LA COTIDIANIDAD DE LA SEGURIDAD INFORMÁTICA

Pedro Javier Guantiva Acosta
Ingeniero de Sistemas
Estudiante de Especialización en Seguridad Informática
Seminario de Investigación Aplicada – SIA 6
Universidad Piloto de Colombia
guantivajav@gmail.com.co

RESUMEN: La seguridad informática ha tomado una gran importancia en los último años, en la medida en que los consumidores de la tecnología han venido simplificando sus actividades diarias con el uso de dispositivos tecnológicos, que ofrecen servicios en la red que van desde una conversación instantánea con un amigo, la compra de un libro o la realización de una transferencia bancaria. Las amenazas informáticas que existen en la web, actualmente atacan en gran medida a las empresas y a las personas en común, con el fin de hurtar su información y llevar a cabo acciones delictivas en contra de ellas. Es así como el papel fundamental de la seguridad informática, se refleja en los mecanismos que se adoptan para blindar la información de cada una de las personas o empresas que la implementen. Por lo tanto, es necesario entrar a pensar que la seguridad es responsabilidad de cada individuo y no solamente de las organizaciones.

PALABRAS CLAVE: amenaza, consumidor de tecnología, individuo, información, seguridad informática.

ABSTRACT: Information Security has taken a great importance in the last years, to the extent that consumers of technology have been simplifying their daily activities with the use of technological devices that provide network services ranging from an instant conversation with a friend, buying a book or making a bank transfer. The threats that exist on the web, now attack largely to companies and individuals in common, in order to steal your information and carry out criminal actions against them. Thus, the critical role of information security, is reflected in the mechanisms adopted to shield the information from each of the individuals or companies that implement it. Therefore, it is necessary to go to think that security is the responsibility of each individual, not just organizations**.**

KEY WORDS: consumer technology, information, information decurity, threat, simplifying.

1. INTRODUCCIÓN

Los sistemas informáticos hoy en día representan la solución a grandes problemas de empresas y personas, en cuanto al manejo de su propia información, la simplificación de tareas cotidianas, suplir necesidades de comunicación desde un ámbito social o comercial, entre otros aspectos. Con el transcurso de los días y el avance constante de la tecnología, cuyo fin es ofrecer mayores beneficios a sus consumidores, las amenazas y ataques informáticos también han aumentado en cantidad, así mismo su evolución y sofisticación ha sorprendido a la comunidad informática.

Es así como la seguridad informática desempeña un papel importante en todo lo referente a la protección de la información de personas y organizaciones, sobre todo aquella que es considerada como confidencial (cuentas bancarias, contraseñas de portales bancarios, correos electrónicos, redes sociales, etc.). En el ámbito empresarial la información se puede encontrar en diversos medios de almacenamiento, como los digitales, impresos, cintas de respaldo, entre otros;

con lo cual si no se cuenta con los controles adecuados de protección, la información puede ser vulnerada y utilizada para acciones delictivas las cuales pueden llegar a convertirse en defraudaciones de gran valor para el individuo u organización que las experimenta.

Es así como se debe pensar más en que la seguridad informática es mucho más cotidiana de lo que se considera, pues el entorno actual de las personas y organizaciones tiene una gran interacción con la tecnología, ya que han depositado en ella toda la confianza para simplificar actividades rutinarias u operativas, almacenar información personal y organizacional, y entre otros aspectos, se han generado nuevas tendencias de comunicación en ámbitos de redes sociales llegando al punto de producir una necesidad de consumo por parte de los usuarios que acceden a dichas redes.

2. LA SEGURIDAD INFORMÁTICA Y SU APLICABILIDAD

Actualmente el ser humano ha dispuesto mayor interés en fortalecer su propia seguridad, la de su familia, su ámbito laboral, etc. Uno de los aspectos más relevantes para proteger en un ámbito cotidiano y el cual se convierte en el mayor activo de una persona u organización, es la información, la se ha convertido en el objetivo principal de los delincuentes con fines lucrativos. Teniendo en cuenta que el hombre siempre ha dispuesto de herramientas para la ejecución de sus tareas, simplificar sus procesos y obtener mayor eficiencia; es posible cuestionarse cuál ha sido el factor que ha influido en el transcurso de los años para que las personas adopten más medidas en pro de su seguridad; si se mira atrás y de forma retrospectiva, 30 años atrás existían problemas de delincuencia, el objetivo principal para la delincuencia era entrar de forma física y organizada a un entidad y extraer los bienes de mayor valor y poder adquisitivo; con lo cual no se manejaban de forma común los conceptos de “malware”, “phising”, “spoofing”, etc., la información tenía controles de acceso efectivos pero en la mayoría de los casos de forma manual, con lo cual las personas y las organizaciones no les preocupaba de forma incisiva lo que sucediera con ella.

A medida en que la tecnología empezó a convertirse en la aliada de las personas y las empresas, sobre todo porque permitía obtener simplicidad de los procesos que ejecutaban a diario, almacenar y ordenar grandes volúmenes de información y datos en lo que ahora se llamaba un “sistema de información”, gracias a su gran capacidad, versatilidad y facilidad de manejo; los hábitos de las personas y las organizaciones a la hora de administrar su información, empezaron a cambiar notablemente y mejorar notablemente en términos de eficiencia cada vez que se lograba simplificar un proceso.

Pero al tiempo en que la tecnología evolucionaba y su consumo se incrementaba por más usuarios; la delincuencia no se quedó atrás y es así como en la medida en que encontraron falencias de seguridad en las empresas, sus objetivos tomaron un nuevo rumbo y empezaron desarrollar amenazas informáticas con el fin de traspasar las barreras de protección de las organizaciones y lograr llegar al centro de sus sistemas de información; el premio a estas intrusiones era el robo de información confidencial y sensible de las compañías [1].

Es así como se ha llegado a la necesidad de crear y establecer estándares y protocolos, implementación de reglas de acceso a los sistemas; con el fin mitigar y reducir el riesgo de penetración a la infraestructura de una empresa, siendo allí en donde reposa el activo más importante, “la información”.

La seguridad informática comprende componentes de software y hardware, protegiendo los elementos más vulnerables a amenazas o ataques, pero se debe tener en cuenta que estos eventos en la mayoría de los casos se asocian al tipo “informático”, la información puede estar expuesta a fallos de infraestructura a raíz de situaciones que no han sido previstas con anterioridad, o por condiciones inevitables que se escapan de todo plan de contingencia existen (ej. Desastres naturales como inundaciones terremotos, ataques terroristas, etc.) [1]. Gran parte de los líderes mundiales y quienes cuentan con todo el andamiaje militar y bélico para afrontar guerras, exponen sus temores hacia la posibilidad de que con base a un adecuado manejo de las tecnologías de telecomunicaciones e información, estas sean la causa necesaria para generar un campo de batalla entre diferentes estados o naciones.

Actualmente en los Estados Unidos, las empresas son obligadas a implementar “La ley orgánica de protección de patos”, la cual busca proteger los datos sensibles de cualquier tipo de robo o pérdida de calidad, con lo cual, de llegar a presentarse generaría innumerables pérdidas de información que podría llegar afectar a empresas, gobiernos, ciudades, etc.

3. EL USO DEL INTERNET Y LOS USUARIOS

Hoy es una realidad el uso del internet en la cotidianidad del hombre, actividades como realizar compras de bienes y servicios en línea, realizar pagos de obligaciones bancarias, servicios de entretenimiento, círculos sociales en redes sociales, entre otros más aspectos; han generado con el transcurrir de los años una dependencia a la tecnología, con lo cual el término “actual” ha tomado una connotación efímera, pues la innovación del momento pasa a ser obsolescencia en cuestión de días. Uno de los factores negativos que ha tenido esta “dependencia” ha sido la delincuencia digital, en donde reportes de cibercrimen indican que uno de cada cinco personas conectadas a la red son víctimas de ataques informáticos, estos pueden presentarse a través de las redes sociales, teléfonos inteligentes, establecimientos de café internet, entre otros [2].

Para el año 2012 y según un informe de la empresa Symantec, 9,7 millones de colombianos fueron víctimas de delitos informáticos, los cuales hacen parte de los 556 millones en el mundo que fueron afectados por este flagelo. Los medios más utilizados se relacionan con elementos de alta cotidianidad para las personas, como el uso de redes sociales, teléfonos de última generación y con gran desempeño orientado a la conexión web. Los usuarios que fueron afectados por un delito informático, estuvieron implicados en temas de suplantación de usuarios dentro de las redes sociales, estafas, pérdida de información por la infecciones de virus, malware, spyware, entre otras amenazas; todo esto gracias a la ejecución de programas inseguros sin la respectiva precaución del usuario.

En la actualidad se ha venido presentado un alto número de casos de violación de privacidad, el espionaje informático como se le conoce hoy en día, está generando un alto nivel de preocupación en los usuarios, dado que consideran que su privacidad ha sido vulnerada y expuesta ante los delincuentes informáticos. En el año 2013 un estudio realizado por la empresa Eset, reveló que para el 2014 en latinoamérica los usuarios sufrirán de problemas relacionados con la pérdida de seguridad en internet, el cibercrimen, la proliferación de virus informáticos en estaciones de trabajo, teléfonos inteligentes, etc.

Según el informe mencionado, los usuarios de internet se sienten vulnerables de manejar su información en la nube, pues la evolución del cibercrimen ha puesto en jaque un sin número de esquemas de seguridad de las empresas que prestan este servicio. Uno de los factores más relevantes que contribuyen con esta situación, obedece a la gran masificación del uso de internet y los servicios integrados que allí se encuentran, en donde el usuario común ya ha empezado a cuestionarse en qué condiciones de seguridad y privacidad se encuentra la información que almacena en los distintos sitios web que utiliza con cierta frecuencia.

Es así como varios países han ido implementando distintas regulaciones y normativas, con el fin de proteger a los usuarios de la web acerca de los contenidos que a diario consumen, dado que es una gran realidad que en internet se pueden encontrar distintas temáticas que pueden llegar a afectar el aspecto social de las personas; entre estos temas están la piratería, fraude electrónico, pedofilia, pornografía, asuntos de seguridad nacional, etc. Existen algunos ejemplos muy sonados acerca de vulneración de información, como el sucedido con Edward Snowden quien en 2013 expuso ante la opinión pública una gran cantidad de información confidencial y de ámbito de seguridad nacional para los Estados Unidos.

Por lo tanto, la privacidad de los datos almacenados en la nube por parte de los usuarios y basados con lo sucedido en el caso de Edward Snowden, han generado una gran preocupación por parte de los usuarios al tener la sensación de exponer su privacidad al ámbito público, es por esto que ya se piensa en términos de “seguridad de la información”, pues es una realidad que el auge que hoy en día tienen las redes sociales como medio de comunicación para los usuarios, han incrementado los volúmenes de información personal que es subida por parte de estos, sin que en algunos se tengan en cuenta los controles necesarios para proteger los datos sensibles que afecten su propia su seguridad.

Es posible determinar que la falta de concienciación de los usuarios sobre controles de seguridad que deben tener en su propia protección, en algunos casos se llega a la consideración de implementar una serie de herramientas informáticas como “firewall”, “ids”, “antivirus”, etc., con la percepción de haber eliminado las brechas que exponen la información, sin tomar en cuenta los hábitos humanos que en la mayoría de los casos pueden representar la mayor amenaza para la vulneración de la información. Esta condición se puede corroborar con la siguiente tendencia:

Mayor preocupación por la privacidad en internet → implementación de soluciones de seguridad → falta de concienciación en aspectos de seguridad de la información → la información y privacidad del usuario es comprometida.

Por lo tanto, el solo hecho de tener una gran preocupación sobre la privacidad de la información, no significa que se tomen las medidas correctas y que solo con el uso de herramientas se cierren las brechas de exposición de información de forma suficiente; por el contrario, las personas y las organizaciones deben invertir mucho en la concienciación propia, dado que siempre el eslabón más débil para la seguridad informática será el “usuario” [3].

4. LA SEGURIDAD INFORMÁTICA Y EL ÁMBITO EDUCATIVO

Con la entrada de las nuevas tecnologías y el acceso a las redes sociales, se ha presentado un cambio considerable en la forma en que dos personas pueden llegar a relacionarse, pues la tendencia actual apunta hacia el uso de herramientas tecnológicas que han venido suprimiendo el contacto físico y personal.

Este efecto se ha venido notando con especial evolución dentro de la población infantil y adolescente, pues ellos han encontrado en el internet la respuesta a sus necesidades de comunicación, diversión, educación y por supuesto el acceso a las redes sociales; es aquí en donde se presenta una de las mayores vulnerabilidades para dicha población, pues se presenta una gran probabilidad de exposición a ser engañados y por consiguiente caer en algún tipo de abuso por parte de personas inescrupulosas.

Es aquí en donde la seguridad informática empieza a cuestionarse sobre cuál es el alcance que hoy en día tienen los menores de edad sobre el internet, cuáles son sus hábitos de navegación y sobre todo, cuál es el control y vigilancia que ejercen los padres de familia sobre sus hijos y los contenidos que estos últimos consultan.

Fig. 1 Vulnerabilidad infantil / adolescente [4]

En la actualidad dentro del ámbito escolar es muy frecuente escuchar sobre el “matoneo” o “bullying”, pero con el acceso a las nuevas tecnologías, las amenazas ahora se realizan por este medio, es ahora como el término ha sido ajustado a esta nueva realidad y se habla ahora de “ciberbullying”, término que hace referencia a un mecanismo de amenaza personal a través de una red social.

Una de las principales causas de matoneo o “ciberbullying” en la población estudiantil, obedece a la exposición excesiva de datos privados tanto propios como ajenos, aspecto que está sirviendo de insumo para los delincuentes informáticos, como los hackers, los ingenieros sociales, etc.; quienes son los encargados de inducir a los usuarios de dicha población, a ingresar a páginas de pornografía, a páginas inseguras para descarga de software malicioso, etc.

Un hecho muy notable pero negativo, es la promoción de la violencia estudiantil a través de las redes sociales, cuyos abusos están llevando a las víctimas del “ciberbullying” a hacer silencio y no llegar a realizar algún tipo de denuncia sobre este delito, pues son amenazadas por medio de canales electrónicos y de forma constante; lo que está generando que la población afectada esté cayendo en enfermedades de tipo emocional y mental; esto gracias a los cuadros de depresión sobre los cuales caen las personas afectadas por este mal, cabe decir que en los peores casos, se ha presentado casos de suicidio a raíz de esta situación [4].

A pesar de este la aparición del fenómeno negativo del “ciberbullying”, según el Ministerio de Tecnología de la Información y Comunicación

(MinTIC), asegura que para el año 2013, 8 de cada 10 colombianos se mostrarán activos en la web. Según un estudio por parte de la Universidad de la Sabana en Colombia realizado a estudiantes entre los 12 y 18 años de edad, con el fin de conocer sus hábitos de navegación, arrojó respuestas como las siguientes:

- El promedio de edad de iniciación de los estudiantes en internet es de los 9 años.
- El 68% de los adolescentes se conectan diariamente, el 30% entre 3 y 6 días y el 2% una o dos veces a la semana.
- El 32% de estudiantes se conectan tres horas al día, un 20% cinco, el otro 20% entre una y tres y el 6% restante una hora o menos.
- El 89% de los jóvenes se conectan desde su casa, el 5% desde el colegio, el 4% desde una consola de videojuegos y el 2% desde un café internet.
- 27% ingresan a Facebook, el 2% a Skype, el 17% a Google, el 1% a YouTube, el 10% a Hotmail, el 6% chatea, el 3% juega en línea, el 2% ve pornografía y el 1% hace apuestas.
- 45% de los jóvenes se conectan para interactuar, el 19% por distracción, el 13% para descarga música y videos, el 12% para fines académicos, el 7% para buscar información de interés personal, el 3% para conocer gente y el 1% para escapar de la cotidianidad [4].

Por lo tanto, es posible demostrar que los adolescentes de hoy en día, se encuentran constantemente conectados a internet y cuya exposición a un cibercrimen, no es controlada y tenida en cuenta por parte de los padres del presente. Es así como se vuelve prioritario que existan espacios de interacción entre padres e hijos, donde los primeros deben estar atentos y controlando el acceso a la internet por parte de sus hijos.

Para que la seguridad informática tenga efecto en el ámbito educativo, es necesario que los docentes de las instituciones en conjunto con los padres de familia, diseñen e implementen estrategias que permita proteger a sus hijos de ataques de abuso informático, para ello es muy requerido que los padres de familia tomen conciencia, sobre las libertades que conceden a sus hijos al momento de interactuar con internet.

No obstante, es necesario brindar la ayuda necesaria al menor que ha sido víctima de acosos informático, enseñarle los diferentes mecanismos que existe para protegerse de abusos, así mismo, se debe llegar a acuerdos entre padres e hijos sobre el alcance de la navegación y así no exponer a ningún miembro de la familia a temas de abuso y acoso informático.

5. SEGURIDAD INFORMÁTICA EN EL ÁMBITO EMPRESARIAL

El auge que han tenido las amenazas hacia los sistemas informáticos, con el fin de lograr sustraer información confidencial de un individuo u organización, alterar el normal funcionamiento de un servicio web prestado por una empresa a sus clientes, o el simple hecho de vulnerar a los usuarios a través de portales web falsos, envío de elementos maliciosos a través de correos electrónicos, descarga de productos en páginas que cautivan al usuario pero que esconden sus intenciones reales; está ocasionando que la confidencialidad, integridad y disponibilidad de la información de una organización se vea cada día más expuesta a ser comprometida y utilizada de forma inapropiada, con el fin de alcanzar objetivos de índole delictivo con lo cual puede llegar a impactar el valor reputacional de un empresa y así provocar su extinción en el mediano plazo.

Según el concepto por parte de Jon Parkes (vicepresidente de preventa de Intel Security), para el año 2020 habrá un aproximando de 15 billones de dispositivos que serán utilizados para la comunicación y el almacenamiento de la información, en este aspecto, las empresas no serán ajenas a este fenómeno dado que en hoy en día basan su operación en el uso de estas herramientas tecnológicas, las cuales deberán estar comunicadas constantemente entre sí transportando y almacenando la información sensible de una organización, la cual corresponde a su mayor activo; es por esto que se debe hacer uso de la mayor cantidad de elementos que la seguridad informática ofrece para la protección de la información, pues ya es una realidad que los activos materiales de una organización se están convirtiendo en activos digitales los cuales se encuentran almacenados en distintas instancias como “data center”, “sistemas virtualizados” o almacenados en la “nube”; por tal motivo las organizaciones deben contar con la mayor seguridad y protección posible cada vez que exista

una interacción operacional de dichos activos con elementos tecnológicos.

Sin embargo, uno de los aspectos que aún es común en las organizaciones, es la falta de inversión constante en temas de seguridad informática, esta situación obedece en gran medida a las limitantes presupuestales de las empresas, las cuales a pesar de ser conscientes de la necesidad de implementar soluciones de seguridad, enfocan sus esfuerzos económicos en satisfacer otras prioridades de negocio [5].

6. ALTERNATIVAS PARA UNA SEGURIDAD INFORMÁTICA EFECTIVA

Tanto las personas como las organizaciones, pueden contar con diversas alternativas para proteger su información sensible e incrementar la privacidad de sus datos que se exponen en internet, entre las medidas más comunes se encuentran los siguientes aspectos [6]:

- Instalación de herramientas de antivirus, en los equipos sobre los cuales se accede a internet.
- Implementación de soluciones de cortafuegos (firewall), con el fin controlar el tráfico de navegación hacia internet.
- Navegar en sitios seguros y de confianza, los cuales no expongan las condiciones de seguridad de los equipos de cómputo, ya sea por descargas silenciosas de códigos maliciosos o infección de virus informáticos, que pongan en riesgo la información almacenada.
- Protección de los mecanismos de comunicación, mediante el uso efectivo de contraseñas con un alto nivel de seguridad.
- Ejecución de copias de respaldo de la información, en dispositivos de almacenamiento externo tales como: discos externos, cintas de seguridad, la nube, custodia de dispositivos flash, entre otros.
- Cifrado de archivos, carpetas o discos, que contengan información sensible.
- Aplicar técnicas de borrado seguro de archivos, es importante saber que en la mayoría de los casos es posible recuperar un archivo o carpeta con información, si éstos han sido solamente eliminados del computador personal, es por ello que es muy conveniente la utilización de herramientas especializadas para no dejar rastro alguno de la información eliminada.
- Uso del software libre no siempre es la mayor garantía para la seguridad informática, es conveniente que las herramientas utilizadas estén muy bien calificadas para así evitar mayores incidentes de seguridad.
- Tomar medidas sobre el acceso físico a los equipos de cómputo, es de vital importancia que se controle el compartir carpetas en red de modo público, con lo cual cualquier usuario puede acceder a información confidencial y así mismo vulnerarla.

Es posible contar con muchas más alternativas de protección de información para personas comunes y empresas, pero es claro que los riesgos de tecnología para una organización han cambiado con el transcurrir del tiempo, en donde las amenazas son cada vez más especializadas. Por lo tanto, la protección de la información debe ser uno de los objetivos más importantes y prioritarios para una organización y sobre todo para su departamento de tecnología, pero no a veces no basta solo con implementar infraestructura tecnológica en una organización que apunte a controlar amenazas de spam, malware, accesos no autorizados a la red, etc.; si dentro de la misma organización no se ha generado la necesidad la implementación de modelos de gestión y gobierno, que contribuyan con el aseguramiento de los procesos internos y sobre todo, de la información que es generada en cada uno de ellos.

Es así como una organización puede hacer uso de la implementación de modelos de gestión y dirigidos hacia la “seguridad”, entre los más distinguidos se encuentra:

- Sistema de Gestión de Seguridad de la Información – ISO 27001: Es un estándar internacional que presenta los distintos requisitos para la implementación de un sistema de gestión, en donde siguiente el modelo PHVA, puede controlar todos los procesos que intervienen en la seguridad de la información, logrando así establecer controles, responsables, métricas, etc., con lo cual una organización puede llegar a fortalecer la confidencialidad, integridad y disponibilidad de la información, a través de una adecuada gestión del riesgo, un entendimiento

riguroso de los requerimientos de seguridad de la información en la compañía [7].

- COBIT: Es un marco de gestión y control, que brinda las directrices y buenas prácticas para administrar las actividades de tecnología de la información. Este modelo también responde a la ejecución de una serie de procesos, con el fin de brindar un enfoque de negocio a la organización, en alineación a los objetivos corporativos de la misma, por lo tanto su modelo lo enfatiza en el gobierno y control de los procesos de una organización, siguiendo una serie de buenas prácticas que contribuyan con el aseguramiento de la confidencialidad, integridad y disponibilidad de la información [8].
- Implementación de políticas y procedimientos de seguridad, que determinen las directrices necesarias para la protección de la información dentro de una compañía.

Por lo tanto, es necesario que exista una conciencia de control dentro de una organización, para que la información pueda fluir de manera segura y de forma eficiente, sin que se presenten situaciones de riesgo que pongan entre dicho la reputación de una compañía, si ésta se viera expuesta al compromiso de su información. Es así como existen modelos y estándares de gestión que conllevan a blindar los procesos internos y externos relacionados con la información; herramientas informáticas que ofrecen grandes beneficios de protección de la información y así un sin número de soluciones; pero todo esto pierde validez si no existe un alto compromiso de la alta dirección en apoyar las iniciativas de implementación para modelos de gestión; así mismo, debe existir un alto compromiso por parte de todos los usuarios de una organización y que acceden a información sensible de la compañía como fruto de su operación diaria, en este aspecto se referencia la conciencia que un usuario debe tener al momento se dar cumplimiento a las normas y políticas que son definidas por la alta dirección, en relación a la ejecución de los procesos operativos bajo el enfoque de protección de la información que se ve involucrada.

7. CONCLUSIONES

La seguridad informática en la actualidad, representa la mejor arma de defensa para empresas y hogares, ante la exposición inminente a un ataque informático y que ponga en riesgo la información de una organización.

Para un delincuente informático existen diversos ambientes con el fin de obtener información de manera fraudulenta, los cuales van desde el ámbito laboral hasta llegar al ámbito personal, solo con el fin de encontrar una puerta de entrada para saquear la información de una organización.

No siempre la solución para la seguridad informática se hacer grandes inversiones económicas para la adquisición de herramientas, es necesario aplicar un conjunto de normas y políticas que apalanquen un sistema de gestión de seguridad de la información, el cual sea aplicado y cumplido por cada miembro de la organización, sin importar su nivel.

La pérdida y exposición de la información personal al no tener implementadas las medidas necesarias, hacen de la persona que está navegando en internet, una presa fácil para el delincuente informático.

Es necesario que en la medida en que evoluciona la tecnología, las personas y las organizaciones sean responsables de su uso, esto solo se logra adoptando una postura responsable y consciente de los riesgos existentes al momento de exponer la información sensible de una persona o de una organización.

REFERENCIAS

[1] Hoy Digital. *Seguridad informática: Más allá que la Pérdida de Información Valiosa.2013. Recuperado el 03 de agosto de 2015 de la página web: http://hoy.com.do/seguridad-informatica-mas-alla-que-la-perdida-de-informacion-valiosa/*

[2] El Mundo .Com. *Seguridad informática, necesidad real del usuario TIC. 2012. Recuperado el 03 de agosto de 2015 de la página web: http://www.elmundo.com/movil/noticia_detalle.php?idx=207082&*

[3] Eset LA. *Tendencias 2014: El desafío de la privacidad en Internet. 2013. Recuperado el 04 de agosto de 2015 de la página web: http://www.eset-la.com/pdf/tendencias_2014_el_desafio_de_la_privacidad_en_internet.pdf.*

[4] Sisgecom. *Acoso en la Red: "Ciberbullying" al Asecho. 2014. Recuperado el 05 de agosto de 2015 de la página web: http://sisgecom.com/tag/seguridad-informatica/*

[5] Portafolio.co. *La seguridad informática se contrajo 15 % en ventas. 2015. Recuperado el 10 de agosto de 2015 de la página web: http://www.portafolio.co/negocios/la-seguridad-informatica-se-contrajo-15-venta.*

[6] Riseup.net. Asamblea del Hacklab. *Seguridad informática: recomendaciones básicas para los usuarios. 2015. Recuperado el 10 de agosto de 2015 de la página web: https://we.riseup.net/hacklab+asamblea/seguridad_informatica*.
[7] Norma ISO 27001:2005. *Sistema de Gestión de la Seguridad de la Información. 2015. Material educativo Seminario de Investigación Aplicada SIA 6. Universidad Piloto de Colombia.*
[8] COBIT 4.1. *Control Objectives for Information and Related Technology. 2015. Material educativo Seminario de Investigación Aplicada SIA 6. Universidad Piloto de Colombia.*