ANÁLISIS DE RIESGO DE LOS SERVICIOS DE BANCA EN LÍNEA OFRECIDOS ACTUALMENTE EN COLOMBIA.

MITZY MILADY MANCERA ALVARADO
SONIA YAMILE ORTEGA CARRILLO

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIAS FISICOMECÁNICAS
ESCUELA DE INGENIERIA ELÉCTRICA, ELECTRÑÓNICA Y TELECOMUNICACIONES
ESPECIALIZACION EN TELECOMUNICACIONES
BUCARAMANGA
2010

ANÁLISIS DE RIESGO DE LOS SERVICIOS DE BANCA EN LÍNEA OFRECIDOS ACTUALMENTE EN COLOMBIA.

MITZY MILADY MANCERA ALVARADO
SONIA YAMILE ORTEGA CARRILLO

PROYECTO DE GRADO

Director:
JORGE MEDINA VILLALOBOS
Ingeniero Electrónico
Especialista en Telecomunicaciones

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIAS FISICOMECÁNICAS
ESCUELA DE INGENIERIA ELÉCTRICA, ELECTRÑÓNICA Y TELECOMUNICACIONES
ESPECIALIZACION EN TELECOMUNICACIONES
BUCARAMANGA
2010

Dedicado a mis padres Edgar Antonio Mancera Hidalgo y Zuleima Alvarado, soy lo que he llegado a ser gracias a ustedes. A mi hija Kiara Giselle Arroyo Mancera que ha sido mi principal centro de motivación para emprender mis proyectos de vida y terminarlos con satisfacción.

Mitzy Milady Mancera Alvarado

Dedico este trabajo a: Luis Hernán Ortega Albarracín, mi padre. Gracias por tu apoyo incondicional y tus concejos.

Sonia Yamile Ortega Carrillo

AGRADECIMIENTOS

Agradezco de todo corazón:

A mis padres, por su amor, comprensión y apoyo.

A mi hija por ser mi razón de vida y motivación para salir adelante

A mis hermanos por los concejos y compañía que me brindan, aunque la mayor parte del tiempo estamos distantes, sé que cuento con ellos de corazón.

A Dios por llenar mi vida de dichas y bendiciones, principalmente la de poder contar con mis padres, hermanos e hija que me han brindado todo su entusiasmo para cumplir a feliz término mis metas.

A mis amigos y compañeros de clase que siempre han estado en la disposición en colaborar y compartir sus experiencias de vida.

A todo el personal del programa Especialización en telecomunicaciones tanto Administrativo como Docente por su disposición y ayudas brindadas.

A Jorge Alberto Medina Villalobos, nuestro Director de Trabajo de grado por su dedicación, paciencia y apoyo en culminar a feliz término el trabajo en este documento consignado.

Mitzy Milady Mancera Alvarado

Agradezco en primera instancia a Dios porque gracias a él este sueño se ha hecho realidad. También a nuestro director Ingeniero Jorge Medina Villalobos quién solo le debemos respeto y admiración, a nuestros profesores de Especialización, a nuestros compañeros de estudio, al equipo Administrativo, Ingeniero Jorge Hernando Ramón Suarez, a las Ingenieras Tatianita, Dianita, Elianita; a mis padrinos Alvaro Ignacio Lopez y Mercedes Sepulveda, a mis hermanos Marly, Magdy y Jesús. Y a todos aquellos que de una u otra manera colaboraron para que este sueño se hiciera realidad.

Sonia Yamile Ortega Carrillo

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

INDICE DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

- **Adware:** Cualquier programa que automáticamente se ejecute, que puede recopilar información del usuario lo quien provoca preocupación por la privacidad.
- **Ataques de Inyección SQL CGI:** Este tipo de ataque permitiría a un atacante circunvenir los controles de autenticación del portal y leer, borrar o modificar datos del portal y leer, modificar o borrar datos de la base de datos e incluso tomar control del sistema en forma remota.
- **Autenticación:** asegurar que solo los individuos autorizados tengan acceso a los recursos.
- **CGI:** Common Gateway Interface. Es un mecanismo de comunicación entre el servidor web y una aplicación externa cuyo resultados de la ejecución son objetos MIME.
- **Comercio electrónico:** Abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar.
- **Confidencialidad:** Se refiere al de evitar la divulgación accidental o intencional de la información**.**
- **Denegación del servicio:** Un ataque de denegación de servicio inhabilita al sistema para que éste pueda operar en su normalidad, por lo tanto imposibilita a las partes la posibilidad de realización de operaciones transaccionales. Éstos son de extrema sencillez y la identificación del atacante puede llegar a ser imposible**.**

- **Disponibilidad:** Garantiza que los usuarios siempre puedan hacer uso de los recursos de una manera confiable.
- **Entidad de Certificación:** Es aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.
- **Firma digital.** Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.
- **Integridad:** Garantiza que la información es exacta y completa. Identifica los datos que han sido alterados.
- **Intercambio Electrónico de Datos (EDI):** La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto.
- **Mensaje de datos:** La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax.
- **Modificación de información:** La modificación de datos permite alterar el contenido de ciertas transacciones como el pago, la cantidad o incluso la propia orden de compra.

- **Nessus:** Escaneador remoto de seguridad. Analizador de vulnerabilidades creado por Renaud Deraison.
- **Objetos MIME:** (Multipurpose Internet Mail Extension). Mime es una especificación que permite anexar objetos a correos para que puedan ser enviados por Internet. Con mime, un cliente de correo o un navegador Web puede enviar y recibir cosas como documentos de texto, de cálculo, de audio, video o fotos, en un correo electrónico.
- **Repudio:** El rechazo o negación de una operación por una de las partes puede causar problemas a los sistemas de pago. Si una parte rechaza un previo acuerdo con la respectiva, ésta deberá soportar unos costos adicionales de facturación.
- **Robo de información:** El robo de información mediante escuchas de red, permite obtener información del usuario como números de cuentas o de tarjetas de crédito, balances de cuentas o información de facturación. Estos ataques, también, permiten el robo de servicios normalmente limitados a suscriptores. Por el hecho de conocer la realización de una transacción roza la invasión de la privacidad**.**
- **Sistema de Información:** Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.
- **Suplantación de identidad:** La suplantación de identidad permite al atacante realizar operaciones en nombre de otro. Una situación de este tipo permitiría a un poseedor de miles de números de tarjetas de crédito la realización de numerosas pequeñas operaciones que representen en su totalidad una cantidad significativa. También puede interesar al atacante la suplantación de identidad del usuario de banca virtual.

- **Syslog:** es una norma que se caracteriza por no haber sido consensuada ni legitimada por un organismo de estandarización, generalmente aceptada y ampliamente utilizada por iniciativa propia para el envío de mensajes de registro en una red informática IP. Un mensaje de registro suele tener información sobre la seguridad del sistema, aunque puede contener cualquier información. Junto con cada mensaje se incluye la fecha y hora del envío.
- **Trazabilidad en seguridad informática:** Se refiere al proceso o acción que permite guardar registros o logs de todas las acciones que realiza un individuo dentro de un sistema informático. De manera que si en algún momento pasa algo extraño, se pueda reconstruir los hechos mediante la revisión de los logs.
- **Vulnerabilidades:** Las vulnerabilidades de un sistema surgen a partir de errores individuales en un componente, sin embargo nuevas y complejas vulnerabilidades surgen de la iteraccion entre varios componentes como el kernel del sistema, sistemas de archivos, servidores de procesos entre otros. Estas vulnerabilidades generan problemas de seguridad para la red en cuestión**.**

RESUMEN

TÍTULO
ANÁLISIS DE RIESGO DE LOS SERVICIOS DE BANCA EN LÍNEA OFRECIDOS ACTUALMENTE EN COLOMBIA*

AUTORAS
MITZY MILADY MANCERA ALVARADO
SONIA YAMILE ORTEGA CARRILLO**

PALABRAS CLAVES
BANCA ELECTRONICA, DELITO INFORMATICO, AMENAZAS, VULNERABILIDADES, ANALISIS DEL RIESGO, PROTECCION DE DATOS, USUARIOS, EXPERTOS.

DESCRIPCIÓN
Hoy en día La banca electrónica es un servicio adicional suministrado por cada una de las entidades bancarias que facilita al usuario la realización de: consultas del estado de cuenta, compras, pagos, y demás, desde una terminal cualquiera. El problema radica en la seguridad de los sistemas online, en la posibilidad de ataques malintencionados en la red, no solo en las entidades bancarias, también en instituciones del sector público y privado. En general toda entidad que funcione o promueva sus servicios a través de la red se expone a ser víctima de un ataque en cualquiera de las modalidades de delito informático, de esta manera surge el interrogante: ¿Cómo garantizar la seguridad de las transacciones bancarias en línea en Colombia?
Para el análisis de riesgo de los portales web se implementaron tres encuestas, dos a usuarios de la banca electrónica, una a expertos en el área de sistemas y seguridad informática, las cuales se publicaron en el sitio web de portaldeencuestas, una alternativa gratuita en linea. En el proceso de auditoría de seguridad las validaciones fueron enfocadas a detectar vulnerabilidades o fallas de configuración en los servidores web de los portales de banca electrónica en Colombia. Para la ejecución de estas auditorías se utilizaron los siguientes programas: Tenable Nessus, Foundstone SSL Digger. Según los resultados obtenidos los portales reportan 18 vulnerabilidades, de las cuales representan riesgos bajos, riesgos medios y otras de riesgo alto. Algunas vulnerabilidades en particular están relacionadas con ataques de Inyección de SQL y otras en la mala selección de algoritmos de cifrado aceptados por el portal SSL. En muchos casos, los administradores de los portales no son cuidadosos y permiten que el portal negocie durante el establecimiento de la VPN, el uso de algoritmos desactualizados o inseguros.

* Trabajo de grado
** Facultad de Ingenierías Fisicomecánicas. Escuela de Ingeniería Eléctrica, Electrónica y Telecomunicaciones. Director: Esp. Jorge Alberto Medina Villalobos

SUMMARY

TITLE
ANALYSIS OF RISK OF THE SERVICES OF BANKING ON LINE OFFERED NOWADAYS IN COLOMBIA*

AUTHORS
MITZY MILADY MANCERA ALVARADO
SONIA YAMILE ORTEGA CARRILLO**

KEY WORDS
ELECTRONIC BANKING, IT CRIME, THREATS, VULNERABILITIES, ANALYSIS OF THE RISK, PROTECTION OF INFORMATION, USERS, EXPERTS.

DESCRIPTION
Nowadays the electronic banking is an additional service supplied by each of the bank companies who facilitates the accomplishment to the user of: consultations of the bank statement, purchases, payments, and others, from a terminus anyone. The problem takes root in the safety of the systems online, in the possibility of ill-disposed assaults in the network, not only in the bank companies, also in institutions of the public and private sector. In general any entity that works or promotes his services across the network is exposed to being a victim of an assault in any of the modalities of IT crime, hereby the question arises: how to guarantee the safety of the bank transactions on line in Colombia?

For the analysis of risk of the web portals three surveys were implemented, two to users of the electronic banking, one to experts in the area of systems and IT security, which were published in the web site of portaldeencuestas, a free alternative on line.

In the process of safety audit the validations were focused to detecting vulnerabilities or faults of configuration in the web servants of the portals of electronic banking in Colombia. For the execution of these audits the following programs were in use: Tenable Nessus, Foundstone SSL Digger.

According to the obtained results the portals bring 18 vulnerabilities, of which they represent low risks, average risks and others of high risk. Some vulnerabilities especially are related to assaults of SQL's Injection and others in the bad selection of algorithms of coding accepted by the portal SSL. In many cases, the administrators of the portals are not careful and allow that the portal should negotiate during the establishment of the VPN, the use of out of date or insecure algorithms.

* Work Degree

** Faculty of Engineerings Fisicomecánicas. School of Electrical, Electronic Engineering and Telecommunications. Directress: Esp. Jorge Alberto Medina Villalobos

INTRODUCCIÓN

A medida que avanza la globalización y la conectividad de las nuevas tecnologías de la información y comunicación (TICs) se hace cada vez más evidente, la seguridad de la información y con ella los principios de: confidencialidad, integridad y disponibilidad; cobra notoria fuerza en términos de movilidad, servicio al cliente y calidad del servicio.

El sector financiero es sin duda alguna, uno de los más favorecidos con los nuevos servicios de la sociedad de la información, y por ende, uno de los más preocupados porque sus clientes puedan acceder de forma segura y confiable a sus recursos económicos a través de los nuevos canales de banca electrónica. No obstante, el auge de nuevas tecnologías y el empleo de las mismas en la aparición de nuevas conductas delictivas, han obligado a los estados y a los diferentes entes reguladores a tomar partido en la relación existente entre el sector financiero y sus usuarios; definiendo así los deberes y derechos de los participantes del negocio a nivel legal, e incluso, definiendo los requisitos mínimos de seguridad que permitan aplicar y velar por la protección del cuentahabiente y el cumplimiento de las leyes y regulaciones normativas del sector.

Un servicio de banca electrónica segura, que ofrezca excelentes niveles de servicio al cliente y que cumpla con estándares internacionales de calidad, implica costos financieros elevados para cualquier entidad del sector; costos que sin duda alguna, terminan siendo transferidos al cuentahabiente que hace uso de los servicios de eBanking; por lo tanto, es absolutamente necesario, realizar tareas periódicas de análisis de riesgo en el sector para determinar cuándo estos sobrecostos por seguridad son realmente necesarios, obteniendo un buen balance entre seguridad-costo-beneficio.

1. PLANTEAMIENTO DEL PROBLEMA

1.1. SITUACIÓN PROBLEMA

Debido al auge de las transacciones a través del Internet, los sistemas bancarios han incrementado sus servicios on-line para ofrecer a sus cuentahabientes un mayor acercamiento a sus portafolios. La banca en línea, ofrece a sus clientes la posibilidad de realizar consultas a sus estados bancarios, compras, pagos, y demás, desde una terminal cualquiera. En la actualidad, el acceso al servicio de e-Banking es posible a través de una cuenta de usuario y una contraseña que el cliente mismo puede configurar registrándose en el portal del banco al cual se encuentra adscrito.

El número de ataques malintencionados a la red, del cual han sido víctimas no solo la entidades financieras, en buena medida involucra también organizaciones del sector público y privado (escuelas, colegios, universidades, hospitales, estaciones de radio, particulares, etc.), en fin, todo negocio que funcione o promueva sus servicios a través de la red, se expone a sufrir ataques en las distintas modalidades de crimen informático, tales como: amenazas contra la autenticidad (suplantación de identidad), la integridad, la confidencialidad, robo de información, ingeniería social, entre otros. De esta manera surgen la interrogante: ¿Cómo garantizar la seguridad de las transacciones bancarias On-line en Colombia?

De continuarse presentando esto en las entidades bancarias, el número de ataques desde terminales externas podría producir mayores pérdidas económicas e incrementar la desconfianza en los usuarios y como consecuencia de ello, la fuga de capitales de inversión afectaría la estabilidad y la permanencia de la banca.

1.2. OBJETIVOS

1.2.1. Objetivo General

Realizar un análisis de riego en los procesos transaccionales bancarios en-Línea en Colombia, considerando los controles existentes y sus recomendaciones respectivas.

1.2.2. Objetivos Específicos

Revisar la normatividad actual referente a los requerimientos mínimos de seguridad y calidad en el manejo de información a través de Internet, en la distribución de productos y servicios para clientes y usuarios, definidos por la Circular Reglamentaria externa 052 de la Superintendencia Financiera de Colombia.

Aplicar una encuesta virtual a usuarios de esta modalidad, para estimar un porcentaje de ocurrencia en situaciones fraudulentas, de este tipo de servicios.

Generar informes de resultados de las encuestas realizadas mediante la herramienta informática EL Generador de encuestas[1].

Realizar análisis de riesgos de los procedimientos genéricos empleados actualmente en los procesos transaccionales electrónicos de los bancos.

Proponer controles adicionales que permitan disminuir los riesgos en las transacciones bancarias en línea.

[1] Herramienta opcional para la generación de resultados. Realizado como proyecto de grado para optar por el título de ingeniero de sistemas Universidad de Pamplona, autor Ing. Mitzy Milady Mancera Alvarado.

Elaborar el documento guía de análisis para el manejo de situaciones fraudulentas en esta modalidad de servicio.

1.3. JUSTIFICACIÓN

En el mundo globalizado, donde el Internet ha transformado “el hacer de las cosas”, el sistema financiero no podría permanecer ajeno y visto la necesidad de incurrir en la era de los servicios en-línea. La necesidad de invertir en el área de seguridad, más que un gasto debe ser visto como un valor agregado para los usuarios e inversionistas pues, permite garantizarles la fiabilidad a la hora de realizar sus transacciones.

Los usuarios que están al tanto de la innovación, la cual crece de forma exponencial, utilizan el Internet como una opción cómoda y módica para realizar sus actividades por medio de aplicaciones web, pese a que en determinado momento, podrían quedar expuestos a posibles fraudes.

En la actualidad, la mayoría de las empresas del sector financiero, permiten a sus cuentahabientes el acceso a sus sistemas de información financiera en-línea a través de una interface web que interactuará de forma transparente con los procesos bancarios internos de la entidad, sin embargo, el acceso a estos portales de servicio se realiza mediante un proceso de autenticación basado, únicamente, en algo que el usuario sabe (usuario, contraseña); este mecanismo de autenticación débil no garantiza la seguridad del usuario y lo expone a situaciones de fraude y robo entre otros. Las empresas bancarias deben tomar medidas y garantizar políticas de seguridad, es decir, que desde la misma máquina del usuario se validen los datos mediante el uso adecuado de protocolos seguros que garanticen el éxito de una transacción. Si bien es cierto que el sistema financiero ha realizado grandes esfuerzos por proteger su infraestructura tecnológica, también lo es, que no ha hecho el propósito de mejorar los esquemas de autenticación para el usuario final.

Este trabajo se propone analizar la situación actual del usuario final y ofrecer alternativas viables tanto para el cuentahabiente como para estas entidades. Por otra parte se aplicaran en este estudio los conocimientos recibidos en la especialización en telecomunicaciones de la Universidad Industrial de Santander. Al desarrollo de este proyecto se cumple con el requisito para optar al título de especialista en telecomunicaciones de la escuela de Eléctrica de la Universidad Industrial de Santander UIS.

1.4. ESTADO DEL ARTE

En la encuesta mundial de RSA sobre seguridad del consumidor en-línea del año 2010, se realizó un estudio consultando a más de 4,500 personas de 22 países, acerca de los riesgos de seguridad en-línea que enfrentan con sus entidades y de esta manera, medir el nivel de conocimiento de los encuestados respecto a las amenazas más recientes.

El estudio se llevó a cabo con la finalidad de medir a los proveedores de servicios financieros respecto a, si son conscientes y si cuentan con las medidas necesarias en caso de posibles ataques. En América Latina, participaron y fueron representados más de 950 encuestados de los siguientes países: Brasil, Chile, Colombia, México y Perú.

Frente al interrogante ¿con cuáles de los siguientes tipos de amenazas en línea está familiarizado?, el 65% indicó que era consciente de la amenaza de la práctica de phishing y de lo que significaba.

El irrelevante hecho de que el fraude en-línea y el delito cibernético vaya en gradual incremento, resulta de gran interés para los medios de comunicación y se han convertido en un tema muy difundido en las noticias, hecho que concuerda con la preocupación de los consumidores, 59% de los encuestados de América Latina afirmó estar “muy” preocupado por la amenaza de los ataques de phishing, también se concluyó que los bancos y

las redes sociales son los sitios más concurridos por los delincuentes en-línea.

La percepción de los consumidores respecto a lo que significa ser una víctima de phishing puede variar (desde recibir un mensaje de correo electrónico de phishing hasta hacer clic en un enlace y brindar información personal a un sitio de phishing), el porcentaje de consumidores que afirman haber sido atacados es, aun así, alarmante. Brasil es el país latinoamericano con más víctimas en esta modalidad de ataque con un 41%(ver informe anexo), seguido de Perú con el 31%, en tercer lugar le corresponde a México con el 30%, Chile con un 29% y Colombia con el 24%. Aunque nos encontremos en quinto lugar, no significa que se deba bajar la guardia sino al contrario, se debe tomar medidas preventivas en materia de políticas de seguridad informática para evitar que el número de ataques en esta modalidad aumente, no obstante, se parte de la idea de que los autores del phishing copian el diseño de una comunicación legítima de un banco, comercio minorista en-línea u otra organización, y ya no tienen el nivel de gramática deficiente que hacía que estos intentos de ataque de phishing fueran tan evidentes, lo que indica que podrían estar empleando una técnica de tecnología avanzada al respecto.

También se encontraron hallazgos interesantes en los parámetros de medición respecto al método de seguridad más sólido para la identificación de usuarios (además del nombre de usuario y la contraseña) cuando se inicia sesión en el sistema bancario en línea. El 94% de los encuestados de América Latina afirmaron de estar relativamente preocupados o muy preocupados por la posibilidad de que su información personal sea robada o se pueda acceder a ella por medio del sitio de su sistema bancario en-línea. Como resultado, el 90% de esos mismos encuestados también afirmó que los bancos deberían implementar un método de seguridad más sólido que el uso de un nombre de usuario y una contraseña para iniciar sesión en el

sistema bancario en línea; el 96% afirmó esperar que sus bancos realizaran un monitoreo de sus transacciones bancarias en línea. Debe destacarse que solo el 65% de los encuestados de América Latina sentía que su banco ofrecía un método de autenticación más sólido que la seguridad básica de un nombre de usuario y una contraseña.

Respecto a la pregunta ¿**Cuán seguro se siente al realizar operaciones bancarias mediante su teléfono móvil**?, de nuevo corresponde el primer lugar con un 47% (relativamente seguro), es decir corresponde aun a un número aproximado de 447 personas encuestadas en Latino América de 950. Lo que indica el sentimiento de seguridad de los usuarios de servicio móvil aún es muy bajo. Los usuarios del sistema bancario móvil son un grupo nuevo y en aumento, y los delincuentes en-línea apenas están comenzando a atacarlos.

Así mismo frente a la alternativa de impacto que tendría una seguridad más sólida en su confianza respecto a las transacciones en línea, el 96% de los Latino Americanos afirmó que se sentiría más confiado; el 74%, que se sentiría "considerablemente" más confiado; y el 22%, que se sentiría "relativamente" más confiado. Estas cifras son muy superiores a las de otras regiones. De los encuestados, el 42% en los Estados Unidos, el 50% en Australia y el 46% en Asia afirmaron que se sentirían "considerablemente" más confiados.

Cuándo se consultó a los consumidores latinoamericanos, acerca de su predisposición a utilizar un nuevo método de seguridad si el banco lo ofreciera, el 99% afirmó que estaría entre relativamente y muy dispuesto a usarlo. Todos los encuestados de Colombia y México declararon que estarían dispuestos a utilizar un mejor método de seguridad si su banco se lo ofreciera.

El panorama de la tendencia del comercio electrónico a nivel Colombiano se visiona favorable, no obstante el temor de los clientes fundamentado en un

historial de ataques y una tecnología poco robusta obliga a la necesidad de que la banca se vea en la necesidad de invertir en materia de política de seguridad de la información, para ello la superintendencia financiera decretó la circular 052 de requerimientos mínimos que deben ser cumplidos por las entidades vigiladas, en áreas de la seguridad y calidad de la información.

2. EL DELITO INFORMÁTICO

Debido a las características complejas en cuanto a la arquitectura de las redes, se adoptan nuevas medidas que permiten proporcionar una adecuada protección contra el uso indebido del internet. Los delitos informáticos, y sobre todo por su característica de ser considerados como delitos globales[2], adoptan una condición necesaria y vitalmente importante como lo es la creación de un marco jurídico internacional unificado y enfocado hacia la lucha contra la ciberdelincuencia.

Hoy en día a pesar de que todos los países del planeta están conectados a Internet, muchos de ellos no cuentan con una la ley de delitos informáticos, incluso, entre aquellos países que presentan diferencias significativas en la concepción de las conductas delictivas, al punto que se dificulta su aplicación y hacen imposible la colaboración internacional en los procesos de investigación, juicio y sanción de los comportamientos criminales. La falta de una armonización del marco jurídico a nivel mundial, en relación con el delito informático, se ha convertido en una cuestión que requiere la atención urgente de todas las naciones. A si mismo se han realizado varios intentos por armonizar los términos utilizados y las conductas delictivas, siendo las más importantes la presentada por el Consejo de Europa en el Convenio de

[2] Delito Global: Delito que se comete en todo el mundo, con la consiguiente crisis radical del principio de territorialidad del Derecho Penal. Emilio Suñe, El Delito Informático como motor de cambios conceptuales en el Derecho Penal, http://www.alfa-redi.org/rdi-articulo.shtml?x=888

Cibercriminalidad de Budapest en 2001; y la Agenda Global de Ciberdelincuencia propuesta por la UIT en el 2007.

2.1. DEFINICIONES

Al la fecha, se han realizado múltiples intentos para definir el termino Delito Informático o Ciberdelito sin embargo, para los estudiosos del tema, aún no existe una única definición que logre agrupar todas las conductas delictivas y que, al mismo tiempo, no permita interpretaciones erróneas; por lo tanto se procederá a enunciar algunas de las definiciones más reconocidas en el medio.

La Unión Americana, respecto a crímenes tradicionales define el crimen cibernético como: "**Toda conducta con respecto a los sistemas cibernéticos que se clasifica como un delito punible por el presente Convenio**". A los sistemas cibernéticos y medios incluidos en esta propuesta, equipo o redes de ordenadores usados para transmitir, coordinar, o controlar las comunicaciones de datos o programas involucrados en actividades que se consideran ilegales[3].

El autor mexicano Julio Tellez Valdez [W-8] señala que los delitos informáticos son "**actitudes ilícitas en que tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)**".

El tratadista penal italiano Carlos Sarzana, sostiene que los delitos informáticos son "**cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo**". Concepto bastante cuestionable puesto que podría darse el caso de que ocurra un acto delictivo con el hadware o con una parte del mismo y no se

[3] Propuesta de la Convención Internacional sobre el Delito Cibernético y el Terrorismo por el Stanford Universidad (2000).

considere como delito informático aunque en su efecto si es un delito, pero no informático.

Por otra parte el ciberdelito hace referencia inmediatamente a quienes de una u otra forma lo ocasionan, las posibles causas y porqué la actitud frente a ciertas tendencias nuevas en materia de procesamiento de información pueden o no considerarse delito informático. La propuesta de la Unión Europea en la Decisión del Marco del Consejo relativo a los ataques contra los sistemas de información del 19 de abril de 2002, incluye también una definición funcional respecto al cibercrimen o delito informático: "La delincuencia informática se debe entender como los ataques contra los sistemas de información definida en la presente Decisión reglamentada en el marco del 2001", Resolución de la Asamblea General de las Naciones Unidas 55/63 y 56/121 sobre la lucha contra el uso delictivo de tecnologías de la información[4]. Como ejemplo de perspectiva internacional puede citarse el Artículo 1.1 del Proyecto de Convenio Internacional para la Protección contra la Ciberdelincuencia y el Ciberterrorismo (CISAC)[5], en el que por ciberdelincuencia se refiere a los actos relativos a los cibersistemas.[6]

Por otro parte el Consejo Europeo adoptó la Recomendación de 1989 dándole enfoque funcional, y relacionándolo el cibercrimen simplemente como los delitos enumerados y definidos en las directrices propuestas o recomendación a los legisladores nacionales. En esa misma instancia la

[4] Disponibilidad de datos y sistemas informáticos (1), (2) los delitos informáticos, (3) delitos relacionados con el contenido, (4) delitos relacionados con las infracciones de derechos de autor y derechos conexos.

[5] The Stanford Draft International Convention (CISAC) was developed as a follow up to a conference hosted in Stanford University in the United States in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf ; For more information see: Goodman/Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf ; Sofaer, Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[6] TÉLLEZ VALDÉS, Julio, Derecho Informático, 3ª.ed., Ed. Mc Graw Hill, México, 2003, Pág.

Unión Africana (TI delitos o crímenes de TI) describe un delito informático como: "**Cualquier delito penal que requiere investigación, para los cuales las autoridades investigadoras a cargo deben obtener acceso a la información que está siendo procesada o transmitida en los sistemas informáticos, o sistemas de procesamiento electrónico de datos**".

Rogers afirma, que la mayoría de la literatura internacional en materia criminológica, acerca de delincuentes informáticos; a menudo erróneamente llamados "hackers" y de acuerdo en que "las teorías clásicas del evento criminológico con una matriz psicodinámica de coeficientes para explicar los delitos que se derivan inconscientemente en conflictos, pero no puede aplicarse fácilmente a los delitos que requieren gran exactitud, planificación y racionalidad". Como es el caso con la mayoría de tipos de delitos informáticos, en efecto el fenómeno de la piratería, que es difícil de interpretar con teorías clásicas en criminología, debido principalmente a la identificación de referencias en cuanto a evidencias que se encuentra bajo ese ambiente tan visiblemente variante; sin embargo tampoco esta definición define claramente que es un delito informático.

Puesto que su naturaleza denota distintas formas de origen. No existe un único criterio que comprenda todos los actos mencionados en el Proyecto de Convenio de Stanford sobre la ciberdelincuencia y que a su vez excluya los delitos que se cometen exclusivamente por medios físicos. El hecho de que no haya una única definición de "ciberdelito" no es importante siempre y cuando el término no se utilice como término jurídico. La definición bastante común de este término la da la ITU entiéndase como delito informático: "**Cualquier actividad delictiva en la que se utilizan como herramienta los computadores o redes, o éstos son las víctimas de la misma, o bien el medio desde donde se efectúa dicha actividad delictiva**"[7]. En otras

[7] See for example: *Carter*, Computer Crime Categories: How Techno-Criminals Operate, FBI Law Enforcement Bulletin, 1995, page 21, available at:

palabras se considera ciberdelito toda acción o conducta ilícita premeditada a través del uso de herramientas software mediante ataques en uno o distintos modos destinados a perturbar o dañar el normal comportamiento de un sistema de información.

2.2. TIPOS DE ATACANTES

Afirmar: "que el grado de seguridad de un sistema es inversamente proporcional a la operatividad del mismo", es acercarse a la realidad puesto que: no puede haber un sistema cien por ciento seguro y que opere en forma eficiente sin afectar el desempeño del mismo, por lo tanto, es necesario adecuar a las políticas de seguridad del sistema y los requerimientos por parte de quienes van a interactuar con él mismo. En vista de lo anteriormente analizado respecto al delito informático, se tratará un tema bastante interesante como es el mundo Hacker. Se hará énfasis en los aspectos más irrelevantes del ciberdelito en sus distintas modalidades. Al respecto los investigadores Raoul Chiesa[8], Stefania Ducci y Silvio Ciappi en su tratado "Hacker Profiling", hace hincapié en el aspecto psicológico mediante una encuesta realizada, donde agrupan la información obtenida en tres categorías: Los datos personales, los datos relacionales, y los datos técnicos y criminológicos

Para la primera categoría, se recolectaron datos personales de la situación en cada individuo: información como la edad, sexo, país de origen y ciudad de residencia, aspecto físico, personalidad, condiciones psicofísicas, el uso de sustancias que alteran el estado de ánimo (medicamentos y alcohol), la educación, situación social y antecedentes familiares.

---

http://www.fiu.edu/~cohne/Theory%20F08/Ch%2014%20-%20Types%20of%20computer%20crime.pdf ; *Charney*, Computer Crime: Law Enforcement's Shift from a Corporeal Environment to the Intangible, Electronic World of Cyberspace, Federal Bar News, 1994, Vol. 41, Issue 7, page 489 et. seqq.; *Goodman*, Why the Policy don't care about Computer Crime, Harvard Journal of Law & Technology, Vol. 10, No. 3; page 469.

[8] Chiesa Raoul, Ducci Stefania, Ducci Silvio, "Profiling Hackers", UNICRI 2009 Pag. 264.

Otro aspecto no menos importante es el área de actividad profesional. Partiendo de lo anterior se toma la información esencial para "penetrar" un mundo que no es el nuestro, mostrando los conflictos, las dependencias y problemas actuales en la esfera personal de cada sujeto.

Por último, el tercer caso analiza los aspectos más interesantes, estrechamente ligados al mundo de hacking, desde el punto de vista técnico: hace hincapié al uso del apodo y a la edad en que se aborda la piratería por el momento; la posible presencia de un solo técnico especialista variará su enfoque de piratería informática, phreaking, y carding, en redes de comunicaciones de diferentes tecnologías. Ver (Tabla No1. “Descripción, Preferencias Hacking (Solo / Grupo), Objetivos y Motivaciones” Tomada del tratado de “Profiling Hackers”).

Tabla 1. “Descripción, Preferencias Hacking (Solo / Grupo), Objetivos y Motivaciones”

Categoria	Descripción	Actúa Solo/En grupo	Objetivos / Victimas	Motivaciones
Wannabe Lamer	9-8 años "Quiero ser un hacker, pero no puedo 'Hack' it "	Grupo	Usuario final	Hacer cosas de Hackers está de moda, está “In”
Script-kiddie	10-18 el chico escribe código	Grupo	PMI vulnerabilidades conocidas	Para ventilar la ira y los medios llamar atención de los medios de comunicación

Cracker	17-35 años El destructor	Individual / grupo	Compañías privadas	Para promover otro poder y obtener atención de los medios.
Hacker Ético	15-50 años El Hacker "por excelencia "	Individual rara vez en grupo, por Diversión o investigación.	Grandes corporaciones y sistemas complejos, Siempre que haya una vulnerabilidad es un reto o valor a investigar	Por curiosidad, para aprender, por razones altruistas, para mejorar habilidades de trabajo
Hacker experto silencioso, paranoico,	16-50 años Altamente especializados hacker, poco comunicativo, extremadamente paranoico	Individual	No específico	Por curiosidad por aprender individualmente.
Cyber warrior	18-50 años El mercenario	Individual	Las empresas y "Emblemáticos" Órganos, usuarios finales.	Para obtener ganancia financiera.
Espía Industrial	22-50 años El espía industrial	Individual	Negocios, empresas,	Para obtener ganancias

			corporaciones, Multinacionales.	financieras
Agente de Gobierno	25-45 años Agente del gobierno (la CIA, Mossad, el FBI, etc)	Individual o en grupo	Los gobiernos, sospecha estratégica de terroristas, industrias, personas	Profesionalmente (Espionaje/la lucha contra el espionaje, vulnerabilidad de la prueba, actividad seguimiento)
Hacker Militar	25-45 años Reclutado para combatir "Con un ordenador"	Individual o en grupo	Los gobiernos, Industrias estratégicas	Profesional y por una causa (Controlar y perjudicial sistemas)

Tabla 2. " El respeto de la ética hacker, daños causados, y conciencia de la ilegalidad de las acciones".

Categoría	Respeto por la ética hacker	Daños o Violación a Sistemas	Conciencia de llegalidad de acciones propias
Wannabe lamer	No están familiarizados con los principios de la ética hacker.	Si, inadvertida o deliberadamente o por ambos (Falta de experiencia o habilidades técnicas).	Si, pero ellos piensan que no pueden ser capturados.

Script-kiddie	No ellos forman su propia ética.	No, pero algunas veces modifican o eliminan los datos.	Si, pero encuentran justificación para sus acciones.
Cracker	No hay ética hacker.	Si, siempre deliberadamente.	Sí, pero culpan de sus acciones, a los distribuidores de software o sistemas inseguros
Ethical hacker	Si, pero ellos lo definen.	No sólo puede suceder por accidente.	Sí, pero consideran que su actividades moralmente aceptable
Hacker experto silencioso, paranoico	No, ellos tienen su propia ética personal, a menudo muy cerca de la ética hacker.	No	Si, pero ellos se sienten culpables acerca de los problemas causados al administrador y otras víctimas.
Ciber Guerrero	No	Sí, además de modificar / borrar / robar los datos los venden.	Si, puesto que no tiene escrúpulos al respecto.
Espía Industrial	No, pero siguen algún tipo de “reglas No escritas”.	No, se dedican a robar y vender información	Sí, pero no tienen escrúpulos al respecto
Agente del Gobierno	No, ellos traicionan la	Sí, incluido el borrado / editado / robo de los datos) /	N/A

	ética hacker	(por medio de la "ocultación" de Ataques.	
Hacker militar	No, ellos traicionan la ética hacker	Sí, incluido el borrado / editado / robo de los datos) / (por medio de la "ocultación" de Ataques.	N/A

2.2.1. **Wannaber Lamer:** Esta es la categoría más "divertida". Los lammer informáticos de este tipo se encuentran prácticamente en cualquier lugar de Internet, porque están pública y constantemente pidiendo ayuda de diverso tipo. Por lo general, todo lo que necesita hacer es navegar con un bajo "perfil", en algunos portales podrá hallar indicios de los comentarios de estos personajes.

2.2.2. **Script kiddie:** Están "culturalmente avanzados", una característica particular es que no son hackers que exploran sino que utilizan de lo que ya disponen, dado que su especialidad es el uso de herramientas desarrolladas por otros para llevar a cabo sus ataques. Por lo general, se conectan a diario a los sitios desde los que pueden descargar la última versión de la herramienta de explotación, por ejemplo, la lista de correo BugTraq *. Gozan de reconocimiento en el mundo hacking, suficiente como para decir que el menos capaz de script-kiddies es etiquetado punto-y-clicker, y sus ataques son llamados "apuntar y hacer clic ataques, lo que indica que se ha investigado muy poco al respecto. A veces, script-kiddies (principalmente

[9]

2.2.3. **Crackers:** Originalmente, el significado o señalamiento que se le hacía a alguien que sustraía o viola fraudulentamente la protección de los fuentes de software comercial. Recientemente, el término ha empezado a aparecer en los diarios y en listas de correo y donde se califica a los crackers como "violentos" piratas informáticos, es decir, los hackers que están contentos de convertirse en una pesadilla para los administradores de sistemas. Comparado con las categorías anteriores, los hackers se reprodujeron de distinta forma, como son en realidad tienen el know-how para causar estragos. Ellos tratan de mantenerse en el sistema como siempre y cuando sea posible, y cuando creen que están perdiendo el control, "Cancelan", borran los registros, y cualquier tipo de huella, ya sea importante o no. Convirtiéndose así una categoría muy peligrosa.

2.2.4. Hacker Ético: Tienen un amplio nivel de experticia y conocimientos generales de sistemas operativos. En general se cree que los hackers sólo dominan UNIX y Linux, lo cual es completamente falso. Entran y violan el

[9] "37337 K-rad IRC # hack 0-día Exploitz" Guy. Para parafrasear irónicamente ese nombre críptico, podríamos describir este tipo de hacker como "el chico cool que va en el canal de IRC #hack para decir que ha hazañas disponible 0-día (exactamente igual que los comerciantes cuentan con el IRC que son mensajeros 0-día).*

sistema. Son traviesos, impertinente, curiosos entre otras cosas (hay muchos informes disponibles al respecto) entrará en tu sistema, a explorarlo rápidamente (si es un equipo grande o una gran red, puede ser que busquen un poco "más afondo" con fines puramente "didácticos"), incluso suelen hacérselo saber. A menudo, ellos son ingenuos y hablan acerca de sus acciones públicamente, dando por sentado que no han hecho nada malo.

2.2.5. **Hacker experto, silencioso o paranoico:** Estos hacker son temibles, más astutos y no los motiva el dinero. Este tipo de hacker es paranoico, por lo que será muy difícil de localizar ya que suelen ocultarse o camuflarse muy bien. Detectar su presencia es prácticamente imposible. El hacker paranoico se quedará en su sistema por muy largos períodos de tiempo, sin hacer nada grave o desagradable. Explorarán sólo lo que es de su interés (Por ejemplo no leerá correos electrónicos privados, pero si se atrevería a revisar el syslog * archivos y similares, uno por uno). Él no está interesado en la fama. No "lo hago por el dinero" Lo hace para sí mismo, por su experiencia y know-how. Él es muy capaz y competente puesto que conoce muchos sistemas operativos; explorará, pero no perderá el tiempo tratando de impresionar a nadie. Si detecta la presencia de este hacker, lo cual es altamente improbable, inmediatamente detectado desaparecerá sin dejar huella.

2.2.6. **Cyber-Guerrero:** Son mercenarios, han adquirido habilidades muy grandes en los años. Probablemente provienen de una de las categorías descritas anteriormente, y han elegido su camino. Se venden al mejor postor, pero rechazan ciertos tipos de solicitudes. Sus objetivos son de bajo perfil. Muy rara vez atacan a una multinacional; la probabilidad de que ataquen a un

2.2.7. **Espía Industrial:** El dinero es la motivación. Su lema es "hacerlo" por el dinero. Son altamente cualificados, con mucha experiencia, y son peligrosos especialmente si se trata de encontrar material confidencial confianza. Por desgracia comienzan formando parte de esta categoría, gente que accede a la información sensible de forma ilegal, en el interior de la empresa para la que trabajan, y la utilizan para beneficio personal. En los últimos años, se han incrementado exponencialmente, los hackers que pertenecen a esta categoría dado el gran número de delitos de congresistas corrupto y personalidades de cuello blanco.

2.2.8. **Agente del Gobierno:** Este hacker se emplea para espionaje, contraespionaje, y supervisar información de los gobiernos, individuos, los grupos terroristas, y las industrias estratégicas (como en el sector de la defensa, o los proveedores de energía, agua, gas, etc.), integran el FBI o son Agentes de la CIA, o son miembros del Mossad y otras agencias de inteligencia. En realidad, aunque pueda parecer extraño o excesivo para calificarlos como "Agentes secretos" a la par con las demás categorías, la historia muestra cómo casos de este tipo matrimonio entre el mundo de la piratería y el mundo de la inteligencia-las agencias ya constituidas en la mitad de la década de 1980.

Todo esto ha contribuido a cambiar la imagen que se tenía de los hackers informáticos sofisticados a piratas informáticos. En Colombia, para proteger las entidades tanto en el sector público como en el privado, el gobierno adoptó a través de la ley 1273 una nueva figura jurídica denominada (De la protección de la información y de los datos") cuya finalidad es precisamente castigar a aquellas personas que atenten contra la confidencialidad, integridad y disponibilidad de la información y afecte el desempeño normal de las empresas. Por lo tanto es menester tener unas condiciones de contratación, tanto con empleados como con contratistas, claras y precisas para evitar incurrir en la tipificación penal.

2.3. MODALIDADES DE DELITO INFORMATICO O CIBERCRIMEN.

El término delito informático incluye una gran cantidad de ofensas, lo cual hace que sea difícil crear una tipología o un sistema de clasificación del cibercrimen, no obstante, el Concejo Europeo en la Convención de Cibercrimen distingue cuatro tipos de ofensas (Ver Tabla N°3):

2.3.1. Ofensas contra la confidencialidad, la integridad y disponibilidad de los datos y los sistemas de información:

Cada una de las ofensas en esta categoría, atenta contra (al menos) uno de los principios de la seguridad de la información (confidencialidad, integridad y disponibilidad). A diferencia de los delitos contemplados por la legislación penal desde hace siglos (por ejemplo, robo u homicidio), estos aparecieron apenas sesenta años atrás. Para poder interponer una acción judicial contra estos actos es preciso que la ley contemple en sus disposiciones no sólo la protección contra la manipulación de bienes tangibles sino que extienda su protección a los nuevos principios de protección de datos y sistemas de información.

2.3.2. Ofensas relacionadas al contenido: Esta categoría cubre todos los contenidos que son considerados ilegales como lo son: la pornografía infantil, la xenofobia y los insultos a los símbolos religiosos. El desarrollo de instrumentos legales para lidiar con estas ofensas varía dependiendo del enfoque nacional, el cual, tiene en cuenta los fundamentos culturales y los principios legales que rigen dicha nación.

2.3.3. **Ofensas relacionadas a la propiedad intelectual y los derechos de autor:** Una de las funciones vitales de la Internet, es la diseminación de información, por tal razón, compañías de todos los tamaños a nivel mundial, la usan para distribuir información acerca de sus productos y servicios, no obstante, también enfrentan dificultades relacionadas con el manejo de su imagen y sus marcas corporativas, las cuales suelen ser utilizadas para la producción comercialización de productos falsificados.

2.3.4. Ofensas relacionadas con los sistemas de cómputo: En esta categoría se cubre las ofensas que requieren de un sistema de cómputo para ser cometidas. A diferencia de las categorías anteriores, estas ofensas no siempre son tan rigurosas en la protección de principios legales.

Tabla 3. Descripción y ejemplos de las diferentes ofensas

Categoría	Ofensa	Definición	Ejemplos
Ofensas contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas de información.	Acceso Ilegal (Hacking, Cracking)	Se considera acceso ilegal o abusivo, cuando alguien sin autorización, o fuera de lo acordado, accede en todo o en parte a un sistema informático.	Acceso abusivo a un sistema informático.[10] Intercepción de datos informáticos.[11] Uso de software malintencionado para la obtención de credenciales. Suplantación de sitios web para captura de información personal (Phishing). Circunvenir los controles de acceso de un sistema informático.
	Espionaje de Datos	Con cierta frecuencia, la información sensible es almacenada en sistemas de cómputo, Su valor, y la posibilidad de acceder esta información de forma remota, hace que el espionaje sea algo	Cabe citar las siguientes técnicas o estrategias utilizadas por los espías: Software para explorar los puertos desprotegidos.

[10] Ley 1273 de 2009, Código Penal Colombiano, art. 269A.
[11] Ley 1273 de 2009. Código Penal Colombiano, art. 269C.

		muy interesante. El espionaje de datos es un claro ejemplo de la explotación del eslabón más débil en la seguridad, el usuario.	Software para burlar las medidas de protección. "Ingeniería social"[12] La peska de datos ("phishing") consiste en tratar de obtener por fraude información confidencial.
Ofensas contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas de información.	Intercepción Ilegal de Comunicaciones	Con la creciente popularidad de los servicios IP, es posible que los legisladores tengan que evaluar hasta qué punto se ofrece una protección a estos servicios, similar a las interferencias telefónicas.[13] Al interceptar las comunicaciones de datos desde cualquier lugar situado en el interior de este así el canal se encontrara cifrado, los delincuentes serían capaces de descifrar y adueñarse	Intercepción de datos informáticos. Violación ilícita de comunicaciones.[14]

[12] La ingeniería social consiste en la manipulación de seres humanos con la finalidad de obtener acceso a sistemas informáticos.
[13] NOTA: Atacar cualquier infraestructura de comunicaciones (por ejemplo, líneas fijas o inalámbricas) y cualquier servicio Internet (por ejemplo, correo electrónico, charlas o comunicaciones VoIP) o intervenir las comunicaciones entre usuarios (como mensajes de correo electrónico) o interceptar transferencias de datos, o cualquier otra forma mal intencionada es considerado delito.
[14] Código Penal Colombiano, Art. 192.

		de la información. Para esto generalmente suelen elegir el nombre de una estación conocida de tal forma que los usuarios acaben seleccionando probablemente el punto de acceso fraudulento	
	Manipulación de datos	Los delincuentes pueden atentar contra la integridad de los datos de las siguientes formas: Borrarlos, Suprimirlos, Alterarlos, Restringir el acceso a los mismos.	Los virus son un ejemplo bastante común de pérdida de datos.[15] La infección por virus y han aumentado sobremanera el número de sistemas informáticos infectados.[16] Daño informático. [17]

[15] MOTA: Anteriormente, los virus informáticos se distribuían por dispositivos de almacenamiento, tales como disquetes, mientras que hoy en día los virus se distribuyen por Internet anexos a los mensajes de correo electrónico o a los ficheros que descargan los usuarios.
[16] NOTA: Los virus modernos son capaces de abrir puertas traseras por las que los piratas pueden tomar el control del computador o cifrar los ficheros del mismo de modo que las víctimas no puedan acceder a sus propios ficheros, a no ser que paguen para obtener la clave.
[17] Ley 1273 de 2009, Código Penal Colombiano, art. 269D

	Interferencia al sistema de información	Es posible realizar ataques físicos a los sistemas, siempre y cuando el delincuente tenga acceso físico a él, evidenciando el riesgo de que los equipos se dañen. [18] Desde el punto de vista jurídico, resulta más complejo el tema de los timos por la web.	Ataques a distancia contra servidores como es el caso de los gusanos informáticos; o en su efecto el ataque de denegación del servicio (DoS). El gusano o software malicioso una vez invernado en el sistema operativo, puede detener el buen funcionamiento y utilizar los recursos del mismo para reproducirse a sí mismo por Internet.[19] [20] Obstaculización ilegítima de sistema informático o red de telecomunicación.[21]
Ofensas	Material erótico o	Internet suele considerarse un medio anónimo característica que aprovechan	La penalización del material erótico y

[18] NOTA: En la mayoría de las legislaciones penales, el daño físico no plantea mayores problemas, dado que son similares a los casos clásicos de daño o destrucción de propiedad.
[19] En el 2000, en sólo un breve intervalo de tiempo, se lanzaron diversos ataques DoS contra empresas conocidas tales como CNN, Ebay y Amazon. Como resultado de ello, algunos de los servicio quedaron indisponibles durante horas e incluso días.
[20] NOTA: La interposición de una acción judicial contra los ataques de DoS y de gusanos informáticos plantea grandes dificultades a la mayoría de las legislaciones penales, por cuanto no implican ningún daño físico contra los sistemas víctimas de tales ataques. Además de la necesidad de penalizar los ataques por la web, la cuestión de si la prevención y denuncia de ataques contra la infraestructura esencial requiere un enfoque legislativo independiente sigue siendo objeto de debate.

[21] Ley 1273 de 2009. Código Penal Colombiano, art. 269B.

relacionadas con el Contenido.	pornográfico	muy bien los consumidores de pornografía.	pornográfico varía según el país.
	Pornografía Infantil	Distribución de pornografía infantil e intercambio de material por la red han resultado así como reclutamiento y trata de menores a través de blogs, paginas, foros, redes sociales, etc.	Alojar en su propio sitio imágenes, textos, documentos o archivos audiovisuales que impliquen directa o indirectamente actividades sexuales con menores de edad. Alojar en su propio sitio material pornográfico, en especial en modo de imágenes o videos, cuando existan indicios de que las personas fotografiadas o filmadas son menores de edad. Alojar en su propio sitio vínculos o links, sobre sitios telemáticos que contengan o distribuyan material pornográfico relativo a menores de edad.[22]

[22] Col. Ley 679 de 2001, prevención y persecución a la pornografía infantil y el turismo sexual.

Ofensas relacionadas con el Contenido.	Racismo, lenguaje ofensivo y exaltación a la violencia.	Aparte de la propaganda, Internet utiliza para vender ciertas mercancías, por ejemplo artículos relacionados con la ideología nazi, como banderas con símbolos, uniformes y libros, que se ponen a disposición en plataformas de subastas y cibertiendas especializadas.	Como ejemplos de sitios web de incitación a la violencia cabe citar los que contienen instrucciones para fabricar bombas.
	Delitos contra la religión	Son cada vez más los sitios web con material que algunos países consideran que atenta contra la religión. La protección de las diferentes religiones y símbolos religiosos varía de un país a otro.	Declaraciones antirreligiosas por escrito. Otros ejemplos son la difamación de religiones o la publicación de caricaturas.
	Apuestas ilegales y juegos en línea.	Los Informes muestran que algunos de estos juegos se han utilizado para cometer delitos, en particular: Intercambio y presentación de pornografía infantil; fraude; casinos en línea; y difamación. La reglamentación del juego dentro y fuera de Internet varía de un país a otro. Los casinos en línea	

		también pueden utilizarse para lavar dinero y financiar el terrorismo.	
	Difamación e información falsa	Internet puede utilizarse para divulgar información errónea con la misma facilidad que la información fidedigna. Los sitios web pueden contener información falsa o difamatoria, especialmente en los foros y salas de charla donde los usuarios pueden publicar sus mensajes sin la verificación de los moderadores.	Ahora bien, los delincuentes pueden utilizar esta misma tecnología para: Publicar información falsa (por ejemplo, sobre los rivales); difamar (por ejemplo, sitios web dedicados a la propaganda negra); revelar información confidencial (por ejemplo, publicar secretos de Estado o información comercial confidencial).[23]
	Correo basura y amenazas conexas	Aunque la tecnología de filtrado sigue desarrollándose, los remitentes siempre encuentran la forma de burlar estos sistemas – por ejemplo, evitando utilizar palabras clave. Al recurrir a redes zombi (o robot) constituidas por miles de	Spam, cadenas por email, etc.

[23] Col. Código Penal Colombiano, Título V, art. 220-223.

		sistemas informáticos, cada computador envía sólo unos cientos de mensajes.	
Propiedad Intelectual y Derechos de Autor.	Derechos de Autor	Los falsificadores pueden utilizar la imagen de marca y el diseño de una determinada empresa para comercializar productos falsificados, copiar logotipos y productos, y registrar su nombre de dominio. Las empresas que distribuyen sus productos directamente por Internet pueden tener problemas de carácter jurídico con las violaciones de los derechos de autor puesto que sus productos se pueden descargar, copiar y distribuir.	Páginas de descarga de material protegido por derechos de autor. Programas para intercambio de archivos (P2P)

	Marcas	Los delitos más graves son entre otros: La utilización de marcas en actividades delictivas con el propósito de engañar a las víctimas y los delitos en materia de dominios. En la mayoría de los casos, los delincuentes intentan vender el dominio a la empresa a un precio más elevado o utilizarlo para vender productos o servicios engañando a los usuarios con su supuesta conexión a la marca.	Ejemplo la peska, en las que se envían a los usuarios de Internet millones de correos electrónicos similares a los de empresas legítimas por ejemplo consignando su marca, la ciberocupación ilegal, que describe el procedimiento ilegal de registrar un nombre de dominio idéntico o similar al de la marca de un producto o de una empresa, la "apropiación indebida de dominio" o registro de nombres de dominio que han caducado accidentalmente.
Ofensas relacionadas con los sistemas de computo.	Fraude y fraude por computador.	Esta categoría abarca numerosos delitos para cuya realización se necesita disponer de un sistema informático. A diferencia de las categorías anteriores, estos delitos generales, que no suelen ser tan estrictos en la protección de principios jurídicos.	En esta categoría se incluyen: El fraude informático, la falsificación informática, la peska y el robo de identidad, la utilización indebida de dispositivos.

3. REVISION CONCEPTUAL DE LA NORMATIVA NACIONAL

3.1. LEY 527 DE 1999, "MENSAJE DE DATOS, FIRMA Y COMERCIO ELECTRÓNICO"

El principal objetivo de la Ley de 527 de 1999, es adoptar un marco normativo que avale los desarrollos tecnológicos sobre mensajes de datos, firmas y comercio electrónico, de manera que se pueda dar pleno valor jurídico a los mensajes electrónicos de datos que hagan uso de esta tecnología.

La nueva Ley de Comercio Electrónico es clara en establecer que cuando una norma exija que la información conste por escrito, este requisito queda satisfecho con un mensaje de datos, si la información que éste contiene es accesible para su posterior consulta y el mecanismo utilizado como firma permite identificar al remitente.

3.1.1. Definiciones

- **Mensaje de datos:** Se refiere a la información generada, enviada, recibida, almacenada comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax.
- **Comercio electrónico:** Abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar.
- **Firma o firma electrónica:** Información creada o utilizada por el signatario, asociada al mensaje de datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado.
- **Firma digital o firma cierta:** Se entenderá como un valor numérico que se ad-hiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido (función hash[24]), vinculado a la clave del iniciador y al

[24] La función hash que no es más que un algoritmo capaz de evitar que la criptografía asimétrica, en las firmas digitales, retarde el proceso de descifrado. La función hash analiza el documento y, basándose en

texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

3.1.2. Atributos jurídicos de una firma cierta

En adelante, la firma digital tendrá los mismos efectos de la firma escrita, siempre y cuando cumpla con unos requisitos mínimos:

- Es única a la persona que la usa.
- Es susceptible de ser verificada.
- Está bajo el control exclusivo de la persona que la usa.
- Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.
- Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

3.1.3. Ventajas de la firma digital sobre la firma electrónica:

Es un instrumento que garantiza la autenticidad del remitente de un mensaje de datos. Adicionalmente garantiza la integridad del mismo (certeza sobre la integridad de su contenido). Esto es así dado que cuando el contenido del documento es alterado, la firma digital es automáticamente invalidada. La firma va ligada inseparablemente al mensaje. Es imposible de falsificar, a diferencia de lo que sucede con la firma manuscrita. Como regla general, su uso por terceras personas se da solo bajo consentimiento del suscriptor o en todo caso por algún tipo de negligencia de su parte.

---

un algoritmo matemático complejo, genera un valor de tamaño fijo para el archivo. Ese valor, conocido como valor hash, se calcula en base a los caracteres del documento. Esto deja claro que, por lo menos teóricamente, el archivo en sí no requiere ser encriptado (en caso de no ser secreto), pero debe ser acompañado del valor hash. De esta forma, cualquier modificación en el archivo original, aunque sea de un solo bit, hará que el valor hash sea diferente, e invalidará el documento.

Tabla 4. Confiabilidad y valor probatorio de algunos tipos de firma

Mecanismo	Confiabilidad	Valor Probatorio	Prueba en Contrario
Firma Escaneada **Correo Electrónico**	**Baja**	**Bajo**	**Alta**
Usuario: Password:	**Baja**	**Medio**	**Alta**
Biométricos	**Media**	**Media**	**Media**
Certificado Digital CA-Cerrada	**Alta**	**Alta**	**Baja**
Certificado Digital CA-Abierta	**Alta**	**Alta**	**Nula**

3.1.4. Entidades de certificación (Certification Authority – CA)

Para que el receptor pueda asociar unívocamente la firma digital del mensaje a un emisor, debe existir una autoridad que certifique que la clave pública efectivamente le corresponde a esa persona. La Autoridad Certificante "da fe" de que una determinada clave pública le corresponde a un sujeto específico mediante la expedición del certificado. Este certificado le es entregado al suscriptor una vez generado el par de llaves, y es utilizado por dicho suscriptor para identificarse en sus operaciones.

En Colombia, las entidades de certificación son aquellas personas jurídicas y privadas, incluidas las Cámaras de Comercio(CERTICAMÁRAS), que poseen el hardware y software necesarios para la generación de firmas digitales, la emisión de certificados sobre la autenticidad de las mismas y la conservación y archivo de documentos soportados en mensajes de datos; suministrando la tecnología necesaria para generar las claves, a la vez que desarrolla los procedimientos requeridos para la identificación de los solicitantes, administra el proceso de emisión, verificación y revocación. Por otra parte controla el funcionamiento y desarrolla nuevas tecnologías para incrementar la confiabilidad y seguridad de las transacciones.

3.2. LEY 1266 DE 2008, "HABEAS DATA"

La jurisprudencia colombiana ha seguido muy de cerca los principios internacionales sobre la protección de datos personales que han sido incorporados en documentos de la Organización de las Naciones Unidas y la Unión Europea. Desde la primera sentencia (T 414/92) la Corte Constitucional de Colombia ha establecido que la persona es el titular y propietario del dato personal. Para ella es obligación de los administradores de bancos de datos administrar correctamente y proteger los archivos y bases de datos que contengan información personal o socialmente relevante y no atentar contra los derechos fundamentales de los ciudadanos.

La ley 1266 de 2008, tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, adicionalmente, desarrolla los derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales. La ley se aplica a todos los datos de información personal registrados en un banco de datos, sean estos administrados por entidades de naturaleza pública o privada.

3.2.1. Definiciones.

En el artículo 3, la ley define los actores del proceso de administración de datos personales de la siguiente forma:

- **Titular de la información:** Es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos.
- **Fuente de información:** Es la persona, entidad u organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación comercial o de servicio
- **Operador de la información:** Persona, entidad u organización que recibe de la fuente datos personales, los administra y los pone en conocimiento de los usuarios.
- **Usuario de información:** Es la persona natural o jurídica que, en los términos y circunstancias previstos en la presente ley, puede acceder a información personal de uno o varios titulares.

Adicionalmente, la ley define el dato personal como cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Clasifica los datos personales como:

- **Dato público:** Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Ej: documentos públicos, sentencias judiciales que no estén sometidos a reserva y el estado civil de las personas.
- **Dato semiprivado:** Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.
- **Dato privado:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

3.2.2. Principios de la administración de datos personales.

- **Principio de veracidad calidad de los registros o datos:** La información contenida en los bancos de datos debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
- **Principio de finalidad:** La finalidad debe ser legítima e informada al titular de la información previa o simultáneamente con el otorgamiento de la autorización.
- **Principio de circulación restringida:** Los datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, **salvo que el acceso sea técnicamente controlable.**
- **Principio de temporalidad de la información.** La información del titular no podrá ser suministrada a usuarios o terceros cuando deje de servir para la finalidad del banco de datos;
- **Principio de interpretación integral de derechos constitucionales:** La presente ley se interpretará en el sentido de que se amparen adecuadamente los derechos constitucionales, como son el hábeas data, el derecho al buen nombre, el derecho a la honra, el derecho a la intimidad y el derecho a la información.
- **Principio de seguridad:** La información que conforma los registros individuales constitutivos de los bancos de datos, así como las consultas que de ella hagan sus usuarios, se deberán manejar con las medidas técnicas que sean necesarias para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta o uso no autorizado;
- **Principio de confidencialidad:** Todas las personas naturales o jurídicas que intervengan en la administración de datos personales que no tengan la naturaleza de públicos están obligadas en todo tiempo a garantizar la reserva de la información.

Derechos de los titulares de la información:

- Frente a las fuentes de información:
  - Ejercer el derecho al habeas data.
  - Solicitar información o pedir la actualización o rectificación de los datos contenidos en la base de datos.
  - Solicitar prueba de la autorización.
- Frente a los operadores de bases de datos:
  - Ejercer el derecho al habeas data.
  - Solicitar el respeto y la protección de los demás derechos constitucionales mediante la utilización del procedimiento de reclamos y peticiones.
  - Solicitar prueba de la certificación de la existencia de la autorización expedida por la fuente o por el usuario.
  - Solicitar información acerca de los usuarios autorizados para obtener información.
- Frente a los usuarios:
  - Solicitar prueba de la autorización.
  - Solicitar información sobre la utilización que el usuario le está dando a la información, cuando dicha información no hubiere sido suministrada por el operador.

3.2.3. Deberes de los actores del proceso de administración de datos

- De los operadores de bases de datos:
  - Garantizar al titular el ejercicio del habeas data.
  - Garantizar, que en la recolección, tratamiento y circulación de datos se respetarán los demás derechos.
  - Permitir el acceso a la información únicamente a las personas autorizadas.
  - Tener y divulgar el manual de políticas y procedimientos.
  - Solicitar la certificación a la fuente de la existencia de la autorización otorgada por el titular.

- Conservar con las debidas seguridades los registros almacenados para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento.
- Realizar periódica y oportunamente la actualización y rectificación de los datos, cada vez que le reporten novedades las fuentes.
- Tramitar las peticiones, consultas y los reclamos formulados por los titulares de la información.

- Deberes de las fuentes de información:
  - Garantizar que la información que se suministre a los operadores de los bancos de datos o a los usuarios sea veraz, completa, exacta, actualizada y comprobable.
  - Reportar, de forma periódica y oportuna al operador, todas las novedades. Actualizar la información.
  - Rectificar la información cuando sea incorrecta e informar lo pertinente a los operadores.
  - Solicitar, cuando sea del caso, y conservar copia o evidencia de la respectiva autorización otorgada por los titulares de la información.
  - Certificar, semestralmente al operador, que la información suministrada cuenta con la autorización.
  - Resolver los reclamos y peticiones del titular.
  - Informar al operador que determinada información se encuentra en discusión por parte de su titular.

- Deberes de los usuarios:
  - Guardar reserva sobre la información que les sea suministrada por los operadores de los bancos de datos, por las fuentes o los titulares de la información.
  - Utilizar la información únicamente para los fines para los que le fue entregada
  - Informar a los titulares, a su solicitud, sobre la utilización que le está dando a la información.

- Conservar con las debidas seguridades la información recibida para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento.

3.3. LEY DE 1273 DEL 2009, "PROTECCION DE DATOS Y SISTEMAS INFORMÁTICOS".

Esta ley tiene por objeto crear un nuevo bien jurídico tutelado, denominado: "de la protección de la información y de los datos", adicionalmente, vela por la preservación integral de los sistemas que utilizan las tecnologías de la información y las comunicaciones (TICs).

Crea un marco legal para los delitos informáticos e impone sanciones que van desde 48 a 96 meses de cárcel y multas de 100 a 1000 salarios mínimos legales vigentes.

Entre las ofensas o conductas delictivas que se tipifican tenemos:

- El acceso abusivo a un sistema informático
- Obstaculización ilegítima de sistema informático o red de telecomunicación
- Interceptación de datos informáticos
- Uso de software malicioso
- Violación de datos personales
- Suplantación de sitios web para capturar datos personales
- Hurto por medios informáticos y semejantes
- Transferencia no consentida de activos.

3.4. CIRCULAR REGLAMENTARIA 052 DE LA SUPERINTENDENCIA FINANCIERA DE COLOMBIA

La superintendencia financiera de Colombia debido al incremento de eventualidades de fraudes y antecedentes de crímenes efectuados a través de la red internet, establece requerimientos mínimos que deben ser cumplidos por las entidades vigiladas, en aras de la seguridad y calidad de la información que se maneja a través de los canales y medios de distribución de productos y servicios para clientes y usuarios. Para tal propósito, cada entidad establece la forma y medios que le permitan dar cumplimiento a los mismos. Toda entidad que ofrezca

el servicio de operaciones transaccionales por Internet debe cumplir con los siguientes requerimientos:

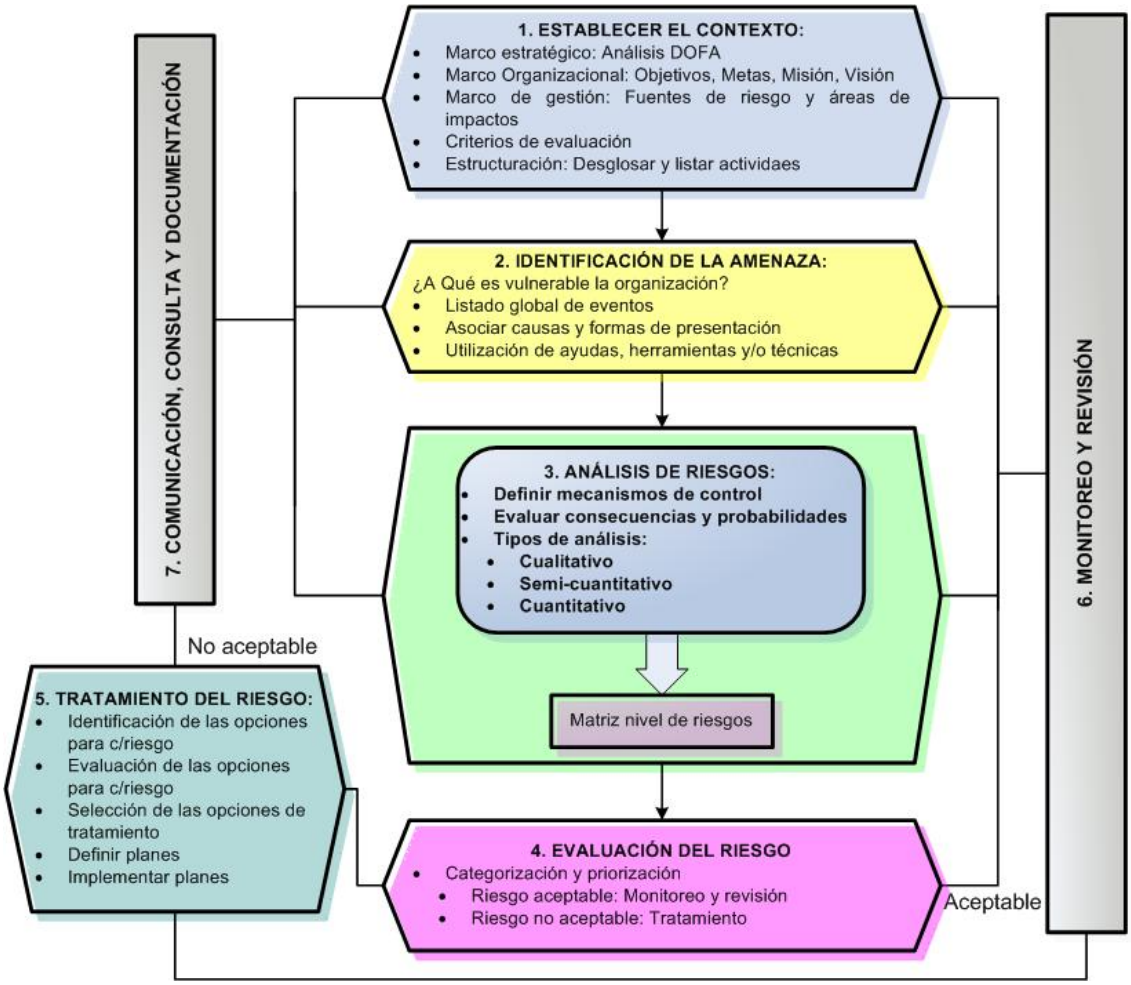
- Implementar los algoritmos y protocolos necesarios para brindar una comunicación segura.
- Realizar como mínimo dos veces al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación usados en la realización de transacciones por este canal.[25]
- Promover y poner a disposición de sus clientes mecanismos que reduzcan la posibilidad de que la información de sus transacciones pueda ser capturada por terceros no autorizados durante cada sesión.
- Establecer el tiempo máximo de inactividad, después del cual se deberá dar por cancelada la sesión, exigiendo un nuevo proceso de autenticación para realizar otras operaciones.
- Informar al cliente, al inicio de cada sesión, la fecha y hora del último ingreso a este canal.
- Implementar mecanismos que permitan a la entidad financiera verificar constantemente que no sean modificados los enlaces (links) de su sitio Web, ni suplantados sus certificados digitales, ni modificada indebidamente la resolución de sus DNS.

[25] Sin embargo, cuando se realicen cambios en la plataforma que afecten la seguridad del canal, deberá realizarse una prueba adicional.

4. METODOLOGIA Y ANALISIS DE RIESGO

La gestión de riesgos se reconoce como una actividad que aplica métodos lógicos y sistemáticos para establecer el contexto, identificación, análisis, evaluación, tratamiento, monitoreo y comunicación de los riesgos asociados a cualquier tipo de actividad ó proceso, por lo cual hoy en día se considera que este proceso es vital y debe ejecutarse en cualquier organización que busque identificar oportunidades y prevenir o minimizar pérdidas. A continuación, se presenta el diagrama de bloques de la metodología que análisis de riesgo que se llevará a cabo.

Figura 1. Metodología de anális de riesgo



Fuente: Herrera Shirley, Análisis de riesgo para aplicaciones P2P.

4.1. ESTABLECER EL CONTEXTO

Este paso enmarca los parámetros básicos para realizar la gestión de riesgos de forma que se define el entorno de todo el proceso de gestión, así como posteriores estudios más detallados.

4.1.1. Marco Estratégico:

El análisis de riesgos que se realizará a continuación estará enfocado a la prestación de servicios financieros mediante el uso de las nuevas tecnologías de la información y comunicación, es decir, la banca electrónica. Se realizará un análisis cualitativo de impacto, teniendo en cuenta la influencia y percepción de los usuarios finales sobre elementos como la calidad del servicio, la seguridad del mismo y la confianza que estos en las instituciones financieras y sus canales electrónicos. Mediante un análisis DOFA se identifican a groso modo algunas características del análisis que pueden representar este tipo de servicios:

- **Dificultades:** Difusión de las ayudas y/o gestión que puede realizar la institución financiera sobre los hábitos de navegación de los usuarios finales.
- **Oportunidades:** Disminución de costos y agilidad en la prestación de servicios financieros a través de las TIC.
- **Fortalezas:** Amplia regulación del mercado y facilidad de acceso a recursos tecnológicos que permiten garantizar la seguridad de los sistemas de información.
- **Amenazas:** Mala imagen y/o desacreditación de la gestión realizada, perdidas de confianza por parte del consumidor. Afectación del patrimonio económico de los clientes e incluso de la institución financiera.

A continuación se presenta la tabla que relaciona las fuentes de riesgo y las áreas de impacto, en el análisis se concluye (Tabla 12):

Tabla 5. Relación fuentes de riesgos y áreas de impacto

Fuentes de Riesgo	Área de Impacto				
	Responsabilidad Legal	Activos Informáticos	Impacto Financiero	Intangibles	QoS
Comportamiento humano	X	X	X	X	X
Nuevas tecnologías	X	X	X	X	X
Información	X		X	X	X
Procesos y procedimientos	X	X	X	X	X

Los responsables directos del proceso de gestión de esta aplicación será el grupo de informática, específicamente; sin embargo, en caso de existir, será el personal dedicado a velar por la seguridad de la información de la entidad financiera pues, sobre ellos recaen entre otras las siguientes funciones: definir políticas sobre el uso adecuado de los recursos, implementar los mecanismos de SI y llevar a cabo el seguimiento de la aplicación y del cumplimiento de las políticas.

4.2. IDENTIFICACION DE LA AMENAZA

Este proceso de identificación de riesgos debe hacerse de forma amplia, sistemática y estructurado, debe incluir tanto los riesgos que estén bajo el control de la organización como los que no, este paso es crucial en el proceso de gestión, debido a que los riesgos potenciales que no se listen en este punto serán excluidos de todo el análisis. Para este análisis, se consideraran las amenazas provenientes de las siguientes fuentes: personas, tecnologías y procesos o procedimientos.

4.2.1. Amenazas asociados a la naturaleza de la información

Dada la naturaleza de dato personal semiprivado otorgado por la ley 1266 de 2008 a la información financiera, este puede verse inmerso en riesgos como:

- **Perdida de confidencialidad:** La información financiera de un individuo puede permitir que este sea determinable, ya sea por su condición económica o por sus hábitos de consumo, por tal razón, la perdida de confidencialidad podría afectar la intimidad de los cuentahabientes.
- **Perdida de integridad:** La alteración del dato financiero puede ocasionar problemas económicos y la imposibilidad de gozar de los servicios bancarios al cuentahabiente. Adicionalmente, toda alteración del dato financiero representará una afección al patrimonio económico del sector inversionista o del consumidor.
- **No disponibilidad:** La imposibilidad de acceder a la información financiera en el momento requerido por parte de su propietario, tendrá como mínimo un impacto en términos de calidad de servicio e imagen de la entidad financiera. Adicionalmente, un usuario final podría verse afectado en términos del costo de la oportunidad al no contar con su información financiera actualizada.

4.2.2. Amenazas originadas por el comportamiento humano

- **Hackers:** Tanto las motivaciones de los atacantes informáticos como su capacidad de ejecutar la amenaza varían dependiendo del perfil del hacker, tal como se presentó en el capítulo 3.
- **Usuario final**: A pesar de ser un usuario valido en el sistema de banca electrónica y cuya motivación para causar daño se entiende inexistente, este suele ser el eslabón más débil de la cadena por dos simples razones:
    - Una gran parte de los usuarios finales son recaídos a seguir las recomendaciones de buen uso de las nuevas tecnologías (ej:

- Los usuarios finales son muy inocentes respecto a la inseguridad informática y a las estafas en línea, convirtiéndose en víctimas de ataques de ingeniería social.
- El usuario final considera en muchas ocasiones que su PC de la casa es un PC seguro, sin embargo, no se preocupa por mantenerlo como tal, es decir, olvida o no se interesa por tener una buena suite de antivirus, firewall, y detector de intrusos; olvida actualizar su sistema operativo y aplicaciones; descarga e instala software desconocido; descarga y abre documentos y archivos multimedia de procedencia desconocida, generando ambientes de baja seguridad o poca higiene informática.

- **Administradores: L**os sistemas operativos y el software en general son seguros o inseguros dependiendo de cómo se hayan configurado. Por defecto, las configuraciones suelen ser inseguras y requieren de la habilidad y conocimiento de los administradores de sistemas para que endurezcan (hardening[26]) la seguridad de los sistemas. Dentro de estos errores de configuración se incluye, entre otras, la mala selección de algoritmos de cifrado para los portales.

4.2.3. Amenazas asociados a las nuevas tecnologías

- **Malware o código malicioso:** Infortunadamente, no todas las nuevas tecnologías buscan algo positivo, con frecuencia aparecen en la red programas cuya finalidad es la de afectar los servicios, alterar la información o simplemente robarla. Se encuentran catalogadas como malware todas las aplicaciones de tipo adware (pop-ups, baners), trackware (barras de herramientas sensibles al contexto) y el spyware (envía a

[26] Security Benchmarks from Center for Internet Security, www.cisecurity.org

terceros información acerca de los hábitos de navegación e información confidencial del usuario), adicionalmente, se incluyen también todos los programas tipo virus, gusanos y troyanos.

- **Cambio de tecnología:** En la actualidad tanto el hardware como el software tienen unas ratas de obsolescencia altas, obligando a que los arquitectos de infraestructura deban elegir entre: continuar usando tecnologías desactualizadas o inseguras o, migrar sus sistemas a nuevas tecnologías impactando las curvas de aprendizaje de los usuarios y de los mismos administradores.
- **Movilidad:** La movilidad aportada por las nuevas tecnologías (Redes WiFi y redes 3G) dificultan el seguimiento y la trazabilidad de las acciones de los cuentahabientes, esto dificulta considerablemente las investigaciones relacionadas con robos electrónicos y fraudes en línea.
- **Errores en el software (bugs y vulnerabilidades):** Como la mayoría de estas aplicaciones son desarrolladas bajo licencias públicas (GNU), es fácil encontrar errores en el código fuente que pueden ser explotados por un atacante, para ejecutar código arbitrario en un sistema remoto. Prueba de ello son las múltiples notificaciones generadas mensualmente por organizaciones como el CERT, Computer Emergency Response Team[27].

4.2.4. Amenazas asociadas a los procesos y procedimientos

- **Proceso de autenticación de usuarios de usuarios:** En la actualidad, la banca realiza diferentes procesos de autenticación dependiendo del tipo de servicio que esté requiriendo el cuentahabiente o del tipo de canal de comunicación que este emplee para acceder a la banca electrónica.
- **Proceso de atención de incidentes:** Los usuarios de la Banca en línea, han sido víctimas en los últimos años, de diferentes estafas informáticas.

[27] CERT: Centro de expertos para la seguridad en Internet, opera en Estados Unidos, Carnegie Mellon University.

No obstante, el procedimiento de respuesta a ese tipo particular de incidentes no es claro para muchos usuarios lo que genera en ellos una fuerte desconfianza al sistema financiero.

- **Procesos de cumplimiento legal y regulatorio:** Las entidades financieras en Colombia, deben acogerse a las regulaciones del sector y en particular a la ley de Habeas Data. El no cumplimiento de estas normativas podría acarrear penalizaciones económicas bastante altas.

4.3. PROBABILIDAD DE OCURRENCIA DE LAS AMENAZAS

Mediante la aplicación de un modelo de encuesta tanto a usuarios de servicios de la banca electrónica y a expertos en el tema de seguridad informática se pretende realizar un sondeo y medir el nivel de vulnerabilidad que se exponen los usuarios del sector Bancario en general teniendo en cuenta las recomendaciones de los expertos.

La encuesta es una percepción de un grupo de profesionales del área informática que han tenido la experiencia en la administración de una red de datos. Contrastando la visión de usuarios del común y comparando los resultados con algunos trabajos sobre la creación de planes de contingencia y políticas de seguridad informática, aplicada a los procesos de banca en línea ofrecidos en Colombia, con el fin de realizar un diagnostico más profundo, se llevó a cabo un pre diagnóstico a los usuarios del sistema en banca en línea. [28]

4.3.1. **Objetivos de la encuesta:** Detectar la percepción de usuarios y expertos respecto a las amenazas y vulnerabilidades que podrían permitir que el escenario de riesgo se presente y así como la probabilidad de que esto ocurra.

[28] NOTA: En la elaboración del presente estudio se utilizo EncuestaTick como software gratuito de encuestas online, con el que se puede crear, enviar y gestionar las encuestas.

Conocer el comportamiento de usuarios, respecto a los servicios transaccional en línea que ofrece la Banca a sus socios y clientes.

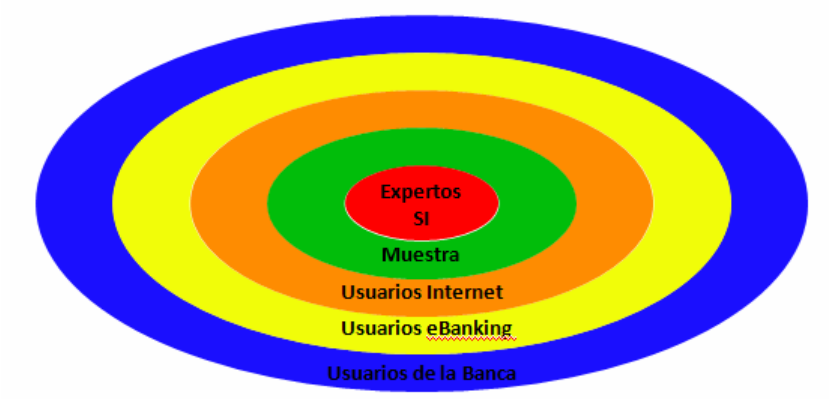
4.3.2. Tipo de investigación:

Investigación descriptiva mediante una interpretación de las dos encuestas aplicadas:

- Encuestas sobre la percepción y hábitos de los usuarios de la banca electrónica nacional.
- Encuesta a expertos de seguridad de la información sobre la seguridad de la banca electrónica en Colombia.

4.3.3. **Marco muestral:** Para construir el marco muestral de la encuesta se seleccionó aleatoriamente un grupo de usuarios del servicio de Banca en línea. Así como expertos en el área de administración de redes de informática.

Figura 2. Marco muestral de la población encuestada



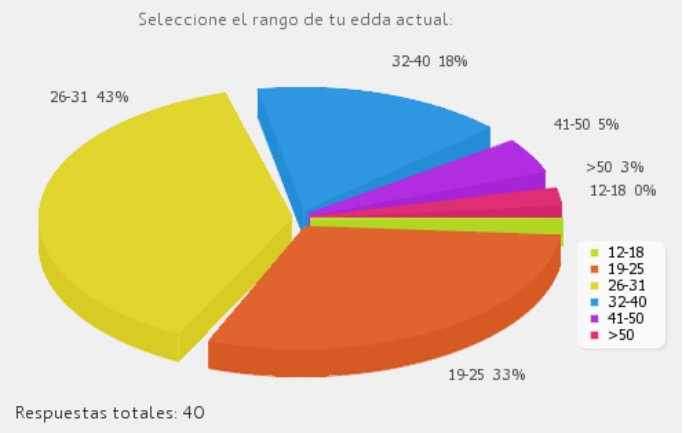
Fuente: Autor

4.3.4. **Período de referencia:** Las encuestas tuvieron lugar en el ciberespacio, durante los días 22 de mayo de 2010 y 15 de junio de 2010.

4.3.5. Resultados de la encuestas sobre la percepción y hábitos de los usuarios de la banca electrónica nacional.

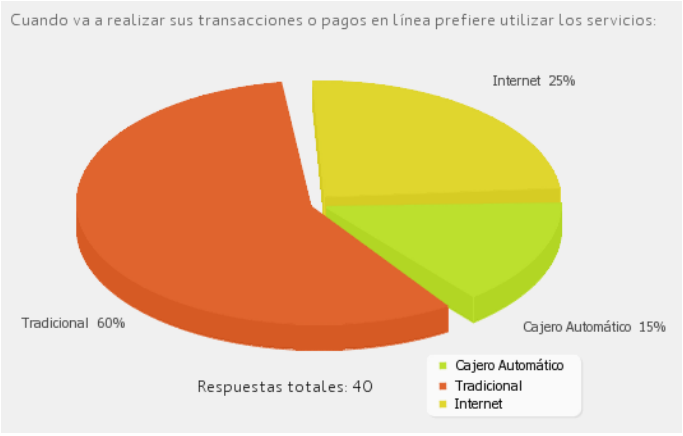
a) El 43% de los encuestados se encuentra entre los 26 y 31 años, un 33% entre 19 y 25, el 18% entre 32 y 40 años, un 5% entre 41y50, y un 5% a la población mayor de 50 años.

Figura 3. Edad de los encuestados



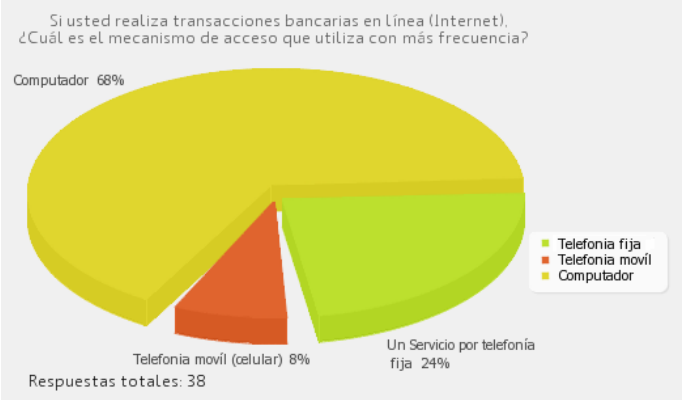
b) El 60% de los usuarios de la banca en línea prefieren realizar sus transacciones bancarias, mediante el servicio tradicional seguidamente de la banca electrónica con un 25%. Un 15% utiliza el internet.

Figura 4. Acceso a servicios bancarios



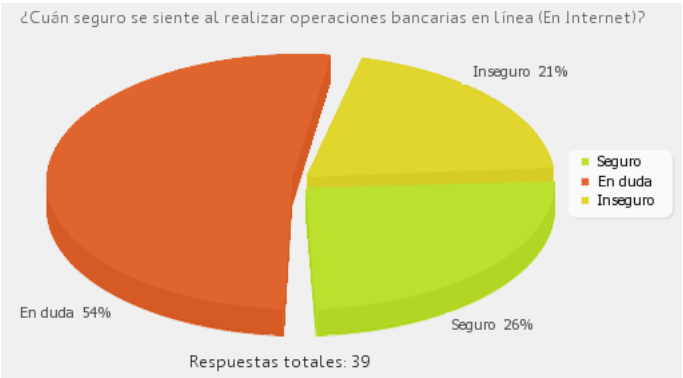
c) De los usuarios de eBanking, el 68% se conecta desde su computador, el 32% restante se divide entre la telefonía fija y la móvil.

Figura 5. Servicios electrónicos utilizados



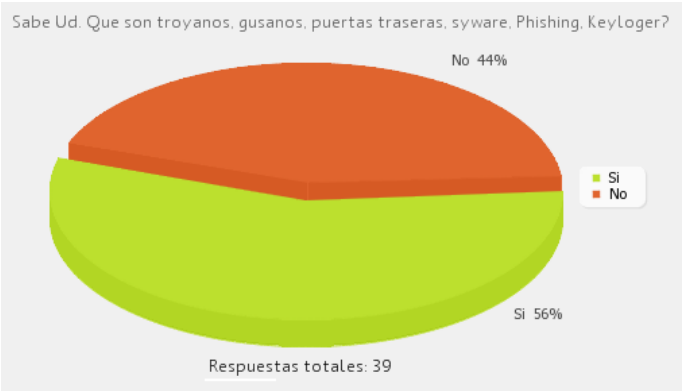
d) El 54% de los usuarios encuestados dudan de la seguridad de los portales bancarios. Sólo el 26% creen que es seguro y un 21% las consideran que los portales no son seguros.

Figura 6. Considera seguro realizar transacciones bancarias en-línea



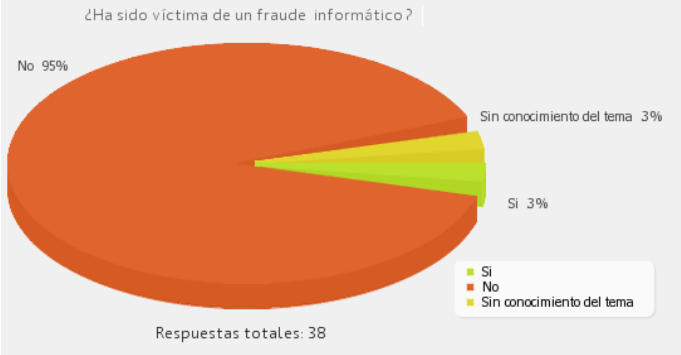
e) El 56% de los encuestados sabe o ha oído hablar de malware (keylogger, gusanos, spyware, troyanos, virus)

Figura 7. Conocimiento sobre malware



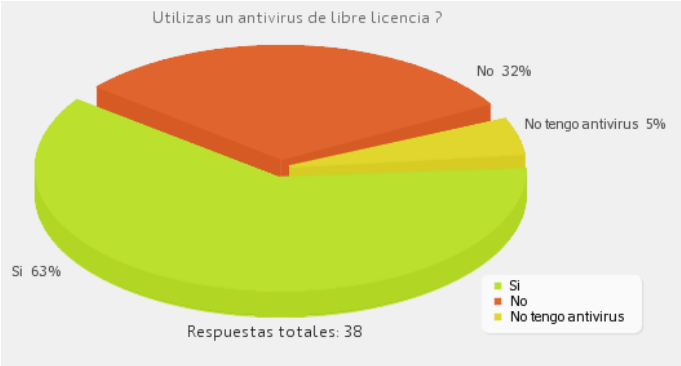
f) Sólo el 3% de los encuestados manifiesta haber sido víctima de fraudes informáticos como robos o suplantaciones de identidad.

Figura 8. Victimas de fraude



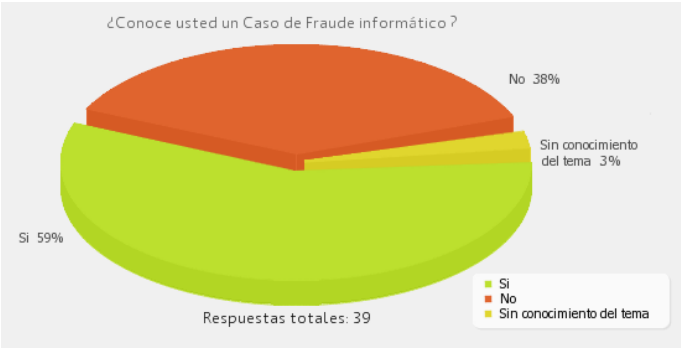
g) Un 63% de los encuestados utiliza antivirus con licencia GNU, y un 5% no poseen antivirus. Sólo el 39% usa antivirus comercial con soporte.

Figura 9. Uso de antivirus



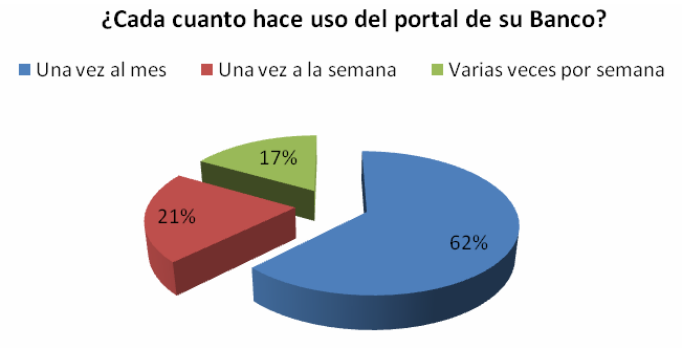
h) El 59% de los encuestados afirman conocer casos de fraudes informáticos.

Figura 10. Conoce algún caso de fraude informático



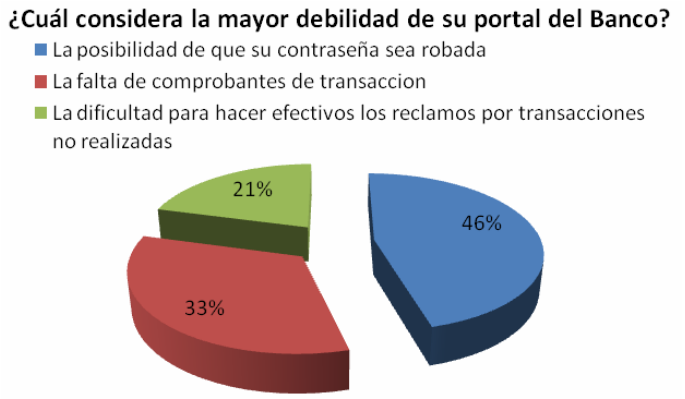
i) El 17% de los usuarios hace uso del portal de su Banco varias veces por semana, mientras que un 21% lo utiliza una vez por semana

Figura 11. Frecuencia de uso del portal



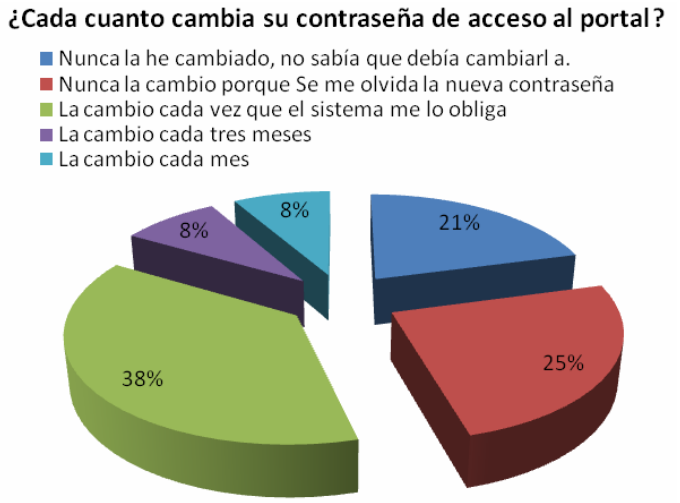
j) El 46% considera que la mayor debilidad del portal es que existe la posibilidad de que su contraseña sea robada. Al 21% le preocupa tener que hacer un reclamo por transacciones no realizadas.

Figura 12. Debilidades del portal



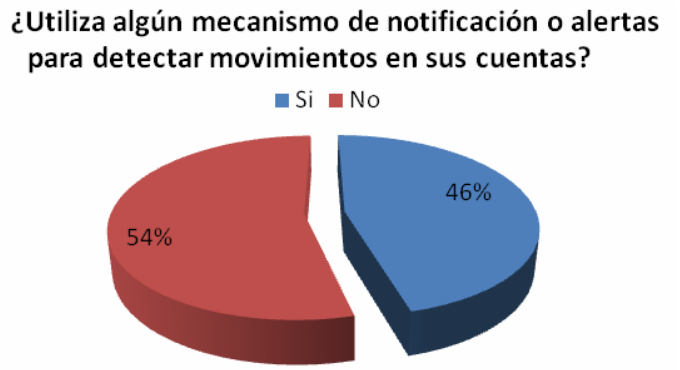
k) Según la encuesta, el 46% de los usuarios no sabe que debe cambiar su contraseña o no la cambia porque la olvida. El 38% sólo la cambia cuando el sistema se lo exige. Sólo el 16% cambia su contraseña voluntariamente.

Figura 13. Cambio de contraseña



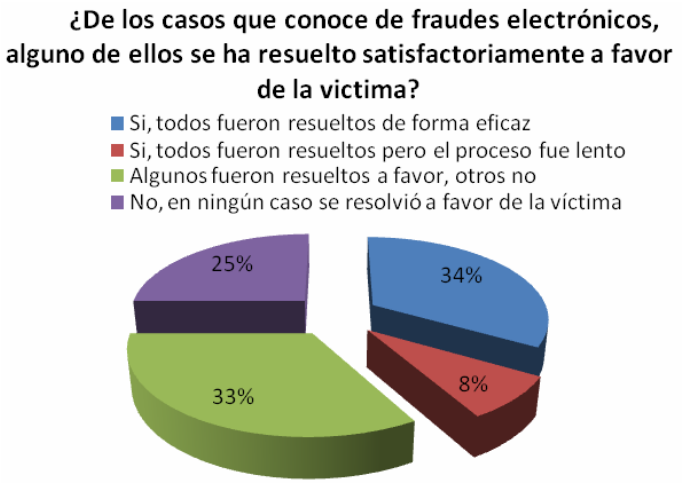
k) Sólo el 46% de los usuarios utiliza algún mecanismo de alertas en tiempo real (SMS, email) para notificar los movimientos de sus cuentas.

Figura 14. Alertas transaccionales



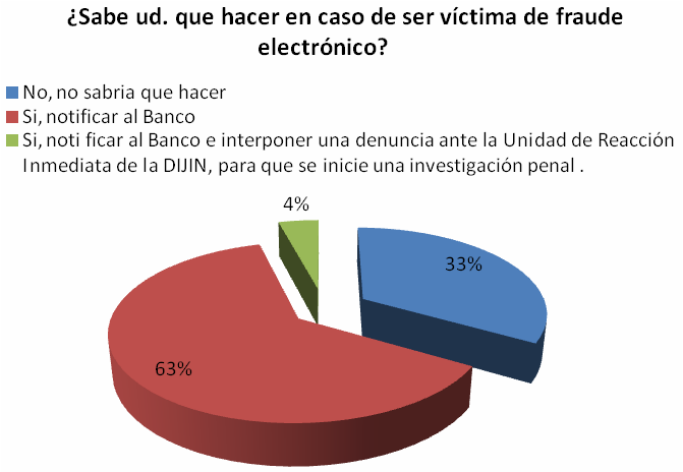
k) El 34% de los usuarios afirman que los casos de fraudes electrónicos fueron resueltos de forma eficaz. Un 33% aseguran que unos fueron resueltos a favor y otros no. El 25% de las reclamaciones fue negada por el Banco.

Figura 15. Resolución de reclamos por fraude



k) El 33% de los usuarios no sabría qué hacer en caso de ser víctima de un fraude. Sólo el 4% de ellos reaccionaría adecuadamente. Es evidente la falta de información al respecto.

Figura 16. Respuesta a incidentes



k) Más del 60% de los

Figura 17. Reconocimiento del portal

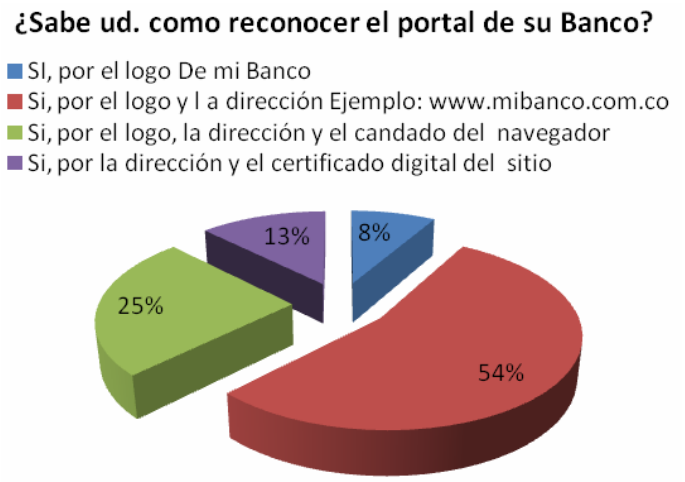
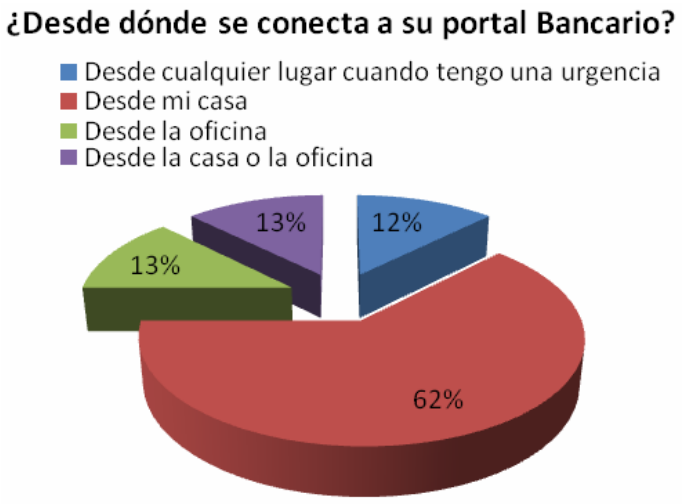


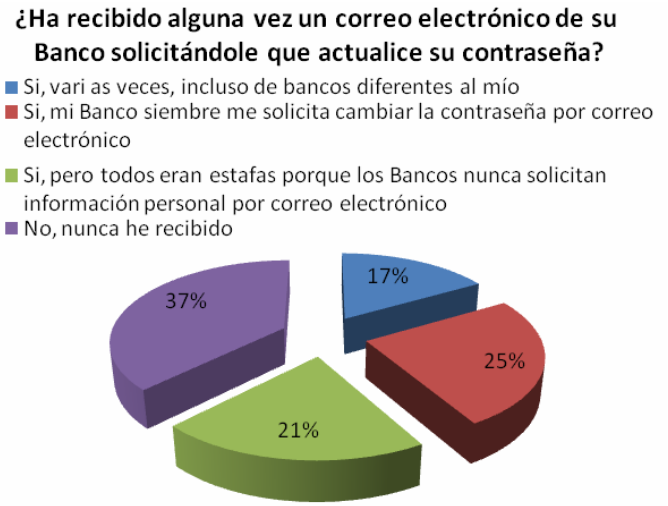
Figura 18. Lugar de conexión.

k) El 88% de los usuarios se conecta a su portal bancario desde el PC de su casa o desde el PC de su oficina. Sólo un 12% de los encuestados se conecta actualmente desde cualquier PC.



k) El 63% de los encuestados ha recibido correos de tipo Phishing, sin embargo, sólo el 21% de los encuestados los reconoce como un método de estafa o fraude electrónico

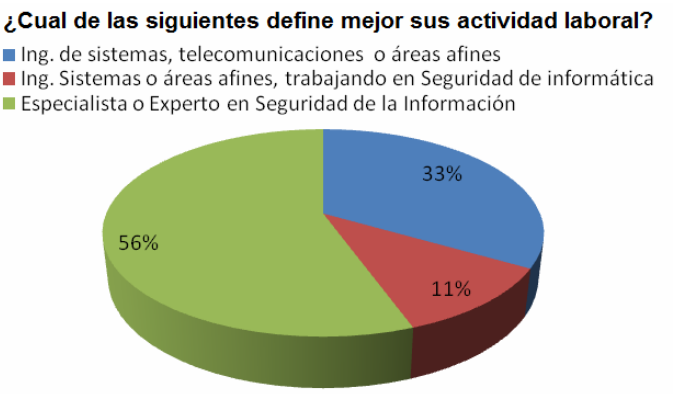
Figura 19. Exposición al Phishing



4.3.6. Resultados de la encuesta a expertos sobre su percepción y hábitos con la banca electrónica nacional.

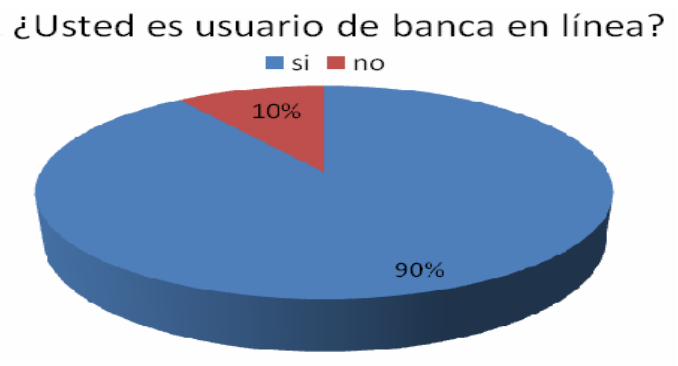
a) El 67% de los encuestados trabaja o tiene experiencia con temas de seguridad de la información. El 33% restante trabaja en áreas afines a las nuevas tecnologías.

Figura 20. Actividad o profesión



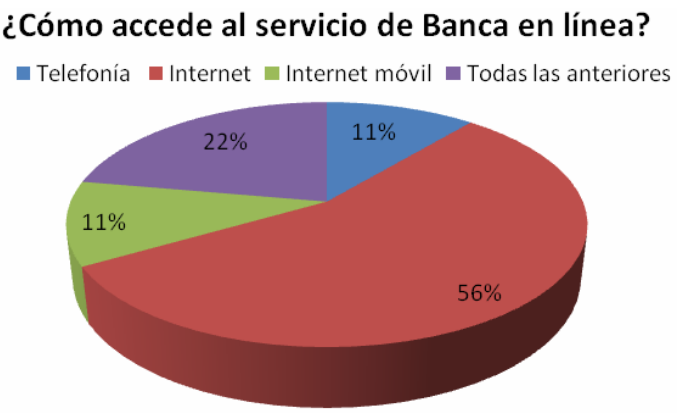
b) El 90% de los encuestados es usuario activo de la banca electrónica.

Figura 21. Acceso a servicios bancarios



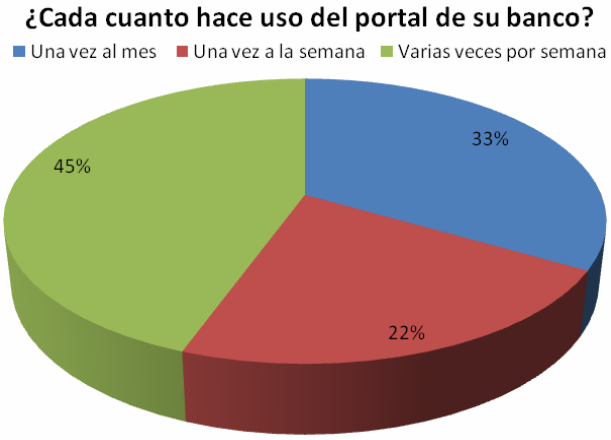
c) El 89% de los encuestados se conecta a través de Internet (móvil o tradicional). El 11% sólo utiliza la telefonía fija para realizar transacciones bancarias.

Figura 22. Canal de acceso a eBanking



d) La totalidad de los respondientes utilizan los servicios de banca electrónica al menos una vez al mes. El 55% lo hace al menos una vez a la semana.

Figura 23. Frecuencia de uso



e) El 89% de los expertos consideran que los portales de la Banca en linea son seguros. Sin embargo, un 44% considera que los incidentes se deben en gran parte a los usuarios no lo saben usar. Un 11% duda de la seguridad de los portales.

f) El 50% de cree que falta observancia y trazabilidad sobre las transacciones. Para el 30% falta capacitación al usuario. El 20% restante divide su opinión entre la necesidad de mecanismos fuertes de autenticación y cifrado.

Figura 24 Seguridad de los portales según expertos

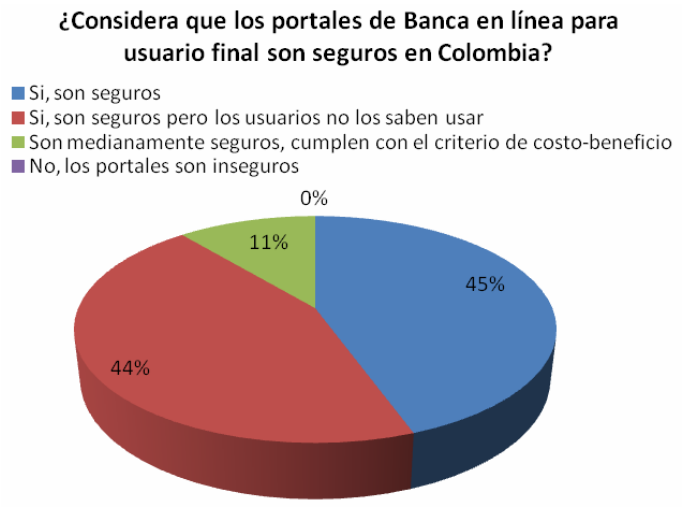
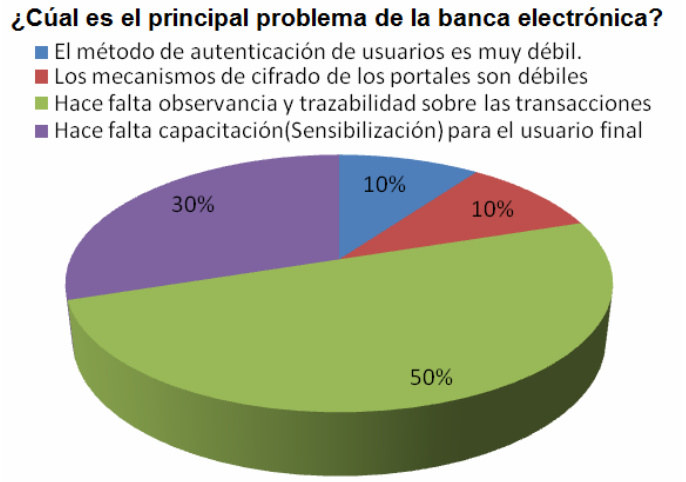
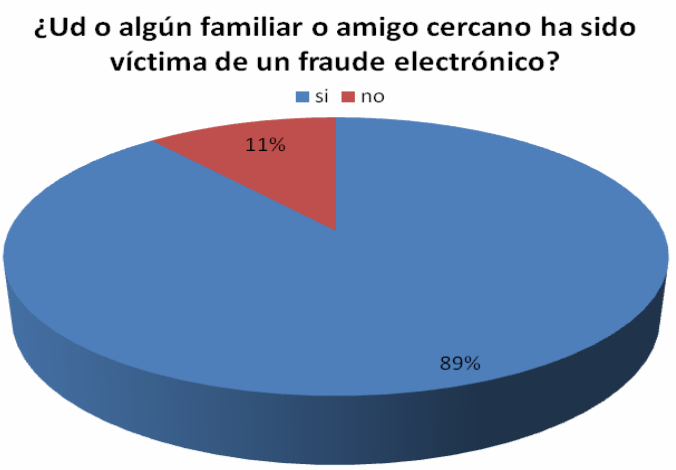


Figura 25. Problemas del eBanking



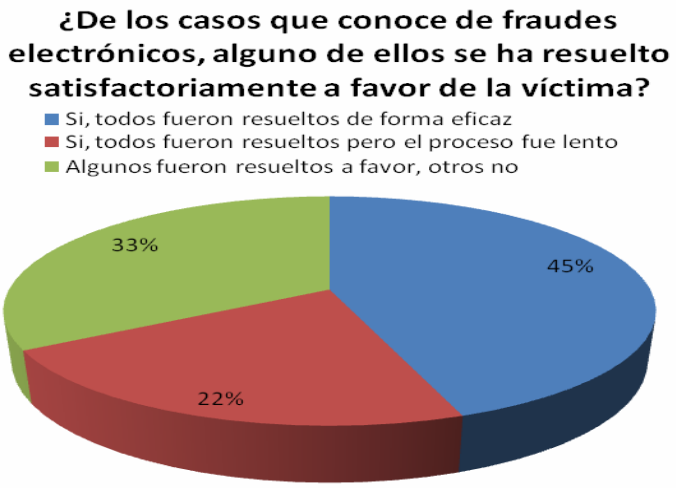
g) El 89% de los expertos encuestados afirma conocer a algún familiar o amigo cercano que ha sido victima de incidente de fraude electrónico.

Figura 26. Incidentes de fraude electrónico



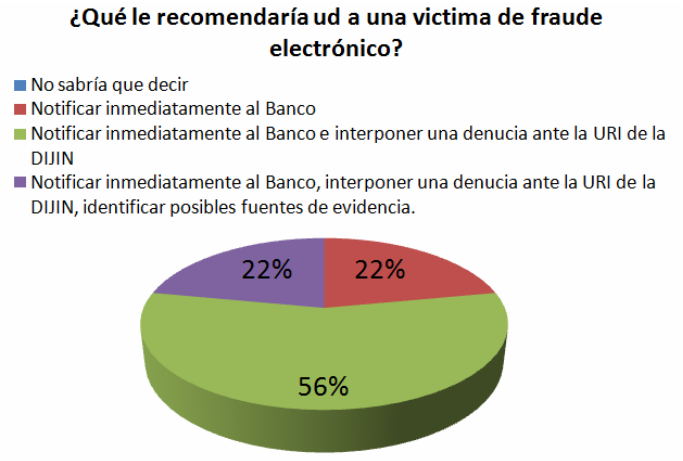
h) Menos de la tercera parte de los incidentes reportados finalizan con respuestas negativas para el usuario final.

Figura 27. Solución de fraudes electrónico



i) El 78 % de los expertos

Figura 28. Incidentes de fraude electrónico



Fuente: PortalDeEncuestas, EncuestaTick

4.3.7. Resultados de la auditoria a los portales de banca electrónica de los principales bancos en Colombia.

Este proceso de auditoría de seguridad sólo incluyó un número reducido de validaciones, todas ellas enfocadas a detectar vulnerabilidades o fallas de configuración en los servidores web de los portales de banca electrónica en Colombia. Adicionalmente, se excluyeron todas las validaciones de tipo intrusivo con el fin de evitar cualquier tipo de afectación en los servicios auditados.

Para la ejecución de estas auditorías se utilizaron los siguientes programas:

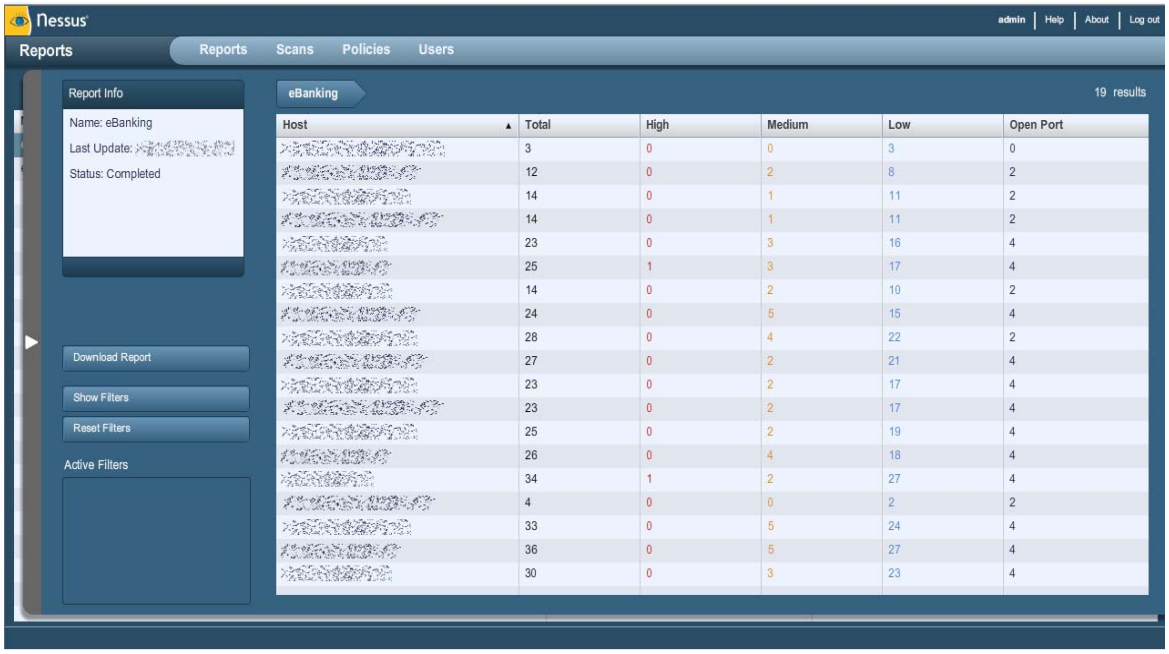
- Tenable Nessus www.tenable.com/nessus
- Foundstone SSL Digger www.foundstone.com

A continuación se presenta la lista de los portales auditados, no obstante, durante el proceso de análisis no se hará alusión a ninguno de estos portales en particular, es decir, en ningún momento este estudio pretende determinar cuál de los portales es el más o menos seguro.

Tabla 6. Relación fuentes de riesgos y áreas de impacto

Portales Auditados	
bancaelectronica.bancoldex.com	www.bancodebogota.com
bancolombia.olb.todo1.com	www.bancodeoccidente.com.co
enlinea.bancocajasocial.com.co	www.bancopopular.com.co
en-linea.colmena.com.co	www.grupohelm.com
linea.davivienda.com	www.hsbc.com.co
servicios.sudameris.com.co	www.latinamerica.citibank.com
wsebra.banrep.gov.co	www.mispagosaldia.com
www.avvillas.com.co	www.santander.com.co
www.bancafeunico.com.co	www.zonapagos.com
www.banco.colpatria.com.co	

Figura 29. Resultado del análisis con Nessus

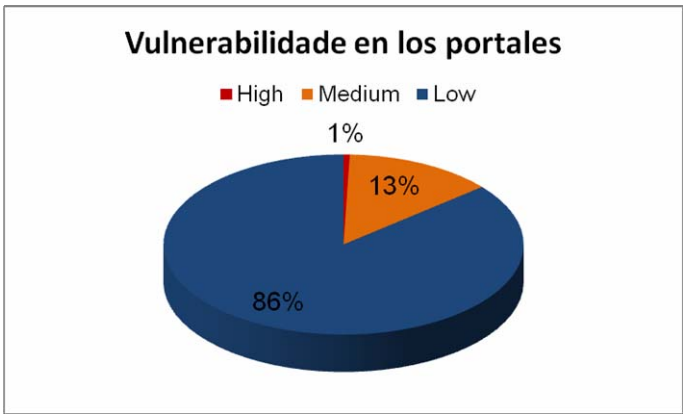


Fuente: Autor

Del proceso de auditoría logró determinar qué:

a) En promedio, los portales reportan 18 vulnerabilidades, de las cuales, el 86% corresponden a errores de configuración que representan riesgos bajos, el 13% de riesgo medio.

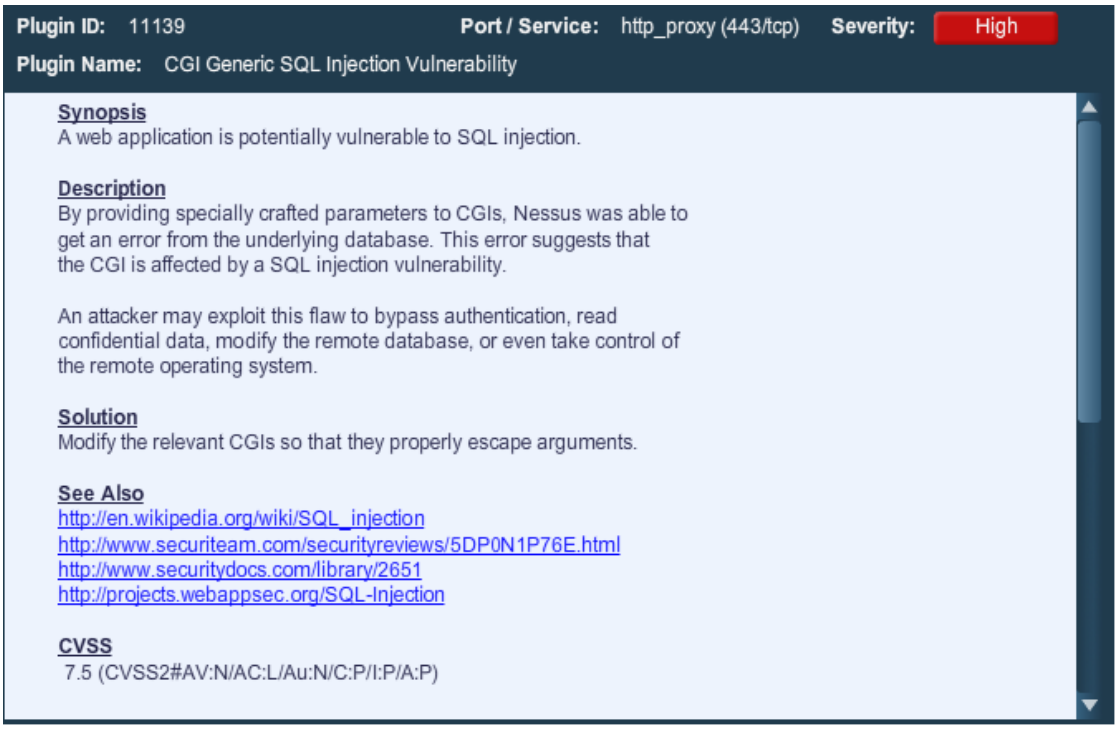
Figura 30. Vulnerabilidades en Portales



Fuente: Autor

b) De los 19 portales analizados sólo 2, es decir, el 10,5% de los portales presentan una vulnerabilidad clasificada como de riesgo alto. Esta vulnerabilidad en particular está relacionada con ataques de Inyección de SQL a través del envío de parámetros alterados a los CGI. Este tipo de ataque permitiría a un atacante circunvenir los controles de autenticación del portal y leer, borrar o modificar datos en la base de datos, incluso, tomar control del sistema de forma remota.

Figura 31. Vulnerabilidades altas en Portales



Fuente: Autor

c) Las vulnerabilidades de riesgo medio, corresponden en su mayoría a una mala selección del grupo de algoritmos de cifrado aceptados por el portal SSL. En muchos casos, los administradores de los portales no son cuidadosos y permiten que el portal negocie durante el establecimiento de la VPN, el uso de algoritmos desactualizados o inseguros.

   Según la firma internacional de consultoría de seguridad Foundstone, en su publicación “The need for stronger ciphers”[29], es posible clasificar el nivel de seguridad de los portales SSL de la siguiente forma:

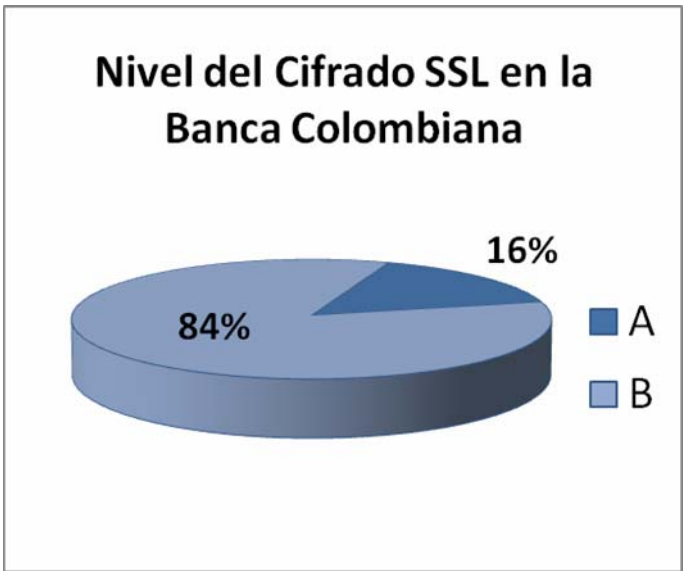
[29] Rudolph Araujo, The need for stronger ciphers, Foundstone Withepapers.

Tabla 7. Calificación de los portales según su nivel de cifrado

Calificación de los portales según su nivel de cifrado	
Sólo soporta algoritmos de máxima seguridad	**A +**
Sólo soporta algoritmos de fuertes o de alta seguridad.	**A**
Soporta al menos un algoritmo débil.	**B**
Sólo soporta algoritmos débiles.	**C**
Soporta al menos un algoritmo inseguro.	**D**
Sólo soporta algoritmos débiles o inseguros	**D -**
Sólo soporta algoritmos inseguros.	**F**

Sólo el 16% de los portales colombianos utilizan sólo algoritmos de cifrado fuerte. El 84% restante, soportan al menos un algoritmo de cifrado débil, este es sin lugar a duda, un error de configuración humano. En general, podría clasificarse como aceptable el nivel de cifrado usado en la banca nacional.

Figura 31. Califiación del nivel de cifrado



Fuente: Autor

4.4. ANÁLISIS CUALITATIVO DE RIESGO

Este análisis hace uso de formas descriptivas para determinar la magnitud de las consecuencias potenciales asociadas a un riesgo y la probabilidad de que éstas ocurran. El valor cualitativo puede ser modificado de acuerdo a las necesidades de la organización y al riego particular evaluado.

Se realiza como una actividad inicial para identificar que riesgos necesitan estudio detallado, cuando el nivel de riesgo no es tal como para invertir tiempo y esfuerzos en un estudio escrupuloso ó cuando no se cuenta con datos numéricos.

Las tablas 8 y 9 son un ejemplo de los indicadores descriptivos que normalmente son empleados:

Tabla 8. Descriptores para consecuencias o impactos

DESCRIPTOR	DETALLE (se hace referencia a consecuencias médicas y financieras)
Bajo	Ningún daño o pérdidas financieras pequeñas. No se afecta la imagen corporativa.
Medio	Pérdidas financieras importantes o afectación a la imagen corporativa a nivel regional.
Alto	Pérdidas financieras considerables, afectación de la imagen corporativa a nivel nacional

Tabla 9. Descriptores cualitativos para probabilidad

DESCRIPTOR	DETALLE (se hace referencia a consecuencias médicas y financieras)
Improbable	Sólo podría ocurrir en situaciones excepcionales
Probable	Ha ocurrido en algunas ocasiones y podría repetirse
Casi cierto	Ha ocurrido en múltiples ocasiones y es casi seguro que volverá a ocurrir.

Nota: como se menciono anteriormente estas tablas pueden modificarse de acuerdo a las necesidades y requerimientos de la organización y la naturaleza de los riesgos, es posible variar el orden, el número o el detalle de cada nivel descriptivo.

La tabla 10 radica su importancia en la determinación exacta del nivel de riesgo, ésta matriz es una relación entre la descripción del impacto y su probabilidad de ocurrencia.

Tabla 10. Matriz nivel de riesgos

PROBABILIDAD	IMPACTO		
	Bajo	**Medio**	**Alto**
Baja	B	B	M
Media	B	M	A
Alta	M	A	A

B = Nivel bajo: Gestionar riesgo mediante rutina

M = Nivel Moderado: Especifica la responsabilidad de la dirección.

A = Nivel Alto: Necesita la atención inmediata de la dirección.

A continuación se presenta la matriz de riesgos para la banca en línea nacional.

Tabla 11. Análisis de riesgo cualitativo para la banca electrónica nacional

Análisis de riesgo cualitativo para la banca nacional			Responabilidad Legal		Activos Informáticos		Financiero		Intangibles Imagen		QoS	
Fuente	Amenaza	P	I	R	I	R	I	R	I	R	I	R
Asociadas a la Información	Perdida de confidencialidad	M	A	A	M	M	A	A	A	A	A	A
	Perdida de integridad	M	A	A	M	M	A	A	A	A	A	A
	Perdida de disponibilidad	M	B	M	M	M	A	A	M	M	A	A
Asociadas al comportamiento humano	Hackers	M	M	M	A	A	A	A	A	A	A	A
	No cumplimiento de políticas por los usuarios	A	B	M	B	M	M	A	B	M	B	M
	Mala higiene informática de los usuarios	A	B	M	A	A	M	A	B	M	B	M
	Administradores - Error de configuración	M	M	M	A	A	A	A	A	A	A	A
Asociadas a la tecnología	Código malicioso	A	B	M	A	A	A	A	M	A	A	A
	Cambio de tecnología	B	B	M	M	B	A	M	B	B	M	B
	Movilidad	B	B	B	B	B	M	B	B	B	A	M
	Vulnerabilidades en el SW	A	B	M	A	A	M	A	A	A	M	A
Asociadas a los procesos	Proceso de autenticación	M	M	M	M	M	A	A	M	M	A	A
	Proceso de atención de incidentes	B	M	M	M	B	A	M	B	B	A	M
	Preceso de cumplimento	A	A	A	M	A	A	A	A	A	A	A

4.5. MITIGACION DEL RIESGO

Gestionar un riesgo, implica priorizar, evaluar, la aplicación de la correspondiente reducción del mismo y realizar controles de evaluación del proceso de riesgo. Dado que la eliminación de todos los riesgos es imposible, es responsabilidad de los altos directivos y gerentes de negocios y funcionarios utilizar el enfoque del menor costo e implementar los controles más adecuados para disminuir el riesgo de la organización a un aceptable nivel, con un mínimo impacto adverso sobre los recursos de la organización.

4.5.1. Opciones de gestión de riesgo

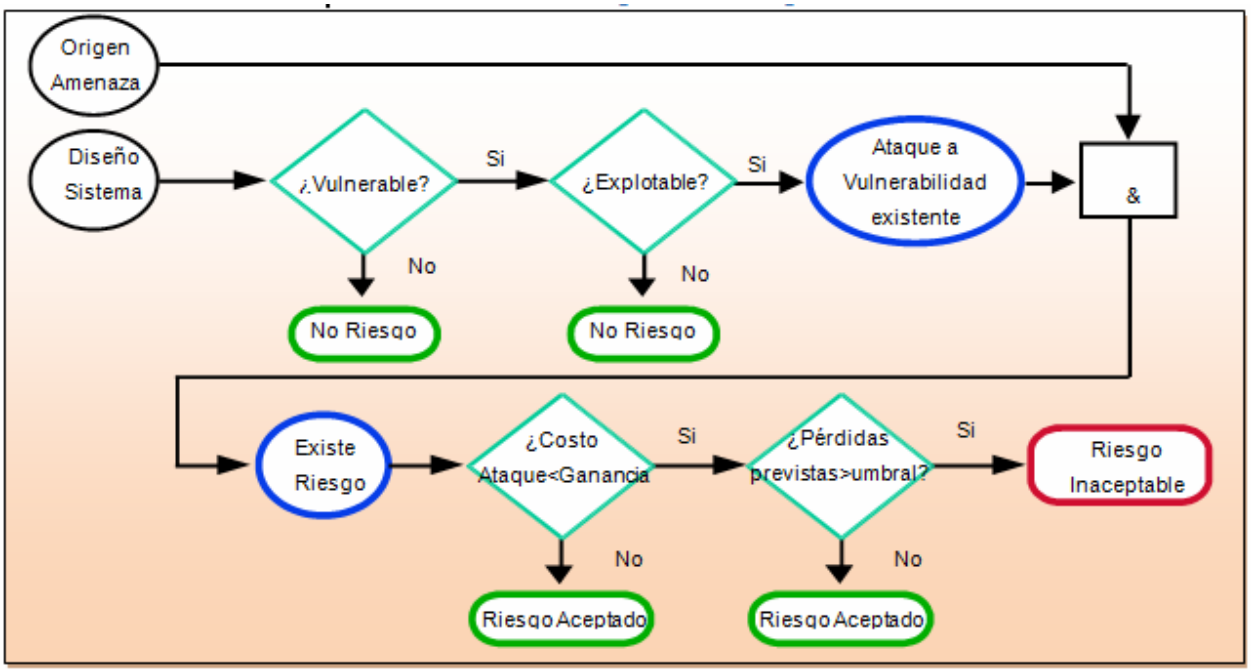
Esta metodología sistemática se utiliza por la alta dirección para reducir el riesgo de la empresa. La mitigación del riesgo puede lograrse a través de cualquiera de las opciones del riesgo siguiente:

- **Asunción del Riesgo:** Aceptar el riesgo potencial y seguir operando el sistema de TI, se debe aplicar controles para reducir el riesgo a un nivel aceptable.
- **Prevención de Riesgos:** Busca evitar el riesgo mediante la eliminación de la causa del riesgo y/o consecuencia (Por ejemplo, renunciar a ciertas funciones del sistema o apagar el sistema cuando los riesgos son identificados).
- **Limitación del riesgo:** Limita el riesgo mediante la implementación de controles que minimizan los efectos adversos de una amenaza al valerse una vulnerabilidad (por ejemplo, el uso de apoyos preventivos y los controles de detección).
- **Riesgo de Planificación:** Gestiona el riesgo mediante el desarrollo de un plan de mitigación de riesgo, además se prioriza, se implementa y se mantiene los controles.

- **Investigación y Reconocimiento:** Se emplea para disminuir el riesgo de la pérdida del reconocimiento de la vulnerabilidad o fallo y apoya la investigación de los controles con el fin de corregir vulnerabilidades.
- **Transferencia de Riesgos:** Se emplea para transferir el riesgo mediante el uso de otras opciones que permiten compensar la pérdida, tales como la compra de seguros.30

Esta estrategia también está articulada en las siguientes reglas de oro, que proporcionan orientación sobre acciones para mitigar los riesgos de las amenazas humanas intencionales:

Figura 32. Estrategia de administración del riesgo



Fuente: Jorge Medina Villalobos

30

Nota: El mejor enfoque consiste en utilizar tecnologías apropiadas de entre los productos de seguridad de varios proveedores, junto con la opción adecuada de mitigación de riesgo o medidas administrativas.

- **Cuando la vulnerabilidad (o defecto, debilidad) existe:** Aplicar técnicas de garantía para reducir la probabilidad de vulnerabilidades**.**
- **Cuando una vulnerabilidad es aprovechada:** Aplicar protecciones a las capas, arquitecturas, a los diseños y los controles administrativos, para reducir al mínimo el riesgo o prevenirlo**.**
- **Cuando el costo del atacante es menor que la ganancia potencial:** Aplicar protecciones a disminuir la motivación de un atacante mediante el aumento de los costos del atacante (por ejemplo, el uso de sistema de controles tales como: Limitar que un usuario del sistema pueda tener acceso y de manera significativa reducir la ganancia de un atacante).
- **Cuando la pérdida es demasiado grande:** Aplicar los principios de diseños arquitectónicos y técnicos y la protección no técnica para limitar el alcance del ataque, de esta manera reducir la posibilidad de pérdida.

4.5.2. APROVECHAMIENTO PARA EL CONTROL DE IMPLEMENTACIÓN

Cuando las acciones se tienen que tomar, la regla aplica lo siguiente:

a) Salida del Paso 1. "Acciones rango de mayor a menor"

Paso 1 priorizar las acciones: En la asignación de recursos, la máxima prioridad debe darse a los riesgos mediante la clasificación de elementos con alto riesgo inaceptable (por ejemplo, el riesgo asignado un Muy Alto o Alto nivel de riesgo). Será necesaria la acción correctiva inmediata para proteger los intereses de una organización.

Paso 2 Evaluar Opciones recomendadas de control: Durante este paso, la viabilidad (por ejemplo, la compatibilidad, la aceptación del usuario) y eficacia (por ejemplo, grado de protección y el nivel de reducción del riesgo) El objetivo es seleccionar la opción de control más apropiado para minimizar los riesgos.

b) Salida del Paso 2 "la lista viable de los controles"

Paso 3. Conducta Análisis Costo-Beneficio: Sirve de ayuda en la toma de decisiones y para identificar los controles rentables.

c) Salida desde el paso 3 “Análisis de costo-beneficio”. (Describe el costo y los beneficios de aplicación o no aplicación de los controles).

Paso 4. Seleccione Control: Sobre la base de los resultados de los análisis de costo-beneficio, la gestión determina la manera más eficaz en el control de costes para reducir el riesgo de la organización. Los controles seleccionados deben combinar la técnica, operativa, de gestión y control y los elementos para garantizar una seguridad adecuada para el sistema de TI y la organización.

Paso 5. Asignación de Responsabilidad: Personas apropiadas (personal interno o al personal de contratación externa) que tienen la debida experiencia y habilidades para aplicar el control seleccionado.

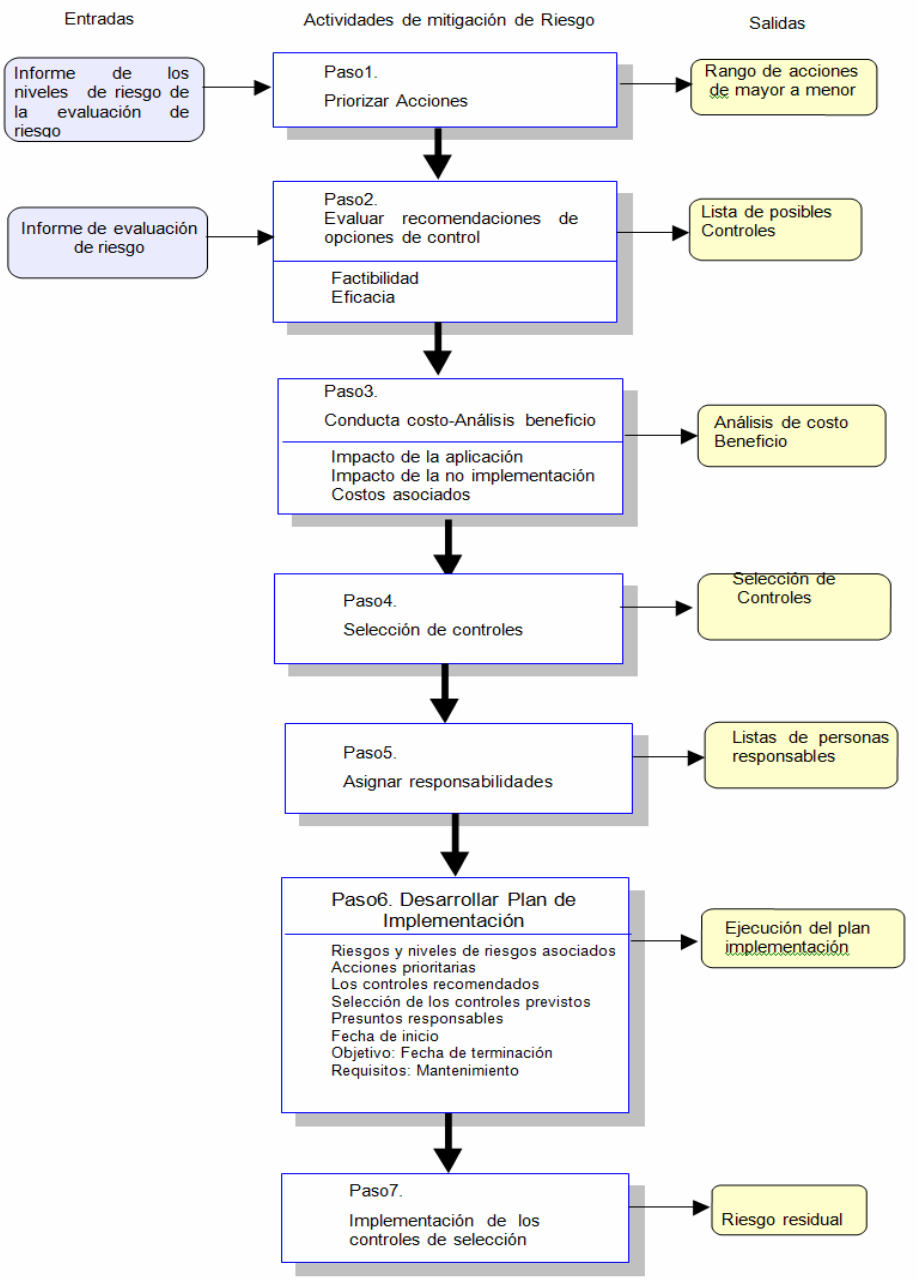
d) La producción de Paso 5. “La lista de las personas responsables”.

Paso 6. Desarrollar un Plan de Implementación de salvaguardia: En este paso se desarrolla una aplicación de salvaguardia (Plan de acción). El plan como mínimo, contendrá la siguiente información:

- Riesgos (vulnerabilidad pares de amenazas) y los niveles de riesgo asociados (salida de riesgo informe de evaluación) - Los controles recomendados (salida de informe evaluación de riesgos).
- Establecimiento de prioridades con las acciones (con prioridad a los temas son muy elevados y de alto riesgo los niveles)
- Selección de los controles programados (determinado sobre la base de la viabilidad, la eficacia, beneficios a la organización, y el costo)
- Recursos necesarios para la aplicación de los controles previstos seleccionados
- Lista de los equipos y el personal responsable
- Fecha de inicio de la ejecución
- Fecha prevista de finalización de la aplicación
- Mantenimiento de los requisitos.

Paso 7. Implementar control seleccionado: Dependiendo de las situaciones individuales, los controles aplicados pueden reducir el nivel de riesgo, pero no eliminarlo.

Figura 32. Estrategia de administración del riesgo



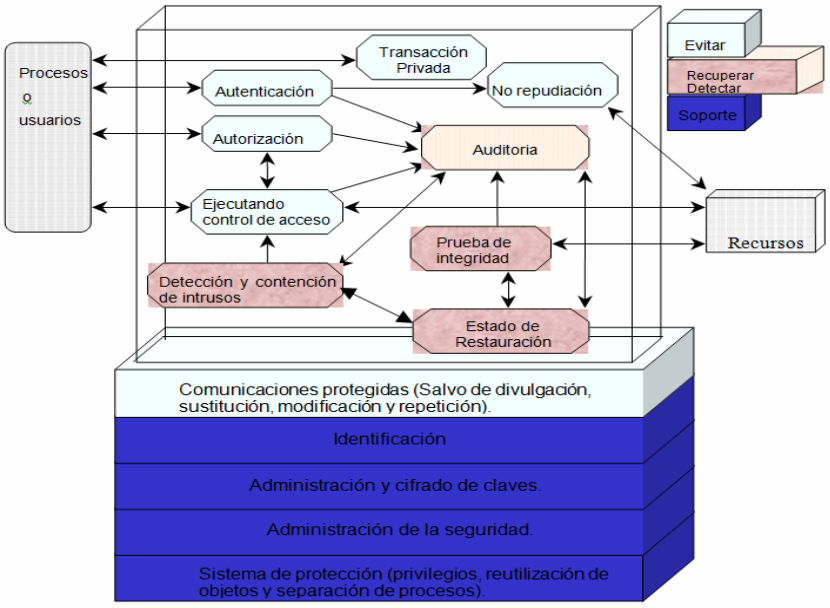
Fuente: Itu Toolkit For Cybercrime Legislation

4.5.3. CATEGORÍAS DE CONTROL

El objetivo del control de la seguridad es reducir las vulnerabilidades a un nivel tolerable y minimizar los efectos de un ataque. Para alcanzar estos objetivos, una organización debe determinar el impacto que puede generar un ataque en la organización y la probabilidad de que esto suceda. Existen varios tipos de control:

- **Control disuasivo:** Reduce la probabilidad de un ataque deliberado**.**
- **Control preventivo:** Protege las vulnerabilidades y procura que los ataques no sean exitosos. Inhibe los intentos de violación a las políticas de seguridad.
- **Control correctivo:** Reduce los efectos de un ataque en la organización.
- **Control por detección:** Descubre ataques y activa controles preventivos o correctivos. Genera advertencias de violaciones o intentos de violaciones a las políticas de seguridad. El control por detección incluye controles como rastros de auditoría, métodos de detección de intrusos y sumas de comprobación.

Figura 33. Controles del riesgo



Fuente: Itu Toolkit For Cybercrime Legislation

Las organizaciones pueden analizar el alcance de la reducción del riesgo generado por los nuevos o mejorados controles en términos de la probabilidad de amenaza de reducción o de impacto, los dos parámetros que definen el nivel de riesgo para la organización.

5. CONCLUSIONES

La seguridad informática es una idea subjetiva [Schneier Bruce, Beyond Fear. Thinking Sensibly about security in an uncertain world. Copernicus Books. 2003], mientras la inseguridad informática es una idea objetiva, es por ello que no es fácil tener control absoluto sobre la seguridad informática, porque lo subjetivo es incierto, esto no ocurre con la inseguridad informática, que sabemos a ciencia cierta, que nos va a ocurrir si continuamos conviviendo irresponsablemente con las vulnerabilidades y los riesgos inherentes de nuestros sistemas informáticos.

El concepto de seguridad lleva asociado otro concepto que le da sentido: “El valor”, solo se debe proteger aquello que creemos tiene un valor importante para nosotros, la seguridad debe estar íntimamente asociada al valor que le damos a los objetos que deseamos proteger. En esencia, la información es uno de los elementos que más nos importa proteger, porque es propio de la organización específica, ya que sin duda alguna constituye uno de los mayores activos de cualquier organización.

El mayor problema de hoy es que los servicios que más utilizamos no tuvieron en cuenta el factor del comportamiento humano. Los expertos encuestados coinciden en afirmar que la gran mayoría de usuarios no tienen una buena higiene informático en sus equipos, lo cual los expone a la gran cantidad de amenazas que se encuentran en la red.

Tal vez el mejor control para proteger la información de los usuarios finales es el uso de tecnologías de redes privadas virtuales sobre protocolo SSL (VPN-SSL) como las que utiliza el sector financiero, no obstante, parece ser que los administradores de los portales no son consientes de ello y no se esmeran en configurar los algotirmos más fuertes para el cifrado de la información. Muestra de ello se ve en los resultados del proceso de auditoría de los portales.

Un plan de gestión de seguridad informática no puede existir sin capacitación especializada para los encargados de esta labor. Entre las certificaciones más apetecidas por el mercado se encuentra la CISSP, Certified Information Systems Security Profesional. Le siguen en preferencia la GIAC, CISA, CISM, SSCP y otras más orientadas a productos específicos que de igual forma empiezan a ser requeridas por los profesionales de redes y seguridad informática.

Los oficiales de seguridad de la información de cada organización, deberá velar por los sistemas de gestión de seguridad de la información, y esto no se reduce a la sóla gestión del riesgo y la definición de las políticas, es necesario empezar a incluir procesos que permitan capacitar a los nuevos e inclusos a los antiguos cuentahabientes acerca de los riesgos del ciberespacio y de la importancia de que sus computadores personales se encuentren siempre actualizados y seguros.

BIBLIOGRAFIA

CALLEGARI, Lida. Delitos informáticos y Legislación. Revista de la Facultad de Derecho y Ciencias Políticas num, 70, p.115. Medellín: Universidad pontificia Bolivariana, 1985.

CASTRO OSPINA, Sandra, Delitos Informático. La información como bien jurídico y Los delitos informáticos en el Nuevo Código Penal. [online], jul 15 de 2002. Disponible en :http//delitosinformaticos.com./delitos/Colombia.shtml.

CHIESA RAOUL, DUCCI STEFANIA Y CIAPPI SILVIO. Profiling Hackers. The Science of Criminal Profiling as Applied to the World of Hacking. Milan, Italy, 2007. URL: http://www.taylorandfrancis.com.

EL CIBERDELITO: GUÍA PARA LOS PAÍSES EN DESARROLLO. División de Aplicaciones TIC y Ciberseguridad. Departamento de Políticas y Estrategias. Sector de Desarrollo de las Telecomunicaciones de la UIT. Proyecto de abril de 2009.

GUERRERO MATEUS, María Fernanda. El fraude Informático en la Banca. Aspectos Criminológicos. S/. s.n. 1995. p.49.

HERRERA HERNANDEZ, Shirley Paola: ANÁLISIS DE RIESGOS PARA APLICACIONES P2P. Bucaramanga: Universidad Industrial de Santander, 2007.

ITU TOOLKIT FOR CYBERCRIME LEGISLATION. Developed through the American Bar Association's Privacy & Computer Crime Committee Section of Science & Technology Law With Global Participation. ITU Telecommunication Development Sector Draft Rev. February 2010.

MEDINA VILLALOBOS, Jorge Alberto "Seguridad en redes de datos" Libro para la Especialización en Telecomunicaciones Universidad Industrial de Santander, Bucaramanga 2009.

RIASCOS GOMEZ, Libardo Orlando. El Habeas Data. Una visión constitucional, legislativa y en proyectos de leyes estatutarias. Texto mecanografiado, publicado virtualmente en forma parcial en: www.informatica-juridica.com y La obtención y comercialización ilegal de datos personales es un delito: Ley 1273 de 2009. Artículo publicado en www.eltiempo.com el 11 de enero de 2009.

SCHJOLBERG, Stein. The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva. December 2008.

TORRES TORRES, Henry William: Derecho Informático. Ediciones Jurídicas Gustavo Ibáñez. 2002.

INDICE

ANEXOS

SEGURIDAD EN TUS TRANSACCIONES ON-LINE

I. PRIMER MODELO ENCUESTA A USUARIOS

1 - Seleccione el rango de tu edad actual:(Obligatorio)

- 12-18
- 19-25
- 26-31
- 32-40
- 41-50
- >50

2 - Cuando va a realizar sus transacciones o pagos en línea prefiere utilizar los servicios:(Obligatorio)

- Cajero Automático
- Tradicional
- Internet

3 - Si usted realiza transacciones bancarias en línea (Internet), ¿Cuál es el mecanismo de acceso que utiliza con más frecuencia?

- (Obligatorio)
- Un Servicio por telefonía fija
- Telefonía móvil (celular)
- Computador

4 - ¿Cuán seguro se siente al realizar operaciones bancarias en línea (En Internet)? (Obligatorio)

- Seguro
- En duda
- Inseguro

5 - ¿Realiza consultas a productos y/o servicios que involucren transacciones de comercio electrónico (compras, remates, home banking)? (Obligatorio)

- Si
- No

6 - ¿Con que frecuencia realiza transacciones de comercio electrónico?

- (Obligatorio)
- Todos los días
- Ocasionalmente
- Nunca

7 - Si nunca realiza transacciones de comercio electrónico, seleccione la acción que considere se adecue a su situación:

- La plataforma resulta difícil de utilizar
- Prefiero el método tradicional
- Desconfía del sistema

8 - ¿Cambia regularmente su contraseña de las tarjetas de crédito y/o debito? (Obligatorio)

- Si
- No

9 - Sabe Ud. Que son troyanos, gusanos, puertas traseras, syware, Phishing, Keyloger? (Obligatorio)

- Si
- No

10 - Te ha llegado a tu email un mensaje de premio? (Obligatorio)

- Si
- No

11 - Cual es el navegador que mas utilizas? (Obligatorio)

- Internet explorer
- Mozilla firefox
- Otro

12 - Utilizas un antivirus de libre licencia? (Obligatorio)

- Si

- No
- No tengo antivirus

13 - ¿Ha sido víctima de un fraude informático (robo, Suplantación de identidad en Internet)? (Obligatorio)

- Si
- No
- Sin conocimiento del tema

14 - ¿Conoce usted un Caso de Fraude informático (robo, suplantación de identidad en internet, falsificación de identidad)? (Obligatorio)

- Si
- No
- Sin conocimiento del tema

15 - ¿Usted cree que las entidades bancarias deban garantizar métodos más seguros en las transacciones bancarias en línea? (Obligatorio)

- Si
- No

16 - Por qué cree o no que las entidades bancarias deban garantizar métodos más seguros en las transacciones bancarias en línea?
(Obligatorio)_____

II. SEGUNDO MODELO ENCUESTA A USUARIOS:

1 - ¿Ha utilizado alguna vez los servicios de Banca en línea?(Obligatorio)

- SI
- No

2 - ¿Qué tipo de acceso suele usar para servicio de Banca en línea utiliza? (Obligatorio)

- Telefonía (fija o móvil)
- Internet
- Internet y telefonía

3 - ¿Considera que el portal de Internet de su Banco es seguro?(Obligatorio)

- SI
- No

4 - ¿Cada cuanto hace uso del portal de su Banco?(Obligatorio)

- Una vez al mes
- Una vez a la semana
- Varias veces por semana

5 - ¿Cuál considera la mayor debilidad de su portal del Banco?(Obligatorio)

- La posibilidad de que su contraseña sea robada
- La falta de comprobantes de transacción
- La dificultad para hacer efectivos los reclamos por transacciones no realizadas

6 - ¿Cada cuanto cambia su contraseña de acceso al portal de su banco?(Obligatorio)

- Nunca la he cambiado, no sabía que debía cambiarla.
- Nunca la cambio porque se me olvida la nueva contraseña
- La cambio cada vez que el sistema me obliga
- La cambio cada tres meses La cambio cada mes

7 - ¿Utiliza algún mecanismo de notificación o alertas (SMS, email) para detectar movimientos en sus cuentas?(Obligatorio)

- Si
- No

8 - ¿Ha sido víctima de algún tipo de fraude electrónico?(Obligatorio)

- Si
- No

9 - ¿Algún familiar o amigo cercano ha sido víctima de un fraude electrónico?(Obligatorio)

- Si
- No

10 - ¿De los casos que conoce de fraudes electrónicos, alguno de ellos se ha resuelto satisfactoriamente a favor de la victima?(Obligatorio)

- Si, todos fueron resueltos de forma eficaz
- Si, todos fueron resueltos pero el proceso fue lento
- Algunos fueron resueltos a favor, otros no
- No, en ningún caso se resolvió a favor de la víctima

11 - ¿Sabe ud. que hacer en caso de ser víctima de fraude electrónico?(Obligatorio)

- No, no sabría qué hacer
- Si, notificar al Banco
- Si, notificar al Banco e interponer una denuncia ante la Unidad de Reacción Inmediata de la DIJIN, para que se inicie una investigación penal.

12 - ¿En que rango de edad se encuentra?(Obligatorio)

- 15 -25
- 26-35
- 36-55 Mayor a 55

13 - ¿Sabe ud. como reconocer el portal de su Banco?(Obligatorio)

- Si, por el logo de mi Banco
- Si, por el logo y la dirección Ejemplo: www.mibanco.com.co
- Si, por el logo, la dirección y el candado del navegador
- Si, por la dirección y el certificado digital del sitio

14 - ¿Desde dónde se conecta a su portal Bancario?\n\n(Obligatorio)

- Desde cualquier lugar cuando tengo una urgencia
- Desde mi casa
- Desde la oficina
- Desde la casa o la oficina.

15 - ¿Ha recibido alguna vez un correo electrónico de su Banco solicitándole que actualice su contraseña?(Obligatorio)

- Si, varias veces, incluso de bancos diferentes al mío
- Si, mi Banco siembre me solicita cambiar la contraseña por correo electrónico
- Si, pero todos eran estafas porque los Bancos nunca solicitan información personal por correo electrónico No, nunca he recibido

III. MODELO ENCUESTA A EXPERTOS:

1. ¿Cuál de las siguientes describe mejor su área de trabajo?

- Ing. de sistemas, telecomunicaciones o áreas afines.
- Ing. Sistemas o áreas afines, trabajando en Seguridad de Informática
- Especialista o Experto en Seguridad de la Información.

2. ¿Usted es usuarios de la Banca en línea?

- Si
- No

3. ¿Cómo accede al servicio de Banca en línea?

- Telefonía
- Internet
- Internet móvil.
- Todas las anteriores.

4. ¿Cada cuanto hace uso del portal?

- Una vez al mes
- Una vez a la semana
- Varias veces por semana

5. ¿Considera que los portales de Banca en línea para usuario final son seguros en Colombia?

- Si, son seguros.
- Si, son seguros pero los usuarios no los saben usar.
- Son medianamente seguros, cumplen con el criterio de costo-beneficio.

- No, los portales son inseguros.
- No sabe.

6. ¿Cuál es el principal problema de la Banca en línea? (NOTA: mirar si es posible que esta pregunta tenga múltiples respuestas)

- El método de autenticación de usuarios es muy débil.
- Los mecanismos de cifrado de los portales son débiles.
- Hace falta observancia y trazabilidad sobre las transacciones.
- Hace falta capacitación (sensibilización) para el usuario final.

7. ¿Ud. o algún familiar o amigo cercano ha sido víctima de un fraude electrónico?

- Si
- No

8. ¿De los casos que conoce de fraudes electrónicos, alguno de ellos se ha resuelto satisfactoriamente a favor de la victima?

- Si, todos fueron resueltos de forma eficaz.
- Si, todos fueron resueltos pero el proceso fue lento.
- Algunos fueron resueltos a favor, otros no.
- No, en ningún caso se resolvió a favor de la víctima.

9. ¿Qué le recomendaría ud. a una víctima de fraude electrónico?

- No sabría qué decirle.
- Notificar inmediatamente al Banco.
- Notificar inmediatamente al Banco e interponer una denuncia ante la Unidad de Reacción Inmediata de la DIJIN, para que se inicie una investigación penal.
- Notificar inmediata mente al Banco, interponer la denuncia en la URI de la DIJIN, e identificar los elementos que puedan constituir evidencia del hurto (extractos bancarios, facturas electrónicas, correos electrónicos, equipos de computo desde hizo o hace transacciones).

10. ¿En qué rango de edad se encuentra?

- 15 – 25 años
- 25 – 35 años
- 45 – 55 años
- Más de 55 años