Niveles de confidencialidad de la información durante su trasmisión en las redes informáticas bancarias.

¿Cuál es el nivel de confidencialidad de la información durante su trasmisión en las redes informáticas bancarias para la reducción del fraude informático?

Eduardo Solís Hernández

Universidad Latinoamericana de Ciencia y Tecnología

2012

Resumen

En nuestra sociedad actual la industria de la informática ha tenido un gran crecimiento y una evolución constante con el descubrimiento de nuevas tecnologías que facilitan los procesos que se realizan cotidianamente en las organizaciones, dentro de estas evoluciones se encuentran los equipos telemáticos y las redes computacionales que brindan una amplia gama de tareas y servicios a realizar.

Con la evolución de las redes computacionales, sus tareas y servicios se han vuelto más complejo el manejo de la información que se trasmite por los diferentes tipos de redes, ya sea en las redes de área local, redes virtuales, redes de áreas metropolitanas e inclusive la misma Internet, es ahí donde surge la inquietud por parte de las organizaciones y de los usuarios de ¿Cual es el nivel de confidencialidad de la información durante su trasmisión en las redes informáticas bancarias?

Esta inquietud es planteada por las diferentes tipos de organizaciones que trasmiten información sensible de sus transacciones bancarias, como el pago de servicios públicos, pagos a proveedores, pagos a acreedores y el pago de la planilla de la organización. Esta inquietud surge de que si la información que es enviada por medio de las redes bancarias es accesada por terceros

puede provocar perdidas económicas a la organización o la información se pudiera utilizar para cualquier tipo de fraude informático trayendo consigo algún tipo de consecuencia legal, por tales razones en todo momento se debe de garantizar la confidencialidad de la información cuando es trasmitida por las redes informáticas bancarias, sin que esta sea accesada y manipulada, garantizando su integridad y confidencialidad.

El Organismo de Investigación Judicial (OIJ) en conjunto con el departamento de Investigaciones de las entidades bancarias, se han planteado la meta de disminuir el fraude informático en perjuicio de dichas entidades, a través de la creación de una cultura institucional en la instrucción del colaborador como del cliente de la entidad bancaria mediante la divulgación de los tipos de fraude informáticos, manera de detectarlos y como realizar una denuncia oportuna.

Con el aumento de los casos de fraude informáticos reportados al Organismo de Investigación Judicial (OIJ) por medio de los clientes y las entidades bancarias, el departamento de tecnología de la información de dichas entidades han aumentado sus niveles de seguridad en el acceso a las cuentas de sus usuarios mediante la creación de dispositivos adicionales (tokens, claves dinámicas) en el momento de ser accesadas y actualización de sus protocolos de seguridad en sus redes informáticas, esto para garantizar que la información no sea accesada por terceros que puedan provocar algún perjuicio al cliente como a la entidad bancaria.

Abstract

In our society today the computer industry has had tremendous growth and constant evolution with the discovery of new technologies that facilitate the processes that take place daily in organizations within these developments are telematics equipment and computer networks that provide a wide range of tasks and services performed.

With the development of computer networks, tasks and services have become more complex handling of the information transmitted by the different types of networks, either in local area networks, virtual networks, metropolitan area networks and even the Internet itself, is where there is concern on the part of organizations and users What is the level of confidentiality of information during its transmission in computer networks banking?

This concern is raised by the different types of organizations that transmit sensitive information of their banking transactions, such as utility payments, payments to suppliers, payments to creditors and payment of the return of the organization. This concern arises that if the information is sent through the banking network is accessed by others can cause economic losses to the organization or the information could be used for any type of computer fraud bringing some kind of legal consequence, for such reasons must at all times ensure the confidentiality of information when it is transmitted through the banking networks, although this is accessed and manipulated, ensuring its integrity and confidentiality.

The Organismo de Investigación Judicial (OIJ) in conjunction with the Research Department of the banks, have set the goal of reducing computer fraud to the detriment of those entities, through the creation of an institutional culture of collaborative instruction as the client of the bank through the dissemination of computer fraud types, how to detect and how to make a timely complaint.

With the increase in computer fraud cases reported to the Organismo de Investigación Judicial (OIJ) by customers and banks, the department of information technology of these entities have increased their levels of security for access to the accounts their users by creating additional devices (tokens, dynamic key) at the time of being accessed and update their security protocols

in computer networks, this to ensure that the information not be accessed by third parties which may cause some harm to client and the bank.

Introducción

Objetivo General

Verificar los niveles de confidencialidad de la información durante su trasmisión en las redes informáticas bancarias.

Objetivos Específicos

- Investigar los diferentes protocolos para la seguridad de la información durante su trasmisión en las redes informáticas bancarias.
- Enunciar los tipos de cifrado de la información durante su trasmisión en las redes informáticas bancarias.
- Mencionar los conceptos de delito y fraude informativo.

Justificación

Con la evolución de las redes computacionales, sus tareas y servicios se han vuelto más complejo el manejo de la información que se trasmite por los diferentes tipos de redes, ya sea en las redes de área local, redes virtuales, redes de áreas metropolitanas e inclusive el mismo internet.

Al volverse más complejo el manejo de la información por el constante crecimiento de las tareas y servicios que necesita la red para poder trasmitir la información de los diferentes organizaciones que envían información sensible como datos del negocio, datos contables, transacciones bancarias, datos personales de clientes y empleados.

Se necesita verificar si el nivel de la confidencialidad que se utiliza es el más adecuado o necesita algún tipo de mejora, esto con la finalidad de que la información no sea accesada por

terceros que puedan provocar pérdidas económicas o la información se utilice para algún tipo de fraude informático.

Por tales razones en todo momento se debe de garantizar la confidencialidad de la información cuando es trasmitida por los diferentes tipos de redes bancarias, sin que esta sea accesada y manipulada, garantizando la integridad, la confidencialidad, generando un alto nivel de confianza por parte de las organizaciones y sus clientes.

Revisión Bibliográfica

Concepción de la seguridad de la información

En la seguridad de la información es importante señalar que su manejo está basado en la tecnología y debemos de saber que puede ser confidencial: la información está centralizada y puede tener un alto valor. Puede ser divulgada, mal utilizada, ser robada, borrada o saboteada. Esto afecta su disponibilidad y la pone en riesgo. La información es poder, y según las posibilidades estratégicas que ofrece tener acceso a cierta información, ésta se clasifica como:

- Crítica: Es indispensable para la operación de la empresa.
- Valiosa: Es un activo de la empresa y muy valioso.
- Sensible: Debe de ser conocida por las personas autorizadas

Existen dos palabras muy importantes que son riesgo y seguridad:

- Riesgo: Es todo tipo de vulnerabilidades, amenazas que pueden ocurrir sin previo aviso y producir numerosas pérdidas para las empresas. Los riesgos más perjudiciales son a las tecnologías de información y comunicaciones.

- Seguridad: Es una forma de protección contra los riesgos. (Wikipedia, Concepción de la seguridad de la información, 2011)

Confidencialidad de la información

Es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados. A groso modo, la confidencialidad es el acceso a la información únicamente por personas que cuenten con la debida autorización. (Wikipedia, Confidencialidad, 2011)

Un ejemplo de confidencialidad de la información seria el acceso a una cuenta de usuario a través de la pagina web de una identidad bancaria, al ser ingresada la identificación y la clave del usuario, el sistema intenta verificar la confidencialidad mediante una consulta de la información ingresada en sus bases de datos y si algún dato de la identificación y/o clave del usuario no coincide con los datos almacenados, se ha producido una violación a la confidencialidad y no tendrá el acceso solicitado a la cuenta de usuario.

Al ser la información considerada de un alto valor, se debe de garantizar que no sea accesada por terceros y que no sea corrompida su confidencialidad, es ahí donde entra en un papel muy importante los protocolos de seguridad, los cuales permiten regular y normar el acceso de la información en las redes informáticas.

Protocolos de seguridad en las redes informáticas

Los protocolos de seguridad son un conjunto de reglas que gobiernan dentro de la transmisión de datos entre la comunicación de dispositivos para ejercer una confidencialidad, integridad, autenticación y el no repudio de la información. Se componen de:

- Criptografía (Cifrado de datos), se ocupa del cifrado de mensajes un mensaje es enviado por el emisor lo que hace es transposicionar u ocultar el mensaje hasta que llega a su destino y puede ser descifrado por el receptor.
- Lógica (Estructura y secuencia). Llevar un orden en el cual se agrupan los datos del mensaje el significado del mensaje y saber cuando se va enviar el mensaje.
- Autenticación. Es una validación de identificación es la técnica mediante la cual un proceso comprueba que el compañero de comunicación es quien se supone que es y no se trata de un impostor. (Wikipedia, Protocolos de Seguridad de la Información, 2011)

Los protocolos de seguridad son fundamentales en las redes informáticas para garantizar la detección de accesos no autorizados y prevenir que se realicen algún tipo de actividad ilícita con la información que pueda traer perdidas a la organización.

Dentro de las redes informáticas se conoce bajo el nombre de protocolo al lenguaje, que es un conjunto de reglas formales, que permiten la comunicación de distintas computadoras entre sí. (tiposde.org, Tipos de protocolos, 2012)

Dentro de las distintas redes existen numerosos tipos de protocolos, entre ellos:

TPC/IP: este es definido como el conjunto de protocolos básicos para la comunicación de redes y es por medio de él que se logra la transmisión de información entre computadoras pertenecientes a una red. Este protocolo es el que provee la base para los servicios más utilizados como por ejemplo transferencia de ficheros, correo electrónico y login remoto. (tiposde.org, TCP/IP, 2012)

TCP (Transmision Control Protocol): este es un protocolo orientado a las comunicaciones y ofrece una transmisión de datos confiable. (tiposde.org, TCP, 2012)

HTTP (Hypertext Transfer Protocol): este protocolo permite la recuperación de información y realizar búsquedas indexadas que permiten saltos intertextuales de manera eficiente. (tiposde.org, HTTP, 2012)

FTP (File Transfer Protocol): este es utilizado a la hora de realizar transferencias remotas de archivos. Lo que permite es enviar archivos digitales de un lugar local a otro que sea remoto o al revés. Generalmente, el lugar local es la PC mientras que el remoto el servidor. (tiposde.org, FTP, 2012)

SSH (Secure Shell): este fue desarrollado con el fin de mejorar la seguridad en las comunicaciones de internet. Para lograr esto el SSH elimina el envío de aquellas contraseñas que no son cifradas y codificando toda la información transferida. (tiposde.org, SSH, 2012)

SMTP (Simple Mail Transfer Protocol): este protocolo está compuesto por una serie de reglas que rige la transferencia y el formato de datos en los envíos de correos electrónicos. SMTP suele ser muy utilizado por clientes locales de correo que necesiten recibir mensajes de e-mail almacenados en un servidor cuya ubicación sea remota. (tiposde.org, SMTP, 2012)

ARP (Address Resolution Protocol): por medio de este protocolo se logran aquellas tareas que buscan asociar a un dispositivo IP, el cual está identificado con una dirección IP, con un dispositivo de red, que cuenta con una dirección de red física. ARP es muy usado para los dispositivos de redes locales Ethernet. Por otro lado, existe el protocolo RARP y este cumple la función opuesta a la recién mencionada. (tiposde.org, ARP, 2012)

Cifrado de datos

El cifrado se puede entender como el hecho de guardar algo valioso dentro de una caja fuerte cerrada con llave. Los datos confidenciales se cifran con un algoritmo de cifrado y una clave que los hace ilegibles si no se conoce dicha clave. Las claves de cifrado de datos se determinan en el momento de realizar la conexión entre los equipos. El uso del cifrado de datos puede iniciarse en su equipo o en el servidor al que se conecta. (Microsoft, Cifrado de datos, 2012)

Las conexiones de red admite dos tipos de cifrado:

- Microsoft MPPE: Cifra los datos de las conexiones de acceso telefónico basadas en el Protocolo punto a punto (PPP) o de las conexiones de red privada virtual (VPN) basadas en el Protocolo de túnel punto a punto (PPTP). Se aceptan los esquemas de cifrado MPPE de clave de 128 bits (alto nivel), de clave de 56 bits y de clave de 40 bits (estándar). MPPE proporciona seguridad de datos para la conexión PPTP entre el cliente VPN y el servidor VPN. (Microsoft, Cifrado punto a punto de Microsoft(MPPE), 2012)
- Seguridad de Protocolo de Internet (IPSec): Representa la tendencia a largo plazo hacia las redes seguras, es un conjunto de servicios de protección y protocolos de seguridad basados en criptografía. Como no requiere cambios en las aplicaciones o en los protocolos, IPSec se puede instalar fácilmente en las redes existentes. (Microsoft, Cifrado de seguridad del protocolo de Internet (IPSec), 2012)

MPPE e IPSec aceptan varios niveles de cifrado, como se muestra en la tabla No.1.

Tabla No.1

Tipo de cifrado	Nivel de cifrado admitido
Estándar MPPE	de 40 bits y de 56 bits
MPPE reforzado	de 128 bits
IPSec DES	de 56 bits
IPSec Triple DES	3DES

Fuente: Microsoft, Cifrado de datos, 2012

Delito informático

El delito informático, o crimen electrónico, o bien ilícito digital es el término genérico para aquellas operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar computadoras, medios electrónicos y redes de Internet. Sin embargo, las categorías que definen un delito informático son aún mayores y complejas y pueden incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados. Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados. (Wikipedia, Delito informático, 2012)

Fraude Informático

El fraude informático es inducir a otro a hacer o a restringirse en hacer alguna cosa de lo cual el criminal obtendrá un beneficio por lo siguiente:

1. Alterar el ingreso de datos de manera ilegal. Esto requiere que el criminal posea un alto nivel de técnica y por lo mismo es común en empleados de una empresa que conocen bien las redes de información de la misma y pueden ingresar a ella para alterar datos como generar información falsa que los beneficie, crear instrucciones y procesos no autorizados o dañar los sistemas.
2. Alterar, destruir, suprimir o robar datos, un evento que puede ser difícil de detectar.
3. Alterar o borrar archivos.
4. Alterar o dar un mal uso a sistemas o software, alterar o reescribir códigos con propósitos fraudulentos. Estos eventos requieren de un alto nivel de conocimiento.

Otras formas de fraude informático incluye la utilización de sistemas de computadoras para robar bancos, realizar extorsiones o robar información clasificada. (Wikipedia, Fraude, 2012)

Fraude Informático en Costa Rica

En Costa Rica el Código Penal indica en su Articulo 217.bis que "Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema." (Codigo Penal, 2012)

Por lo cual existe una regulación que impone penas de cárcel a las personas y/u organizaciones que se dediquen a realizar este tipo de labor ilícita.

Metodología

Para conocer cuál es la percepción de los profesionales en informática de Costa Rica que laboran en el área bancaria, tienen acerca del nivel de confidencialidad de la información durante su transmisión en las redes informáticas bancarias, incluyendo su conocimiento sobre los diferente tipos de protocolos de seguridad en las redes informáticas, los tipos de cifrado de los datos en las redes informáticas, su conocimiento sobre la definición de fraude informático y las sanciones que se establecen en el Código Penal sobre este tipo de delito; se realizará un estudio cuantitativo.

El alcance de este trabajo de investigación se considera como correlacional, dado que se analizarán la percepción de los profesionales de informática sobre 2 conceptos específicos los cuales son el nivel de confidencialidad y la reducción del fraude informático.

Este estudio recolectará y analizará los datos para responder la pregunta de investigación establecida. Para ello se creo una encuesta dirigida a este grupo de estudio. Se diseñará un cuestionario y se publicará en la herramienta Google Docs, la cual es un instrumento utilizado para la recolección de datos, los cuales serán analizados y tabulados. Con este proceso se obtendrán los hallazgos requeridos para la realización de esta investigación, de manera que servirán para dar respuesta precisa al objeto de estudio.

La muestra que se utilizará es de tipo no probabilística por el motivo que se seleccionará una cantidad de 50 profesionales en informática de los 6665 inscritos en el Colegio de Profesionales en Informática y Computación de Costa Rica (CPIC, 2012), por ser profesionales en el área tienen un conocimiento sobre el tema del estudio.

La encuesta se enviará por correo electrónico a 50 profesionales en informática en diferentes áreas del Banco de Costa Rica: Redes, Soporte Técnico, Soporte al Cliente Interno, Seguridad de la Infraestructura de la Red, Desarrollo de Aplicaciones, Soporte de Bases de Datos, Administradores de Sistemas y Telecomunicaciones.

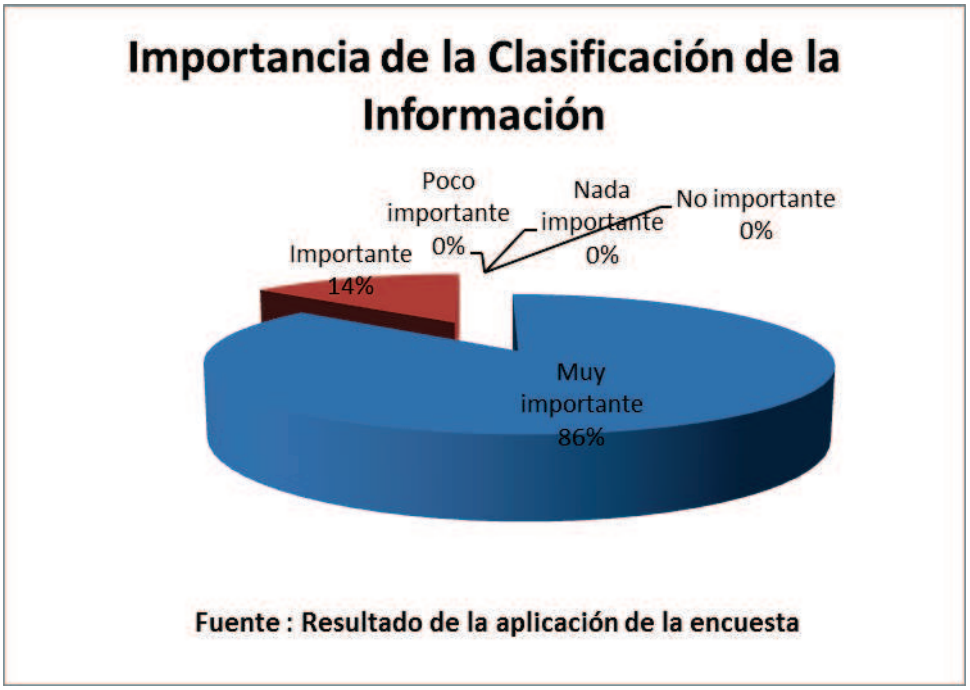
Se estudiarán los datos obtenidos por medio de la herramienta Google Docs y Microsoft Excel 2010 de Microsoft y se procederá con la divulgación de los resultados a obtener, elaboración de la discusión y como punto final se realizarán las conclusiones y recomendaciones.

Resultados

La encuesta sobre los niveles de confidencialidad de la información durante su trasmisión en las redes informáticas bancarias se realizo a 50 profesionales en informática en diferentes áreas del Banco de Costa Rica por medio de la herramienta Google Docs a partir del 11 de noviembre y culmino el 19 de noviembre del 2012. En el proceso de análisis y tabulado de la información recolectada se obtuvo que de los 50 encuestados un 80% corresponde a hombres y un 20% a mujeres, mientras que en el rango de edad, el 68% tiene entre 20 y 30 años, el 28% comprende los 31 y 40 años, mientras un 4% comprende los 41 a los 50 años.

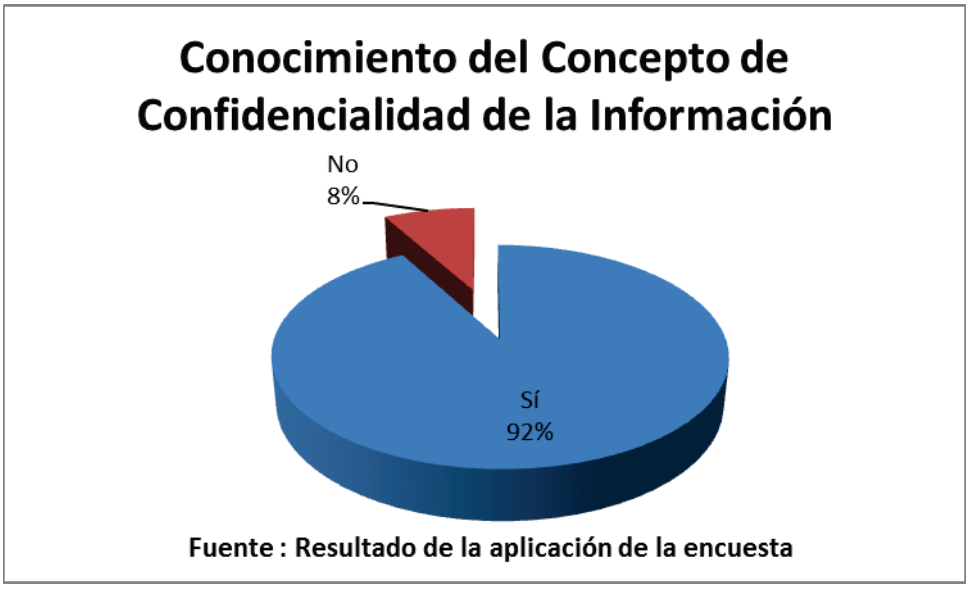
Así mismo un 86% considera Muy Importante la clasificación de la información como critica, valiosa y sensible, mientras un 14% la consideran como importante, cabes destacar que ninguno de los encuestados utilizó las opciones poco importante, nada importante y no importante según lo muestra el gráfico No.1.

Gráfico No.1



Con respecto al conocimiento que deben de poseer los profesionales en informática del concepto de confidencialidad de la información un 92% si conoce el concepto y solo un 8% no conoce el concepto, como lo muestra el gráfico No.2.

Gráfico No.2



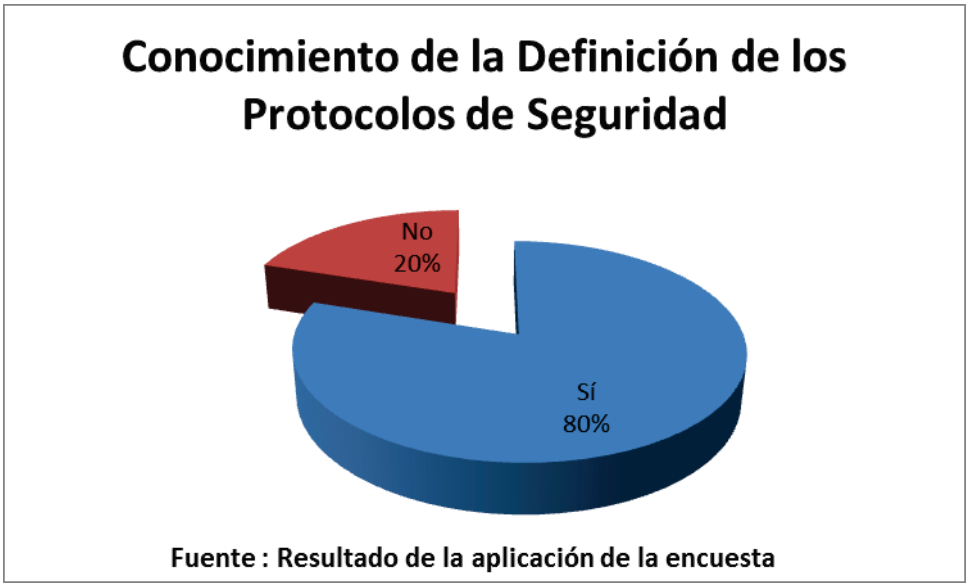
Como se muestra en el gráfico No.3, el 100% de los encuestados si consideraron que los protocolos de seguridad son importantes para la confidencialidad de la información en las redes informáticas bancarias.

Gráfico No.3

Fuente : Resultado de la aplicación de la encuesta

Referente a la definición de protocolos de seguridad, un 80% de los encuestados indico que si conocen el concepto, mientras un 20% indico que no tenían conocimiento del concepto de protocolos de seguridad, como se muestra en el gráfico No.4.

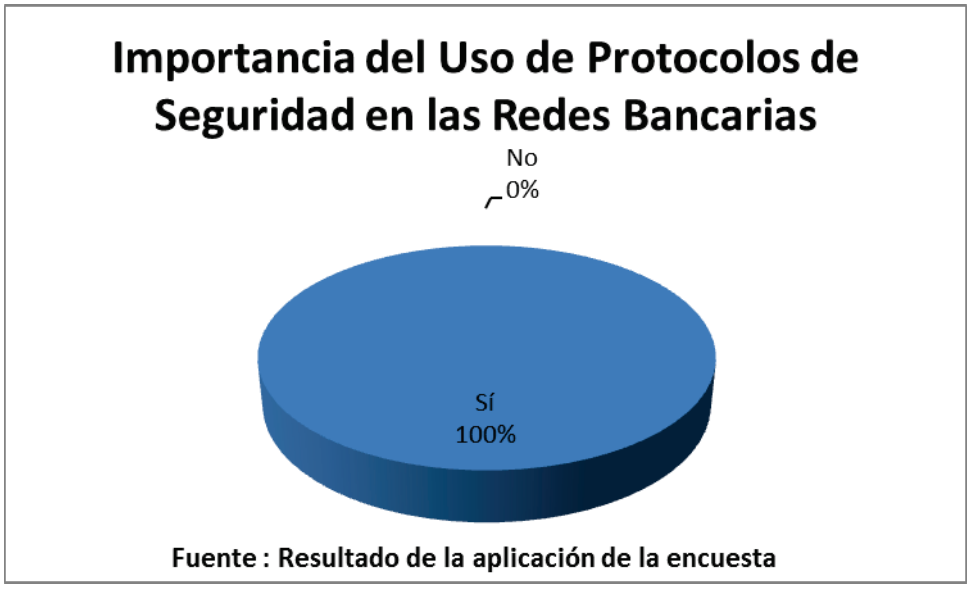
Gráfico No.4



Fuente : Resultado de la aplicación de la encuesta

Como se puede observar en el gráfico No.5 el 100% de los encuestados consideraron que si es importante el uso de protocolos de seguridad en las redes bancarias.

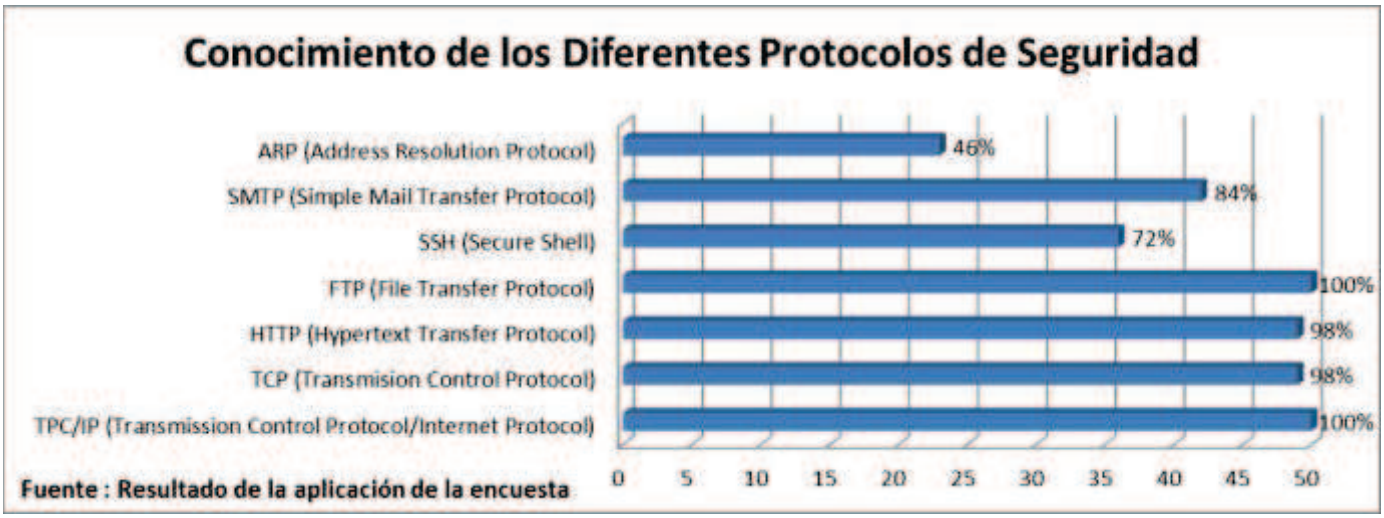
Gráfico No.5



Fuente : Resultado de la aplicación de la encuesta

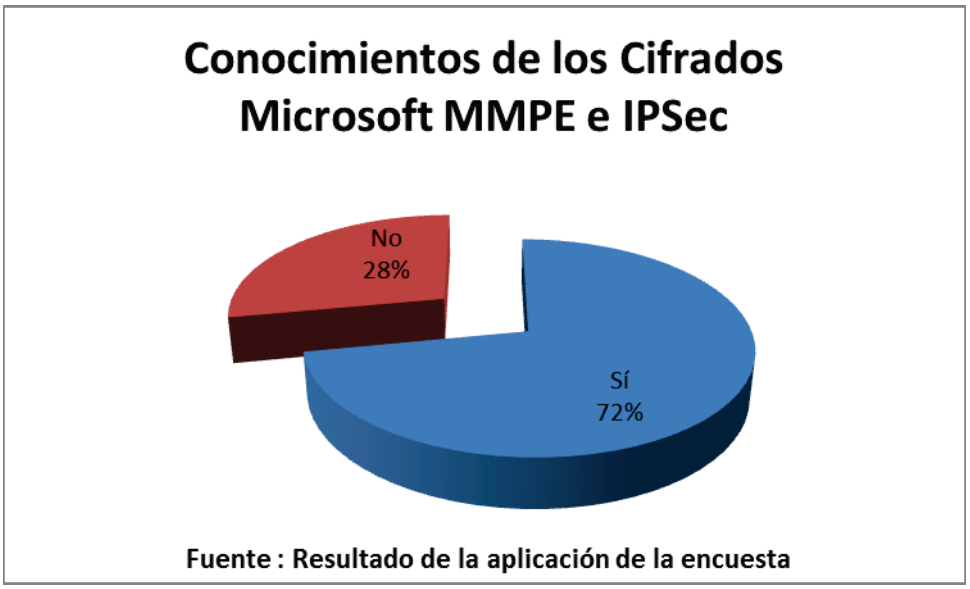
El gráfico No.6 muestra el conocimiento de los encuestados referente a los diferentes protocolos de seguridad, siendo los protocolos TCP/IP y FTP los más conocidos con un 100% y el protocolo ARP es el menos conocido con un 46%.

Gráfico No.6



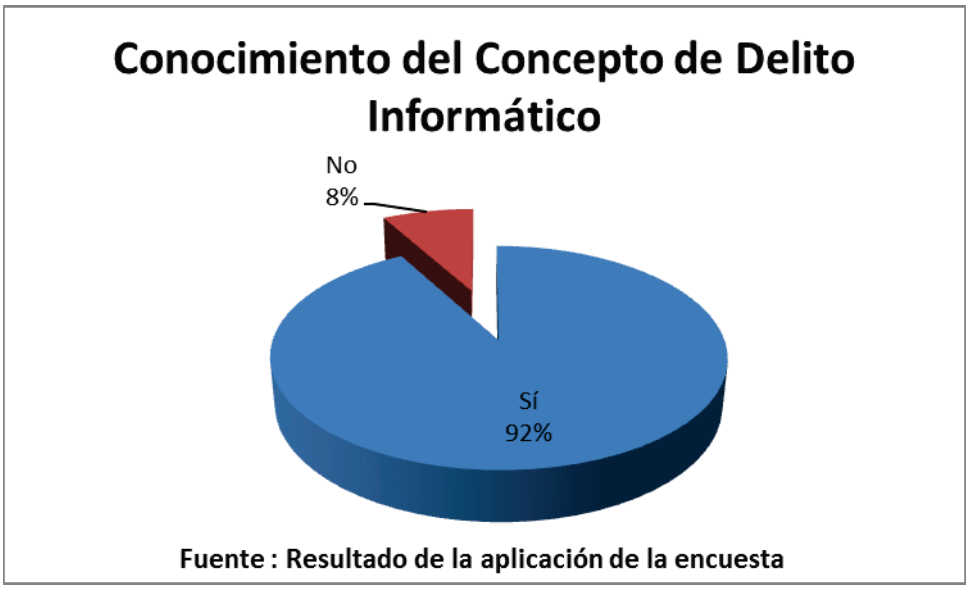
Como nos muestra el gráfico No.7 referente a los conocimientos de los cifrados Microsoft MMPE e IPSec que se utilizan en las redes informáticas, un 72% de los encuestados si conocen alguno o los 2 tipos de cifrados, mientras un 28% no tenía ningún conocimiento.

Gráfico No.7



Referente al conocimiento del concepto de delito informático un 92% si conoce el concepto y un 8% no conoce el concepto de delito informático, como lo ilustra el gráfico No.8.

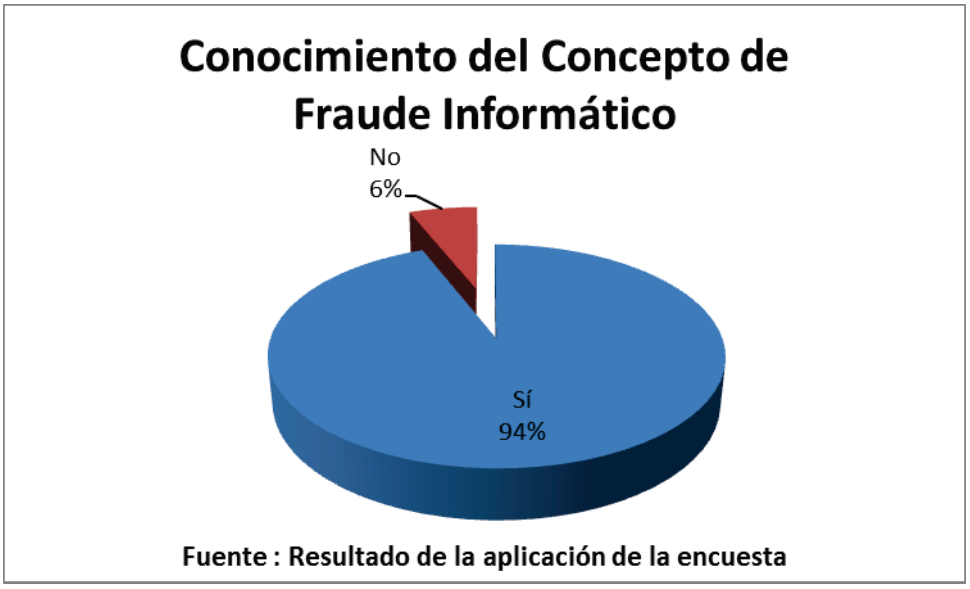
Gráfico No.8



Fuente : Resultado de la aplicación de la encuesta

Como se observa en el gráfico No.9 un 94% de los encuestados si conoce el concepto de delito informático y solo un 6% no conoce el concepto.

Gráfico No.9.



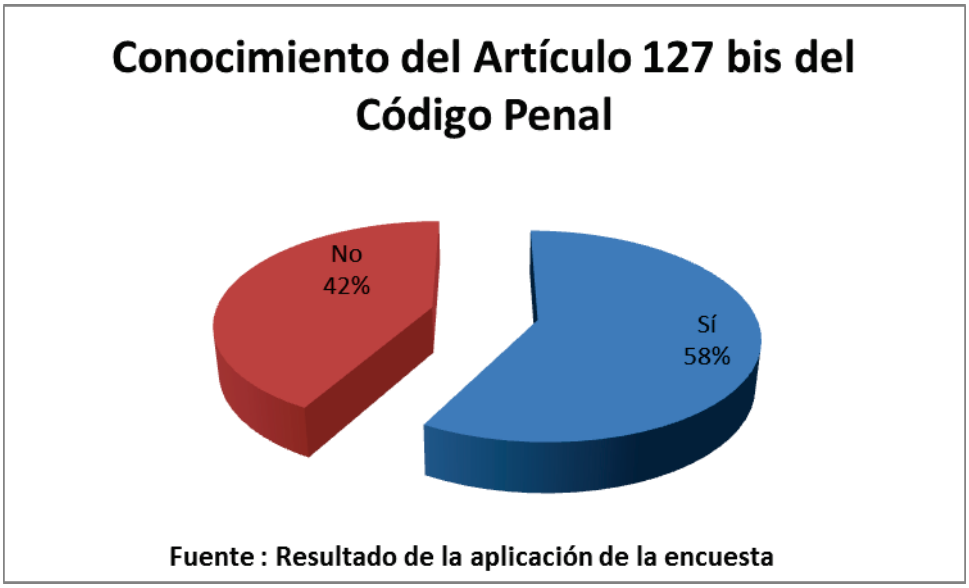
Fuente : Resultado de la aplicación de la encuesta

El gráfico No.10 muestra que en el tema de las medidas de seguridad y dispositivos adicionales utilizados por las entidades bancarias para prevenir el fraude informático, un 66% consideran que si son los más adecuados y un 34% indican que no son los más indiciados.

Gráfico No.10

En relación con el conocimiento del artículo 127 bis del Código Penal de Costa Rica donde se impone una pena de prisión de uno a diez años a la persona que cometa fraude informático, un 58% sí conocía el artículo y un 42% no sabía sobre el tema, como se referencia en el Gráfico No.11.

Gráfico No.11



Fuente : Resultado de la aplicación de la encuesta

Discusión

Los datos que se presentaron en la revisión bibliográfica fueron investigados y recopilados de documentación en el área de las redes informáticas, tomando en cuenta criterios de profesionales en informática relacionados en el área de las redes bancarias, incluyendo los conceptos de confidencialidad de la información, seguridad en las redes, protocolos de seguridad de la información, protocolos de encriptación de la información, así mismo se investigaron los conceptos tanto de delito como de fraude informático y su aplicación en la legislación costarricense.

Luego de haber recopilado, analizado y tabulado la información obtenida a través de las encuestadas realizadas a los profesionales en informática en diferentes áreas del departamento de tecnología del Banco de Costa Rica se establece que un 86% considera Muy Importante la clasificación de la información como critica, valiosa y sensible, mientras un 14% la consideran como importante, estos resultados demuestran que los encuestados tienen un buen conocimiento de la clasificación anteriormente mencionada de la información.

De los encuestados el 92% de los profesionales en informática afirman que si tienen un conocimiento del concepto de confidencialidad de la información, mientras solo un 8% indicó no conocer el concepto, demostrando que la mayoría de los profesiones si tienen un amplio conocimiento del concepto de confidencialidad de la información.

Con respecto al tema de los protocolos de seguridad de la información, el 100% de los encuestados indicaron que los protocolos de seguridad son de suma importancia para regular y normar el acceso a la información en las redes informáticas bancarias y así garantizar que no sea accesada por terceros y que no sea corrompida su confidencialidad. El 80% de los profesionales en informáticas encuestados indico tener conocimiento del concepto de protocolos de seguridad y un 20% indico desconocer el concepto, así mismo el 100% de los encuestados indico que es de suma importancia el uso de los protocolos de seguridad en las redes informáticas bancarias, dando esto un resultado positivo referente al tema de los protocolos de seguridad y su importancia en la aplicación en las redes informáticas bancarias para garantizar la confidencialidad de la información.

Continuando con el tema de los protocolos de seguridad, los cuales son de suma importancia en las redes informáticas bancarias, como se ha demostrado durante el análisis y discusión de los resultados de este tema. Existen diferentes tipos de protocolos de seguridad que se aplican en los tramos de las redes informáticos se consulto a los profesionales en informática el conocimiento de los más importantes dando esta consulta como resultado que los protocolos que más conocen los encuestados son el TCP/IP (Transmission Control Protocol/Internet Protocol) con 100% de conocimiento, el TCP (Transmision Control Protocol) y el HTTP (Hypertext Transfer Protocol) ambos respectivamente con un 98% de conocimiento, mientras que el protocolo menos conocido por parte de los profesionales en informática es el ARP (Address Resolution Protocol) con solo

un 46% de respuestas afirmativas sobre su conocimiento. Estos resultados obtenidos reflejan que los profesionales en informática consultados tienen un amplio conocimiento de los protocolos de seguridad que se utilizan en las redes informáticas bancarias y su aplicación en la confidencialidad de la información.

Otro tema que se consulto a los profesionales en informática fue el conocimiento de los tipos de cifrados que se utilizan en las redes informáticas obteniéndose como resultado que el 92% si conoce alguno o los 2 tipos de cifrados y un 28% no tenía conocimiento de los cifrados Microsoft MMPE e IPSec que son los que se implementan en el cifrado de la información en las redes informáticas bancarias.

Referente al tema de las medidas de seguridad y dispositivos adicionales como claves dinámicas, tokens, códigos de usuario, generación automática y aleatorias de contraseñas desechables para el acceso a las cuentas que utilizan las entidades bancarias tanto en la banca estatal como la banca privada son las más adecuadas para garantizar la confidencialidad de la información, el 66% de los profesionales en informática encuestados afirmo que si les parecen las más adecuadas y un 34% respondió que no.

Uno de los puntos abarcados durante el proceso de investigación fue la reducción del fraude informático, por lo cual se investigó sobre los temas de delito informático, fraude informático, el panorama costarricense referente al fraude informático y que sanciones impone la legislación de la República de Costa Rica mediante el código penal. A lo cual a los profesionales en informáticas se les consultó sobre este tema obteniendo como resultado que un 92% de los profesionales en informático afirmo conocer el concepto de delito informático y solo un 8% indico desconocer del tema, así mismo se les consultó a los profesionales en informática el

conocimiento sobre el concepto de fraude informático, obteniéndose como resultados que el 94% de los encuestados conocen el concepto y un 6% desconoce del tema.

Continuando con el tema del fraude informático se investigo si la legislación costarricense impone algún tipo de sanción y se encontró que en el código penal indica que el código penal en su Articulo 217bis, impone una pena de prisión de uno a diez años a la persona que cometa fraude informático, por tal sanción se consulto a los encuestados si conocían dicha sanción, obteniéndose como resultado un 58% si conocía el artículo y un 42% no sabia sobre la sanción.

Demostrando con estos resultados que la mayoría de los profesionales en informática consultados conocen los conceptos de delito y fraude informático, como sus repercusiones al cometerlos y a las sanciones que pueden estar expuestos.

Conclusiones y Recomendaciones

Con base en la investigación realizada y los datos recopilados, sobre confidencialidad de la información, protocolos de seguridad, tipos de encriptación de la información, delito y fraude informático, sanciones de la legislación referente al fraude informático, se concluye que los profesionales en informática, tienen un amplio conocimiento sobre los temas anteriormente descritos y se le da respuesta a la pregunta de investigación de ¿Cuál es el nivel de confidencialidad de la información durante su trasmisión en las redes informáticas bancarias para la reducción del fraude informático?, obteniéndose a través de los procesos de análisis y discusión de resultados que el nivel de seguridad es el optimo para garantizar la confidencialidad de la información y disminuir el fraude informático.

Se concluye que el resultado positivo a la pregunta en que se baso el trabajo de investigación, se dio por el conocimiento de los profesionales en informática referente a los temas de protocolos, encriptación de datos, delito y fraude informático, así mismo las entidades bancarias han utilizado los protocolos de seguridad y algoritmos de encriptación de los datos más adecuados para garantiza la confidencialidad de la información. Adicionalmente el fraude informático en las entidades bancarias no ha traído muchas repercusiones dado que las entidades bancarias están preparadas para impedir el fraude, con la aplicación de herramientas tecnológicas, aunque si es cierto que el fraude informático no se ha eliminado un 100%, pero si ha disminuido de una manera considerable, por el tiempo y esfuerzo que se le dedica a este tema tan importante en las entidades bancarias.

Aunque la mayoría de los profesionales en informática encuestados afirmaron que las medidas de seguridad y dispositivos adicionales para el acceso a las cuentas que utilizan las entidades bancarias son las más adecuadas para garantizar la confidencialidad de la información, son las más aptas, hay un porcentaje de los encuestados que no están de acuerdo con las medidas tomadas por la entidades bancarias y que las mismas deben de aumentar e irlas variando con el tiempo por el motivo que consideran que las personas dedicadas a este tipo de fraude han estado violando las medidas de seguridad actualmente utilizadas.

De acuerdo con los resultados obtenidos durante la investigación, los procesos de análisis y discusión de los resultados obtenidos al aplicar el instrumento de investigación se recomienda a las entidades bancarias, actualizar a sus profesionales en informática constantemente en temas de protocolos de seguridad y encriptación de datos, dado que las redes se encuentran en una evolución constante como las tecnologías que las conforman y así garantizar la integridad y confidencialidad de la información.

Así mismo las entidades bancarias deben de mantener una mayor comunicación con los clientes internos y externos referente a las medidas de seguridad que tienen a su disposición, como deben de utilizarlas y cuales son los diferentes tipos de fraude informático, la manera de detectarlos para no caer en el fraude y como deben de referirse a las autoridades correspondientes para denunciar si fueron victimas del fraude, dado que los cliente actualmente no estas muy informados sobre a quien deben de interponer las respectivas denuncias.

Bibliografía

Código Penal, C. R. (24 de octubre de 2012). *Organización de los Estados Americanos*. Obtenido de Organización de los Estados Americanos: http://www.oas.org/juridico/mla/sp/cri/sp_cri-int-text-cpenal.pdf

CPIC. (26 de octubre de 2012). *Lista Colegiados Activos al día.* Obtenido de CPIC: http://www.cpic.or.cr/web/index.php?option=com_phocadownload&view=category&id=8:estatus-del-colegiado&Itemid=18#

Microsoft. (23 de octubre de 2012). *Cifrado de datos*. Obtenido de technet.microsoft.com: http://technet.microsoft.com/es-es/library/cc785633(v=ws.10).aspx

Microsoft. (23 de octubre de 2012). *Cifrado de seguridad del protocolo de Internet (IPSec)*. Obtenido de technet.microsoft.com: http://technet.microsoft.com/es-es/library/cc757613(v=ws.10).aspx

Microsoft. (23 de octubre de 2012). *Cifrado punto a punto de Microsoft(MPPE)*. Obtenido de technet.microsoft.com: http://technet.microsoft.com/es-es/library/cc757532(v=ws.10).aspx

tiposde.org. (22 de octubre de 2012). *ARP*. Obtenido de tiposde.org: http://www.tiposde.org/informatica/513-tipos-de-protocolos/

tiposde.org. (22 de octubre de 2012). *FTP*. Obtenido de tiposde.org: http://www.tiposde.org/informatica/513-tipos-de-protocolos/

tiposde.org. (22 de octubre de 2012). *HTTP*. Obtenido de tiposde.org: http://www.tiposde.org/informatica/513-tipos-de-protocolos/

tiposde.org. (22 de octubre de 2012). *SMTP*. Obtenido de tiposde.org: http://www.tiposde.org/informatica/513-tipos-de-protocolos/

tiposde.org. (22 de octubre de 2012). *SSH*. Obtenido de tiposde.org: http://www.tiposde.org/informatica/513-tipos-de-protocolos/

tiposde.org. (22 de octubre de 2012). *TCP*. Obtenido de tiposde.org: http://www.tiposde.org/informatica/513-tipos-de-protocolos/

tiposde.org. (22 de octubre de 2012). *TCP/IP*. Obtenido de tiposde.org: http://www.tiposde.org/informatica/513-tipos-de-protocolos/

tiposde.org. (22 de octubre de 2012). *Tipos de protocolos*. Obtenido de tiposde.org: http://www.tiposde.org/informatica/513-tipos-de-protocolos/

Wikipedia. (22 de julio de 2011). *Concepción de la seguridad de la información*. Obtenido de Wikipedia: http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n#Concepci.C3.B3n_de_la_seguridad_de_la_informaci.C3.B3n

Wikipedia. (22 de julio de 2011). *Confidencialidad*. Obtenido de Wikipedia: http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n#Confidencialidad

Wikipedia. (22 de julio de 2011). *Protocolos de Seguridad de la Información*. Obtenido de Wikipedia: http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n#Protocolos_de_Seguridad_de_la_Informaci.C3.B3n

Wikipedia. (24 de octubre de 2012). *Delito informático*. Obtenido de Wikipedia: http://es.wikipedia.org/wiki/Delito_inform%C3%A1tico#Fraude

Wikipedia. (24 de octubre de 2012). *Fraude*. Obtenido de Wikipedia: http://es.wikipedia.org/wiki/Delito_inform%C3%A1tico#Fraude

Anexos

Cuestionario

Niveles de confidencialidad de la información durante su trasmisión en las redes informáticas bancarias.

El presente formulario forma parte de un trabajo de investigación del estudiante Eduardo Solís Hernández que lleva como título: Niveles de confidencialidad de la información durante su trasmisión en las redes informáticas bancarias. Estas preguntas están orientadas a profesionales en informática, tienen como objetivo conocer las opiniones relacionadas sobre los niveles de confidencialidad de la información. Las respuestas son estrictamente confidenciales, no se le solicita en ninguna de las preguntas indicar su nombre ni la empresa para la cual labora, ni ningún otro dato personal. Los resultados serán contabilizados y expresados en gráficos estadísticos. Este cuestionario responde al trabajo final necesario para aprobar el seminario de graduación de la Licenciatura en Ingeniería Informática con énfasis en Redes y Sistemas Telemáticos de la Universidad Latinoamericana de Ciencia y Tecnología (ULACIT). Completar este cuestionario no debería tomar un tiempo mayor a 10 minutos. Se le agradece su gentileza en completar la totalidad del cuestionario.

1. La información es poder y según las posibilidades estratégicas que ofrece tener acceso a cierta información, esta se clasifica como Crítica, Valiosa y Sensible. ¿Según el texto anterior en que grado de importancia encuentra la clasificación de la información mencionada?
    a) Muy importante
    b) Importante
    c) Poco importante

d) Nada importante

e) No importante

2. La confidencialidad de la información se entiende como la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados y dar acceso únicamente a personas que cuenten con la debida autorización. ¿Conocía la definición anteriormente descrita de confidencialidad de la información?

    a) Sí

    b) No

3. La información se considera de un alto valor por lo cual se debe de garantizar que no sea accesada por terceros y que no sea corrompida su confidencialidad, por lo cual se considera de suma importancia los protocolos de seguridad, para regular y normar el acceso a la información en las redes informáticas. ¿Según la afirmación anterior considera que los protocolos de seguridad son importantes para la confidencialidad de la información?

    a) Sí

    b) No

4. Los protocolos de seguridad son un conjunto de reglas que gobiernan dentro de la transmisión de datos entre la comunicación de dispositivos para ejercer una confidencialidad, integridad, autenticación y el no repudio de la información. ¿Conocía la definición anteriormente descrita de protocolos de seguridad?

    a) Sí

    b) No

5. ¿Considera importante el uso de protocolos de seguridad en las redes informáticas bancarias?
    a) Sí
    b) No
6. De los siguientes protocolos de seguridad seleccione los protocolos que conoce o ha escuchado.
    a) TPC/IP (Transmission Control Protocol/Internet Protocol)
    b) TCP (Transmision Control Protocol)
    c) HTTP (Hypertext Transfer Protocol)
    d) FTP (File Transfer Protocol)
    e) SSH (Secure Shell)
    f) SMTP (Simple Mail Transfer Protocol)
    g) ARP (Address Resolution Protocol)
7. Las conexiones de red admiten dos tipos de cifrado, los cuales son Microsoft MPPE y Seguridad de Protocolo de Internet (IPSec). ¿Según la afirmación anterior, conocía alguno de los 2 tipos de cifrado?
    a) Sí
    b) No
8. ¿Conoce el concepto de delito informático?
    a) Sí
    b) No
9. ¿Conoce el concepto de fraude informático?
    a) Sí

b) No

10. ¿Considera que las medidas de seguridad y dispositivos adicionales utilizados por las entidades bancarias para reducir el fraude informático en el acceso a la información son las más adecuadas?

    a) Sí

    b) No

11. ¿Sabia que el código penal de Costa Rica en su Articulo 217bis, impone una pena de prisión de uno a diez años a la persona que cometa fraude informático?

    a) Sí

    b) No

12. ¿Cuál es su género?

    a) Masculino

    b) Femenino

13. ¿Cuál es el rango de edad en el que se encuentra usted?

    a) 20-30

    b) 31-40

    c) 41-50

    d) Más de 51 años.

San Pedro, 05 de diciembre, 2012

Señores
ULACIT

Estimados señores:

Por este medio hago constar que el estudiante Eduardo Solís Hernández me ha presentado el documento denominado "¿Cuál es el nivel de confidencialidad de la información durante su transmisión en las redes informáticas bancarias para la reducción del fraude informático?"

He corregido los errores de ortografía y redacción que se trasladan al escrito y he comprobado que se realizaron los cambios correspondientes en el documento.

Por lo tanto, considero que se encuentra listo para ser presentado ante la Universidad.

Atentamente,

M.Sc. Marianela Abellán Vargas
Carné 10702
Filóloga