importante que cada organización cuente con un plan estratégico de políticas de seguridad informática, que sea capaz de resguardar y proteger la información y demás recursos lógicos que representan valor para dicha

organización. Además de eso, el plan de seguridad debe abarcar más allá de los recursos lógicos e intangibles; se deben tomar en cuenta los recursos físicos como computadoras, impresoras, fotocopiadoras y demás hardware que utilice la compañía, así como el inmueble en el que se trabaje y los recursos humanos.

Por lo tanto, al momento de pensar en crear un plan de seguridad para protección de la organización y todos los recursos que maneja, tanto lógicos como físicos, debe conocerse a profundidad cada elemento y su funcionamiento, así como todo lo que implica poseer dicho recurso, sus debilidades, vulnerabilidades, riesgos y el posible impacto que algún tipo de amenaza podría ocasionarle.

2.2.1. Identificación y análisis de recursos

Para planear la implementación de un sistema de seguridad, se debe:

- En primer lugar debe realizarse un inventario sobre todos los recursos con los que se cuenta, tanto físicos como lógicos e identificar sus características.

- Identificar la relación que existe entre los recursos y la influencia que se ejercen uno sobre otro y cómo afectaría a los demás el daño que pudiera ocurrir en alguno de ellos.

2.2.1.1. Activos

Son los recursos propios de una organización y que ayudan a que esta lleve a cabo sus funciones y logre sus objetivos. Los activos de un sistema

informático son: hardware, software, información, redes, instalaciones, servicios y recursos humanos.

2.2.1.1.1. Datos

Constituyen la información, núcleo de la organización y todos los demás recursos están para procesarlos y protegerlos. Generalmente son almacenados y organizados en bases de datos.

2.2.1.1.2. Hardware

Equipo físico que contiene todo el software y permite su ejecución y la interacción con el mismo. En este conjunto están incluidos todos los periféricos, *router*, módem, servidores y demás accesorios necesarios para el funcionamiento de los equipos parte del sistema.

2.2.1.1.3. Software

Conjunto de todos los programas que se ejecutan para procesamiento de la información (sistemas operativos, aplicaciones instaladas).

2.2.1.1.4. Redes

Internet o demás redes metropolitanas, así como las propias de la organización. Representan la vía de comunicación y transmisión de datos.

2.2.1.1.5. Instalaciones

Lugares que almacenan los sistemas informáticos y de comunicación. Se refieren al inmueble, comúnmente oficinas, edificios, locales o vehículos.

2.2.1.1.6. Servicios

El conjunto de servicios de comunicaciones, seguridad o transferencia de información que se ofrecen al cliente o también a los usuarios como correo electrónico, productos en línea, entre otros.

2.2.1.1.7. Recurso humano

Conjunto de personas que conocen e interactúan con el sistema, programadores, administradores, usuarios, entre otros.

2.2.2. Análisis de vulnerabilidades y riesgos

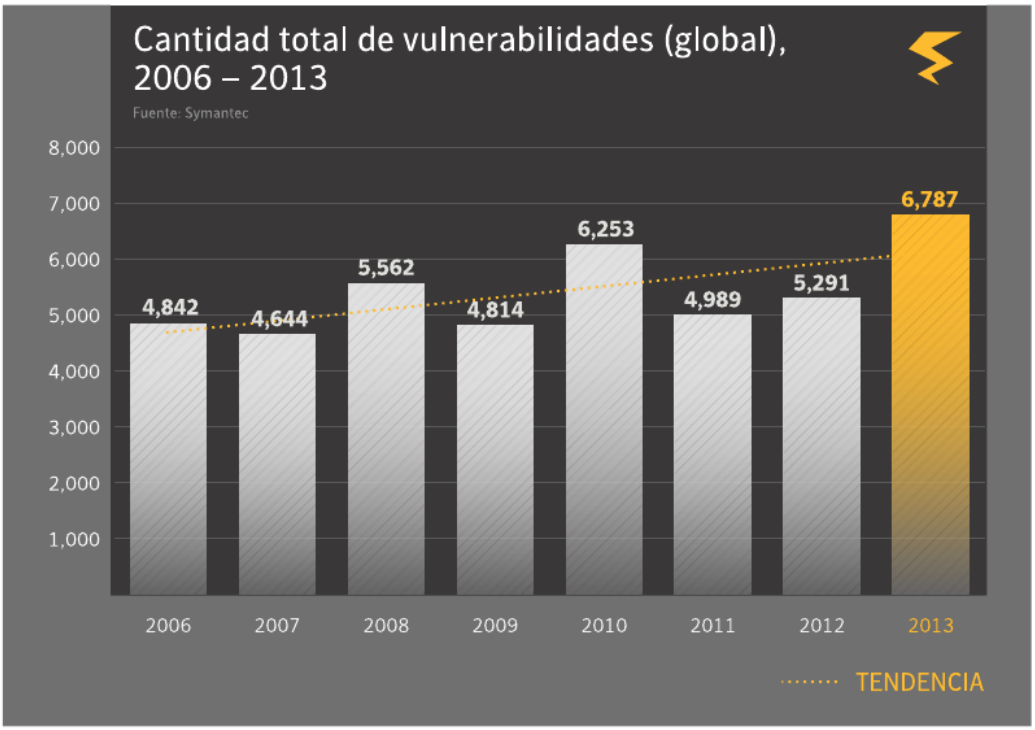
Los riesgos siempre están presentes cuando se trata del manejo de información, sobre todo cuando un tercero llega a involucrarse.

2.2.2.1. Vulnerabilidades

Las vulnerabilidades son debilidades que comprometen la seguridad de un sistema informático. Son probabilidades de que una amenaza se materialice contra un recurso de la organización, se pueden originar por diversidad de factores como errores de configuración, factores técnicos, ambientales, entre otros.

Cada activo de la empresa es diferente en su totalidad, por lo cual se debe tomar en cuenta las vulnerabilidades de cada uno. En la figura 3 se observa una gráfica que indica la cantidad de vulnerabilidades a nivel global de 2006 a 2013.

Figura 3. **Cantidad total de vulnerabilidades (global)**



Fuente: Symantec. *Tendencias de seguridad cibernética*. https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf. Consulta: 23 de octubre de 2014. p. 21.

2.2.2.2. Riesgos

Son las probabilidades de que cierta amenaza se desarrolle sobre un activo aprovechando las vulnerabilidades del mismo. En la tabla II se observan algunos tipos de riesgo que existen y el factor de peligro de cada uno. Cada organización puede reaccionar ante los riesgos según su plan de seguridad, es decir de manera distinta, pero tiene tres alternativas por optar:

- Tratarlo por transferencia: dejar que personas especializadas de alguna organización que se dedique a riesgos, se encargue de reparar.
- Aplicar medidas de la organización para anularlo.
- Asumirlo sin realizar ninguna acción.

Algunas preguntas efectivas para la identificación de riesgos en la organización son:

- "¿Qué puede ir mal?"
- "¿Con qué frecuencia puede ocurrir?"
- "¿Cuáles serían sus consecuencias?"
- "¿Qué fiabilidad tienen las respuestas a las tres primeras preguntas?"
- "¿Se está preparado para abrir las puertas del negocio sin sistemas, por un día, una semana, cuánto tiempo?"
- "¿Cuál es el costo de una hora sin procesar, un día, una semana?"
- "¿Cuánto tiempo se puede estar *off-line* sin que los clientes se vayan a la competencia?"
- "¿Se tiene forma de detectar a un empleado deshonesto en el sistema?"
- "¿Se tiene control sobre las operaciones de los distintos sistemas?"
- "¿Cuántas personas dentro de la empresa, (sin considerar su honestidad), están en condiciones de inhibir el procesamiento de datos?"
- "¿A qué se llama información confidencial y/o sensitiva?"
- "¿La información confidencial y sensitiva permanece así en los sistemas?"
- "¿La seguridad actual cubre los tipos de ataques existentes y está preparada para adecuarse a los avances tecnológicos esperados?"
- "¿A quién se le permite usar qué recurso?"

- "¿Quién es el propietario del recurso? y ¿quién es el usuario con mayores privilegios sobre ese recurso?"
- "¿Cuáles serán los privilegios y responsabilidades del administrador vs. la del usuario?"
- "¿Cómo se actuará si la seguridad es violada?"

Posteriormente se debe determinar el nivel de riesgo obtenido y la evaluación de costos por riesgo identificado. La figura 4 muestra el riesgo de *malware* por sector, en una empresa.

2.2.3. Políticas de seguridad

Para poder controlar la información propia en cualquier ámbito de tratamiento se deben conocer a profundidad las políticas de seguridad que ofrece el proveedor del servicio.

2.2.3.1. Definición de protección y política de seguridad

Protección en informática, se refiere a evitar el daño ya sea que llegue a la información, o algo que lo produzca. Para ello se implementan políticas de seguridad.

Una política de seguridad es un documento en el cual se establecen pautas, según el enfoque de la organización en cuanto a seguridad.

Contiene los principios de seguridad sobre los cuales se han de basar las normas, procedimientos y estándares. Debe ser conocida y acatada por todos

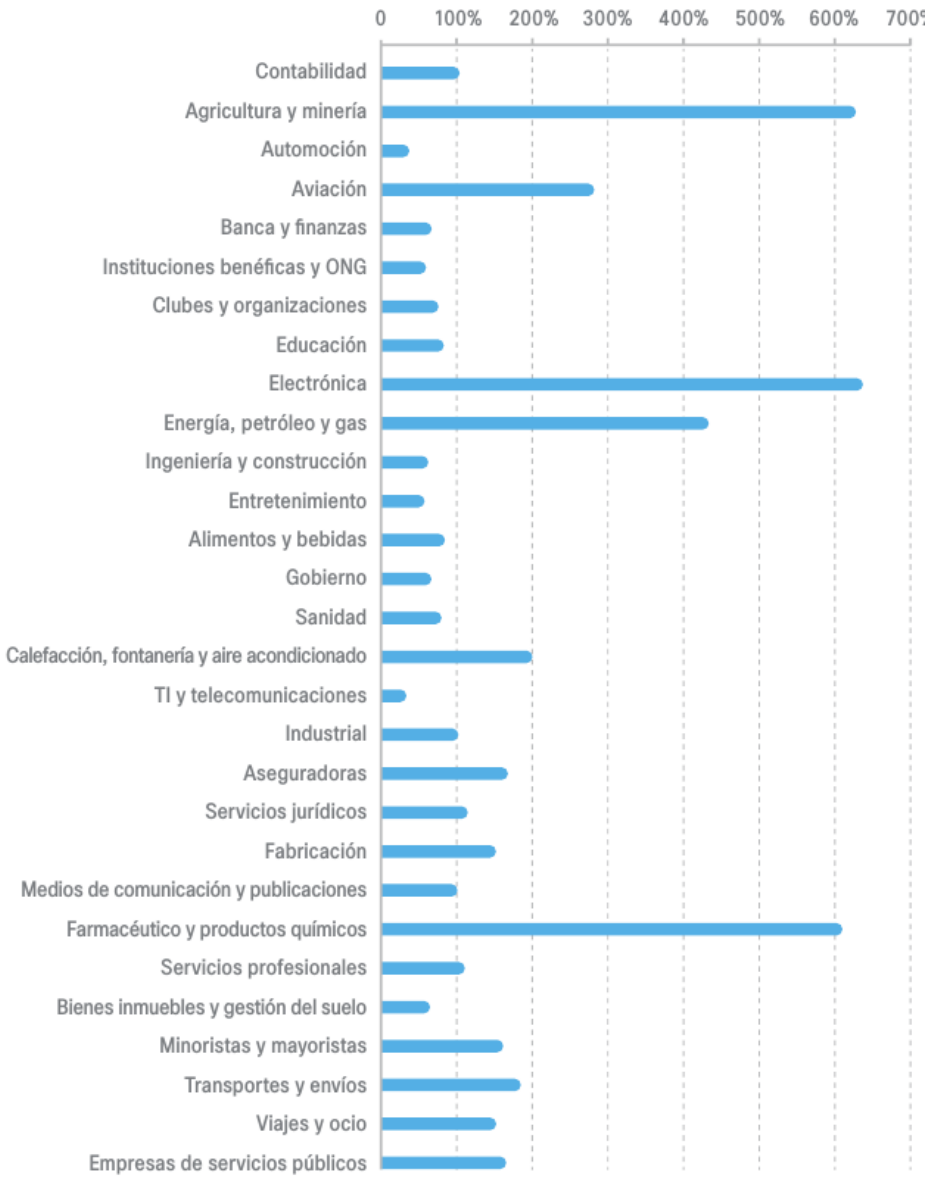
los miembros de la organización y creada, bajo el consentimiento absoluto de la gerencia.

Tabla II. **Tipos de riesgos–factor**

Tipo de riesgo	Factor
Robo de hardware	Alto
Robo de información	Alto
Vandalismo	Medio
Fallas en los equipos	Medio
Virus informáticos	Medio
Equivocaciones	Medio
Accesos no autorizados	Medio
Fraude	Bajo
Fuego	Muy Bajo
Terremotos	Muy Bajo

Fuente: elaboración propia.

Figura 4. **Riesgos de los sectores y encuentros con *malware* web**



Fuente: Cisco Systems, *Inc. Informe anual de seguridad Cisco*. http://www.cisco.com/assets/global/ES/pdfs/executive_security/sc-01casr2014_cte_lig_es_35330.pdf. Consulta 25 de octubre 2014.

Entre los principios que debe contener, se encuentran:

- Eficacia: es garantizar que la información que sea utilizada, es necesaria y que sea entregada de forma oportuna, consistente y útil, para el desarrollo de las diversas actividades.

- Eficiencia: asegurar el uso adecuado de los recursos, según sean los requerimientos.

- Integridad: que sea procesada la información adecuada y suficiente, para cumplir con las actividades.

- Exactitud: la información debe estar libre de errores/fallos.

- Disponibilidad: la información debe estar accesible cuando se necesita, es decir, no deben existir interrupciones significativas en el proceso. Para cumplir esto se involucra el uso de técnicas de resguardo y recuperación de la información.

- Legalidad: toda la información, incluyendo su proceso y transporte, debe cumplir con las regulaciones establecidas.

- Confidencialidad: la información está protegida de accesos no autorizados. Solo puede acceder el usuario designado para ello.

- Autorización: todo transporte, proceso o transacción, debe cumplir con la autorización adecuada.

- Protección física: garantizar que todos los medios de proceso o almacenamiento, cuenten con medidas de protección que evitan una intrusión al sistema.

- Propiedad: asegurar que los usuarios tienen establecidos adecuadamente los derechos sobre la información que usan para realizar sus tareas.

- No repudio: garantizar los medios necesarios, para que el receptor de la comunicación pueda corroborar completamente, la autenticidad del emisor.

2.2.3.2. Parámetros para establecer políticas de seguridad

Al realizar la implementación de políticas de seguridad es recomendable involucrar las áreas propietarias de los activos y servicios que la organización posee, dado que ellos tienen la experiencia suficiente y la capacidad de establecer el alcance y realzar características del área en cuestión. La comunicación también es un factor primordial en el desarrollo de las políticas; todo el personal debe estar al tanto y ser involucrado en el desarrollo e implementación del plan de seguridad, con los beneficios por recurso, riesgos y demás elementos.

Es necesaria la identificación de los niveles de autoridad para la toma de decisiones relacionadas con el bien de los recursos con los que se cuenta. Asimismo, debe desarrollarse un proceso de monitoreo periódico en los ámbitos de implementación.

3. AMENAZAS

3.1. Definición de amenaza informática

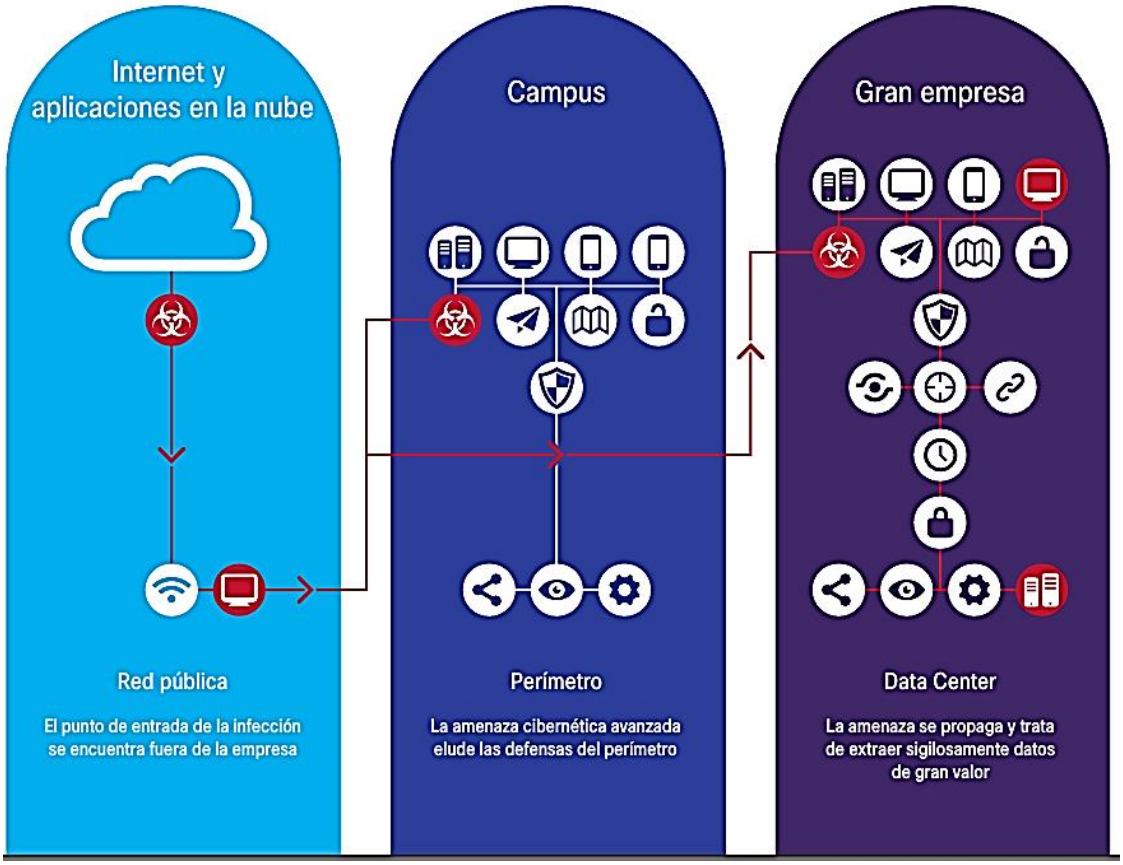
En informática, cualquier acción o evento que sea capaz de ocasionar algún daño sobre elementos del sistema o perturbaciones a la información, causando pérdidas materiales o lógicas, es conocido como una amenaza informática. Este tipo de vulnerabilidades puede presentarse en cualquiera de las partes que conforman una computadora (software, hardware). Muchas amenazas son inevitables e incluso no pueden ser pronosticadas, por lo que cada sistema informático debe contar con la protección necesaria para controlar el efecto de acción de una amenaza, según sea el tipo de sistema que se maneje.

Existe gran cantidad de amenazas para sistemas informáticos, formas en que pueden ser atacados, infectados o hasta sufrir robos de información. Es importante conocer la constitución de las amenazas y la figura 5 muestra la anatomía de las mismas. Las amenazas informáticas suelen mostrar muy poco o nada de los síntomas que ocasionan, por lo que pueden vivir sumergidas en el sistema durante un largo tiempo, sin ser detectadas.

3.2. Clasificación de amenazas

A continuación se detallan los conceptos de los tipos de amenaza a los que está expuesto cualquier usuario que adopta un servicio informático.

Figura 5. **Anatomía de una amenaza moderna**



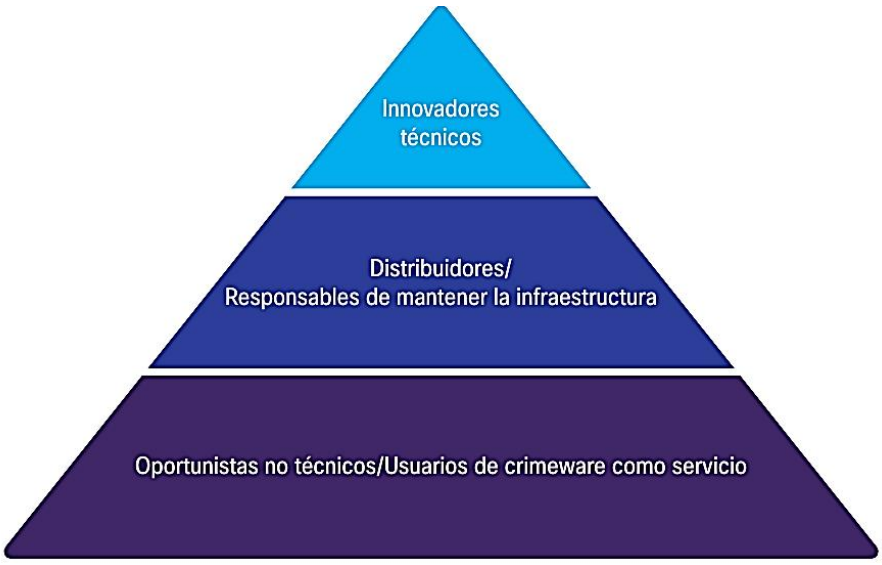
Fuente: Cisco Systems, *Inc. Informe anual de seguridad Cisco*. http://www.cisco.com/assets/global/ES/pdfs/executive_security/sc-01casr2014_cte_lig_es_35330.pdf. Consulta: 28 de octubre de 2014.

3.2.1. Amenaza humana

Una amenaza humana son todos aquellos seres humanos atacantes del sistema informático que buscan causar un daño significativo o llevar a cabo el robo de algún recurso; a estas personas comúnmente se les llama: *hacker*.

El término “*hacker*” se ha ido distorsionando con el pasar de los años y se cree que son personas con un profundo conocimiento sobre máquinas y que se aprovechan de ello para realizar estafas sobre cualquier organización. Sin embargo, *hacker* es en realidad una persona que vive aprendiendo y es paciente, indaga en aspectos minuciosos para alimentar sus conocimientos y todo lo ve como un reto, una meta por alcanzar. Es importante reconocer que en el campo de los ciberdelincuentes también existe determinada jerarquía, la cual se detalla en la figura 6.

Figura 6. **La jerarquía del ciberdelincuente**



Fuente: Cisco Systems, *Inc. Informe anual de seguridad Cisco*. http://www.cisco.com/assets/global/ES/pdfs/executive_security/sc-01casr2014_cte_lig_es_35330.pdf. Consulta 13 de octubre 2014.

En muchos casos, no solamente en el área de la informática, el espíritu de esta cultura se extiende a cualquier área del conocimiento humano donde la creatividad y la curiosidad son importantes. Principalmente buscan la liberación

del software y la información. Actualmente este término es mayormente aplicado a todos los usuarios que se agrupan en distintas comunidades que tienen distintas funcionalidades en lo que respecta a la informática y, sobre todo, al manejo de la información en internet.

3.2.1.1. Otras amenazas humanas

Además de las amenazas humanas previamente expuestas, existen otras que es importante mencionar dado que también representan peligros para la información de los usuarios.

3.2.1.1.1. *Copyhackers*

Es la persona que realiza copias de contenido multimedia ajeno y los vende y distribuye de forma ilegal.

3.2.1.1.2. Samurai

Es una persona que se dedica a realizar investigaciones sobre fallos de seguridad bajo contrato o encargo, a cambio de dinero. Se basan en el pensamiento de que cualquier persona u organización puede ser atacada; solamente es necesario que alguien lo requiera y tenga con qué pagarlo.

3.2.1.1.3. *Crackers*

Personas con fines maliciosos, entran en sistemas vulnerables y hacen daño en el mismo por deseos de venganza o simple diversión. También diseñan programas para romper la seguridad, comúnmente empleando ingeniería inversa.

3.2.1.1.4. *Phreakers*

Se le llama a la persona que practica la actividad de engaño a compañías telefónicas, *phreaking*. Realiza investigaciones sobre los sistemas telefónicos para obtener beneficios, como llamadas gratuitas.

3.2.1.1.5. Creadores de virus

Personas que crean software malicioso para penetrar en los sistemas computarizados. Realizan investigaciones para conocer las vulnerabilidades de los sistemas y se filtran en el medio utilizando la ingeniería social; de esta forma crecen y se reproducen.

3.2.1.1.6. *Wannaber*

Persona que quiere imitar a otra. Desea realizar las actividades de un *hacker*, pero su coeficiente no es suficiente para ser uno de ellos.

3.2.1.1.7. *Newbie*

Principiante curioso en el ámbito de *hacking*. Empiezan a indagar en sistemas pequeños y de fácil acceso implementando la técnica de prueba y error.

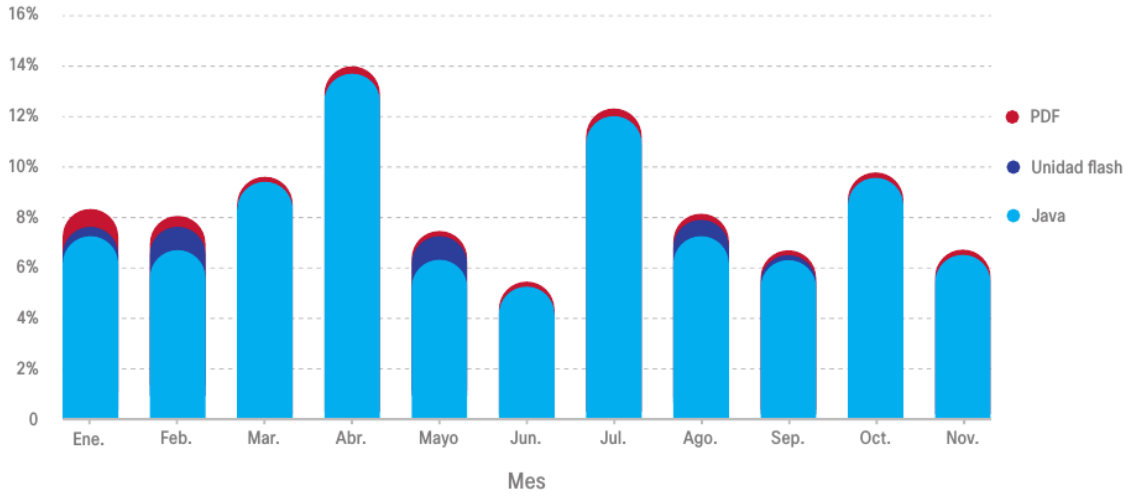
3.2.1.1.8. Lammer

Son personas que se jactan de realizar *hacking*, cuando en realidad no poseen los conocimientos necesarios. Generalmente causan estragos de software para aparentar que tienen conocimientos de *hacker*.

3.2.2. Amenaza lógica

Todo software malicioso llamado malware, que fue creado para dañar sistemas informáticos o incluso fallos en la programación de las aplicaciones, que aun no siendo su fin pueden ocasionar daños o pérdidas, significativos. Algunos ejemplos se muestran en la figura 7.

Figura 7. **Ataques malintencionados generados mediante PDF, *flash* y Java**



Fuente: Cisco Systems, *Inc. Informe anual de seguridad Cisco.* http://www.cisco.com/assets/global/ES/pdfs/executive_security/sc-01casr2014_cte_lig_es_35330.pdf. Consulta 15 de octubre de 2014.

Para lograr la identificación de amenazas, es necesario tener un conocimiento previo de los tipos de ataques, la forma de funcionamiento, el tipo de acceso y los objetivos del atacante. Las consecuencias de los ataques se clasifican en:

- Corrupción de información

- Negación de servicio (*Denial of Service - DoS*)
- Filtración (*leakage*)

3.2.2.1. Ejemplos

A continuación se muestran ejemplos de los ataques mencionados en la figura 7, con el fin de que el usuario prevenga los posibles ataques que pueden venir de esa forma así como las infecciones por tipo de *malware* que se muestran en la tabla III.

3.2.2.1.1. Software incorrecto

Se le denomina software incorrecto a los programas que contienen errores de programación existentes, gracias a programadores que de forma involuntaria fallaron al momento de creación de la aplicación. A estos errores se les llama: *bugs*.

3.2.2.1.2. Puertas traseras

Secuencia dentro del código, por la que se pueden saltar partes del sistema de seguridad para poder acceder al sistema informático.

Pueden ser utilizadas con fines dañinos o simplemente para utilizar una entrada secreta, pero es riesgoso dado que pone en peligro al sistema al dejar una puerta abierta entre la seguridad general.

3.2.2.1.3. Gusanos

Programas informáticos que tienen la capacidad de duplicarse a sí mismos; se propagan de máquina a máquina. Sin embargo, a diferencia de los virus, son capaces de replicarse y crecer, sin necesidad de la ayuda de una persona.

3.2.2.1.4. Virus

Es un programa o parte de código que es cargado en la computadora sin que el usuario se dé cuenta o en contra de su voluntad y tiene por objeto alterar las funciones normales de la computadora y destruir la información almacenada. Generalmente, reemplazan archivos ejecutables por código infectado.

3.2.2.1.5. Caballo de Troya

Es un tipo de virus que se disfraza de programas o archivos que realizan lo que el usuario espera o necesita, pero en realidad ejecuta funciones ocultas con el objeto de infectar y causar daño. Busca crear una puerta trasera que dé acceso al atacante no autorizado para que realice lo que requiera en la computadora.

3.2.3. Amenaza física

Amenazas ocasionadas por las personas o la naturaleza del medio físico donde se encuentra ubicado el sistema informático.

Tabla III. **Infecciones por tipo de *malware***

Tipo de malware	Porcentaje
Troyanos	78,97 %
Virus	6,89 %
Gusanos	5,83 %
Adware/spyware	5,03 %
Otros	3,27 %

Fuente: *Informe anual PandaLabs*. http://www.pandasecurity.com/spain/mediacenter/src/uploads/2014/07/Informe-Anual-PandaLabs-20132.pdf. Consulta 2 de noviembre de 2014.

3.2.3.1. Clasificación de amenazas físicas

Además de existir ataques cibernéticos que atentan contra la información del usuario, existen situaciones naturales que pueden causar daños en la misma.

3.2.3.1.1. Terremotos

Fenómenos naturales que ocasionan fuertes sacudidas a raíz de la liberación de energía que se acumula como ondas sísmicas. La magnitud de un terremoto varía, puede ser muy fuerte o casi pasar desapercibida; en este caso sería un simple temblor. Según la magnitud del terremoto será el daño ocasionado a los elementos del sistema informático.

3.2.3.1.2. Incendios

Los incendios pueden provocar daños irreparables dado que el fuego es una de las principales amenazas físicas por los riesgos que implica. Puede destruir muy fácilmente el hardware y muchas veces por consiguiente, también el software; por lo tanto deben implementarse sistemas antifuego para proteger la información lo mejor que se pueda.

3.2.3.1.3. Instalaciones eléctricas

Al trabajar con equipos de cómputo se trabaja también con electricidad y se debe considerar una serie de aspectos que pueden ser causas graves de daños a raíz de la utilización de electricidad. En las instalaciones eléctricas se deben considerar los siguientes aspectos: ruidos electromagnéticos, forma segura de cableado, pisos de placas extraíbles, un buen sistema de aire acondicionado y emisiones electromagnéticas.

3.2.3.1.4. Inundaciones

Fenómeno natural que ocurre según la ubicación del sistema informático o fallas de infraestructura. Es la ocupación del agua de áreas que en condiciones normales se encuentran secas; se producen debido al efecto del ascenso temporal del nivel del río, lago u otro.

3.3. Análisis de las amenazas

El realizar un análisis de los riesgos y amenazas que pueden abordar un sistema informático, requiere la investigación y análisis secuencial de todos los elementos que conforman el sistema en sí, sus vulnerabilidades, riesgos,

seguridad existente, posible impacto que causaría un ataque sobre determinada pieza.

Para dotar al sistema de políticas de seguridad que garanticen control sobre las amenazas, riesgos y vulnerabilidades que puedan presentarse, es necesario suministrar al sistema informático de constantes revisiones sobre cada uno de los elementos y recursos que lo componen en diferentes tiempos, pues al estar interrelacionados, el fallo de un solo elemento puede producir errores en cadena y dañar gran parte del sistema o el sistema en su totalidad. Identificar los riesgos y amenazas del sistema permitirá conocer los riesgos potenciales que amenazan la seguridad del mismo, por lo que las amenazas pueden ser analizadas en tres momentos diferentes: prevención, detección y recuperación.

3.3.1. Prevención

Prevención se refiere a la fase inicial, es decir estar previamente preparado. Se compone de mecanismos que aumentan la seguridad de un sistema durante su funcionamiento normal. Consiste en condicionar el sistema con un conjunto de normas estáticas para protegerlo de posibles ataques.

3.3.2. Detección

Se refiere a las acciones que se llevan a cabo mientras se realiza el proceso. Son mecanismos orientados a revelar violaciones o estragos en la seguridad. Por lo general son programas de auditoría, sin verificaciones adicionales que detectan y reportan acciones anormales.

3.3.3. Recuperación

La recuperación conlleva todas las acciones que se realizan posterior a un ataque. Son mecanismos que se aplican cuando violaciones al sistema han sido detectadas para regresar al sistema a un estado estable o normal

3.4. Tipos de amenaza

Los tipos de amenaza que se presentan son por la forma de acción y los efectos que tiene sobre los elementos afectados según el momento y forma en que se ejecuten. Esta definición de tipos engloba la clasificación que se presenta en la sección 3.2.

3.4.1. Por el origen

Las amenazas por el origen pueden ser externas o internas. En un entorno externo es posible que alguna forma de amenaza humana o lógica pueda entrar y realizar alteraciones o robo de recursos; sin embargo, limitar el entorno externo no quiere decir que se tendrá un sistema seguro, garantizando ningún tipo de ataque.

3.4.1.1. Amenazas internas

Tienen origen cuando ciertas personas poseen acceso autorizado a la red o sistema de forma lógica o de forma física. Una amenaza interna es alguien que tiene conocimiento del funcionamiento del software y del funcionamiento en general, conoce las políticas internas y los demás roles que se juegan en el sistema. Por lo general conocen información valiosa y saben cómo acceder a ella.

Generalmente son más serias que las amenazas externas porque el personal técnico interno tiene conocimiento excesivo sobre funcionamiento, ubicación, arquitectura de la seguridad, entre otros, y no se tiene control de tráfico interno pues la mayoría de respaldos y protección existente se da con temor y prevención de amenazas externas.

3.4.1.2. Amenazas externas

Generalmente son amenazas humanas que trabajan fuera de la organización, no tienen autorización de acceso para ingresar a la red o al sistema informático por lo que realizando acciones no autorizadas logran ingresar a la red, principalmente desde internet. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos.

3.4.2. Por el medio

Según el medio de desarrollo de operación del atacante, existe una división de amenazas:

- Ingeniería social: es la manipulación de las personas buscando convencerlas para que realicen acciones que revelen lo necesario para superar las barreras de seguridad.

- *Phishing*: es un tipo de estafa que se realiza con el fin de obtener información confidencial de personas u organizaciones, como claves de acceso, datos de cuentas específicas, contraseñas, entre otros.

- Virus: amenaza lógica que tiene por objetivos la alteración del funcionamiento normal de un ordenador.

- Denegación de servicio**:** es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

3.4.3. Por el efecto

Las amenazas que entran en el círculo “por el efecto”, se estudian por la forma de realización del ataque hacia un usuario (persona u organización) y la magnitud que tiene dicho ataque. Entre los más comunes cabe mencionar:

- Estafas
- Robo de información
- Suplantación de identidad, publicación de información personal
- Destrucción de información
- Anulación de funcionamiento de sistemas

4. SEGURIDAD A NIVEL DE USUARIO

4.1. Información

Existen diversos modelos para la clasificación de la información, varían en cuanto a popularidad y es importante tomar en cuenta, el objetivo de una organización, para la elección del modelo, dado que este se debe ajustar a dichos objetivos.

4.1.1. Tipos de información

La información se puede clasificar según su estado para el usuario y para terceros que se involucran directa o indirectamente con ella. Los tipos de información son:

4.1.1.1. Confidencial o sensible

Es la información cuyo acceso es restringido con un elevado grado de confidencialidad y solamente tiene acceso un grupo pequeño de usuarios, donde debe realizarse una serie de controles estrictos. Ejemplo de ello son:

- Planes de fusión de empresas
- Datos sobre cuentas bancarias
- Fórmulas críticas sobre patentes

Los que manejan este tipo de información o inclusive el mismo dueño, debe clasificar y procesar, de acuerdo con el procedimiento de trato de la información.

Además, si es requerido, se debe incluir un registro histórico de toda modificación que se haga sobre dicha información.

4.1.1.2. Restringida

Es acceso de restricción media sobre el cual es necesario realizar conjunto establecido de controles, para asegurar el acceso a la información. A este tipo de información pueden accesar, por ejemplo, empleados con un nivel de seguridad medio, en una organización.

4.1.1.3. Pública

Información de libre acceso, la cual se encuentra disponible para toda la comunidad y se realizan controles mínimos para su acceso.

4.1.1.4. Privada

Es la que se encuentra relacionada, únicamente con el individuo; esta se refiere a aquella que afecta la intimidad personal, la seguridad nacional o simplemente se encuentra excluida por la ley.

4.1.1.5. Uso interno

Es la que se relaciona con las operaciones del día a día. Se refiere a la información que surge de los procesos que se están realizando.

4.1.2. Manejo de la información

La información, es la materia prima para la toma de decisiones, y de su calidad, depende en gran parte, la calidad de la toma de decisiones por parte de analistas o interesados en general.

El manejo de la información es un proceso que involucra al encargado del mismo con un rol de informador, pero para realizar dicha tarea tiene que estar informado, es decir, debe, en primer lugar, crear una representación de la realidad, con los datos adquiridos, para disponer de ello y dar dicha representación a los interesados.

El manejo de la información, involucra las siguientes características:

- Dinámico: dado que se encuentra con movimiento continuo
- Inevitable: se necesita la transmisión de significados
- Irreversible: una vez realizado, no se puede borrar o deshacer
- Bidireccional: existe una respuesta hacia ambas direcciones
- Verbal y no verbal: implica la utilización de ambos lenguajes

Sin duda, el manejo de la información es un factor de gran importancia que el usuario debe tomar en cuenta al momento de navegar en internet. Uno de los temores más grandes es la privacidad, dado que es algo que no se puede garantizar de forma absoluta. De forma contradictoria, la forma tradicional de navegar y compartir contenido es muy abierta, y las personas desean privacidad, compartiendo información personal, imágenes y demás contenido privado.

Está claro que la información no se refiere solamente a datos personales, nombre, dirección, cuenta bancaria, sino que está incluida la información comprendida por gustos particulares, preferencias, forma de actuar y absolutamente todo lo que nos rodea.

Las empresas y sitios web, no solamente saben quiénes somos, sino que tienen información de lo que alguien hace o le gusta, llegando al punto de predecir, qué es lo que alguien hará o le gustará.

Esto puede poner a pensar y hace surgir la duda, de que si el anonimato perfecto existe. Y la respuesta es que sí, pero solamente bajo ciertos límites y de forma transitoria. Por ejemplo, si se usa una computadora pública, para realizar un acceso anónimo a información privada, con una cuenta falsa, realizar el rastreo puede ser muy difícil, al menos identificar la información asociada al responsable, por medio del acceso que hizo, sería casi imposible

4.2. Plan de aseguramiento

Este es un documento que describe de forma detallada los cambios, controles y medidas que se han de implementar, con la finalidad de mantener el sistema íntegro, mitigando los riesgos conocidos.

Como resultado del análisis de vulnerabilidades, se obtienen medidas de control, las cuales son planteadas en el plan de aseguramiento, con el fin de reducir el riesgo ligado a dichas vulnerabilidades, tanto en aspectos tecnológicos, como funcionales.

4.2.1. Protección física

Una forma de proteger la información es de forma física, es decir

4.2.1.1. Instalaciones

Este apartado se enfoca al aseguramiento del edificio salas e instalaciones en general, a nivel físico. Para realizar esto se identifican sectores en el lugar, de común acceso, para los usuarios, después los sectores a los que se debe tener acceso restringido, con su respectivo nivel de seguridad asociado.

Después se establece un perímetro de seguridad, según el cual se establece una zona de confianza, en la cual se implementan medidas de protección con lo que se pueda tener cierto grado de seguridad.

Con esto se pretende mantener el acceso controlado a ubicaciones críticas en las instalaciones, mediante distintos sistemas, como una recepción o un sistema de identificación.

El aseguramiento de las instalaciones incluye establecer métodos de autenticación, según sea el nivel de restricción del área a la que se necesite ingresar; para ello existen muchos métodos y se clasifican, según lo que utilizan para verificar la identidad:

- Algo que el usuario sabe:
    - Contraseñas
    - Frases secretas o de acceso

- Algo que el usuario posee:

    - Tarjetas magnéticas o con chips inteligentes
    - Llaves

- Algo que el usuario es:

    - Huella digital
    - Reconocimiento de retina
    - Reconocimiento de voz

Pueden agregarse controles como señalización de sectores, notas, separación de áreas de procesamiento, carga y descarga, asegurar los accesos al edificio y similares.

4.2.1.2. Equipo

También se debe analizar la protección del equipo, en este aspecto se evalúa, entre otros, su distribución física, que involucra las funciones y equipamiento, asociadas a usuarios y que podrían comprometer la información.

Otra medida es mantener alejados suministros peligrosos, tales como combustibles o materiales inflamables.

Es fundamental tener un conocimiento completo de la red, e individualizar todos sus componentes con su respectiva dirección física y lógica. Para realizar dicha tarea, se presenta un mapa que registra la información y se denomina: mapa de elementos de red.

El control de cambios de equipo es un punto clave en el cual se debe de mantener el equipamiento de acuerdo con los intervalos de servicio y recomendaciones brindadas por el proveedor, el personal que brinda mantenimiento a los mismos debe ser el autorizado; se ha de llevar un control de las posibles fallas del sistema y la validación de que cada mantenimiento cumpla con los requisitos impuestos.

4.2.2. Protección lógica

Con la implementación de protección lógica se pretende establecer reglas, para proteger el robo, alteración y el deterioro de la confidencialidad de la información.

4.2.2.1. Información

Entre las amenazas que se deben evitar, se encuentran:

- Escucha no autorizada: se refiere a obtener información a partir de conversaciones o comunicaciones, involucra el aseguramiento a los accesos de red, ubicación de cables, entre otros.

- Ingeniería social: consiste en la manipulación de personas, para que de forma involuntaria, realicen cosas que normalmente no harían, como mostrar su contraseña o ceder un acceso a información restringida.

- Obtención de clave de acceso: es espiar a las víctimas para obtener claves de acceso, contraseñas y demás.

- Enmascaramiento: un intruso puede tomar la identidad de un usuario autorizado, con el simple hecho de tomar su usuario y contraseña. Con esto ya puede realizar las acciones según los permisos que hayan sido asignados al propietario.

Otro punto de gran importancia, es la eliminación segura de información, debido a los desperdicios que se dejan alrededor de un sistema, tales como:

- Documentación antigua
- Listados de empleados obsoletos
- Dispositivos de almacenamiento que ya no se usan

Pueden servir para obtener información sensible, si no son eliminados de manera segura.

Se debe prestar especial atención a la eliminación de:

- Documentos oficiales
- Grabaciones
- Papel copia
- Cintas magnéticas
- Discos removibles
- Datos de prueba
- Documentación del sistema

Según la clasificación de la información se debe dar controles con los que se validen las restricciones especiales, dependiendo de la información si es pública o privada, restringida o secreta.

4.2.2.2. Sistema operativo

El sistema operativo, es la base de la plataforma de aplicación, para mantenerlo seguro hay que establecer parámetros en ciertos aspectos que se listan a continuación:

- Actualización periódica: se refiere a mantener al día el software de las estaciones de trabajo y servidores, con el fin de eliminar vulnerabilidades y mantener la versión que se considere adecuada, de acuerdo con los requerimientos funcionales y las mejoras implementadas por el fabricante.

- Aplicación de parches que publican los proveedores en todos los equipos. Para esto se recomienda usar un software de distribución, según sea la cantidad de máquinas.

- Estandarización de servidores: deben seguir un estándar para su identificación y configuración. Es muy práctica la elaboración de *scripts* que establezcan los parámetros de configuración de manera automática, sin intervención del equipo.

- Control de acceso remoto: realizar controles adecuados para evitar el acceso no autorizado a los equipos. Se sugiere limitar el acceso a un grupo restringido de usuarios, utilizando medios seguros.

- Protección al inicio del sistema: establecer la configuración de arranque y restringir el inicio de los servidores desde otro medio, como discos, entre otros.

- Desconexión de las unidades de red no utilizadas: todas las conexiones que no se necesitan, deben ser removidas para evitar un intento de conexión por parte de usuarios no autorizados.

- Apagado seguro: para apagar el sistema se deben solicitar las credenciales adecuadas.

- Manejo de tipos de cuentas de usuario: se establecen permisos según el tipo de cuenta y los usuarios incluidos en dicho grupo.

4.2.2.3. Datos

Se debe controlar y administrar el acceso de los usuarios sobre los recursos lógicos como archivos, bases de datos, software, almacenes de datos y llevar un control de los accesos no autorizados, robos o descubrimiento de información.

Se restringe entre otros, el uso del espacio de almacenamiento, creando directorios dedicados o mediante el uso de políticas de usuario. Esto también ayuda a proteger la confidencialidad e integridad de los datos de los usuarios y ofrece una herramienta de trabajo para los grupos, al permitir compartir datos entre usuarios del mismo grupo y negar el acceso, al resto.

Con esto se pueden crear grupos, según sea la funcionalidad del sector y la tarea que realicen. Por otra parte se debe en conjunto, un control de cambios del software y del análisis de impacto sobre los mismos.

5. APORTE

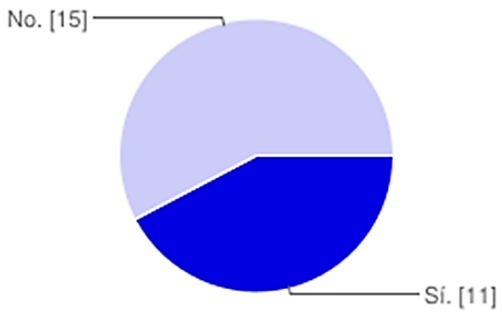
5.1. Contexto de la investigación

Para complemento de la teoría expuesta se presentan estadísticas con información obtenida a partir de la elaboración de una encuesta con preguntas afines al tema de seguridad industrial y el conocimiento que las personas poseen ante distintos aspectos de importancia, la cual fue resuelta por cincuenta estudiantes de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala. A continuación se detalla la información obtenida.

5.2. Evaluación realizada

- ¿Cambiar periódicamente la contraseña de su wifi evita completamente que cualquier intruso se conecte a su red?

Figura 8. **Resultados pregunta 1**

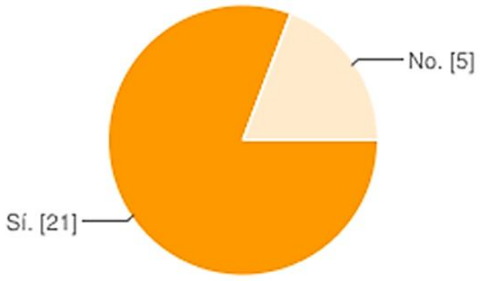


Fuente: elaboración propia.

Como se evidencia en los resultados de la figura 8, un elevado porcentaje de los encuestados afirma que cambiar la contraseña es un método efectivo, sin embargo, no es una acción que brinde seguridad, solamente complica el acceso pero no es infalible, pues si ya hubo una intrusión en la red es muy probable que vuelva a suceder. Lo recomendable en este caso es que se cambie la seguridad de la red en sí, para prevenir el acceso no autorizado, por esta vía.

- ¿El modo de navegación privada evita que se guarde información sobre las páginas web que se visitan, las búsquedas que se realizan o las contraseñas que se introducen?

Figura 9. **Resultados pregunta 2**

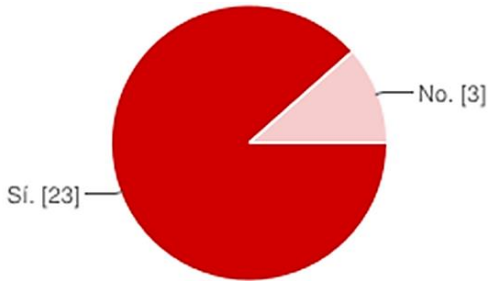


Fuente: elaboración propia.

El modo de navegación privada permite al usuario navegar por la web, sin almacenar información sobre las acciones que éste realiza, tal como se describe en la figura 9, donde un 81 % de los encuestados está en lo correcto.

- ¿Al conectarse a una red wifi pública se corre el riesgo de que roben sus datos almacenados en su dispositivo (portátil, teléfono inteligente, *tablet*, etc.)?

Figura 10. **Resultados pregunta 3**



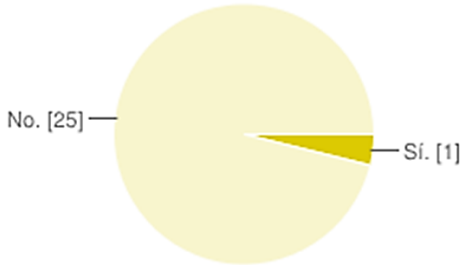
Fuente: elaboración propia.

A pesar de que el 88 % de las personas encuestadas opina que sí, el riesgo no se debe a que el acceso sea público, sino que se ve involucrada la seguridad del propio sistema, dado que esta es la última barrera que protege a la información.

- Cuantos más programas antivirus se tengan instalados en el ordenador, es mejor. Menos virus se colarán en él.

La cantidad no implica calidad, y según los resultados de la figura 11, se tiene una buena percepción de esto, dado que esto puede ser negativo para el desempeño del sistema operativo y no garantiza mejor seguridad.

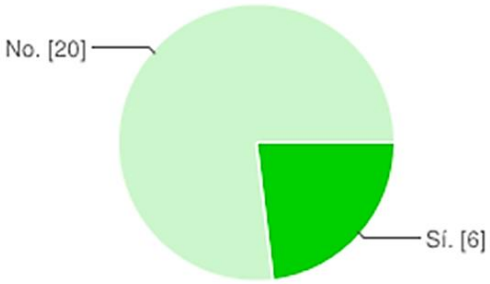
Figura 11. **Resultados pregunta 4**



Fuente: elaboración propia.

- ¿Es recomendable tener apuntadas las contraseñas en algún lugar, así si se olvidan por algún motivo, pueden ser consultadas rápidamente?

Figura 12. **Resultados pregunta 5**

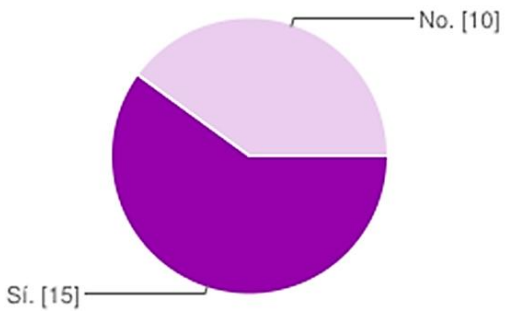


Fuente: elaboración propia.

Esto no es recomendable dado que el robo de las notas físicas, donde se encuentran las contraseñas, puede comprometer toda la seguridad del sistema. Pese a esto, un 23 % de los participantes prefieren esto, debido en muchos casos a la facilidad de esta práctica, pero puede que no tomen en cuenta los riesgos que involucra.

- ¿Cree que todas las claves de acceso a servicios de internet son de interés para los delincuentes?

Figura 13. **Resultados pregunta 6**



Fuente: elaboración propia.

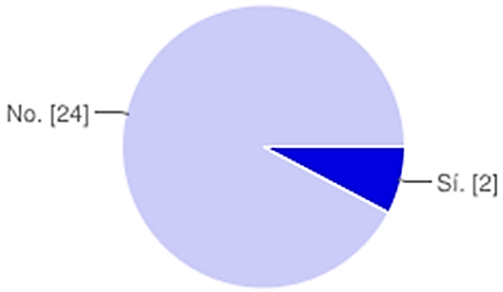
En la figura 13 se evidencia que un 38 % de la muestra, opina que no y están en lo correcto, debido a que según el concepto de información expuesto en capítulos anteriores, la información vale según el uso que se le dé.

- ¿Cree que las imágenes son de los pocos archivos que se pueden abrir con tranquilidad ya que no contienen virus?

Es falso, dado que todos los archivos corren este riesgo, por lo que se deben tomar las precauciones del caso, tal como tener un software antivirus, evitar abrir archivos, provenientes de personas desconocidas, entre otros.

Cerca del 8 % de personas entrevistadas, opina que abrir una imagen es seguro y según lo expuesto, están equivocadas.

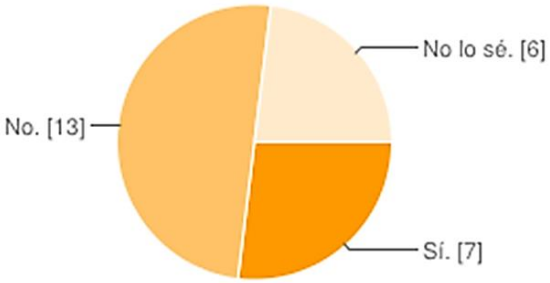
Figura 14. **Resultados pregunta 7**



Fuente: elaboración propia.

- ¿Ha sido víctima de algún ataque informático?

Figura 15. **Resultados pregunta 8**



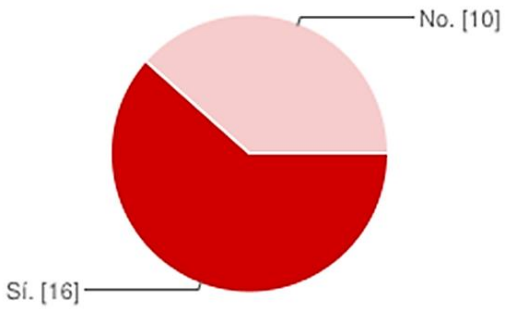
Fuente: elaboración propia.

Según la figura 15 el 27 % afirma que sí ha sido víctima de un ataque, el 50 % que no y el resto no sabe.

- ¿Cuenta con algún software antivirus, instalado en su computadora?

  El 62 % de los encuestados afirman tener un software antivirus instalado, contra un 38 % que no, como se muestra en la figura 16.

Figura 16. **Resultados pregunta 9**



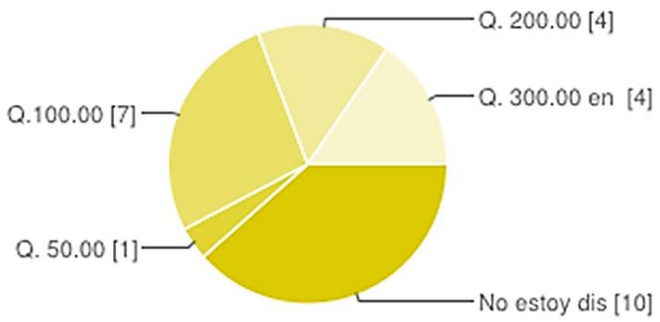
Fuente: elaboración propia.

- ¿Hasta cuánto está dispuesto a pagar por un antivirus (licencia personal de un año)?

  El software antivirus es una de las formas más comunes de proteger el sistema operativo, existe una gran variedad, desde el precio, hasta las herramientas que ofrecen.

  El 38 % de los encuestados no está dispuesto a pagar, pese a que según lo anterior, no concuerda con el porcentaje que afirma tener uno instalado.

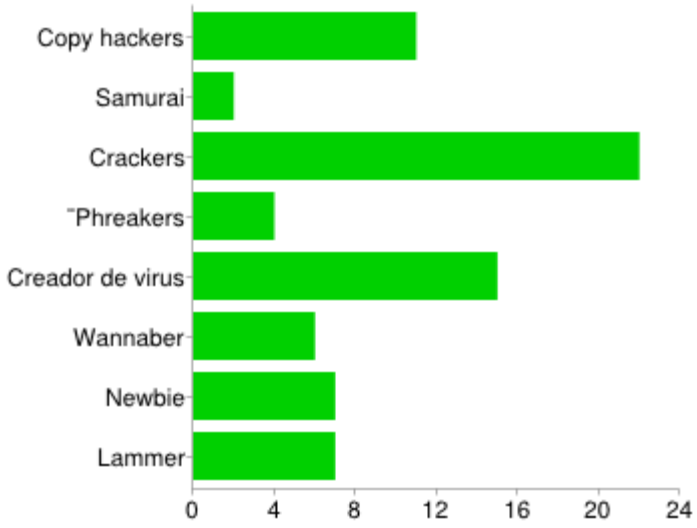
Figura 17. **Resultados pregunta 10**



Fuente: elaboración propia.

- De las siguientes amenazas informáticas humanas, ¿Cuáles conoce?

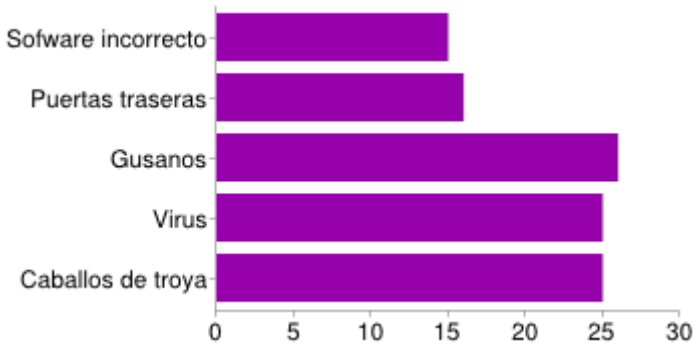
Figura 18. **Resultados pregunta 11**



Fuente: elaboración propia.

- De las siguientes amenazas lógicas ¿Cuáles conoce?

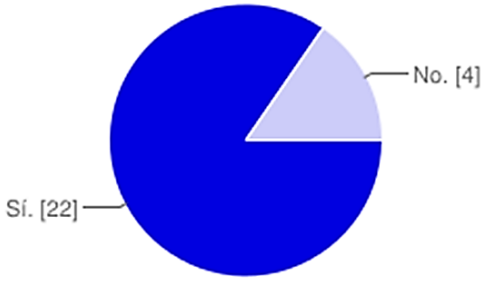
Figura 19. **Resultados pregunta 12**



Fuente: elaboración propia.

- ¿Cree que para mantener segura la información se debe tomar en cuenta la protección de las instalaciones y equipos?

Figura 20. **Resultados pregunta 13**



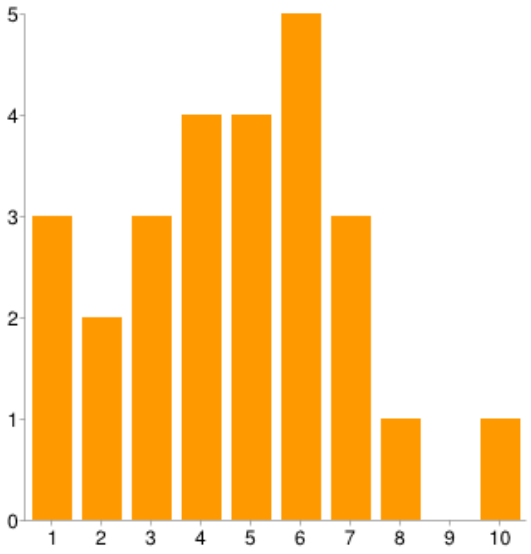
Fuente: elaboración propia.

Según la figura 20 el 85 % de los encuestados están en lo correcto, como se explica en el capítulo 2, las instalaciones y equipos se deben asegurar, para proteger el acceso a la información.

- En escala de 1 a 10 ¿Qué tan dispuesto está a sacrificar rendimiento de su computadora a cambio de seguridad?

El rendimiento es un factor que se suele ignorar cuando se involucra la seguridad. Para tener un sistema seguro, se debe tener un equilibrio entre ambos factores.

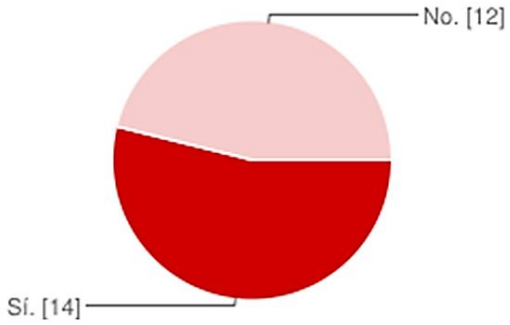
Figura 21. **Resultados pregunta 14**



Fuente: elaboración propia.

- ¿Usted mantiene su equipo al día con parches de seguridad?

Figura 22. **Resultados pregunta 15**



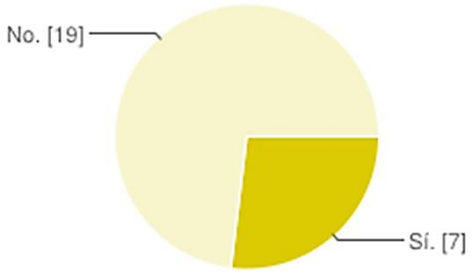
Fuente: elaboración propia.

En este aspecto, las respuestas están bastante equilibradas. Sin embargo, el 42 % de personas que no mantienen al día los parches de seguridad, podrían experimentar problemas en consecuencia.

- ¿Es más seguro navegar por internet en una computadora que hacerlo con teléfonos inteligentes y *tablets*?

Un 73 % opina que sí, según la encuesta, esto se ve reflejado en la figura 23, esto depende principalmente del software que use el dispositivo, más que este en sí, dado que el navegador web es la primera barrera de seguridad al navegar por la red.

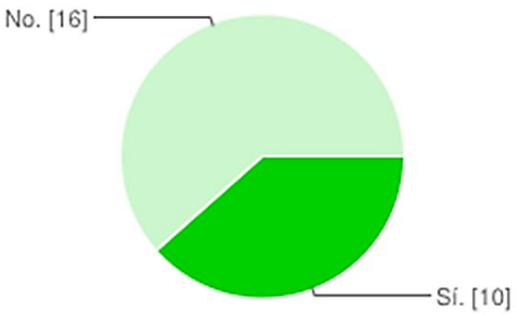
Figura 23. **Resultados pregunta 16**



Fuente: elaboración propia.

- ¿Usted toma en cuenta y planifica la seguridad para sus dispositivos?

Figura 24. **Resultados pregunta 17**

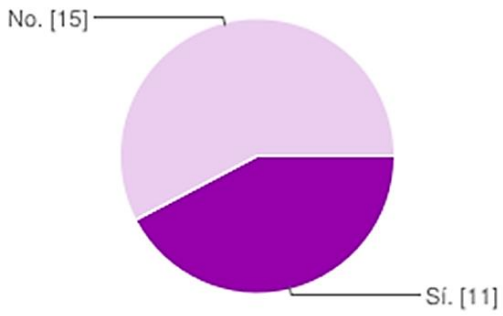


Fuente: elaboración propia.

Un 32 % afirma planificar la seguridad para sus dispositivos, tal como se explica en el capítulo 2, el plan de seguridad abarca desde lo físico, hasta lo lógico y todo entorno a la información.

- ¿Mantiene periódicas copias de seguridad de su información?

Figura 25. **Resultados pregunta 18**



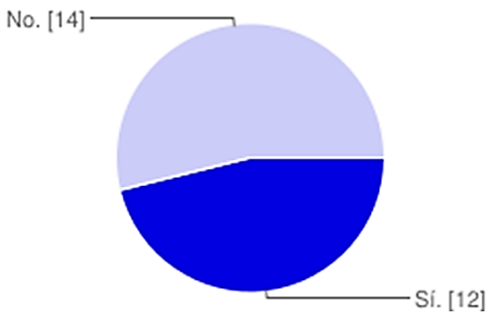
Fuente: elaboración propia.

Las copias de respaldo son de gran importancia, dado que sirven de contingencia ante una eventualidad. Tal como se explica en el capítulo 2, además de la clasificación de la información. En este caso, como se ve en la figura 25, un 78 % afirmó tener copias de seguridad de su información.

- ¿Ha usted tomado información ajena sin autorización (fotos, música, documentos, entre otros.)?

Un 54 % de los entrevistados afirmó haber tomado información sin permiso, esto es un delito informático.

Figura 26. **Resultados pregunta 19**



Fuente: elaboración propia.

5.3. Discusión de resultados

Con base en la investigación realizada y en las respuestas brindadas por los participantes, se puede concluir que un gran porcentaje de los estudiantes encuestados tiene las nociones básicas sobre seguridad y conoce sus conceptos.

Además de que hacen uso de diversas herramientas como el software antivirus, mantienen copia de respaldo de su información y conocen el uso de la navegación privada en los navegadores.

También se incluyó el tema de conexiones inalámbricas como el caso de wifi, el robo de información entre otros.

Para mitigar estos riesgos, se pueden utilizar las técnicas descritas en los capítulos anteriores, como por ejemplo, la creación de un plan de contingencia para las amenazas.

CONCLUSIONES

1. La importancia de la información se basa en quién la posee y el uso que le da.

2. Se estableció que los riesgos comunes, a los que se exponen los usuarios y según las encuestas realizadas, son el robo de identidad, malware y robo de información, entre otros.

3. Existe una serie de recomendaciones o pasos a seguir, necesarias para identificar las amenazas y vulnerabilidades de un sistema informático y de cómo, basándose en un análisis de riesgos, establecer las medidas a implementar, ante las amenazas que sufre un usuario.

4. La seguridad informática se originó desde la evolución de la tecnología y se implementó desde la etapa de diseño de un sistema. Es primordial para el resguardo de la información y confidencialidad de la misma, ya que esta es de gran valor para la organización.

5. Una vulnerabilidad es una debilidad que posee el sistema o alguno de los recursos que lo conforman; un riesgo es el desarrollo de una amenaza sobre un activo, aprovechando las vulnerabilidades del mismo. Mientras que una amenaza es algo repetitivo y que ya atacó o comprometió la seguridad del sistema.

6. Cualquier terminal puede ser blanco de un criminal, sin que necesariamente exista relación alguna con la organización o estar incluso

a grandes distancias; por dicha razón es importante que las organizaciones o incluso personas particulares implementen políticas de seguridad, tanto de seguridad física como seguridad lógica, protegiendo así todos los activos que posee la organización.

RECOMENDACIONES

1. La información es un activo de la organización y en ocasiones su valor radica en que esta se mantenga privada, por lo que es importante que se tengan establecidos los riesgos a los que se está expuesto y las medidas del caso, para su prevención.

2. La seguridad no es tema de departamentos o personal especializado, sino es cuestión de cultura, por lo que el usuario debe tomar las medidas pertinentes para el aseguramiento de la información y así salvaguardar su integridad.

3. El aseguramiento de la información no se refiere únicamente a crear barreras de software que protejan el acceso a los datos, sino que hay que tomarlo de forma, integrar e involucrar todos los factores que intervienen.

4. Toda terminal o dispositivo de acceso a un sistema puede ser un posible punto de ataque, por lo que se debe tener especial cuidado con el manejo de las credenciales y los dispositivos.

BIBLIOGRAFÍA

1. AGUILERA LÓPEZ, Purificación. *Seguridad informática*. Madrid, España: EDITEX, 2010. 240 p. ISBN 9788497717618.

2. BORGHELLO, Cristian. *Seguridad de la información.* [en línea]. <http://www.segu-info.com.ar/tesis/>. [Consulta: 17 de septiembre de 2009].

3. Cisco Systems, Inc. *Informe anual de seguridad de CISCO 2014.* [en línea]. <http://www.cisco.com/assets/global/ES/pdfs/executive_security/ sc-01casr2014_cte_lig_es_35330.pdf>. [Consulta: 12 de octubre de 2014].

4. Detica, Cabinet Office 2011. *The cost of cyber crime.* [en línea]. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf>. [Consulta: 18 de octubre de 2014].

5. FUENTES, Sacha. *Defiende tu PC. Guía de seguridad para ordenadores personales.* [en línea]. <http://www.defiendetupc.com/>. [Consulta: 5 de octubre de 2014].

6. PWC in association with infosecurity Europe. *2014 Information Security Breaches Survey* [en línea]. <https://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf>. [Consulta: 24 de octubre de 2014].

7. Software Technologies LTD. *Check point security report 2014.* [en línea]. <http://www.checkpoint.com/documents/ebooks/security-report-2014/files/assets/common/downloads/Check%20Point%20Security%20Report%202014.pdf>. [Consulta: 13 de octubre de 2014].

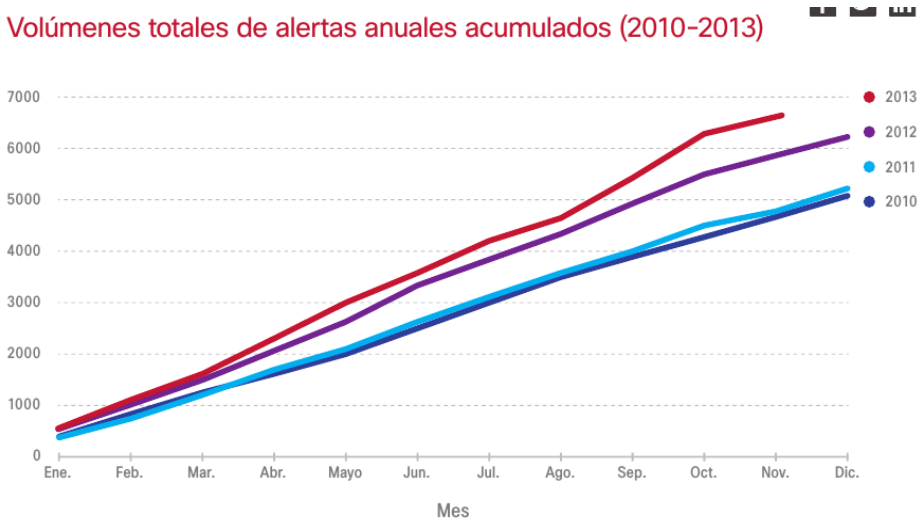
8. Symantec. *Internet security threat report 2014.* [en línea]. <http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf>. [Consulta: 22 de octubre de 2014].

9. _____. *Tendencias de seguridad cibernética en América Latina y el Caribe.* [en línea]. <https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf>. [Consulta: 9 de noviembre de 2014].

10. Trustwave, Smart security on demand. *2014 Trustwave global security report.* [en línea]. <http://www.slideshare.net/worldwidebranding/2014-trustwave-global-security-report>. [Consulta: 11 de noviembre de 2014].

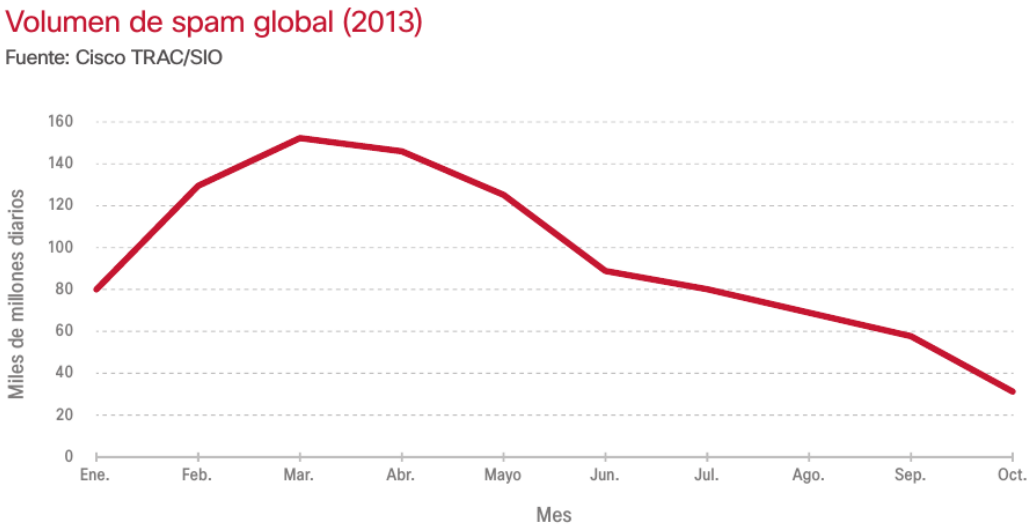
ANEXOS

Anexo 1. **Volúmenes de alertas acumuladas anuales**



Fuente: Cisco Systems, *Inc. Informe anual de seguridad Cisco*. http://www.cisco.com/assets/global/ES/pdfs/executive_security/sc-01casr2014_cte_lig_es_35330.pdf. Consulta 15 de octubre de 2014.

Anexo 2. **Volumen de spam global (2013)**



Fuente: Cisco Systems, Inc. Informe anual de seguridad Cisco (2014). http://www.cisco.com/assets/global/ES/pdfs/executive_security/sc-01casr2014_cte_lig_es_35330.pdf. Consulta 15 de octubre de 2014.