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

TÉCNICAS Y HERRAMIENTAS INADVERTIDAS DE LA INGENIERÍA SOCIAL UTILIZADAS PARA OBTENER INFORMACIÓN QUE COMPROMETA LA SEGURIDAD DE UN SISTEMA

Diana Patricia Mazariegos Sánchez

Asesorado por el Ing. Pedro Pablo Hernández Ramírez

Guatemala, noviembre de 2011

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

TÉCNICAS Y HERRAMIENTAS INADVERTIDAS DE LA INGENIERÍA SOCIAL UTILIZADAS PARA OBTENER INFORMACIÓN QUE COMPROMETA LA SEGURIDAD DE UN SISTEMA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

DIANA PATRICIA MAZARIEGOS SÁNCHEZ
ASESORADO POR EL ING. PEDRO PABLO HERNÁNDEZ RAMÍREZ

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, NOVIEMBRE DE 2011

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Ing. Alfredo Enrique Beber Aceituno
VOCAL II	Ing. Pedro Antonio Aguilar Polanco
VOCAL III	Ing. Miguel Ángel Dávila Calderón
VOCAL IV	Br. Juan Carlos Molina Jiménez
VOCAL V	Br. Mario Maldonado Muralles
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. César Augusto Fernández Cáceres
EXAMINADOR	Ing. Ludwing Federico Altán Sac
EXAMINADOR	Ing. Oscar Alejandro Paz Campos
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

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:

TÉCNICAS Y HERRAMIENTAS INADVERTIDAS DE LA INGENIERÍA SOCIAL UTILIZADAS PARA OBTENER INFORMACIÓN QUE COMPROMETA LA SEGURIDAD DE UN SISTEMA

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha enero de 2011.

Diana Patricia Mazariegos Sánchez

Universidad de San Carlos de Guatemala

Facultad de Ingeniería
Escuela de Ciencias y Sistemas

Guatemala, 26 de octubre de 2011

Ing. Carlos Azurdia
Coordinador de Tesis
Facultad de Ingeniería
Escuela de Ciencias y Sistemas

El motivo de la presente es para informarle que he asesorado el trabajo de graduación de la alumna **Diana Patricia Mazariegos Sánchez**, titulado **"Técnicas y herramientas inadvertidas de la Ingeniería Social utilizadas para obtener información que comprometa la seguridad de un sistema"**, a mi parecer cumple con los requisitos planteados como trabajo de tesis,

Atentamente,

Ing. Pedro Pablo Hernández Ramírez
Asesor de tesis
Colegiado: 7240

Pedro Pablo Hernández Ramírez
Ingeniero en Ciencias y Sistemas
Colegiado 7240

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

Guatemala, 27 de Octubre de 2011

Ingeniero
Marlon Antonio Pérez Turk
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 de la estudiante **DIANA PATRICIA MAZARIEGOS SÁNCHEZ** carné **2001-17556,** titulado: **"TÉCNICAS Y HERRAMIENTAS INADVERTIDAS DE LA INGENIERIA SOCIAL UTILIZADAS PARA OBTENER INFORMACIÓN QUE COMPROMETA LA SEGURIDAD DE UN SISTEMA",** 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

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

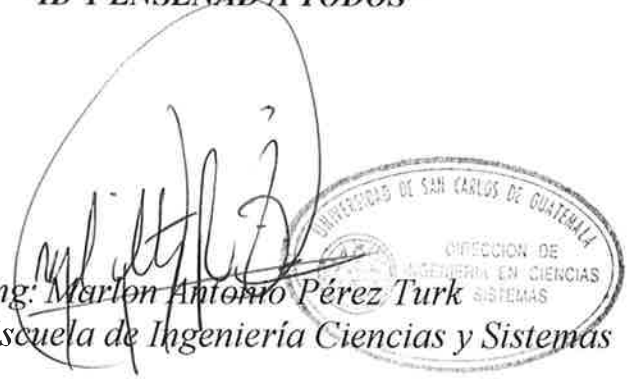
ESCUELA DE CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA
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, de trabajo de graduación titulado ***"TÉCNICAS Y HERRAMIENTAS INADVERTIDAS DE LA INGENIERÍA SOCIAL UTILIZADAS PARA OBTENER INFORMACIÓN QUE COMPROMETA LA SEGURIDAD DE UN SISTEMA",*** *presentado por la estudiante DIANA PATRICIA MAZARIEGOS SÁNCHEZ, aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"



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

Guatemala, 10 de noviembre 2011

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

Ref. DTG.480-2011

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: **TÉCNICAS Y HERRAMIENTAS INADVERTIDAS DE LA INGENIERÍA SOCIAL UTILIZADAS PARA OBTENER INFORMACIÓN QUE COMPROMETA LA SEGURIDAD DE UN SISTEMA,** presentado por la estudiante universitaria, **Diana Patricia Mazariegos Sánchez,** autoriza la impresión del mismo.

IMPRÍMASE.

Ing. Murphy Olympo Paiz Recinos
DECANO

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, noviembre de 2011

/cc
c.c. archivo.

ACTO QUE DEDICO A:

Dios	Porque lo reconozco como mi único proveedor, Él me ha dado todo lo que tengo.
Mis padres Marco Antonio Mazariegos y María Antonieta Sánchez	Por todo lo que sembraron en mí a lo largo de mi vida, representan el mejor regalo de Dios. Los amo.
Mis hermanas Adriana, Claudia y Lucrecia	Porque han sido siempre el apoyo que he necesitado. Las admiro mucho a cada una.
Mis sobrinas Jimena, Daniela, Diana y a mi sobrino Diego	Con todo mi amor.
Personal del Centro de Cálculo de la Facultad de Ingeniería	Por ser mi segunda familia, en especial a Susan Gudiel, Shirley Samayoa, Benjamín Cuc y Juan Fernando García.
Mis amigos Melissa García, Javier Solís y Ricardo Mazariegos	Porque no he encontrado en nadie más lo que he recibido de ustedes. Los respeto y admiro.

Las familias García Barneond, Cataví Jiménez y Mazariegos Castillo	Porque he sentido su apoyo de una u otra forma. Gracias porque en sus hogares he sentido encontrar el mío propio.
Marisol Lemus, Violetta Estrada, Lucrecia Yax, Helda Cataví, Rita Caballeros y Hugo Rosales	Porque forman parte importante en mi vida.

AGRADECIMIENTOS A:

Ingeniero Pedro Pablo Hernández Ramírez	Por el apoyo recibido en la realización de mi trabajo de graduación.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES I
GLOSARIO III
RESUMEN VII
OBJETIVOS IX
INTRODUCCIÓN XI

1. INGENIERÍA SOCIAL 1
   1.1. ¿Qué es la Ingeniería Social? 1
      1.1.1. Definición 1
      1.1.2. Objetivo 2
      1.1.3. Historia 2
      1.1.4. Seguridad Informática 4
         1.1.4.1. Sistemas de Información 4
         1.1.4.2. Definición de Seguridad Informática 6
         1.1.4.3. Tipos de Seguridad Informática 7
      1.1.5. Diferencia de la Ingeniería Social y los demás ataques a la Seguridad Informática 8
   1.2. Elementos de la Ingeniería Social 9
      1.2.1. El comportamiento humano 9
      1.2.2. La persuasión 10
      1.2.3. Medios de comunicación 11
      1.2.4. El entorno social 12

2. EL ATAQUE INFORMÁTICO 13
   2.1. Tipos de ataque 13

2.1.1. En función del impacto 13
2.1.1.1. Activos 13
2.1.1.2. Pasivos 15
2.1.2. En función de la forma 16
2.1.2.1. Directos 16
2.1.2.2. Indirectos 16
2.1.3. En función de sus herramientas 17
2.1.3.1. Engaño tecnológico 17
2.1.3.2. Engaño a la persona 17
2.1.3.3. Engaño sofisticado 17
2.2. Tipos de atacante 18
2.2.1. En función de su ubicación 18
2.2.1.1. Atacante externo 18
2.2.1.2. Atacante interno 18
2.2.2. En función de su objetivo 19
2.2.2.1. *Hacker* 19
2.2.2.2. *Cracker* 19
2.2.2.3. *Phreaker* 20
2.2.2.4. *Lamer* 20
2.2.2.5. *NewBie* 20
2.3. Perfil del atacante 20
2.3.1. Perfil psicológico 21
2.3.2. Perfil académico/laboral 21

3. EL ATAQUE MÁS EXITOSO: EL INADVERTIDO 23
3.1. Herramientas 24
3.1.1. *Spyware* 24
3.1.2. *Phishing* o Suplantación de Identidad 25
3.1.3. *Vishing* (*Voice phISHING*) 26

3.1.4. *Smishing* (*SMs phISHING*) 26
3.1.5. *Spam* 27
3.1.6. *Scareware* o *Rogueware* 28
3.2. Técnicas 29
3.2.1. La reciprocidad 30
3.2.2. El compromiso y la consistencia 30
3.2.3. La validación social 31
3.2.4. La autoridad 31
3.2.5. El gusto 32
3.2.6. La escasez 33

4. ÁMBITO LEGAL 35
4.1. Legislación 35
4.2. Importancia de la legislación para los delitos informáticos 35
4.3. Ley de Delitos Informáticos 37
4.3.1. Comité regulador 38
4.3.1.1. Funciones 38
4.3.1.2. Organización 39
4.3.2. Sanción penal 40
4.3.3. Situación actual de la iniciativa 47
4.4. Ley de Acceso a Información Pública 49
4.4.1. Ámbito de aplicación (Artículo 4) 50
4.4.2. Sujetos obligados (Artículo 6) 50
4.4.3. Definiciones (Artículo 9) 51
4.4.3.1. Información pública 51
4.4.3.2. Información confidencial 51
4.4.3.3. Información reservada 51
4.4.3.4. Datos personales 52

4.4.3.5. Datos sensibles o datos personales sensibles....52
4.4.4. Procedimiento de acceso a la información pública....52
4.4.5. Sanción penal....53

5. BUENAS PRÁCTICAS PARA RESGUARDAR LA SEGURIDAD DE UN SISTEMA....55
5.1. Empresas....55
5.1.1. A nivel técnico....55
5.1.2. Educación de directivos....56
5.1.3. Educación de empleados....57
5.1.4. Definición de roles....57
5.2. Usuarios....58
5.2.1. A nivel técnico....58
5.2.2. Aspectos de la conducta humana como principales obstáculos de la persuasión....58

CONCLUSIONES....61
RECOMENDACIONES....63
BIBLIOGRAFÍA....65
ANEXO....69

ÍNDICE DE ILUSTRACIONES

FIGURAS

1. Elementos de un Sistema de Información……5
2. Crecimiento de la telefonía móvil en Guatemala de 2004 al primer semestre 2010..... 28

TABLAS

I. Estadísticas del uso de la *Internet* en la Región Centroamericana…….36
II. Sanciones penales asociadas a los delitos informáticos……..41
III. Sanciones penales asociadas a Ley de Acceso a la Información Pública……...53
IV. Proceso Legislativo para la aprobación de una ley o de reforma de leyes…….69

GLOSARIO

Amenaza Presencia de uno o más factores de diversa índole, que de tener la oportunidad, atacaría al sistema produciendo daños, aprovechando el nivel de vulnerabilidad del mismo.

Ataque Amenaza materializada.

Certificado digital Es un conjunto de datos que permiten la identificación del titular del Certificado, intercambiar información con otras personas y entidades de manera segura y firmar electrónicamente los datos que se envían de tal forma que se pueda comprobar su integridad y procedencia.

Comercio electrónico Conocido en inglés como *e-Commerce*, consiste en la compra y venta de productos/servicios a través de medios electrónicos, principalmente en la *Internet*. Se utiliza las tarjetas de crédito como forma de pago.

Dirección IP	Etiqueta numérica que identifica de manera lógica y jerárquica a un elemento de comunicación (interfaz) de un dispositivo que está conectado a una red utilizando el protocolo de *Internet* (*Internet Protocol*).
Dominio/Nombre de Dominio	Nombre único que identifica a un sitio *Web* en la *Internet*.
Firma digital	Esquema matemático que sirve para demostrar la autenticidad de un mensaje digital o de un documento electrónico. Brinda al destinatario la seguridad que el mensaje fue creado por el remitente y no fue alterado durante la transmisión. Se utilizan para la distribución de *software*, transacciones financieras y en otras áreas donde es importante detectar la falsificación y la manipulación.
Firma electrónica	Cualquier medio electrónico que es utilizado para identificar a una persona o entidad. Una firma electrónica reconocida tiene el mismo valor legal que la firma manuscrita. Su principal característica es su cualidad de ser inmodificable.

Freeware	Define un tipo de *software* no libre, que se distribuye sin costo. El *software Freeware* está disponible para su uso, por tiempo ilimitado e incluye una licencia de uso que permite su redistribución pero con algunas restricciones, dependiendo de lo que indique la licencia que incluye.
Impacto	Es la consecuencia de la materialización de una o más amenazas sobre el elemento objetivo. El daño causado.
P2P	*Peer to Peer*. Red de pares o red entre iguales o red entre pares o red punto a punto, es una red de computadoras que se comportan como iguales entre sí, es decir, actúan como clientes y servidores respecto a los demás nodos de la red y permiten el intercambio directo de información en cualquier formato, entre las computadoras interconectadas.
Perfil de usuario	Datos de configuración de un usuario.
Pop-Ups	Son ventanas *Web* emergentes, que aparecen de repente en la pantalla del navegador de *Internet* frente a cualquiera otra que esté abierta. Emergen de alguna página *Web* o programa.

Riesgo	Posibilidad que se materialice una amenaza, aprovechando vulnerabilidades.
Shareware	Define un tipo de *software* en el que el usuario puede evaluar de forma gratuita el producto, pero con limitaciones en el tiempo de uso o en algunas de las formas de uso o con restricciones en las capacidades finales. El objetivo es que el usuario pague al finalizar el tiempo limitado (trial) y con la finalidad de habilitar toda su funcionalidad.
VoIP	Voz sobre Protocolo de *Internet* es un grupo de recursos que hace posible que la señal de voz viaje a través de una red, empleando el Protocolo de *Internet*, es decir, la señal de voz no viaja en forma analógica como en el teléfono, sino en forma digital, a través de paquetes en la red.
Vulnerabilidad	Probabilidad que existe que una amenaza se materialice contra un elemento objetivo

RESUMEN

La presente investigación pretende brindar un aporte concreto y significativo al extenso banco de información existente en la *Internet*, sobre la Ingeniería Social. Se identifican y analizan las técnicas y las herramientas inadvertidas para el usuario, basadas en la filosofía de la Ingeniería Social y que han sido las más comunes para alcanzar el éxito en la intrusión a un sistema, y así poner en riesgo la seguridad del mismo.

Debido a que el concepto más general que se le puede dar a la Ingeniería Social, indica que es el arte de persuasión, muchos escritores e informáticos coinciden que es una práctica propia de la humanidad y se remonta a los inicios de la misma.

Muchos han sido los que han escrito acerca de la Ingeniería Social. Desde aficionados a la tecnología, expertos en informática, escritores como Carlos Martín Pérez y sus obras El Gran Juego y Estrategia y Mente, reconocidos sociólogos como Manuel Castells y su obra La Era de la Información y los mismos Ingenieros Sociales que han sido reconocidos a nivel mundial por sus prácticas en el rama, menciono al reconocido Kevin Mitnick y su libro El Arte de la Intrusión.

La nota diferencial de la era de la información con respecto a las anteriores épocas históricas, es el gran protagonismo de los ciudadanos, para este contexto, entiéndase los usuarios de la informática.

Debido a que la información es uno de los activos más importantes de las empresas, también se ha hecho necesario manejar conceptos sobre la seguridad informática, que se define como la disciplina que se encarga de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

Dentro de los factores de análisis de la Seguridad Informática, se encuentran los datos e información, la infraestructura y el personal, para efectos de la presente investigación, se analiza a las personas en su rol de usuarios de los sistemas, ya que estudios indican que se producen más fallos de seguridad por intervención del factor humano que por fallos en la tecnología.

Tanto la Ingeniería Social como la Seguridad Informática, hacen uso de técnicas, que son procedimientos o conjuntos de reglas, normas o protocolos que se utiliza como medio para llegar a un cierto fin. La técnica supone que, en situaciones similares, una misma conducta o un mismo procedimiento producirán el mismo efecto.

La Ingeniería Social utiliza las técnicas que surgen de la necesidad de modificar el medio para adaptarlo a sus necesidades. Supone el razonamiento inductivo y analógico de la conducta humana, que en situaciones similares un mismo procedimiento genera el mismo efecto.

OBJETIVOS

General

Identificar las herramientas y las técnicas inadvertidas que utiliza una persona por medio de la Ingeniería Social para comprometer la seguridad de un sistema.

Específicos

1. Determinar las causas más comunes que comprometen la seguridad de un sistema, a través de sus usuarios finales.

2. Determinar y analizar buenas prácticas a nivel de usuarios finales, que nos ayuden a resguardar la seguridad de un sistema.

3. Contrastar en la investigación, la filosofía que sustenta la Ingeniería Social y su contraparte respectiva dentro del marco legal y social.

INTRODUCCIÓN

La presente investigación aborda como tema central, las técnicas y herramientas inadvertidas que un usuario malicioso utiliza por medio de la Ingeniería Social para obtener información que ponga en riesgo la seguridad de un sistema.

En el ámbito computacional, la Ingeniería Social puede definirse como las técnicas de intrusión que basan su éxito en las debilidades de las personas, más que en las debilidades del *software*. Es por ello que el principio que sustenta la Ingeniería Social, es que en cualquier sistema; los usuarios son el eslabón más débil.

Dentro del concepto de la Ingeniería Social, se definen y clasifican una serie de tretas, artimañas y engaños que se elaboran para confundir al usuario aprovechando sus intereses políticos, económicos, sentimentales, religiosos o de otra índole, así como cualquier otra conducta humana que logre una acción por parte del mismo. Es por ello que el primer capítulo de la presente investigación, menciona las definiciones básicas y necesarias para comprender el contexto en el que dichas técnicas y herramientas logran exitosamente poner en tela de juicio la seguridad del sistema objetivo del ataque.

Posterior a facilitar la información básica al lector, es imperante mencionar las causas más comunes por las que los usuarios de los sistemas se convierten en los eslabones más débiles de la cadena de seguridad, y para ello, se enfoca las bases y fundamentos de la Ingeniería Social.

La investigación de este tema se realizó por el interés de conocer dentro de todas las amenazas existentes en contra de la seguridad de un sistema, las más peligrosas, es decir; las ocultas o inadvertidas. Para analizar esto, es necesario mencionar como logran el éxito los ataques ocultos al pasar inadvertidos ante los usuarios.

En el ámbito profesional de la informática y ante la era tecnológica que actualmente se vive, no es un problema tener acceso a la información, el problema radica en la escasa o nula educación de los usuarios de los sistemas ante las reacciones necesarias para evitar un ataque inadvertido; cabe mencionar que la mayoría de dichos usuarios no son conocedores del área de la informática. Es por eso que el aprendizaje se vuelve indispensable para romper los efectos de la Ingeniería Social, y el enfoque legal y social brinda las bases para la mencionada y tan necesaria educación, ya que como parte de un sistema, si se vulnera una parte del mismo, se vulnera el sistema completo.

Para el desarrollo de la presente investigación, se tomaron las bases de la Teoría del Aprendizaje Social, el cual, su tema central es el pensamiento humano y los factores que determinan su comportamiento. Esta teoría, se basa en la creencia de que la conducta humana está determinada por una relación tripartita entre factores cognitivos, las influencias del medio ambiente y el comportamiento.

1. INGENIERÍA SOCIAL

1.1. ¿Qué es la Ingeniería Social?

1.1.1. Definición

Según el diccionario de la Real Academia de la Lengua Española, la Ingeniería es el estudio y aplicación, por especialistas, de las diversas ramas de la tecnología. Son actividades realizadas por expertos, por conocedores de una rama específica.

En el ámbito computacional, la Ingeniería Social puede definirse como las técnicas de intrusión, que basan su éxito en las debilidades de las personas, más que en las debilidades del *software*. Es por ello que el principio que sustenta la Ingeniería Social, es que en cualquier sistema los usuarios son el eslabón más débil.

Dentro del concepto de la Ingeniería Social, se aborda una serie de tretas, artimañas y engaños que se elaboran para confundir al usuario, aprovechando sus intereses políticos, económicos, sentimentales, religiosos o de otra índole, así como cualquier otra conducta humana que logre una acción por parte del mismo. Dichas acciones, pueden poner en tela de juicio la seguridad del sistema objetivo del ataque.

1.1.2. Objetivo

El objetivo específico de la Ingeniería Social es obtener acceso a los sistemas para cometer acciones ilegales en contra de la información del sistema objetivo, tales como:

- El espionaje industrial
- Robo de identidad
- Fraudes
- Intrusión en las redes.

1.1.3. Historia

Actualmente se maneja mucho el concepto de la Era de la Información, con el que se refiere al período que está fuertemente ligado a las tecnologías de la información y la comunicación, en donde la información se mueve más rápido que en un movimiento físico.

El crecimiento exponencial del acceso a la *Internet*, la digitalización de procesos y el uso de las telecomunicaciones, se pueden mencionar como características de la Era de la Información, conocida por algunos autores como la Sociedad de la Información. Está ligada completamente con el avance tecnológico que el mundo ha vivido, el cual tuvo como punto de partida con la primera computadora ENIAC, que fue utilizada con propósitos de investigación por parte del ejército de los Estados Unidos alrededor de 1943.

El surgimiento de esta nueva sociedad, dio como resultado el nacimiento de un nuevo paradigma social, el paradigma tecnológico, el cual formula nuevas reglas o principios que se toman como base para la toma de decisiones a nivel

social, tanto en el campo económico, como en la estructura organizacional de las empresas, ya que este paradigma considera como elemento fundamental, el uso de la tecnología y los sistemas de información para dar eficiencia a los procesos en función de las necesidades de los clientes. Ante tal cambio que se fue expandiendo, todas las áreas de la sociedad fueron afectadas por nuevos términos y orilladas a la búsqueda del ingreso al nuevo paradigma.

Consultando el artículo La Edad de la Informática, la Cibersociedad, se coincide que la nota diferencial de la era de la información con respecto a las anteriores épocas históricas, es el gran protagonismo de los ciudadanos, para este contexto, entiéndase los usuarios de la informática.

Una de las formas más genéricas de comprender la Ingeniería Social, es definirla como el arte de la persuasión. Por lo tanto, se puede decir que la Ingeniería Social es tan antigua como los métodos de persuasión utilizados por la humanidad para lograr un efecto en la actitud de otra persona, es decir, para modificarla, generar una reacción en específico o eliminarla. Es decir, el origen de la Ingeniería Social se remonta a los inicios de las primeras sociedades.

El hombre empezó a utilizar la persuasión como un método de influencia social para aplicarlo en aspectos de publicidad y mercadeo, sin embargo, estos métodos han ido cambiando de fines, conforme la era de la información va transcurriendo. Aspectos como el escaso conocimiento de informática, legislación menos rigurosa en cuanto a la propiedad de la información, la inocencia o ingenuidad de las personas ante ataques a los sistemas y la vulnerabilidad de los mismos, fueron los detonantes críticos para el éxito de la Ingeniería Social.

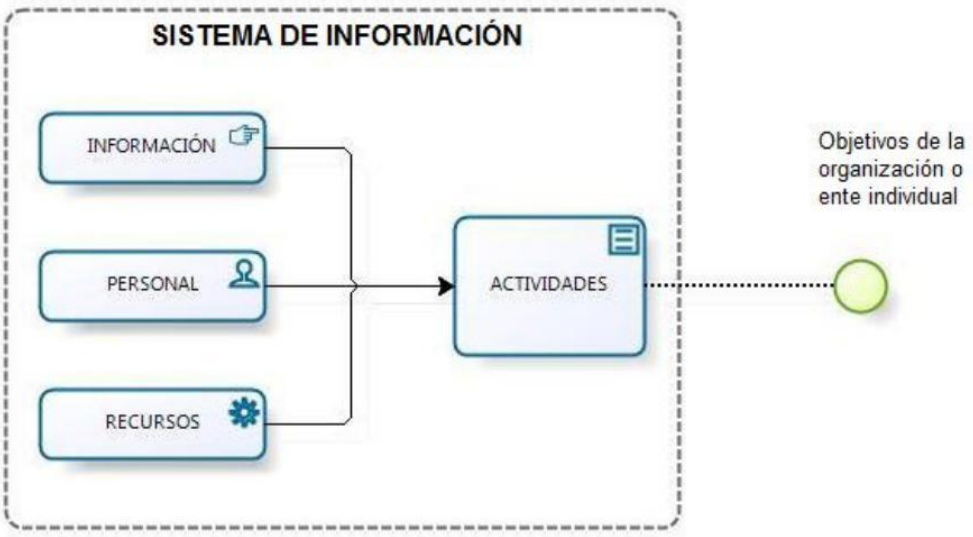
El término se utiliza traducido literalmente de su uso en el idioma inglés *Social Engineering* y tiende a ser comprendido de una manera diferente a lo que realmente significa. Por la presencia de la palabra Social y la palabra Ingeniería, no se asocia con actos delictivos y de manipulación. Sin embargo, según la Real Academia de la Lengua Española se entiende por Ingeniero a una persona que realiza con ingenio las trazas y modos de conseguir o ejecutar algo. Y el ingenio se define como la industria, maña y artificio para conseguir lo que se desea. Por lo tanto, el término de Ingeniero Social se le aplica las personas que utilizan el ingenio para lograr su objetivo, en este caso, obtener información importante y no pública de una organización o ente individual.

1.1.4. Seguridad Informática

1.1.4.1. Sistemas de Información

Los sistemas de información son conjuntos de elementos interrelacionados entre sí, para lograr un objetivo en común, para este tema de estudio, el objetivo en común es lograr la eficiencia en el funcionamiento de una organización o ente individual. Algunos de los elementos más importantes que se pueden mencionar en un sistema de información, se detallan en la figura 1.

Figura 1. **Elementos de un Sistema de Información**



Fuente: AGUILERA LÓPEZ, Purificación. Seguridad Informática. Madrid: EDITEX, S.A. (2010) p. 8.

- Recursos

Pueden ser físicos, recursos no informáticos y lógicos, dentro del contexto del sistema de información, por ejemplo; las aplicaciones informáticas y los sistemas operativos.

- Personal

Personas que trabajan en la organización. El elemento personal puede actuar sobre todos los elementos del sistema, dependiendo del rol que desempeñe en el mismo.

- Información

Conjunto de datos organizados que tienen un significado. Constituye uno de los activos más importantes de la empresa, tiene un canal directo e indirecto con los usuarios asociados al sistema.

- Actividades

Son las tareas que se realizan en la organización utilizando los anteriores elementos, y que a través de ellas se busca alcanzar los objetivos de la organización o ente individual.

1.1.4.2. Definición de Seguridad Informática

Debido a la gran importancia que conforme el paso del tiempo han adquirido y siguen adquiriendo los sistemas de información a nivel empresarial, se ha vuelto necesario e indispensable manejar el concepto de Seguridad Informática, que se define como la disciplina que se encarga de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un Sistema de Información seguro y confiable.

Dentro de los factores de análisis de la Seguridad Informática, se encuentran los datos e información, la infraestructura y el personal, para efectos de la presente investigación, se analiza a las personas en su rol de usuarios de los sistemas, elemento que también es protagónico de la Ingeniería Social.

Son cantidades económicas significativas, las que las empresas invierten en Seguridad Informática para proteger la información en contra de amenazas o peligros, obviando la educación en los usuarios de los sistemas como arma principal contra los ataques a su información.

El personal como elemento del sistema de información, utiliza los recursos y la información en sus actividades, ya sean administradores, programadores, usuarios internos, usuarios externos y el resto del personal de la organización; es por ello que en el ámbito de la Seguridad Informática, los usuarios juegan un papel muy importante en su aplicación.

Sin embargo, a diferencia del resto de los elementos de los Sistemas de Información, que pueden ser personalizados en su configuración y se esperan comportamientos específicos, el factor humano puede llegar a ser muy manipulable en su comportamiento, circunstancia que es aprovechada por los practicantes de la Ingeniería Social, para lograr su objetivo, utilizando el comportamiento humano como su mejor elemento para persuadir.

Por las características del comportamiento humano y los factores que le rodean, los usuarios son el eslabón más débil de la cadena de seguridad.

1.1.4.3. Tipos de Seguridad Informática

- Activa

Este tipo de seguridad, abarca los métodos y técnicas de defensa para reducir, o en el mejor de los casos, evitar los riesgos que amenazan al Sistema de Información.

- Pasiva

Este tipo de seguridad, contempla los métodos y técnicas a implementar una vez producido el ataque a la seguridad, para facilitar la recuperación y agilizarla.

1.1.5. Diferencia de la Ingeniería Social y los demás ataques a la Seguridad Informática

Los ataques a la Seguridad Informática (véase capítulo 2: el Ataque Informático), dependiendo del elemento del sistema a atacar, utilizan las vulnerabilidades existentes en los componentes físicos y lógicos, es decir, en la infraestructura o aplicaciones de *software*, para lograr su objetivo. Por lo tanto, se puede decir que los atacantes aprovechan la vulnerabilidad de los recursos físicos y lógicos.

La Ingeniería Social no hace uso de ninguna vulnerabilidad del sistema, si en caso las tuviera. Este es completamente irrelevante para el Ingeniero Social, ya que su herramienta principal es el ingenio y las técnicas utilizadas se basan en la persuasión, por lo tanto, no necesita tener conocimiento de informática, de redes o manejo de sistemas plataforma para servidores, ya que el aspecto que aprovecha es lo manipulable de la conducta humana. La vulnerabilidad que aprovecha la Ingeniería Social es la de los usuarios.

1.2. Elementos de la Ingeniería Social

1.2.1. El comportamiento humano

El comportamiento humano ha sido objeto de estudio desde muchas perspectivas, entre ellas; la psicológica y la social. Tiene como elementos situacionales los contextos social y cultural, las circunstancias políticas, las condiciones ambientales y cualquier otra situación en la cual se lleve a cabo el comportamiento humano, éste es manifestado con pensamientos, sentimientos, expectativas, etc.

El mismo autor, Arturo Silva detalla en su obra Criminología y Conducta Antisocial, tres modalidades del comportamiento humano que han sido aceptadas en el ámbito científico, siendo éstas:

- Modalidad motora del comportamiento humano
- Modalidad fisiológica del comportamiento humano
- Modalidad cognoscitiva del comportamiento humano.

La Ingeniería Social, se centra dentro del contexto de la modalidad cognoscitiva, que está basada en estructuras, procesos, estrategias, funciones y contenidos que por definición ejercen un efecto en el individuo o la persona.

Dentro de los factores que afectan el comportamiento humano, es la genética, la actitud y las normas sociales, éste último puede provocar presión sobre el individuo para realizar o no ciertos comportamientos.

1.2.2. La persuasión

Persuadir consiste en inducir, mover u obligar a alguien para que reaccione de cierta forma, es decir; la persuasión busca que el sujeto crea, piense o haga algo, aunque tal vez no quiera, pero no se da cuenta que lo hace.

Las actitudes abordadas por las personas, determinan su comportamiento, es por ello que la persuasión pretende manipular el comportamiento humano para lograr un objetivo.

Los métodos o estrategias de persuasión se definen como sigue:

- La reciprocidad

En el comportamiento humano, es normal tender a pagar un favor con otro.

- El compromiso y la consistencia

Cuando la persona incurre en un compromiso, ya sea de forma verbal o escrita, utiliza todos los medios posibles para llevar a la realidad dicho compromiso, incluso si las razones por las que lo adquirió, se han modificado o eliminado antes de llevarlo a cabo.

- La validación social

Las personas hacen lo que ven que otras personas hacen.

- La autoridad

Existe la tendencia en la humanidad de obedecer a personas que ejercen cierta autoridad sobre ellos, aunque no estén de acuerdo de realizar dichos actos.

- El gusto

Una primera persona se siente a gusto con, o le simpatiza una segunda, la primera será convencida fácilmente por la segunda para realizar cierto acto. También es una tendencia.

- La escasez

Cuando hay escasez, hay demanda; es decir, la necesidad de obtener algo, crea la tendencia de reaccionar en la búsqueda de lo que se necesita.

1.2.3. Medios de comunicación

Los medios de comunicación no sólo son utilizados con fines publicitarios; informativos y educativos, sino también son utilizados como medios de persuasión muy efectivos. Los mensajes en todo medio posible, ya sea directa o indirectamente, son utilizados por la Ingeniería Social para influir en la opinión, creencia o comportamiento de una persona. No sólo utiliza el medio de comunicación como tal, sino que incluye una idea específica en el mismo para obtener un resultado específico. Puede ser que el medio de comunicación sea utilizado para exponer una verdad, sin embargo, la Ingeniería Social utiliza formas para exponerla de manera que genere en la persona una reacción más emocional que racional.

1.2.4. El entorno social

El entorno de los usuarios de los sistemas, conforma una variable crítica para la Ingeniería Social. El ámbito personal, empresarial y social genera características en los usuarios que son explotadas por la Ingeniería Social para lograr sus fines. El entorno social está sujeto a las condiciones de vida y de trabajo, el nivel académico, su nivel de ingresos y la comunidad a la que pertenece. Todas estas variables definen las tendencias de cada persona, sus intereses, sus reacciones, sus pensamientos, sus necesidades, y por lo tanto, sus decisiones.

2. EL ATAQUE INFORMÁTICO

Se le llama ataque informático a las acciones que realiza una o varias personas con el objetivo de hacer daño a un sistema informático, el cual es un sistema de información que utiliza la tecnología para agilizar sus procesos.

2.1. Tipos de ataque

Un ataque se hace presente, cuando una amenaza en contra del sistema, se materializa.

2.1.1. En función del impacto

Por el impacto provocado en el elemento objetivo, los ataques pueden clasificarse en activos y pasivos.

2.1.1.1. Activos

Se le llama Ataque Activo, cuando alteran la información, entiéndase modificar, agregar, eliminar o dañar información. También incluye el bloqueo o la saturación de los canales de comunicación. A continuación se mencionan algunos ejemplos:

- DoS/DDoS (*Denial of Service/Distributed Denial of Service*)

Estos ataques van dirigidos a la red, su objetivo es perder servicios en ejecución, generalmente, la pérdida de la conectividad, tal como su nombre lo indica: denegación del servicio. DDos es una ampliación de DoS.

- *Buffer Overflow*

Es un estado de la memoria, que el sistema operativo detecta como error, y consiste en copiar una gran cantidad de datos sobre un área de memoria que no es suficiente para la demanda.

- *Exploits*

Consisten en fragmento de datos o piezas de *software* que utiliza un error o vulnerabilidad del sistema, para generar una interrupción o comportamiento no deseado a nivel *hardware* o *software*. Pueden ser locales o remotos.

- *Rootkits*

Son componentes que tienen la finalidad de auto ocultarse y ocultar otros procesos o elementos del sistema. Dichos elementos pueden ser utilizados por el atacante para implementar puertas de acceso al sistema.

- *Cross Site Scripting*

Es un ataque basado en la validación de datos en HTML incrustado. Permite la inyección de código malicioso dentro de las aplicaciones *Web*. Está diseñado para ejecutar código de *scripting*.

- *SQL Injection*

Es una vulnerabilidad en la validación de las entradas a la base de datos del sistema, debido al filtrado incorrecto de las variables utilizadas por el programador. Implica inyectar código *sql*, en donde se requiera para alterar las operaciones a la base de datos desde un cliente. Este tipo de ataque requiere conocimiento avanzado por parte del atacante.

2.1.1.2. Pasivos

Se le llama Ataque Pasivo, cuando se realiza un acceso a la información del sistema sin una autorización correspondiente a la tarea. Consiste sólo en el acceso, no en la alteración. A continuación se mencionan algunos ejemplos:

- *Footprinting*

También reconocida como Recolección de Datos. Técnica mediante la cual el atacante obtiene información sobre su víctima.

- Enumeración

Se utiliza para hacer un inventario de los recursos que posee un sistema.

- *Scanning*

Consiste en envío de paquetes a través de la red para descubrir puertos que están escuchando, e identificar los servicios que la víctima está ejecutando.

- *Sniffers*

Aplicaciones que capturan el tráfico de la red.

- *KeyLoggers*

Es un proceso en *background* que registra las pulsaciones del teclado para registrarlas en un archivo y enviarlas por la *Internet*. Este proceso recopila información importante.

2.1.2. En función de la forma

Por la forma en que el atacante dirige su ataque al elemento objetivo, los ataques pueden clasificarse en directos e indirectos.

2.1.2.1. Directos

Se le llama Ataque Directo, al ataque que no utiliza intermediarios para alcanzar su elemento objetivo.

2.1.2.2. Indirectos

Se le llama Ataque Indirecto, al ataque que utiliza intermediario para alcanzar su elemento objetivo.

2.1.3. En función de sus herramientas

Por las herramientas que el atacante utiliza para dirigir su ataque al elemento objetivo, los ataques pueden clasificarse en engaño tecnológico, engaño a la persona o engaño sofisticado.

2.1.3.1. Engaño tecnológico

Un engaño tecnológico, ocurre cuando los medios para obtener la información, son de tipo tecnológico o de infraestructura, por ejemplo, suplantación de servidores.

2.1.3.2. Engaño a la persona

Un engaño a la persona, utiliza los mecanismos de persuasión mencionados anteriormente para obtener la información que el atacante desea, por ejemplo, suplantación de la identidad, abuso de confianza, etc.

2.1.3.3. Engaño sofisticado

Un engaño sofisticado, es un híbrido entre los dos anteriores, utiliza información personal y asocia a elementos conocidos por la víctima, para luego presentárselo a la misma y crear un ambiente de confianza.

2.2. Tipos de atacante

2.2.1. En función de su ubicación

Por la ubicación del atacante desde la perspectiva organizacional víctima, los atacantes pueden ser internos y externos a la misma.

2.2.1.1. Atacante externo

Generalmente, un atacante externo es una persona ajena a la organización o ente individual víctima. No importando las razones, el atacante puede poner como objetivo una organización o ente individual para lanzar sus ataques de manera remota. Puede tener un contacto o relación indirecta con su víctima, pero no es parte oficial de la organización ni persona cercana al individuo atacado. Sus fines pueden ser variados, desde una curiosidad mal sana, hasta hurtar información confidencial y que esto sea el punto de partida de un robo económico o de información de mayor magnitud, que impacte grande y negativamente a la organización o ente individual.

2.2.1.2. Atacante interno

Este tipo de atacantes son los más peligrosos, debido a que sus ataques son más difíciles de detectar a pesar que están más cerca de las reglas de seguridad de la organización. El peligro y el impacto asociado al ataque, incrementan en función del puesto que desempeñe el atacante interno, ya que puede ser un usuario que interactúe directamente con la información o indirectamente. Sus razones pueden variar al igual que el atacante externo.

2.2.2. En función de su objetivo

Existen tantos tipos de ataques a la Seguridad Informática, como vulnerabilidades en los sistemas y herramientas tecnológicas. Cada uno con un objetivo específico. Para dar una clasificación en función al objetivo del ataque, los atacantes también llamados piratas informáticos, pueden conocerse de muchísimas formas, a continuación se mencionan las principales:

2.2.2.1. *Hacker*

Este tipo de atacante tiene amplia experiencia en sistemas informáticos y conocimientos avanzados sobre el funcionamiento de los mismos. También tienen conocimientos en lenguajes de programación, redes, electrónica y servidores. Sus principales razones para infiltrarse en los sistemas, son la curiosidad, el gusto por el arte de la intrusión y su interés en demostrar sus capacidades, pero generalmente no roban información ni alteran los sistemas; es decir, sus ataques son pasivos.

2.2.2.2. *Cracker*

Este tipo de atacante tiene una particular pasión por romper los sistemas y *software*, y su única labor es el uso de *cracks*, que son llaves que legalizan el uso de un sistema sin límite de tiempo y dinero. Una vez que ha creado los *cracks*, los difunden en la *Internet* y se vuelven de dominio público, lo cual es el ataque más dañino para las empresas que desarrollan sistemas que se comercializan.

2.2.2.3. *Phreaker*

Este tipo de atacante tiene especialidad en telefonía, tanto de tierra como móvil. Su conocimiento va más allá de las redes, tiene conocimiento técnico de los dispositivos y su funcionamiento. Es un *cracker* en el teléfono, busca su intrusión en las redes públicas y privadas de telefonía.

2.2.2.4. *Lamer*

Este tipo de atacante es el más común en la *Internet*, son atacantes que se dicen ser *Hackers*, sin embargo, no tienen las bases del conocimiento necesario para entrar en esa clasificación. Su ataque es peligroso debido a que hacen uso de todas las aplicaciones disponibles en la *Internet* para obtener información confidencial y atacar a su víctima, pero sin una noción clara de lo que hace. Sus acciones están basadas en el deseo de sentirse competente y demostrarlo al mundo, aunque ésta no sea la realidad.

2.2.2.5. *NewBie*

Este tipo de atacante es similar al *Lamer*, pero a diferencia de ellos, al implementar las aplicaciones disponibles en la *Internet*, no se apasiona por hacer público el éxito de su ataque, sino se apasiona en continuar aprendiendo. El objetivo de sus ataques es el continuo aprendizaje de la materia.

2.3. Perfil del atacante

Dependiendo del fin por el cual el Ingeniero Social ataca, existen ciertas características que definen el perfil del mismo.

2.3.1. Perfil psicológico

- En general, es de sexo masculino entre los 18 y 30 años de edad
- Razones de motivación: lucro, popularidad o amor al arte
- No cuenta con registro delictivo en otras modalidades
- No es sociable
- Encuentra gran complacencia en realizar con éxito sus actos de intrusión
- Tendencia definida a lo místico
- Curioso
- Adictos a la *Internet*
- Pérdida de la noción del tiempo transcurrido en línea.

2.3.2. Perfil académico/laboral

- Alto potencial intelectual
- Posee conocimientos técnicos de computación
- Posee gran imaginación y habilidad creativa
- En muchos casos, empleado de confianza en una organización
- Actitud de reto frente a los sistemas que administra
- No trabajan en equipo, generalmente sus actos los realizan solos
- Autodidactas
- Gusto por la lectura asociada a la informática.

3. EL ATAQUE MÁS EXITOSO: EL INADVERTIDO

El éxito del ataque inadvertido radica no sólo en obtener información confidencial, sino en obtenerla sin ser detectado. Como se mencionó anteriormente en los Tipos de Ataques (ver capítulo 2, inciso 2.1.3), un engaño a la persona, utiliza los mecanismos de persuasión para obtener la información que el atacante desea, es por ello que se define como el ataque más exitoso. Los otros tipos de ataque apelan a las vulnerabilidades tecnológicas, y las empresas contrarrestan peligros de intrusión en esa área, contratando personal especializado en Seguridad Informática. Dicho especialista puede educarse en la materia, y con un buen equipo de trabajo, modela la infraestructura adecuada y establece niveles de seguridad para las aplicaciones de la empresa, para los usuarios y a nivel de *hardware*.

Sin embargo, los engaños a las personas, son ataques que difícilmente pueden contrarrestarse. Aspectos de la conducta humana no pueden controlarse y es difícil identificar reacciones específicas en la misma. Aunque una concientización al personal puede ser de mucha utilidad, la reacción de una persona ante un ataque es impredecible debido a los factores que afectan la conducta humana en determinadas situaciones, como el miedo, el nerviosismo o la ansiedad. Una actitud de alerta puede ser aprendida, sin embargo, difícilmente puede ser permanente.

Debido al factor humano, los ataques más exitosos, lejos de ser los que burlan la seguridad de la infraestructura y de los sistemas, son los que logran engañar al humano, en otras palabras, la Ingeniería Social.

3.1. Herramientas

A continuación se detallan las herramientas más comunes utilizadas por la Ingeniería Social para engañar a las personas, los ataques que no son detectados por el usuario como una amenaza, o simplemente se aprovechan de la distracción, poca atención o poco conocimiento del usuario para lograr su cometido.

3.1.1. *Spyware*

Se le denomina *Spyware* a todo componente de *software* que es utilizado para espiar dentro de los sistemas. Básicamente su objetivo es obtener información de los sistemas y utiliza el mecanismo de espionaje, es decir, obtener la información sin que su tarea sea detectada. Su medio de navegación es la *Internet* y los datos que le interesan son por ejemplo:

- Tendencias del usuario para la navegación
- Sitios visitados más frecuentemente
- Operaciones comúnmente realizadas por el usuario
- Contenidos instalados en la computadora
- Dirección IP
- Etc.

Todo dato que revele un perfil de usuario, ya que ésta información es buscada por empresas que encuentran en dicho perfil un cliente o usuario potencial. Las formas más comunes de penetrar son a través de *pop-ups* comerciales, las cuales son ventanas de publicidad que se disparan al momento de navegar por algunas páginas *Web*, a través de intercambio de archivos (P2P) y la descarga de *software freeware* y *shareware*.

3.1.2. *Phishing* o Suplantación de Identidad

El *Phishing* es una forma de estafa diseñada para obtener información relevante del usuario, por ejemplo, contraseñas, números de tarjetas de crédito, pines, firmas, información sobre cuentas bancarias, etc. Conocida en español, como Suplantación de Identidad.

Sus medios de propagación son correos electrónicos donde se despliega a la víctima, enlaces a sitios de supuestas entidades, donde el usuario es invitado a ingresar información personal. Entiéndase entidades bancarias, promociones de sorteos, ofertas y premios ofrecidos con tan sólo proporcionar información en formularios.

Esta herramienta requiere de conocimiento por parte del atacante en el caso que la página *Web* apunte a un dominio existente, ya que requiere vulnerar servidores y alterar archivos de configuración para que el usuario acceda al sitio pirata creyendo que accede al auténtico, también conocido como *Pharming.*

Existe otro método menos laborioso, cuando el engaño es solamente visual. El atacante se disfraza utilizando una página cuyo aspecto visual es exactamente igual a la de una entidad existente. El usuario ingresará la información solicitada, creyendo que es un sitio de confianza y sin verificar la dirección ubicada en el navegador. A ésta forma de *Phishing* también se le llama Clonación de Páginas y no requiere hacer uso de vulnerabilidades del sistema que se desea clonar, por lo tanto, no requiere de mucho conocimiento por parte del atacante.

3.1.3. *Vishing (Voice phISHING)*

Se le llama *Vishing* o VoIP *Phishing* a una variante del *Phishing* que incluye el uso del protocolo Voz sobre IP para ejecutar el engaño. De la misma forma que el *Phishing*, el ataque se envía a través de correos electrónicos, y en lugar de desplegar a la víctima un enlace a un sitio de la *Internet*, se le ofrece un número telefónico, generalmente gratuito donde puede registrar información o actualizarla para participar en sorteos, premios, ofertas de interés al usuario o inclusive para ofrecer ayuda para bloquear cuentas de banco, tarjetas de débito o crédito que se han reportado robadas.

La llamada dispara un sistema de respuesta por voz que solicita la información de palabras directas de la víctima o a través del ingreso de números de tarjetas, cuentas bancarias o pines por el teclado del teléfono. Podría parecer que este tipo de ataques es menos propenso a obtener víctimas, sin embargo, una respuesta a través del teléfono representa menos trabajo que el ingreso de información por la computadora, esa es la premisa de su éxito.

3.1.4. *Smishing (SMs phISHING)*

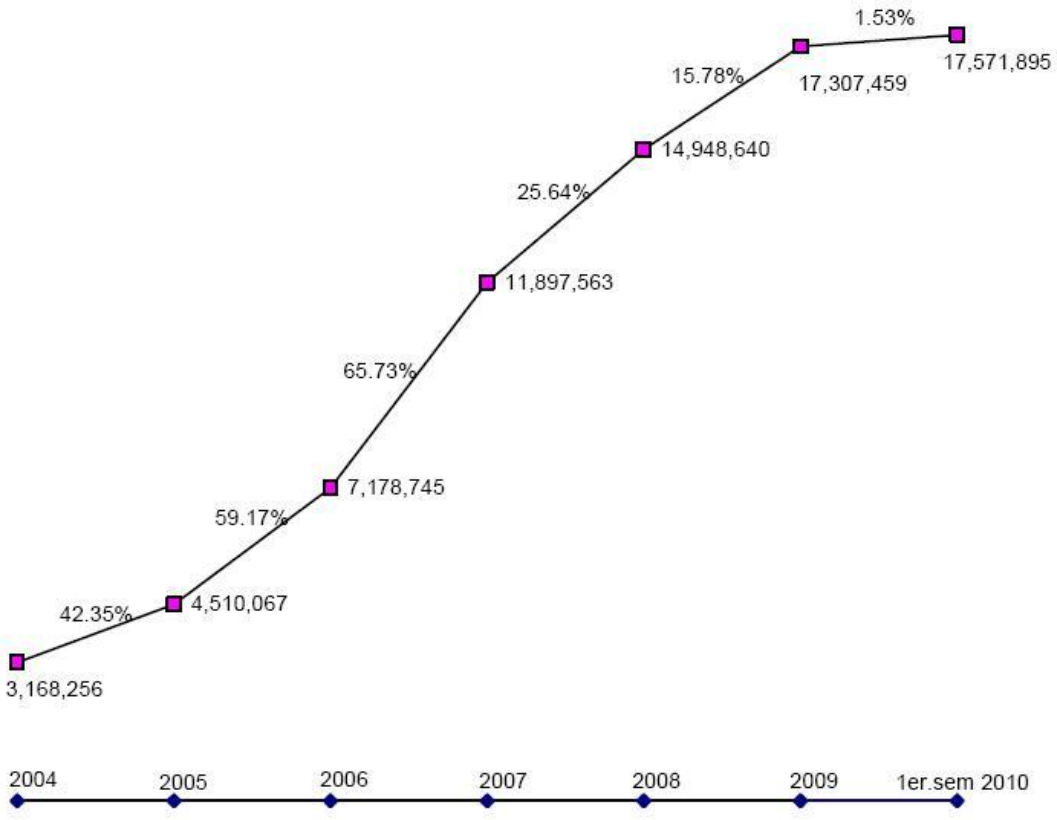
Se le llama *Smishing* a una variante del *Phishing* que incluye el uso de mensajes de texto vía telefónica para ejecutar el engaño. El ataque se envía a través de mensajes de texto a teléfonos móviles obteniendo información privada por medio de suscripciones falsas, participación en sorteos, premios y oportunidades laborales bien remuneradas. Esta herramienta también puede instalar código malicioso en el dispositivo móvil.

3.1.5. *Spam*

Se le llama *Spam* a los envíos masivos de mensajes no deseados a las bandejas de correo electrónico, también llamados correos basura. Dichos mensajes van cargados de publicidad y de código malicioso. Debido al crecimiento en el uso de los teléfonos celulares, el *Spam* se direcciona también a estos dispositivos.

Es importante mencionar que el uso de la telefonía fija y móvil ha ido en aumento en Guatemala año con año, es por ello que estas herramientas están siendo utilizadas cada día más por los Ingenieros Sociales. Hace una década era menos frecuente el uso de los dispositivos telefónicos móviles ya que el acceso a dichos recursos era escaso o limitado. Según la Superintendencia de Telecomunicaciones de Guatemala y sus estadísticas reveladas en cuanto al crecimiento de telefonía móvil, se presenta un crecimiento aproximado de 3 millones de usuarios por año. En el 2005 los usuarios eran 4 510 067 y para el primer semestre del 2010 se registraron 17 571 895. La figura se muestra a continuación:

Figura 2. **Crecimiento de la telefonía móvil en Guatemala de 2004 al primer semestre 2010**



Fuente: Superintendencia de Telecomunicaciones, (s.f.). www.sit.gob.gt. Consulta: enero 2011, de www.sit.gob.gt/index.php?page=situacion-de-la-telefonia-en-guatemala

3.1.6. *Scareware o Rogueware*

Se le llama *Scareware* a todas las aplicaciones que engañan a los usuarios al detectar supuestas amenazas en el sistema y a través de la *Internet*, ofrecen herramientas o aplicaciones para contrarrestarlas. En pocas palabras, simulan aplicaciones para Seguridad Informática. Estas herramientas esperan

que cuando el usuario sea inducido a eliminar un peligro, instalará *software* inmediatamente para eliminarlo. Tiene gran éxito ante usuarios muy confiados en que están recibiendo ayuda, sin embargo, la amenaza radica en el *software* que el usuario instala como respuesta al peligro detectado.

Como el usuario puede presentar ciertas reservas para instalar cualquier aplicación que se le ofrezca, el *Scareware* logra su cometido disfrazándose generalmente de *software* antivirus que debe instalarse en la computadora o que puede escanear el sistema en línea.

Las páginas *Web* de los antivirus son un blanco favorito para estas herramientas, ya que los usuarios sienten la confianza de escanear en línea su computadora o probar una nueva versión del antivirus. Esto es lo que busca el *Scareware* para infiltrar código malicioso, tal como ocurrió con el sitio del reconocido antivirus *Kaspersky* que en octubre del 2010 cuando los usuarios descargaban algunos de los productos ofrecidos por la empresa, se les re direccionaba automáticamente a una página pirata.

3.2. Técnicas

Ya que se han mencionado las herramientas que utilizan los Ingenieros Sociales, se hace necesario abordar algunas habilidades de los atacantes para aplicar sus conocimientos. En todos los ataques perpetrados por estos personajes, quedan en manifiesto sus técnicas de persuasión para poder inducir o provocar la respuesta favorable de la víctima.

Las técnicas de persuasión abordadas por el Ingeniero Social, apelan a las conductas del comportamiento humano (véase capítulo 1, inciso 1.2.2) para lograr un objetivo. El primer paso de un ataque radica en un proceso de

investigación, el cual consiste en recopilar la mayor información de la víctima y su entorno para definir posibles intereses y tendencias que le brindan al atacante los argumentos necesarios para el desarrollo de un plan de ataque. El Ingeniero Social busca la manera de establecer un canal de comunicación persuasivo haciendo uso de sus estrategias.

3.2.1. La reciprocidad

En el comportamiento humano existe la tendencia de ser recíproco. Una vez se obtiene un favor por parte de una persona, se aprovecha la primera oportunidad para hacer algo a favor del que lo hizo con nosotros. Averiguado el contexto dentro del que se encuentra la víctima, el Ingeniero Social ofrece o promete cierta ayuda o productos que no necesariamente le fueron requeridos. La mayoría de veces, esta conducta provoca confianza y da la oportunidad de no cerrar ese canal de comunicación establecido. Muchas veces puede hacerse pasar como un elemento que forma parte de la empresa y que necesita un favor que obviamente pagará después con otro.

Esta técnica se fundamenta en tratar a los demás como nos tratan a nosotros. Si el Ingeniero Social lanza un favor a su víctima, ésta tiende a adquirir obligaciones en un futuro, que puede traducirse en la revelación de algún dato o el acceso a determinada área o información. Por ejemplo, para sacar cierta información íntima, el Ingeniero Social tendrá que hacerlo primero con la víctima. Confesión con confesión se paga.

3.2.2. El compromiso y la consistencia

Es común en el comportamiento humano, dar mucho valor a un compromiso verbal en el que haya incurrido. Incluso puede ser que la labor por

la que se comprometió ya no se haga necesaria, sin embargo, si el Ingeniero Social logra provocar que la víctima se comprometa a hacer o averiguar algo en específico, ésta estrategia aumenta la probabilidad del éxito de su ataque.

El Ingeniero Social está consciente que el éxito también depende muchas veces de la perseverancia y la consistencia, por lo tanto, antes de ejecutar el ataque, puede establecer contacto con la víctima más de una vez. Esto le generará una identidad delante de su presa y le abre la puerta a la confiabilidad.

3.2.3. La validación social

Uno de los perfiles de víctima que el Ingeniero Social tiene seguro, es aquel personaje excluido socialmente. Le es más fácil persuadir o manipular a una persona que busca la aprobación o aceptación social y que podría hacer cualquier cosa por lograr aceptación o por la necesidad de quedar bien con los demás.

El comportamiento humano tiene la tendencia a creer que el hacer lo que los demás hacen, reduce el riesgo de rechazo o el riesgo a cometer errores. Todos los seres humanos en alguna forma dejamos actuar a la validación social en nuestra vida, e incluso la hacemos partícipe de nuestras decisiones, por ejemplo, cuando se consulta una lista de mejores productos, productos más vendidos, artículo más consumido, *software* más utilizado, canciones más escuchadas, etc.

3.2.4. La autoridad

Para el Ingeniero Social no es necesario tener conocimientos avanzados en Informática, como ya se ha mencionado. Independientemente de éste

hecho, durante el ataque va a pretender convencer a la víctima que está interactuando con un experto de la Informática o con un alto ejecutivo de la institución a la que ataca. El comportamiento humano también se caracteriza por la tendencia de obedecer a una figura que ejerza cierta autoridad sobre nosotros, aunque no sea necesario que se esté de acuerdo con las decisiones tomadas por dicha figura. Hace uso de premisas intimidantes o amenazantes para provocar temor en la víctima, y así conseguir lo que desee. A continuación se mencionan algunos ejemplos:

- Le habla el director del departamento de Recursos Humanos y me urge que me brinde el detalle de ese documento.
- Si usted no colabora con esa información, puede provocar un grave error en el sistema que atrase el pago del mes de muchos empleados.

Esta estrategia apela a la tendencia de pensar que un empleado que ocupa un puesto mayor que el nuestro dentro de la jerarquía de la organización tiene más conocimiento que nosotros. También toma en cuenta la simbología que puede representar un servidor público, por ejemplo; un policía, un médico, un bombero, etc.

3.2.5. El gusto

Esta estrategia es muy utilizada por los Ingenieros Sociales, ya que sus resultados aseguran un éxito total. La víctima es persuadida por personas agraciadas o por mensajes con contenido sumamente atrayente para la víctima, por ejemplo, mensajes en la *Internet* con mujeres u hombres altamente atractivos, contenido sexual, dinero fácil, etc. Todo este material induce al usuario a ingresar a sitios o descargar aplicaciones e instalarlas, abriendo la puerta a los contenidos de espionaje.

También incluye utilizar modales amigables y detalles agradables que logran una empatía con su víctima. Si el ataque es verbal, busca la forma de lograr con su víctima una identificación intelectual con sus pensamientos, sentimientos o actitudes, apelando al puesto que desempeñe, la condición del clima, la hora laboral, entre otros. Utiliza la adulación para crear ese ambiente de confianza con su víctima y obtener información del contexto que le rodea. Es por ello que personajes positivos, inteligentes, fuertes, bondadosos, con gran sentido del humor o súper héroes tienen tanta influencia en los demás.

3.2.6. La escasez

Cuando el Ingeniero Social detecta con la investigación previa al ataque las necesidades de su víctima, su persuasión se basa en esta técnica ya que la conducta humana tiende a buscar lo que necesita o cree necesitar. La estrategia de apelar a la escasez, explota los sentimientos y deseos de las personas, entiéndase la curiosidad, la compasión, entre otros.

4. ÁMBITO LEGAL

4.1. Legislación

Tal como se ha mencionado al inicio de esta investigación, la era de la información está fuertemente ligada con la tecnología de la información y la comunicación (véase capítulo 1, inciso 1.1.3), y el incremento exponencial que presenta el uso de las mismas, hace necesario para el bienestar social de un país, tener normas que regulen su acceso y su utilización con el fin de gozar de sus beneficios y minimizar los impactos negativos si en caso los hubiera.

4.2. Importancia de la legislación para los delitos informáticos

Internet World Stats es un sitio *Web* internacional que registra el uso de la *Internet* en más de 233 países y regiones, también registra estadísticas de población y datos de investigación en el mercado en la *Internet*. El sitio brinda una herramienta muy útil de estadísticas de Comercio Electrónico, investigación en línea del mercado internacional, datos de banda ancha, población mundial, entre otros.

Este sitio refleja las estadísticas más recientes de Centro América en el uso de la *Internet* realizadas en la fecha 31 de marzo de 2011.

Tabla I. **Estadísticas del uso de la *Internet* en la Región Centroamericana**

PAÍS	POBLACIÒN	USUARIOS 2000	USUARIOS 2011	PORCENTAJE POBLACIÓN	CRECIMIENTO
Costa Rica	4 576 562	250 000	2 000 000	44,3%	700 %
El Salvador	6 071 774	40 000	975 000	16,1 %	2 337,5 %
Guatemala	13 824 463	65 000	2 280 000	16,5 %	3 407,7 %
Honduras	8 143 564	40 000	958 500	11,8 %	2 296,3 %
Nicaragua	5 666 301	50 000	600 000	10,6 %	1 100,0 %
Panamá	3 460 462	45 000	959 900	27,7 %	2 033,1 %

Fuente: Miniwatts Marketing Group. (s.f.). Internet World Stats. Consulta: agosto 2011, de http://www.internetworldstats.com/central.htm

De acuerdo a los datos anteriores, Guatemala es el país que mayor crecimiento ha tenido en el uso de la *Internet* a nivel centroamericano. Debido a este innegable aumento del protagonismo de la *Internet* en la sociedad guatemalteca, se vuelve imperante el análisis y el planteamiento de una regulación legal en el tema. De la misma forma, como el uso de la tecnología va en crecimiento, también se abren las posibilidades al aumento de los crímenes en este ámbito, por lo tanto, se hace necesario definir estrategias de prevención y combate ante dichos crímenes.

Todas las áreas de la sociedad están siendo influenciadas por la tecnología, entiéndase educación, salud, industria, etc. Por lo tanto, la implementación de una ley que regule las actividades dentro de los Sistemas de Información puede incluso brindar una atmósfera de confianza a futuros inversionistas que busquen el desarrollo tecnológico o industrial en Guatemala.

4.3. Ley de Delitos Informáticos

El Congreso de la República de Guatemala recibió 2 iniciativas de ley que disponen aprobar la Ley de Delitos Informáticos, la cual pretende sancionar de manera penal todas aquellas actividades que se definen como delitos informáticos. Una con registro 4054 conocida en el pleno el 19 de agosto de 2009 con nombre Ley contra el Cibercrimen y presentada por los Diputados Mariano Rayo y José Alejandro Arévalo y la segunda con registro 4055 conocida en el pleno el 18 de agosto de 2009 y presentada por los Diputados Francisco Contreras, Mario Mazariegos y Félix Ruano con el nombre Iniciativa de Ley que dispone aprobar la Ley del Cibercrimen.

La Comisión de Legislación y Puntos Constitucionales, con la ayuda de personas expertas en la materia, debe revisar de manera legal y técnica ambas iniciativas y unificarlas, ya que tienen el mismo objetivo. Posterior a eso, se busca mejorarla a través de audiencias a personas o instituciones que deseen opinar o agregarle valor. El proceso para ser aprobada es largo en el tiempo, y la versión de la iniciativa que es entregada inicialmente, va reflejando mejoras durante el mismo.

Según indicaciones del diputado Francisco Contreras, se recibieron muchas sugerencias al proyecto de ley por parte de personas y entidades nacionales e internacionales. A continuación se exponen los puntos más destacados.

4.3.1. Comité regulador

El dictamen favorable a la propuesta de ley, indica la creación del Comité de Respuesta a Incidentes de Seguridad Informática para Guatemala, CSIRT-gt por sus siglas en idioma inglés, el cual será adscrito al Ministerio de la Defensa Nacional.

4.3.1.1. Funciones

- Proactivas

  Educación, asesoramiento técnico, alertas y promoción de estándares de seguridad.

- Reactivas

  Asistencia a incidentes de seguridad informática y formulación de recomendaciones para la prevención de los mismos.

- Investigación y desarrollo

  Generar proyectos de investigación y desarrollo de tecnologías asociadas a la seguridad informática.

4.3.1.2. Organización

- Comité Director

Cada una de las siguientes instituciones formará parte de este Comité, a través de un representante:

- Ministerio de la Defensa
- Ministerio de Relaciones Exteriores
- Ministerio Público
- Ministerio de Gobernación
- Superintendencia de Bancos
- Superintendencia de Telecomunicaciones
- Secretaría Técnica del Consejo Nacional de Seguridad.

- Comité Operativo

Cada una de las siguientes instituciones formará parte de este Comité, a través de dos o más delegados:

- Ministerio de la Defensa
- Ministerio Público
- Ministerio de Gobernación.

Cada uno de los miembros del Comité Operativo deberá contar con acreditación de seguridad informática extendida por un ente certificador debidamente autorizado y cumplir con el perfil establecido.

- Personas Adheridas

Cada uno de los organismos del Estado, sus instituciones y dependencias, deberán formar parte del CSIRT-gt, a efecto de participar activamente en la generación y cumplimiento de las políticas de seguridad informática a nivel nacional.

4.3.2. Sanción penal

El dictamen favorable de la propuesta de ley, indica que tendrán sanción penal los hechos que se consideran en la tabla descrita posteriormente, si se cometen dentro del territorio de la República de Guatemala, si son cometidos fuera del mismo, el responsable quedará sujeto a las disposiciones si dentro del territorio son producidos los efectos de los hechos. La siguiente tabla condensa el detalle y las sanciones penales asociadas a cada delito que presentan tanto la iniciativa de ley como su dictamen favorable respectivo. Donde tiempo en prisión está en años y multa en número de veces el salario mínimo legal vigente.

Tabla II. **Sanciones penales asociadas a los delitos informáticos**

DELITO	DESCRIPCIÓN	TIEMPO EN PRISIÓN	MULTA
Delitos contra la confidencialidad, integridad y disponibilidad de los datos y tecnologías de la información.			
Acceso ilícito.	Quien acceda a sistema que haga uso de tecnologías de la información, sin autorización o excediéndola.	2 – 4	100-500
Daño informático.	Quien sin estar autorizado, alterare, destruyere, inutilizare, suprimiere, modificare, o de cualquier modo o por cualquier medio, dañare un sistema que utilice tecnologías de la información o un componente de éste.	4 – 8	100-500
Reproducción de dispositivos de acceso.	Quien de manera deliberada, cree, utilice, altere, capture, grabe, copie o transfiera de un dispositivo de acceso a otro similar, o cualquier instrumento destinado a los mismos fines, los códigos de identificación y/o acceso al servicio o sistema que haga uso de tecnologías de la información, que permita la operación paralela, simultánea o independiente de un servicio legítimamente obtenido.	4 – 8	100-500

Continuación tabla II …

Dispositivos fraudulentos.	Quien produzca, utilice, comercialice u ofrezca sin autorización o causa legítima, uno o varios programas informáticos, equipo, material o dispositivo cuyo uso principal sea el de emplearse como herramienta o medio para cometer los delitos regulados en la presente ley.	3 – 7 para solicitante.	100-700
		4 – 8 para quien produce, comercializa u ofrece.	
		3 – 7 para quien lo utiliza.	
Espionaje informático.	Quien sin estar facultado para ello, se apodere, obtenga, revele, transmita o difunda el contenido, parcial o total, de sistema que utilice tecnologías de la información o dato informático, de carácter público o privado.	6 – 10	200-700
	La pena será aumentada en una tercera parte cuando afecte la intimidad o privacidad de las personas.		

Continuación tabla II …

Violación de la disponibilidad.	Quien por cualquier medio, provoque la denegación de acceso a redes, información y sistemas que utilicen tecnologías de información, a las personas que están legitimadas para hacerlo.	6 - 10	100-500
	- Cuando se deniegue la confirmación de identidad del destinatario o del remitente, ocasionando repudiación de los sistemas a las personas que están autorizadas o legitimadas para hacerlo.	12 - 15	200-800
	- Cuando la denegación de acceso sea provocada por el envío masivo de mensajes electrónicos, publicitarios o de cualquier otra índole.		
Fraude informático.	Quien para obtener algún beneficio para sí mismo o para un tercero, mediante cualquier artificio tecnológico o manipulación de sistema que haga uso de tecnologías de la información, o, a sus componentes, procure la transferencia no autorizada de cualquier activo patrimonial en perjuicio de otro.	4 – 8	100 - 1 000

Continuación tabla II …

Interceptación ilícita.	Quien intercepte de forma deliberada e ilegítima por cualquier medio, datos informáticos en transmisiones restringidas, dirigidas u originadas en un sistema que utilice tecnologías de la información, incluidas las emisiones electromagnéticas provenientes o efectuadas dentro del mismo, que transporte dichos datos informáticos.	6 – 10	100 - 1 000
	La pena será aumentada en una tercera parte, cuando la interceptación se cometa desde un sistema que utilice tecnologías de la información conectado a otro sistema de la misma naturaleza.		
Falsificación informática.	Quien a través de cualquier medio, copie, altere, sustituya deliberada e ilegítimamente datos informáticos de un sistema que haga uso de tecnologías de la información o uno de sus componentes, generando un resultado no auténtico o para inducir a usuarios a la provisión de datos personales y/o financieros.	4 – 8 años	100 - 1 000
	La pena será aumentada en una tercera parte, si la intención es que el resultado sea utilizado a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente.		

Continuación tabla II …

Delitos contra la persona.		
Delitos de Pornografía Infantil.	Cuando las infracciones establecidas en el Código Penal Decreto Número 17-73, y el Decreto Número 09-2009 sobre Ley Contra la Violencia Sexual, Explotación y Trata de Personas, se cometan a través del empleo de sistemas que utilicen tecnologías de la información, o de cualquiera de sus componentes.	Penas establecidas en el Código Penal Decreto Número 17-73 y 09-2009 sobre Ley Contra la Violencia Sexual, Explotación y Trata de Personas, exceptuando su contenido en el Artículo 16.
Control de Acceso a Pornografía Infantil.	Los proveedores de servicio de *Internet*, deberán establecer normas mínimas de seguridad para bloquear el acceso a portales o páginas *Web* que contengan material pornográfico infantil, y, en caso de incumplimiento, se les considerará coautores juntamente con las personas responsables de los delitos relativos a la pornografía infantil en lo que fuera aplicable.	

Continuación tabla II …

Difusión y alteración de imágenes personales.	Quien sin la autorización explícita y por escrito del titular, modifique, altere, envíe, difunda, transmita o almacene imágenes de otra persona por medio de sistemas que utilicen tecnologías de la información, para fines fraudulentos o con intención de perjudicar el honor de una persona. No constituyen delito o falta las publicaciones que contengan denuncias, críticas o imputaciones contra funcionarios o empleados públicos por actos efectuados en el ejercicio de sus cargos.	4 – 6	100-300
Uso de identidad ajena.	Quien haga uso de una identidad ajena, a través de medios que utilicen tecnologías de la información.	3 – 7	300-700
Delitos contra la nación y actos de terrorismo.			
Delitos contra la nación.	Los actos que se realicen a través de un sistema que utilice tecnologías de la información, que atenten contra los intereses fundamentales y seguridad de la nación, tales como el sabotaje, el espionaje o proveer información no autorizada.	10 – 20	1 000 - 10 000

Continuación tabla II …

Actos de terrorismo informático.	Todo aquel que con el uso de sistemas que utilicen tecnologías de la información, ejerza actos de terrorismo contra la infoestructura (medio generador por el cual una nación convierte los activos, ya sea materiales en bruto, tecnologías o ideas, en productos de valor y servicios) del Estado.	10 – 20	1 000 - 10 000

Fuente: Congreso de la República de Guatemala. Iniciativa de Ley 4055 [en línea]: http://www.congreso.gob.gt/iniciativas.php?id=4298 [Consulta: agosto 2011]

4.3.3. Situación actual de la iniciativa

La Red Iberoamericana ElDerechoInformatico.com, a través de su corresponsal oficial en Guatemala, el Licenciado José Leonett, realizó una entrevista el pasado 16 de diciembre de 2010 al diputado Mariano Rayo Muñoz para conocer detalles de la iniciativa de ley y su actual situación.

En dicha entrevista, el diputado Rayo señala que con el objeto de establecer el avance de la propuesta de regulación se tomó en cuenta el informe Estado situacional y perspectivas del derecho informático en América Latina y el Caribe, el cual, analiza la situación de la regulación en materia de delitos informáticos y delitos por medio de las tecnologías de la información.

El Consejo de Europa, que engloba a 47 miembros y a países que incluso no forman parte de los 27 de la Unión Europea, celebró el acuerdo Budapest sobre Cibercrimen que procura la unificación de la legislación de los países

miembros. Este acuerdo se originó debido al riesgo que parte de la digitalización, globalización de las redes y la información electrónica de ser utilizada para cometer delitos informáticos, así mismo, exige la necesidad de aplicar con carácter prioritario, una política penal común contra la ciberdelincuencia y pretende fomentar la cooperación internacional contra la misma. Sin embargo, a la fecha de la entrevista al diputado Rayo, ningún país de América Latina ha firmado ni ratificado dicho acuerdo, lo que indica que se está abordando dicha área de manera aislada al resto del mundo.

Para finales del 2010, la Comisión de Legislación y Puntos Constitucionales firmó el dictamen número 17-2009 favorable a la iniciativa de ley 4055, para que continúe con el trámite de aprobación final y se incorpore al ordenamiento jurídico nacional. Sus ponentes esperaban que fuera aprobada durante el primer trimestre del presente año 2011 para luego ser implementada una campaña de difusión, lo que incluye una amplia capacitación a los operadores que justicia con respecto al tema.

Hasta la fecha actual, hay muchos temas al respecto de esta propuesta de ley que se necesitan re-definir, analizar, debatir y ampliar. Sus ponentes han hecho una invitación pública a todos los sectores involucrados directa o indirectamente con el tema para que formen parte activa de la mejora de la propuesta antes que llegue al Pleno del Congreso y entre en vigencia.

Tal como lo indica el Proceso Legislativo del Congreso de la República de Guatemala (vea ANEXO: Proceso Legislativo de aprobación de una ley o de reforma de leyes), la iniciativa de ley se considera en su fase inicial, ya que se encuentra en los 3 primeros pasos de los 10 identificados, y tomando en cuenta que la ley no establece un límite de tiempo para la aprobación de una propuesta, se asume que se necesita bastante para lograr su publicación.

Como referencia se puede mencionar que existen iniciativas de ley que han culminado su proceso legislativo en 45 a 50 meses (por ejemplo la iniciativa de ley 3550 –Ley de Participación Ciudadana- del año 2006), según información publicada el sitio *Web* del Congreso de la República.

Cabe reiterar la invitación a participar en este proyecto, listando los distintos sectores y sus representantes que actualmente son parte activa del mismo a través de mesas de diálogo, conferencias, entrevistas, etc.

- Consejo Nacional de Ciencia y Tecnología
- Universidad de San Carlos de Guatemala
- Universidad Rafael Landívar
- Universidad del Valle de Guatemala
- Universidad Francisco Marroquín
- Asociación Guatemalteca de Exportadores –AGEXPORT
- Cámara de Industria de Guatemala
- Ministerio de Relaciones Exteriores
- Ministerio de la Defensa Nacional
- Ministerio Público
- Entidades privadas
- Ciudadanos, estudiantes y catedráticos.

4.4. Ley de Acceso a Información Pública

En septiembre del 2008, el Congreso de la República de Guatemala aprobó por unanimidad la Ley de Acceso a la Información Pública, asunto que ocasionó mucha contienda en el país debido a su naturaleza. Dicha ley garantiza a los ciudadanos su derecho de acceso a la información que se encuentre en manos de los funcionarios públicos.

Cabe mencionar en el contexto de la presente investigación, que dicha ley fue protagonista de muchos desacuerdos, debido a que hoy en día, revelar información de la organización puede ser punto de partida para que muchos delincuentes (no solo informáticos), obtengan la información inicial para su ataque, la cual puede ser un nombre, un puesto, un procedimiento, etc.

La ley quedó plasmada en el Decreto 57-2008 del Congreso de la República de Guatemala y a continuación expongo lo que concierne al tema.

4.4.1. Ámbito de aplicación (Artículo 4)

Toda la información relacionada al derecho de acceso libre a la información contenida en registros, archivos, fichas, bancos, o cualquier otra forma de almacenamiento de información pública, en custodia, depósito o administración de los sujetos obligados, se regirá por lo que establece la Constitución Política de la República de Guatemala y la presente ley.

4.4.2. Sujetos obligados (Artículo 6)

Es toda persona individual o jurídica, pública o privada, nacional o internacional de cualquier naturaleza, institución o entidad del Estado, organismo, órgano, entidad, dependencia, institución y cualquier otro que maneje, administre o ejecute recursos públicos, bienes del Estado, o actos de la administración pública en general, que está obligado a proporcionar la información pública que se le solicite.

4.4.3. Definiciones (Artículo 9)

Para la presente ley, se entiende por:

4.4.3.1. Información pública

Información en poder de los sujetos obligados contenida en los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades o la actividad de los sujetos obligados y sus servidores públicos, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier medio sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico y que no sea confidencial ni estar clasificado como temporalmente reservado.

4.4.3.2. Información confidencial

Información en poder de los sujetos obligados que tenga acceso restringido o haya sido entregada por personas individuales o jurídicas bajo garantía de confidencialidad, por mandato constitucional o disposición expresa, de una ley.

4.4.3.3. Información reservada

Información pública cuyo acceso se encuentra temporalmente restringido por disposición expresa de una ley, o haya sido clasificada como tal, siguiendo el procedimiento establecido en la presente ley.

4.4.3.4. Datos personales

Lo relativo a cualquier información concerniente a personas naturales identificadas o identificables.

4.4.3.5. Datos sensibles o datos personales sensibles

Aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o actividad, tales como los hábitos personales, el origen racial, el origen étnico, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud física o psíquicos, preferencia o vida sexual, situación moral y familiar u otras cuestiones íntimas de similar naturaleza.

4.4.4. Procedimiento de acceso a la información pública

Del Artículo 38 al 45, describen el proceso a seguir que inicia por la petición del interesado indicando claramente su identificación, la identificación del sujeto obligado y la información que solicita. Como respuesta a dicha solicitud, la Unidad de Información, donde se presentó el interesado, debe emitir resolución dentro de los diez días siguientes, entregando la información solicitada, notificando la negativa parcial o total de la misma o expresando la inexistencia. Se considerará una prórroga en el tiempo de respuesta, cuando el volumen y extensión de la solicitud así lo requiera, pudiéndose ampliar hasta por diez días más notificando al solicitante dentro de los dos días anteriores a la conclusión del plazo señalado por la ley.

4.4.5. Sanción penal

En los Artículos 61 al 67, se describen las responsabilidades y sanciones correspondientes a la presente ley. Las sanciones se describen en la siguiente tabla, donde tiempo en prisión está en años y multa en quetzales.

Tabla III. **Sanciones penales asociadas a Ley de Acceso a la Información Pública**

DELITO	DESCRIPCIÓN	TIEMPO EN PRISIÓN	MULTA
Comercialización de datos personales.	Quien comercialice o distribuya por cualquier medio, archivos de información de datos personales, datos sensibles o personales sensibles, protegidos por la presente ley sin contar con la autorización expresa por escrito del titular de los mismos y que no provengan de registro públicos.	5 – 8	50 000 - 100 000
Alteración o destrucción de información en archivos.	Quien sin autorización, altere o destruya información de datos personales, datos sensibles o personales sensibles de una persona, que se encuentren en archivos, ficheros, soportes informáticos o electrónicos de instituciones públicas.	5 – 8	50 000 - 100 000
Retención de información.	El funcionario, servidor público o cualquier persona responsable de cumplir la presente ley, que en forma arbitraria o injustificada obstruya el acceso del solicitante a la información requerida.	1 – 3	10 000 - 50 000

Continuación tabla III …

Revelación de información confidencial o reservada.	El servidor, funcionario o empleado público que revelare o facilitare la revelación de información de la que tenga conocimiento por razón del cargo y que por disposición de ley o de la Constitución Política de la República de Guatemala sea confidencial o reservada.	5 – 8	50 000 - 100 000

Fuente: Congreso de la República de Guatemala. Iniciativa de Ley 4055 [en línea]: http://www.congreso.gob.gt/decretos.php?id=13086 [Consulta: agosto 2011]

5. BUENAS PRÁCTICAS PARA RESGUARDAR LA SEGURIDAD DE UN SISTEMA

5.1. Empresas

Las empresas en su calidad de patrono son los entes que deben introducir en sus organizaciones los mecanismos necesarios para contrarrestar el engaño a sus empleados. Los directivos y ejecutivos en conjunto con personal profesional de Tecnologías de la Información deben facilitar los medios para lograr una concientización en cuanto al peligro de ser objeto de engaños inadvertidos que ponga en riesgo la seguridad de los sistemas.

A continuación se mencionan algunas prácticas que se consideran necesarias para resguardar la seguridad de un sistema:

5.1.1. A nivel técnico

Dentro de la presente investigación se aborda al usuario como objetivo del engaño que pone en riesgo la seguridad de un sistema. Sin embargo, estamos conscientes que no sólo en el empleado cae todo el peso del peligro, la configuración de la infraestructura de los sistemas es también la causante de comprometer la seguridad y facilitar los medios donde se llevan a cabo los cibercrímenes.

Existen muchos temas a nivel técnico, a continuación se mencionan las principales prácticas que los expertos en Seguridad Informática recomiendan a los administradores de Tecnologías de la Información:

- Emplear estrategias de defensa en profundidad, que enfaticen sistemas de protección múltiples y mutuamente complementarios para protegerse de fallas específicas en cualquier mecanismo de seguridad informática. Esto debe incluir el uso de antivirus, *firewalls*, sistemas de detección y protección de intrusos que deben ser actualizados periódicamente.

- Desconectar y eliminar los servicios que no son necesarios para el normal funcionamiento de la red de la empresa.

- Evaluar la seguridad regularmente para garantizar que se implementen y se cuenten con los controles adecuados.

- Actualización regular de *software* antivirus para protegerse de la gran cantidad de nuevas amenazas de códigos maliciosos y garantizar que todos los equipos de escritorio, portátiles y servidores se actualicen con todos los parches de seguridad necesarios de su proveedor de sistema operativo.

- Aplicar una política eficaz de contraseñas. Por ejemplo, asegurarse que las contraseñas sean una mezcla de letras y números, que sea obligatorio el cambio de las mismas con frecuencia y que no se incluyan palabras que se encuentren en un diccionario.

5.1.2. Educación de directivos

Generalmente dentro de la estructura de una empresa, el departamento que maneja el presupuesto es el ente que analiza y evalúa todo lo que para la empresa represente una inversión o gasto.

Muchas empresas basan sus decisiones en lo mucho o poco que necesite monetariamente para realizar un proyecto. El departamento de Informática o Tecnologías de la Información siempre tendrá el arduo trabajo de convencer a los directivos de la importancia de proyectos para la seguridad de un sistema. Es por ello que la educación a los directivos con respecto del tema, es una pieza clave para lograr la concientización que se necesita.

Generalmente los directivos no tienen noción del valor de su información y mucho menos tienen noción de lo fácil que podría ser objeto de robo a través de la Ingeniería Social.

5.1.3. Educación de empleados

Como se ha visto hasta el momento, los empleados de la empresa representan el objetivo principal de un engaño, y generalmente, los empleados que no son parte del departamento de Informática, sino aquellos empleados que son usuarios finales de los sistemas y tienen acceso a ellos. En el inciso 5.2 se abordarán más a detalle lo que los usuarios finales deben aprender para evitar ser engañados.

5.1.4. Definición de roles

A cada empleado debe asignársele un rol específico, y con ello asignarle recursos a utilizar e información a gestionar. Los administradores de los sistemas deben limitar los privilegios para su uso a los usuarios que no requieren dicho acceso y deben restringir dispositivos no autorizados, como unidades de discos duros externos, portátiles y otros medios extraíbles.

5.2. Usuarios

5.2.1. A nivel técnico

A continuación se mencionan algunas prácticas a nivel técnico que el usuario debe poner en práctica para evitar ser víctima de la Ingeniería Social:

- No abrir archivos adjuntos a un correo electrónico, a menos que lo estén esperando y provenga de una fuente conocida y confiable.

- No ejecutar *software* que se descarga de la *Internet*, a menos que se haya escaneado en busca de virus.

- Es recomendable no dar clic en los enlaces o archivos adjuntos a los correos electrónicos ya que puede exponer los equipos a riesgos innecesarios.

5.2.2. Aspectos de la conducta humana como principales obstáculos de la persuasión

A continuación se mencionan algunos aspectos de la conducta humana que representan un obstáculo para la persuasión y que se deben tomar en cuenta para educarnos:

- La resistencia al cambio y el rechazo de cualquier idea que suponga una amenaza a sus creencias o costumbres. La conducta humana busca sentirse propietaria de un espacio de intimidad encontrará rechazo a cualquier alternativa que lo amenace.

- El deseo del dominio. En las relaciones interpersonales, el ser humano tiende a necesitar vencer o dominar. Esta conducta en la víctima del Ingeniero Social, representa un gran obstáculo para el atacante.

CONCLUSIONES

1. La educación es la mayor defensa contra los ataques más comunes de la Ingeniería Social y tan poco conocidos por ser inadvertidos.

2. Guatemala actualmente no puede brindar certeza jurídica a los usuarios de la *Internet* y a todos los empresarios que de una u otra forma buscan ampliar su mercado a través de éste medio, es por ello que la aprobación de la iniciativa de Ley de Delitos Informáticos es imperante para el bienestar de la sociedad a nivel económico y legal.

3. A nivel nacional es escasa o nula la información que existe de actividades realizadas dentro del marco del delito informático. No tener una ley al respecto le impide al Ministerio Público y las entidades correspondientes tener registro específico de estos hechos, por lo tanto, no se puede medir el impacto y la importancia para la sociedad guatemalteca.

RECOMENDACIONES

1. Los empresarios deben tomar en cuenta el uso de las redes sociales por parte de los empleados como una amenaza. El Informe sobre las Amenazas a la Seguridad en *Internet*, Volumen XV, realizado y publicado por *Symantec Corporation* en abril de 2010, indica que los atacantes están aprovechando la abundancia de información personal abiertamente disponible en los sitios de redes sociales para realizar ataques dirigidos a personas con puestos clave dentro de las empresas.

2. El congreso de la República de Guatemala debe tener un panorama de los delitos informáticos a nivel nacional e internacional para mejorar y aprobar la iniciativa de ley que existe al respecto, y así, emitir una ley que contemple los avances tecnológicos.

BIBLIOGRAFÍA

1. Agencia Española de Protección de Datos. *Decálogo con recomendaciones para combatir el Spam* [Decálogo] Madrid: Octubre 2005. [en línea]: http://www.agpd.es/portalwebAGPD/-canaldocumentacion/lucha_contra_spam/common/pdfs/CONSEJOS-para-prevenir-el-Spam_guia.pdf [Consulta: enero 2011].

2. AGUILERA LÓPEZ, Purificación**.** *Seguridad informática.* Morlanes, Gonzalo (ed.); del Arco, Teresa (prod.). Madrid: EDITEX, 2010. ISBN: 978-84-9771-761-8.

3. CASTELLS, Manuel. *La Era de la Información.* 5a ed. Volumen III. México: Siglo XXI, 2006. ISBN: 968-23-2337-1.

4. CIALDINI, Robert B. *Influencia, la psicología de la persuasión.* EEUU: William Monrrow & Company, 2001. ISBN: 0-688-12816-5.

5. Council of Europe. *Convenio sobre criminalidad*. Publicado el 23 de noviembre de 2001. Traducción no oficial [en línea]: http://conventions.coe.int/Treaty/en/Treaties/html/185-SPA.htm [Consulta: enero 2011].

6. El Derecho Informático. *Conociendo el anteproyecto de ley del cibercrimen – Guatemala*. Publicado el 16 de diciembre de 2010. Entrevisa [en línea]: http://www.elderechoinformatico.com/index.php?option=com-_content&view=article&id=426:conociendo-el-anteproyecto-de-ley-del-cibercrimen-guatemala&catid=130:elderechoinformatico-guatemala&Itemid=136 [Consulta: enero 2011].

7. ERB, Markus. Gestión de Riesgo. Notas del Taller Centroamericano Ampliando la Libertad de Expresión: Herramientas para la Colaboración, Información y Comunicación seguras. 2008. [en línea]: http://protejete.wordpress.com/gdr_principal/ [Consulta: enero 2011].

8. ESTRAMIANA, José Luis Álvaro. *Fundamentos sociales del comportamiento humano.* España: Editorial UOC, 2003. ISBN: 84-8318-986-0.

9. GARCIA, Víctor Martín. "La Edad de la Informática. La Cibersociedad". Revista Documentación Social. No. 108. (Julio-Septiembre 1997) p. 11-32.

10. Guatemala. Congreso de la República. Iniciativa de Ley 4054 [en línea]: http://www.congreso.gob.gt/iniciativas.php?id=4297 [Consulta: agosto 2011].

11. _____. Iniciativa de Ley 4055 [en línea]: http://www.congreso.gob.gt/iniciativas.php?id=4298 [Consulta: agosto 2011].

12. _____. Ley de Acceso a la Información Pública. Decreto de Congreso de Guatemala 57-2008. Publicada el 23 de noviembre de 2008. [en línea]: http://www.congreso.gob.gt/decretos.php?id=13086 [Consulta: agosto 2011].

13. HOGG, Michael A.; VAUGHAN, Graham. *Psicología social.* Haro, Marcela (trad.); Klajn, Diana (trad.). 5a ed. Madrid: Médica Panamericana, 2010. ISBN: 978-84-9835-227-6.

14. ITNews. Los Orígenes de la Ingeniería Social. Artículo [en línea]: http://www.itnews.ec/documentos/doc_ing_social.pdf [Consulta: enero 2011].

15. La Real Academia de la Lengua Española. Diccionario [en línea]: www.rae.es Madrid: 2011. 22a ed. [Consulta: enero 2011].

16. MITNICK, Kevin; SIMÓN, William L. *El Arte de la Intrusión.* México: Alfaomega, 2007. ISBN: 978-970-15-1260-9.

17. SEOANE BALADO, Eloy. *La nueva era del comercio: El Comercio Electrónico.* España: Ideaspropias, 2005. ISBN: 978-84-934547-2-2.

18. SILVA, Arturo. *Criminología y conducta antisocial.* Escorza T., Miguel (dir. ed.); Schoenfeld, Matilde (co. ed.). México: Pax, 2003. ISBN: 968-860-638-3.

19. Superintendencia de Telecomunicaciones de Guatemala. Estadísticas: Situación de la Telefonía en Guatemala primer semestre 2010 [en línea]: www.sit.gob.gt/index.php?page=situacion-de-la-telefonia-en-guatemala [Consulta: enero 2011].

20. Symantec Corporation. Informe sobre las amenazas a la seguridad en Internet. Publicado en abril de 2010. [en línea]: http://www.symantec.com/es/mx/business/theme.jsp?themeid=threatreport [Consulta: diciembre 2011].

21. YUKOPILA, Bodizar; MÉNDEZ, Saraí. "Estudio sobre Ingeniería Social: El desconocimiento del usuario no prevenido". Revista Generación Digital. 14a ed. No. 7. vol. 2. (Octubre 2008) p. 36-39.

ANEXO

Tabla IV. **Proceso Legislativo para la aprobación de una ley o de reforma de leyes**

NO.	NOMBRE	DESCRIPCIÓN
1	Iniciativa	Documento físico integrado por la exposición de motivos, parte considerativa, fundamentación de ley y articulado, que permite la introducción de un proyecto de ley ante el Pleno del Congreso. Tienen iniciativa para presentar leyes los diputados al Congreso, el Organismo Ejecutivo, la Corte Suprema de Justicia, la USAC y Tribunal Supremo Electoral. (Artículo 174 de la Constitución Política de la República de Guatemala).
2	Pleno	Una vez ingresada a la Dirección Legislativa del Congreso, esta es numerada y puesta en agenda para conocimiento del Pleno del Congreso para que inicie su trámite, en dónde se da lectura a la exposición de motivos para luego ser remitida a la Comisión competente para conocerla, estudiarla y pronunciarse sobre el tema.

Continuación tabla IV …

3	Dictamen	Una vez conocida por la Comisión de trabajo competente, esta emitirá el dictamen correspondiente para presentar su opinión ante el pleno, la cual puede ser favorable, (con ello sigue su proceso la aprobación de la ley) o desfavorable (desecha el proyecto y lo remite al archivo).
4	Primer Debate	Discusión sobre la conveniencia o inconveniencia, constitucionalidad o inconstitucionalidad de sus normas y la oportunidad de su adopción. En esta fase aún no se vota para la aprobación de la ley.
5	Segundo Debate	Discusión sobre la conveniencia o inconveniencia, constitucionalidad o inconstitucionalidad de sus normas y la oportunidad de su adopción. En esta fase aún no se vota para la aprobación de la ley.
6	Tercer Debate	Según artículo 176 de la Constitución Política de la República de Guatemala, es hasta la 3ª. sesión o debate que se puede aprobar la iniciativa, hasta que se tenga suficientemente discutido. (constituyen excepción los casos de urgencia nacional).
7	Aprobación por artículos	Aprobado el proyecto, se inicia la discusión separada artículo por artículo del proyecto.
8	Redacción final	Posterior a la discusión y aprobación por artículos del proyecto, el Pleno aprueba la redacción final, fase en la que todavía cabe el procedimiento de revisión de algún artículo o capítulo.

Continuación tabla IV …

9	Aprobación	Finalizada la fase de redacción final, el Congreso procede a la aprobación final del mismo, se le impone un número y únicamente procede la revisión de Redacción y estilo por parte de la Junta Directiva que se constituye como Comisión de Redacción y Estilo. En un plazo no mayor de 10 días remite el proyecto aprobado al Organismo Ejecutivo para su sanción, promulgación y publicación. Artículo 177 de la Constitución Política de la República de Guatemala.
10	Publicación	El proceso de formación de la ley, por parte del Organismo Legislativo, termina con la remisión del proyecto al Organismo Ejecutivo, quien puede sancionarla y promulgarla o vetarla conforme lo establecido en los artículos 178 y 179 de la Constitución Política de la República de Guatemala.

Fuente: Diagnóstico del Marco Jurídico en Guatemala para promover la Transparencia y el combate a la Corrupción. Comisión para la Transparencia y el combate a la Corrupción, Vicepresidencia de Guatemala. Licda. María Alejandra López C. Diciembre 2010.