La Seguridad Informática

Resumen

Las tendencias actuales sobre tecnologías y sus avances, han dado una serie de facilidades a las personas, tanto en lo laboral como en lo particular, el hogar, lo social, las comunicaciones, etc. permitiendo crear entornos participativos más amplios. La conciencia en el uso de estas tecnologías donde la información que se proporciona es cada vez mayor, sugeriría un cambio de paradigma sobre los hábitos de relacionamiento con los demás. Inicialmente, la idea de una Aldea Global era solamente una teoría que afirmaba que algún día todas las personas podrían estar comunicadas a escala mundial, y no es sino gracias a las redes sociales, que actualmente se tiene acceso a una Aldea Digitalmente Global, pero ¿bajo qué términos y con qué tipo de consecuencias?. En las empresas, un programa de seguridad de la información es un plan para mitigar los riesgos asociados con el procesamiento de la misma, ante lo cual la innovación permanente es la clave para mantenerla; poder ir un paso adelante de aquellos que pretenden sustraerla. El presente artículo pretende enfatizar conceptos poco tratados que ayuden en la administración de información a uno de los eslabones más débiles en la cadena de la seguridad: el factor humano.

Palabras clave: *Información, factor humano, seguridad, integridad, confidencialidad, amenazas, disponibilidad, controles, consejos, riesgos.*

Abstract

The current trend of technological advances has provided people with a series of facilities, as much in the workplace as in their private life the home, social life and communications, etc. This has allowed the creation of wider participatory environments. The conscience in the use of these technologies where the information that is provided is ever greater would suggest a paradigm change relationship habits of with others. Initially the idea of a Global Village was, only a theory that affirmed that someday all the people could communicate on a global scale, and thanks to the social networks, at the moment one has access to a Global Digital Village, but under what terms and with what type of consequences? In companies, a program of information security is a plan to mitigate the risks associated with data interchange. Permanent innovation is the key to maintain it; to be able to stay a step ahead of those that seek to reduce it. This article seeks to emphasize concepts that help administration of information to one of the weakest links in the security chain: The human factor.

Key words: *Information, human factor, security, integrity, confidentiality, threats, availability, controls, advices, risks.*

Cristhian Alexander Rocha Haro, Lcdo.[1]

Ciencias Administrativas y Comerciales

carh-78@hotmail.com

Recibido: Marzo, 2011
Aceptado: Junio, 2011

[1]Analista de Sistemas y Licenciado en Sistemas de Información otorgado por la Escuela Superior Politécnica del Litoral–PROTCOM–FIEC. Docente de la Universidad Estatal de Milagro en la Unidad de Ciencias Administrativas y Comerciales para las carreras de Gestión Empresarial, Economía, Ingeniería en CPA, Ingeniería Comercial. Actualmente cursa una Maestría en Educación Superior en Investigación e Innovaciones Pedagógicas en la Universidad Casa Grande y es miembro del Departamento de Investigación, Desarrollo Tecnológico e Innovación.


SEGURIDAD

INTRODUCCIÓN

Desde el surgimiento de la raza humana en el planeta la información estuvo presente bajo diversas formas y técnicas, muy poco comunes para los tiempos actuales, y en los que el hombre buscaba representar sus hábitos, costumbres e intenciones en diversos medios que pudiesen ser utilizados por él y por otras personas a través de los tiempos, además de la posibilidad de ser trasladados de un lugar a otro. La información valiosa era registrada en objetos preciosos y sofisticados, pinturas magníficas, entre otros, que se almacenaban con mucho cuidado en locales o sitios de difícil acceso, a cuya forma y contenido sólo tenían, quienes estuviesen autorizados o listos para interpretarla (observe figura 1); ejemplo de aquello eran las civilizaciones egipcias, que fueron los primeros en crear sistemas de escrituras basados en jeroglíficos hace millones de años [1].

En la actualidad, la información sigue siendo el objeto de mayor valor para la colectividad y para las organizaciones especialmente por su relevancia en la toma de decisiones. La llamada Sociedad de la Información, que según la enciclopedia Wikipedia define como: "Aquella en la cual las tecnologías facilitan la creación, distribución y manipulación de la información juegan un papel importante en las actividades sociales, culturales y económicas" [4]; ha sido inspirada por países industrializados como sinónimo de progreso social, eficiencia y productividad, desligándolo de la vertiente que, conforme a las reflexiones del sociólogo belga Armand Mattelart (nacido en 1936, autor del libro Historia de la sociedad de la información) apunta a la sociedad de la información como un modo de organización que lleva implícito el control y

Figura 1. Objetos representativos de civilizaciones existentes [2] y [3].

gestión informatizada de la ciudadanía [5].

Desde una perspectiva de la economía globalizada contemporánea, la sociedad de la información concede a las Tecnologías de la Información y Comunicación (TIC's) el poder de convertirse en los nuevos motores de desarrollo y progreso; evidenciándose en la incorporación de las mismas en la mayoría de los procesos y aplicaciones estratégicas, disminuyendo así los tiempos de espera en las transacciones de las organizaciones y reduciendo sus costos. Este progreso presenta nuevas perspectivas, así pues como en la vida real se debe brindar seguridades a los activos adquiridos, también hay que proporcionarlas a la información que se administra de manera digital, adquiriendo este recurso un valor superior inclusive; y es así que la Academia Latinoamericana de la Seguridad Informática proporciona un breve criterio: "La seguridad de la información tiene como propósito proteger la información registrada, independientemente del lugar en que se localice: impresos en papel, en los discos duros de las computadoras o incluso en la memoria de las personas que la conocen" [6].

Es sorprendente como a partir de esta convergencia, y con el apoyo del internet, las personas fueron siendo las protagonistas de su propia evolución, pues a medida que estas se desarrollaban, sentían una necesidad de interactuar con el medio y dejaron de ser simples espectadores para transformarse en creadores de contenidos a través de los blogs, wikis, redes y comunidades virtuales. Por otro lado, las brechas digitales, aunque siguen siendo un obstáculo para el desenvolvimiento en esta nueva sociedad, han ido disminuyendo y en gran parte se debe a la juventud de hoy que tienen una gran voracidad por el uso de las herramientas tecnológicas, llámense celulares, ipods, tablets PC, smart phones o cualquier otro gadget (dispositivo que tiene un propósito y una función específica, de pequeñas proporciones, práctico y a la vez novedoso, a más de tener un diseño más ingenioso que el de la tecnología corriente [7]) que posea la conectividad necesaria para intercambiar información, transferir archivos de música, video, documentos, aplicativos o simplemente el mantenerse en un mundo online.

La seguridad de la información estratégica y sus elementos

Los incidentes de seguridad han hecho que las empresas tomen conciencia de la importancia en la administración de riesgos de

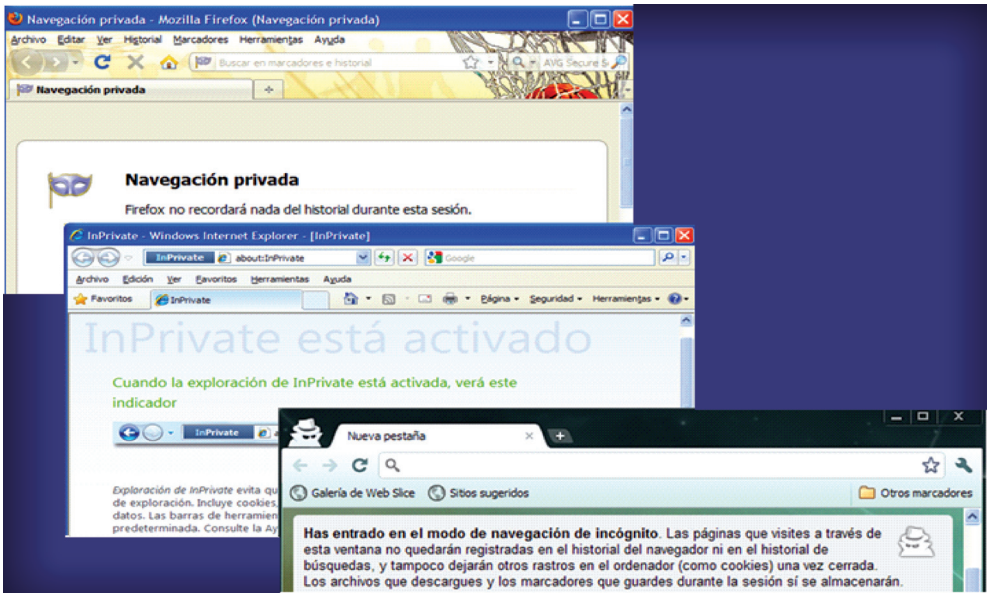

Figura 2. Navegación privada de algunos navegadores web (la mayoría se encuentra en el menú Herramientas de los navegadores)

la información, como estrategia del negocio a través de programas que aunque rudimentarios de cierta forma, están evolucionando y tomando madurez. Mientras algunas compañías han obtenido progresos, otras tantas no se han comprometido a desarrollar programas completos o no las integran a sus procesos de negocios; por lo que demostrar a sus clientes que la seguridad y protección de sus recursos es el centro de sus funciones comerciales, las hacen compañías con programas de seguridad de la información estratégicos.

En una definición más amplia, un programa de seguridad de la información es un plan para mitigar los riesgos asociados con el procesamiento de la información y el uso de los recursos que lo soportan; existiendo tres elementos o principios básicos que la concretan [8], [9]:

- **Integridad:** Este principio asegura que la información sea exacta, completa, sin alteraciones o modificaciones en su contenido, efectuada por usuarios o procesos no autorizados. Una información podrá cambiar tanto en su contenido como en el ambiente que lo soporta.
- **Confidencialidad:** Tiene como propósito prevenir el uso no autorizado de la información, por personas no facultadas para tal efecto. Eso significa que estos datos deben ser conocidos sólo por un individuo o grupo controlado de personas, definidos por el responsable de la información. La privacidad es un tema estrechamente relacionado con este elemento, consiguiéndose últimamente un mejor entendimiento sobre su aplicación
- **Disponibilidad:** Este principio asegura que los usuarios tengan acceso oportuno y fiable a sus recursos de información, permitiendo de esta forma la continuidad del negocio.

Los 10 objetivos identificados	Válido phishes
1 Paypal	8.843
2 Facebook	862
3 Grupo HBSC	668
4 Servicio de Impuestos Internos	376
5 Bradesco	264
6 World of Warcraf	252
7 Vapor	167
8 Bank of America Corporation	167
9 MySpace	166
10 Sulake Corporation	163

Tabla 1. Estadísticas de marzo 2010 sobre phishing a sitios reconocidos
Fuente: Phishtank [12].

El entendimiento de estos tres principios básicos es fundamental en el desarrollo e implementación de toda política de seguridad, a la vez que confluyen en la idea de proteger la información como un recurso del negocio y otorgarle el posicionamiento estratégico que se merece.

Hacia una cultura de seguridad

Aunque la sociedad de la información no está limitada simplemente al Internet, éste ha jugado un papel muy importante

en los tiempos actuales como medio facilitador del acceso a la información y los datos. En este sentido, el reto para los individuos que se desenvuelven en todas las áreas del conocimiento es vivir de acuerdo con las exigencias de este nuevo tipo de sociedad, manteniéndose informados, actualizados y renovando permanentemente; pero sobre todo concibiendo propuestas y generando conocimientos que surjan de los millones de datos que circulan en la red.

Los peligros en la red son cada vez mayores y el internet es una entrada a posibles filtraciones y ataques empleando métodos que están en continua evolución para burlar el software de seguridad de las computadoras; aunque la clave es poder ir un paso por delante de los ciberdelincuentes, los delitos en Internet se suceden a diario y son las personas las primeras en ofrecerse como víctimas. A continuación se expondrán algunos aspectos de seguridad que debe considerar [10]:

- Algunos de los detalles personales que podría compartir en redes sociales, como su escuela, ciudad de nacimiento o fechas de aniversario, son muchas veces los mismos elementos que se usan en las preguntas "secretas" de seguridad en bancos y sitios Web, por lo que un atacante que recolecte suficiente información puede obtener acceso a sus cuentas más importantes de Facebook, Linked In, Twitter, My Space, u otra red social. Para tal efecto, se recomienda revisar su configuración de privacidad en Facebook, que le permite elegir quién puede ver su información personal y ajustarla a sus necesidades de sharing con precaución; igualmente se sugiere no aceptar peticiones de amistad de extraños, pues es probable que de vez en cuando reciba solicitudes de personas que no conoce valiéndose de esta relación en línea y aprovechando esa confianza. Si usted toma en serio la protección de su información personal, no debería aceptar dichas invitaciones.
- Al realizar negocios con empresas de confianza, esté consciente de las políticas de privacidad de los sitios y servicios de la web ahora que el entretenimiento, las compras y la socialización se han transportado a la red, pues cada usuario de internet deja un gran sendero digital de preferencias como: los libros que lee, películas que alquila, personas con las que interactúa, artículos que compra y otros detalles que constituyen una mina de oro de datos demográficos para motores de búsqueda, los anunciantes y cualquiera que quisiera husmear en su computador. Precaviendo esta situación observe en las versiones actuales de navegadores como Explorer, Firefox, Safari y Chrome, que incluyan modos de navegación privada con protección contra phishing integradas que advierten sobre sitios sospechosos (Figura 2), recomendando su uso para cifrar la información sensible que comparte en su transacción; o en su defecto, actualice a la última versión de su navegador web. Estas características aseguran que el historial del sitio, datos de formularios, búsquedas, contraseñas y otros detalles de la sesión actual de internet no se almacenen en la caché de su navegador, protegiendo su navegación de forma segura.

Los 10 objetivos identificados	Válido phishes
1 Paypal	7,991
2 Facebook	1,180
3 Sulake Corporation	1,079
4 Santander UK	680
5 World of Warcraft	379
6 HSBC Group	312
7 Her Majesty' s Revenue and Customs	295
8 NatWwest Bank	213
9 Barclays Bank PLC	206
10 Lloyds TBS	202

Tabla 2. Estadísticas de marzo 2011 sobre phishing a sitios reconocidos
Fuente: Phishtank [13]

De acuerdo a lo observado en las estadísticas sobre ataques a sitios conocidos en el lapso de un año (2010 – 2011), se evidencia un alto índice de ataques especialmente en aquellos sitios como redes sociales, sitios de juegos y banca o compras on-line, en los que la entrega de información personal sensible es alta. Aunque algunos sitios han tomado soluciones para disminuir o prevenir los riesgos de pishing como Paypal, otros han incrementado la frecuencia como Facebook y World of Craft en la que los usuarios intercambian información con otros constantemente sin cuidado alguno y que reafirma la hipótesis sobre la inexistencia de una cultura de protección a la información en las personas, pudiendo reducir sus efectos mediante campañas de difusión sobre medidas de seguridad básicas en los usuarios de la red.

- Siguiendo en la misma línea con el caso arriba mencionado es recomendable el empleo de programas antivirus y/o firewalls de fabricantes conocidos para mantenerse ligeramente seguro y que posean capacidades para identificar spyware, adware, riskware, o sus variantes;

aunque la mayoría de estos productos incorporan tales características, también se sugiere que los mantengan actualizados para una mejor detección de los mismos.

- Otra de las situaciones preocupantes a analizar son las actividades que se realizan por la red, por lo que los juegos en línea son la atracción principal para los niños y en estas circunstancias los delincuentes están a la caza de ellos, incitándolos a visitar sitios sospechosos con anuncios de beneficios o nuevos niveles de juegos y para la cual solicitan información sobre números de cuentas de sus progenitores y que en ciertas situaciones los hijos conocen o encuentran formas de obtenerlas y proporcionarlas ingenuamente o que por situaciones diarias del hogar los padres brindan sin ningún cuidado. Desde ese punto de vista, el controlar las actividades que los hijos realizan por internet es además de una forma de prevención, un pretexto para compartir momentos agradables con ellos.
- Para un mejor nivel de confiabilidad mantenga una política de cambio de contraseñas de manera periódica, en la que utilice contraseñas más fuertes para proteger sus datos. Se recomienda que exista diversidad en la construcción de sus passwords mediante el uso caracteres alfanuméricos, caracteres especiales y en combinación, con una longitud mínima de 8 caracteres y que pueda recordar fácilmente, debido a que las contraseñas más largas son mejores al necesitar más tiempo por parte de los agresores para descifrarlas y burlar esa protección. No use nombres de seres queridos (incluidas mascotas) como contraseñas debido a que existe evidencia que demuestran que las personas no tienen conciencia de compartir esta información con los compañeros del trabajo, exponiéndolas con notas adhesivas en los monitores inclusive, y usando ese criterio como primera opción en un cambio de clave. Recuerde que aunque las contraseñas fuertes ofrecen una buena protección contra los incidentes de seguridad, estas no dejan de ser infranqueables para aquellos que pretenden acceder a su información y que pueden estar muy cerca de lo que se imagina.

Algunos mitos sobre la seguridad

Aunque para algunos escépticos este apartado pudiere sonar insólito, no lo es. Ciertas creencias populares y de la más variada existen en las personas que aún no han sido incluidas digitalmente en la sociedad de la información, pues para que suceda la inclusión digital, se precisa de tres instrumentos básicos que son el computador, el acceso a la red, y el dominio y democratización de esas herramientas que mejoren las condiciones de vida y permitan tener posturas admisibles frente a los criterios que definen las tecnologías como una panacea social.

La siguiente lista presenta ciertos dogmas indebidos sobre seguridad, por lo que no espere una actualización que lo proteja de los temas que se tratan a continuación, pues en estas circunstancias usted es el protagonista de su propia seguridad. Sin embargo, no pierda las esperanzas aún, el buen juicio es la clave para que se proteja de estos problemas y si las tiene en cuenta, puede mejorar en forma significativa la seguridad de los sistemas [14]:

1. Tengo un software antivirus y un cortafuegos, eso es suficiente…

En la era del internet aunque tenga instalado en su PC un programa antivirus que es necesario e importante, este no es suficiente. Los nuevos virus van apareciendo y de manera más agresiva es su accionar, por lo que debe considerar actualizar permanentemente la base de datos de virus de la aplicación, de acuerdo a sus esquemas de navegación en la red o de la cantidad de dispositivos portables provenientes de fuera que conecte a su equipo.

De igual manera el contar con un firewall (cortafuegos) que limita el tráfico de datos provenientes de la red evitando ciertos problemas; no es suficiente por tanto debe considerarse una estrategia global que incluya la red interna de la organización.

2. Solo las grandes empresas son objetivo para los hackers

"¿Por qué se molestarían conmigo, que soy un usuario particular o una empresa pequeña?" Los hackers generalmente andan por la red buscando presas fáciles o empresas pequeñas que no invierten en complejos productos de seguridad, lo que las hacen atractivos para realizar sus hazañas.

3. No usar Windows me libera de esta pesadilla

Microsoft® mantiene esquemas de seguridad bien definidas de lo que llama el Trustworthy Computing o Computación Segura y Confiable mediante soluciones de parches y/o actualizaciones de sus productos y su sistema operativo Windows, en sus diferentes versiones, seduce a muchos piratas a realizar sus intentos de ataque. Pero eso no significa que otras plataformas estén a salvo, Linux o Mac OS presenta también vulnerabilidades, en mayor o menor grado

con denegación de servicios, corrección de vulnerabilidades sobre aplicativos instalados, entre otros.

La solución para tener un equipo más seguro es usar una combinación de herramientas que aunque solas harían poco o nada, juntas pondrán una barrera entre el equipo y la red.

4. Estoy seguro porque uso un software que me dice que estoy seguro

Si bien es cierto que las herramientas de escaneo de vulnerabilidades automatizadas pueden encontrar fallas de seguridad, estas no pueden convertirse en la solución, pues estas herramientas están auditando con base a un registro establecido y estándar para la mayoría de servicios, pero afortunadamente cada programa, servicio o aplicativo web es diferente desde el momento de su concepción hasta su puesta en marcha.

5. El sistema puede llegar a ser 100% seguro

La "seguridad absoluta" no existe. Es cierto que varias empresas ofrecen sus productos o servicios, asegurando que solucionan todos los problemas de seguridades habidas y por haber. Lo que siempre puede hacerse es aumentar la seguridad, con un proceso de mejora continua, que sirve para identificar y minimizar los riesgos constantemente.

6. Revise sus dispositivos portables

¿Algo paranoico es tener que revisar cada dispositivo que se conecte al computador? Aunque desee vivir aislado del mundo, que sería una situación muy poco sugerida en esta época de conectividad, pues el compartir información es una de las situaciones que se efectúa a diario en nuestros sistemas y equipos, y con la portabilidad de los dispositivos en boga debe considerarse que por más robusta que sea el plan de seguridad, una simple fisura destruiría todo lo construido.

Conclusiones

Entre las conclusiones que se pueden obtener del presente artículo, se observa que el factor humano es la parte más débil de la seguridad, debido a que no se ha formado una conciencia en ellos sobre la información que manipulan respecto a la importancia y uso y no como vía de crear paranoias. Además se presentan otras situaciones evidenciadas:

- La información que se maneja es confidencial y de responsabilidad de las personas que la posean, en consecuencia no la divulgue tan fácilmente como pudiere.
- Los delitos informáticos no esperan a las víctimas, a veces éstas se prestan para participar del juego, por lo tanto no proporcione información crediticia por correo electrónico u otro medio que le solicite sin investigar previamente.
- Se sugiere asumirla responsabilidad de mantenerse actualizado e informado sobre los últimas informes sobre delitos y/o virus informáticos existentes en la red.
- Considere la instalación de software de seguridad en su equipo, tales como firewalls, antivirus con anti – spyware activados, y de preferencia manteniéndolos actualizados.
- El auge de redes sociales permiten que se recolecte información personal para ser utilizada por criminales y darle un seguimiento posteriormente. En consecuencia, se sugiere el compartir ésta solamente con personas conocidas y de total confianza.
- La seguridad es una constante innovación y capacitación en la que somos partícipes, no espere ser la siguiente víctima.
- Mantenerse informado ayuda, revise otros aspectos sobre seguridad en el sitio web http://www.identidadrobada.com/ especialmente las referencias [15], [16].

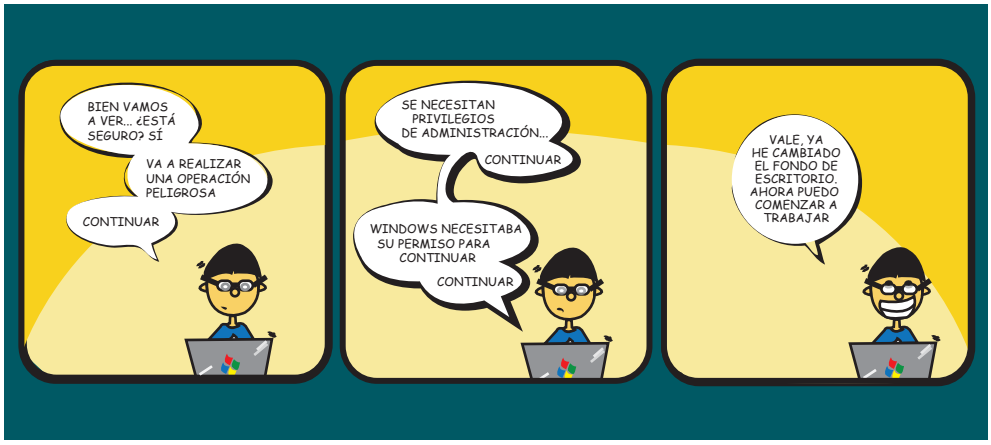

Figura 4. ¿Operación peligrosa en Windows?

Figura 5. Acerca de programas de seguridad en su PC (texto traducido del diseño original al español).

Figura 6. Controlando el spam de la empresa

Figura 7. Una debilidad del respaldo de información

Referencias Bibliográficas

[1] Microsoft: Academia Latinoamericana de Seguridad Informática (s.f.). *Introducción a la seguridad de la información*, Módulo 1. Extraído el 15 de diciembre del 2010 del sitio http://www.microsoft.com/latam/technet/video/alsi.aspx; p. 3

[2] Rossini, R. (s.f.). *Magical Entertainer.* Extraído el 5 de enero de 2011 del sitio http://www.rossinimagic.com/Rleonardocoll.jpg.jpg

[3] Fotos históricas del mundo entero. (s.f.). Extraído el 5 de enero de 2011 del sitio http://www.taringa.net/posts/imagenes/1916194/Fotos-Historicas-del-mundo-entero.html

[4] Wikipedia. *Sociedad de la información.* Extraído el 20 de febrero del 2011 del sitio http://es.wikipedia.org/wiki/Sociedad_de_la_informaci%C3%B3n.

[5] Mattelart, A. (2002). *Historia de la sociedad de la información*. Barcelona: Editorial Paidós.

[6] Microsoft: *Academia Latinoamericana de Seguridad Informática*, op. cit., p. 6.

[7] Wikipedia. Gadget. Extraído el 20 diciembre de 2010 del sitio http://es.wikipedia.org/wiki/Gadget.

[8] Wylder, J. (2004). Strategic Information Security. Boca Raton, Florida: Auerbach Publications, pp. 4, 5.

[9] Stamp, M. (2006). *Information Security: Principles and Practice.* New Jersey: Wiley Interscience, pp. 1, 2; 6, 7.

[10] Bradley, T. (2010). *Cómo detener 11 amenazas encubiertas para la seguridad.* En PCWorld Ecuador, edición de Mayo, pp. 34 – 39.

[11] PhishTank. (s.f). PhishTank: Out of the Net, into the Tank. Extraído el 25 de febrero del 2011 del sitio http://www.phishtank.com/

[12] Stats Phishing. (2010). *Estadísticas sobre phishing a sitios identificados.* Extraído el 25 de febrero del 2011 del sitio http://www.phishtank.com/stats/2010/03/

[13] Stats Phishing. (2011). *Estadísticas sobre phishing a sitios identificados.* Extraído el 25 de febrero del 2011 del sitio http://www.phishtank.com/stats/2011/03/

[14] Portantier Information Security. (s.f.). *Mitos sobre la seguridad de la información.* Extraído el 25 de febrero del 2011 del sitio http://www.portantier.com/recursos/publicaciones

[15] Identidad robada. (s.f.). *Consejos de seguridad.* En el sitio web http://www.identidadrobada.com/consejos/

[16] Identidad robada. (s.f.). *Por delante del cibercrimen.* En el sitio web http://www.identidadrobada.com/por-delante-del-cibercrimen-3/

[17] CRYPTEX (s.f). *Seguridad de la Información.* Extraído el 26 de febrero del 2011 del sitio http://seguridad-informacion.blogspot.com/