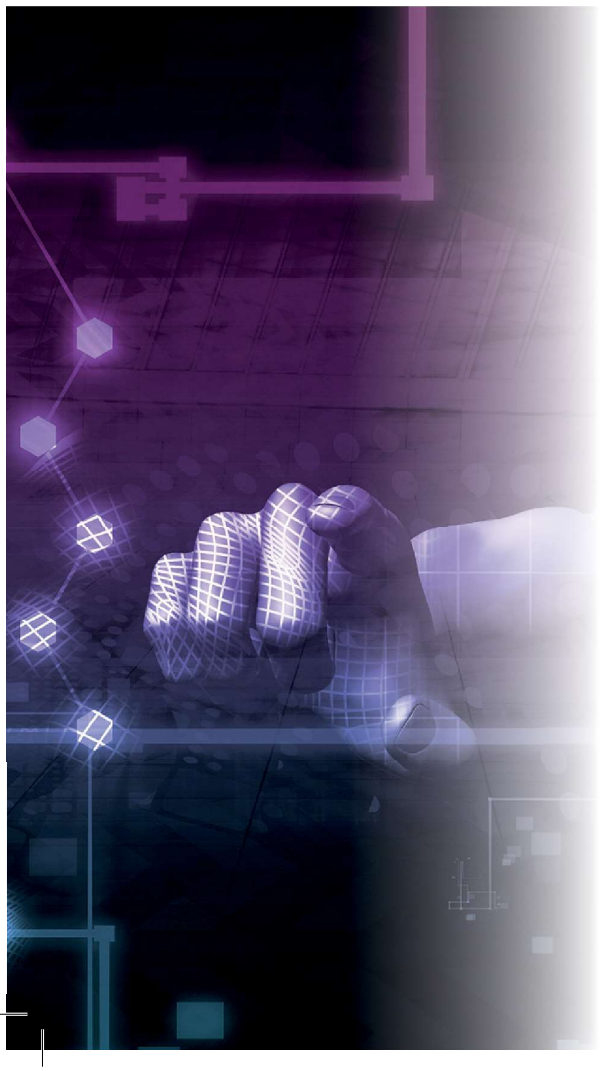
4 Uso y seguridad de la información de clientes en las empresas y/o entidades financieras de Colombia

Use and security of customer information in business and / or financial institutions in Colombia

Autores: Alberto Cruz Cruz y Flagler Sierra Viasus.
Estudiantes de Administración de Empresas.
Investigador: Miguel Antonio Alba Suárez.
Grupo de investigación: Gestión, Organizaciones y Sociedad.
Facultad de Ciencias Económicas, Administrativas y Contables.
Universidad Libre, Bogotá.



Resumen

A través del presente artículo se explica que la seguridad en las tecnologías de la información y comunicaciones (TICS), se hace tan necesario como la funcionalidad misma. Resguardar la disponibilidad, integridad y confidencialidad de sus datos, al igual las operaciones, es un inmenso reto que se hace a diario, es algo complejo, por su evolución y los riesgos que día a día se vuelven y se tornan más sofisticados, al estar cada vez los usuarios o beneficiarios mejor conectados y menos controlados.

* Artículo recibido en marzo, 2016. Este trabajo es sometido como requisito para optar por el título de Administrador de Empresas en la Universidad Libre Seccional Bogotá.
D. Cruz es estudiante de Administración de Empresas de la Universidad Libre 2015. Teléfono 310-200-6947. e-mail: Daniela.cruzc@unilibrebog.edu.co.
F. Sierra es estudiante de Administración de Empresas de la Universidad Libre 2015. Teléfono 311-809-1753. e-mail: Flagler.sierrav@unilibrebog.edu.co

En la actualidad el auge de la globalización ha iniciado una intensificación de la competitividad en todos los sectores de la economía. Ello simboliza que, cada vez más, los oferentes de bienes y servicios, son obligados a mantener su mirada a la calidad y en la mejora incesante para ser elegidos por los clientes; pero de otra parte, la protección de la información se ha venido desprotegiendo debido a problemas de seguridad críticos con múltiples fallos, que en cierta forma son explorados crackers como Anonymous y Hacker generan grandes pérdidas en los sectores en que son implementadas en el mundo y en Colombia.

Es así que este documento especifica sobre la importancia de la concientización sobre el uso y seguridad de la información de clientes en las empresas y/o entidades financieras de Colombia.

Palabras clave:
Clientes, Colombia, empresas, información, seguridad, uso, ingeniería social.

Abstract

Through this article that security in the information technology and communications (ICT), is as necessary as the functionality itself. Protect the availability, integrity and confidentiality of their data, like operations, it is a huge challenge that is done daily, is complex, its evolution and the risks that every day become and become more sophisticated, being more and better connected users or beneficiaries and less controlled.

Today the rise of globalization has begun an intensified competitiveness in all sectors of the economy. This symbolizes that, increasingly, suppliers of goods and services, are required to keep their eyes on quality and continual improvement to be chosen by customers; but on the other hand, the protection of information has been deprotecting due to critical security issues with multiple failures, which in some ways are explored crackers as Anonymous and Hacker generate large losses in sectors that are implemented in the world and in Colombia. Thus, this document specifies the importance of awareness on the use and security of customer information in business and / or financial institutions in Colombia.

Key words:
Customers, Colombia, businesses, information security, use, social engineering.

I. Introducción

Mediante este documento; se afirma que desde hace algunos años, la información ha sido considerada como uno de los activos más valiosos e importantes de una compañía y más aun de las entidades financieras; de otra parte los costos derivados de pérdida de seguridad no son sólo costes económicos directos, sino que también afectan a la imagen de la empresa, por lo que, cada día más, la seguridad de la información forma parte principal de los objetivos de todas las organizaciones y, no obstante, y a pesar de la concienciación generalizada, varias compañías no se enfrentan a este aspecto con la firmeza con la que se debiera tratarse.

La presente investigación documental se realizó con antecedentes, experiencias, y métodos e investigaciones documentales

tales como libros, artículos de revista que presentaron aspectos relevante con relación al **uso y seguridad de la información de clientes en las empresas y/o entidades financieras de Colombia**, con la siguiente argumentación al respecto; el tema general tenido en cuenta es resaltar los eminentes riesgos en las grandes empresas.

Ahora bien la incesante evolución, sofisticación y crecimiento de la tecnología, al igual que los ataques cibernéticos en las organizaciones empresariales, colocan de manifiesto la urgente necesidad de implementar las medidas necesarias y controles que posibiliten la protección a la compañía ante las posibles amenazas a los activos informáticos informacionales. De igual manera hace necesario diseñar un sistema de seguridad informático que logre salvaguardar los recursos y herramientas informáticas de la estructura empresarial, apoyando a la organización a desempeñar sus objetivos.

La gestión de la seguridad de la información debe efectuarse mediante un proceso de orden sistemático, documentado y conocido por toda la organización empresarial.

Al mismo tiempo, garantizar un nivel de protección general es virtualmente imposible, inclusive en el caso tal de disponer de un presupuesto ilimitado. El gran propósito de un sistema de gestión de seguridad de la información es, efectivamente, certificar y garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma totalmente documentada, sistemática, repetible, adecuada y eficiente a los cambios que se originen en los riesgos, el entorno y las tecnologías.

Es de saber que, la inseguridad de las tecnologías de la información para las organizaciones es (Un concepto dual en seguridad informática)[1] es una de las inminentes necesidades implementar la seguridad en la información para establecer "estándares y buenas prácticas"[2] en pro del beneficio de las empresas y sus clientes.

A continuación se abordaran las siguientes temáticas: tipos de ataques que existen actualmente, la ingeniería social y la implementación de estándares de uso y seguridad de la información, donde se revisarán los métodos de control y metodologías para la gestión de seguridad de la información.

II. Experiencias, hechos y tipos de ataques

Al llegar a este punto se evidenciaran algunos casos y experiencias que han ocurrido en estos últimos años, así mismo afirmaciones relacionadas directamente con la temática seguridad de la información.

Por otra parte se mostraran los diferentes tipos de ataques con algunas series de recomendaciones para no caer en manos de ingenieros sociales.

Hecho N°1 La cierta complejidad de medidas requeridas para asegurar los sistemas de información, es mayor cada día, rigiendo a

1 J. Cano, «Inseguridad informática: Un concepto dual en seguridad informática», *Revista de Ingeniería Universidad de los Andes*, n° 19, 2004.

2 Asociación Colombiana de Ingenieros de Sistemas ACIS, «https://seguinfo.wordpress.com,» 4 junio 2011. [En línea]. Available: https://seguinfo.wordpress.com/2011/06/04/xi-acis-jornada-de-seguridad-informatica-en-colombia-2011/. [Último acceso: 21 marzo 2016].

todos los interesados, a precisar el desarrollo de esquemas, que se tengan en cuenta el carácter globalizado de las Tecnologías de la Información, y las dificultades con delitos informáticos, que son cada día más críticos. Un ejemplo, en los Estados Unidos se reportaron en el año 2010, 303.809 incidentes de seguridad informática, con un promedio de 25.317 por mes (en comparación, la IFCC recibió 20.014 quejas en sus primeros seis meses).[3] Esto quiere decir que los incrementos en ese país son elevados, y tan solo en ese año. (CRIME COMPLAINT).

Hecho N°2 Según (Noticias CM&), los problemas que evidenció la comunidad de crackers más popular en la actualidad "Anonymous", el 30 de Noviembre del 2011, la cual aseguró que accedió a cuentas de clientes importantes en bancos de Estados Unidos como Chase Bank, Bank of America y a tarjetas de crédito de Citibank que les hurtara dinero para entregarlo a los pobres a través de instituciones benéficas.[4]

Hecho N°3 (Stel, 2014), afirma que el mundo pelea con armas convencionales en el campo de batalla, pero también en el ciberespacio y por ende, lo tiene absolutamente asumido como tal. Recordemos que las guerras convencionales tienen un tiempo, un espacio u enemigo identificado, un inicio y un fin mientras que las que se libran en el ciberespacio, son anárquicas por naturaleza, al menos por ahora. La "intifada del ciberespacio" se libra hoy y se seguirá librando por mucho tiempo más.

Hecho N°4: El 14 de abril de 2005 el diario la Gaceta, de la provincia de Tucumán, Argentina, público que un colombiano, Ricardo Alfonso Ureche Lotero, robo más de 228.000 dólares de cuentas Bancarias de Bélgica, Estados Unidos, Noruega, y cuatro entidades bancarias de Argentina.

El cracker, fue sorprendido cuando accedía en forma ilícita al portal de internet de un banco, utilizando claves de acceso y números de cuenta de usuarios del sistema bancario, información robada de ordenadores varios, usando un programa espía tipo troyano, software de origen japonés que logro instalar en los ciberbares y que ordenaba otras computadoras de otros cibercafés, remitir lo códigos de acceso a cuentas predeterminadas.

Si bien las operaciones fueron múltiples, las que permitieron la captura, fueron las desarrolladas en movimientos a cuentas de Bogotá, desde Barranquilla, Cartagena, Ibagué, Tunja, Medellín, Cali y San Andrés Islas, entre otras ciudades.[5]

Es de saber que este tipo de personas son expertas informáticas, de acuerdo a (Ripoll, 2012), es el tipo de persona que utiliza ordenadores ajenos para cometer delitos[6] pero ahora bien, debe existen cualesquier tipo de modalidades para ejecutar otros tipos de delitos.

---

3 INTERNET CRIME COMPLAINT CENTER, «http://www.ic3.gov,» 2010.[Enlínea].Available: http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf.

4 NOTICIAS CM&, «CRAKERS,» Canal de noticias por fecha, Bogotá, 2011.

5 E. Stel, Seguridad y defensa del ciberespacio, Buenos Aires: DUNKEN, 2014

6 J. Ripoll, Seguridad en los Sistemas Informáticos (SSI), Valencia: Etsinf, 2012.

Tipos de ataques

De acuerdo (Segu.info, 2000). A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar "agujeros" en el diseño, configuración y operación de los sistemas.[7]

Son innumerables los autores que narran minuciosamente y sistemáticamente las técnicas y las catalogan de acuerdo a diversas características de las mismas. Ante la variedad y las clasificaciones de amenazas y las inminentes apariciones de nuevas técnicas, los ataques serán clasificados y categorizados según la experiencia y conocimiento de cada caso. (Segu.info, 2000).

Es de destacar en el presente artículo que sólo se pretende dar una idea de la cantidad y variabilidad de los mismos, así como que su adaptación (y aparición de nuevos) continúa paralela a la creación de nuevas tecnologías. (Segu.info, 2000).

A este respecto (SEGU.INFO, 2000-2009) "Cabe destacar que para la utilización de estas técnicas no será necesario contar con grandes centros de cómputos, lo que queda fehacientemente demostrado al saber que algunos Hackers más famosos de la historia hackeaban con computadoras (incluso armadas con partes encontradas en basureros) desde la habitación de su hogar".

Cada uno de los ataques abajo descriptos son dirigidos remotamente.

1. La ingeniería social y el phishing

Se define como aquellas conductas y técnicas utilizadas para conseguir información de las personas. Es una disciplina que consiste básicamente en sacarle datos a otra persona sin que esta se dé cuenta de que está revelando información sensible y que normalmente no lo haría.[8] (Salazar, 2014).

Objetivos

Estos pueden ser varios. Entre ellos:

- Conseguir beneficios económicos para los creadores de malware y estafadores debido al ínfimo costo de implementación y el alto beneficio obtenido.
- Realizar compras telefónicamente o por Internet con medios de terceros, conociendo bastante sobre ellos (datos personales, tarjeta de crédito, dirección, entre otros).
- Acceder gratuitamente a Internet si lo que se buscaba era nombre de usuario contraseña de algún cliente que abone algún servicio de Banda Ancha.

Según (Salazar, 2014), sintetiza un ejemplo verídico y es que aún las más grandes empresas que invierten millones de dólares al año en la seguridad de sus datos, fueron víctimas de estos ataques de Ingeniería Social. Un ejemplo donde se muestra la imaginación de los "Ingenieros Sociales", en junio del año 2009 fue sometida a auditoria un empresa de estados unidos La empresa

[7] SEGU.INFO SEGURIDAD DE LA INFORMACION 2000 -2009 disponible en: http://www.segu-info.com.ar/ataques/tipos.htm

[8] D. Salazar, *Técnicas de ataque a la seguridad*, Chiclayo: Escuela de Ingenieria de Sistemas, 2014.

tenía como objetivo demostrar que atreves de las memorias tipo USB se podían transferir virus tipo troyano en los dispositivos que fuese instalada causando daños. Con esa información se puede deducir que una empresa que tenga un nivel de seguridad alto y una inversión considerable en esta misma puede recaer en la ingeniería social.

Pueden existir maneras de mitigar estos ataques y es a través de la Educación. En realidad es una forma efectiva de estar protegido contra la Ingeniería Social.

Las personas por no entrar en situaciones incomodas brinda todo tipo de información, justo en ese momento se destaca un aspecto como lo es enseñar a decir no.

Para este caso no se trata de educación técnica es destacar la educación de la sociedad y las capacitación para que las personas se alerten si consideran en riesgo de un ataque. Generalmente los ingenieros sociales tienen experiencia y podrían engañar a cualquier persona sin tener que hacer mayor esfuerzo. (Salazar, 2014).

Con todo lo mencionado sobre la ingeniería social hasta ahora se puede decir y es evidente ante cualquier lector, que el ser humano es el elemento más débil ante cualquier sistema. Las personas con la responsabilidad en armar una red y tratándose estrictamente en seguridad informática puede tengan en cuenta los más mínimos detalles, siempre es un ser humano el que está al frente de un dispositivo ejecutando acciones y haciendo uso de una red y un sistema.

Formas de ataque: Existen diversas maneras de ataque, también depende de la pericia e ingenio de la persona que tenga intención de realizarlo, estas maneras son:

a) ***Ataques telefónicos:*** Este tipo de ataque se considera eficiente debido que las habilidades de un ingeniero social, por la falta de comunicación visual esto evita que se pueda descubrir de manera simple.

   Ataques vía web: Según (visentini, 2006) hoy en día sólo hacen falta pocas cosas para causar pánico, una conexión a Internet y malas intenciones. este tipo de ataque, cuando el Ingeniero Social juega con la desinformación y sentimientos de las personas, ya que pone en marcha un plan estratégico, que sólo los análisis estadísticos pueden mostrar la eficiencia y eficacia que obtienen al realizarlos. No se trata de otra cosa que un simple correo electrónico del cual no se sospecha y puede venir disfrazado de muchas formas, ya sea que la dirección de correo electrónico resulte familiar o el asunto del e-mail de cierta forma "ataque" los sentimientos como la curiosidad, la avaricia, el sexo, la compasión o el miedo y es donde el usuario se vuelve susceptible a abrirlo. (Salazar, 2014)

2. Phishing

Se define como el engaño tan dañino y eficaz como se pueda imaginar, utilizado siempre para fines delictivos. Básicamente consiste en algún e-mail que procede al parecer de un negocio o empresa legítima y digna de confianza (un banco o compañía de crédito) solicitando "verificación" de los datos y advirtiendo sobre consecuencias que traerían si no se hiciera dicha verificación (D. Salazar, 2014).

Por otro lado el (Gobierno de Aragón, Departamento de Ciencia, Tecnología y Universidad) deduce que el *phishing* es la estafa con más éxito en Internet y consiste en obtener el PIN o las contraseñas mediante engaño, normalmente pidiéndolas en un correo electrónico que simula provenir de un banco o una entidad oficial como, por ejemplo, la Agencia Tributaria. Estos correos son siempre falsos, ya que las contraseñas no se piden nunca por correo. (Gobierno de Aragón, 2014).

Es así que (D. Salazar, 2014), el mensaje y/o notificación por lo general tiene un enlace que conduce a un sitio web fraudulento que a simple vista es idéntico al legítimo, incluso con todos los logotipos propios de la empresa, contenido imágenes, y un formulario que solicita muchos datos (que van desde la dirección hasta la contraseña de acceso de la tarjeta de crédito o débito) que una vez ingresados estos datos por el usuario, van directo a las manos del falsificador.

El phishing tiene como gran aliado al spam, ya que este e-mail fraudulento se envía indiscriminadamente a miles de usuarios tomados de bases de datos, donde siempre alguno (un poco crédulo) ingresará sus datos en esta falsa página web y probablemente los daños que sufrirá serán de un alto impacto. Podría perder todo el dinero de su cuenta bancaria o tarjeta de crédito. (D. Salazar, 2014).

Tipos de ataque de Phishing (Arias, 2014):

a) ***Ataques al servidor DNS:*** Consiste en corromper el DNS **Sistema de Nombres de Dominio** en una red de ordenadores, haciendo que la URL (Localizador de Uniforme de Recursos o Direcciones www) de una web pase a apuntar hacia un servidor diferente del original. Al introducir la URL "dirección" de la web a la que desea ir, un banco por ejemplo, el servidor DNS convierte la dirección en un numero IP, correspondiente al del servidor del banco. Si el servidor DNS es vulnerable a un *ataque de Pharming*, la dirección podrá apuntar hacia una página falsa hospedada en otro servidor con otra dirección IP, que estará bajo control de un defraudador.

b) ***URLs falsas***: Otra manera es la creación de URLs extensas que dificultan la identificación por parte del usuario. un ejemplo simple puede ser:/intermentbanking/eud=65167659Redirecto:ma.algunacosa.dominiofalso.com donde el usuario puede directamente mirar el inicio de la URL y creer que está en una zona segura de la web de su banco, mientras que en realidad está en un subdominio de website.

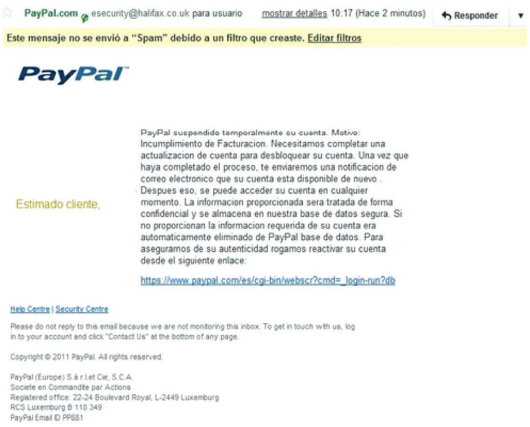
c) ***Formulario HTML falsos en Emails:*** Otra técnica menos frecuente es la utilización de formularios e emails. Con formato HTM. Con eso, un usuario incauto puede incluir directamente en su email las informaciones requeridas por el defraudador, y por eso, este no necesita preocuparse de hacer una clonación de la interfaz del banco.

De acuerdo con lo la información dada anteriormente, la búsqueda por esas informaciones sensibles crece con el aumento de la posibilidad de realizar las más diversas tareas en el confort del hogar. Eso puede a una masa de internautas una sensación de seguridad que es irreal. Se dice irreal, ya

que una vez que internet se ha convertido en una tendencia globalizada, no se espera menos, de que también existan crimines globales. (Arias, 2014).

Aprovechándose de la desatención de ciertos usuarios, los individuos maliciosos desarrollan y ponen en práctica métodos cada vez más sofisticados para cometes acciones ilícitas. Algunos de estos métodos, destacan por su eficacia y su rendimiento, y de entre estos, podemos citar, ciertamente, el ataque de Phishing Scam.[9] (Arias, 2014).

Ejemplo ataque tipo phishing



Fuente:(Qositblog)http://blog.qosit.eu/ataques-de-ingenieria-social-y-phishing/

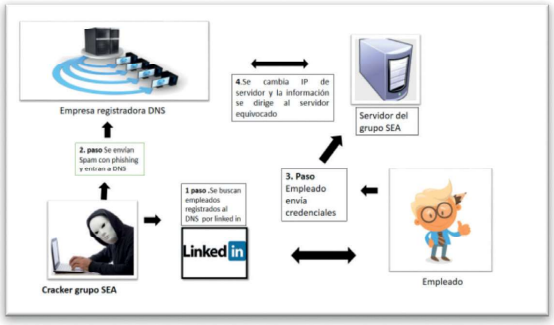
A continuación se cita otro ejemplo de ataque a una web de fuentes de contenido a una empresa del grupo RSA Conference:

El ataque de lo SEA a la web de la RSA Conference

Uno de los casos más recientes de ataque a una web mediante el compromiso de fuentes de contenido externo tuvo lugar en el defacement de la web de la **RSA Conference**, una de las conferencias de seguridad de más prestigio en el mundo. Para poder realizar el ataque, el grupo **SEA** (Syrian Electronic Army), aprovecho que se cargaba un fichero JavaScript desde un servidor web perteneciente a otro dominio. Este fichero se utilizaba para llevar las estadísticas de las visitas a la web y el grupo atacante busco la manera de que se cargara el fichero JavaScript que ellos querían. (Pittari, 2015).

Para ello tenían que conseguir que el nombre de dominio del servidor remoto apuntara a una dirección *IP* controlada por ellos, por lo que revisaron en qué proveedor estaba registrado el dominio del servidor de las estadísticas e hicieron un ataque de *phishing* a los empleados del registrador - que buscaron por Linkedin para robar credenciales de acceso a la gestión de los dominios.[10] (Phats, 2014).

El ataque de lo SEA a la web de la RSA Conference



Fuente: http://www.elladodelmal.com

[9] A. Arias, Las Estafas Digitales, IT Campus Academy, 2014.

[10] E. A. C. Paths, E., Alonso, C disponible en: http://www.elladodelmal.com/2014/08/riesgos-de-seguridad-al-cargar.html

Con una de esas identidades robadas fueron capaces de gestionar el **DNS** del dominio al que pertenecía el servidor de las estadísticas y hacer que el nombre del servidor que cargaba el fichero JavaScript en la web de la **RSA Conference** apuntara a un servidor web controlado por ellos, desde el que cargaron un fichero JavaScript (Paths, 2014).

Afirma (pittari, 2015), que es responsabilidad de quien recibe este mensaje, estar concienciado en que, ninguna entidad solicitará por medio de correo electrónico datos sensibles, personales o credenciales de acceso. Y en caso de recibir este tipo de correos, es importante acceder (no por el vínculo que propone el propio correo fraudulento), al sitio web de la organización impostada y denunciar el intento de phishing.

A. Cómo evitar ser víctima de un intento de ataque

Es de gran importancia estar consciente de las posibles amenazas y de igual manera poder descifrar guías o conductas que puedan evidenciar algunas sospechas.

Los correos electrónicos que no se ha solicitado así como también llamadas telefónicas en las cuales algún personaje tenga la intención de solicitar información de tipo personal o información de la empresa podrían tratarse de un ataque de este tipo si la persona expresa pertenecer a una empresa u organismo que sea de confianza es de suma importancia hacer un cruce de información para verificar que se trate de un personaje seguro. (Pittari, 2015).

Se recomienda evitar la divulgación de información personal o de la empresa sin estar seguro de que el interlocutor tenga el nivel requerido para tener acceso a dicha información generalmente los sitios web falsos tienen un URL similar a la original que no se detona al ojo de un usuario.

B. Qué hacer si hemos sido víctimas de un ataque de phishing. (Pittari, 2015)

Si hemos sido o quizá hemos creído haber sido víctimas de un ataque de ingeniería social o phishinig, en el cual hemos dado información de una organización, se debe comunicar de manera inmediata a la persona encarga de la seguridad de la información, se debe hacer atreves de una notificación de incidencia. El omitir esta notificación se estaría incurriendo en una doble mala práctica, pues se estaría impidiendo que se adopten medidas que protejan a la organización ante un ataque potencial que utilice la información divulgada.

Si la información es de tipo personal o de tipo financiera se debe poner en contacto con la entidad relacionada al incidente y proceder a tomar las medidas correspondientes según la entidad del caso.

C. Qué es el robo de identidad (Pittari, 2015)

En el momento en que las técnicas de ataques de la ingeniería social resulten tener éxito y el cracker tiene acceso a información de alta importancia de la persona que está siendo atacada como podría ser: nombre, fecha de nacimiento, número de identificación, dirección postal, número de cuenta bancaria, etc. estará en disposición de efectuar el robo de identidad del afectado.

El robo de identidad consiste en que el delincuente se presente ante entidades como la persona a la que ha sido afectada pudiendo aportar información consistente y lo suficiente para superar los filtros de seguridad de estas entidades.

El robo de identidad permite que el delincuente pueda realizar diferente acciones como compras, extraer dinero de cuentas, solicitar préstamos, todo ello a nombre del afectado.

En la mayor parte de los casos los afectados no reciben directamente el ataque si no que se hace atreves de una compañía con la cual el afectado tenga alguna relación cercana y esta tenga información del afectado, el delincuente se roba las bases de datos para poder hacer robo de identidad de todos los clientes o usuarios de la organización.

Dado que al dar información personal a las entidades con las que se tiene algún vínculo no se puede dar garantía de no caer en robo de identidad sin embargo se cuenta con maneras de reducir el riego.

D. Cómo saber si hemos sido víctimas del robo de identidad. (Pittari, 2015)

Si la información que permite el robo de identidad esta divulgada, seria por medio de alguna identidad con la que se tiene algún tipo de relación y estaría dada por medio de un ataque se depende que de la entidad que tiene información haga el reporte y comunique la incidencia con el afectado para que este pueda tomar decisiones y estas sean oportunas.

Sin embargo las entidades con las que se tienen las información importante no siempre hace las notificación en el tiempo adecuado o en algunos casos esta notificación no se realiza, por ello se estar alerta a cualquier tipo de situación que puedan mostrar evidencia de este hecho.

E. Qué hacer si hemos sido víctimas de un robo de identidad. (Pittari, 2015)

Los directamente afectados por la ingeniería social, no solo se enfrentan a consecuencias de tipo económico, sino que también existen aspectos relevantes, como consecuencias emocionales que en un individuo pueden influir más que las de tipo económico, si se cree que un usuarios ha sido afectado por este delito, se debe hacer la notificación a las autoridades generalmente la recuperación de una delito de este tipo resulta ser larga, costosa y de alto estrés.[11]

Por otra parte y a este respecto es recomendable que se aproveche las medidas de seguridad adicionales que proporcione la entidad, por ejemplo factor de autenticación doble, número de seguridad para las operaciones, entre otras.

3. Ingeniería Social Inversa

Consiste en la generación, por parte de los intrusos, de una situación inversa a la originada en Ingeniería Social. En este caso el intruso publicita de alguna manera que es capaz de brindar ayuda a los usuarios, y estos lo llaman ante algún imprevisto. El intruso aprovechara esta oportunidad para pedir información necesaria para solucionar

[11] Pittari. S, ataque de ingeniería social, blog.qosit.eu, 2015. Disponible en: http://blog.qosit.eu/ataques-de-ingenieria-social-y-phishing/

el problema del usuario y el suyo propio (la forma de acceso al sistema La **ISI** (ingeniería social inversa) es más difícil de llevar a cabo y por lo general se aplica cuando los usuarios están alertados de acerca de las técnicas de **IS** (ingeniería social.), (SEGU.INFO, 2000-2009).

4. Trashing (Cartoneo)

Generalmente, un usuario anota su login y password en un papelito y luego, cuando lo recuerda, lo arroja a la basura. Este procedimiento por más inocente que parezca es el que puede aprovechar un atacante para hacerse de una llave para entrar el sistema..." nada se destruye, todo se transforma", (SEGU.INFO, 2000-2009).

El Trashing puede ser físico (como el caso descripto) o lógico, como analizar buffers de impresora y memoria, bloques de discos, etc. El Trashing físico suele ser común en organizaciones que no disponen de alta confidencialidad, como colegios y universidades, (SEGU.INFO, 2000-2009).

5. Ataques de Monitorización

Este tipo de ataque se realiza para observar a la víctima y su sistema, con el objetivo de establecer sus vulnerabilidades y posibles formas de acceso futuro, (SEGU.INFO, 2000-2009).

6. Ataques de Autenticación

Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y password, (SEGU.INFO, 2000-2009).

7. Denial of Service (DoS)

Los protocolos existentes actualmente fueron diseñados para ser empleados en una comunidad abierta y con una relación de confianza mutua. La realidad indica que es más fácil desorganizar el funcionamiento de un sistema que acceder al mismo; así los ataques de Negación de Servicio tienen como objetivo saturar los recursos de la víctima de forma tal que se inhabilita los servicios brindados por la misma, (SEGU.INFO, 2000-2009).

8. Amenazas Lógicas - Tipos de Ataques - Ataques de Modificación (Daño)

(SEGU.INFO, 2000-2009), Estos se clasifican de la siguiente forma:

- *Tampering o Data Diddling*: Esta categoría se refiere a la modificación desautorizada de los datos o el software instalado en el sistema víctima (incluyendo borrado de archivos). El Administrador posiblemente necesite darlo de baja por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada. Como siempre, esto puede ser realizado por Insiders u Outsiders, generalmente con el propósito de fraude o de dejar fuera de servicio a un competidor. Son innumerables los casos de este tipo: empleados bancarios (o externos) que crean falsas cuentas para derivar fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes, o contribuyentes que pagan para que se les anule una deuda impositiva. Múltiples Web Sites han sido víctimas del cambio en sus páginas por imágenes.

- ***Borrado de huellas:*** Es una de las tareas más importantes que debe realizar el intruso después de ingresar en un sistema, ya que, si se detecta su ingreso, el administrador buscará como conseguir "tapar el hueco" de seguridad, evitar ataques futuros e incluso rastrear al atacante. Las Huellas son todas las tareas que realizó el intruso en el sistema y por lo general son almacenadas en Logs (archivo que guarda la información de lo que se realiza en el sistema) por el sistema operativo. Los archivos Logs son una de las principales herramientas (y el principal enemigo del atacante) con las que cuenta un administrador para conocer los detalles de las tareas realizadas en el sistema y la detección de intrusos.

- ***Ataques Mediante Java Applets:*** Los más usados navegadores actuales, implementan Máquinas Virtuales Java (MVJ) para ser capaces de ejecutar programas (Applets) de Java. Estos Applets, al fin y al cabo, no son más que código ejecutable y como tal, susceptible de ser manipulado por intrusos. Las restricciones a las que somete a los Applets son de tal envergadura (imposibilidad de trabajar con archivos a no ser que el usuario especifique lo contrario, imposibilidad de acceso a zonas de memoria y disco directamente, firma digital, etc.) que es muy difícil lanzar ataques.

- ***Ataques Mediante JavaScript y VBScript:*** JavaScript (de la empresa Netscape) y VBScript (de Microsoft) son dos lenguajes usados por los diseñadores de sitios Web para evitar el uso de Java. Los programas realizados son interpretados por el navegador. Aunque los fallos son mucho más numerosos en versiones antiguas de JavaScript, actualmente se utilizan para explotar vulnerabilidades específicas de navegadores y servidores de correo ya que no se realiza ninguna evaluación sobre si el código.

- ***Ataques Mediante ActiveX:*** ActiveX es una de las tecnologías más potentes que ha desarrollado Microsoft. Mediante ActiveX es posible reutilizar código, descargar código totalmente funcional de un sitio remoto, etc. Esta tecnología es considerada la respuesta de Microsoft a Java.ActiveX soluciona los problemas de seguridad mediante certificados y firmas digitales. Una Autoridad Certificadora (AC) expende un certificado que acompaña a los controles activos y a una firma digital del programador. Cuando un usuario descarga una página con un control, se le preguntará si confía en la AC que expendió el certificado y/o en el control ActiveX. Si el usuario acepta el control, éste puede pasar a ejecutarse sin ningún tipo de restricciones (sólo las propias que tenga el usuario en el sistema operativo).Es decir, la responsabilidad de la seguridad del sistema se deja en manos del usuario, ya sea este un experto cibernauta consciente de los riesgos que puede acarrear la acción o un perfecto novato en la materia. Esta última característica es el mayor punto débil de los controles ActiveX ya que la mayoría de los usuarios aceptan el certificado sin siquiera leerlo, pudiendo ser esta la fuente de un ataque con un control dañino. La filosofía ActiveX es que las Autoridades de Certificación se fían de la palabra del programador

del control. Evidentemente siempre hay programadores con pocos escrúpulos o con ganas de experimentar. Así, un conocido grupo de hackers alemanes (3), desarrolló un control ActiveX maligno que modificaba el programa de Gestión Bancaria Personal Quicken95© de tal manera que si un usuario aceptaba el control, éste realizaba la tarea que supuestamente tenía que hacer y además modificaba el Quicken, para que la próxima vez que la víctima se conectara a su banco, se iniciara automáticamente una transferencia a una cuenta del grupo alemán. Otro control ActiveX muy especialmente "malévolo" es aquel que manipula el código de ciertos exploradores, para que éste no solicite confirmación al usuario a la hora de descargar otro control activo de la Web.

- *Vulnerabilidades en los Navegadores:* Generalmente los navegadores no fallan por fallos intrínsecos, sino que fallan las tecnologías que implementan, aunque en este punto analizaremos realmente fallos intrínsecos de los navegadores, como pueden ser los "Buffer Overflow"(4). Los "Buffer Overflows" consisten en explotar una debilidad relacionada con los buffers que la aplicación usa para almacenar las entradas de usuario. Precisamente existen fallos de seguridad del tipo "Buffer Overflow" en la implementación de estos dos protocolos. Además la reciente aparición (octubre de 2000) de vulnerabilidades del tipo Transversal en el servidor Web Internet Información Server de la empresa Microsoft. explotando fallas en la traducción de caracteres Unicode, puso de manifiesto cuan fácil puede resultar explotar una cadena no validada. (SEGU. INFO, 2000-2009)

III. Implementación de estándares uso y seguridad de la información

En la actualidad existen varios estándares, modelos, sistemas de gestión y buenas prácticas que fomenten la seguridad de la información en las tecnologías y compañías, dentro del más notable es el estándar **ISO/IEC 15408 Common Criteria**,[12] es una alianza internacional entre varias organizaciones del mundo para que con base al desempeño de las funciones y los niveles de evaluación, se respalde desarrollo, diseño y puesta en la producción con las medidas de seguridad apropiadas para el mercado. SYMANTEC, 1995-2016).

En Colombia, el estándar no es muy común y en Latinoamérica no existe en el momento un centro de investigación que autentifique la aplicación del estándar, pero a medida que la globalización y los retos productivos del país se enfoquen a un desarrollo y producción de tecnología de forma mayoritaria, se hace inminentemente necesario adoptarlo. (SYMANTEC, 1995-2016).

La seguridad en las tecnologías de la información Seguridad Informática, es una de las importantes necesidades que en conjunto con las funcionales es esencial, debido a que una falla en ella forma un impacto directo en contra del objetivo de una empresa por los cuales son diseñados los componentes.

[12] SYMANTEC, 1995-2016

Es así que para la seguridad de las tecnologías de la información existen algunos estándares para las buenas prácticas:

Según (ICONTEC) Instituto Colombiano de Normas Técnicas y Certificación

a) *NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001*

Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información **(SGSI)**, La NTC-ISO/IEC 27001 fue ratificada por el Consejo Directivo del 2006-03-22. Esta norma está sujeta a ser actualizada permanentemente con el objeto de que responda en todo momento a las necesidades y exigencias actuales.

Esta norma cubre todo tipo de organizaciones (por ejemplo: empresas comerciales, agencias gubernamentales, organizaciones sin ánimo de lucro). Esta norma específica los requisitos para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos globales del negocio de la organización.

Especifica los requisitos para la implementación de controles de seguridad adaptados a las necesidades de las organizaciones individuales o a partes de ellas. El SGSI está diseñado para asegurar controles de seguridad suficiente y proporcional que protejan los activos de información y brinden confianza a las partes interesadas.[13]

Asimismo el estándar para la seguridad de la información ISO/IEC 27001 (Information technology, Security techniques, Information security management systems, Requirements) fue certificado y publicado como el estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission. Especificando los requerimientos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI. ICONTEC, 2006)

De otra parte, es sólido con las mejores prácticas definidas en ISO/IEC 27002 y tiene su principio en la norma BS 7799-2:2002, perfeccionada por la entidad de normativización británica, la British Standards Institution (BSI).

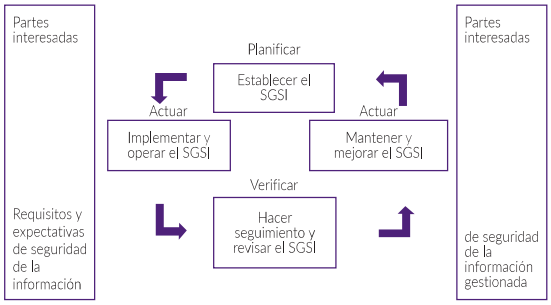
A este respecto (ICONTEC, 2006), la adopción del modelo **PHVA** también reflejará los principios establecidos en las Directrices OCDE (2002), **(**ICONTEC, 2006), que controlan la seguridad de sistemas y redes de información. Esta norma brinda un modelo robusto para implementar los principios en aquellas directrices que controlan la evaluación de riesgos, diseño e implementación de la seguridad, gestión y reevaluación de la seguridad.

EJEMPLO 1
Un requisito podría ser que las violaciones a la seguridad de la información no causen daño financiero severo a una organización, ni sean motivo de preocupación para ésta.

EJEMPLO 2
Una expectativa podría ser que si ocurre un incidente serio, como por ejemplo el

[13] ICONTEC, «http://intranet.bogotaturismo.gov.co,» 03 04 2006. [En línea]. Available: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf.

Hacking del sitio web de una organización, haya personas con capacitación suficiente en los procedimientos apropiados, para minimizar el impacto.



Fuente: Modelo PHVA aplicado a los procesos de SGS (ICONTEC)

(P.H.V.A.)	Descripción
Planificar (establecer el SGSI)	Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.
Hacer (implementar y operar el SCSI)	Implementar y operar la política, los controles, procesos y procedimientos del SGSI.
Verificar (hacer seguimientos y revisar el SGSI)	Evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.
Actuar (mantener y mejorar el SGSI)	Emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del SGSI y la revisión por la dirección, para lograr la mejora continua del SGSI.

Fuente: (ICONTEC)

(MINISTERIO DE ADMINISTRACIONES PÚBLICAS, 2004) Desde que en 1992 la OCDE desarrollara por primera vez las Directrices de Seguridad de los Sistemas de Información, el uso de los sistemas y redes de información, así como el entorno tecnológico de información, en su totalidad, han sufrido grandes cambios. La naturaleza y el tipo de tecnologías que constituyen la infraestructura de la información y comunicaciones también han cambiado de manera significativa. El número y el tipo de dispositivos que integran la infraestructura de acceso se ha multiplicado, incluyendo elementos de tecnología fija, inalámbrica y móvil, así como una proporción creciente de accesos que están conectados de manera permanente.

Como consecuencia de todos estos cambios, la naturaleza, volumen y sensibilidad de la información que se intercambia a través de esta infraestructura se ha incrementado de manera muy significativa. Como resultado de una creciente interconexión, los sistemas y las redes de información son más vulnerables, ya que están expuestos a un número creciente, así como a una mayor variedad, de amenazas y de vulnerabilidades. Esto hace que surjan nuevos retos que deben abordarse en materia de seguridad. Por estas razones, estas Directrices se aplican para todos los participantes de la nueva sociedad de la información y sugieren la necesidad de tener una mayor conciencia y entendimiento de los aspectos de seguridad, así como de la necesidad de desarrollar una "cultura de seguridad".[14] (MIN. RELACIONES EXT.)

[14] MINISTERIO DE ADMINISTRACIONES PÚBLICAS (Organization for economic Co-operation and Development)

b) Cobit

(Objetivos de control para la información y tecnologías relacionadas) es una metodología publicada en 1996 por el Instituto de Control de TI y la ISACA (Asociación de Auditoría y Control de Sistemas de Información) que se usa para evaluar el departamento de informática de una compañía; en Francia está representada por la AFAI (Asociación Francesa de Auditoría y Consejo de TI information technology).

Este enfoque se basa en un índice de referencia de procesos, indicadores de objetivos clave (KGI) e indicadores de rendimiento clave (KPI) que se usan para controlar los procesos para recoger datos que la compañía puede usar para alcanzar sus objetivos.[15] (CCM, 2016).

(CCM BENCHMARK GROUP, 2016). El enfoque COBIT propone 34 procesos organizados en 4 áreas funcionales más grandes que abarcan 318 objetivos:

- Entrega y asistencia técnica.
- Control.
- Planeamiento y organización.
- Aprendizaje e implementación.

Cobit implementa los objetivos de seguridad de la información en Colombia, el propósito de Cobit es brindar a la Alta Dirección de una compañía confianza en los sistemas de información y en la información que estos produzcan. Cobit permite entender como dirigir y gestionar el uso de tales sistemas así como establecer un código de buenas prácticas a ser utilizado por los proveedores de sistemas. Cobit suministra las herramientas para supervisar todas las actividades relacionadas con IT."[16] (L. CAMELO).

Según (Camelo, 2010), afirma las ventajas que ofrece Cobit:

- Cobit es un marco de referencia aceptado mundialmente de gobierno IT basado en estándares y mejores prácticas de la industria. Una vez implementado, es posible asegurarse de que IT se encuentra efectivamente alineado con las metas del negocio, y orientar su uso para obtener ventajas competitivas.

- Suministra un lenguaje común que le permite a los ejecutivos de negocios comunicar sus metas, objetivos y resultados con Auditores, IT y otros profesionales.

- Proporciona las mejores prácticas y herramientas para monitorear y gestionar las actividades de IT. El uso de sistemas usualmente requiere de una inversión que necesita ser adecuadamente gestionada.

- Ayuda a los ejecutivos a entender y gestionar las inversiones en IT a través de sus ciclo de vida, así como también proporcionándoles métodos para asegurarse que IT entregara los beneficios esperados.

c) Magerit

Otra metodología que implementan las empresas en Colombia, según (Carvajal), es

[15] CCM BENCHMARK GROUP, 2016.

[16] L. Camelo, *Seguridad de la Información en Colombia*, Bogotá, 2010.

una metodología exitosa muy probada, es la creada por el Consejo Superior de Informática de España sobre el Análisis y Gestión de Riesgos de los sistemas de Información. La primera versión se hizo en1997, actualmente existe la versión II.[17] (VARVAJAL).

De acuerdo a (Duque, 2010), Magerit es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión. La razón de ser de Magerit está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los usuarios; Con Magerit se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.[18](MAGERINT, DAFP).

d) Octave

(Riesgoscontrolinformatico, 2014) Es la metodología más práctica debido a que esta técnica se basa en la planificación y consultoría estratégica en seguridad basada en el riesgo y rompe con la típica consultoría focalizada en tecnología, para encontrar riesgos tácticos. Debido a que el OCTAVE se enfoca en tres aspectos principales Riesgos Operativos, Prácticas de Seguridad y Tecnología lo que nos permite que esta técnica sea llevada a cabo por un pequeño equipo de gente desde los sectores operativos o de negocios hasta los departamentos de tecnología de la información (IT) trabajan juntos dirigidos a las necesidades de seguridad; y por su misma filosofía de incluir a todos los departamentos de la empresa y que no necesite de gran número de personas para desarrollar la metodología nos permite que se ejecute en pequeñas empresas.[19] (R. CONTROL INFO. 2014).

e) Guías NIST (National Institute of Standars and Tecnology) USA.

NIST es el Instituto Nacional de Normas y Tecnología con sus siglas en inglés, National Institute of Standards and Technology), es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos.

La FISMA (Federal Information Security Management Act) de Estados Unidos, otorgó al NIST, el desarrollo de un conjunto de documentos SP-800 con el objetivo de dar un marco de referencia completo a la gestión de la seguridad de la Información, para que sea aplicado en forma obligatoría por las agencias norteamericanas debido a una ley.

NIST SP 800-53A, es un documento Guía para la Evaluación de la Seguridad de Controles de sistemas de Información Federal y de organizaciones y cumple con el NIST SP 800-53. En el documento Guide for Assessing the Security Controls in Federal

[17] A. Carvajal, «http://52.1.175.72,» [En línea]. Available: http://52.1.175.72/portal/sites/all/themes/argo/assets/img/Pagina/17-ElAnalisisRiesgosBaseSistemaGestionSeguridadInformacionCasoMagerit.pdf.

[18] B. Duque, METODOLOGÍAS DE GESTIÓN DE RIESGOS (OCTAVE, MAGERINT, DAFP), Caldas: Universidad de Caldas, 2010.

[19] «http://riesgoscontrolinformatico.blogspot.es,» 20 marzo 2014. [En nea]. Available: http://riesgoscontrolinformatico.blogspot.es/tags/metodo-elegido-octave/.

Information Systems and Organizations de esta metodología, presenta el desarrollo de planes de evaluación de seguridad y la realización de evaluaciones de control de seguridad que se puede tener a la mano a la hora de realizar las auditorias como mecanismo de evaluación.

A manera de evaluación técnica y/o práctica, NIST presenta un documento NIST-800-115, que remplaza la NIST-800-42 que proporciona directrices para las organizaciones en la planificación y realización de las pruebas de seguridad de la información y evaluaciones de la seguridad técnica, análisis de los resultados y el desarrollo de la mitigación estrategias.[20] (UNAD).

f) Guías de la ENISA (European Network of Information Security Agency)

10 de marzo de 2004 se creó una Agencia Europea de Seguridad de las Redes y de la Información (ENISA). Su objetivo era garantizar un nivel elevado y efectivo de seguridad de las redes y de la información en la Comunidad Europea y desarrollar una cultura de la seguridad de las redes y la información en beneficio de los ciudadanos, los consumidores, las empresas y las organizaciones del sector público de la Unión Europea, contribuyendo así al funcionamiento armonioso del mercado interior. Desde hace varios años, diferentes grupos europeos dedicados a la seguridad, como los CERT/CSIRT, los equipos de detección y respuesta a abusos y los WARP, colaboran para que Internet sea más seguro (MINCOMUNICACIONES).

También afirma que: la *"ENISA"* desea apoyar el esfuerzo realizado por estos grupos aportando información acerca de las medidas que garantizan un nivel adecuado de calidad de los servicios. Además, la Agencia desea potenciar su capacidad de asesorar a los Estados miembros de la UE y los órganos comunitarios en cuestiones relacionadas con la cobertura de grupos específicos de usuarios de las TI con servicios de seguridad adecuados. Por lo tanto, basándose en los resultados del grupo de trabajo ad-hoc de cooperación y apoyo a los CERT, creado en 2005, este nuevo grupo de trabajo se encargará de asuntos relativos a la prestación de servicios de seguridad adecuados (servicios de los CERT) a grupos de usuarios específicos.[21]

(MINCOMUNICACIONES), es así que para asegurar el cumplimiento de sus objetivos según lo precisado en su regulación, las tareas de la agencia se enfocan en:

- Asesorar y asistir a los Estados miembro en temas de seguridad de la información y a la industria en problemas de seguridad relacionados con sus productos de hardware y de software.
- Recopilar y analizar datos sobre incidentes de la seguridad en Europa y riesgos emergentes.
- Promover métodos de gestión de riesgo de la seguridad de la información.

[20] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD), «http://datateca.unad.edu.co,» [En línea]. Available: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/621_metodologa_nistsp800.html.

[21] MINISTERIO DE COMUNICACIONES, REPÚBLICA DE COLOMBIA

Los principales servicios que promueven son:

Servicios Reactivos	Servicios Proactivos	Manejo de Instancias	Gestión de la Calidad de la Seguridad
Alertas y advertencias	Comunicados	Análisis de instancias	Análisis de riesgos
Tratamiento de incidentes	Observatorio de tecnología	Respuesta a las instancias	Continuidad del negocio y recuperación tras un desastre
Análisis de incidentes	Evaluaciones o auditorías de la seguridad	Coordinación de la respuesta a las instancias	Consultoría de seguridad
Apoyo a la respuesta a incidentes	Configuración y mantenimiento de la seguridad		Sensibilización
Coordinación de la respuesta a incidentes	Desarrollo de herramientas de seguridad		Educación/ Formación
Respuesta a incidentes in situ	Servicios de detección de intrusos		Evaluación o certificación de productos
Tratamiento de la vulnerabilidad	Difusión de información relacionada con la seguridad		
Análisis de la vulnerabilidad			
Respuesta a la vulnerabilidad			
Coordinación de la respuesta a la vulnerabilidad			

Fuente: MINCOMUNICACIONES

g) ISM3 - Information Security Management Maturiy Model

Según (Stansfeld, 2007). La seguridad se define como el resultado de la reunión continua y superación de una serie de objetivos. La seguridad en el contexto de un enfoque tiene por objeto garantizar que se cumplan los objetivos de negocio. La definición de la seguridad es ISM3 por lo tanto, depende del contexto.

Tradicionalmente, para ser medio seguro para ser invulnerable (resistente a cualquier posible ataque). El uso de la seguridad en contexto, ser medios fiables que sean fiables, a pesar de los ataques, los accidentes y errores. Tradicionalmente, un incidente es toda pérdida de confidencialidad, integridad o disponibilidad. En virtud de la seguridad en su contexto, un incidente es un incumplimiento de los objetivos del negocio de la organización.

Debe haber un equilibrio entre los negocios, el cumplimiento y necesidades y limitaciones técnicas, como el coste, la funcionalidad, la privacidad, la responsabilidad y riesgo. A medida que los próximos contornos de mesa, el logro de los objetivos de negocio depende de los objetivos del negocio, que a su vez dependen en parte de los objetivos de seguridad. Hay tres tipos de objetivos de seguridad, las derivadas directamente de las necesidades del negocio, las que son consecuencia del entorno normativo y las derivadas del uso de sistemas de información.[22] (Stansfeld, 2007).

h) ITIL

(Information Technology Infrastructure Library) ha demostrado ser una estrategia que apoya tanto la mejora de la calidad en el servicio de las áreas de Tecnología de Información como la mejora en el desempeño generando ventajas competitivas a nivel de la organización. Las mejores prácticas establecidas por ITIL Foundations - Edición 2011, han permitido a las áreas de Tecnología

[22] E. Stansfeld, «http://www.lean.org/,» 2007. [En línea]. Available: http://www.lean.org/FuseTalk/Forum/Attachments/ISM3_v2.00-HandBook.pdf.

de Información vuelvan a posicionarse en el plano estratégico de los negocios a los que dan servicio y que vean a esta como el área estratégica de apoyo para el logro de los objetivos de la organización.[23] (ETIL, 2011)

i) ISO/IEC 15408 Common Criteria

Se define como acuerdo internacional sobre el método de desarrollo seguro, y 7 niveles discretos de la gama de esfuerzo, incluyendo la especificación del trabajo de los evaluadores en cada nivel. De otra parte es un paradigma de arquitectura de seguridad sobre el que se aplica un catálogo coherente y relacionado de funciones de seguridad que permiten establecer un lenguaje común para la expresión de la seguridad de los productos y el sistema de las TI.[24] (COMMON CRITERIA)

Medidas de seguridad

La información es uno de los principales activos de cualquier empresa, es por ello que las nuevas tecnologías de la información y la comunicación se han convertido en una herramienta indispensable para desarrollar cualquier actividad económica, así como un componente clave para mejorar la productividad de las compañías.

De acuerdo al tema de seguridad, existen organizaciones que prestan servicios tecnológicos en seguridad de la información a empresas; es el caso lo relacionado a continuación:

Con respecto a (Symantec, 1995-2016), En nuestros centros de investigación y desarrollo de todo el mundo, más de 3.500 ingenieros de Symantec crean soluciones para ayudar a usuarios individuales y empresas a garantizar la seguridad, la disponibilidad y la integridad de su información.

Rust, Alemania, Jornadas Mundiales de alojamiento - 15 de marzo 2016 - Symantec Corp. (NASDAQ: SYMC), líder mundial en seguridad cibernética, ha anunciado hoy la disponibilidad mundial de cifrado En todas partes, un paquete de seguridad del sitio web disponibles a través de proveedores de alojamiento web. En todas partes de cifrado permite a los proveedores de alojamiento web se integran cifrado en todos los sitios web desde el momento en que se crea. Con el nuevo servicio de seguridad web, proveedores de alojamiento pueden ofrecer una variedad de opciones flexibles, incluido el cifrado sitio web básico incluye como parte de cualquier servicio alojado, y una serie de paquetes de seguridad de alta calidad con niveles cada vez más fuertes de la validación del sitio web, protección y sellos de confianza. Symantec quiere ver el 100% de los sitios web legítimos garantizados para el año 2018, y el cifrado En todas partes se ha desarrollado para apoyar ese objetivo. Symantec será la demostración de cifrado todas partes durante la conferencia mundial de alojamiento Días en Rust, Alemania, 15-18 de marzo de, 2016, stand Z03.

De otra parte, Mountain View, California - 18 de febrero 2016 - Symantec Corp. (NASDAQ: SYMC), líder mundial en seguridad cibernética, ha anunciado hoy que Symantec Endpoint Protection (SEP) ganó

[23] ETIL Foundation - Edicion 2011, «http://www.worldtraiingcolombia.com/,» 2011. [En línea]. Available: http://www.worldtrainingcolombia.com/contenidos.php?Id_Categoria=142..

[24] COMMON CRITERIA, «http://52.1.175.72/,» 2009.

AV-TEST "Mejor Protección Premio 2015" para los usuarios corporativos. Symantec Endpoint Protection fue reconocida por su alto rendimiento constante de la seguridad en todas las pruebas de certificación 2015. [25] (SYMATEC, 1995-2016).

Como prevenirse realmente contra la ingeniería social

Proteger totalmente la empresa de un ataque mediante ingeniería social es imposible. Mientras haya personas en relación con los sistemas informáticos, aquellas representaran un punto débil, una vulnerabilidad potencial que un atacante podrá explotar.

Puesto que es imposible prescindir del elemento humano, debemos intentar limitar al máximo los riesgos.

a) ***Formar y sensibilizar a los usuarios:*** La primera línea de defensa contra los ataques de ingeniería social es formar a todos los usuarios.

   Por definición, cualquier persona que disponga de un código de acceso al sistema puede ser víctima de un ataque. Esto también incluye a los usuarios temporales: bancarios, prestatarios externos, comerciales itinerantes, etc.

b) ***Implementar un punto de alerta de seguridad centralizada:*** Además de la formación, un punto esencial de la lucha contra los ataques de ingeniería social consiste en proporcionar a los empleados de la empresa un número de teléfono que les permita contactar instantáneamente con un responsable del servicio de seguridad, en caso de que tenga alguna duda sobre el origen de un mensaje.

   Debemos partir del principio que, aunque formados de forma conveniente, un usuario no tiene ni la competencia ni el tiempo de analizar con detalle los sucesos que podría parecerles sospechosos.

   Por otra parte, el usuario estimara, con razón, que no es su trabajo lo máximo que objetivamente podemos pedirle es que haga algunas comprobaciones antes de aceptar una directiva, y señalar sistemáticamente todo lo que pueda parecerla sospechoso a los responsables de seguridad.[26] (J MARK ,2004).

IV. Conclusiones

Las empresas, proveedores y clientes de tecnologías de información (TIC), tendrán que tener más sentido de responsabilidad, eso significa que deberían aumentar su rigurosidad y ser más exigentes en aspectos como documentación y creación de software, todo esto bajo un enfoque de control y gestión de seguridad de información y todos los aspectos relacionados con esta misma. También la creación de guías sencillas para la educación de usuarios del internet.

Por otro lado el posible riesgo en seguridad de los programas o software utilizados por las empresas y entidades son cada día más

[25] SYMATEC, «http://www.symantec.com,» 1995-2016. [En línea]. Available: http://www.symantec.com/es/es/about/profile/technology.jsp.

[26] J. Marc, Recursos Informaticos, Seguridad en la Informática de Empresa, Barcelona: Ediciones ENI, 2004. P. 366-368

apropiados, pues los usuarios necesitan garantías que les brinden seguridad y respaldo. Precisamente las certificaciones como La: ISO/IEC 15408Common Criteria contribuye a que el país siga en el mejoramiento de los sistemas de gestión en seguridad de la información y destacarse dentro de la región ya que en los países vecinos aun no es de gran impacto esta temática. Por lo que lidera el desarrollo de tecnología e innovación.

A llegar a este punto sobre la temática se puede concluir haciendo la afirmación que los principales inconvenientes que se presentan en tema de seguridad de información de una organización, no se soluciona al 100% con la implementación de un (SGSI) pues definitivamente la decisión de un usuario que posee datos importantes, no siempre es la mejor. Cabe destacar que al certificarse el riego disminuirá proporcionalmente y servirá para posibles investigaciones futuras.

No obstante la temática de ingeniería social no es fácil de mitigar y contrarrestar, pues existen un número significativo de técnicas para lograr y llevar acabo este delito, en algunos casos la tecnología tiene un papel importante, pero las habilidades para la manipulación de seres humanos también funcionan y estas pueden ir desde obtener datos personales hasta espionaje industrial y provocar grandes daños.

Por otra parte el estudio y capacitación pueden brindar conocimientos y técnicas a los empleados que lo necesiten, con el fin de que puedan reconocer y dar manejo a la situación de la mejor manera, complementando, los métodos utilizados por la ingeniería social deben ser utilizados para la investigación y que esta a su vez permita mitigar estas conductas aunque la responsabilidad sea de los empleados.

Agradecimientos

Los autores quieren agradecer a sus padres, quienes han sido apoyo fundamental en su formación personal y académica, al cuerpo docente de la Universidad Libre seccional Bogotá, en especial a la doctora Clara Inés Camacho Roa, Decana de la Facultad de Ciencias Económicas Administrativas y Contables, al doctor Fabio Romero, Director del Programa de Administración de Empresas, al doctor Luis Humberto Beltrán Galvis, Director del Centro de Investigaciones y al Profesor Miguel Antonio Alba Suarez tutor del grupo de investigación.

Referencias

[1] J. Cano, «Inseguridad informática: Un concepto dual en seguridad informática,» *Revista de Ingeniería Universidad de los Andes*, nº 19, 2004.

[2] Asociación Colombiana de Ingenieros de Sistemas ACIS, «https://seguinfo.wordpress.com,» 4 junio 2011. [En línea]. Available: https://seguinfo.wordpress.com/2011/06/04/xi-acis-jornada-de-seguridad-informatica-en-colombia-2011/. [Último acceso: 21 marzo 2016].

[3] INTERNET CRIME COMPLAINT CENTER, «http://www.ic3.gov,» 2010. [En línea]. Available: http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf.

[4] NOTICIAS CM&, «CRAKERS,» Canal de noticias por fecha, Bogotá, 2011.

[5] E. Stel, Seguridad y defensa del ciberespacio, Buenos Aires: DUNKEN, 2014.

[6] J. Ripoll, Seguridad en los Sistemas Informáticos (SSI), Valencia: Etsinf, 2012.

[7] SEGU.INFO SEGURIDAD DE LA INFORMACIÓN, «http://www.segu-info.com.ar,» 2000-2009. [En línea]. Available: http://www.segu-info.com.ar/ataques/tipos.htm.

[8] D. Salazar, *Técnicas de ataque a la seguridad*, Chiclayo: Escuela de Ingeniería de Sistemas, 2014.

[9] A. Arias, Las Estafas Digitales, IT Campus Academy, 2014.

[10] E. A. C. Paths, «http://www.elladodelmal.com,» 27 agosto 2014. [En línea]. Available: http://www.elladodelmal.com/2014/08/riesgos-de-seguridad-al-cargar.html.

[11] S. Pittari, «http://blog.qosit.eu,» 23 marzo 2015. [En línea]. Available: http://blog.qosit.eu/ataques-de-ingenieria-social-y-phishing/.

[12] SYMANTEC, «http://www.symantec.com,» 1995-2016. [En línea]. Available: http://www.symantec.com/es/es/about/profile/technology.jsp.

[13] ICONTEC, «http://intranet.bogotaturismo.gov.co,» 03 04 2006. [En línea]. Available: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf.

[14] MINISTERIO DE ADMINISTRACIONES PÚBLICAS (Organization for economic Co-operation and Development), «https://www.oecd.org,» 2004. [En línea]. Available: https://www.oecd.org/sti/ieconomy/34912912.pdf.

[15] CCM BENCHMARK GROUP, «http://es.ccm.net,» marzo 2016. [En línea]. Available: http://es.ccm.net/contents/596-cobit-objetivos-de-control-para-la-informacion-y-tecnologias-re.

[16] L. Camelo, *Seguridad de la Información en Colombia*, Bogotá, 2010.

[17] A. Carvajal, «http://52.1.175.72,» [En línea]. Available: http://52.1.175.72/portal/sites/all/themes/argo/assets/img/Pagina/17-ElAnalisisRiesgosBaseSistemaGestionSeguridadInformacionCasoMagerit.pdf.

[18] B. Duque, METODOLOGÍAS DE GESTIÓN DE RIESGOS (OCTAVE, MAGERINT, DAFP), Caldas: Universidad de Caldas, 2010.

[19] «http://riesgoscontrolinformatico.blogspot.es,» 20 marzo 2014. [En línea]. Available: http://riesgoscontrolinformatico.blogspot.es/tags/metodo-elegido-octave/.

[20] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD), «http://datateca.unad.edu.co,» [En línea]. Available: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/621_metodologa_nistsp800.html.

[21] Ministerio de Comunicaciones, República de Colombia, Diagnóstico de la Situación Actual - Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea, Bogotá: Área de Investigación y Planeación p. 95, 2008.

[22] E. Stansfeld, «http://www.lean.org/,» 2007. [En línea]. Available: http://www.lean.org/FuseTalk/Forum/Attachments/ISM3_v2.00-HandBook.pdf.

[23] ETIL Foundation - Edicion 2011, «http://www.worldtrainingcolombia.com/,» 2011. [En línea]. Available: http://www.worldtrainingcolombia.com/contenidos.php?Id_Categoria=142..

[24] COMMON CRITERIA, «http://52.1.175.72/,» 2009. [En línea]. Available: http://52.1.175.72/portal/sites/all/themes/argo/assets/img/Pagina/Criterioscomunespara Monitoreary EvolucionarIa SeguridadInform_ticaen Colombia-JACL-Password.pdf.

[25] SYMATEC, «http://www.symantec.com,» 1995-2016. [En línea]. Available: http://www.symantec.com/es/es/about/profile/technology.jsp.

[26] J. Marc, Recursos Informáticos, Seguridad en la Informática de Empresa, Barcelona: Ediciones ENI, 2004.