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

PROPUESTA DE PÓLIZA DE SEGURO PARA EL CIBER-RIESGO EN GUATEMALA

Karen Rocío García Ortíz
Asesorado por el Ing. Jorge Armin Mazariegos Rabanales

Guatemala, julio de 2009.

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

PROPUESTA DE PÓLIZA DE SEGURO PARA EL CIBER-RIESGO EN GUATEMALA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR:

KAREN ROCÍO GARCÍA ORTIZ
ASESORADO POR EL ING. JORGE ARMIN MAZARIEGOS RABANALES

AL CONFERÍRSELE EL TÍTULO DE

INGENIERA EN CIENCIAS Y SISTEMAS

GUATEMALA, JULIO DE 2009

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Inga. Glenda Patricia García Soria
VOCAL II	Inga. Alba Maritza Guerrero Spínola de López
VOCAL III	Ing. Miguel Ángel Dávila Calderón
VOCAL IV	Br. Milton De León Bran
VOCAL V	Br. Isaac Sultán Mejía
SECRETARIA	Inga. Marcia Ivónne Véliz Vargas

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Ludwing Federico Altán Sac
EXAMINADOR	Inga. Virginia Victoria Tala Ayerdi
EXAMINADOR	Ing. Edgar Estuardo Santos Sutuj
SECRETARIA	Inga. Marcia Ivónne Véliz Vargas

HONORABLE TRIBUNAL EXAMINADOR

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

PROPUESTA DE PÓLIZA DE SEGURO PARA EL CIBER-RIESGO EN GUATEMALA,

tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, en julio de 2008.

F. _____

Karen Rocío García Ortíz

Guatemala, 27 de enero del 2009.

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

El motivo de la presente es para informarle que he revisado el trabajo de graduación de la alumna Karen Rocío García Ortíz, titulado "**PROPUESTA DE PÓLIZA DE SEGURO PARA EL CIBER-RIESGO EN GUATEMALA**", a mi parecer cumple con los requisitos planteados como trabajo de graduación,

Atentamente,

Ing. Armin Mazariegos
Colegiado 5547
Asesor

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

Guatemala, 11 de Febrero de 2009

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

Respetable Ingeniero Pérez:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **KAREN ROCIO GARCIA ORTIZ,** titulado: **"PROPUESTA DE POLIZA DE SEGURO PARA EL CIBER-RIESGO EN GUATEMALA"**, y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

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

Atentamente,

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

ESCUELA DE CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÌA
ESCUELA DE CIENCIAS Y SISTEMAS
TEL: 24767644

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, de trabajo de graduación titulado ***"PROPUESTA DE POLIZA DE SEGURO PARA EL CIBER-RIESGO EN GUATEMALA",*** *presentado por la estudiante KAREN ROCIO GARCIA ORTIZ, aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"

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

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

Guatemala, 23 de juLio 2009

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

Ref. DTG.263.09

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al trabajo de graduación titulado: **PROPUESTA DE PÓLIZA DE SEGURO PARA EL CIBER-RIESGO EN GUATEMALA,** presentado por la estudiante universitaria **Karen Rocío García Ortiz,** procede a la autorización para la impresión del mismo.

IMPRÍMASE.

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Ing. Murphy Olympo Paiz Recinos
DECANO

Guatemala, julio de 2009

/cc

DEDICATORIA A:

DIOS Que este trabajo sirva para agradececer un poco de todo aquello que me ha dado.

MIS PADRES Edgar Javier García Jiménez y Rosa María Ortíz de García, que este trabajo los llene de satisfacción y orgullo, para que sepan que han hecho una buena labor.

MIS HERMANOS Edgar Estuardo, Gabriela María y Andrea Lucía, para que tengan un ejemplo más de superación y lucha por alcanzar las metas propuestas.

MI ESPOSO Fernando José Chavarría Recinos, que esté orgulloso de mí siempre.

AGRADECIMIENTOS A:

DIOS	Por darme la vida y la oportunidad de alcanzar una meta más.
JESUCRISTO	Por enseñarme el valor de terminar las tareas que comenzamos.
MIS PADRES	Por todo el apoyo recibido siempre y por insistirme para culminar esta carrera.
MI ESPOSO	Por estar siempre a mi lado y apoyarme a lo largo de este trayecto.
MI FAMILIA	Mis hermanos, mis primos, mis tíos y mis abuelos, por el apoyo recibido.
MIS AMIGOS	Por todo el apoyo recibido siempre.
ING. ARMIN MAZARIEGOS	Por darme el apoyo, las enseñanzas, la instrucción que necesitaba para presentar este trabajo de graduación.
LIC. EDUARDO ZUMBADO	Por el apoyo recibido en el área de especialización.
MI TIO HERBERT	Por el apoyo recibido para culminar este trabajo.

ÍNDICE GENERAL

íNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

Actuario Profesional titulado especializado en cálculos matemáticos y con conocimientos estadísticos, jurídicos y financieros, cuya principal misión es asesorar a las aseguradoras en todas aquellas materias técnicas financieras que son esenciales para determinar las tarifas, las primas del seguro, etc.[1]

Ciberespacio Es el lugar virtual del encuentro de las personas que utilizan las redes electrónicas.[2]

Copyright Es el derecho que ejerce cada autor sobre su propia obra, sobre su distribución y utilización.[3]

CEO *Chief Executive Officer*. Director ejecutivo. Es el encargado de máxima autoridad de la gestión y dirección administrativa en una empresa, organización o institución.[4]

CPU Unidad central de un ordenador que permite especificar cómo funcionará tu ordenador. Es el cerebro del tu computadora.[5]

Dicotomía División en dos partes.[6]

e-mail El e-mail, o correo electrónico, es uno de los servicios más usados en Internet, que permite el intercambio de mensajes entre las personas conectadas a la red de manera similar al correo tradicional.[7]

Firewall Mecanismo de seguridad en Internet frente a accesos no autorizados. Básicamente consiste en un filtro que mira la identidad de los paquetes y rechaza todos aquellos que no estén autorizados o correctamente identificados.[8]

Fraude Acto mediante el cual una persona, engañando a otra o aprovechándose del error en que se halla, obtiene ilícitamente alguna cosa o un lucro indebido.[9]

Gestión de riesgos La gestión de riesgos es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales.[10]

HIPPA *Health Insurance Portability and Accountability Act.* Ley de Responsabilidad y Transferibilidad de Seguros Médicos. Esta ley establece que si un empleador ofrece una cobertura médica, ésta no puede ser denegada al asegurado basado en su estado de salud. También protege los datos del asegurado para que nadie pueda utilizarlos negativamente.

Hacker	Experto informático especialista en entrar en sistemas ajenos sin permiso, generalmente para mostrar la baja seguridad de los mismos o simplemente para demostrar que es capaz de hacerlo.[11]
Hardware	Dispositivos físicos que comprenden un sistema de computación.[12]
Informática	Conjunto de conocimientos y herramientas científicas, técnicas y tecnológicas que se encarga del tratamiento racional y estructurado de la información por medios automáticos electrónicos digitales.[13]
Internet	Conjunto de computadoras o servidores, conectado en una red de redes mundial, que comparten un mismo protocolo de comunicación, y que presentan servicios a las computadoras que se conectan a esa red.[14]
Malware	Es un software que tiene como objetivo infiltrarse en o dañar un ordenador sin el conocimiento de su dueño y con finalidades muy diversas, ya que en esta categoría encontramos desde un troyano hasta un spyware.[15]
Organización empresa compañía	Conjunto de personas organizadas con un objetivo especifico. Está constituida por un grupo de personas que interactúan entre sí, deben desarrollar un conjunto de acciones, utilizar habilidades, enfoques y técnicas que posibiliten el logro de determinados resultados.[16]

Outsourcing Modalidad de contratación por la que una compañía contrata a otra compañía externa para realizar servicios que originalmente se realizaban en la propia empresa. El objetivo es reducir costes y mejorar los servicios.[17]

Póliza de seguro Es el instrumento con que se perfecciona y prueba el contrato. Debe contener todas las normas que de forma general, particular o especial regulan la relación contractual convenida entre el Asegurador y el Asegurado[18]

Retención Es la parte del riesgo que no se transfiere a una reaseguradora, y que es la parte que asume la aseguradora dependiendo de sus capacidades de pago, sus reservas y su solvencia económica.[19]

Sitio web Conjunto de páginas web alojadas generalmente en un mismo servidor, haciendo referencia todas ellas a una misma empresa, organización, o información.[20]

Software Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.[21]

Spyware Es un programa que obtiene información personal, la cual puede ser posteriormente utilizada para cometer fraude o para conocer los hábitos de navegación y/o consumo de un usuario. Generalmente el spyware se instala sin consentimiento del usuario.[22]

Tecnología Aplicación del conocimiento científico u organizado a las tareas prácticas por medio de sistemas ordenados que incluyen las personas, las organizaciones, los organismos vivientes y las máquinas.[23]

TI Tecnologías de Información. Aquellas herramientas y métodos empleados para recabar, retener, manipular o distribuir información. Se encuentra generalmente asociada con las computadoras y las tecnologías afines aplicadas a la toma de decisiones.[24]

TIR Tasa interna de retorno. Es la tasa de crecimiento que se espera generar de un proyecto.

VPN Valor presente neto. El valor presente neto de una inversión es la diferencia entre la suma del flujo de efectivo descontado que se espera de la inversión y la cantidad que se invirtió inicialmente.

VPN Red privada virtual (Virtual Private Network). Es una red de computadoras en la que algunos los enlaces entre los nodos son hechos con conexiones abiertas en redes más grandes, con la salvedad que estas conexiones no son públicas.

Virus Programa de ordenador que puede infectar otros programas o modificarlos para incluir una copia de sí mismo. Los virus se propagan con distintos objetivos, normalmente con finalidades fraudulentas y realizando daños en los equipos informáticos.[25]

Vulnerabilidad Fallo o agujero de seguridad detectado en algún programa o sistema informático que los virus utilizan para propagarse e infectar.[26]

RESUMEN

“Propuesta de póliza de seguro para el ciber-riesgo en Guatemala”, proporciona todos los elementos necesarios para plantear una póliza que cubra el ciber-riesgo o riesgo electrónico. Debido a las características tan especiales de este tipo de riesgo, se explican las herramientas especiales que pueden ser utilizadas.

El ciber-riesgo cubre toda la parte de informática que puede venir a la mente. Desde el robo físico de tecnología, cualquier desperfecto electrónico en un sistema hasta la información que transporta ese sistema y para quién está disponible esta información. Toda empresa debe estar conciente de los riesgos que corren y necesita sentirse protegida para proteger sus activos. Es por eso que encontramos en el mercado, desde hace varios años, programas de antivirus, cortafuegos, y políticas internas que protegen. Pero cada vez los atacantes encuentran maneras de escabullirse ante todo lo anterior.

Para completar esta protección que la empresa necesita sobre todos estos riesgos, encontramos el seguro. Toda empresa debe admitir, que aunque cumpla a cabalidad las políticas de seguridad, aún así es vulnerable a un ataque externo, e incluso interno. El seguro proporciona este porcentaje de protección que hacía falta. A esto se le llama, transferir los riesgos. Para una buena administración de riesgos, debe existir transferencia de riesgos. Una empresa no puede ser especialista en todas las cosas y por eso transfiere los riesgos a otra empresa que sea especialista en riesgos de tipo electrónico.

A pesar de que encontramos la necesidad de este tipo de seguro, en Guatemala no encontramos ninguna aseguradora que ofrezca este tipo de seguro y es porque no se siente equipada para ampararlo pero ya existen empresas especializadas en auditoría externa y puede realizar el trabajo que no dominan las aseguradoras guatemaltecas.

En el presente trabajo, existe una propuesta de una póliza de seguro para que cualquier aseguradora pueda ponerlo en práctica con las modificaciones que considere necesarias.

OBJETIVOS

General

Proponer una póliza de seguro que cubra el ciber-riesgo.

Específicos

1. Definir lo que implica administración de ciber-riesgos.
2. Definir lo que implica crear una póliza de seguro para un ciber-riesgo.
3. Definir el panorama local e internacional respecto a las pólizas de seguro para ciber-riesgos.
4. Crear una póliza de seguro que cubra el ciber-riesgo.

INTRODUCCIÓN

Desde el invento de la computadora, hasta el día de hoy, la sociedad ha sufrido muchos cambios y estos cambios se han dado de una forma acelerada. Luego del invento de la computadora surgió la red de computadoras, y el hombre lograba conectar dos o más computadoras para tener comunicación entre ellas. Luego surgen las redes de redes de computadoras, para dar luz a lo que ahora conocemos como Internet, una red tan amplia que abarca todo el mundo. Ahora una persona desde Guatemala se puede comunicar con cualquier otra persona en cualquier otra parte del mundo. Esto ha abierto las puertas y ha eliminado las fronteras entre países permitiendo transacciones de comercio a través de todo el mundo. Así como se han abierto las puertas para la comunicación y el comercio, también los riesgos se han multiplicado.

Así como ha ido evolucionando la tecnología, también han ido evolucionando los riesgos que ésta acarrea, cayendo por fin en un mundo sin barreras y desprotegido. Los riesgos que se corren a través de Internet son muy distintos a los que se corren al ocurrir un incendio, un accidente, un robo a mano armada, entre otros; los bienes que se aseguran no son los mismos. No son los mismos porque el bien que se arriesga en un incendio, un accidente, un robo a mano armada es tangible, tiene un valor en el inventario de la empresa; pero cuando se arriesga en Internet, se arriesgan bienes muchas veces que no son tangibles, que no están en el inventario de la empresa, como por ejemplo: ¿cuánto cree usted que puede valer la información que tiene almacenada en su computadora de la oficina? No solamente eso, ¿cuánto cree que puede valer la información que tienen en un banco como cuentas, teléfonos, direcciones?

Para poder responder estas preguntas, lo primero que debe definirse es realmente ¿cuáles son todos los riesgos que se corren a través de Internet y no solo a través de Internet sino a través de una computadora? Una vez definido, la conclusión es obvia: la necesidad de protección sobre los riesgos a los que está expuesto a través de Internet. Alguien puede decidir no correr riesgos y no realizar ninguna transacción que sea de tipo electrónico, pero aunque no quiera utilizar el sitio web de su banco, el sitio web igual está expuesto con su información a través del Internet. Si no desea realizar una transacción de comercio electrónico, no arriesga pero tampoco obtiene los beneficios de realizarla. Para ser competitivos en esta industria se deben tomar los riesgos, pero administrarlos con sabiduría.

Una de las formas más sabias de administrar los riesgos, es transferirlos y dejar que alguien más se encargue de ellos. Este es el papel que debe cumplir una aseguradora. Una aseguradora debe ser capaz de proporcionar el marco adecuado para la administración del riesgo y además poder cuantificar el valor del bien asegurable. La aseguradora debe facilitar una póliza de seguro que cubra este tipo de riesgos, y definirla de tal modo que no existan ambigüedades en la misma.

El presente trabajo de graduación pretende contextualizar los riesgos que se corren a través del uso de la computadora y a través de Internet; cómo una empresa puede administrar y protegerse de estos riesgos; cuál es el panorama internacional de este tipo de riesgo y las aseguradoras que lo cubren; y, proponer una póliza de seguro que cubre este tipo de riesgo.

El presente trabajo no pretende, en ninguna manera, que la póliza de seguro sea totalmente aplicable debido a la amplitud de contenido e investigación que esto puede abarcar. Sin embargo, la póliza de seguro que aquí se propone es buena para que cualquier aseguradora guatemalteca que esté interesada pueda, con sus respectivas modificaciones, aplicarla fácilmente.

1. CIBER RIESGO

1.1. Panorama actual

Para conocer la situación de los peligros y amenazas a las que se está expuesto actualmente en el Internet y en todo el ambiente en el que se desarrollan las interacciones del ciber-espacio se enfocan tres puntos:

- La situación actual del crimen en el ciber-espacio.
- Un panorama general de la autenticación del correo electrónico.
- La lucha para sobrevivir en el ciber-espacio.

1.1.1. Ciber-crimen

Se puede definir el ciber-crimen esencialmente como difundir la tecnología y sistemas de información para cometer hurto, extorsión, robo de identidad, fraude y, en algunos casos, espionaje corporativo. Se debe tomar en cuenta que existen diferencias notables entre un delincuente de la calle y un delincuente en el ciber-espacio, ya que estos últimos permanecen invisibles y sin rastro.

El ciber-crimen es penetrante, no discrimina, además de estar incrementando dramáticamente; robo de grandes sumas de dinero, tanto de individuos como de grandes corporaciones. Gran cantidad de personas están cometiendo ciber-crimen debido al riesgo mínimo que se corre y a los bajos requisitos de habilidades para cometerlo, además de que promete tener ganancias extremadamente altas.

Es impresionante la cantidad de información comprometedora que se puede encontrar en Internet simplemente realizando una búsqueda sobre el tema, tales como números de tarjetas de crédito, cuentas financieras, entre otros. Aún así las instituciones financieras motivan a los clientes a utilizar comercio electrónico y banca en línea para reducir sus costos de operación. Algunas de estas instituciones fallan al no invertir en seguridad para sus sistemas de información pues simplemente proveen al cliente de un usuario y una contraseña para la autenticación, haciendo que los programas de detección de teclado sean altamente eficientes contra sus víctimas.

La ley está mal equipada para prevenir la gran ola de crecimiento del ciber-crimen. Entrenamiento insuficiente, recursos limitados (personal, equipo, presupuesto), barreras en la cooperación, remedios legales anticuados o inexistentes, falta de cooperación entre países y paradigmas culturales crean un terreno fértil para el éxito del ciber-crimen.

Muchas víctimas no parecen entender la relación que existe entre sus pérdidas y el ciber-crimen; peor aún, ven esto como un crimen imposible de investigar y perseguir. Para que el ciber-crimen sea reconocido como un tema de importancia, debiera existir una comunidad reforzada por la ley en donde las víctimas pudieran reportar dichos incidentes.

1.1.2. Correo electrónico

El correo electrónico fue concebido en un mundo muy distinto al que se vive hoy en día. Era un mundo pequeño, existía una comunidad pequeña y realmente no había que preocuparse demasiado por los delincuentes. Generalmente, si alguien hacía algo mal se podía tratar con medios sociales; “evitar” es muy eficaz en comunidades pequeñas. El correo electrónico es una de las primeras tecnologías, fue concebida antes que el Internet tuviera auge; debido a ello, las tecnologías sobre las que funciona el correo electrónico no son las adecuadas para la seguridad.

Realmente ahora existen dos tecnologías de comunicación muy importantes: la Web (una tecnología por medio de la cual se saca información) y el correo electrónico (una tecnología por medio de la cual, se ingresa información).

El correo electrónico tiene un defecto fundamental desde sus inicios: la falta de autenticación. Esto significa que cualquiera en el Internet puede, en teoría, enviar un correo electrónico a cualquiera aparentando ser una tercera persona. Por ejemplo, no existe ninguna forma de probar que un mensaje que dice ser del banco, realmente tiene algo que ver con el banco.

1.1.3. La lucha por sobrevivir

Existe una dicotomía real, pero no exacta, de complejidad versus seguridad; es en cierto grado mensurable y las noticias en ese frente no son buenas. La industria de software vende productos que no calzan naturalmente y que al copiarlos, no guardan completa fidelidad. Para continuar haciendo dinero, el surtidor de software debe vender actualizaciones, mantenimiento, o ambas. El mantenimiento se vende mejor cuando el producto es inestable o difícil de usar; la necesidad de mantenimiento es admitir la complejidad del software. Nuevas características, que son como para obligar de cualquier manera a los usuarios complacidos para hacer una recompra del producto que ya tienen, tienden a ser por lo menos lineares (10 nuevas características) si no es que geométricos (10% de nuevas características)[27]. Ausentes de perfección, cada nueva característica viene con nuevos modos de fallo, y las características pueden interactuar entre ellas algunas veces; por lo tanto, el número potencial de modos de fallo naturalmente puede crecer más rápido que el número de características.

Se estima que del veinte al cincuenta por ciento de las composturas para fallos conocidos, introducen fallos desconocidos[28]. Por lo tanto, hablando racionalmente, viene una época donde muchos de estos fallos deberán quedarse permanentemente en su lugar y completamente documentados en lugar de arreglarlos. Exceptuando los inusuales, oscuros y casos especiales de defectos de seguridad que se introducen intencionalmente en los productos, los defectos de seguridad son un subconjunto de todos los defectos no intencionales y van a crecer junto con la complejidad de un sistema. El problema es que para cada falla de seguridad que permanezca en un sistema con una completa documentación dibuja un punto de atención en el producto y sus usuarios. Si el estimado es correcto (que del veinte al cincuenta por ciento de las composturas para fallos conocidos, introducen fallos desconocidos) y dejar un fallo de seguridad en su lugar es un anatema, entonces solo podemos concluir:

La existencia distribuida de fallos de seguridad es una característica permanente del mundo digital. Mientras más complejo sea el producto, tiene más probabilidades que se de la característica anterior.

Es muy difícil hacer un producto de seguridad que no sea objeto de mal uso. En realidad, los ataques en contra de productos de seguridad parecen estar aumentando más rápidamente que todos los productos de software en el agregado, haciendo que los productos de seguridad sean sobre representados, estadísticamente hablando, blancos de ataques.

Los productos de seguridad son, por ejemplo, hechos específicamente contra los ataques de negación de servicio. La política es deshabilitar las cuentas después de tres intentos fallidos de acceso en un intervalo corto. Entonces, alguien podría simplemente hacer un intento fallido para todos los usuarios que tiene el sistema (y mientras más grande sea el sistema, es más fácil encontrar usuarios reales). Para combatir estos ataques de conjeturas, alguien emplea pruebas computacionales de autorización realmente caras. Ahora bien, si el costo para iniciar autorización es menor que el costo para negarla, entonces nos encontramos con la asimetría de la cual se compone la negación de servicio.

Para hacer un producto que cualquiera quiera tener (y cualquiera pueda tener), ese producto debe ser vulnerable a caer. Este no es un insulto específico, para aclarar, pero estos productos vulnerables tienden a ser la opción del mercado masivo. Esto es especialmente cierto en productos de software, ya que crecen más rápidamente en complejidad que lo que los usuarios crecen en habilidades. La ley de Moore dice que la intensidad computacional crezca el doble cada dieciocho meses[29], pero ningún usuario empieza a pensar el doble de rápido en dieciocho meses.

Los dispositivos de consumidor, en esta época de Internet, perciben un mayor porcentaje de valor si su facilidad de conexión es mayor. La ley de Moore duplica el desempeño del CPU por dólar cada 18 meses, pero la capacidad de almacenar información se duplica cada 12 meses, y ancho de banda más rápido se duplica hasta cada nueve meses. Esto significa que el dispositivo electrónico económicamente óptimo, incluyendo la computadora, cambia a través del tiempo en dirección a tener más datos moviéndose más a menudo. Si esta tasa de 18:12:9 es razonablemente exacta y se mantiene por diez años, obtenemos 2 órdenes de la magnitud de CPU, pero 3 de capacidad de almacenamiento y 4 de ancho de banda. Si mantenemos el diseño de la computadora constante, una década con este crecimiento, produce 10 veces más datos en la computadora de lo que tenemos ahora.

Si esta predicción de enriquecimiento de datos es cierta, no tiene alguien que ser un experto para imaginarse que el colapso entre datos y CPU será el foco principal para ataques que transiten en redes más veloces. Probablemente esto ya sea una realidad, en que una computadora portátil perdida es un costo financiero menor por reponer, pero los datos que ésta contenía ni es menor, ni tiene costo financiero aparente. Este es un punto importante a tomar en cuenta, ya que marca la diferencia entre el mundo digital y el físico. Si se roban los datos de una computadora, queda completamente funcional; nadie podrá notar inmediatamente que esa información está perdida (así como cuando se roban un carro en la carretera), pero descubrirán que robaron los datos solamente si es utilizada en una forma que sea visible para la víctima. En el mundo digital, no existe el principio de exclusión (si yo tengo tu carro, tu no lo tienes; pero si yo tengo tu información, tu también).

La complejidad se eleva debido a que el interés personal de los vendedores de software lo demanda. Los avances de magnitud que hay en los laboratorios hacen mejoras en las computadoras y los dispositivos de computadoras, haciéndolos más disponibles para mayor número de personas. La tasa entre la habilidad (por persona) y la potencia (por computadora) está cayendo rápidamente, y no podría ser diferente. Como el precio por el hardware está cayendo, son los datos los que asumen la preponderancia de valor. Los ladrones robaban banco cuando allí era donde estaba el dinero; ahora roban datos, y sería sorprendente si no lo hicieran. Como cualquier mercadólogo y oficial de inteligencia sabe, la fusión de datos incrementa el valor de los datos que realmente tengo.

Alguien podría sugerir que el público general no sabe lo vulnerable que es esto, pero este estado de ignorancia está expandiéndose cada vez más; y, mientras que el público general sienta que ayuda menos, más se siente necesitado de protección. El público siente que no ayuda, lo que amortigua la iniciativa por ayudar.

Cuando los atacantes asumen poco o ningún riesgo al atacar, ellos van a atacar simplemente. Cuando los atacantes puedan utilizar la automatización, ellos van a atacar con vigor. Los atacantes pueden ganar la batalla con las armas levantadas, cuando sus costos operacionales son solamente una pequeña fracción de los costos operacionales de los que se deben defender. Los atacantes pueden montar asaltos sin mostrar señales de advertencia, por lo que los que defienden deben estar siempre en alerta máxima. Todas estas cosas pueden obtenerse en la arena digital, y cuando eso suceda, la única estrategia es esperar lo peor.

Esperar lo peor requiere inteligencia, la inteligencia requiere vigilancia, y la vigilancia requiere mecanismos para vigilar y que esto no dependa de la intención o la decisión de aquellos que están bajo vigilancia. El público está demandando una protección que se siente incapaz de obtener por sí solo. Está empeñado en la idea de que los malos resultados vienen de un error de alguien, a quien se le puede asignar la responsabilidad. Tiene erróneo el principio (ten cuidado de ti mismo) pero correcta la práctica (asignar el riesgo a aquellos con mayor capacidad para manejarlo). Todo lo anterior hace que pongan en el extremo último de sus prioridades vigilar y asignan el deber (y la responsabilidad) de proteger a aquellos con mayor número de recursos, no importando si es lo correcto o no.

Si el futuro nos depara más datos; si esos datos son transferibles y son la única tienda real de valor, entonces hemos venido a cumplir la predicción de Grace Murray Hopper 1987:

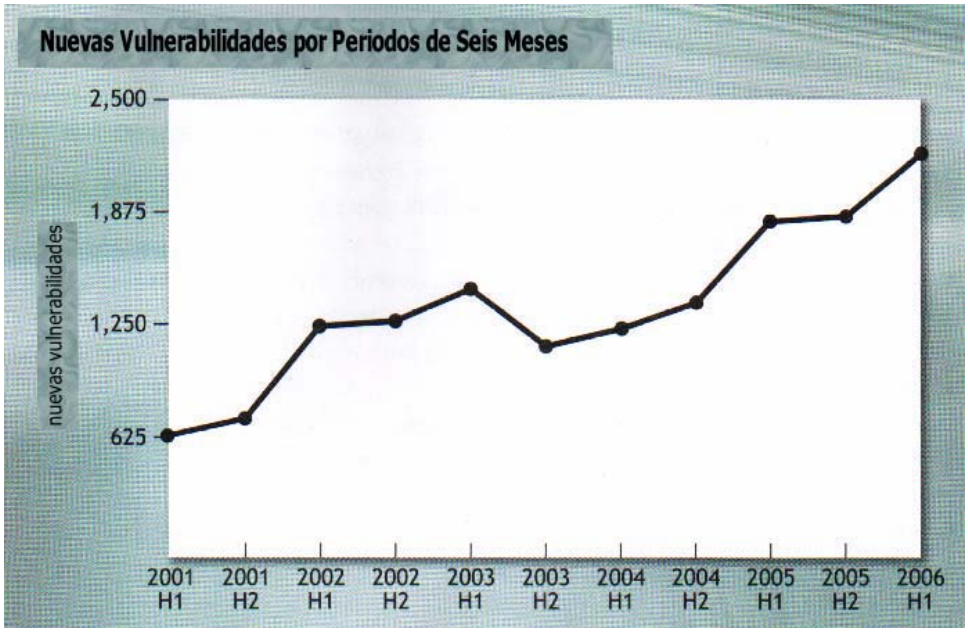
“Algún día, en la hoja de balance corporativo, habrá alguna entrada que diga: ‘Información’; en donde, en la mayoría de los casos la información será más valiosa que el hardware que la procesa.”[30]

La relevancia de los datos en la hoja de balance se puede calcular por medio del valor de liquidación de una compañía dedicada netamente a la información. Si vamos a cuidar algo al punto de proteger el activo (valor de datos), entonces debemos seleccionar una unidad para observar. Para lograrlo se debe formular una pregunta abierta: ¿es la unidad a observar una porción de datos, o es la unidad a observar una persona? ¿Se construye la estructura para vigilar datos o personas? Para resolver esta pregunta, se tienen aspectos resueltos, a lo que se le llama usualmente *DRM (Digital Rights Management)*, gerencia de datos vigilados, pero está obstaculizado por los datos que residen en una ubicación hostil.

La complejidad, a la que la industria de software llama progreso, está generando más fallas sutiles. Esto es un error físico, no humano. La unidad de volumen de código puede estar mejorando pero la cantidad de código que se puede ejecutar por unidad de tiempo o por x cantidad de dinero está creciendo en tarifas geométricas. Por lo tanto, para el riesgo constante que existe, la funcionalidad del software debe crecer a tarifas geométricas, para que lleguen a estar al mismo nivel. Se debe correr más y más rápido para estar al mismo nivel. Esta es la realidad en lo que se refiere a competencia, y en términos de seguridad.

Mientras observamos el siguiente gráfico, debemos recordar que en el mismo período de tiempo ha habido incrementos espectaculares en la compra de software para evitar las vulnerabilidades y la curva aún continúa creciendo.[31]

Figura 1. Nuevas vulnerabilidades por períodos de seis meses



Fuente: Geer, Daniel E. (2006). **"Crime online"**. Acm Queue, November 2006 Vol.4 No. 9, Pág. 47

Ahora que existe una idea más concreta acerca del panorama actual del Internet, podemos decir que en el Internet corremos riesgos altos, riesgos de comprometer nuestra información, riesgos de dañar nuestra reputación, riesgos de comprometer la información importante de nuestros clientes, entre otros.

1.2. Riesgo

El riesgo puede definirse como una combinación entre la probabilidad que ocurra un evento y sus consecuencias. En todo tipo de empresas, existe la probabilidad que ocurran eventos y consecuencias de estos eventos que constituyen oportunidades para beneficio o amenazas para el éxito.

Un ejemplo del riesgo es un hombre que salta fuera de un avión con un paracaídas en su espalda. El hombre puede no estar seguro si el paracaídas se va a abrir o no. El está tomando el riesgo puesto que está expuesto a una incertidumbre. Si el paracaídas falla al abrir, él podría morir. Si el hombre saltara del avión sin paracaídas, tiene la certidumbre que va a morir, por lo que no corre ningún riesgo.

Un sinónimo de incertidumbre es ignorancia. Enfrentamos riesgos porque somos ignorantes sobre el futuro. Después de todo, si fuésemos omniscientes, no existirían riesgos. Como la ignorancia es una experiencia personal, el riesgo es obligatoriamente subjetivo.

Otro ejemplo es un hombre que llega a un aeropuerto para tomar un vuelo. El clima es amenazante, y es posible que su vuelo sea cancelado. Existe la incertidumbre del status del vuelo y él se expone a esa incertidumbre. Sus planes de vuelo serán interrumpidos si el vuelo fuese cancelado, por lo tanto, debe enfrentar el riesgo.

Una mujer también llega al aeropuerto para tomar el mismo vuelvo. Ella llamó primero y confirmó que su vuelo no había sido cancelado. Para ella existe menos incertidumbre, por lo que corre menor riesgo.

En este ejemplo, existen dos individuos expuestos al mismo evento. Como ellos tienen diferentes niveles de incertidumbre, ellos tienen diferentes niveles de riesgo. El riesgo es subjetivo.

El riesgo es una experiencia personal, no solamente porque es subjetivo, sino porque las consecuencias se sufren individualmente. De cualquier forma, se puede hablar de compañías tomando riesgos, en la actualidad, las compañías son conductores del riesgo.

1.3. Ciber-riesgo

Un nuevo tipo de riesgo se está haciendo notar con los gerentes de riesgo a través del mundo. Se le nombra ciber-riesgo, riesgo de comercio electrónico, riesgo informático, riesgo electrónico, riesgo de tecnología o riesgo tecnológico[32]. El ciber-riesgo puede definirse como riesgos, responsabilidades y soluciones asociadas con procesos e interacciones electrónicas que se presentan de conducir actividades de negocio a través de redes de computadoras.

Anteriormente se presentó el panorama actual del Internet y es visible que se corre muchos riesgos, tanto a nivel individual como en corporaciones completas.

Miles de compañías operan en un ambiente de negocios dependiente de una red. Para prosperar, las compañías delegan más y más en los proveedores de Internet, proveedores de servicios de aplicación y socios. Al hacer esto, las corporaciones son más eficientes, pero se exponen a mayor peligro con ladrones expertos que amenazan redes completas de una organización.

Este peligro emergente tiene el potencial de hacer estragos en la reputación profesional de una organización y destruir al consumidor y la confianza de los socios.

El Internet es sinónimo de cambio, y de hecho, ha definido el cambio en nuestra sociedad hoy en día. Todos los negocios están trabajando duro para determinar como enganchar el poder del Internet; y el cambio, solamente está comenzando.

El Internet promete un ambiente sin frontera, económicamente global, permitiendo la comunicación y el comercio electrónico instantáneo de manera impensable aún unos cuantos años antes. Pero la apertura del Internet trae nuevas responsabilidades tanto como vulnerabilidades sin precedente para aquellos que quieren destruir o robar activos vitales o interrumpir el negocio.

Los atacantes no solo tienen fácil acceso a los activos financieros, sino también tienen oportunidades más abundantes y mejores para el robo de información, sabotaje, espionaje industrial e interrupción de negocio. La dependencia en sistemas de información obliga al negocio a crecer, pero las dependencias e independencias crean vulnerabilidades dañinas.

La dependencia de Internet permite que los atacantes puedan:

- Esconder su identificación.
- Evadir riesgo físico al actuar a través de terminales remotas.
- Explotar las vulnerabilidades antes de que su existencia sea conocida por los expertos de seguridad.
- Utilizar vulnerabilidades recién descubiertas y hazañas asociadas desarrolladas por otros hackers que están comunicados en el inframundo hacker.
- Tomar ventaja de las interdependencias inherentes de casi todas las redes.
- Usar sistemas inseguros, como herramientas de ataque, de lugares sin relación con la empresa.

La tecnología es un gran ecualizador. Desafortunadamente, un simple atacante con un computador y acceso a Internet tiene las herramientas para atacar incluso al blanco mejor defendido y distante. Como parte de la infraestructura crítica de una nación, las instituciones financieras enfrentan una amenaza dañina y creciente.

Almacenar información electrónicamente y compartirla en red permite enviar, recibir y acceder rápidamente a la información desde cualquier punto del mundo. No tomando en cuenta los beneficios que la tecnología aporta al mundo empresarial, han surgido nuevos riesgos que se debe considerar:

- Robo o manipulación de información privada.
- Virus.
- Fraude.
- Revelar información privada de clientes.
- Infracción de copyright.
- Negación de servicios.

Las amenazas contra la seguridad continúan creciendo, haciendo difícil para las compañías mantener la paz con un número cada vez mayor de riesgos. Mientras estas compañías podrían preferir evitar todos los riesgos de seguridad y privacidad TI (Tecnología de Información), esto es extremadamente difícil, si no es que imposible. Por lo tanto, tener estrategias efectivas de administración de riesgos (incluyendo transferencia de riesgo a seguros) es un paso importante para administrar las exposiciones asociadas con hacer negocios en el mundo interconectado de hoy. Incluso con la mejor seguridad de datos, los riesgos responsables nunca van a ser cero.

El incremento de la dependencia en procesos electrónicos y tecnología basada en red ha dado inicio a nuevos retos para compañías de todos los tamaños y formas. El mayor reto es encontrar la forma de manejar ciber-riesgos.

La continua exposición de ciber-riesgos, impacta en todo aspecto de la organización (activos, operaciones, finanzas y capital). El ciber-riesgo corre muy dentro de la organización e incluye riesgo tanto para activos físicos como no físicos. Mucha gente se preocupa por el hardware y el hardware es la parte fácil de la ecuación, lo que realmente importa son los datos y la disponibilidad de la red. Desafortunadamente, muchas compañías todavía piensan que están envueltas en activos físicos.

Existe preocupación por que los ataques en contra de una red cada vez sean más sofisticados. Aún con este crecimiento, las personas están dispuestas a tomar mayores riesgos y adoptar nuevas tecnologías.

1.4. ¿Qué se ha hecho hasta ahora?

La mayoría de las organizaciones han adoptado un enfoque reactivo ante la seguridad de la información ("no me preocupo hasta que algo sucede"), debido a la falta de conciencia directiva ante el retorno de cualquier inversión efectuada en asegurar los activos de información de la organización.

1.4.1. Políticas para mitigar el riesgo

Como se ha mencionado, la seguridad toma diferente significado en el mundo interconectado de hoy. Tener sistemas seguros de información es un proceso complejo que envuelve varios factores:

- Avances tecnológicos continuos
- Cambios estratégicos como outsourcing de TI (Tecnología de Información).
- Vulnerabilidades de seguridad en productos de hardware y software.
- Adquisiciones que requieren integración de diferentes sistemas de un modo seguro.
- Leyes y regulaciones de seguridad y privacidad
- La naturaleza cambiante del perfil de amenaza electrónica.

El concepto de gestión de riesgos se deriva de la responsabilidad que tienen las empresas en el buen gobierno corporativo de sus sistemas de información; en concreto, podríamos definir los ciber-riesgos como: Las pérdidas y responsabilidades que una organización afronta como resultado de usar Internet, sistemas informáticos y correo electrónico.

Gestión de riesgos significa buscar de forma proactiva los retos que el ambiente actual presenta. Esto indica que la mejor forma de empezar puede ser realizando una evaluación de los riesgos que existen para la empresa. El ciber-riesgo debe ser parte de una estrategia de administración de riesgos que abarque todo en la empresa; estrategia que incluye evaluaciones de riesgo, el establecimiento de políticas y procedimientos relacionados con seguridad, y la privacidad de red. El mejor enfoque para mitigar el ciber-riesgo incluye una combinación de control de pérdidas, lenguaje de control, retención y transferencia de riesgo a una póliza que lo cubra.

Las actividades que implica la administración de riesgos son:

- Defensa: se refiere a cómo el sistema está protegido de ataques y usualmente se utilizan contadores o controles para medirlo.
- Prevención: involucra reducir vulnerabilidades e implementar medidas para reducir ataques.
- Detección: incluye identificar y caracterizar cualquier intento de ataque, ya sea mientras ocurre, o después.
- Respuesta: incluye tomar medidas correctivas en respuesta a un ataque para detenerlo o reducir su impacto.
- Respuesta y recuperación: se refiere a cómo y qué tan bien es mitigado el daño y reparado, y también a cómo y qué tan bien la información y la funcionalidad se recuperan cuando el ataque fue exitoso.

La problemática relacionada con una adecuada gestión de riesgos tecnológicos ha estado condicionada por los siguientes factores:

- Los ciber-riesgos de la organización no han sido tradicionalmente cubiertos adecuadamente, ni por las medidas de seguridad pertinentes ni por la cobertura de riesgo ofrecida por las pólizas de responsabilidad tradicionales.
- La protección contra las pérdidas en la confidencialidad, integridad y disponibilidad de la información es cada vez más una preocupación para todas las organizaciones.

1.4.2. Análisis de riesgos y la toma de decisiones

Un Análisis de Riesgos es un procedimiento de ayuda a la toma de decisiones, cuyos destinatarios finales son los responsables máximos de la organización (Dirección General). Su objetivo último es estimar el valor de los activos de información y sus riesgos asociados.

Sus resultados constituyen, sobre todo, una guía para que la organización tome decisiones sobre su nivel de riesgo: cual es el nivel considerado razonable por la organización y qué controles o procesos de seguridad serán los más adecuados para conseguirlo.

Tras conocer los riesgos, la organización deberá decidir entre las siguientes estrategias de negocio:

- Mitigar el riesgo, mediante la implantación y mantenimiento de controles de seguridad que reduzcan al máximo estos riesgos y que los mantengan a un nivel aceptable.
- Asumir ciertos riesgos: ya que sus consecuencias acarrean menor coste económico y estratégico que la inversión necesaria para su reducción.
- Transferir estos riesgos, bien a un prestador de servicios especializado (outsourcer) mediante un Acuerdo de Nivel de Servicio (SLA) con responsabilidad asociada, o bien, mediante la contratación de una póliza de riesgo electrónico.

2. CREACIÓN DE UNA PÓLIZA DE SEGURO PARA EL CIBER-RIESGO

2.1. El seguro

Se han escrito muchas definiciones, todas más o menos significan lo mismo, unas más, otras menos, definen lo que es el seguro, pero entre ellas, la que mejor encaja los aspectos que rigen esta disciplina es la siguiente: El seguro es la cobertura recíproca y colectiva, por parte de muchas economías amenazadas igualmente por peligros comunes, eventuales y tasables en dinero, y por las cuales el asegurado ha pagado una suma de dinero llamada prima para que esta responda en el eventual caso de que suceda un siniestro amparado por la póliza de seguro. En la definición anterior quedan unidos todos los elementos que hacen que el seguro sea una realidad.

2.1.1. Contrato de seguro

Es un documento por intermedio del cual la compañía o el asegurador, se comprometen a pagar en dinero, a reparar o a reponer cualquier bien o bienes asegurados, que se encuentren claramente identificados en las condiciones particulares de la póliza, y que aparecen como amparados, sean o no propiedad del asegurado o que se encuentren bajo su responsabilidad o en custodia y que sufran algún daño o pérdida de carácter inmediato, fortuito, accidental e involuntario.

Es una condición sin discusión que las pérdidas o daños que sufran los bienes asegurados, sean a consecuencia de una o varias de las coberturas, riesgos o peligros que aparezcan claramente cubiertos o amparados en la póliza del seguro.

Se debe tener muy claro y entender que el contrato de seguro es un "contrato de buena fe", esto quiere decir que tanto el asegurado como la compañía, actúan de buena fe. La compañía acepta por su lado como buena la declaración del asegurado cuando manifiesta su interés asegurable sobre los bienes que propone le sean asegurados, como ya se dijo, sean o no de su propiedad declarándolos en buen estado, su buen funcionamiento y su preexistencia; generalmente la compañía, no pre-juzga ninguna falsedad en esa declaración, sin embargo le asiste el derecho de aceptar o rechazar cualquier solicitud de seguro que a su juicio no sea ni clara ni precisa, puede inspeccionarlos antes de rechazarlos o aceptarlos, según se desprenda de la inspección.

El asegurado manifiesta su confianza y acepta de buena fe el documento llamado póliza de seguro, que la compañía le extiende, en donde está escrito que se compromete y responsabiliza a indemnizar al asegurado de cualquier pérdida o daño que sufran los bienes allí identificados, siempre y cuando el asegurado haya cumplido con todos los requisitos especificados en el contrato, que no haya violado ninguna disposición del mismo y mucho menos que la reclamación presentada por el siniestro acaecido sea de carácter fraudulento o violatorio contra alguna o algunas leyes vigentes del país, tanto civiles como penales, si así fuere el reclamo es válido, en caso contrario el seguro puede ser declarado nulo y sin valor legal.

Se dice que el contrato de seguro es un contrato de adhesión, esto significa que el asegurado se adhiere a todas y cada una de las condiciones impresas en la póliza, que la compañía emite y le entrega. Es un documento registrado ante las autoridades fiscalizadoras de la Superintendencia de Bancos de Guatemala, entidad que controla a las compañías de seguros y de fianzas. El asegurado no puede cambiar dichas condiciones.

Elementos del contrato de seguro

- Elementos personales
    - Asegurador
    - Asegurado
        - Beneficiario
        - Intermediario
        - Reasegurador
- Elemento reales
    - Riesgo
    - Interés asegurable
    - Prima
- Elementos formales
    - Póliza

2.1.1.1. Asegurador

- Es la Compañía que emite la póliza en un Seguro Directo.
- Las empresas de seguros de naturaleza mercantil, cualquiera que sea el origen de su capital, solo pueden constituirse y organizarse como sociedad anónima, conforme a las leyes del país y para tal efecto citamos que la Sociedad Anónima, es una sociedad formalmente mercantil, de carácter capitalista, se identifica una denominación, tiene un capital dividido y representado en títulos llamados acciones y los socios limitan su responsabilidad hasta el monto total de sus acciones que son de su propiedad.
- El asegurador al aceptar el riesgo del asegurado queda obligado a responder por una eventual indemnización en el caso de presentarse un evento o siniestro que es la ocurrencia del riesgo asegurado.

2.1.1.2 Asegurado

- Es la persona interesada en traslación del riesgo.
- Es la persona o entidad que adquiere una póliza ante un asegurador que le cubre y le protege de un interés asegurable que ésta tiene, ya sea patrimonial de cosas o personas.
- ¿Cuándo decimos que es una persona o entidad?
    - Persona:
        - Es todo ser capaz de adquirir ejercer derechos y contraer obligaciones, pueden ser personas :
        - Individuales o
        - Jurídicas
    - La personas son sujeto de derecho

2.1.1.3 Riesgos

En el capítulo uno está definido el riesgo; para más detalle, dirigirse al mismo.

2.1.1.4 El interés asegurable

De lo visto en el elemento riesgo se infiere que: Quién no está expuesto al riesgo de sufrir por cualquier causa o motivo, pérdida o daño de carácter económico como consecuencia de cualquier suceso perjudicial carece de justificación para asegurarse contra los efectos de ese suceso; y consecuentemente, que quien está expuesto a esa eventualidad por más remota que su ocurrencia se antoje necesita recurrir a la protección del seguro.

Es evidente que no concurriendo la condición "*sine-qua-nom*"(sin la cual no) del interés asegurable, sería absolutamente injustificable adquirir un seguro sobre las personas y sobre todas las cosas: muebles inmuebles corporales e incorporales para protegerse en caso se llegara a producir uno o varios siniestros determinados sobre ellas de tal manera que resumiendo lo que es el interés asegurable decimos que es la individualización del objeto asegurable sobre el cual recae el seguro.

2.1.1.5 La prima

Es el precio del seguro, o sea que es la cantidad de dinero que el asegurado debe pagarle a la compañía para que esta tome a su cargo, los riesgos a que están expuestos los bienes asegurados, o sea que en caso de una pérdida o daño, la compañía le indemnizará en las cantidades ajustadas después de la realización del correspondiente ajuste, ya que por ello ha recibido la prima adecuada, siempre que no existen violaciones a las estipulaciones del contrato.

Según los términos de ley, la prima debe ser pagada en el momento de la celebración del contrato, sin embargo se puede convenir un pacto en contrario al fraccionar dicha prima en hasta seis pagos o en otra forma de pago según se convenga.

La falta de pago de las primas dan como resultado la cancelación de la póliza de seguro, por ello se fija la condición resolutoria expresa, que dice "es y queda convenida la condición resolutoria expresa que si el asegurado deja de pagar la prima en el plazo fijado como pacto en contrario, el contrato de seguro queda resuelto y sin ningún efecto ni validez legal desde el día del vencimiento del período de pago, sin necesidad de declaratoria judicial, ni la emisión de endoso de cancelación y la compañía relevada de cualquier responsabilidad, de conformidad con lo previsto en los artículos 1278 y 1581 del Código Civil"[33]

2.1.1.6 Póliza de Seguro

La póliza de seguro es el documento escrito y suscrito por la compañía, y mismo tiene la fuerza legal necesaria para que cualquiera de las partes lo haga valer ante cualquier autoridad civil, en caso de alguna desavenencia.

En este documento aparecen todas las obligaciones y los derechos tanto del asegurado como de la compañía suscriptora y debe llenar todos los requisitos que la ley fija, que son los siguientes:

- Lugar y fecha en que se emita.
- Nombres y domicilio del asegurador y asegurado y la expresión en su caso, de que el seguro se contrata por cuenta de un tercero.
- La designación de la persona o del bien asegurado.
- La naturaleza de los riesgos cubiertos.
- El plazo de vigencia del contrato con indicación del momento en que se inicia y de aquel en que termina.
- La suma asegurada.
- La prima o cuota del seguro y su forma de pago.
- Las condiciones generales y demás cláusulas estipuladas entre las partes.
- La firma del asegurador, la cual podrá ser autógrafa o sustituirse por su impresión o reproducción.

Los anexos y endosos deben indicar la identidad precisa de la póliza a la cual correspondan y las renovaciones además el período de ampliación de la vigencia del contrato original.

2.1.1.7 Suma asegurada

Es el valor que el asegurado le asigna a los bienes, objetos del seguro y que traslada a la compañía de seguros, la misma sólo determina la máxima responsabilidad de la compañía en un momento dado, pero no determina ni la propiedad ni la preexistencia de los bienes cubiertos, lo cual debe ser probado en caso de siniestro, por parte del asegurado, por los medios legales que la ley determina, tales como recibos y facturas de compra y pago, escrituras públicas de compra/venta, etc.

La suma asegurada sirve también para fijar el precio del seguro por el sencillo procedimiento de multiplicar, la suma asegurada por la tasa o tipo de prima, fijada por la compañía para obtener el valor de la prima neta a la que hay que adicionarle el monto de los gastos e impuestos, para establecer el valor total de las primas o sea la prima bruta que el asegurado debe pagarle a la compañía por sus servicios.

Otra de las características típicas de la suma asegurada, le da el hecho que la misma se puede aumentar en cualquier tiempo de la vigencia del seguro cuando el asegurado lo solicite a la compañía y ésta lo acepte por haber aumentado los bienes de su propiedad o por haber crecido su negocio; así mismo, la suma asegurada se puede disminuir en cualquier tiempo de la vigencia de la póliza, ya sea por el pago parcial de algún siniestro, asegurado o cubierto por la póliza o por haber perdido el interés asegurable. En el caso de un siniestro con pérdida total se termina el seguro, aunque la póliza no haya finalizado su período de vigencia, por haber desaparecido los bienes objetos del seguro, no habiendo por lo tanto ninguna suma asegurada que respaldar.

2.1.2 Co-aseguro

El coaseguro no es más que la participación de varias compañías o personas naturales o jurídicas en una relación de Seguros, nos explicamos:

Cuando un asegurado no quiere asegurar el 100% del valor de sus bienes, sino que sólo una parte, él se convierte automáticamente en su propio asegurador por la diferencia que deja de asegurar; ¿por qué? porque como generalmente no se sabe que parte de sus bienes le trasladó a la Compañía de Seguros y que parte no aseguró, se convierte en forma automática en Coasegurador de la Compañía.

El fenómeno anterior también se da entre las compañías de Seguros sobre todo en negocios de montos muy elevados, para entenderlo, se desarrolla el siguiente ejemplo:

El Asegurado tiene bienes por valor de 100 millones de quetzales.

La Compañía “líder” o “abridora” sólo desea asegurar un 40% o sea sólo 40 millones, qué hacer con el resto de 60 millones?, buscar Coaseguro local o extranjero, sea como sea hipotéticamente vamos a suponer que se consigue un Coaseguro de 4 Compañías, que deciden participar en el negocio en las siguientes proporciones: Compañía “A” con un 25% o sean 25 millones, Compañía “B” con 15% o sean 15 millones, Compañía “C” con 10% o sean 10 millones y compañía “D” con 10% o sean 10 millones.

Para lograr una mejor comprensión de cómo funciona el Coaseguro, se muestra el cuadro resumen de la participación de cada una de las Compañías que toman el nombre de “Compañías Coaseguradoras” en dicho cuadro resumen se observa claramente la participación de cada una de ellas y su porcentaje de participación, así como de las sumas aseguradas. Así, en ese mismo porcentaje es su responsabilidad y su aporte a cualquier siniestro que se suscite ya que todas deben pagar, aunque generalmente es, a la Compañía abridora o líder, a quien deben pagarle, pues ésta casi siempre se reserva el derecho, por ser la líder del manejo de siniestro y ajuste, así como del pago del mismo, veamos:

Tabla I. Cuadro resumen del co-aseguro

Núm.	COMPAÑIA PARTICIPANTE DEL NEGOCIO	%	MONTO COASEGURADO
1	Compañía Abridora o Líder.	40 %	Q.40.000.000.00
2	Compañía Coaseguradora "A"	25 %	Q.25.000.000.00
3	Compañía Coaseguradora "B"	15 %	Q.15.000.000.00
4	Compañía Coaseguradora "C"	10 %	Q.10.000.000.00
5	Compañía Coaseguradora "D"	10 %	Q.10.000.000.00
	TOTALES	100%	Q.100,000,000.00

2.1.3 Reaseguro

El reaseguro no es otra cosa que el seguro que compran las Compañías aseguradoras, generalmente a nivel internacional, para respaldar sus operaciones; sobre todo cuando han tomado responsabilidades muy grandes.

Cuando las Compañías aseguradoras captan y suscriben negocios en su mercado local, generalmente ya tienen uno o varios contratos de reaseguros tomados a principio del año que les respaldan todas sus operaciones directas.

Sin embargo, a pesar de tener uno o varios contratos de reaseguro, cuando las responsabilidades tomadas son muy grandes se tienen que buscar otras modalidades de reaseguro como lo son los reaseguros facultativos locales o extranjeros para poder responderles a los asegurados.

Dentro del contrato de reaseguro existe una participación del asegurador directo del seguro y que se llama retención. Las Compañías, una vez canalizada su retención que es la máxima responsabilidad que directamente asume como su participación tanto en las ganancias como en las pérdidas de las operaciones de sus negocios de seguro, transfiere al reasegurador de su contrato la responsabilidad y las primas cobradas en las cantidades o en los porcentajes convenidos previamente y aceptados en el contrato de reaseguro.

En caso de siniestro, una vez avisada la Compañía aseguradora directa por el asegurado, tiene ésta que avisarle a su vez a sus reaseguradores, informándoles lo más claro posible del siniestro, sus características y circunstancias; para que este último haga las provisiones necesarias de reserva de fondos para siniestros en curso, mientras se recibe el informe final del ajustador nombrado.

2.2. El seguro contra ciber-riesgos

El negocio de seguros está abordando el impacto del Internet en muchos frentes, y teniendo que hacer esto a una velocidad que no está acostumbrado.

El seguro tradicional no podría cubrir la mayoría de los costos legales de ataques en el ciberespacio, como lo son: destrucción de datos, robo de información de clientes, y denegación de servicio.

Es difícil asesorar un nuevo ambiente de riesgo y el rol que debe jugar el asegurar el ciber-riesgo en una institución financiera.

Casi todos los programas de seguros tradicionales no cubren varios tipos de riesgo:

- Responsabilidad por robo de información privada o confidencias que incluye la ola creciente de robo de identidad
- Pérdidas por interrupción del negocio o gastos extras debido a ataques de hacker o virus que interrumpen las operaciones (incluyendo invasores internos y ataques de negación de servicio)
- Responsabilidad por ataques en contra de terceros, utilizando la red de información de la institución financiera.
- Robo de contraseñas por medios no electrónicos.

Como principales vulnerabilidades de un ambiente interconectado que podrían ser cubiertos por una póliza de seguro están:

Reclamos a terceros

- Por pérdidas económicas derivadas de la imposibilidad de acceder a sus sistemas informáticos.
- Por errores u omisiones en el suministro de servicios tecnológicos a sus clientes (Responsabilidad civil profesional)
- Por daños a sistemas o registros informáticos de terceros (virus o hacking de empleados).
- Por violación de la confidencialidad, derechos de privacidad y demás normativa de protección de datos de carácter personal
- Por calumnia o difamación a través del correo electrónico o la web.
- Por violación de derechos de propiedad intelectual en el contenido del correo electrónico o de la web.

Reclamos de sus empleados

- Por uso inadecuado de la información confidencial de los trabajadores por parte de la empresa.
- Por un entorno de trabajo inapropiado (acoso sexual o racial a través de medios electrónicos,…)

Daños o pérdidas propias

- Gastos incurridos en la reparación de los daños causados a sus sistemas informáticos y en encontrar, reemplazar o restaurar sus registros informáticos dañados por un virus o hacker.
- Pérdidas causadas por la incapacidad de prestar sus servicios electrónicos como resultado de un virus o un hacker.
- Extorsión con amenaza de introducir en sus sistemas electrónicos un virus o código malicioso, o de difundir sus registros.
- Pérdidas sufridas por robo a través de sus sistemas electrónicos.
- Gastos legales incurridos en la defensa legal de sus derechos de propiedad intelectual en Internet.
- Gastos derivados de la contratación de una consultora de Relaciones Públicas para mitigar los daños producidos a su imagen por la ocurrencia de un sinistro cubierto bajo la póliza.

2.2.1. Ciber-responsabilidad

Generalmente, la cobertura de seguros está asociada con la protección de activos tangibles, pero ahora encontramos que existen activos que no son tangibles como la información o los datos que podemos encontrar dentro de la computadora.

Es muy difícil tener protección contra los virus creados y lanzados inmediatamente después de descubierta una vulnerabilidad, ya que esto no permite que se tenga tiempo de responder por parte de los antivirus. La estrategia reactiva no sirve y podrían propagarse graves daños sin posibilidad de prevención.

Si el ataque de virus produce un gran impacto, los grandes directivos de la empresa van a enterarse y solo pueden entender el daño ocasionado por la cuantificación de los mismo y las responsabilidades asociadas a estos daños ocurridos, no importando las características técnicas del virus. Esto, además como casi nadie cuenta con herramientas para cuantificar los daños, va a producir un choque entre tecnología y negocio en la empresa.

Las pólizas que cubren el ciber-riesgo, como parte de un plan de gestión de riesgos, deben cubrir la pérdida por daños, entre otras cosas mediante el pago de expertos en seguridad que reparen los sistemas que sufrieron daños y además recuperen los datos perdidos; también deben cubrir la pérdida del tiempo que no se pudo realizar ninguna operación.

No solamente eso, sino que si el virus es muy avanzado, puede hasta utilizar los sistemas que están infectados para atacar otras empresas, añadiendo la probabilidad de que las otras empresas afectadas por medio de nuestros sistemas, demanden a la empresa primeramente infectada, por los daños producidos. También este tipo de seguro cubre algún daño ocasionado a la empresa por daños a la reputación de la misma por alguna falla producida debido al virus propagado.

No es algo fuera de lo común, o algo que solamente a ciertas empresas pueda ocurrirles, realmente es algo que está ocurriendo cada vez como mayor frecuencia y alcanza los titulares de prensa.

La cobertura de este tipo de seguro puede contemplar todas las áreas del ciber-riesgo: daños en los sistemas propios de información; demandas contra los empleados de la empresa (un ejemplo de ello es acoso sexual por algún medio electrónico); daños contra terceros ocasionados por empleados, directivos o socios de la empresa.

Este tipo de seguro se conoce poco debido a varias razones: una de ellas es la falta de comprensión, análisis y gestión del riesgo y la ignorancia sobre este problema por parte del sector asegurador, que generalmente no está muy enterado de este tipo de riesgo y le resta importancia.

2.2.2. ¿A quiénes interesa?

Cualquier empresa que utilice sistemas de computación está expuesta al ciber-riesgo, no solamente compañías que manejen ventas por Internet.

Las instituciones financieras operan en una economía global e interconectada, y tomando en cuenta que las redes de computadoras están firmemente integradas en casi cualquier proceso de negocio. Es básico para una propuesta de valor de cualquier institución financiera, proveer una plataforma segura y de confianza para conducir transacciones e intercambiar información. La plataforma, sin embargo, se basa solamente en parte en las propiedades físicas de las instituciones. Se ha expandido para incluir un sistema distribuido de cómputo que habilita el comercio electrónico con clientes, proveedores y socios, que cada vez es más un procedimiento operacional estándar. Las limitaciones físicas han sido removidas por el Internet y la habilidad de las instituciones de conectar sus propias plataformas electrónicas a la estructura pública del Internet. El enfoque de este trabajo son los riesgos crecientes que han emergido con este desarrollo tecnológico y lo que las instituciones financieras están haciendo al respecto.

Notar que con el crecimiento del comercio electrónico, lo cual requiere que la organización se conecte con los clientes y los socios, incrementa la amenaza de fraude financiero y el robo de la información almacenada de los clientes desde el interior o el exterior de la organización.

Las firmas de servicios financieros están tomando varios pasos para combatir estos riesgos, como utilizar programas anti-virus, establecer estándares de seguridad y crear firewalls. De cualquier modo, la forma de protección que más recientemente ha emergido contra ciber-riesgo es la póliza de seguro el ciber-riesgo.

Como nuevos riesgos emergen día con día, es posible que hasta las instituciones financieras más diligentes, no estén protegidas adecuadamente para algunas vulnerabilidades emergentes del comercio electrónico.

Se ha infiltrado en firmas de servicios financieros tan rápido como en el Internet. Afortunadamente el sector de servicios financieros se ha tomado la amenaza de este riesgo muy en serio.

3. MERCADO INTERNACIONAL

3.1. Respecto a las aseguradoras

Desde que el comercio electrónico surge como un método viable para hacer negocios ha habido un aumento en acciones indeseables que han creado el ciber-riesgo como lo conocemos ahora. Durante este período, las aseguradoras manejaron reclamos de asegurados que nunca contemplaron, usando pólizas que fueron fundadas dentro de una medio muy confuso.

Consecuentemente, una práctica común en el desarrollo de pólizas de seguros es excluir ciertos datos (no específicamente protección de datos lógicos ni físicos). Las aseguradoras deben analizar las pólizas y recomendar a sus clientes que se documenten al respecto. Las organizaciones deben hacerse conscientes de la creciente responsabilidad sobre sus infraestructuras para comprometerse en la educación de los riesgos tecnológicos que afectan su ambiente y las opciones para tratar con estos riesgos. Existen muchas organizaciones que no obtienen cobertura para ciber-riesgo ya sea porque no tienen el mínimo en infraestructura requerido por las aseguradoras o porque los costos son muy elevados.

La geografía juega un factor importante en cuanto a la disponibilidad de opciones de seguros para las organizaciones.

Cualquier empresa relacionada con tecnología debe preparar y conducir un análisis costo-beneficio profundo antes de escalar a nuevas tecnologías de seguridad o planificar una estrategia de seguridad. Si la empresa trabaja con sistemas computacionales o sitios web, necesita ciber-protección responsable. La aplicación del ciber-seguro está prevista para actuar como asesor superficial de la postura tecnológica actual de la empresa.

La evaluación es una herramienta estratégica utilizada para determinar si a una empresa se le puede conceder cobertura o no. Habrá preguntas realizadas a la organización respecto a si ha sufrido o no algún incidente previo que involucre su red o ambiente electrónico. Si la empresa falla al revelar cualquier detalle relacionado con un incidente previo, la aseguradora deberá dejar de procesar la solicitud debido a que no llena los requisitos. Las aseguradoras deben lidiar con dos resultados distintos de impacto financiero para una empresa, fraude financiero y robo de propiedad de información. El robo de identidad está en aumento y es uno de los generadores de dinero ilegales más remunerables en el mundo de la tecnología. Si se determina que la empresa es de confianza, el robo de información de clientes puede hundir a la organización, destruir sociedades y destruir la credibilidad de la empresa. Aunque se determinara que la empresa no es de confianza, esta exposición puede, muy fácilmente, dañar la integridad de la entidad de negocios.

El fraude está de moda en la industria de seguros, en años anteriores el método más efectivo para detectar actividad legal en una investigación simplemente era cuestión de descubrir fraude accidentalmente. Originalmente, la tecnología capaz de detectar fraudes estaba diseñada en programas de código que mostraban circunstancias sospechosas y conocidas; por ejemplo, una institución financiera puede mostrar retiros de cuentas de Q10,000.00 en efectivo para cuentas personales de cheques. Eventualmente, artistas del fraude aprenderían que retiros múltiples de Q9,999.99 o menos, no mostrarían ninguna alerta. Múltiples retiros de este tamaño pueden ser muy lucrativos.

Luego, las bases de datos relacionales y las herramientas de análisis permitieron a las aseguradoras detectar y desactivar el fraude que afecta las empresas. Este proceso empleaba lenguajes de consulta usando evaluaciones *'if, then, else'* permitiendo así procesar grandes volúmenes de datos. Esto, asistido con identificación de patrones y tendencias para predecir de mejor manera áreas potenciales de fraude. No obstante, este proceso requería que la aseguradora revisara las disparadores conocidos, identificarlos y usar este proceso para confirmar sus sospechas. Incluso cuando los patrones de fraude fueran detectados, el tiempo y el esfuerzo que tomaba hacer los cambios necesarios en el sistema generalmente dejarían al asegurador arreglando el problema mucho tiempo después que el perpetrador haya seguido su rumbo hacia una nueva oportunidad. Estas metodologías no valían la pena aún cuando el fraude no fuera cubierto. El valor en relación con la póliza generalmente probaba ser dañino y no valía el costo de daño de la confidencialidad del asegurado; mientras que la aseguradora examinaba la legitimidad de la posición del reclamador para luego ser cuidadosamente examinado.

La tecnología de fraude ha ganado mayor terreno en los últimos años ofreciendo sets de herramientas y software con técnicas avanzadas de computación. Estas técnicas han permitido a los investigadores aprender de la experiencia y mejorar su habilidad para entender más la detección de fraudes e identificación de patrones. La inteligencia artificial permitirá al software examinar más detalles minuciosos de las tácticas de fraudes y asistir a los encuestadores en detectar fraudes más rápidamente. Estas técnicas van a mejorar la carga de detección del elemento humano y reducir el número de positivos falsos que son necesarios para examinar. Pero los perpetradores van a continuar refinando sus capacidades de fraude y encontrando nuevas formas para infiltrarse en sistemas de información de las empresas.

Combinando la nueva generación de herramientas de combate contra el fraude con estas técnicas nuevas y avanzadas de análisis predictivo y optimización adaptable provee a la industria de seguros la oportunidad de ganar terreno en la competencia de fraude. Esto puede permitir a las aseguradoras acercarse al seguimiento de esta forma de crimen pero no necesariamente dar armonía con el lado equivocado de la ley.

Hoy en día, los riesgos del fraude cibernético están en aumento. Ellos pueden incluir retos sigilosos de espionaje para conducir ataques que incluyen negación de servicios y desfiguración web. Las aseguradoras se han dado cuenta que las pólizas de Responsabilidad General del pasado no concuerdan con los requerimientos de los estándares de hoy. Las aseguradoras han sugerido que las empresas adquieran pólizas específicamente diseñadas para interrupciones específicas, como eventos de hacker. Esto va a requerir mayor financiamiento para protegerse contra lo no identificado. Si se decide limitar la protección, las empresas van a encontrar que cuando se trata de rechazar acciones legales de los clientes y socios de negocios, pueden hasta quedarse solos. Cobertura de virus y gusanos es una forma de seguro que no ha madurado, debido a la naturaleza de estas formas de virus que dañan profundamente más que a la superficie.

Los corredores representan a las empresas por una forma de desarrollo de tecnología de pólizas que coinciden con los requerimientos de protección de la empresa. Ellos pueden crear pólizas a la medida en una forma que se acerquen más a las necesidades del seguro de la empresa en orden a limitar las exposiciones de responsabilidad. En cualquier momento que una organización busca un corredor para representar sus intereses, la organización debe tomarse el tiempo de preguntar y revisar una copia de la propuesta presentada de modo que los requerimientos estén debidamente detallados y comprendidos.

3.2. Respecto al asegurado

Un estudio nuevo muestra que la mayoría de grandes compañías no gastan lo suficiente de sus presupuestos de TI en actualizar sus infraestructuras de seguridad. Esta situación puede generar problemas mayores frente a la legislación gubernamental, las fusiones y las adquisiciones empresariales.[34]

Nemertes Research muestra, mediante un reporte hecho en el año 2003 que un promedio de 2%-3% del total del presupuesto de TI que las compañías asignan para seguridad, no las prepararán adecuadamente para regulaciones gubernamentales, nuevas aplicaciones y/o arquitecturas de servicios Web.

Gastar el 3% en seguridad solamente permitirá contemplar lo básico en seguridad en la mayoría de grandes organizaciones. Al decir lo básico en seguridad incluye el despliegue de cortafuegos y VPN's y controlar el perímetro de seguridad.

Todo el mundo va a decir que la seguridad es esencial y nadie se atreverá a decir que no es importante, pero nadie está dispuesto a invertir lo suficiente en seguridad.

Nemertes encontró que muchas compañías en los últimos cinco años han dado pasos en designar oficiales de seguridad, personal y presupuesto, pero de todas formas se quedan cortos cuando se refiere a financiamiento de proyectos nuevos y necesarios.

Las empresas deberán gastar al menos el 5% del total de su presupuesto TI en seguridad para incorporar las actualizaciones de infraestructura y procesos basados en políticas necesarias para cumplir con las regulaciones gubernamentales pasadas en los últimos ocho años más o menos.

Los requerimientos de seguridad en legislación, como *Health Insurance Portability and Accountability Act* de 1996 (HIPAA), el *Gramm-Leach-Bliley Financial Modernization Act* de 1999, el *Sabarnes-Oxley Act* del 2002 y las iniciativas en curso del *Departament of Homeland Security*, representa una preocupación importante para compañías que actualmente no están dispuestas a invertir en seguridad.

HIPAA establece estándares nacionales para asegurar privacidad en transacciones electrónicas de cuidado de la salud, y da luz a todas las discrepancias de contabilidad en los últimos años. *Sabarnes Oxley* requiere que los administradores tengan fe en los controles internos que sus empresas establecen sobre áreas que incluyen transacciones, informaciones y comunicaciones electrónicas. *Sabarnes-Oxley* va a convertirse una regla de la Comisión de Seguridad e Intercambio. El *Gramm-Leach-Bliley Act* destruyó las barreras de intercambio de información a través de la banca, la seguridad y la industria de seguros de Estados Unidos de América, tanto como proveer varios servicios financieros para el consumidor, pero también requieren que se establezcan muchas regulaciones de privacidad, electrónicas y financieras.

La fina impresión en estas piezas de legislación tiene al CEO o al oficial de Seguridad potencialmente yendo a prisión si se encuentra en violación de estos actos. Las empresas están solamente empezando a envolver sus cabezas alrededor de esas ideas.

Con fusiones y adquisiciones más frecuentes, las empresas deberán invertir más dinero en crear infraestructuras comunes de seguridad a través de departamentos de TI. Se plantea particularmente un gran problema para empresas que proveen servicios financieros. Se encontró que al menos tres cuartos de los ejecutivos de seguridad dicen que el control de acceso, autorización, auditoría y administración de identidad deberían estar entre las prioridades más importantes del presupuesto.

Otras conclusiones mostraron que mientras el 80% no han desplegado aplicaciones de seguridad o web, muchos van a invertir en esta tecnología en el año venidero o más.

Conclusiones principales de la Investigación:

- 52% de las empresas destinan financiamiento para auditoría y documentación, pero este gasto no provee ninguna ganancia incremental en seguridad y el gasto debe repetirse cada año. Nemertes espera el cumplimiento de los gastos generales para continuar desafiando muchas empresas por 2007-2008.
- Más allá del cumplimiento, este presupuesto se distribuyen en anti-malware (43%), cortafuegos y VPN's (41%), y prevención y detección de intrusos (38%). Las empresas han identificado los productos y tecnologías de seguridad que necesitan y se están promoviendo la instalación y actualización de estos sistemas.
- El spyware ha reemplazado el spam, virus y troyanos como la mayor fuente de preocupación, con el 24% citándolo como una preocupación seria, sin embargo el 40% de empresas no tiene una solución automatizada. Nemertes notó una tendencia creciente de las compañías utilizando el navegador Mozilla Firefox para reemplazar Internet Explorer como una solución para spyware (8%) y esta figura espera crecer dramáticamente durante los próximos 12 años.
- Otras cuestiones críticas incluyen gestión de parches, gestión de identidad, y una preocupación creciente sobre ataques distribuidos de negación de servicio.

3.2.1. Spear-phishing

Mensajes de correo electrónico fraudulentos o sitios Web falsos diseñados para robar datos de identidad. Los atacantes intentan convencer a millones de usuarios para que revelen información confidencial. Ahora existe una nueva versión de una vieja estafa, que se denomina "*spear-phishing*". Se trata de un ataque dirigido por correo electrónico que un atacante envía únicamente a un grupo reducido de personas; por ejemplo, los empleados de una empresa. El mensaje de correo electrónico podría parecer auténtico, pero responder es arriesgado, tanto para usted como para su empresa.

3.2.1.1. Cómo funciona una estafa de "phishing" típico

Los atacantes especializados en *"phishing"* no actúan de forma selectiva y, por lo general, envían de forma masiva mensajes de correo electrónico que parecen proceder de organizaciones muy conocidas, como entidades bancarias y casas de subastas, entre otras. Estos mensajes de correo electrónico y ventanas emergentes, así como los sitios Web de los que contienen vínculos parecen "oficiales", de modo que muchas personas pueden llegar a creer que son reales. Hay personas confiadas que responden a peticiones que reciben de esta forma, y en las que se solicitan números de tarjetas de crédito, contraseñas, información sobre cuentas u otros datos personales y financieros.

3.2.1.2. Cómo funciona una estafa de "spear-phishing"

El *"spear-phishing"* hace referencia a cualquier ataque de *phishing* dirigido a un objetivo muy específico. Los atacantes de *"spear-phishing"* envían mensajes de correo electrónico que parecen auténticos a todos los empleados o miembros de una determinada empresa, organismo, organización o grupo. Podría parecer que el mensaje procedente de un jefe o de un compañero que se dirige por correo electrónico a todo el personal (por ejemplo, el encargado de administrar los sistemas informáticos) y quizá incluya peticiones de nombres de usuario o contraseñas.

En realidad, lo que ocurre es que la información del remitente del correo electrónico ha sido falsificada. Mientras que las estafas de *"phishing"* tradicionales están diseñadas para robar datos de personas, el objetivo de las de *"spear-phishing"* consiste en obtener acceso al sistema informático de una empresa. Si responde con un nombre de usuario o una contraseña, o si hace clic en vínculos o abre archivos adjuntos de un mensaje de correo electrónico, una ventana emergente o un sitio Web desarrollado para una estafa de *"spear-phishing"*, puede convertirse en víctima de un robo de datos de identidad y poner en peligro a su organización.

Las estafas de *"spear-phishing"* también se dirigen a personas que utilizan un determinado producto o sitio Web. Los atacantes utilizan toda la información de que disponen para personalizar al máximo posible la estafa de phishing.

3.2.1.3. Los ataques de "spear-phishing" alcanzan los 15,000, según Verisign [35]

Dos grupos de criminales han robado datos de un estimado de 15,000 víctimas, durante los últimos 15 meses, usando ataques de correo electrónico orientados de *"spear-phishing"*, de acuerdo a los investigadores de Verisign.

Verisign ha llevado el rastro de 66 de estos ataques desde Febrero del 2007 y cree que dos grupos sombríos de crimen están detrás del 95% de los incidentes.

A diferencia de los ataques de *"phishing"* típico, que han sido enviados a millones en esperanza de atraer algunas víctimas para sitios web falsos, los correos electrónicos de *"spear-phishing"* contienen información personal, como el nombre de la víctima o el nombre de su jefe para hacerlos parecer legítimos. En los ataques que Verisign lleva rastro, las víctimas han sido engañados para visitar sitios web maliciosos o abrir archivos adjuntos maliciosos también, que después le dejan al atacante una puerta abierta para sus PC's y poder robar información.

Los atacantes realmente han perfeccionado ambos métodos tanto el de entrega, como el del uso de los datos. Todos los correos electrónicos tienen como meta atacar negocios de una manera u otra.

En abril, ellos pusieron en marcha el más exitoso ataque de *"spear-phishing"* que se ha visto hasta el día de hoy. Enviaron correo electrónico orientado a ejecutivos corporativos, informándoles que habían sido demandados. Este ataque funcionó muy bien porque era noble. Esta citación realmente lo toma a uno desprevenido, especialmente a nivel ejecutivo. El miedo de un litigio realmente asustó a la gente.

En mayo, más de 2,000 personas fueron comprometidas con correos de *"spear-phishing"* que decían que venían del Servicio de Ganancias Internas de los Estados Unidos de América (*U.S. Internal Revenue Service*), la Corte de Impuestos de Estados Unidos de América (*United States Tax Cour*t) y el Buró de Mejores Negocios (*Better Business Bureau*), de acuerdo con Verisign.

Verisign no espera que los atacantes de *"spear-phishing"* se den por vencidos. Ahora que han desarrollado este sistema refinado, ellos simplemente seguirán haciendo esto una y otra vez.

3.3. Cobertura de la Póliza de Seguro

Las compañías de seguros ofrecen una numerosa variación de cobertura que realmente es de admirar. Las organizaciones tienen similitudes pero también diferencias muy marcadas en términos del nivel de protección que necesitan para cubrirse contra pérdidas. Esto presenta un panorama en que las organizaciones deben tomar la iniciativa para comprender completamente el nivel de requerimientos de protección en el que están antes de comprometerse en el proceso de aplicación de seguro. El agente de seguro, no necesariamente pedirá un reporte de evaluación de seguridad pero sí necesitará tener una prueba de preparación de infraestructura antes que la aplicación sea procesada. Por ejemplo, si una organización provee servicios para sitios web y tiene por objeto tener un firewall que proteja toda la información de los clientes, pero de todas formas la organización no monitorea regularmente el *firewall*, aplicándoles parches regularmente, monitoreando la tecnología, esto reflejará un riesgo para la empresa. Esta deficiencia en la administración de TI podría dejar a la organización con cobertura cuestionable o con un largo proceso de litigación si los sistemas fueran dañados, hackeados o destruidos. Parte del ejercicio de evaluación es determinar si la organización tiene controles y procedimientos adecuados para mantener una vigilancia constante dentro del ambiente. De otra forma, si ocurre algún daño, la organización puede no tener la habilidad de recuperarse o protegerse de daños técnicos y una litigación potencial.

Si, por ejemplo, una organización solamente tiene la póliza CGL (*Commercial General Liability-Responsabilidad General Comercial*), sería muy ambicioso esperar que esta forma de seguro pudiera proveer suficiente protección contra un incidente de hacking de sitio web o cualquier otro desastre relacionado. Generalmente las organizaciones deben tener por lo menos tres pólizas tecnológicas en su portafolio, siendo estas E&O (*Errors and Omisions*), Responsabilidades de D&O (Directores y Oficiales - *Directors and Officers*) y seguros de EPL (Prácticas de Empleo de Responsabilidad - *Employment Practices Liability*). Si es una organización que está proveyendo, por ejemplo, servicios web en línea, servicios de desarrollo y hosting, y posiblemente otros servicios o combinación de servicios, entonces este es el tiempo de asegurar que la organización tiene una comprensión completa de su negocio crítico. Este mensaje debe transmitirse por toda la organización. No deben existir cosas como información que no se encuentra o no se sabía de esta información reclamando quién debía hacer qué cosa y por qué no se había hecho.

3.4. Panorama Internacional

3.4.1. Opciones de Cobertura de Póliza de Seguro[36]

A pesar de que el ciber-riesgo, es un riesgo bastante especial por encerrar características muy específicas, para una póliza de seguro tienen divisiones bastante similares. Estas divisiones son responsabilidad, propiedad, errores, entre otros. A continuación se presenta una tabla detallada de las opciones que podemos encontrar en el mercado respecto a una póliza de seguro que cubra el ciber-riesgo.

Tabla II. Cobertura de Póliza de Seguro

Opción	Descripción
Responsabilidad General de Crimen a través de Internet	Apunta riesgos asociados con negocios electrónicos, el Internet, redes y activos de información propios o de terceros. Existen limitaciones con este nivel de cobertura. Es esencial revisar las actividades de negocio para asegurar una cobertura apropiada.
Propiedad	Protección contra daño a activos físicos causados por medio del Internet, maquinaria apagada, o equipo programado que opera erradamente. Típicamente, esta póliza no reconoce "datos" como propiedad.
Errores y Omisiones	Protege la organización de reclamos si el cliente de la misma acusa a la empresa de responsable por errores en programación, desempeño de software o el fallo del trabajo realizado para trabajar como se prometió en el contrato.
Responsabilidad Profesional	Provee protección contra los reclamos en que el asegurado está obligado legalmente a pagar como resultado de un error u omisión en su trabajo profesional.
Responsabilidad de Directores y Funcionarios	Requerido por una junta de directores para protegerlos en el caso que fueran demandados en conjunto con sus deberes.
Responsabilidad de Prácticas de Empleo	Protege al empleador de reclamos hechos por empleados con motivo de discriminación (edad, sexo, raza, discapacidad, etc.), ilegalidad, y acoso sexual.

Interrupción de Negocio	Cuando se determina un escenario de desastre potencial, no solo se toma en cuenta el daño físico. Una empresa debe incluir muerte, discapacidad y secuestro de personal clave; Deserción de personal clave hacia la competencia; Robo de secretos de comercio; Manejo de Imagen (percepción pública)
Cobertura de Secuestro/Extorsión & extorsión	Provee cobertura para secuestros y otros eventos a través de una combinación de indemnización financiera y administración de crisis experta.
Responsabilidad de grupo de personal	Cobertura para personal clave, gerentes y empleados.
Cobertura de vida por personas clave	Esta cobertura está diseñada para proteger el negocio de la pérdida de empleados claves. Los procedimientos libres de impuestos de esta póliza pueden utilizarse para encontrar, contratar y entrenar el reemplazo, compensar los negocios perdidos durante la transición o financiar cualquier número de transacciones de negocio.
Cobertura de Responsabilidad de medios	Protege en contra de reclamos provenientes de recolectar y comunicar información. Provee cobertura muy valiosa contra reclamos de difamación e invasión de privacidad así como derechos de autor e infracción de marca.
Responsabilidad de Fidelidad o Crimen	Protege a la organización de pérdida de dinero, seguridad, o inventario resultado de un crimen

Cobertura de Seguridad de Red	Protege a la organización de pérdidas asociadas con acceso no autorizado o robo de datos o actividades de e-business, virus, ataques de negación de servicio así como presuntas transacciones de comercio electrónico no autorizadas.
Propiedad Intelectual	Protege a las compañías de reclamos de derechos de autor, marca, o infracción de patente derivados de operación de la compañía. Elementos como papeles de trabajo, grabaciones, secretos de marca, datos, metodologías, dibujos, programas, documentos o cualquier otro escrito creado, desarrollado o adquirido por la compañía.
Cobertura de Patente	Una póliza que reembolsa al asegurado para gastos de defensa y daños pagados por el asegurado resultado de alegaciones de que el asegurado ha infringido alguna patente, derecho de autor o marca de terceras partes.
Cobertura de violencia laboral	Protección de los gastos que una compañía puede enfrentar como resultado de incidentes de violencia laboral, incluyendo el costo de contratar consultores independientes de seguridad y expertos de relaciones públicas, así como pago de prestaciones en caso de fallecimiento y gastos de interrupción de negocio.

Fuente: Drouin, Denis. **"Cyber Risk Insurance. A Discurse and Preparatory Guide"**. Febrero 9, 2004.

3.4.2. Estadísticas de Amenazas en la industria

En el 2006, CSI/FBI lanzó su encuesta de Crimen y Seguridad en Computadoras. Esta encuesta está basada en respuestas de 616 practicantes de seguridad computacional en corporaciones, agencias gubernamentales, instituciones financieras, instituciones médicas y universidades de Estados Unidos.[37]

La encuesta del 2006 apunta los datos más importantes considerados en anteriores encuestas de CSI/FBI, permitiendo así analizar tendencias importantes de seguridad. Las tendencias a largo plazo consideradas incluyen:

- Uso no autorizado de sistemas de computadoras.
- El número de incidentes sucedidos desde fuera de la organización así como también desde adentro.
- Tipos de ataques o malos usos detectados.
- Acciones tomadas en respuesta a intrusos de computadora.

También apunta a cuestiones emergentes de seguridad. Todos los puntos siguientes están relacionados con decisiones económicas que se toman dentro de una organización relacionadas con seguridad computacional y el modo en que manejan el riesgo asociado con brechas de seguridad:

- Las técnicas que las organizaciones utilizan para evaluar el desempeño de sus inversiones en seguridad computacional.
- Las necesidades en capacitación de seguridad de las organizaciones.
- El gasto de las organizaciones en inversiones de seguridad.
- El impacto del outsourcing en actividades de seguridad computacional.
- El uso de auditorías de seguridad y seguros externos.
- El rol de Acto de Sabarnes-Oaxley del 2002 en actividades de seguridad.
- La porción del presupuesto de tecnologías de información que la empresa invierte en seguridad.

Hallazgos principales

- La fuente de mayores pérdidas financieras sigue siendo ataques de virus. Y la segunda fuente de mayor pérdida sigue siendo acceso no autorizado. Pérdidas financieras relacionadas con computadoras portátiles y robo de propiedad de la información son la tercera y cuarta, respectivamente. Estas cuatro categorías suman más del 74 por ciento de pérdidas financieras.
- La cantidad total de dólares en pérdidas financieras como resultado de brechas de seguridad tiene un decremento sustancial este año, de acuerdo a los encuestados. Aunque una gran parte de este descenso se debe a un decremento en el número de encuestados que podían y estaban dispuestos a proveer estimados de las pérdidas, la cantidad promedio de pérdidas financieras por encuestado también decrementó sustancialmente este año.
- A pesar que se piensa que el outsourcing ha aumentado, los resultados de la encuesta relacionados con outsourcing son similares a los reportados en años anteriores y muestran muy pocas actividades relacionadas con outsourcing de seguridad de información. De hecho, 61 por ciento de los encuestados indicaron que sus organizaciones no dan ninguna función de seguridad al outsourcing. Sobre las organizaciones que hacen outsourcing sobre actividades de seguridad, el porcentaje de actividades de seguridad a las que ha realizado outsourcing es bastante más bajo.
- El uso de ciber-seguro se mantiene bajo, pero puede ir en ascenso.

- El porcentaje de organizaciones que reportan intrusiones de computadora para aplicación de ley, ha revertido el declive de los últimos años, poniéndose en 25 por ciento comparado con 20 por ciento en los años anteriores. Sin embargo, la publicidad negativa que se genera a partir de reportar intrusiones para aplicación de ley es todavía una gran preocupación para muchas organizaciones.
- Muchas organizaciones conducen alguna forma de evaluación económica de sus gastos en seguridad, con el 42 por ciento usado en Retorno de Inversión (ROI), 21 por ciento usado en Tasa Interna de Retorno (IIR), y 19 por ciento usado en Valor Presente Neto (VPN). Estos porcentajes están arriba de los números reportados en años anteriores. Además, en preguntas de respuesta abierta, los encuestados frecuentemente identificaron cuestiones de administración y económicas como presupuesto capital y administración de riesgo como las cuestiones más críticas que ellos enfrentan.
- Más del 80 por ciento de las organizaciones conducen auditorías de seguridad.
- El impacto del Acto Sabarnes-Oxley en seguridad de información continúa siendo sustancial. De hecho, en preguntas de respuesta abierta, los encuestados notaron que la conformidad regular relacionada con seguridad de información está entre las cuestiones críticas más importantes que enfrentan.

- Una vez más, la vasta mayoría de las organizaciones miran que la capacitación en conciencia de seguridad es importante. De hecho, hay un incremento sustancial en la percepción de los encuestados de la importancia de la capacitación en conciencia de seguridad. En promedio, los encuestados de la mayoría de los sectores creen que la organización no está invirtiendo suficiente en esta área.

Resultados que sobresalen

La siguiente tabla muestra el porcentaje de presupuesto de TI dedicado a seguridad. Esta tabla nos muestra que la mayoría dedican un porcentaje del 1%-2% del presupuesto de TI en seguridad.

Tabla III. Porcentaje de presupuesto de TI dedicado a seguridad

Porcentaje de Presupuesto de TI dedicado a seguridad	Porcentaje de encuestados
Más del 10%	13%
8-10%	10%
6-7%	11%
3-5%	6%
1-2%	26%
Menos del 1%	21%
Desconocido	12%

Fuente: Gordon, Lawrence A.; Loeb, Martin P.; Lucyshyn, William; Richardson, Robert. **"2006 CSI/FBI Computer Crime and Security Survey".** 2006.

Tabla IV. Porcentaje de organización que utilizan ROI, VPN y TIR.

	%
ROI	42%
VPN	19%
IIR	21%

Fuente: Gordon, Lawrence A.; Loeb, Martin P.; Lucyshyn, William; Richardson, Robert. **"2006 CSI/FBI Computer Crime and Security Survey".** 2006.

Tabla V. Porcentaje de funciones de Seguridad Computacional que dan a outsourcing

Porcentaje de Funciones	Porcentaje de Encuestados
Ninguna	61%
Hasta el 20%	27%
21-40%	6%
41-60%	4%
61-80%	1%
81-100%	1%

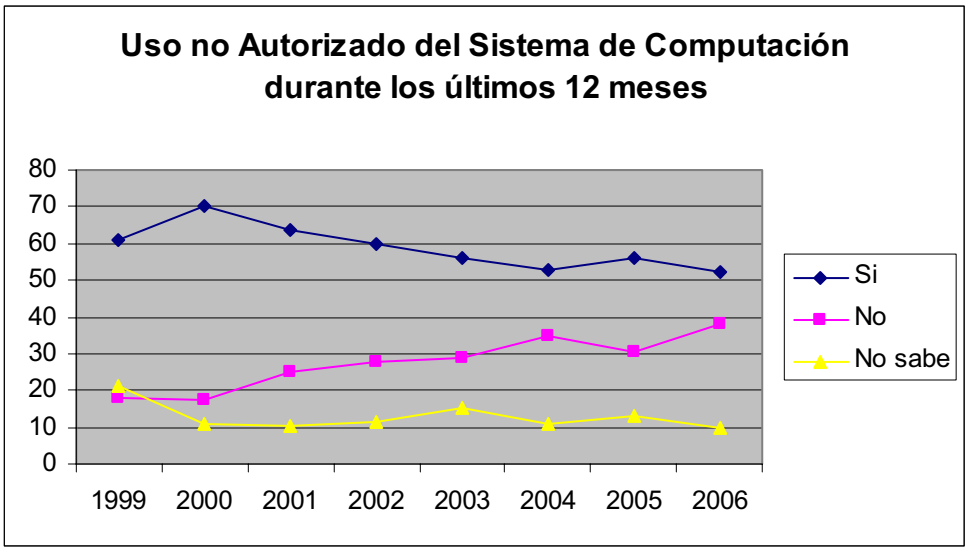
Fuente: Gordon, Lawrence A.; Loeb, Martin P.; Lucyshyn, William; Richardson, Robert. **"2006 CSI/FBI Computer Crime and Security Survey".** 2006.

Tabla VI. ¿Tiene su firma alguna póliza de seguro externo para manejar el ciber-riesgo?

Tiene	No Tiene
29%	71%

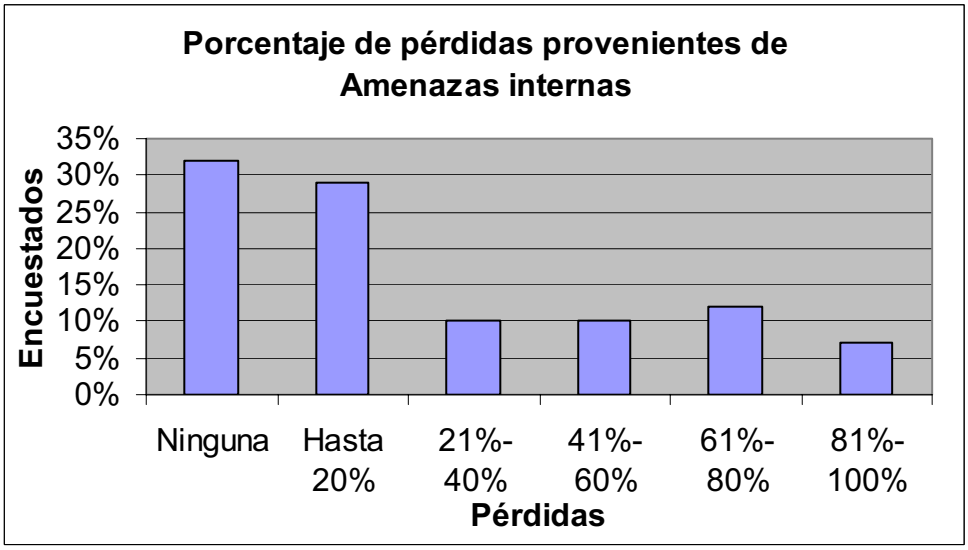
Fuente: Gordon, Lawrence A.; Loeb, Martin P.; Lucyshyn, William; Richardson, Robert. **"2006 CSI/FBI Computer Crime and Security Survey".** 2006.

Figura 2. Uso no autorizado del sistema de computación en los últimos doce meses



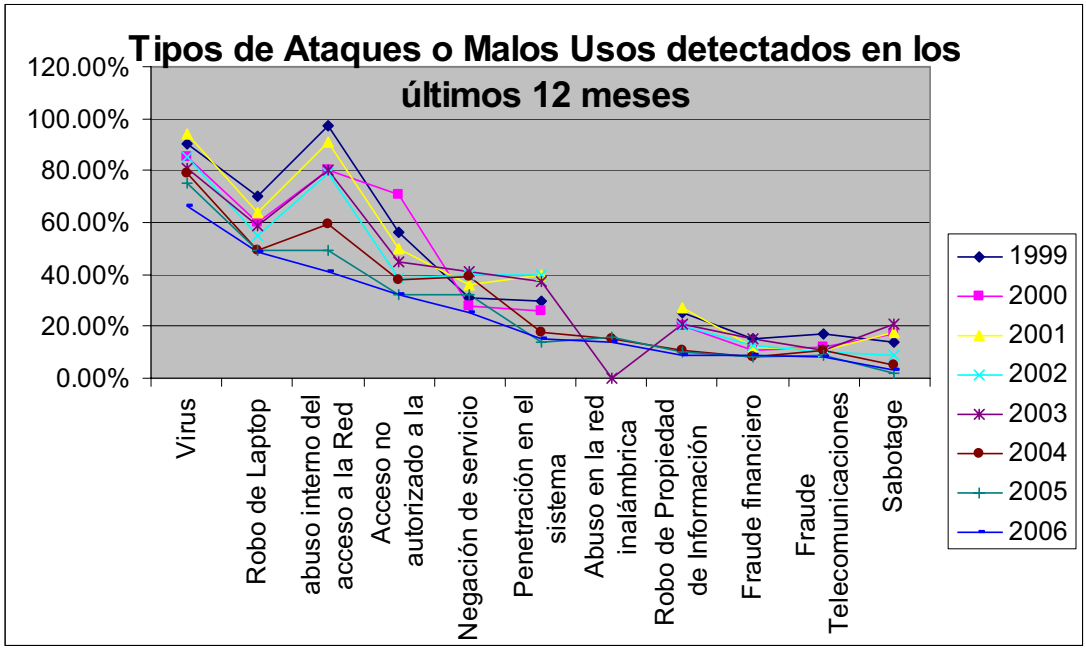
Fuente: Gordon, Lawrence A.; Loeb, Martin P.; Lucyshyn, William; Richardson, Robert. **"2006 CSI/FBI Computer Crime and Security Survey".** 2006.

Figura 3. Porcentaje de pérdidas provenientes de amenazas internas.



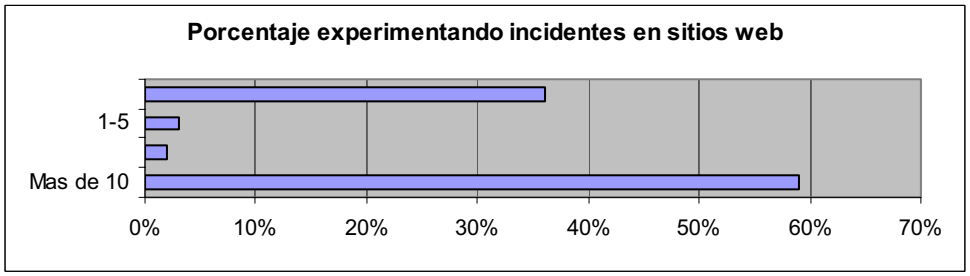
Fuente: Gordon, Lawrence A.; Loeb, Martin P.; Lucyshyn, William; Richardson, Robert. **"2006 CSI/FBI Computer Crime and Security Survey".** 2006.

Figura 4. Tipos de ataques o malos usos detectados en los últimos 12 meses.



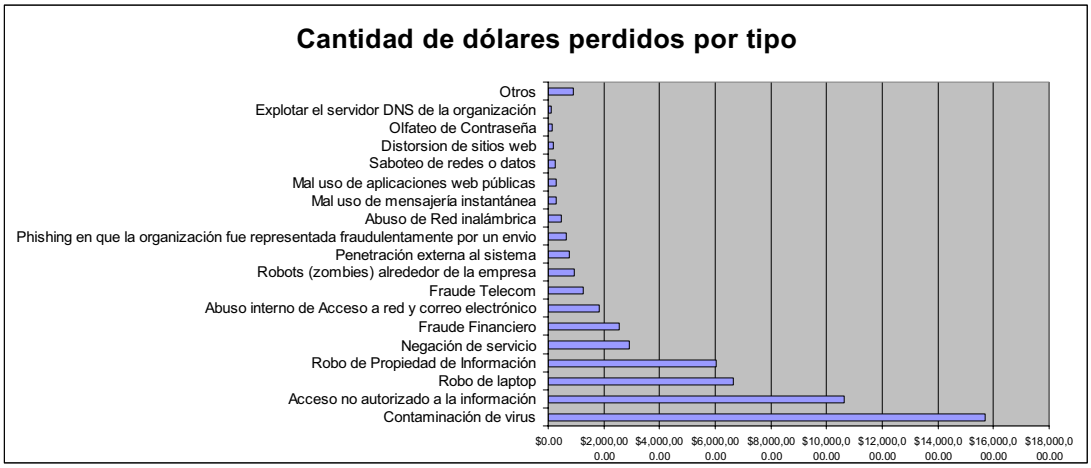
Fuente: Gordon, Lawrence A.; Loeb, Martin P.; Lucyshyn, William; Richardson, Robert. **"2006 CSI/FBI Computer Crime and Security Survey".** 2006.

Figura 5. Porcentaje experimentando incidentes en sitios web.



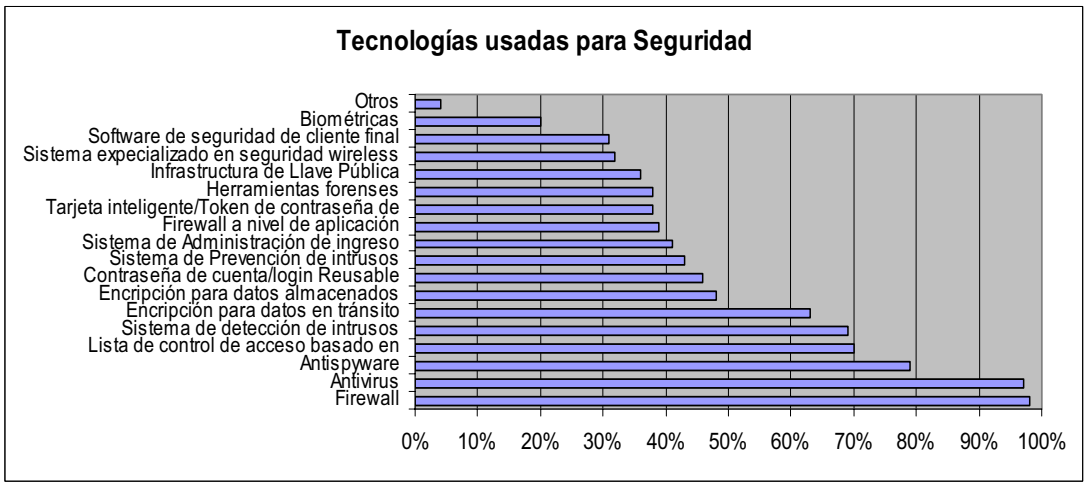
Fuente: Gordon, Lawrence A.; Loeb, Martin P.; Lucyshyn, William; Richardson, Robert. **"2006 CSI/FBI Computer Crime and Security Survey".** 2006.

Figura 6. Cantidad de dólares perdidos por tipo.



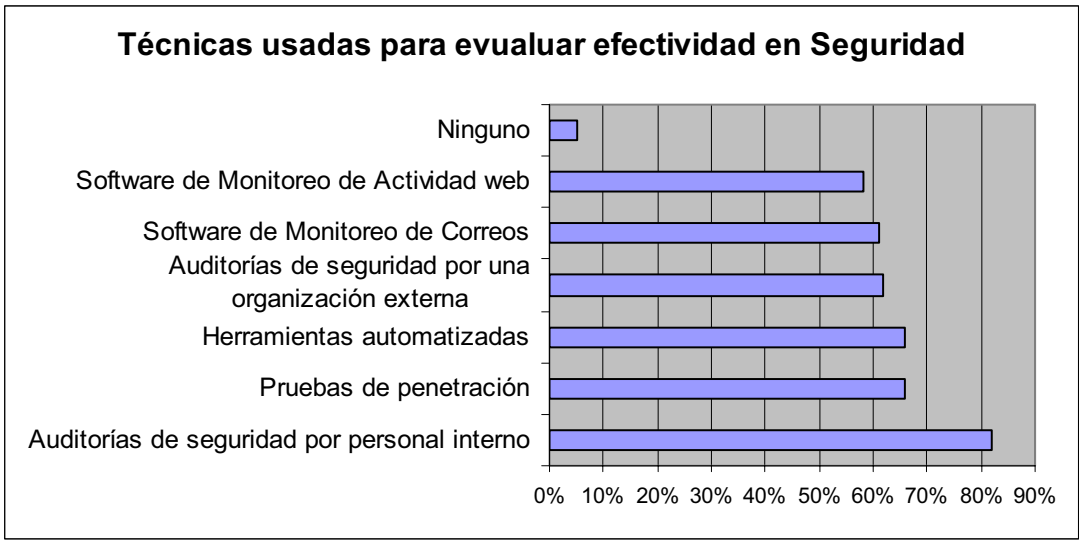
Fuente: Gordon, Lawrence A.; Loeb, Martin P.; Lucyshyn, William; Richardson, Robert. **"2006 CSI/FBI Computer Crime and Security Survey".** 2006.

Figura 7. Tecnologías utilizadas para seguridad



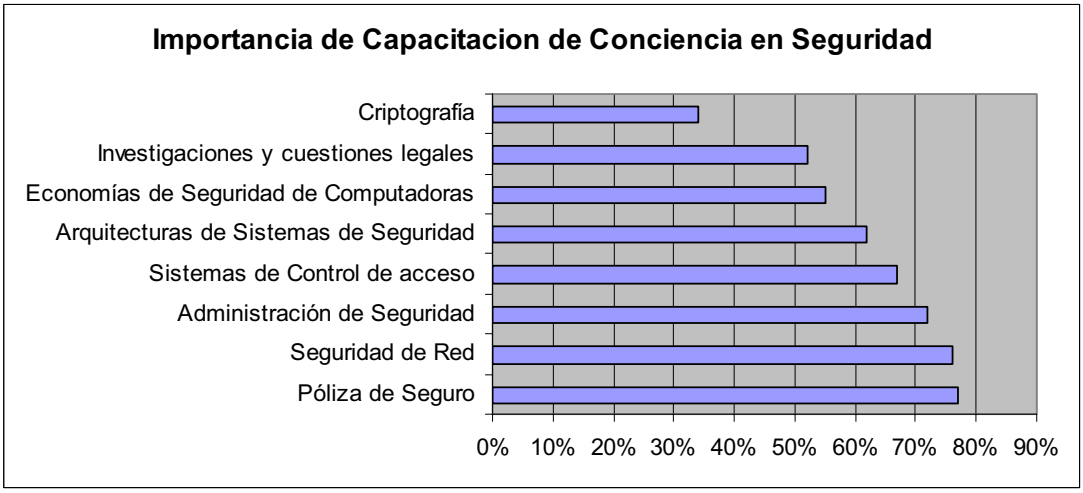
Fuente: Gordon, Lawrence A.; Loeb, Martin P.; Lucyshyn, William; Richardson, Robert. **"2006 CSI/FBI Computer Crime and Security Survey".** 2006.

Figura 8. Técnicas utilizadas para evaluar la efectividad en seguridad.



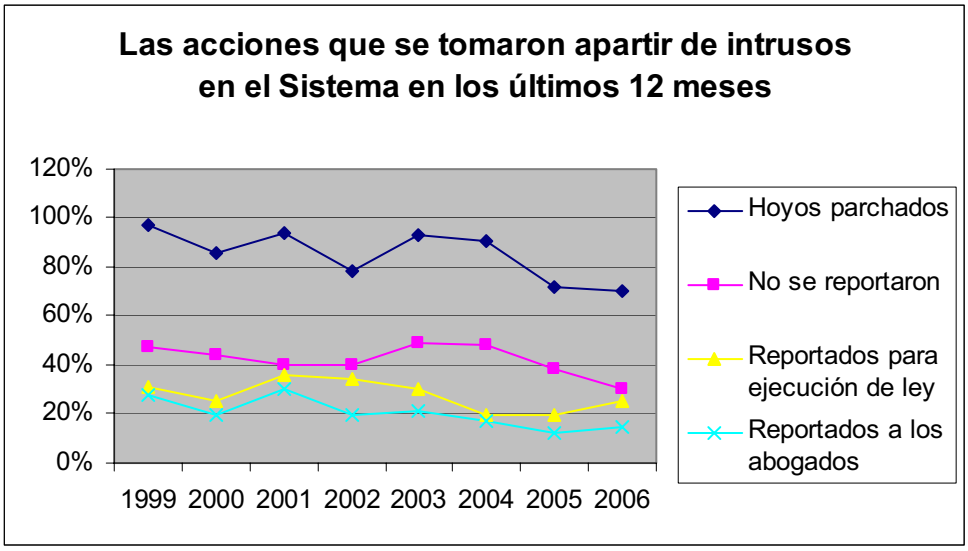
Fuente: Gordon, Lawrence A.; Loeb, Martin P.; Lucyshyn, William; Richardson, Robert. **"2006 CSI/FBI Computer Crime and Security Survey".** 2006.

Figura 9. Importancia en capacitación de conciencia en seguridad



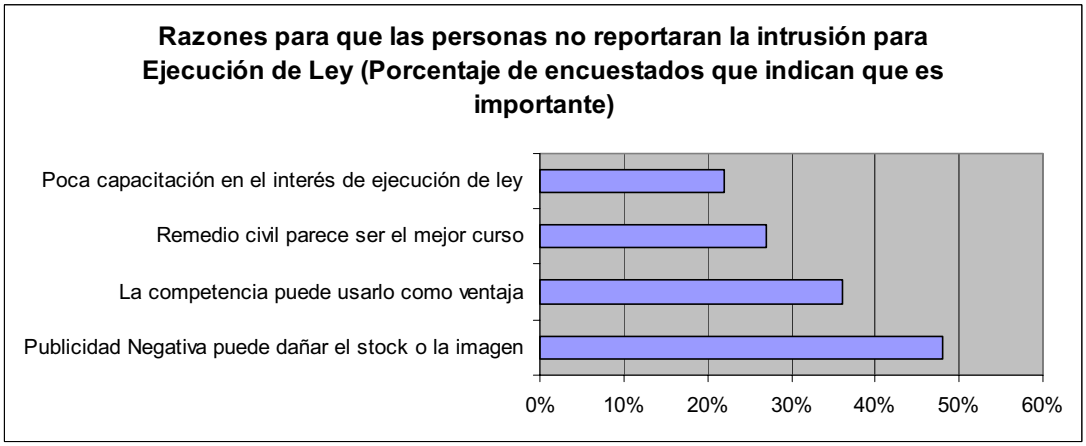
Fuente: Gordon, Lawrence A.; Loeb, Martin P.; Lucyshyn, William; Richardson, Robert. **"2006 CSI/FBI Computer Crime and Security Survey".** 2006.

Figura 10. Las acciones que se tomaron a partir de intrusos en el sistema en los últimos doce meses.



Fuente: Gordon, Lawrence A.; Loeb, Martin P.; Lucyshyn, William; Richardson, Robert. **"2006 CSI/FBI Computer Crime and Security Survey".** 2006.

Figura 11. Razones para que las personas no reporten la intrusión para ejecución de ley



Fuente: Gordon, Lawrence A.; Loeb, Martin P.; Lucyshyn, William; Richardson, Robert. **"2006 CSI/FBI Computer Crime and Security Survey".** 2006.

3.4.3. Empresas que ofrecen este tipo de Seguro

A lo largo de los últimos cinco años, el mercado del ciber-seguro se ha extendido por todo el mundo y ha ampliado la gama de opciones que ofrecen. Dentro de las empresas que ofrecen este tipo de seguro, se encuentran tanto grandes empresas de seguros como algunas pequeñas pero más especializadas. Algunos corredores venden solamente pólizas de responsabilidad, pero la mayoría ofrece una combinación de cobertura de propiedad, robo, y responsabilidad. Mayormente, los productos de ciber-seguro están diseñados para mercados específicos, como por ejemplo a empresas que se dedican a dar servicios financieros. En la siguiente tabla se muestran algunas empresas que ofrecen este tipo de servicio.

Tabla VII. Cobertura que ofrecen los corredores de ciber-seguro más grandes

	Cobertura	ACE	AIG	CHUBB	CNA	ST. PAUL TRAVELERS	ZURICH
Propiedad y Robo	Destrucción de Información o Software	X	X	X	X	X	X
	Recuperación de virus y otros códigos maliciosos		X	X	X	X	X
	Interrupción de negocios	X	X	X	X	X	X
	Negación de Servicio	X	X	X	X		X
	Robo de información		X	X	X		X
	extorsión cibernética	X	X	X	X		X
	Pérdidas debidas a actos terroristas	X	X	X	X	X	X
Responsabilidad	Seguridad de Red	X	X	X	X	X	X
	Daño a medios electrónicos de contenido	X	X	X	X	X	X
	Brecha privada de confidencialidad	X	X	X	X	X	X

En la tabla anterior se muestran las empresas más grandes que ofrecen este tipo de seguro y las coberturas respectivas que ofrece cada uno. Lo que se puede concluir de la tabla anterior es que todas estas empresas incluyen dentro de los paquetes que ofrecen, una gran diversidad de opciones para el cliente. Con esto los clientes pueden sentirse más seguros y confiados. Como se puede apreciar ahora, existe una amplia gama de aseguradoras que contemplan este tipo de seguro. En el siguiente capítulo se puede apreciar un ejemplo de una póliza de seguro que AIG ofrece.

4. PÓLIZA DE SEGURO QUE CUBRA EL RIESGO DE SEGURIDAD DE RED Y PROPIEDAD INTELECTUAL EN GUATEMALA

“American International Group, Inc. (AIG) es líder mundial de seguros y servicios financieros. Actualmente se puede encontrar en más de 130 países alrededor del mundo”[38]. AIG ofrece una amplia gama de seguros que van desde seguros de vida hasta seguros para comercios, incluyendo seguros contra el ciber-riesgo. Dentro del seguro contra ciber-riesgo que ofrecen, tienen una amplia variedad y ofrecen cobertura contra interrupción de negocio; empleados; administración de crisis para robo de identidad; administración de crisis; ciber-extorsión; activos de información; dispositivos de Internet; y, seguridad y privacidad, cada uno es un módulo de la póliza. A continuación se toma como referencia la Póliza de Seguro contra ciber-riesgo que ofrece, pero adaptada a Guatemala, y específica en el módulo de seguridad y privacidad.[39]

Esta póliza pretende dar un ejemplo para implementar una póliza en Guatemala, está revisada y validada por el Licenciado Eduardo Zumbado, Actuario de la Aseguradora G&T de Guatemala. Existen datos como el valor de la póliza que requieren de mucha investigación para calcularlo y este trabajo de graduación no pretende realizar esos cálculos que deben ir basados en estadísticas de incidencias de estos riesgos en empresas de Guatemala.

4.1. Póliza

4.1.1. Acuerdos del seguro:

Este seguro cubre la responsabilidad civil por daños y perjuicios y la defensa de los asegurados que pudieran sobrevenir sobre el asegurado por un evento cubierto por la póliza, según se detalla en la cláusula con respecto a reclamos realizados contra un asegurado y reportados a nosotros durante el período de vigencia de la póliza sujeto a los términos, condiciones, exclusiones y otras limitaciones en esta póliza,

4.1.1.1. Cobertura a: responsabilidad civil por daños y perjuicios

Debemos pagar gastos, en exceso a la retención aplicable, todas aquellas ocasiones en que el asegurado o cualquier asegurado adicional estén legalmente obligados a pagar tantos daños como gastos por reclamos incurridos por un reclamo realizado contra el asegurado o el asegurado adicional, y reportado a nosotros por escrito durante el período de la póliza por hechos ilícitos que usted haya realizado.

4.1.1.2. Cobertura b: defensa de los asegurados

Nuestro deber para defender a los asegurados: Tenemos el derecho y la obligación de defender una demanda dada en contra de un asegurado por incurrir en hechos ilícitos cubiertos por esta póliza, aunque la demanda sea sin fundamento o fraudulenta.

4.1.1.2.1. Gastos de reclamo: debemos pagar por gastos de reclamo en que cualquier asegurado incurre teniendo nuestro consentimiento por escrito en defensa de una demanda por hechos ilícitos cubiertos por esta póliza que ocurrieron durante el período de la póliza.

4.1.1.2.2. Nuestro derecho para investigar y resolver reclamos: tenemos el derecho, pero no la obligación de investigar cualquier reclamo en contra del asegurado. En caso de que investiguemos cualquier reclamo y el asegurado incurriera en gastos por reclamo, una vez que tenga nuestro consentimiento por escrito como resultado de esta investigación, debemos pagar los gastos por reclamo.

4.1.1.2.3. Su derecho a resolver: Usted puede resolver cualquier reclamo de este seguro si y solo si (i) todos los asegurados están de acuerdo, y (ii) sin incurrir en pérdidas en exceso de la retención.

4.1.1.2.4. Cuándo termina nuestra obligación para defenderlo: nuestra obligación termina cuando se agote el límite de la póliza de responsabilidad o el sublímite aplicable de responsabilidad por pago de pérdidas, incluyendo gastos de reclamo. Nuestra obligación para defenderlo también termina si usted falla o se rehúsa a consentir una resolución que nosotros recomendamos y que el que reclama va a aceptar. Entonces usted debe defender el reclamo a sus propias expensas. Como consecuencia de tal falla o negativa; nuestra responsabilidad por pérdidas no puede exceder el monto por el cual nosotros podríamos haber resuelto el reclamo que usted podría haber consentido, sumándole los gastos por reclamo incurridos antes de la fecha de tal falla o negativa.

4.1.2. Definiciones:

4.1.2.1. “Acceso no autorizado” se refiere a la obtención de acceso a un sistema computacional por una persona o personas no autorizadas.

4.1.2.2. “Acción reguladora” es una petición por información, demanda investigativa civil o procedimiento civil iniciado por una queja o petición similar, presentada por o en beneficio de una agencia gubernamental que reclama un peligro a la privacidad como fue definido en la definición de peligro a la privacidad, que pueda, dentro de lo razonable, dar lugar a una demanda cubierta.

4.1.2.3. “Asegurado” se refiere a cada:

4.1.2.3.1. Uno de ustedes; y

4.1.2.3.2. Asegurado.

4.1.2.4. “Asegurado adicional” se refiere a cualquier persona o entidad (i) que una organización ha acordado expresamente por escrito, antes de cometer un hecho ilícito, agregar como un asegurado bajo esta póliza, pero solamente por hechos ilícitos de la organización; y (iii) cualquier empleado de la entidad descrita o enlistada.

4.1.2.5. “Asegurado nombrado” se refiere a la entidad nombrada en las Declaraciones.

4.1.2.6. “Ataque de computadora” se refiere al acceso no autorizado, uso no autorizado, recepción o transmisión de código malicioso o al ataque de negación de servicio que:

4.1.2.6.1. Altera, copia, se apropia equivocadamente, corrompe, destruye, interrumpe, elimina, daña o previene, restringe u obstaculiza el acceso a un sistema computacional;

4.1.2.6.2. Resulta en divulgación de información privada o confidencial almacenada en un sistema computacional; o

4.1.2.6.3. Resulta en robo de identidad.

4.1.2.6.4. Si cualquiera de lo anterior es intencional o sin intención alguna, malicioso o accidental, fraudulento o inocente, dirigidos específicamente para usted o distribuidos a nivel general, no importando si el perpetrador espera obtener una ganancia o no.

4.1.2.7. “Ataque de negación de servicio” se refiere a un ataque puesto en marcha por una persona(s) que envía un volumen excesivo de datos electrónicos a un sistema computacional, con el propósito de agotar la capacidad de dicho sistema computacional, e impedir el acceso a aquellos que están autorizados por ley. El consumo en exceso de los recursos del sistema computacional, no debe ser considerado un ataque de negación de servicio si es causado por un error en la determinación de las necesidades de capacidad.

4.1.2.8. “Código malicioso” se refiere a una pieza de código corrupto o dañino no autorizado. “código malicioso” incluye, pero no se limita a: virus de computadoras, “troyanos”, “gusanos”, y “bombas de tiempo y lógicas”.

4.1.2.9. “Control administrativo” se refiere a: (1) intereses propios representando más del cincuenta por ciento (50%) de los votos, citas o designación de poder para la selección de una mayoría de: la Junta Directiva de una corporación, los miembros del comité administrativo de una alianza estratégica o sociedad, o los miembros de la junta administrativa de una compañía de responsabilidad limitada; o (2) teniendo el derecho, de conformidad con el contrato por escrito o los estatutos, carta, acuerdo operativo o documentos similares de una organización, para elegir, citar o designar una mayoría de: la Junta Directiva de una corporación, el comité administrativos de una alianza estratégica o sociedad, o la junta administrativa de una compañía de responsabilidad limitada.

4.1.2.10. “Daños” se refiere a cualquier cantidad de dinero que a cualquier asegurado se le ha solicitado legalmente pagar, establecido por juzgados, advertencias de arbitro, o las que son suscitadas contra un asegurado, o por resoluciones negociadas, ya sea por la aseguradora o por usted incluyendo, pero no limitada a:

4.1.2.10.1. Intereses de prejuicio;

4.1.2.10.2. Intereses de post-juicio que se adquieran después de entrar en juicio y antes de que la aseguradora le pague, le ofrezca pagar o depositar esa parte del juicio, dentro del sublímite aplicable de responsabilidad; y

4.1.2.10.3. La definición está sujeta a las limitantes enunciadas en la Definición de pérdida

4.1.2.11. “Demanda” se refiere al procedimiento civil para socorro monetario, no-monetario o de mandato judicial que comienza a razón del servicio de una denuncia o escrito similar; sin embargo, la demanda no tendrá incluida una acción regulatoria. Demanda incluirá también un procedimiento de arbitraje obligatorio en el cual los daños son reclamados, los cuales usted debe enviar o hacer enviar con nuestro previo consentimiento escrito.

4.1.2.12. “Empleado” se refiere a cualquier empleado pasado, presente o futuro, incluyendo a los empleados de medio tiempo, vacacionista, o temporal, considerados así solamente por hechos ilícitos realizados durante el desempeño del empleo mismo. También incluye cualquier trabajador pasado, presente o futuro pero solamente si cometió hechos ilícitos en el desempeño del trabajo realizado.

4.1.2.13. “Falla(s) de seguridad” se refiere a:

4.1.2.13.1. Una falla como tal o inhabilidad de la seguridad de su sistema computacional para mitigar pérdida del mismo o prevenir un ataque de computadora; o

4.1.2.13.2. Robo físico de hardware o firmware controlado por una organización (o componentes de la misma) en que están almacenados datos electrónicos. Robo físico ejecutado por cualquier otra persona que no sea el asegurado, estando en alguno de los locales ocupados y controlados por una organización.

4.1.2.13.3. “Falla de seguridad” también debe incluir la presente falla e inhabilidad arriba descrita, resultando del robo de una contraseña o código de acceso de alguno de los locales de su organización, su sistema computacional, o algún ejecutivo, director o empleado de la organización por medios no-electrónicos en violación directa de una política o procedimiento de seguridad escrito específicamente para una organización.

4.1.2.14. “Gastos de reclamo” se refiere a lo razonable y necesario en (i) honorarios y gastos cargados por un abogado designado por la aseguradora y (ii) otros honorarios, costos y gastos incurridos en defensa o investigación de un reclamo contra el asegurado, ya sea designado por la aseguradora o por un asegurado previo el consentimiento por escrito.

4.1.2.15. “Hecho ilícito” se refiere a cualquier omisión del deber, negligencia, hecho, error u omisión real o alegada que resulte en un fallo de seguridad; o en un peligro a la privacidad.

4.1.2.16. “Internet” se refiere a la red de computadoras pública en todo el mundo comúnmente conocida como Internet, así como existe actualmente o como podría ser manifestada en el futuro.

4.1.2.17. “Información confidencial corporativa” se refiere a cualquier comercio secreto, datos, diseño, interpretación, predicción, fórmula, método, práctica, proceso, registro, reporte u otro objeto de información de una tercer parte no-asegurada, y la cual está (i) bajo su cuidado, custodia o control; (ii) no disponible para el público en general, y es: (iii) provisto a usted bajo un acuerdo mutuo para el acuerdo escrito confidencial/de no-divulgación; o (iv) marcado “confidencial” o de otra manera específicamente diseñado por escrito como “confidencial” por tal tercera parte.

4.1.2.18. “Información personal identificable” se refiere a cualquiera de los siguientes a su cuidado, custodia o control: (1) información por la cual un individuo puede ser identificable o contactado de forma única y responsable, incluyendo sin limitación, el nombre, dirección, número telefónico, número de afiliación al IGSS, números de cuentas, balances de cuentas, historial de cuentas y contraseñas del individuo; (2) información concerniente a un individuo que se considera “información personal no pública”.

4.1.2.19. “Información privada” se refiere a lo siguiente:

4.1.2.19.1. Información identificable en relación a su persona, o que permita identificar a su persona.

4.1.2.19.2. Información confidencial corporativa.

4.1.2.20. “Límite de responsabilidad de póliza” se refiere al límite agregado de responsabilidad establecido como tal en las Declaraciones.

4.1.2.21. “Material” se refiere a contenido en cualquier forma, incluyendo contenido escrito, impreso, en video, electrónico, digital o contenido digitalizado:

4.1.2.21.1. En emisiones, incluyendo, pero no limitándose a, televisión, películas animadas, cable, televisión satelital y emisiones de radio;

4.1.2.21.2. En publicaciones, incluyendo, pero no limitándose a, periódico, boletín, revista, libro y otras publicaciones literarias, monográficas, guías, directorio, juego de pantalla, script de películas, publicaciones de video.

4.1.2.21.3. En publicidad; o

4.1.2.21.4. Desplegado en un sitio de Internet.

4.1.2.22. “Nosotros”, “aseguradora”, y “nuestro” se refiere a la aseguradora nombrada como tal.

4.1.2.23. “Organización” se refiere a: (1) el asegurado nombrado; y (2) cada subsidiario.

4.1.2.24. “Peligro de privacidad” se refiere a cualquier actual o supuesto:

4.1.2.24.1. Divulgación no autorizada por usted de información privada o usted falla en proteger información privada de apropiación indebida, incluyendo, sin limitación, cualquier violación no intencional de su póliza de privacidad o apropiación indebida que resulte en robo de identidad;

4.1.2.24.2. Falla el titular de información en proteger información personal identificable de apropiación indebida, siempre que cualquiera falla para proteger dicha información no incluye ningún hecho ilícito, intencional, deshonesto, fraudulento o criminal, error u omisión si se cometió por:

4.1.2.24.2.1. El titular de información

4.1.2.24.2.2. Cualquier oficial o director de titular de información, elegido o citado; o

4.1.2.24.2.3. Cualquier empleado (que no sea un oficial) o contratista independiente contratado por un titular de información si existe un titular de información electo o citado que posee, en cualquier momento, conocimiento del hecho intencional, deshonesto, fraudulento, criminal o ilícito realizado por tal empleado o contratista independiente que causaron una pérdida directa hacia un asegurado o cualquier otra persona.

4.1.2.24.3. El fallo por su parte en informar o advertir sobre un robo de identidad tanto real como potencial, pero solo si tal robo de identidad resultase directamente de las definiciones vistas anteriormente; o

4.1.2.24.4. La violación de cualquier estatuto de privacidad federal, estatal, extranjero local en relación a una reclamo por daños por las definiciones vistas anteriormente.

4.1.2.25. “Pérdida” se refiere a la suma total de daños y gastos de reclamo. “Gastos por reclamo”, “daños” y “pérdida” no se refiere a y esta póliza no debe cubrir: (1) compensación, beneficios, cargos generales o gastos de cualquier asegurado o los empleados del asegurado; (2) costos de producción o el costo de recordatorio, reproducción, reimpresión o corrección de material por cualquier persona o entidad; (3) su costo de proveer, corregir o redesarrollar, o completar cualquier servicio profesional; (4) cualquier costo o gasto incurrido por cualquier persona o entidad para retirar o retener material, medios de comunicación, medio (incluyendo CD’s, DVD’s, cassettes y LP’s), productos (incluyendo productos de otros que incorporen los productos que usted ofrece) o servicios profesionales del mercado o por falta de uso a causa de tal retiro o retención; (5) multas o penalidades civiles o criminales impuestas contra usted; (6) impuestos en contra de usted; (7) cualesquiera cantidades para las cuales un asegurado no es financieramente responsable o para las cuales no exista recurso legal contra el asegurado; (8) los costos y gastos de cumplimiento por cualquier mandato judicial o cualquier otra forma de socorro equivalente; (9) el valor monetario de cualquier transferencia hacia, desde o entre cuentas de un asegurado; (10) daños liquidados; y (11) cuestiones que pueden ser consideradas no asegurables en virtud de las leyes vigentes conforme a la cual esta póliza se construirá.

4.1.2.26. “Período de póliza” se refiere al período establecido como tal en las Declaraciones.

4.1.2.27. “Primera fecha de creación” se refiere a la fecha enunciada en las Declaraciones.

4.1.2.28. “Política de privacidad” se refiere a las políticas y prácticas de la organización destinadas a proteger la confidencialidad de la información privada, incluyendo sin limitación, declaraciones por escrito o en forma electrónica con respecto a la colección, difusión o tratamiento de información personalmente identificable.

4.1.2.29. “Publicidad” se refiere al material en cualquier publicidad o promoción incluyendo de marca, patrocinadores y/o adicionales.

4.1.2.30. “Reclamo” significa:

4.1.2.30.1. Una demanda escrita u oral por dinero, servicios, socorro no monetario por mandato judicial.

4.1.2.30.2. Una demanda, o,

4.1.2.30.3. Una acción regulatoria

4.1.2.31. “Reclamo de acción grupal” se refiere a cualquier reclamo derivado de un hecho ilícito que resulta en un peligro de privacidad:

4.1.2.31.1. Surgido en nombre de un grupo o supuesto grupo de demandantes (sean o no certificados como tales);

4.1.2.31.2. De otro modo, surgido sobre una base representativa; o

4.1.2.31.3. Alegando o derivando del mismo hecho ilícito o una serie continua, repetida o relacionada de los hechos ilícitos como cualquier reclamo descrito en los subpárrafos precedentes (ee)(1) o (ee)(2).

4.1.2.32. “Robo de identidad” se refiere a la apropiación indebida de información privada que resulta en, o podría resultar en el uso ilícito o fraudulento de esta información, incluyendo sin limitación, emulación fraudulenta de la identidad de un individuo o empresa.

4.1.2.33. “Secreto comercial” se refiere a información (incluyendo cualquier idea) que ha sido reducida a un formulario escrito o electrónico, incluyendo fórmula, compilación, patrón, programa, dispositivo, método, proceso, o técnica que: (1) deriva valor económico independiente, actual o potencial, de no ser conocido a nivel general, de su divulgación o uso; (2) es objeto de esfuerzos razonables para mantener su secreto; y (3) es utilizada, capaz de ser utilizada, o está destinada a ser utilizada en comercio.

4.1.2.34. “Seguridad” se refiere al hardware, software o firmware cuyas funciones o propósito es mitigar pérdida de o prevenir un ataque de computadora. Seguridad incluye, sin limitaciones, firewalls, filtros, DMZ’s software para protección de virus de computadora, detección de intrusos, el uso electrónico de contraseñas o identificación similar de usuarios autorizados. Seguridad también incluye sus políticas y procedimientos específicos por escritos con la intensión de prevenir el robo de una contraseña o código de acceso por medios no electrónicos.

4.1.2.35. “Sistema computacional” se refiere al hardware, software, firmware y componentes de computadora, incluyendo los datos almacenados electrónicamente en ella, enlazados todos a través de una red de dos o más computadoras, incluyendo las redes que se acceden por el Internet, intranets, extranets, o redes virtuales privadas.

4.1.2.36. “Su sistema computacional” se refiere a un sistema computacional bajo la propiedad, operación y control de su organización.

4.1.2.37. “Sublimite de responsabilidad” se refiere a cada uno de los sublímites de responsabilidad respectivos establecidos en las Declaraciones

4.1.2.38. “Subsidiario” se refiere a:

4.1.2.38.1. Cualquier entidad lucrativa para la cual el asegurado nombrado tiene el control administrativo (“entidad de control”) en o antes de la creación del período de póliza ya sea directa o indirectamente a través de una u otras entidades de control más; o

4.1.2.38.2. Las entidades listadas como tal con nuestro consentimiento como agregado a esta póliza.

4.1.2.39. “Titular de información” se refiere a un tercero al que usted tiene ha provisto de información personal identificable.

4.1.2.40. “Trabajador subcontratado” se refiere a cualquier persona provista por un contratista o agencia de empleo que bajo un acuerdo entra a una organización y a cualquier contratista o agencia contratados para desempeñar funciones relacionadas con el comportamiento de un negocio de la empresa.

4.1.2.41. “Uso no autorizado” se refiere al uso de un sistema computacional por una persona o personas no autorizadas o una persona o personas autorizadas de una forma no autorizada.

4.1.2.42. “Usted”, “asegurado” o “su” se refiere a cada una y toda (1) organización y (2) empleado de una organización.

4.1.3. Eventos cubiertos

4.1.3.1. Cualquier impericia, negligencia, acto, error u omisión como tal o bajo reclamo que resulte de:

4.1.3.1.1. Una falla o inhabilidad en la seguridad de su sistema computacional para mitigar la pérdida del sistema o prevenir un ataque computacional.

4.1.3.1.2. Robo físico de hardware en que estén almacenados datos electrónicos o firmware, ejecutado por cualquier otra persona que no sea el asegurado, estando en alguno de los locales de la empresa asegurada.

4.1.3.1.3. Falla o inhabilidad (en la seguridad de su sistema computacional para mitigar la pérdida del sistema o prevenir un ataque computacional) que resulte del robo de una contraseña o código de acceso de algún local, de su sistema computacional, de algún ejecutivo, director o empleado de la empresa.

4.1.3.1.4. Divulgación no autorizada por parte suya de información privada.

4.1.3.1.5. Falla en proteger información privada de apropiación indebida.

4.1.3.1.6. Falla en informar o advertir sobre un robo de identidad tanto real como potencial.

4.1.4. Exclusiones

Esta póliza no cubre ningún reclamo sobre:

4.1.4.1. Cualquier responsabilidad u obligación bajo cualquier contrato o acuerdo, incluyendo, sin limitación, cualquier precio contractual, garantía o estimado de costo que haya sido excedido; sin embargo esta exclusión no aplica a:

4.1.4.1.1. La responsabilidad que usted tendría en ausencia de dicho contrato o acuerdo; o

4.1.4.1.2. Con respecto a un Peligro a la privacidad, cualquier responsabilidad u obligación bajo un acuerdo de confidencialidad o de no divulgación.

4.1.4.2. Con respecto a un “peligro a la privacidad”:

4.1.4.2.1. La recolección de información privada, incluyendo, sin limitación (i) métodos de recolección por medio de “cookies” electrónicas, “spiders”, spybots, spambots, spyware, adware, wire-tapping, código malicioso, mantener un log de teclas presionadas, dispositivos de rastreo, chip o etiqueta de identificación por frecuencia de radio, bugging (poner micrófonos) o cámaras de video; o (ii) el fallo al notificar apropiadamente: (a) el propósito por el cual la información privada está siendo recolectada y utilizada; (b) información de contacto para quejas y preguntas; (c) aquellos grupos a quienes les será revelada la información privada; (d) las opciones del individuo o entidad a la que usted está recolectando la información privada; o (e) los medios que usted ofrece para limitar el uso o la revelación de información privada; proveyendo, sin embargo, que esta exclusión no aplicará a cualquier reclamo cubierto o hecho ilícito que resulte en un peligro a la privacidad.

4.1.4.2.2. La integridad de la información privada, incluyendo si la información privada es: (i) relevante y confiable para el propósito para el que es recolectado o para el que se piensa utilizar; (ii) confiable; (iii) completa; o (iv) actual;

4.1.4.2.3. Su provisión, o falla al proveer, acceso a información privada a aquellos individuos o entidades con derecho real o reclamado para dicho acceso, incluyendo, sin limitantes, el fallar en proveer a un ente o individuo la habilidad de corregir, enmendar o borrar información privada.

4.1.4.2.4. Su distribución de mercadeo, correos electrónicos o publicidad no solicitada, incluyendo, sin limitantes, mensajes electrónicos no solicitados, publicidad en chat's, publicidad en pizarras de anuncios, publicidad en grupos de noticias, anuncios por medio de pop-ups o pop-unders en Internet, bombardeo de maquinas de fax, envío de correos físicos o tele marketing; sin embargo, esta exclusión no aplicara a cualquier reclamo o hecho ilícito que haya resultado de un peligro a la privacidad; o

4.1.4.2.5. Su distribución, creación, exhibición, presentación, impresión, reproducción, publicación, divulgación, despliegue, investigación o serialización de cualquier material.

4.1.5. Límite de responsabilidad (para todas las pérdidas, incluyendo gastos de reclamo)

4.1.5.1. El total de límite de responsabilidad de la póliza establecido es lo máximo que se les pagará como pérdida en esta póliza, en el total, para todas las coberturas combinadas, no importando el número de personas, ocurrencias, reclamos o entidades cubiertas por esta póliza, o reclamantes o reclamos recibidos contra cualquier asegurado.

4.1.5.2. Daños, gastos de reclamo y pérdidas, son todos parte de y sujetos al límite y los sublimites de responsabilidad de la póliza.

4.1.6. Retención

4.1.6.1. Retención: para cada reclamo, la aseguradora solamente debe ser responsable por la cantidad de pérdida derivada de dicho reclamo que exceda a la cantidad aplicable de retención. De dichas cantidades de retención deberán hacerse cargo los asegurados y permanecer no asegurado con respecto a todas las pérdidas. En caso de que un reclamo dispare más de una cantidad de retención, entonces para ese reclamo, la cantidad de retención más alta debe ser considerada la cantidad aplicable de la retención de pérdidas provenientes a dicho reclamo. Una cantidad de retención individual debe aplicarse a pérdidas provenientes de todos los reclamos alegando los mismo hechos ilícitos, o series de hechos ilícitos continuos, repetidos o relacionados.

4.1.7. Notificación y autoridad:

4.1.7.1. General: Cualquier notificación relacionada con esta póliza debe ser presentada a nosotros. Esta sección debe incluir la dirección física del lugar a donde pueden notificar alguna anomalía, los reclamos o cualquier duda o cambio que se tenga respecto a la póliza. Cada nombrado de asegurado debe actuar de acuerdo con todos y cada asegurado con respecto a la recepción o entrega de cualquier notificación bajo esta póliza, incluyendo, pero no limitado a, notificación de un reclamo y notificación de cancelación. Si se envía por correo electrónico, la fecha del envío constituye la fecha en que dicha notificación o información fue entregada y la prueba del envío debe ser prueba suficiente de notificación.

4.1.7.2. Reclamos: para cualquiera y toda cobertura que bajo esta póliza se ofrece en base a los reclamos hechos y reportados:

4.1.7.2.1. Antes de que la cobertura aplique, un asegurado debe notificarnos por escrito de un reclamo hecho primero contra un asegurado tan pronto sea posible, pero en todo evento no más tarde que el fin del período de la póliza o cualquier período extendido de reporte aplicable; y

4.1.7.2.2. Si durante el período de póliza o durante un período extendido de reportes aplicable un asegurado debe ser advertido de cualquier circunstancia que razonablemente se puede esperar que surja un reclamo realizado en contra de un asegurado por un hecho ilícito que ocurre previo finalizar el período de póliza, y, durante el período de póliza o cualquier otro período extendido de reportes aplicable, un asegurado nos entrega notificación de (i) dichas circunstancias, (ii) las demandas por hechos ilícitos anticipados, y (iii) las razones para anticipar dicho reclamo, con todos los particulares, como fechas, personas y entidades involucradas, luego cualquier reclamo que es realizado subsecuentemente en contra de un asegurado derivado de dicho hecho ilícito o el mismo hecho ilícito o series de hechos ilícitos continuos, repetidos o relacionados, debe ser tratados como un reclamo realizado en contra de dicho asegurado y reportado a nosotros en el tiempo en que tal notificación de dichas circunstancias fue entregado.

4.1.7.3. Para todas y cualquier cobertura que esta póliza ofrece con base a una ocurrencia, usted debe notificarnos por escrito de cualquier reclamo en contra de usted tan pronto sea posible.

4.1.8. Derechos y deberes especiales del asegurado nombrado

Usted está de acuerdo que cuando es más de una persona natural o entidad cubierta bajo esta póliza, los asegurados nombrados listados en esta póliza deben actuar en nombre de todos los asegurados como para:

4.1.8.1. Entregar y recibir notificación, incluyendo, pero no limitado a, notificación de reclamos y cancelación;

4.1.8.2. El ejercicio o la disminución de cualquier derecho a un período extendido de reporte;

4.1.8.3. La resolución de cualquier disputa en relación con la cobertura ofrecida o supuestamente ofrecida por esta póliza;

4.1.8.4. El pago de primas y recepción de devolución de primas, si existiera; y

4.1.8.5. Aceptación de cualquier endoso u otro cambio a esta póliza.

4.1.9. Responsabilidades del asegurado

4.1.9.1. Revisar y actualizar sus pólizas de privacidad por lo menos una vez al año.

4.1.9.2. Contratar a un oficial en jefe de privacidad o establecer una posición en el organigrama de la empresa que sea responsable por la administración y aprobación de sus pólizas de privacidad.

4.1.9.3. Pasar una auditoría de privacidad externa o recibir una certificación de privacidad cada dos años.

4.1.9.4. Completar una auditoría interna o asesoramiento para determinar sí cumple con las regulaciones y leyes concernientes a los derechos de protección de privacidad cada año. Resolver las recomendaciones recibidas.

4.1.9.5. Establecer políticas en la empresa que restringa el acceso de archivos de consumos y clientes a los empleados.

4.1.9.6. Proveer capacitación para sus empleados en privacidad, seguridad de datos y cuestiones relacionadas.

4.1.9.7. Usted debe tener acuerdos en relación a compartir o intercambiar datos con otra empresa.

4.1.9.8. Si a usted le externalizan tecnología o funciones de procesamiento de datos debe requerir una demostración de seguridad en los sistemas computacionales.

4.1.9.9. Usted debe tener un programa de protección contra virus en su sistema. Este antivirus debe ser aprobado por nosotros.

4.1.9.10. Usted debe tener un firewall que proteja su sistema. Este firewall debe ser aprobado por nosotros.

4.1.9.11. Usted debe correr un proceso que actualice el software, parches y antivirus en su sistema computacional.

4.1.9.12. Usted debe tener controles físicos de seguridad colocados para controlar el acceso a su sistema computacional.

4.1.9.13. Usted debe tener un plan de respuesta ante un incidente de seguridad, establecido y bien estructurado.

4.1.9.14. Usted debe tener a una persona o un grupo responsable por la seguridad de información.

4.1.9.15. Usted debe establecer estándares de configuración en firewalls, routers, y sistemas operativos.

4.1.9.16. Usted debe tener un programa que periódicamente pruebe los controles de seguridad.

4.2. Datos generales para la póliza

4.2.1. Nombre de la aseguradora

4.2.2. Número de póliza

4.2.3. Asegurado Nombrado: [nombre del asegurado]

4.2.3.1. Dirección de correo: [dirección del asegurado]

4.2.4. Período de póliza: desde [fecha de inicio] hasta [fecha de fin]

4.2.5. Total de la póliza: Q[#,###.00]. El valor de la póliza se basa en estadísticas de incidencia de los riesgos asegurados y se debiera incluir en una secuencia que se realice sobre este trabajo de graduación.

4.2.6. Incluye los siguientes campos que se deben llenar:

4.2.6.1. Retención:

4.2.6.2. Fecha de creación

4.2.7. Nombre y dirección de la aseguradora: [nombre y dirección de la aseguradora que aplique]

4.2.8. Cobertura de seguridad de red: en esta sección se debe incluir un cuestionario que permita conocer al negocio.

4.2.9. Información histórica: en esta sección se incluye un cuestionario que permita conocer la historia del negocio, buscando previos ataques o vulnerabilidades del sistema.

CONCLUSIONES

1. Administración de ciber-riesgos implica entender primero qué son los ciber-riesgos y cuáles son los ciber-riesgos a los que está expuesta la compañía. Luego de conocer estos ciber-riesgos, la compañía debe crear políticas que la protejan; y dentro de estás políticas, una que no debe faltar y es fundamental es transferir estos riesgos a una aseguradora experta en ellos.

2. Para poder crear una póliza de seguro para cubrir un ciber-riesgo se realiza el mismo procedimiento que para una póliza de cualquier seguro. Dentro de lo que resalta, está la especificación del bien asegurado, que en este caso es el que cambia, porque puede ir desde una computadora física hasta la información que contenga una computadora; y, la suma asegurada que se determina dependiendo de estadísticas que muestren el porcentaje de incidencia de este tipo de riesgos.

3. El seguro contra ciber-riesgos es ya un hecho y está implantado en casi cualquier parte del mundo, pero en Guatemala no existe ninguna compañía que ofrezca este tipo de seguro.

4. Para poder crear una póliza de seguro que cubra el ciber-riesgo se debe tomar en cuenta primero que los activos que se están asegurando muchas veces no son tangibles, tanto la aseguradora como el cliente deben llegar a un acuerdo sobre el valor real del activo a asegurar.

5. En la Póliza de Seguro se debe delimitar con mucho detalle lo que va a asegurar y establecer el estado actual del bien asegurable.

6. En la Póliza de Seguro se debe incluir con el máximo detalle posible, las definiciones de los términos utilizados en la misma. Esto ayuda para no caer en ambigüedades entre el cliente y la aseguradora.

RECOMENDACIONES

1. En Guatemala, la población que tiene acceso a Internet ha crecido lo suficiente como para establecer como necesidad una ley que sustente y ampare el seguro contra ciber-riesgos, para poder proteger a todo ciudadano contra cualquier robo o manipulación de información.

2. Una campaña de información a la población guatemalteca para que sean concientes del peligro que corren a través de Internet o utilizando cualquier tipo de software.

3. La propuesta de esta Póliza de Seguro necesita de estadísticas sobre incidentes del ciber-riesgo en Guatemala para poder realizar cálculos para asignarle un monto a la prima y así completar parte de lo que falta para llevarla a la práctica.

4. En Guatemala, deben existir leyes que protejan tanto al asegurado como a la aseguradora sobre cualquier anomalía respecto a un ciber-seguro.

5. La implementación de está póliza de seguro en Guatemala es realmente urgente, para mejorar incluso las políticas de intercambio entre países y realmente saltar fronteras en el comercio.

REFERENCIAS

1. **“Diccionario”**.
   https://www.cmcool.es/CajaMadrid/Home/cruce/0,0,83018$P1%3D28,00.html
   2001-2009.

2. **“Glosario”**.
   http://www.economicas-online.com/glosarios/terminos.htm
   Marzo 2008.

3. **“Glosario C”**.
   http://www.hooping.net/glosario-c.aspx
   1995-2008.

4. **“Director Ejecutivo”**.
   http://es.wikipedia.org/wiki/CEO
   Mayo 2009.

5. **“Glosario básico de términos en la informática actual”**.
   http://www.ordenadores-y-portatiles.com/glosario-de-informatica.html
   2009.

6. **“Dicotomía”**.
   http://es.wikipedia.org/wiki/Dicotomía
   Mayo 2009.

7. **“Glosario”**.
   http://www.datarecsa.com/Glosario/glosarioe.htm
   2008.

8. **“Glosario de términos sobre internet”**.
   http://www.emprendedores.cl/estudios_trabajos/glosario.htm
   2008.

9. **“Glosario”**.
   http://www.mundonotarial.com.mx/Notario/Glosario_2.htm
   2000.

10. **“Gestión de Riesgos”**.
    http://es.wikipedia.org/wiki/Gestión_de_riesgos
    Junio 2009.

11. **“Diccionario del Hardware”**.
    http://www.conozcasuhardware.com/diccio/
    2009.

12. **“Glosario”**.
    http://www.laopinion.com/glossary/h.html
    2009.

13. **“Definiciones”**.
    http://www.asesoriainformatica.com/definiciones_i.htm
    2004-2009.

14. **“Glosario”**.
http://www.economicas-online.com/glosarios/terminos.htm
Marzo 2008.

15. **“Malware”**.
http://es.wikipedia.org/wiki/Malware
Junio 2009.

16. **“Términos”**.
http://www.uh.cu/facultades/fcom/portal/interes_glosa_terminos.htm
2009.

17. **“Diccionario de marketing y tecnología”**.
http://www.perugrafico.com/articulos/diccionario-de-marketing.htm
Junio 2009.

18. **“Glosario del asegurado”**.
http://www.eumed.net/cursecon/dic/glos-segur.htm
2009.

19. **“Definición”**.
http://www.segurb2b.com/informacion/dicc_segurosb.cfm?letra=R
2009.

20. **“Documentación”**.
http://www.navactiva.com/web/es/atic/doc/glosario/internet/?letra=S
2009.

21. **“Glosario”**.
http://proyectos.cip.cu/directorio_personalidades/wiki/glosario
2009.

22. **“Temas”**.
http://www.e-gobierno.gob.mx/wb2/eMex/eMex_Glosario_de_terminos_Seguridad?page=31
Junio 2009.

23. **“Glosario”**.
http://www.tribunaantimperialista.cu/libros/Libros_3/ciencia3/159/htm/sec_9.htm
2009.

24. **“¿Qué son las TIC y por qué son tan importantes?”**.
http://pedagogia2008-sherina.blogspot.com/2008/01/qu-son-las-tic-y-porque-son-tan.html
Enero 23, 2008.

25. **“Glosario de términos sobre Internet y Spam”**.
https://www.agpd.es/portalweb/glosario/glosario_internet_spam/index-ides-idphp.php
2004.

26. **“Glosario Informático y de Internet”**.
http://www.marcelopedra.com.ar/glosario_V.htm
Noviembre 2008.

27. Geer, Daniel E. (2006).
"Crime online". Acm Queue.
Noviembre 2006 Vol.4 No. 9, Pág. 42

28. Geer, Daniel E. (2006).
"Crime online". Acm Queue.
Noviembre 2006 Vol.4 No. 9, Pág. 44

29. Fernández-Font Pérez, Rafael.
"Moore y la ley de Moore".
http://petra.euitio.uniovi.es/~arrai/historia/trilobytes/5-Moore%20y%20la%20ley%20de%20Moore/Moore.htm.
2009.

30. Geer, Daniel E. (2006).
"Crime online". Acm Queue.
Noviembre 2006 Vol.4 No. 9, Pág. 46.

31. Geer, Daniel E. (2006).
"Crime online". Acm Queue.
November 2006 Vol.4 No. 9, Pág. 47

32. McEachern, Cristina.
"**Don't Panic. Financial Services Firms Seem to Have Cyber Risk Under Control**".
http://www.financetech.com/printableArticle.jhtml?articleID=14703178.
Marzo 08, 2001.

33. **Código Civil de Guatemala.**
Art 1278 y 1581.
2009.

34. **"Study shows enterprises under-spending for security"**
http://www.nemertes.com/press_releases/study_shows_enterprises_under_spending_for_security. August 15, 2005.

35. McMillan, Robert.
"Spear-phishing attacks have hooked 15,000 says verisign".
http://www.networkworld.com/news/2008/060608-spear-phishing-attacks-have-hooked-15000.html?hpg1=bn.
Junio 06, 2008.

36. Drouin, Denis.
"Cyber Risk Insurance. A Discurse and Preparatory Guide"
Febrero 9, 2004.

37. Gordon, Lawrence A.; Loeb, Martin P.; Lucyshyn, William; Richardson, Robert.
"2006 CSI/FBI Computer Crime and Security Survey"
http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf. 2006.

38. Amadis. **"American internacional Group"**
http://es.wikipedia.org/wiki/American_International_Group.
Diciembre 29, 2008.

39. AIG. “**Network, Security and Privacy and ID Theft (AIG netAdvantage)**”.
http://www.aig.com/Network-Security-and-Privacy-Insurance-(AIG-netAdvantage)_20_2141.html.
2009.

BIBLIOGRAFÍA

1. Aparicio, Fernando.
   "**Ciber-Responsabilidad: Los Seguros de Riesgo Electrónico**".
   http://www.borrmart.es/articulo_redseguridad.php?id=201&numero=15
   Enero, 2008.