CAPÍTULO II

DELITOS CIBERNÉTICOS

1. DEFINICIÓN Y CLASIFICACIÓN DE LOS DELITOS CIBERNÉTICOS

1.1 Definición

Los delitos cibernéticos, delitos electrónicos o delitos informáticos (*computer crimes*), han sido definidos de distintas maneras. De acuerdo con el concepto típico, Tellez Valdés los define como "*actitudes ilícitas en que se tienen a las computadoras como instrumento o fin*". [19] El mismo autor en cita indica cuál es el concepto típico de los delitos informáticos, indicando que son: "*las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin*".

Por su parte, María de la Luz Lima al referirse a los Delitos Informáticos, que ella denomina "*Delitos Electrónicos*", indica: "*delito electrónico en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un*

19 TÉLLEZ VALDEZ, Julio, Derecho Informático, Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, México, 1987, pág. 105.

sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin."[20]

Nosotros proporcionamos como definición de delitos informáticos, la siguiente: **Acción u omisión, típica, antijurídica y culpable, que se realiza por medio de un sistema que haga uso de las tecnologías de la información o un componente de éste, o que lesione la integridad, disponibilidad o confidencialidad de la información**.

1.2 Clasificación

Molina Salgado cita una clasificación de los delitos informáticos, de la manera siguiente:

- **Como Instrumento o Medio**. En esta categoría se encuentran las conductas criminógenas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito.

- **Como fin u objetivo**. En esta categoría encuadramos a las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física.[21]

Nosotros consideramos que los delitos informáticos deben clasificarse atendiendo al "*bien jurídico*" que específicamente

20 LIMA MALVIDO, María de la Luz. Delitos Electrónicos. Academia Mexicana de Ciencias Penales, Editorial Porrúa, México, pág. 100.

21 MOLINA SALGADO, Jesús Antonio, Delitos y otros ilícitos informáticos en el Derecho de la Propiedad Industrial, Editorial Porrúa, México, 2003, pág. 19.

se trata de tutelar. En ese sentido, proporcionamos la siguiente clasificación:

1.2.1 Delitos contra la Integridad.

En esta categoría podemos encuadrar:

a) Daño informático.
b) Falsificación informática.
c) Fraude informático.[22]

1.2.2 Delitos contra la Disponibilidad.

Dentro de esta categoría podemos citar el delito de Violación a la Disponibilidad.

1.2.3 Delitos contra la Confidencialidad

a) Espionaje informático.
b) Acceso ilícito.
c) Reproducción de dispositivos de acceso.
d) Interceptación ilícita.

1.2.4 Delitos de pornografía infantil.

Todas aquellas conductas tipificadas como Pornografía Infantil, reguladas en el Código Penal o en la Ley Contra la Violencia Sexual, Explotación y Trata de personas, o en cualquier otro cuerpo normativo, siempre y cuando se realicen por medio de un sistema que utilice tecnologías de la información.

---

22 Dentro de la categoría de "***delitos contra la integridad***" encuadramos al delito de "***fraude informático***" debido a que el fraude informático implica, de una u otra manera, alteración de datos o del sistema, lo cual consideramos que afecta la integridad. Sin embargo, no tenemos ninguna objeción para encuadrar al fraude informático dentro de una categoría de delitos contra el "***patrimonio***", debido a su naturaleza de afectación patrimonial.

1.2.5 Delitos contra la Propiedad Intelectual.

Todas aquellas conductas tipificadas como violatorias a los derechos de propiedad intelectual, regulados en la Ley de Propiedad Industrial y Ley de Derechos de Autor y Derechos Conexos, o en cualquier otro cuerpo normativo, siempre y cuando se realicen por medio de un sistema que utilice tecnologías de la información.

Flores Salgado señala como elementos del tipo penal, que se deben considerar para denominar a un delito como "***delito electrónico***", los que textualmente se citan a continuación:

a. El *bien jurídico tutelado* mediante la sanción de los delitos informáticos es la pureza técnica que presupone la informática y el resguardo de los medios involucrados en la computación electrónica.

b. El *elemento objetivo* es todo atentado que signifique dañar o desviar el correcto uso de la máquina, con la finalidad de causar un perjuicio que redunde en un beneficio moral o material para sí o para otro, por el uso indebido de una computadora sin la correspondiente autorización.

c. El *elemento subjetivo* debe estar constituido por el dolo o la culpa con que actúa el sujeto activo del delito informático.

d. Con relación al *sujeto activo* de los delitos informáticos se ha observado que, por lo general, son personas de un determinado nivel de inteligencia y educación, superior al común, mismos que pueden ser los programadores que violan o utilizan controles protectores del programa o sistema; los analistas de sistemas, que generalmente

son los únicos que conocen la operación completa de ellos; los analistas de comunicaciones, que diseñan la seguridad del sistema de comunicaciones; supervisores que tienen conocimiento integral de las operaciones y debilidades del sistema de seguridad; personal técnico y de mantenimiento, que suele tener libre acceso a los centros de cómputo y conoce los sistemas operativos y bases de datos, etcétera.

e. El *sujeto pasivo* en los delitos informáticos se puede constituir por las entidades bancarias, como víctimas frecuentes por la creciente utilización de las transferencias de fondos de forma electrónica, donde se movilizan cantidades importantes de dinero mediante símbolos electrónicos, como único tipo de registro.[23] También podemos mencionar que, el sujeto pasivo, es toda víctima que sufre cualquier tipo de lesión, mediante el uso de un sistema que utilice tecnologías de la información.

2. DELITO DE ACCESO ILÍCITO

2.1 Aspectos generales del Acceso Ilícito

El delito de acceso ilícito se refiere al ingreso no autorizado a uno o varios sistemas que utilicen tecnologías de la información.

En el proyecto de ley de Cibercrimen, el acceso ilícito se encuentra regulado en el artículo 5, dentro del capítulo de los delitos contra la *confidencialidad, integridad y disponibilidad de datos y tecnologías de la información*. El artículo 5, del proyecto de ley,

23 FLORES SALGADO, Lucerito, Derecho Informático, Editorial Patria, primera edición, México, 2009, págs. 132 y 133.

establece que comete el delito de acceso ilícito, quien acceda a sistema que haga uso de tecnologías de la información, o, a sus componentes, sin autorización o excediéndola, estableciendo que el responsable será sancionado con prisión de dos a cuatro años y multa de cien a quinientas veces el salario mínimo legal vigente.

Este tipo de delito tiene relación con la "*confidencialidad*", como un atributo de la información. La conducta ilícita, de acceso ilícito, puede considerarse como una conducta ilícita principal o accesoria. Es ***principal*** si la intención del sujeto activo es simplemente la intromisión al contenido de un sistema informático, tal es el caso de aquel sujeto, que le apasiona conocer el funcionamiento interno de un sistema informático, aunque su finalidad no sea la de causar un daño. En el medio informático a este sujeto se le denomina "***hacker***" y sus actos se originan para determinar vulnerabilidades de sistemas o para burlar las medidas de seguridad.

Por razones obvias, el comúnmente denominado ***hackeo ético***, esto es, el acceso autorizado por el titular del sistema, no es materia del delito de "acceso ilícito", ya que éste se realiza por medio de un experto en seguridad informática, para detectar las vulnerabilidades de los sistemas o servidores, contribuyendo así, a mejorar las condiciones de seguridad y porque aquí sí existe autorización por parte del titular.

Es ***accesorio*** o ***preparatorio*** el acceso ilícito, cuando se accesa a un sistema informático para realizar otro tipo de acciones preparatorias de otro delito. Así, por ejemplo, para obtener una contraseña o para la instalación de interceptores de teclado, denominados comúnmente como "*keyloggers*", los cuales registran cada una de las teclas pulsadas y, por consiguiente, todas las contraseñas que se utilizan en el computador o dispositivo.

Debe tenerse presente que existen otros delitos informáticos que subsumen al delito de acceso ilícito, siempre y cuando, esos delitos, se realicen de manera conjunta con el acceso. Así tenemos la conducta de acceso y daño al sistema, en forma conjunta, que se debe tipificar como un delito de "***daño informático***"; la conducta de acceso y transferencia de activos por medio de sistemas informáticos, en forma conjunta, que se debe tipificar como un delito de "***fraude informático***"; la conducta de acceso y provocación de denegación de acceso a redes, información y sistemas, que debe sancionarse como "***violación a la disponibilidad***"; la conducta de acceso e interceptación de datos informáticos, que debe tipificarse como "***interceptación ilícita***"; o, la conducta de acceso y copia, alteración o sustitución de datos informáticos de un sistema, generando un resultado no auténtico, que debe tipificarse como el delito de "***falsificación informática***". Por estas razones, el legislador debe tener en cuenta que los delitos que entrañan acceso ilícito, tales como el daño informático, la violación de disponibilidad, la falsificación informática, el fraude informático, entre otros, deben ser sancionados, dependiendo del caso concreto, con la pena correspondiente al delito que tenga señalada mayor sanción.

Si el acceso se realiza en forma separada, debe tipificarse, únicamente, como delito de acceso ilícito. Si, posteriormente se utiliza la información del acceso ilícito para la comisión de otro delito, estaríamos ante la figura del "*concurso de delitos*"[24] y, según

24 El TITULO VI, CAPÍTULO III, del Código Penal de Guatemala, Decreto 17-73 del Congreso de la República, se refiere al CONCURSO DE DELITOS de la forma siguiente: Artículo 69.- Concurso real. Al responsable de dos o más delitos, se le impondrán todas las penas correspondientes a las infracciónes que haya cometido, a fin de que las cumpla sucesivamente, principiando por las más graves, pero el conjunto de las penas de la misma especie no podrá exceder del triple de la de mayor duración, si todas tuvieren igual duración, no podrán exceder del triple de la pena. Dice el artículo 70.- En caso de que un solo hecho constituya dos o más delitos, o cuando uno de ellos sea medio necesario de cometer el otro, únicamente se impondrá la pena correspondiente al delito que tenga señalada mayor sanción, aumentada hasta en una tercera parte.

el tipo de concurso de delitos que corresponda de conformidad con la ley penal.

2.2 Agravantes en el Delito de Acceso Ilícito

En el proyecto de ley de Cibercrimen se establece que, la pena será de tres a seis años de prisión y multa de doscientas a setecientas veces el salario mínimo legal vigente, en los siguientes casos:

2.2.1 Cuando, para acceder al sistema se suplante la identidad del destinatario o del remitente.

Como ejemplo de esta agravante podemos citar las diferentes técnicas para obtener el dato de usuario y clave de acceso (*password*) de la víctima, a través de:

a) *Ingeniería social*, obteniendo la identidad y *password* de un usuario válido por medio argucias o engañando al usuario.

b) La captura de la contraseña y usuario, usando un *keylogger* instalado en la máquina.

c) *Phishing*, haciendo creer al usuario que accesa a una página válida y éste ingresa su usuario y *password.*

d) Un *troyano*[25], que captura el usuario y las claves de acceso de la máquina de la víctima para, posteriormente, retransmitirla al ciberdelincuente.

25 Un *troyano* o *caballo de Troya* consiste en un programa o software malicioso que, al momento en el cual el usuario decide ejecutarlo, le ocasiona daños al sistema. El término "*troyano*" (del inglés "*trojan horse*") proviene de la historia del Caballo de Troya mencionado en la obra la Odisea de Homero.

e) Interceptar las transmisiones de una red, capturando el tráfico de la misma y filtrando el usuario y *password.*

2.2.2 El hecho de utilizar programa, equipo, material o dispositivo para obtener acceso a sistema que utilice tecnologías de la información o cualquiera de sus componentes, para ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de dichos servicios. Con relación a esta agravante citamos los ejemplos siguientes:

a. Cuando el ciberdelincuente intercepta la señal de una red inalámbrica desprotegida, proveyendo acceso a Internet a otros usuarios que, con conocimiento o sin él, hacen uso de este servicio.

b. Al desarrollar herramientas de *software*, que le permiten romper la clave de protección de video juegos, juegos en línea o *software* de oficinas o aplicativos, vendiendo copias del programa a terceros.

c. Por medio de la captura de la contraseña y usuario, usando un *keylogger* instalado en la máquina de la víctima.

2.2.3 Cuando el acceso se realice al generar, copiar, grabar, capturar, utilizar, alterar, divulgar, traficar, desencriptar, descodificar o de cualquier modo descifrar los códigos de acceso, información o mecanismos similares o falsificando cualquier tipo de dispositivo de acceso al mismo. Citamos

los siguientes ejemplos:

a. Por ataques de los denominados de "*fuerza bruta*", rompiendo las claves de acceso.

b. Por medio de la replicación de *tokens* o dispositivos de acceso.

c. Por medio de *packet sniffers*[26], que les permitan acceder a paquetes válidos en la red y posteriormente grabarlos, copiarlos, alterarlos o desencriptarlos.

d. Nuevamente se puede utilizar el *phishing* para copiar las claves de acceso.

e. Infección de la máquina por medio de un *troyano*.

2.2.4 El hecho de utilizar programa, equipo, material o dispositivo para obtener acceso a equipos o sistemas que utilicen tecnologías de la información o cualquiera de sus componentes, haciendo uso no autorizado del mismo, para procesar o realizar cualquier tipo de acción no autorizada por el propietario o legítimo usuario. Esta agravante puede tener lugar cuando se utilice *malware* como los llamados troyanos, pudiéndose mencionar aplicativos prediseñados como el famoso ZEUS, que permite convertir a la computadora de la víctima en un *bot*, que formará parte del *malware* denominado *botnet*, el cual es utilizado por el atacante para lanzar ataques de

26 Los ***packet sniffers*** tienen diversos usos como monitorear redes para detectar y analizar fallos o ingeniería inversa de protocolos de red. También es habitual su uso para fines maliciosos como: robar contraseñas, interceptar mensajes de correo electrónico, espiar conversaciones de *chat*.

denegación de servicio, robo de usuarios y contraseñas, envió de *spam*, entre otras actividades ilícitas.

2.3 Derecho comparado en materia de Acceso Ilícito

El delito de "*acceso ilícito*", también llamado "*acceso indebido*" o "*acceso sin autorización*", se encuentra regulado en distintas legislaciones de la forma siguiente:

ACCESO ILÍCITO

Consejo Europeo	Convenio Budapest o Convención de Ciberdelincuencia	Artículo 2. Acceso Ilícito. Acto deliberado e ilegítimo a todo o parte de un sistema informático.
Estados Unidos de América	Cada Estado cuenta con legislación específica. Se cita como ejemplo el cuerpo normativo de *Michigan Compiled Laws Section* 752.794	Regula el acceso ilícito (*access to computers*) ligado al tema del fraude informático, es decir, el acceso indebido es sancionado cuando tenga como finalidad una apropiación indebida.

Argentina	Ley 26.388 que contiene reformas al Código Penal de Argentina. 04 de junio del 2008.	ARTICULO 5º — Incorpórese como artículo 153 bis del Código Penal, el siguiente: Artículo 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.
Venezuela	Ley Especial Contra los Delitos Informáticos. 04 de septiembre 2001.	Artículo 6. **Acceso indebido**. El que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.
Chile	Ley Relativa a Delitos Informáticos No. 19223. 28 de mayo de 1993.	Artículo 2. El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o **acceda** a él, será castigado con presidio menor en su grado mínimo a medio.
México	Código Penal, artículo 211 *bis* 2	Sanciona el **acceso ilícito** a sistemas y equipos de informática.

Colombia	Ley No. 1273-2009, que contiene reforma del Código Penal de Colombia. 05 de enero del 2009.	*Artículo 269A:* ***ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO****. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*
Francia	Ley No. 88-19	En el artículo 462-2, se sanciona tanto el **acceso** al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.
Alemania	Ley contra la Criminalidad Económica	Sanciona el espionaje de datos o información.

República Dominicana	Ley No. 53-07, contra Crímenes y Delitos de Alta Tecnología. 23 de abril del 2007.	Artículo 6. El hecho de **acceder** a un sistema electrónico, informático, telemático o de telecomunicaciones, o a sus componentes, utilizando o no una identidad ajena, o excediendo una autorización, se sancionará con las penas de tres meses a un año de prisión y multa desde una vez a doscientas veces el salario mínimo.
España	Código Penal de España	Artículo 197. El que para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses. 2.- Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

Una de las finalidades del Derecho Comparado consiste en establecer e inferir similitudes y diferencias, a partir de la comparación y análisis de figuras jurídicas, para poder crear uniformidad a nivel internacional. En el caso de los delitos cibernéticos es imprescindible esa comparación y análisis debido a que, tal como se ha indicado, una de las características de este tipo de delitos consiste en su naturaleza *transfronteriza*, lo cual obliga a los Estados a apoyarse mutuamente en cuanto a cuerpos normativos, entes de prevención y defensa de ataques informáticos, tribunales especializados y entes de investigación con asistencia jurídica mutua.

En la tabla comparativa, de las normas que regulan el delito de acceso ilícito, podemos encontrar algunas diferencias, en lo que respecta a la regulación utilizada en el Proyecto de Ley de Cibercrimen de Guatemala. Las diferencias se concentran, básicamente, en las situaciones agravantes de la pena, las cuales, nuestro Proyecto de Ley sí contempla, y obedece a que debe regularse una sanción más drástica para este tipo de conductas.

En la Ley de Delitos Informáticos o Cibercrimen de República Dominicana, el legislador dispuso subdividir el delito de "acceso ilícito" en la forma siguiente:

- **Códigos de Acceso**. En la Ley de República Dominicana y con relación al delito de "códigos de acceso", se sanciona el hecho de divulgar, generar, copiar, grabar, capturar, utilizar, alterar, traficar, descencriptar, descodificar o de cualquier modo descifrar los códigos de acceso, información o mecanismos similares, a través de los cuales se logra el acceso ilícito a un sistema que utiliza tecnologías de la información.

- **Clonación de dispositivos de acceso**. Se refiere a la clonación o copia de un dispositivo de acceso de un sistema informático.

- **Acceso ilícito para servicios a terceros**. El hecho de utilizar un programa, equipo, material o dispositivo para obtener acceso a un sistema electrónico, informático, telemático o de telecomunicaciones, o a cualquiera de sus componentes, para ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos.

La Comisión de trabajo, que participó en la elaboración del Proyecto de Ley de Cibercrimen, consideró, por técnica legislativa y para evitar un complejo análisis y determinación de actos específicos que entrañan un acceso ilícito, unificar las variables o subdivisiones del acceso en un solo artículo, esto es, en el artículo 5 del Proyecto, y establecer situaciones agravantes como las antes indicadas. El criterio tomado por el equipo de trabajo se basó, fundamentalmente, en que las subdivisiones de acceso ilícito indicadas, siempre implicarán la intrusión a un sistema o sus componentes y, por ello, debía sancionarse como acceso ilícito.

2.4 Acceso Ilícito y Violación de Correspondencia

Debido a la conducta de intrusión a un sistema, que implica el acceso ilícito, es posible que se pueda pensar, equivocadamente, que existe sinonimia entre el delito de *violación de correspondencia* con el *acceso ilícito*, ya que éste último implica el conocimiento de la información contenida dentro del sistema informático accesado.

El delito de violación de correspondencia se encuentra regulado en el artículo 217 del Código Penal, Decreto 17-73 del Congreso de la República, que establece: "*Artículo 217.- **Violación de correspondencia y papeles privados**. Quien, de propósito o para descubrir los secretos de otro, abriere correspondencia, pliego cerrado o despachos telegráficos, telefónicos o de otra naturaleza, que no le estén dirigidos o quien, sin abrirlos, se impusiere de su contenido será sancionado con multa de quinientos a cinco mil quetzales.*"

Si tratamos de buscar una figura delictiva similar al acceso ilícito, que sea aplicable para cuestiones físicas, indudablemente pensaríamos en el delito de ***ALLANAMIENTO***, ya que implica el ingreso a una morada ajena. Pensemos que una persona ingresa a un inmueble que constituye la residencia de otra persona. Estando adentro, encuentra correspondencia consistente en cartas o despachos y decide abrirlos y conocer su contenido. La conducta de esta persona se podría encuadrar en las figuras delictivas de: (a) ***ALLANAMIENTO***, delito regulado en el artículo 206 del Código Penal de Guatemala, por haber ingresado al inmueble, y, (b) ***VIOLACIÓN DE CORRESPONDENCIA***, regulado en el artículo 217 del Código Penal de Guatemala, por haber abierto y conocido el contenido de los documentos privados. De igual manera sucede con el acceso ilícito, ya que el sujeto accesa al sistema y, una vez adentro, puede tener a su disposición archivos o datos que constituyan correspondencia. Si el sujeto activo o *hacker* decide abrir o conocer la correspondencia contenida en el sistema informático, entonces incurriría en los delitos de ***ACCESO ILÍCITO*** y ***VIOLACIÓN DE CORRESPONDENCIA***.

El delito de espionaje informático, también puede generar confusión con el delito de violación de correspondencia. Su punto

de distinción radica en que, el espionaje informático implica el apoderamiento, obtención, revelación, transmisión o difusión del contenido, parcial o total, de un sistema que utilice tecnologías de la información. El objeto del espionaje informático es el sistema informático o sus componentes, no la información que entrañe correspondencia, aunque sí podría ser información sensible o confidencial. Si el espía informático se apodera, adicionalmente, de correspondencia, su conducta deberá encuadrarse en los delitos de ***ESPIONAJE INFORMÁTICO*** y ***VIOLACIÓN DE CORRESPONDENCIA***.

2.5 Tipos de Ataques al Sistema

Existen diferentes tipos de intrusión o ataques al sistema que utiliza tecnologías de la información, los cuales deben conocerse para poderlos encuadrar dentro del delito de acceso ilícito. Esto no significa que únicamente los accesos que se desarrollarán a continuación impliquen acceso al sistema, ya que debe entenderse que: todo acceso a un sistema que utilice tecnologías de la información, sin autorización, implica acceso ilícito. Además, en materia de Cibercrimen los delincuentes innovan constantemente las formas o tipos de ataques cibernéticos. A continuación se citan algunos tipos o mecanismos de intrusión o acceso a sistemas:

2.5.1 Ingeniería social

Cuando se piensa en un ataque al sistema, se considera que éste será dirigido a los componentes tecnológicos de los sistemas y el esfuerzo se concentra en proteger a dichos componentes. Sin embargo, las personas, como usuarios de dichos sistemas, constituyen una parte de los sistemas de información, al igual que los componentes tecnológicos. Los usuarios tienen sus propias

vulnerabilidades y, pueden constituir la primera parte del sistema en sucumbir a ciertos tipos de ataques.

La ingeniería social es un tipo de ataque que emplea el *engaño* o *artificio,* para convencer a un usuario a que proporcione datos sensibles o viole pautas de seguridad. En ese sentido, la ingeniería social se traduce en un mecanismo que utiliza el delincuente para accesar a sistemas informáticos.

La ingeniería social se considera uno de los pasos más importantes en el proceso de intrusión de un sistema, ya que permite al o los atacantes, obtener información valiosa que permitirá realizar cualquier otra acción dentro del sistema. Es por ello que se le considera la precursora de otros tipos de ataques a sistemas. Estos ataques dependen del factor humano, al igual que en la tecnología, los síntomas pueden ser vagos y difíciles de identificar. Estos pueden provenir de una persona, vía correo electrónico o por teléfono.

La ingeniería social, generalmente toma ventaja de usuarios que carecen de conocimiento técnico, pero también puede ser a la inversa, si el atacante finge ser un usuario que necesita ayuda.

El *phishing* es un tipo extremadamente común de ingeniería social. A través de un ataque de *phishing*, el sujeto atacante envía un correo electrónico, haciéndose pasar por una institución reconocida, ya sea ésta financiera, bancaria, de beneficencia o cualquier otra institución que tenga, como característica, la interacción de los clientes y la facultad correspondiente para el movimiento de fondos. Lo más común, de estos correos, es que solicitan del recipiendario el dato de usuario y clave de acceso, número de cuenta, número de cédula o documento de identidad personal, fecha de nacimiento o cualquier otro dato confidencial, que ayude al ciberdelincuente en la consecución de sus fines: "*verificar si la cuenta es legítima*".

Valiéndose de la argucia consistente en que por motivos de seguridad se requiere verificar su cuenta, el delincuente logra convencer a la víctima y ésta remite el correo electrónico con los datos que se le requirieron; con esta información, el ciberdelincuente puede llevar a cabo el hurto o apropiación de valores o de identidad.

Ejemplos:

a. Un empleado de la Sección de Sistemas, de una entidad que brinda servicio de consultas a una base de datos, que almacena información sobre leyes y reglamentos, recibe una llamada por parte de un "usuario", quien le indica que está tratando de ingresar a la base de datos, pero, desafortunadamente, no se recuerda de su usuario y clave. El empleado de soporte le pregunta su nombre y el sujeto le indica un nombre de un usuario válido, y así, el empleado, para apoyarlo, le indica cuál es su usuario y le reinicia la clave de acceso.

b. Un ejecutivo de una firma de *marketing* recibe un correo electrónico, en el cual le remiten un vídeo sobre los mejores goles del mundial. El ejecutivo, quien es muy aficionado a este deporte, prontamente pulsa sobre el archivo ejecutable y espera que se despliegue el vídeo. Al cabo de un tiempo no sucede nada y el ejecutivo concluye que no sirvió el archivo que recibió y decide revisar el consolidado financiero de la empresa, abre el explorador, teclea la dirección de su banco *www.mibanco.com.gt* y le despliega una página del banco donde le solicita su usuario y clave, él la ingresa y, seguido de ello, se cierra el explorador. Esto le parece extraño y vuelve a intentarlo,

vuelve a ingresar su usuario y su clave y el explorador le despliega el mensaje que su clave es invalida, vuelve a intentarlo y sucede lo mismo. Muy enojado llama a su banco y expone su problema. El personal de soporte técnico le indica que él recién ingresó al sistema y que cambió la clave; él indica que en ningún momento ha efectuado ningún cambio; el empleado le contesta que sí y que su cuenta presenta una serie de transferencias electrónicas o retiros que exceden los CIEN MIL QUETZALES (Q.100,000.00).

c. En el medio guatemalteco circuló un correo electrónico donde se le indicaba al remitente que hiciera *click* sobre determinado enlace para saber quién lo había borrado de sus amigos en *Hotmail* o *MSN*; esta página requería el dato de usuario y clave para ingresar a la cuenta de correo. La página estaba destinada a apoderarse del dato del nombre y contraseña de los usuarios. Esta técnica consiste en pedirle al usuario final su usuario o correo electrónico y luego la contraseña; estos datos son enviados luego a la base de datos del autor de la página, almacenando la información y posteriormente poder ingresar a estos correos. Una vez que el atacante tiene acceso a los correos electrónicos de la víctima, puede localizar todos aquellos mensajes provenientes de entidades bancarias, que podrían contener información sobre contraseñas y usuarios, así como estados de cuenta, direcciones físicas, datos de identidad, etcétera.

2.5.2 Ataques por software

El ataque por software toma como objetivos: un sistema operativo, una aplicación o protocolo[27]. La meta de este ataque por *software* es interrumpir o deshabilitar el software que está corriendo en la computadora de la institución, ente u organización o para explotar, en alguna medida, el haber obtenido acceso a un simple sistema o a una red. Este puede ser usado solo o en combinación con otro tipo de ataque, como la ingeniería social.

Este tipo de ataque tiene una variedad de formas, usa software para monitorear la actividad de la red para, de esta forma, capturar y descodificar las comunicaciones que sobre ésta sucedan. Estos paquetes de información, regularmente contienen información para la autorización de acceso, nombres y claves de acceso, la cual podrá ser utilizada más tarde para acceder a recursos con acceso restringido.

2.5.3 Ataques por scaneo de puertos

Es un tipo de ataque por *software,* por medio del cual un atacante potencial escanea las computadoras y dispositivos que están conectados a Internet u otra red, para observar qué puertos TCP[28] o UDP[29] están escuchando y qué servicios del sistema están

27 Security+: A *CompTIA Certification*, edition 1.0.

28 *Transmission Control Protocol* - Protocolo de Control de Transmisión. Se trata del protocolo más usado de Internet. Un protocolo de red es una especificación detallada de las "reglas" que deben seguir los diferentes programas que emplean una red de comunicaciones, para intercambiar información.

29 *User Datagram Protocol* - Protocolo de Datagrama de Usuario. Protocolo abierto, no orientado a la conexión (como el TCP) y por lo que no establece un diálogo previo entre las dos partes, ni tampoco mecanismos de detección de errores.

activos. Este es el primer paso que da un atacante: "conocer las vulnerabilidades del sistema".

Actualmente, existe software que detecta si el sistema está siendo objeto de un escaneo de puertos. Entre las herramientas que utilizan los atacantes tenemos los siguientes: *Nmap, SuperScan, Strobe, Nessus*, entre otras.

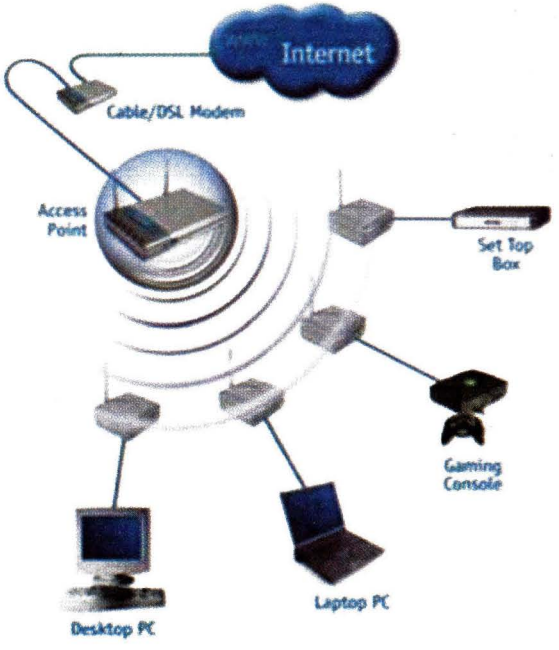
A continuación citamos un cuadro que contiene los comandos pertinentes, usados con la herramienta *Nmap*, para determinar cuáles son los puertos abiertos en el sistema. Veamos:

```
C:\nmap\nmap -sS -V 200.4?.65.15?
Starting Nmap 4.10 < http://www.pocofiable.org/nmp > AT 2012-01-01 03:02 Hora este del Pacifico
DNS resolution of 1 IPs Took 2.53s.
Initiating SYN Stealth Scan against cable-baq-co- 108.203.98.solidet.com.gt < 200.4?.65.15?> [1679 ports] at 03:02
Discovered open port 80/tcp on 200.4?.65.15?
Discovered open port 1110/tcp on 200.4?.65.15?
Discovered open port 3306/tcp on 200.4?.65.15?
The SYN Stealth Scan took 21.88s to scan 1679 total ports.
Host cable-baq-co-108.203.98.solidet.com.gt <200.4?.65.15?> appears to be up ... good.
Interesting ports on cable-baq-co-108.203.98.solidet.com.gt <200.4?.65.15?>:
Not shown: 1662 closed ports
PORT     STATE    SERVICE
69/tcp   filtered tftp
80/tcp   open     http
113/tcp  filtered auth
135/tcp  filtered msrpc
136/tcp  filtered profile
137/tcp  filtered netbios-ns
138/tcp  filtered netbios-dgm
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
593/tcp  filtered http-rpc-epmap
1001/tcp filtered unknown
1025/tcp filtered NFS-or-IIS
1110/tcp open     nfsd-status
1214/tcp filtered fasttrack
1433/tcp filtered ms-sql-s
1444/tcp filtered mar cam-lm
3306/tcp open     mysql
Nmap finished: 1 IP address <1 host up> scanned in 23.235 seconds
                Raw packets sent: 1846 <81.204KB> | Rcvd: 1745 <69.812KB>|
```

2.5.4 Ataque por escucha

También conocido como *sniffing attack,* usa software especial de monitoreo para obtener acceso a redes privadas. Estas escuchas son regularmente efectuadas sobre redes inalámbricas (*wireless*), que están pobremente protegidas o que funcionan con la configuración por defecto. Para obtener acceso el atacante debe estar dentro del rango de propagación o de alcance de la señal inalámbrica. Este tipo de ataque es difícil de detectar.

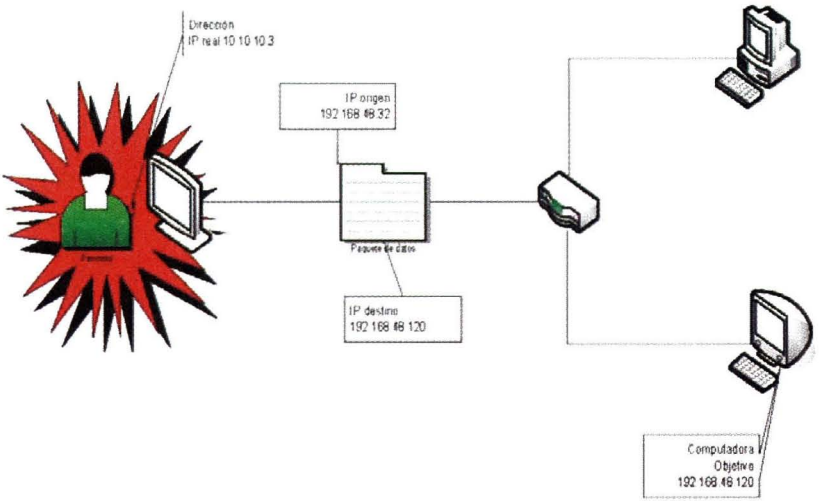
El software más conocido para este tipo de escucha es el *Dsniff, Ethereal y el WinPcap.*



2.5.5 Ataques por IP Spoofing

Este tipo de ataque sucede cuando el atacante crea un paquete IP con una dirección IP creada y usa este paquete para obtener acceso a un sistema remoto.

Ejemplo:



La gráfica representa a un atacante con una dirección 10.10.10.3, el cual no tiene acceso al *host* destino 192.168.48.120, la aplicación que autentica el acceso, únicamente lo hace para tres octetos la red 192.168.48.x, facilitando al atacante la creación de un paquete IP, especialmente creado, que en este caso es la 192.168.48. 32.

Como el *router* del borde de red, no está configurado para rechazar paquetes IP que contengan direcciones IP internas, el *router* tomará como válido el paquete y lo remitirá a la máquina objetivo, concediendo el acceso al sistema al atacante.

2.5.6 Ataque por Secuestro de Red (*Hijacking*)

Es un ataque de software, donde el atacante toma el control de una sesión de red TCP, después que la sesión es autenticada, obtiene el acceso a los datos o a los recursos de red usando una identidad legítima de un usuario de la red. Este tipo de ataque proporciona la apariencia de que el sistema o conexión se perdió y, el administrador, posiblemente nunca sepa que fue objeto de un ataque.

Este método explota principalmente el mecanismo de control de sesión web, que normalmente es administrado por un *token*. Debido a que el protocolo *http*, utiliza muchas conexiones TCP, el servidor web necesita reconocer cada una de las conexiones realizadas por los usuarios. El método, comúnmente utilizado, consiste en aquel en el cual un Servidor Web envía al *browser* o navegador un *token* después de ser autenticado.

Un *token* se compone, normalmente, de una serie de ancho variable, pudiendo ser empleado de diferentes maneras, como por ejemplo: en la *URL –uniform resource locator-*, en la cabecera de una *cookie*.

En este tipo de ataque, la sesión es comprometida por el robo del *token* o por la predicción de la composición del *token* y, de esta manera, obtener acceso no autorizado.

¿Por qué podría verse comprometida la señal?

1. Porque los *token* de control de acceso son predecibles.
2. La sesión está siendo escuchada o es objeto de un *sniffing*.

3. Ataques del lado del cliente, XSS, Código *JavaScript* especialmente diseñado, troyanos y otro *malware* que persiga los mismos fines.
4. *Man-in-the-middle.*
5. *Man-in-the-browser.*

2.5.7 Ataque por replicación

En este tipo de ataque, el atacante captura el tráfico de red y almacena ésta para posteriormente retransmitirla, y así, obtener acceso a una computadora específica o red[30].

Este ataque es particularmente exitoso, cuando el atacante captura paquetes que contienen usuarios, *passwords* u otros datos de autenticación. En la mayoría de los casos, un ataque de este tipo nunca es descubierto.

2.5.8 Ataque de hombre en medio (*Man in the middle*)

El atacante se inserta entre dos computadoras, usuario – servidor, servidor – servidor, para obtener acceso a sus transmisiones de datos. El atacante captura y lee cada paquete, responde a estos, y reenvía éste al anfitrión previsto; ambos, el remitente como el destinatario, creen que ellos se están comunicando directamente con el otro.

Este tipo de ataque le permite al atacante manipular la comunicación, y puede ser utilizado para posteriores accesos.

---

30 Ob. Cit.

2.5.9 Ataque de denegación de servicio (*Denial of service*)

Es un tipo de ataque por software, en el cual un atacante trata de desactivar el sistema que provee el servicio de red, realizando lo siguiente:[31]

- Conectándose a una red con un flujo grande de datos, que consume todo el ancho de banda disponible.
- Enviando datos diseñados para explotar fallos conocidos de las aplicaciones.
- Enviando múltiples solicitudes de servicio, que consumen los recursos de los sistemas.

Este ataque es usualmente dirigido hacia los servidores y *routers*, previniendo que estos respondan a solicitudes legítimas de la red.

2.5.10 Ataque por Denegación de Servicio Distribuido

Es un tipo de ataque de denegación de servicio extendido, que usa un gran número de sistemas y redes distribuidas y que lanzan, de manera simultánea, peticiones para múltiples recursos.

El atacante puede haber realizado previamente lo siguiente:

Haber comprometido previamente decenas, cientos o miles de sistemas, que generen una gran cantidad de tráfico de red hacia el objetivo seleccionado.

31 Idem.

Usar tecnología, para manipular y redireccionar una gran cantidad de tráfico de red hacia el objetivo u objetivos seleccionados.

También lo puede hacer por medio del *hacktivismo*, donde uno de los grupos más populares actualmente es *anonymous*, que coordinan una gran cantidad de personas para direccionar tráfico de red hacia los objetivos seleccionados.

Aprovecharse de que el sistema objetivo tiene la configuración por defecto del sistema, los errores o *bugs* de los programas instalados, o introducir software no autorizado, que transforma a la computadora en un *Zombie* o *Drone* que dirige las computadoras que lanzan el ataque.

Existen diversos tipos de ataques de este tipo, que varían en complejidad y sofisticación, y mencionamos los siguientes:

2.5.10.1 Ataque Smurf

Este tipo de ataque relaciona a tres partes: (1) El atacante, (2) La red intermediaria y, (3) La víctima.

El atacante envía una solicitud tipo general o *broadcast* usando el comando *ping* para hacer la solicitud a la red intermediaria (generalmente, es una red con docenas de estaciones, que el atacante conoce que responderá la petición realizada por el comando *ping*)[32]. Pero el atacante modifica la solicitud del comando *ping*, alterando la dirección IP[33] y colocando la dirección IP de la víctima, recibiendo ésta todas las respuestas.

32 Ob. cit.

33 Internet Protocol: este es el protocolo de comunicación, que permite identificar las computadoras dentro de una red local o dentro de la Internet, regularmente en la versión IPV4 está conformada por cuatro octetos, que van de 1 a 254 bits.

Como la solicitud fue hecha usando el método de comunicación del tipo *broadcast*, que se caracteriza por no discriminar sobre la estación a la cual va dirigido el mensaje, sino llega a todas las estaciones de la red, de esta misma manera son enviadas las respuestas por todas la estaciones de la red, estas respuestas irán dirigidas a la IP de la víctima; esta gran carga de respuestas hace que se caiga el servidor, servicios o el sistema de la víctima.

2.5.10.2 Buffer Overflow

Este ataque toma ventaja de aplicaciones o sistemas operativos con limitaciones de espacio en el *buffer*[34], para ello, el atacante envía datos muy largos, que hacen un uso intensivo del *buffer*.

Cuando el sistema operativo trata de procesar este dato, el sistema se cae; un ejemplo de éste es el llamado *Ping de la muerte* (antiguamente usado), donde el atacante envía una solicitud de servicio usando el comando *Ping* sobredimensionado, éste no es soportado por el computador y sufre un *buffer overflow* o una sobrecarga en el *buffer*.

Es importante destacar que para realizar un ataque cibernético no es indispensable tener altos conocimientos en informática. Es de conocimiento en la comunidad cibernauta que existen tiendas o sitios en Internet a través de los cuales se promueve la venta de herramientas o programas para realizar delitos cibernéticos. Como ejemplo de estos sitios citamos el sitio www.darkmarket.ws a través del cual se ofrecen programas de ataques DoS o DDoS, y donde también se pueden alquilar *botnets* (zombi) y proxys (ocultadores de IP, también conocidos como anonimizadores).

34 Espacio lógico donde se colocan, por espacio temporal, cierta cantidad limitada de datos, para que el computador pueda realizar otras operaciones o pagineos.

3. DELITO DE DAÑO INFORMÁTICO

3.1 Aspectos generales del daño

El delito de daño ha sido definido, en la doctrina penal, como cualquier deterioro o detrimento doloso de bienes; como la antisocial actitud que se revela con la destrucción total o parcial de las cosas, por el perjuicio patrimonial que para el propietario y poseedores significa y por el atentado colectivo que representa toda disminución de medios de riqueza inmediata o potencial.

Vemos que el hecho punible tiene aparejada la característica de "***dolo***", en forma congruente con la regulación del daño a que se refiere el artículo 278 del Código Penal, Decreto 17-73 del Congreso de la República, que dispone: "*Quien, **de propósito**, destruyere, inutilizare, hiciere desaparecer o de cualquier modo deteriorare, parcial o totalmente, un bien de ajena pertenencia, será sancionado con prisión de seis meses a dos años y multa de mil a diez mil quetzales.*"

El daño, en sentido amplio, puede surgir como consecuencia del "**dolo**", de la "**culpa**" o del "**riesgo**" asumido por una persona que causa daño a otra.

Todo daño apareja responsabilidad civil, ya que la víctima tiene derecho a solicitar la reparación del daño, basado en el postulado del derecho ***neminem leadere*** (no perjudicar a otro injustamente).

En el ordenamiento jurídico guatemalteco, y con relación a la responsabilidad civil derivada del daño, encontramos la norma contenida en el artículo 1645 del Código Civil, Decreto 106, que dispone: "*Toda persona que cause daño o perjuicio a otra, sea*

***intencionalmente**, sea por **descuido** o **imprudencia**, está obligada a repararlo, salvo que demuestre que el daño o perjuicio se produjo por culpa o negligencia inexcusable de la víctima.*"

El daño patrimonial está definido en el artículo 1,434 del Código Civil, Decreto 106, así: "*Los daños, que consisten en las pérdidas que el acreedor sufre en su patrimonio, y los perjuicios, que son las ganancias lícitas que deja de percibir, deben ser consecuencia inmediata y directa de la contravención, ya sea que se hayan causado o que necesariamente deban causarse.*"

Como se puede apreciar, la distinción del daño civil con el delito de daño, según nuestro Código Penal y Código Civil, estriba en el **dolo**, es decir, la intención de causar daño. De manera que todo acto humano, **deliberado**, que cause daño, deberá tipificarse como el ***delito de daño***; teniendo la víctima el legítimo derecho de iniciar, de conformidad con la ley, la persecución penal para lograr la condena del delincuente y, al mismo tiempo y dentro del mismo proceso penal o en otro juicio de naturaleza civil, a su elección, accionar la pretensión de la reparación civil como consecuencia del deterioro o detrimento en su patrimonio y, así, lograr la condena del demandado, al pago de "***daños y perjuicios***".

El autor Alberto Enrique Nava Garcés, al hablar del daño o sabotaje informático, indica que es el acto de borrar, suprimir o modificar, sin autorización, funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.[35]

El ***daño informático*** se concibe como la conducta encaminada a **alterar**, **destruir**, **inutilizar**, **suprimir**, **modificar** o de cualquier

35 Nava Garcés, Alberto E. ***La Prueba Electrónica en Materia Penal***, editorial Porrúa, México, 2011, pág. 41.

modo o por cualquier medio, **dañar un sistema** que utilice tecnologías de la información o un componente de éste.

Según el Proyecto de Ley de Delitos Informáticos o Cibercrimen, el delito de daño informático se debe sancionar con prisión de cuatro a ocho años y multa de cien a quinientas veces el salario mínimo legal vigente.[36]

A nuestro criterio, la definición proporcionada en el Proyecto de Ley de Delitos Informáticos, que actualmente se encuentra en discusión en el Congreso de la República de Guatemala, contiene una definición más precisa del delito de daño informático, toda vez que se refiere al daño o alteración de un sistema que utilice tecnologías de la información o un componente de éste.

En congruencia con lo aquí expuesto, debe tenerse presente que el daño informático debe ser un **acto deliberado** o **doloso**. La víctima del daño informático tiene el derecho, además, de exigir la aplicación de la pena en contra del delincuente, a ser resarcida por las pérdidas patrimoniales y por las ganancias lícitas dejadas de percibir, como consecuencia del daño sufrido en sus bienes (sistema informático).

3.2 Daño Informático

Cuando se habla de daño informático se está haciendo referencia a la alteración negativa de la "integridad", "disponibilidad"

36 El daño informático está regulado en el artículo 6 del Proyecto de Ley de Cibercrimen, de la forma siguiente: "*Quien ilegítimamente 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 será sancionado con prisión de cuatro a ocho años y multa de cien a quinientas veces el salario mínimo legal vigente.*"

y "confidencialidad" de cualquier ***activo digital*** (redes, sistemas computacionales, computadoras, programas de computadoras, datas computacionales, el contenido de los datos y el tráfico de los datos).

Un acto de *terrorismo cibernético* dirigido a la infraestructura crítica informática[37], se puede considerar el acto más paradigmático de un daño informático, puesto que, lo que se busca es la inutilización, por cualquier medio, de los activos informáticos.

El daño informático se definió en el artículo 6 de la Iniciativa de Ley de Delitos Informáticos, de la forma siguiente:

> "***Artículo 6. Daño informático.*** *Comete el delito de 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, será sancionado con prisión de cuatro a ocho años y multa de cien a quinientas veces el salario mínimo legal vigente.*" (El énfasis es nuestro).

3.2.1 Verbos rectores del daño informático

Para una mejor comprensión de la norma citada, consideramos necesario ilustrar cada uno de los verbos rectores utilizados en la figura del "daño informático". Veamos los ejemplos siguientes:

37 **Infraestructura crítica informática**: Son los activos, sistemas, redes, físicas o virtuales, que son vitales para la sobrevivencia del Estado. Que su incapacidad o destrucción podría tener un efecto debilitante en la seguridad de la nación, seguridad económica, salud pública, seguridad financiera, servicios públicos, agua, luz, telefonía, o en una combinación de ellos.

3.2.1.1 **Alterar. Estamos ante una alteración de un sistema que utiliza tecnologías de la información o un componente de éste, cuando existe un cambio, modificación o ajuste, no autorizado, de un activo digital. Ejemplo:**

Solicitud HTTP de tráfico ilícito (HTTP Request Smuggling)

Una solicitud HTTP de tráfico ilícito consiste en enviar un formato especial de solicitud HTTP, que será analizado de manera diferente por el sistema que realiza la solicitud y por el sistema final; por lo que el atacante podría pasar de contrabando una solicitud a un sistema, sin que el otro sistema sea consciente de ello. Este ataque permite explotar otros ataques, como envenenamiento de caché, secuestros de sesión, *Cross-site Scripting* (XSS) y lo más importante, la capacidad de pasar por alto la protección de *firewall* de aplicaciones *web*.

Básicamente, el ataque consiste en la presentación de una solicitud HTTP que encapsula una segunda petición HTTP en la misma cabecera (http://www.owasp.org/Segal, Ory, 2009).

```
GET /some_page.jsp?param1=value1&param2=
Content-Type: application/x-www-form-
Content-Length: 0
Foobar: GET /mypage.jsp HTTP/1.0
Cookie: my_id=1234567
Authorization: Basic ugwerwguwygruwy
```

Debe tenerse en cuenta que, cuando existe una actividad de "***phishing***" se produce una alteración del sistema informático, lo cual debe tipificarse como daño informático. La actividad de "*phishing*", generalmente, constituye un acto preparatorio para la consumación de otro delito, como el caso del Fraude Informático.

3.2.1.2 **Destruir. Se refiere a la modificación de un sistema que utiliza tecnologías de la información, lo cual provoca su inutilización o la eliminación permanente de un activo digital.**

Dentro del esquema de seguridad, la protección de los activos informáticos que se protegen son: *Hardware*, *software* y la *información*.

La acción que realiza el atacante –delincuente-, puede ir direccionada a cualquiera de los activos informáticos relacionados. La destrucción del *hardware* puede ser posible por un inadecuado nivel de seguridad en el acceso a éstos, permitiendo que éstos puedan ser accedidos por el atacante.

En cuanto al *software*, esto puede ser posible por un *virus*, que provoca la inutilización del programa, destruyendo los registros y archivos ejecutables, que pueden provocar, en algunos casos, la inutilización de un dispositivo de forma definitiva.

En cuanto a la información, de igual manera, los virus pueden ser una herramienta muy útil para destruir la integridad de la información, agregando información o haciendo inaccesible el registro, la base de datos o el archivo que la contiene.

Pero, en un sentido más amplio, un ataque de *phishing*, si bien no implica la destrucción del activo informático, sí puede llegar a destruir la imagen de una entidad bancaria o de sitios de comercio electrónico, destruyendo parcial o totalmente los medios de producción y de vida de un cliente y su calificación crediticia.

3.2.1.3 **Inutilizar, suprimir o modificar.** Se refiere a la alteración de un activo informático que provoca, que el propietario del mismo, no pueda utilizarlo de la manera como está previsto. El hecho delictivo informático, que puede conjugar estas tres acciones, es un *virus informático*.

La finalidad del delincuente al inutilizar, suprimir o modificar un sistema que utiliza tecnologías de la información, es alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario.

3.2.2 Virus

Los *virus* habitualmente suprimen o alteran archivos ejecutables por otros infectados con el código de éste. Pueden inutilizar o destruir, de manera intencionada, los datos almacenados en un computador.

Dentro de las distintas formas de dañar un sistema tenemos los denominados "*virus*", que el autor Jimeno García, citado por Nava Garcés, define como: "*Son*** *claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un*

virus puede ingresar a un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del "Caballo de Troya".

Jimeno García, citado por Nava Garcés, proporciona una clasificación de los virus, de manera enunciativa y no limitativa y, para el efecto indica:

- **Virus de sector de arranque**. Infecta la parte del disco usada para arrancar.
- **Virus de ficheros**. Infecta los ficheros ejecutables, no sólo los de extensión, exe.
- **Virus de sobreescritura**. Escribe el código vírico sobre el fichero, dejándolo inservible.
- **Virus añadido** (***appenders***). Infectan el fichero sin destruirlo.
- **Virus de macro**. Infectan las macros de documentos de texto.
- **Virus de compresión.** La utilizan para evitar que aumente el tamaño como una forma de ocultación.
- **Virus de cavidad**. Hace uso de los espacios libres de los ficheros.
- **Virus de directorio**. Aprovecha la estructura de los directorios.
- **Virus multiplataforma**. Afectan a diferentes sistemas operativos: Windows, Mac OS.

- **Virus multiproceso**. Infecta el kernel32dll, centro de llamadas del S.O.

- **Virus multipartito**. Utiliza varias técnicas de infección: arranque, ejecutable.

- **Virus parásito**. Aquel que pega su código al ejecutable infectado.

- **Virus de compañía** (***companion***). Crea un fichero con extensión.COM para infectar uno con extensión. EXE del mismo nombre, que el sistema ejecutará antes.[38]

Cada día surgen cientos de virus nuevos y únicamente son noticia los virus que tienen una programación que causa efectos más destructivos de los sistemas informáticos. Dentro de los mecanismos de "autodefensa", en materia de Ciberseguridad, los usuarios deben ser diligentes en cuanto a la actualización de los mecanismos antivirus y así evitar daños a sus sistemas.

3.2.3 Armas cibernéticas

Arma cibernética consiste en cualquier dispositivo que pueda ser utilizado en tareas de ataque, defensa y destrucción de fuerzas o instalaciones enemigas ubicadas en el ciberespacio, y que sus efectos pueden trascender en el mundo físico. A diferencia de los denominados "virus", que son mecanismos de destrucción o inutilización de datos o información contenida en un ordenador sin aspectos

38 Ob. Cit. La Prueba Electrónica en Materia Penal.

bélicos, la denominación de armas cibernéticas se emplea, generalmente, cuando estamos en una situación de conflicto bélico o en asuntos de guerras cibernéticas que involucra a dos o más Estados.

Las denominadas armas cibernéticas son creadas como política de algunos Estados para defender su soberanía en un nuevo campo de batalla denominado "*ciberespacio*", aunque no se limita a éste, ya que sus efectos son sensibles en el espacio físico, alterando armas o dispositivos tangibles. También pueden ser utilizadas para obtener información de otros Estados (ciberespionaje).

Generalmente, las armas cibernéticas son creadas y utilizadas por los Estados desarrollados o que tienen un alto nivel de infraestructuras informáticas, como es el caso de Estados Unidos de América, China, Rusia, Alemania, Israel, Irán, entre otros.

Estados Unidos de América recientemente creó un Cibercomando encargado de defender las redes militares estadounidenses y realizar ofensivas cibernéticas, entre otras funciones. El propio presidente de Estados Unidos de América, Barack Obama, ha manifestado públicamente que, para beneficio del país que representa, deben acelerarse los trabajos de creación o perfeccionamiento de armas cibernéticas, especialmente en el objetivo de rastrear el programa nuclear de Irán.

Se considera que el año 2011 fue el año de auge de las armas cibernéticas, ya que muchos Estados manifestaron su interés y disposición para desarrollar y desplegar dichos mecanismos de carácter bélico.

El 1 de junio del 2012 el Diario estadounidense *The New York Times*, indicó que el presidente de Estados Unidos, Barack Obama, había ordenado, en forma secreta y durante los primeros meses de su mandato, incrementar sofisticados ataques contra los sistemas informáticos de Irán para sabotear sus instalaciones nucleares. Se dice que fue el primer ataque de Estados Unidos usando armas cibernéticas. Se indicó en el Diario en mención, que la iniciativa de ataque cibernético se planteó en el año 2006 durante la administración del expresidente George W. Bush, y se le dio el nombre en clave de "Juegos Olímpicos".

Como las más recientes y potentes armas cibernéticas podemos citar las siguientes:

3.2.3.1 Stuxnet. Se considera que el desarrollo de este programa o arma cibernética pudo representar un costo superior a los 500,000 euros. El objetivo principal de este software malicioso fueron los sistemas especiales que empleaban los programas de monitorización y control industrial de Siemens.

Este componente de *malware*, por sus características, como pasar inadvertido dentro del sistema, incubándose por un tiempo prolongado y cambiando paulatinamente el proceso al interceptar las órdenes del software de Siemens SCADA y reemplazarlas con comandos maliciosos variando el funcionamiento del equipo, hizo pensar a muchos expertos que los diseñadores de Stuxnet tenían en mente un objeto de ataque: las centrífugas de enriquecimiento de uranio en la planta iraní de Natanz.

Como consecuencia de lo anterior, a finales de noviembre del 2010, el presidente iraní, Mahmud Ahmadineyad, declaró públicamente sobre los problemas ocasionados por la ofensiva cibernética en un número limitado de centrífugas.

Algo novedoso e importante de *Stuxnet*, consistió que no solo fue dirigido contra objetos virtuales, sino contra una infraestructura real.

3.2.3.2 ***Flame*** **(Worm.Win32.Flame).** Arma cibernética descubierta a finales de mayo del 2012. En el mes de junio del 2012, el Diario estadounidense *The New York Times*, informó que *Stuxnet* y *Flame* fueron desarrollados por dos servicios secretos en conjunto: la Agencia Central de Inteligencia (CIA) de Estados Unidos y la "Unidad 8200" del servicio de inteligencia militar israelí.

Esta arma cibernética fue descubierta por la compañía de seguridad en Internet denominada KASPERSKY. Los representantes de Kaspersky Lab consideran que Flame es el *software* de espionaje más complejo descubierto hasta la fecha. Es un programa malicioso especializado en "ciberespionaje", a través del cual se puede sustraer información valiosa, incluyendo contenidos de la pantalla de ordenador, información sobre sistemas específicos, archivos almacenados, datos de contacto y conversaciones. Es capaz de obtener información de audio.

De manera que cualquier alteración, modificación o daño, ya sea a través de un virus, arma cibernética o *malware* en general, deberá ser considerado como daño informático,

salvo que implique la tipificación de una figura delictiva de mayor impacto, como podría ser el "terrorismo cibernético", entre otras.

Lo trascendental, para poder tipificar el delito de daño informático, es la determinación, dentro del proceso legal, de cualquier alteración, destrucción, inutilización, supresión o modificación, que cause un daño a un sistema que utilice tecnologías de la información. Importante será, que el Juzgador, no se confunda con tanta variante de virus, ataques cibernéticos y mecanismos que al final del día, producen un daño informático, tal como se ha indicado.

3.3 Consecuencias del daño producido por negligencia o culpa

Como se indicó en el apartado anterior, el delito de daño informático se produce por un acto deliberado; no obstante ello, puede suceder que se produzca un daño informático por "negligencia" o "culpa" de una persona, y que afecte bienes ajenos; como por ejemplo, al no establecer medidas de seguridad y control en el uso de equipos o sistemas informáticos, lo cual debe ser materia de ***responsabilidad civil***.

En otras palabras, el daño informático puede producirse como consecuencia de: (**a**) Un **acto doloso** o **deliberado**, caso en el cual estaríamos ante la figura del "***delito de daño informático***"; y, (b) Un **acto producido por culpa** o **negligencia**, que estaríamos ante la figura de "***responsabilidad civil***" por "***daño patrimonial***", que sería materia única y exclusivamente de una acción de "***daños y***

perjuicios" y de conformidad con el procedimiento que establece nuestro ordenamiento adjetivo civil.

Los efectos extensivos del daño informático pueden ser muy amplios, y podríamos estar ante situaciones que ameriten el análisis particular de figuras jurídicas como el denominado "***daño indirecto***", que, por ejemplo, podría ocasionarse por la transmisión de un "*virus*" y que afecte a un número indeterminado de personas. Con relación al denominado "daño indirecto", debemos determinar *¿hasta qué punto la persona es responsable de las consecuencias del daño generado por su negligencia o culpa*? Para dar respuesta a esta interrogante debemos determinar: si la persona que comete el daño debe ser responsable única y exclusivamente por el daño directo o por la cadena de daños que se podrían generar como consecuencia de dicho daño.

POTHIER considera que el autor de una culpa no debe reparar sino las consecuencias inmediatas de ella. En materia de responsabilidad, citó un ejemplo de los daños directos e indirectos de la manera siguiente: *Un tratante de ganado comete la culpa de vender una vaca apestada. El animal vendido muere y toda la manada del comprador perece por contagio. El comprador, privado así de su ganado, no puede ya cultivar sus tierras; falto de recursos, no paga a sus acreedores; éstos embargan los bienes de aquél y los venden a precio vil.* POTHIER se cuestiona: En esta catarata de perjuicios *¿dónde se detiene la responsabilidad del vendedor*?; *¿hasta dónde es su culpa la causa de los daños sufridos por el comprador*? POTHIER respondía que el comprador no estaba obligado, sino por la pérdida de la vaca vendida y por los animales alcanzados por el contagio, daños directos, pero no por la falta de cultivo de tierras, ni del embargo, daños indirectos.[39]

39 Duque Gómez, Jose N. **Compilación y extractos del Daño**, primera edición, 2001, editora jurídica de Colombia, pág 419.

En materia de daños informáticos puede suceder que una persona, por culpa o negligencia, no emplee medidas de seguridad informática en sus sistemas, lo cual puede permitir que, su sistema o computador, pueda ser utilizado como una herramienta para producir daños a terceras personas, como puede suceder en el caso de las denominadas redes zombi (*botnets)*.

Sobre el particular, la mayoría de tratadistas sostienen que debe responsabilizarse al sujeto activo, únicamente por las consecuencias directas del daño, salvo que exista una intencionalidad de producir los daños indirectos. Esto se fundamenta en las medidas de seguridad que cada persona debe emplear a sus sistemas, y así como en el ejemplo citado por POTHIER en cuanto a la vaca apestada, el comprador debió prever esa posibilidad y tomar las medidas de seguridad adecuadas para evitar los daños indirectos.

3.4 Derecho comparado en materia de Daño Informático

El delito de daño informático se encuentra regulado en distintas legislaciones de la forma siguiente:

DAÑO INFORMÁTICO

Consejo Europeo	Convenio Budapest o Convención de Ciberdelincuencia.	Artículo 4. Atentado contra la integridad de datos. Todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.
Estados Unidos de América	Ley Federal de Abuso Computacional que modificó la ley de 1984.	Prohíbe la transmisión de un programa, información, códigos o comandos que causan daño computacional, a los sistemas informáticos, redes, información, datos o programas.
Argentina	Ley 26.388 que contiene reformas al Código Penal de Argentina. 04 de junio del 2008.	ARTICULO 10 — Incorpórase como segundo párrafo del artículo 183 del Código Penal, el siguiente: En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.
Venezuela	Ley Especial contra los Delitos Informáticos. 04 de septiembre 2001.	Artículo 7. Sabotaje o daño a sistemas. El que destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.
Chile	Ley Relativa a Delitos Informáticos No. 19223. 28 de mayo de 1993.	Artículo 2. El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Alemania	Ley contra la Criminalidad Económica.	Prohíbe la destrucción, cancelación, inutilización, eliminación o alteración de datos y sistemas informáticos. También prohíbe la tentativa.
Colombia	Ley No. 1273-2009, que contiene reforma del Código Penal de Colombia. 05 de enero del 2009.	*Artículo 269D:* DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

4. DELITO DE REPRODUCCIÓN DE DISPOSITIVOS DE ACCESO

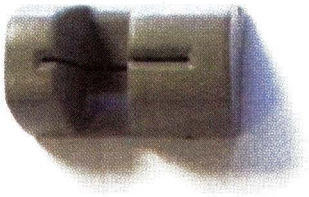
Cuando hablamos de reproducción de dispositivos de acceso, se refiere a la replicación intencional de un componente tecnológico, que permite ingresar a un sistema que tiene a resguardo información o activos de diferente índole.

En la actualidad, este delito se está realizando con mayor frecuencia, y los delincuentes cibernéticos usan dispositivos que combinan tecnología e ingenio.

Este delito está regulado en el artículo 7, de la Iniciativa de Ley de Delitos Informáticos, que literalmente dice:

> "***Artículo 7. 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, será sancionado con prisión de cuatro a ocho años y multa de cien a quinientas veces el salario mínimo legal vigente.*"

El ejemplo clásico que se puede mencionar son los ATM Skimmers, aunque en este tema también estaríamos ante un posible "concurso de delitos", debido a que está relacionado con el "fraude informático"; sin embargo, por fabricación de dispositivos de acceso es muy ilustrativo para el tema que nos ocupa. Los delincuentes realizan réplicas de los dispositivos de captura de información de las tarjetas de crédito o débito de los ATM´s, también utilizan teclados que sobreponen en el teclado original, el cual contiene dispositivos de comunicación o de otra especie, que permite la transmisión de la información contenida en la banda magnética, al delincuente que se encuentra cerca del área. Las siguientes fotografías demuestran lo explicado:



Ranura Real

Dispositivo Agregado

El Dispositivo cubre la ranura real.

Ya instalado en el ATM

40 http://krebsonsecurity.com/2010/01/would-you-have-spotted-the-fraud/

Este teclado se sobrepone al teclado original y transmite a otro dispositivo la clave del usuario.

5. DELITO DE ESPIONAJE INFORMÁTICO

5.1 Aspectos generales del espionaje informático

El delito de espionaje informático, también conocido como "ciberespionaje", está regulado en el artículo 9, de la Iniciativa de Ley de Delitos Informáticos. Dicha norma dice así:

41 http://krebsonsecurity.com/all-about-skimmers/

> *"Artículo 9. Espionaje informático. Comete el delito de 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, será sancionado con prisión de seis a diez años y multa desde doscientas a setecientas veces el salario mínimo legal vigente.*
>
> *La pena será aumentada en una tercera parte cuando, para la realización del hecho, se creare o desarrollare sistema que utilice tecnologías de la información, dispositivo o dato informático que afecte la intimidad o privacidad de las personas."*

Este delito también tiene relación con el delito de "*acceso ilícito*" y, por ello, puede configurarse un "*concurso de delitos*", dependiendo del caso concreto. En el delito de espionaje informático, el delincuente no se limita al puro acceso al sistema, toda vez que es necesario que se **apodere**, **obtenga**, **revele**, **transmita** o **difunda** el contenido, parcial o total, del sistema o dato informático.

En el delito de espionaje informático, el bien jurídico tutelado por el legislador lo constituye la información y, específicamente, el atributo de "***confidencialidad***" de la misma. En el Título Primero, Sección Segunda, artículo 4, de la Iniciativa de Ley de Delitos Informáticos se define a la "confidencialidad" como "***un atributo de la información para prevenir su divulgación a personas o usuarios no autorizados***".

Es imprescindible que el ordenamiento jurídico contemple normas jurídicas para proteger todo tipo de relaciones jurídicas. El espionaje informático puede realizarse, por ejemplo, para obtener "***secretos empresariales***", lo cual es común actualmente, e implica que, no sólo estaríamos ante la tipificación del delito de espionaje informático, sino que, además, se abre la puerta para la sanción de prácticas desleales entre comerciantes y que serían materia de "*competencia desleal*"; entre otras acciones legales que podrían promoverse en contra del delincuente, de conformidad con la Ley de Propiedad Industrial, Decreto 57-2000 del Congreso de la República de Guatemala.

Una de las principales razones, por las cuales un Estado debe contar con legislación relativa a "*delitos informáticos*" o "*cibercrimen*", es para cumplir con su deber de brindar "***seguridad jurídica***" a sus habitantes. Por ello, consideramos que ha sido muy atinado el contenido del segundo considerando de la Iniciativa de Ley de Delitos Informáticos, que actualmente se encuentra en discusión en el Congreso de la República. En dicho cuerpo normativo, no vigente por el momento, se consideró que en Guatemala ya existe regulación sobre *comercio electrónico,* según el contenido de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto número 47-2008 del Congreso de la República de Guatemala, y que, en consecuencia, se hace necesario emitir una nueva ley especial para prevenir y sancionar los delitos de naturaleza informática, que pueden afectar el objeto o materia de la normativa de comercio electrónico. En ese sentido, los comerciantes y cualquier persona en general, deben estar protegidas de los actos de cibercrimen, que podrían perjudicar gravemente sus diversas relaciones jurídicas.

5.2 Herramientas utilizadas para espionaje informático

En la actualidad existen diversas maneras de obtener la información, de manera que el propietario de la información no se entere, y poder así, realizar espionaje.

En primer lugar, podemos mencionar el denominado "***keylogger***" (derivado del inglés: ***key*** –tecla- y ***logger*** –registrador-, es decir, "***registrador de teclas***"), que constituye un tipo de técnica que permite la captura de las pulsaciones del teclado, para memorizarlas en un fichero y/o enviarlas a través de Internet.

Suele usarse como *malware* del tipo *daemon*, permitiendo que otros usuarios tengan acceso a contraseñas importantes, como los números de tarjeta de crédito, usuario y contraseña de la cuenta de banco u otro tipo de información privada que se quiera obtener.

Estos pueden ser enfocados en *hardware* o en *software*.

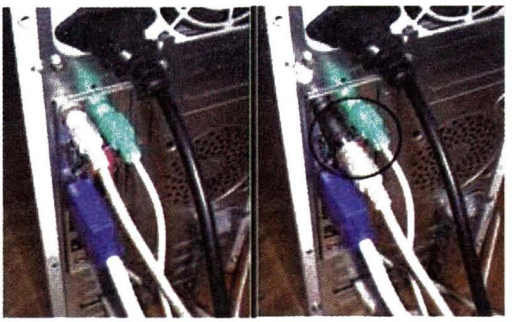
5.2.1 De *Hardware*. Los que utilizan el *hardware*, a su vez se dividen en tres:

5.2.1.1 Del tipo adaptador. El cual, como su nombre lo indica, son adaptados a la entrada estándar de los teclados por cable, éstos son fáciles de detectar con una revisión rápida de la conexión del teclado al CPU. La dificultad del perpetrador radica en la necesidad de tener acceso físico al teclado que pretende violar.

5.2.1.2 Del tipo dispositivo. Este requiere de un nivel técnico avanzado o, como mínimo, el perpetrador

requiere conocimiento en soldado, puesto que debe desemsamblar el teclado y soldar el dispositivo adentro del teclado. Igualmente, requiere tener acceso físico al teclado.

5.2.1.3 **Teclado especialmente diseñado.** Este tipo de ***keylogger***, viene integrado en un teclado y son comercializados de esa manera, por lo tanto su detección es casi imposible. Sin embargo, requiere de utilizar medidas de ingeniería social para hacer llegar el teclado a la víctima.



Como podría verse un *Keylogger*, basado en *hardware* instalado

5.2.2 De Software. Los que utilizan software, a su vez pueden dividirse en tres:

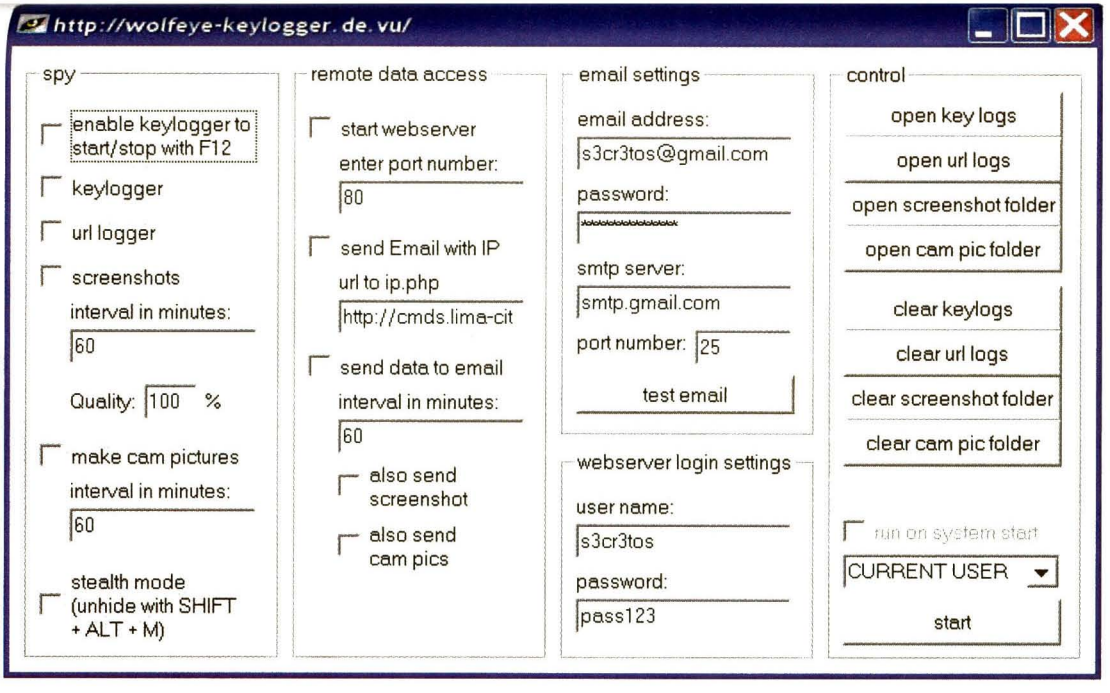
5.2.2.1 Los que se alojan en el núcleo del sistema. Estos *keylogger* son fáciles de implementar y, a su vez, fáciles de detectar. Requieren de conocimientos de las API; éstos están diseñados, de tal manera, que se alojen en el núcleo del Sistema Operativo, pueden funcionar como *driver* del teclado en el sistema. De esta manera, accede fácilmente a

la información que se está enviando o produciendo por el usuario.

5.2.2.2 **Los que se activan en el momento de comenzar a usar el teclado.** Son conocidos como enganchados, ya que, una vez que el usuario comienza a usar el teclado, éste se activa y comienza a registrar todo tipo de operaciones realizadas por medio del teclado.

5.2.2.3 **Por medio de funciones especialmente diseñadas.** Éstas presentan como problema un alto consumo de CPU.

Cuando se realizan los *keyloggers* por medio de *software*, su distribución puede realizarse por medio de troyanos, virus informáticos o gusanos.



Pantalla de un *keylogger* por software, que permite su funcionamiento en modo oculto. Se aprecia en la imagen la posibilidad de configuración.

6. DELITO DE VIOLACIÓN A LA DISPONIBILIDAD

6.1 Aspectos generales

Disponer, significa la facultad de "***usar***" o "***utilizar***" determinado bien o cosa. Esa facultad, de disponer o de usar, se origina por un derecho de "propiedad", "posesión", o por cualquier otro título que legitime o faculte a "usar", "poseer" o "disponer" determinado bien.

Así, por ejemplo: el propietario de un bien inmueble tiene el derecho de "poseer", "usar" o "disponer" de ese bien, porque ha adquirido ese derecho por virtud de un acto intervivos (compra-venta, donación o cesión), por disposición de última voluntad (sucesión *mortis* causa) o por hecho natural (aluvión o avulsión).

En el ciberespacio, al igual que en el mundo físico, existen bienes de ***dominio público*** y de ***dominio privado***. Así, por ejemplo: En el mundo físico las calles son de dominio público y, por ello, podemos transitar libremente por ellas; sin embargo, una casa ubicada a la orilla de esa calle es un bien privado y, si ingresamos sin autorización, estaríamos cometiendo el delito de allanamiento. En el ciberespacio funciona de la misma manera: Las calles las podríamos equiparar a las redes y la casa sería un sitio web de acceso restringido. Si ingresamos a un sistema informático, sin autorización, estaríamos cometiendo el delito de acceso ilícito, tal como se indicó en este mismo capítulo.

En materia de derecho informático, el bien sobre el cual se tiene el derecho de "uso" o "posesión", lo constituye la "***INFORMACIÓN***" que se encuentra contenida en un sistema

informático. En el artículo 4 de la Iniciativa de Ley de Delitos Informáticos, se define a la "***disponibilidad***" como una característica de la información, para garantizar que ésta se encuentre disponible, en cualquier momento, para quien tiene la autorización de acceder a ella, sean personas, procesos o aplicaciones.

Regresando a las normas del mundo físico, cuando un sujeto "impide" o "obstaculiza" nuestro derecho de "uso" o "disfrute" de nuestra propiedad, el ordenamiento jurídico provee al afectado, de mecanismos de "restitución" del "uso" o "disfrute" de esa propiedad y, considera al sujeto activo, como un "usurpador" o "detentador", según sea el caso. En el derecho informático se crean mecanismos de prevención y sanción a las conductas tendientes a la obstaculización del "uso" o "disponibilidad" de la información, regulándose así, el delito de ***VIOLACIÓN A LA DISPONIBILIDAD***. Según el artículo 10 de la Iniciativa de Ley en mención, se establece que la persona que, 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, se sancionará con pena de seis a diez años de prisión y multa desde cien a quinientas veces el salario mínimo legal vigente.

En el Convenio sobre la Ciberdelincuencia, del 23 de noviembre del 2001, conocido también como "Convención de Budapest", la violación a la disponibilidad se regula como parte del tema de "***ataques a la integridad del sistema***"; según consta en el artículo 5, que dice: "*Ataques a la integridad del sistema: "Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar, como delito en su derecho interno, la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.*"

Al obstaculizarse a una persona el acceso a redes, información o sistemas, se pueden producir una diversidad de consecuencias que trascienden en la esfera jurídica, como por ejemplo: (**a**) Se produce la comisión del delito de violación a la disponibilidad para prevenir y sancionar este tipo de conductas. (**b**) Al crearse la indisponibilidad de un sistema se puede afectar, gravemente, a un comerciante que ofrece sus productos o servicios, por medio de ese sistema informático. (**c**) También puede existir la posibilidad de que, la finalidad del delincuente, haya sido la de contribuir a una práctica de "competencia desleal". Y, (**d**) La víctima podría sufrir cuantiosas pérdidas por la indisponibilidad del sistema, que se traducirían en una condena al pago de daños y perjuicios en contra del sujeto activo.

El término ***disponibilidad***, estrictamente en materia informática, se refiere al aseguramiento de que la información se encuentre disponible para que, la persona autorizada para tenerla, la posea en el lugar y en el tiempo que desee.

En la práctica, la disponibilidad de la información requiere de ***sistemas de control,*** como por ejemplo: *back-ups* de la información, planeamiento de las capacidades, procedimientos y criterios para el sistema de autenticación, procedimientos para el manejo de incidentes, administración de remoción de medias computacionales, procedimientos de sostenimiento de la información, equipo de mantenimiento y pruebas, procedimientos para monitorear los sistemas en uso y procedimientos de continuidad de negocios.

Monitorear y revisar incidentes de seguridad, niveles de servicio y el rendimiento del sistema a tiempo, es una manera de ser proactivo en la prevención y asegurarse la disponibilidad.[42]

---

42 ISMS Auditor/Lead Auditor Course pág 10.

6.2 Información sensitiva o crítica

Toda organización debe definir y distinguir qué parte de la información que posee es crítica o sensitiva. Para cada organización este proceso es diferente, parte de la valoración del riesgo, envuelve la valoración de activos de información en el orden de calcular el riesgo y el nivel de seguridad requerido para proteger estos activos, usando un adecuado sistema de controles.

Garantizar la disponibilidad implica, también, la prevención de ataque de *denegación de servicio*.

La disponibilidad, además de ser importante en el proceso de seguridad de la información, es, además, variada, en el sentido de que existen varios mecanismos para cumplir con los niveles de servicio que se requiera; tales mecanismos se implementan en: infraestructura tecnológica, servidores de correo electrónico, de bases de datos, de web, mediante el uso de *clusters* o arreglos de discos, equipos en alta disponibilidad a nivel de red, servidores espejo, replicación de datos, redes de almacenamiento (SAN), enlaces redundantes. La gama de posibilidades dependerá de lo que queremos proteger y el nivel de servicio que se quiera proporcionar.

6.3 Ataque de Denegación de Servicio

La denegación de servicio (DoS) tiene como finalidad dejar indisponible un recurso (página, aplicaciones, servidores) para el cual fue diseñado. Hay muchas formas de poner un servicio indisponible para los usuarios legítimos, por ejemplo: (**a**) A través de la manipulación de paquetes de red y, (**b**) Por medio de programación lógica, aprovechando las vulnerabilidades de los recursos, entre otros mecanismos. Si un servicio recibe un

gran número de solicitudes, puede dejar de prestar servicio a los usuarios legítimos. De la misma manera, un servicio puede tener una vulnerabilidad y, ésta ser explotada por medio de un programa especialmente diseñado para esa finalidad, o también aprovechar la forma en que el servicio maneja los recursos.

A veces el atacante puede inyectar y ejecutar un código arbitrario en el desarrollo de un ataque de denegación de servicio, con el fin de acceder a la información crítica o ejecutar comandos en el servidor. Los ataques de denegación de servicio degradan, considerablemente, la calidad del servicio experimentado por los usuarios legítimos. Se presentan grandes retrasos en la respuesta, exceso de pérdidas y, las interrupciones del servicio, resultan en un impacto directo en la disponibilidad[43].

6.4 Modos de ataque

6.4.1 *DoS User Specified Allocation*

Si los usuarios pueden proporcionar, directa o indirectamente, un valor donde se especifique el número de un objeto a crear en el servidor de aplicaciones, y si el servidor no impone un límite físico superior a ese valor, es posible que se comience a ejecutar procesos fuera de la memoria disponible. El servidor puede empezar a asignar el número requerido de objetos especificados; pero, si se trata de un número extremadamente grande, puede causar serios problemas en el servidor; posiblemente puede llenar su memoria total disponible y provocar una baja en su rendimiento.

El siguiente es un ejemplo sencillo de código vulnerable en Java:[44]

43 http://www.owasp.org/index.php?title=Denial_of_Service&setlang=es

44 Idem.

```
String TotalObjects = request.getParameter ("numberofobjects"); int NumOfObjects = Integer. parseInt (TotalObjects); ComplexObject unArray []
```

6.4.2 *DoS User Input as a Loop Counter*

Al igual que en el problema anterior, en cuanto a lo especificado por el usuario en la asignación de objetos, si el usuario puede, directa o indirectamente, asignar un valor que será utilizado como un contador en una función de *bucle*, esto puede causar problemas de rendimiento en el servidor.

El siguiente es un ejemplo de código vulnerable en Java:

```
public class MyServlet extiende ActionServlet {public void doPost (HttpServletRequest solicitud, HttpServletResponse respuesta) throws ServletException, IOException {. . . String [] valores = request.getParameterValues ("CheckBoxField"); / / Proceso de los datos sin comprobar la longitud de rango razonable - mal! for (int i = 0; i values.length <; i + +) {/ / un montón de lógica para procesar la solicitud}. . . }. . . }
```

Como podemos ver en este ejemplo sencillo, el usuario tiene control sobre el contador de *bucle*. Si el código dentro del *bucle* es muy exigente, en términos de recursos, y un atacante obliga a que éste se ejecute en un número muy elevado de veces, esto puede disminuir el rendimiento del servidor en el manejo de otras solicitudes, causando una condición de denegación[45].

45 Ob. Cit.

6.4.3 *DoS Storing Much Data in Session*

Se debe tener cuidado de no almacenar demasiados datos en un objeto de sesión de usuario. Almacenar demasiada información en la sesión, como es el caso de grandes cantidades de datos recuperados de la base de datos, puede causar la negación de servicio. Este problema se exacerba si a los datos de sesión se les da un seguimiento antes de la entrada, el usuario puede lanzar el ataque sin la necesidad de una cuenta[46].

6.4.4 *DoS Loching Customer Accounts*

El primer caso de denegación de servicio envuelve al sistema de autenticación, considerándolo como una aplicación objetivo. Una defensa común, para impedir el descubrimiento por *fuerza bruta* de contraseñas de los usuarios, es bloquear una cuenta de uso después de tres a cinco intentos fallidos de inicio de sesión. Esto significa que, incluso, si es un usuario legítimo, éste sería incapaz de entrar al sistema, hasta que su cuenta haya sido desbloqueada. Este mecanismo de defensa puede convertirse en un ataque DoS, si existe una solicitud válida y si el atacante logra encontrar una manera de predecir cuentas válidas de inicio de sesión.

Hay pros y contras en la política de bloqueo de cuentas, después de intentos fallidos, o en aquellos sistemas en que se les permite a los clientes elegir su nombre de cuenta. Este puede ser reducido con la utilización de sistemas como el *CAPTCHA*[47] y similares. [48]

46 Idem.

47 CAPTCHA, son las siglas de "*Completely Automated Public Turing test to tell Computers and Humans Apart* (Prueba de Turing pública y automática para diferenciar máquinas y humanos). A propósito, el creador de este mecanismo de verificación fue el científico guatemalteco y profesor de ciencias de la computación, Luis von Ahn. El término CAPTCHA se empezó a utilizar en el año 2000.

48 Idem.

6.4.5 DoS Failure to Release Resources

Si se produce un error, en la aplicación que previene la liberación de un recurso en uso, puede no estar disponible para su uso posterior, ejemplos pueden ser:

- Una aplicación bloquea un archivo para escribir y, luego, se produce una excepción, pero no se cierra de forma explícita y bloquea el archivo.

- Memoria por goteo, en lenguajes donde el desarrollador es responsable de la gestión de memoria, tales como C y C + +. En el caso de que exista un error, éste hace que la lógica normal del programa sea eludida, la memoria asignada no se puede quitar y puede ser dejada, en tal estado, que el recolector no puede recuperarla.

- El uso de objetos de conexión de base de datos donde los objetos no están siendo liberados, si se produce una excepción. Un número de las solicitudes repetidas puede causar que la aplicación consuma todas las conexiones a la base de datos, si el código todavía mantiene abierto el objeto de la base de datos, nunca liberará los recursos.

El siguiente es un ejemplo de código vulnerable en Java. En el ejemplo, tanto la conexión y *Callable Statement* deberían ser cerrados en un bloque finally.[49]

---

49 Ob. cit.

```
public class AccountDAO {... ... createaccount public void
(AccountInfo ACCT) lanza AcctCreationException {... ... try
{CONN conexión = DAOFactory.getConnection (); calStmt
CallableStatement = conn.prepareCall (...), ... ... calStmt.
executeUpdate (); calStmt.close (); conn.Close ();} catch (java.
sql.SQLException e) {throw AcctCreationException (...);}}}
```

6.4.6 *DoS Buffer Overflow*

Cualquier lenguaje, donde el desarrollador tiene la responsabilidad directa en la gestión de asignación de memoria, especialmente C y C + +, tiene el potencial para un desbordamiento de *búfer*. Mientras que el riesgo más grave, relacionado con un desbordamiento de *búfer*, es la capacidad de ejecutar código arbitrario en el servidor, el primer riesgo proviene de la negación de servicio, que puede ocurrir si la aplicación se bloquea[50].

El siguiente es un ejemplo simplificado de código vulnerable en C:

```
desbordamiento de vacío (char * str) {char buffer [10];
strcpy (buffer, str); / / peligrosas! } Int main () {char * str =
"Esto es una cadena que es más grande que el búfer de 10";
desbordamiento (str);}
```

Si este ejemplo de código se ejecuta, causaría un fallo de segmentación y de volcado de núcleo. La razón es que strcpy

50 Idem.

intenta copiar 53 caracteres en una matriz de 10 elementos, tratando de sobreescribir lugares adyacentes de la memoria. Si bien este ejemplo anterior es un caso muy sencillo, la realidad es que, en una aplicación basada en web, puede haber lugares en los que la entrada del usuario no está controlada en cuanto a su longitud, lo que hace este tipo de ataque posible[51].

6.4.7 Ataque de Denegación de Servicio Distribuida (DDoS)

¿Qué es un *DDoS*? Es el método de ataque que utiliza múltiples *hosts* para lanzar un largo y coordinado ataque a una máquina, con el objeto de denegar el acceso o dejar no disponible un sistema.

El tráfico o respuestas, que la red de la víctima o servicio seleccionado (DNS, HTTP) recibe, es más que los recursos normales utilizados para atender ese tipo de solicitudes.

Los servicios legítimos son interrumpidos, el ancho de banda, el espacio en disco o el tiempo de procesamiento, son también consumidos o interrumpidos.

Existe una variedad de herramientas para realizar ataques distribuidos. Dentro de estos podemos mencionar los *sniffers* y los *keyloggers* (surgidos en los años 90) que capturan información y recientemente, herramientas de acceso remoto, que permite a un atacante obtener el control sobre una máquina.

Los troyanos, son un ejemplo de esto (*B02K, NetBus, and RingZero*), *sniffers*, y otras herramientas utilizadas para recolectar información y para obtener el control remoto de las máquinas.

---

51 Idem

Las herramientas actuales combinan diferentes *toolkits* para aprovechar una combinación de amenazas, donde diferentes herramientas hacen una variedad de actividades como: obtener información, explotar vulnerabilidades, iniciar ataques y transmitir información sensible o confidencial.

6.4.7.1 Características de un ataque DDoS

- Utilizan para su ataque varios componentes o herramientas.
- Utilizan *hosts* comprometidos para, posteriormente, integrarlos a la red.
- Los ataques son dirigidos a una sola víctima; esta víctima puede ser cualquier computadora que les parezca o represente un valor rentable.
- Los ataques DDoS son activados a control remoto por una computadora maestra.
- La comunicación entre la computadora maestra y la red puede estar encriptada.

Existen otros métodos que pueden ser utilizados por intrusos, para comprometer el sistema e instalar herramientas, que les permitan tomar el control de la computadora. Pueden usar la ingeniería social para obtener contraseñas, aprovechar vulnerabilidades, difundir código malicioso, entre otros.

7. DELITO DE FRAUDE INFORMÁTICO

7.1 Aspectos generales del Fraude Informático

Debido al ánimo de lucro y al uso de herramientas informáticas que encubren al delincuente, el delito de fraude informático, hoy en día, es considerado como uno de los delitos más populares que se cometen por Internet.

Algunos tratadistas consideran que no existe distinción entre la figura del *Fraude Informático* con el *Fraude* o *Estafa*. Otros, consideran además, que no debe sobre-regularse las figuras delictivas, ya que consideran que, de una u otra forma, el fraude informático entraña ardid o engaño, al igual que la Estafa que forma parte del Código Penal.

En el caso de Guatemala, el delito de Estafa se encuentra regulado en el artículo 263 del Código Penal, que establece: "***Artículo 263.- Estafa propia***. *Comete estafa quien, induciendo a error* ***a otro****, mediante ardid o engaño, lo defraudare en su patrimonio en perjuicio propio o ajeno.*" (El énfasis es propio).

En la Iniciativa de Ley de Delitos Informáticos, el delito de Fraude Informático se encuentra regulado en el artículo 11, que dice: "***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, será penado con prisión de cuatro a ocho años y multa desde cien hasta mil veces el salario mínimo legal vigente.*" (El énfasis es propio).

Sobre el particular debemos aclarar: En primer lugar que, no obstante que en ambos delitos (Estafa y Fraude Informático) la finalidad que persigue el delincuente es obtener lucro ilícito –*animus lucrandi*-, el Fraude Informático se diferencia de la Estafa debido a que en ésta última el ardid o engaño se ejerce directamente contra las ***personas***; en cambio, en el Fraude Informático su objetivo no son las personas sino los ***sistemas informáticos***. En otras palabras, en la Estafa la manipulación recae sobre las personas individuales y, en el Fraude Informático, la manipulación es de los sistemas informáticos, aunque con la misma finalidad fraudulenta. En segundo lugar, en el fraude informático, comúnmente, la pérdida patrimonial, ocasionada a la víctima es mínima, toda vez que este delito se configura mediante la afectación de ***patrimonios colectivos***, como es el caso de las cuentas bancarias, en las cuales el delincuente se apropia de sumas dinerarias mínimas, pero de un gran volumen de víctimas, para evitar ser descubierto. En los códigos penales suele tipificarse como "*delito patrimonial*" cuando se afecte una suma considerable de dinero y, se tipifica como "*falta*", cuando la suma dineraria es mínima y esto incide en la pena a aplicar.

Ángel Montes de Oca, al comentar sobre la jurisprudencia argentina y sobre el problema en cuanto a la tipificación del fraude informático o estafa informática, indica: "*En otros ámbitos, la jurisprudencia se mostró más ambivalente; tal el caso de la estafa informática. La interpretación sostenía que el Código Penal no permitía calificar como estafa la obtención mediante ardid de bienes o servicios por medio de computadoras (hardware o software), lo que determinaba que las acciones delictivas sobre programas de ordenador (con proyección también al software utilizado vía Internet para venta de bienes) quedaran calificados como hurto.*"[52]

52 MONTES DE OCA, ANGEL, Derecho de Internet, Editorial Heliasta S.R.L., 2004, Buenos Aires, Argentina, pág. 62.

Por las razones anteriores, consideramos que debe regularse el Fraude Informático, como norma de carácter especial y distinta de la Estafa y del Hurto que regula el Código Penal.

Con relación a la motivación de este tipo de delito informático, Francisca Moreno, analista de amenazas MTIS (MTIS Treta Analyst) de McAffe Labs dijo: *"En la actualidad el cibercrimen tiene motivos financieros, a diferencia de algunos años atrás, cuando las motivaciones eran la búsqueda de gloria o, simplemente el placer de hacerlo."*[53]

7.2 Clases de Fraude Informático

Por ser los más comunes, citamos los siguientes:

7.2.1 Subasta en línea

La subasta en línea constituye un mecanismo de *oferta al público,* en la cual las personas presentan sus "*pujas electrónicas*"; es decir, ofrecen determinada suma dineraria por el producto o servicio objeto de la subasta o remate. La subasta en línea constituye uno de los servicios más difundidos en Internet. En el sitio denominado "*eBay*", que constituye el mercado de subastas en línea más importante del mundo, en el año 2006, se vendieron mercancías por un valor superior a los 20,000 millones de dólares.

Los dos tipos de engaño más comunes en la subasta en línea son:[54]

---

53 http://tecno.americaeconomia.com/noticias/quien-esta-detras-del-cybercrimen. Sitio consultado el 04 de junio del 2012 a las 15:35 horas.

54 http://ftc.gov/os/2004/03/bealsfraudtest.pdf

- Ofrecer mercancías no disponibles para la venta y exigir su pago antes de la entrega.
- Adquirir mercancías y solicitar su envío, sin intención de pagar por ellas.

7.2.2 Estafa nigeriana

Este tipo de engaño se realiza mediante una operación "aleatoria", es decir, opera como un juego de lotería, en el cual una persona recibe un ofrecimiento a cambio de aportar determinada suma de dinero. El destinatario del mensaje, a sabiendas de que perderá determinada cantidad, apuesta por ganar el ofrecimiento. Así también, el destinatario puede proporcionar datos de cuentas bancarias que posteriormente podrían ser utilizadas para actos delictivos.

7.2.3 *Phishing*

Es considerado el delito informático que tipifica, claramente, el Fraude Informático. Se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El *phisher*, se hace pasar por una persona o empresa de confianza, en una aparente comunicación oficial electrónica; por lo común un correo electrónico, algún sistema de mensajería instantánea o, incluso, utilizando también llamadas telefónicas.

Dado el creciente número de denuncias de incidentes relacionados con el *phishing*, se requieren métodos adicionales de protección. Se han realizado intentos con leyes que castigan la práctica, con campañas para prevenir a los usuarios y con la

aplicación de medidas técnicas a los programas[55].

Mundialmente, el 80% del *phishing* esta dirigido a los bancos[56]. Guatemala no ha sido la excepción, los intentos más recientes de *phishing* han tomado como objetivo a clientes de los bancos más importantes del país. La forma de llegar a los clientes de los bancos ha sido de forma indiscriminada, haciendo acopio del nombre de la técnica "*Phishing*". Utilizan para ello bases de datos de direcciones de correo electrónico robadas, o adquiridas de forma fraudulenta.

También los ataques pueden ser más directos o dirigidos a un objetivo en especial, en donde el *phisher* es capaz de establecer con qué banco la víctima tiene relación y, de ese modo, enviar un *e-mail* falseado apropiadamente. En términos generales, esta variante hacia objetivos específicos en el *phishing* se ha denominado *spear phishing* (literalmente *pesca con arpón*). Los sitios de Internet, con fines sociales, también se han convertido en objetivos para los *phishers*; dado que mucha de la información provista en estos sitios puede ser utilizada en el robo de identidad. Algunos expertos han otorgado una tasa de éxito de un 90% en ataques *phishing* en redes sociales[57].

Los principales daños provocados por el *phishing* son:

- Robo de identidad y datos confidenciales de los usuarios. Esto puede conllevar pérdidas económicas para los usuarios o incluso impedirles el acceso a sus propias cuentas.

55 http://es.wikipedia.org/wiki/Phishing

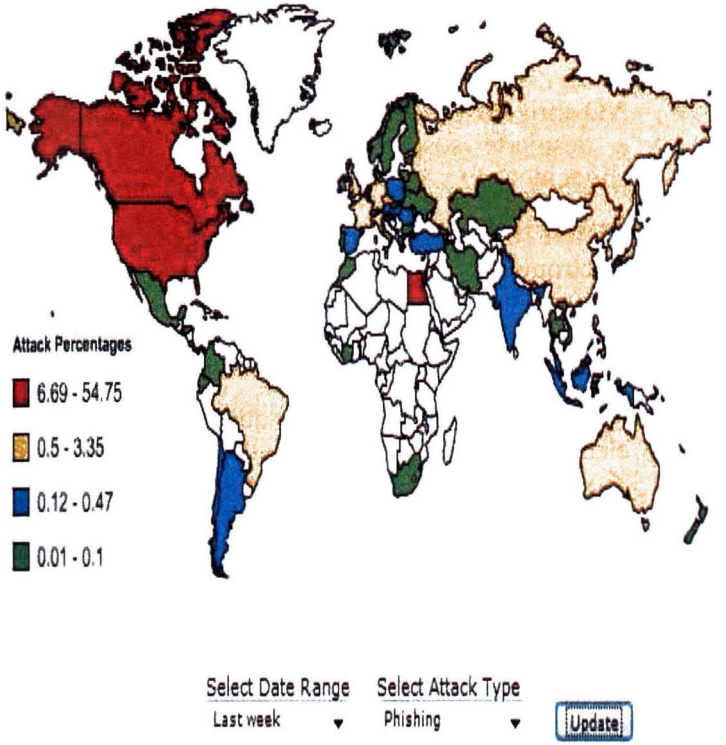
56 http://www.pandasecurity.com/spain/homeusers/security-info/cybercrime/phishing/

57 Tom Jagatic and Nathan Johnson and Markus Jakobsson and Filippo *Menczer*. Social *Phishing*. A publicarse en Communications of the ACM. 3 de junio del 2006. (en inglés).

- Pérdida de productividad.

- Consumo de recursos de las redes corporativas (ancho de banda, saturación del correo, fuga de información estratégica, entre otros).

En la figura que se presenta a continuación, extraída del sitio http://www.antiphishing.org, se aprecia la incidencia del *phishing* en el mundo, la cual corresponde a la semana del 14 al 18 de febrero del 2011.



El *phishing* es un tipo de *crimenware*[58] de amplio uso a nivel mundial, ya que, la inversión como el riesgo es mínima, desde el punto de vista de los delincuentes. Regularmente las víctimas, pocas veces hacen público el hecho, ya que muchas veces éstos han aceptado *e-mails* desconocidos o claramente identificados como *spam*.

Existen, en la actualidad, sitios en Internet en los cuales se puede reportar las páginas o sitios web que se sospecha sean *phishing*. Esta medida ayuda a evitar que otras personas caigan en estos sitios y sean timados.

Existen buenas prácticas para evitar ser sorprendido por este tipo de *crimenware*, entre las cuales se pueden mencionar:

- **NO** abrir correos de los cuales se desconozca el remitente, o despierte sospechas, aún siendo de un remitente conocido.
- **VERIFICAR** la fuente de origen de los correos electrónicos.
- **NO** remitir información sensible vía *e-mails*, como números de cuenta, usuario o *password*.
- **NUNCA** ingresar en los *links* que estén adjuntos a correos electrónicos, mejor copie el enlace y péguelo en la barra de direcciones de su navegador.

Lo que debemos tener claro es que la actividad de *phishing*, por sí sola, constituye un *acto preparatorio*, que luego se traducirá en el delito de fraude informático o en cualquier otro hecho ilícito, en el cual se haga uso de la información objeto del *phishing*.

58 El denominado "*crimenware*" es un tipo de software que ha sido especificamente diseñado para la ejecución de delitos de índole financiera por medio de la Internet.

8. DELITO DE FALSIFICACIÓN INFORMÁTICA

8.1 Aspectos generales de la Falsificación Informática

Cuando hablamos de "*falsedad*", nos referimos a todo aquello que ***no es*** *verdadero*, que se aparta de la verdad. Por ello, se dice que falsedad es todo "***mudamiento de la verdad***". O sea que, falsedad equivale a "*mentira*", a algo "*irreal*" o "*no auténtico*". Falsedad significa poner lo "***falso***" en lo que debiera ser "***verdadero***".

La falsedad puede configurarse de dos maneras: (**1**) Mediante la "**simulación**", cuando se representa algo fingiendo o imitando lo que ***no es***, es decir, que estamos ante la sustitución total de lo verdadero. (**2**) Mediante la "**alteración**", cuando se modifica o cambia la esencia o forma de algo, es decir, se altera algún elemento del objeto verdadero, caso en el cual estaríamos ante una sustitución parcial de lo verdadero.

Debido a que no toda la mentira es punible, el derecho penal ha tipificado los casos en los cuales la "simulación" o "alteración" de la verdad constituye un delito. Así tenemos el artículo 321 del Código Penal, que regula la denominada "Falsedad Material" y establece: "*Quien hiciere, en todo o en parte, un documento público falso, o alterare uno verdadero, de modo que pueda resultar perjuicio, será sancionado con prisión de dos a seis años.*" La denominada "Falsedad Ideológica" está regulada en el artículo 322 del mismo cuerpo legal, que establece: "*Quien, con motivo del otorgamiento, autorización o formalización de un documento público, insertare o hiciere insertar declaraciones falsas concernientes a un hecho que*

el documento deba probar, de modo que pueda resultar perjuicio, será sancionado con prisión de dos a seis años."

Como podemos apreciar, actualmente el objeto material, en el delito de falsedad, se refiere al documento. El documento consiste en toda declaración materializada procedente de una persona que figura como su autor, cuyo contenido tiene eficacia probatoria en el ámbito jurídico.

Específicamente, el delito de falsedad documental se produce ante la "alteración" o "simulación" de un documento de los denominados "públicos", es decir, aquellos autorizados por funcionario o notario público en el ejercicio de sus funciones.

En materia informática, si bien es cierto que en legislaciones avanzadas ya se habla de "documentos públicos electrónicos" como las denominadas "escrituras públicas electrónicas" o "protocolo electrónico" (que se refieren a documentos con la categoría de "públicos" para efectos de eficacia probatoria), en Guatemala tenemos algunos actos, comunicaciones o transacciones que, con la entrada en vigencia de la Ley para el reconocimiento de las comunicaciones y firmas electrónicas, Decreto 47-2008, se regulan como actos de naturaleza pública o privada; pero, se incluye la salvedad de que los servicios de certificación de firma electrónica no elevan, a dichos actos, a la categoría de "**documentos públicos**". [59]

59 El artículo 1 de la Ley para el reconocimiento de comunicaciones y firmas electrónicas, Decreto 47-2008 del Congreso de la República, establece: "ARTICULO 1.- Ámbito de aplicación. La presente ley será aplicable a todo tipo de comunicación electrónica, transacción o acto jurídico, público o privado, nacional o internacional, salvo en los casos siguientes:
a) En las obligaciones contraídas por el Estado en virtud de Convenios o Tratados Internacionales.
b) En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo.
El Estado y sus instituciones quedan expresamente facultados para la utilización de

Ahora bien, lo cierto del caso es que actualmente, en nuestro país, no existen normas que sancionen y prevengan la "simulación" o "alteración" de los datos contenidos en un sistema informático, donde existen otros factores de fuente de información. Algunos especialistas en el tema de la falsificación informática han indicado que actualmente existen computadoras capaces de generar mensajes, y por ello se cuestionan sobre la autonomía de la "máquina" para crear su propia fuente de información. Lo importante aquí será proteger la información –como bien jurídico tutelado-.

En el artículo 13, de la Iniciativa de Ley de Delitos Informáticos, se regula la denominada "***Falsificación Informática***", de la manera siguiente: "*Quien, a través de cualquier medio copie, altere o 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, será penado con prisión de cuatro a ocho años y multa desde cien hasta mil veces el salario mínimo legal vigente.*" Como podemos apreciar, en la norma pre-transcrita el objeto de la "simulación" o "alteración" lo constituyen los **datos informáticos**. Los datos son

las comunicaciones y firmas electrónicas. En las transacciones y actos realizados exclusivamente entre sujetos privados y que no afecten derechos de terceros, las partes podrán convenir en la aplicación de los mecanismos previstos en esta ley o bien de cualesquiera otras alternativas que deseen para asegurar la autenticidad e integridad de sus comunicaciones electrónicas.

Las disposiciones contenidas en esta ley se aplicarán sin perjuicio de las normas relativas a la celebración, la formalización, la validez y la eficacia de los contratos y otros actos jurídicos; el régimen jurídico aplicable a las obligaciones; y de las obligaciones que para los comerciantes les establece la legislación vigente. Las normas sobre la presentación de servicios de certificación de firma electrónica que recoge esta ley, no sustituyen ni modifican las que regulan las funciones que corresponde realizar a las personas facultadas, con arreglo a derecho, para dar fe de la firma en documentos o para intervenir en su elevación a públicos." (El énfasis es propio).

hechos que describen sucesos, son representaciones simbólicas. Los datos pueden ser comunicados por varios tipos de símbolos, tales como letras, números, gestos, etcétera. Técnicamente, a los datos procesados se les denomina "***información***", tal como se aprecia en el siguiente gráfico:

De manera que los datos deben ser procesados para constituir información. Cuando nos referimos a la información electrónica, los "datos" se refieren a: archivos, bases de datos, documentos de texto, imágenes, voz y vídeo, codificados en forma digital y que están contenidos en un sistema informático o en uno de sus componentes.

El bien jurídico tutelado en la falsificación informática es la "***información***" y, específicamente, la "***integridad de la información***", la cual no debe alterarse o modificarse.

Consideramos apropiada la definición contenida en el artículo 13 de la mencionada iniciativa de Ley de Delitos Informáticos, toda vez que protege a los datos informáticos que se encuentran contenidos en un sistema que haga uso de tecnologías de la información o uno de sus componentes. Sanciona drásticamente toda aquella conducta de "alteración" o "simulación" de dichos datos que genere un resultado falso o no auténtico, cumpliéndose así con la protección de la integridad de la información.

8.2 Clasificación de las falsificaciones informáticas

El autor Nava Garcés, al referirse a las FALSIFICACIONES INFORMÁTICAS, las analiza desde dos puntos de vista, los cuales se citan textualmente de su fuente:

- "Como **objeto**: Cuando se alteran datos de los documentos almacenados en forma computarizada.

- Como **instrumentos**: Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color, con rayos láser, surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, los cuales son de tal calidad que sólo un experto puede diferenciarlos de los auténticos."[60]

9. DELITO DE INTERCEPTACIÓN ILÍCITA

9.1 Aspectos generales de la interceptación ilícita

Según el Diccionario de la Real Academia Española, interceptar significa detener algo en su camino, interrumpir, obstruir una vía de comunicación.

---

60 Ob. Cit. La Prueba Electrónica en Materia Penal. Pág. 41.

En términos de informática, el objeto de la interceptación lo constituye la transferencia de "***datos informáticos***", los cuales son definidos como toda representación de hechos, instrucciones, caracteres, información o conceptos expresados de cualquier forma que se presente a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.[61]

El delito de interceptación ilícita se encuentra regulado en el artículo 12 de la Iniciativa de Ley número 4055 del Congreso de la República, y consiste en la interceptación, de forma deliberada, por cualquier medio, de 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. Se sanciona a quien intercepte datos informáticos en su origen, destino o en el interior de un sistema informático.

En la Iniciativa 4055 se incluye una agravante al delito de interceptación ilícita, y ésta se origina cuando la interceptación se cometa desde un sistema que utilice tecnologías de la información conectado a otro sistema de la misma naturaleza.

El Convenio de Ciberdelincuencia regula la interceptación ilícita en el artículo 3º, estableciendo que cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un

61 La definición de los denominados "*datos informáticos*" la encontramos en el artículo 4 de la Iniciativa de Ley de Delitos Informáticos, número 4055 del Congreso de la República de Guatemala.

sistema informático que contenga dichos datos informáticos. Según este Convenio, cualquier parte podrá exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Como parte del Derecho Comparado, relativo al delito de "***interceptación ilícita***", citamos la normativa del Código Penal de Colombia que, mediante la Ley 1273 del cinco de enero del dos mil nueve, reformó el Código Penal colombiano y que, según su parte considerativa, a través de dicha reforma se crea un nuevo bien jurídico tutelado (denominado "de la protección de la información y de los datos") y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones. En dicha normativa se regula el delito de INTERCEPTACIÓN DE DATOS INFORMÁTICOS así: "*El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte, incurrirá en pena de prisión de treinta y seis a setenta y dos meses.*"

La norma del Derecho Comparado citada, hace la salvedad de que puede existir "interceptación lícita", es decir, aquella interceptación autorizada por juez competente. En el caso particular de Guatemala, cabe mencionar que, mediante el Decreto 21-2006 del Congreso de la República de Guatemala, Ley contra la Delincuencia Organizada, se regula la interceptación "lícita", grabación y reproducción, con autorización judicial, de comunicaciones orales, escritas, telefónicas, radiotelefónicas, informáticas y similares que utilicen el espectro electromagnético, así como cualesquiera de otra naturaleza que en el futuro existan.[62]

62 El artículo 48 de la Ley contra la Violencia Organizada, Decreto 21-2006 del Congreso de la República, establece: "ARTÍCULO 48.- **Interceptaciones**. Cuando sea necesario evitar, interrumpir o investigar la comisión de los delitos regulados en

Dentro del Título III, denominado "*Organismos Competentes y Reglas de Derecho Procesal*", Capítulo II, denominado "*Medidas Cautelares y Procesales*", artículo 36, de la Iniciativa de Ley 4055 del Congreso de la República, Proyecto de Ley de Delitos Informáticos, se incluye un mecanismo de "***interceptación de datos***", al establecerse que se faculta al Ministerio Público, con autorización de juez competente, a interceptar, obtener y/o grabar los datos generados por sistema que utilice tecnologías de la información, necesarios para la investigación penal relativa a delitos informáticos.[63]

9.2 Tipos de ataques para realizar interceptación

La interceptación ilícita, la realizan los ciberdelincuentes por medio de ataques de *software* para ejecutarse, los cuales pueden ser:

---

los artículos 2, 3, 4, 5, 6, 7, 8, 9, 10 y 11 de la presente ley, podrá interceptarse, grabarse y reproducirse, con autorización judicial, comunicaciones orales, escritas, telefónicas, radiotelefónicas, informáticas y similares que utilicen el espectro electromagnético, así como cualesquiera de otra naturaleza que en el futuro existan.

63 El artículo 36 de la Iniciativa de Ley 4055 dice: "***Interceptación de datos relativos al contenido***. *Se faculta al Ministerio Público, con autorización de juez competente, a lo siguiente:*

a) *Por sus propios medios, podrá* ***interceptar****, obtener y/o grabar los datos generados por sistema que utilice tecnologías de la información, necesarios para la investigación;*

b) *Por sus propios medios o con colaboración del CSIRT-gt, podrá alterar, suspender o borrar cualquier actividad, que haga uso de sistema que utilice tecnologías de la información, en la comisión de los delitos establecidos en la presente ley; y,*

c) *Obligar a cualquier proveedor de servicios:*

1. *A facilitar la obtención, grabación o, a* ***interceptar*** *los datos relativos a comunicaciones específicas transmitidas dentro del territorio nacional, por medio de un sistema que utilice tecnologías de la información.*
2. *Por sus propios medios, obtenga o grabe los datos relativos al tráfico generado por sistemas que utilicen tecnologías de la información, necesarios para la investigación.*"

9.2.1 *Sniffing Attack*

Este tipo de ataque utiliza software especial de monitoreo, para obtener acceso a las comunicaciones de una red privada, ya sea para apropiarse del contenido de la propia comunicación o para obtener nombres de usuario y contraseña para futuros ataques. Estos ataques pueden realizarse en redes locales o en redes *wireless*. En una red, a la cual se conecta el usuario por medio de cable, el atacante debe tener acceso físico a la misma o al conector para el cable de red. En una red inalámbrica, el atacante necesita un dispositivo de recepción en las proximidades de la red inalámbrica. Esta interceptación de señal es muy difícil de detectar, salvo que la red pueda detectar la conexión de equipos desconocidos al requerir una dirección IP de un servidor DHCP.

Algunos *software* utilizados para interceptar las transmisiones de las redes son: ***Dsniff, Thereral y WinPcap***, entre otros.

9.2.2 *IP Spoofing Attacks*

Es un tipo de ataque de *software,* en el cual el atacante crea paquetes de IP con una dirección IP de origen falso, y utiliza los paquetes para tener acceso a un sistema remoto.

Un signo de un ataque de suplantación de IP es un paquete de red desde una fuente externa, que parece haberse originado desde una dirección de origen interno.

9.2.3 *Hijacking Attacks*

Un ataque de *Hijacking* (secuestro) es un ataque de *software,* a través del cual, el atacante toma el control de una sesión de red TCP, después que el usuario se autentica, para acceder a datos o recursos de red. Utiliza la identidad del usuario legítimo de la red. Durante un ataque de secuestro, el atacante puede tener acceso a los paquetes a medida que pasan de un huésped a otro, o desconectar uno de los anfitriones y continuar la comunicación con la otra parte. Un ataque de secuestro podría manifestarse en una conexión que, de forma inesperada, cae o se desconecta, pero lo más probable es que el usuario nunca sepa que su sesión ha sido secuestrada.

9.2.4 *Replay Attacks*

Es un tipo de ataque, donde el atacante captura el tráfico de red y lo almacena para retransmitir, en un momento y lugar apropiado para el atacante, y obtener acceso no autorizado a un específico *host* o red. Este ataque es particularmente exitoso, cuando un atacante captura paquetes que contienen usuarios, *passwords* u otro tipo de datos que le permitan autenticación. En muchos de estos casos el ataque no es descubierto, sin embargo, en los casos donde lo apropiado es el número de cuenta y clave de acceso a bancos o entidades financieras, la víctima se entera al llegar su estado de cuenta o el balance de saldos de su banco, ya que con esta información los fondos son retirados.

9.2.5 *Man in the Middle Attacks*

Es un tipo de ataque de *software*, donde un atacante se inserta él mismo, en medio de dos *hosts,* para lograr acceso en la transmisión de datos.

El atacante captura y lee cada paquete, los responde y envía al receptor del objeto, de manera que, tanto el emisor como el receptor creen que se comunican directamente entre sí.

Este engaño permite, al o a los atacantes, manipular la comunicación, en lugar de simplemente observar pasivamente. El ataque *man in the middle* se utiliza para tener acceso a la información de autenticación y la infraestructura de red para futuros ataques, o para obtener acceso directo al contenido del paquete. Por lo general, no habrá signos de que este tipo de ataque está en curso o acaba de tener lugar.

Figura No. 1 Hijacking Attack

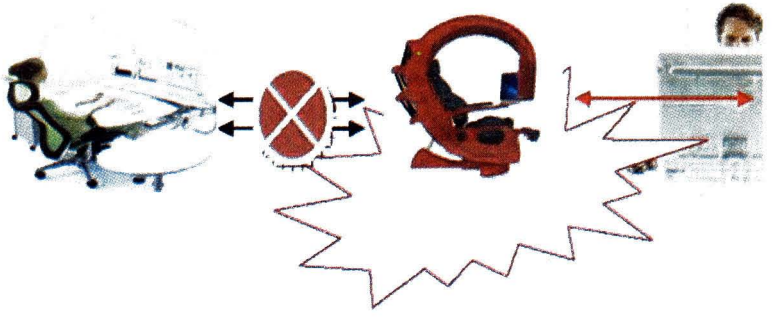


Figura No. 2 **Replay Attack**

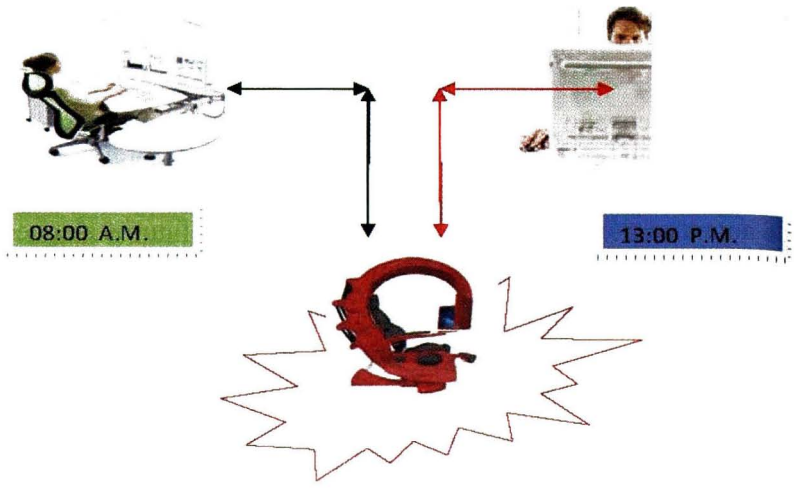
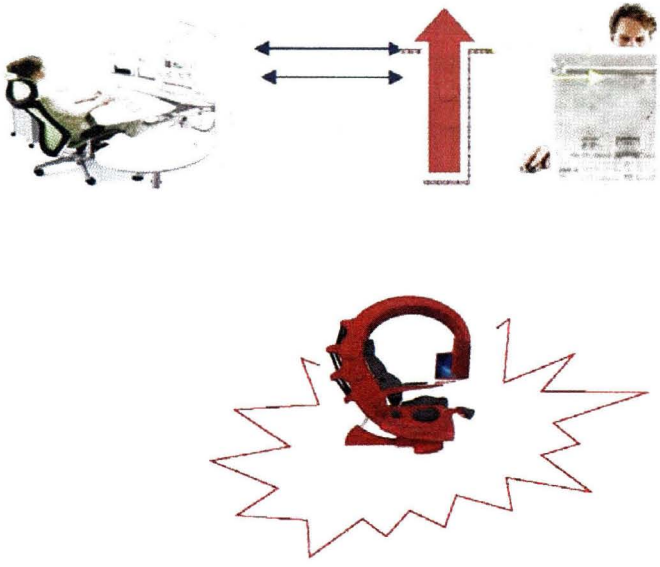


Figura No. 3 **Man in the middle**



10. DELITO DE *SPAM*

10.1 Aspectos generales del denominado *SPAM*

Mucho se ha cuestionado la naturaleza ilícita del *Spam*[64]. Algunos lo consideran como un derecho enmarcado dentro de la libertad de comercio, ya que el *Spam* se utiliza como un mecanismo de publicidad a menor costo, comparado con los medios publicitarios tradicionales. Otros, consideran que el *Spam* debe considerarse como delito, ya que afecta gravemente el Derecho a la Privacidad. En ese sentido, el legislador debe ponderar el derecho preferente entre: (1) Derecho a la privacidad y (2) Libertad de Comercio.

Con relación a la práctica de ***Spamming***, el autor Molina Salgado indica: "*La palabra spamming no tiene un significado en el idioma inglés, por lo que tampoco existe una traducción de dicho nombre al español. El término Spamming puede ser todavía desconocido para muchos, sin embargo, esta palabra seguramente será mejor conocida y empleada, más frecuentemente en los próximos años, en la medida que la práctica identificada con dicho nombre se desarrolle. El Spamming es la acción de enviar, a varias personas, correos electrónicos que contienen anuncios publicitarios y/o promociones comerciales, sin la previa solicitud de los receptores.*"[65]

64 Comúnmente se ha denominado "*Spam*" al "*correo no deseado*", también llamado "*correo basura*", que son los mensajes no solicitados, no deseados o de remitente desconocido. Este tipo de mensajes se envían de manera masiva o en grandes cantidades que perjudican al receptor. Se considera que la palabra "*Spam*" proviene de la segunda guerra mundial, cuando los familiares de los soldados les enviaban alimentos enlatados, dentro de los cuales se encontraba la carne enlatada marca "*Spam*", comida que en Estados Unidos era y es muy común. El correo no deseado también se puede dirigir por medio de mensajes de texto.

65 MOLINA SALGADO, Jesús Antonio, Delitos y otros ilícitos informáticos en el Derecho de la Propiedad Industrial, Editorial Porrúa, México 2003, Pág. 52. Este autor, al referirse a la violación de derechos de propiedad industrial y derechos de

La regulación del *Spam* varía en cada legislación. Por ejemplo, en la Ley número 28493 de Perú, ***"Ley que regula el uso del correo electrónico comercial no solicitado (SPAM)***", en su artículo 6º establece los casos en los cuales un correo electrónico comercial no solicitado es considerado ILEGAL. Los casos son los siguientes:

1. Cuando no cumpla con alguno de los requisitos establecidos en el artículo 5º de la Ley en mención.[66]

---

autor, por medio de la práctica *Spamming,* indica: "Sin embargo, en muchas ocasiones los emisores de los correos electrónicos publicitarios llegan a afectar los derechos marcarios y derechos de autor de terceros, por el uso indebido del *spamming*. Es decir, además de que el *spamming* puede ser molesto para muchos de los receptores de los mensajes, los emisores pueden hacer publicidad comparativa engañosa o tendenciosa, así como llevar a cabo actos de competencia desleal con relación a los productos o servicios de sus competidores. Asimismo, existen particulares y empresas que se aprovechan de una cuenta de correo electrónico, obtenida de alguna empresa o página famosa de Internet, para llevar a cabo el *spamming* y obtener un beneficio, haciendo creer a los receptores que existe una relación entre la página famosa y el producto o servicio que se promueve. Por ejemplo, suponiendo que existe una persona que obtuvo una cuenta de correo electrónico de la página www.yahoo.com (siendo en donde se prestan diversos servicios, como búsquedas, información sobre clima, viajes, noticias, etc.), ésta usa la dirección viajes@yahoo.com para promocionar su página en la que se ofrecen servicios de agencia de viajes (como reservación de hoteles y boletos de avión en todo el mundo). En este caso, los receptores de los mensajes supondrán que se trata de una promoción o publicidad de la empresa Yahoo, Inc., lo cual es totalmente falso."

66 El artículo 5º. De la Ley 28493 de Perú, establece: "Correo electrónico comercial no solicitado. Todo correo electrónico comercial promocional o publicitario no solicitado, originado en el país, debe contener:
a) La palabra "publicidad", en el campo del "asunto" (o subject) del mensaje.
b) Nombre o denominación social, domicilio completo y dirección de correo electrónico de la persona natural o jurídica que emite el mensaje.
c) La inclusión de una dirección de correo electrónico válido y activo de respuesta, para que el receptor pueda enviar un mensaje para notificar su voluntad de no recibir más correos no solicitados o la inclusión de otros mecanismos, basados en Internet, que permita al receptor manifestar su voluntad de no recibir mensajes adicionales."

2. Contenga nombre falso o información falsa que se oriente a no identificar a la persona natural o jurídica que transmite el mensaje.

3. Contenga información falsa o engañosa en el campo del "asunto" (o *subject*), que no coincida con el contenido del mensaje.

4. Se envíe o transmita, a un receptor que haya formulado el pedido, para que no se envíe dicha publicidad, luego del plazo de dos (2) días.

En España, la Ley 34/2002 de España, denominada "***Ley de Servicios de la Sociedad de la Información***" (***LSSI***) dispone: "*Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas. Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente. En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo, gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.*"

Inicialmente, el *Spam* fue incluido en la Iniciativa 4055 del Congreso de la República, Ley de Delitos Informáticos, específicamente en el artículo 12 que dece:

> *"Artículo 12. Envío masivo de correo electrónico. Quien, por medio de sistemas que utilicen tecnologías de la información, envíe anuncios no solicitados a las direcciones de correo electrónico de personas que carezcan de una relación preexistente, personal o comercial con el remitente, salvo que dicha persona haya expresado previamente su consentimiento o permiso, será penado con prisión de dos a cuatro años y multa desde cien hasta quinientas veces el salario mínimo legal vigente.*

La pena se aumentará en una tercera parte, en los siguientes casos:

a) Cuando el envío de mensajes electrónicos, publicitarios o de cualquier otra índole, tenga como fin la obtención de las direcciones de correo electrónico para crear una base de datos, para su posterior comercialización;

b) Cuando el envío de mensajes electrónicos, publicitarios o de cualquier otra índole, utilice una base de datos de direcciones electrónicas obtenidas sin autorización de los legítimos usuarios."

No obstante la regulación que se proponía en la Iniciativa 4055, la Honorable Comisión de Legislación y Puntos Constitucionales del Congreso de la República consideró pertinente suprimir el artículo 12 de dicho proyecto de ley, por considerar que se podría afectar la *libertad de comercio* y, por ende, que de regularse dicha figura delictiva se estaría abriendo la posibilidad de algún vicio que ameritara su denuncia de inconstitucionalidad. A nuestro juicio, es necesario que dentro de la legislación guatemalteca se incluya

normativa *anti-Spam,* debido a los efectos perjudiciales que éstas acciones producen en los usuarios y que afectan su privacidad y la disponibilidad del sistema.

La diferencia del *Spam,* con los medios tradicionales de publicidad en los buzones físicos, la podemos encontrar en lo siguiente:

1. El *Spam* se genera a través de un envío masivo de mensajes de datos de carácter comercial. De igual manera, surge lo mismo, en el envío de publicidad a buzones físicos.

2. En el *Spam*, los receptores no han pedido recibir esa información. De igual manera sucede con los buzones físicos.

3. En el *Spam* los emisores infringen la normativa vigente sobre recogida y tratamiento de datos de carácter personal, ya que se apoderan de información consistente en datos personales que existen en bases de datos y utilizan indiscriminadamente dicha información.

4. Con el *Spam* se genera el desbordamiento de la capacidad de almacenaje del buzón de correo electrónico, lo que implica la indisponibilidad del servicio de correo mientras se vacía la bandeja.

El sujeto activo o *spammer* utiliza diversos mecanismos para llevar a cabo su tarea de enviar correos masivos. En algunos casos se realizan estas actividades con la colaboración de los Proveedores de Servicio de Internet (ISPS), como sucede en el caso de la formalización de un contrato atípico denominado "***Pink Contract***",

que consiste en un acuerdo entre una persona individual o jurídica, denominada *Spammer*, y un Proveedor de Servicio de Internet, por medio del cual el ISP, a cambio de una remuneración (comúnmente muy onerosa), permite al *Spammer* realizar una actividad abusiva en la red.

Según Nava Garcés, el *Spam* puede presentarse de diferentes maneras, las cuales se citan textualmente de su fuente:

a) El llamado ***spam*** (***call spam***). Este tipo de *spam* se define como intentos de iniciación de sesión en masa no solicitados (es decir invitar solicitudes), tratando de establecer comunicación por medio de voz, vídeo, mensajería instantánea o cualquier otro tipo de sesiones de comunicación. Si el usuario debe contestar, el *spammer* procede a transmitir su mensaje mediante el tiempo real de medios de comunicación. Este *spam* es clásico de telemercadeo, es llamado *spam* mediante telefonía IP (protocolo de Internet por sus siglas en Inglés *Internet Protocol* IP) o "*spit*".

b) *Spam* de mensajería instantánea (***IM spam***). Este tipo de *spam* es muy similar al del correo electrónico, está definido por mensajes instantáneos no solicitados enviados en abundancia, cuyo contenido es el mensaje que el *spammer* desea transmitir; sin embargo, cualquier otra solicitud que genere contenido al aparecer en automático en la pantalla del usuario, será suficiente. Puede incluir también invitaciones con temas de cabecera largos o invitaciones que contengan texto HTML. Este tipo de *spam* es llamado *spam* sobre mensajería instantánea o "*spim*".[67]

67 Ob. Cit. Prueba Electrónica en Materia Penal. Pág. 49.

Lo cierto del caso, es que el *Spam* genera un perjuicio económico y la incomodidad de eliminar correos comerciales. El correo electrónico constituye un "dato personal"[68] que se proporciona a las personas con quienes el usuario desea tener comunicación, y no para recibir mensajes de contenido publicitario o comercial. Existe la agravante en el *Spam* cuando su contenido es, además, ofensivo o entraña actos ilegales, como calumnia, injuria o difamación. Así mismo, el *Spam* facilita la propagación de virus debido a que el usuario, por estar acostumbrado a recibir mensajes de remitentes desconocidos, podría abrir la puerta para la activación de cualquier tipo de *malware*.

Algunos estudiosos del tema consideran que el *Spam* puede solucionarse a través de códigos de conducta u otros instrumentos. Por ejemplo, los ISPS tienen la posibilidad de bloquear sus servidores a los *spammers*. Sin embargo, hoy en día, existen muchas técnicas para burlar los filtros de los ISPS, lo cual complica aún más la situación. Nuestro criterio consiste en que sí es necesario tener una normativa *anti-spam*, toda vez que la creación de filtros o sistemas de bloqueo son demasiado onerosos y debe ser política de Estado, a través del Congreso de la República, proveer mecanismos de seguridad a todo nivel, lo que incluye la regulación de normas *anti-spam*.

68 De conformidad con lo que establece el artículo 9 de la Ley de Acceso a la Información Pública, Decreto 57-2008 del Congreso de la República de Guatemala, un ***dato personal*** consiste en aquellos: "*relativos a cualquier información concerniente a personas naturales identificadas o identificables.*"

10.2 Datos estadísticos sobre el *Spam*

En el año 2010, la tasa media global de *spam* para ese año fue de 89,1%, lo que demostró un aumento de 1,4% en comparación con el año 2009. La proporción de *spam* enviada desde redes de bots fue muy superior para el año 2010, que representa aproximadamente el 88,2% de todo el *spam*.

El más grande cambio en 2010 fue en el envío de *spam* de lugares a medida, más *spam* fue enviado desde Asia y América del Sur a principios de ese año, pero al final del año la mayoría se ha enviado desde Europa, lo que representa aproximadamente el 30% del *spam* mundial.

A finales del año 2009, el 96% del *spam* enviado estaba en idioma inglés, pero este número ha disminuido lentamente durante el año 2010. Ha caído a un mínimo histórico de 90% en agosto del 2011, donde ha permanecido desde entonces. 10% del *spam* enviado se encuentra ahora en idiomas locales.

A pesar de muchos intentos de interrumpir las actividades de las *botnets* a lo largo del año 2010, al final del año el número total de robots activos volvió aproximadamente al mismo número a finales del año 2009, con aproximadamente cinco millones de *botnets* enviadores de *spam* en todo el mundo. Sin embargo, el número medio de correos electrónicos, no deseados, enviados desde cada *bot* disminuyó aproximadamente 85 correos electrónicos por *bot* por minuto.

Hubo, sin embargo, algunas excepciones especialmente en Rustock[69], que siguió dominando y fue responsable de 47,5% de todo el *spam* a finales del año.

69 Herramienta rootkit, difícil de detectar, se presume responsable de la instalación de redes zombies.

En 2010, la tasa media de *malware* en el tráfico de correo electrónico fue de 1284,2 mensajes de correo electrónico (0,352%), casi sin cambios en comparación con 1 en 286.4 (%) para el año 2009.

Aproximadamente el 23,7% del *malware* bloqueado en 2010 contenía un vínculo malicioso dentro del cuerpo del mensaje, en comparación con el 15,1% en 2009. En 2010 se fueron más de 339.600 ejemplares de *malware* distintos, identificados en los correos electrónicos bloqueados, lo que representa un aumento de más de cien veces en comparación con 2009. Esto es, en gran parte, debido al crecimiento en las variantes de *malware* polimórfico, por lo general, originados a partir de herramientas que permiten una nueva versión del código que se genera de forma rápida y sencilla. Un ejemplo de esto es la familia de troyanos Bredolab de propósito general, vinculados con la Pandex y botnets Cutwail, que representaron aproximadamente el 7,4% de todo el *malware* en correos electrónicos en 2010.

Fuente: *Message Labs Intelligence Anual report* 2010.