Seguridad informática y seguridad de la información en el mundo, como factor de enseñanza en Colombia

Parra, Carlos Humberto
Universidad Piloto de Colombina
Bogotá, Colombia
pcarlosh2@hotmail.com

Abstract- This document wants to show a topic that since not long ago has become very complex and equality important in the world, as it is information security. Countries, enterprise and the people although have seen the last cybercrime and massive theft of information, don't takes awareness and many organization or government agencies not have enough security for guarantee data and information.

Resumen— En este documento se aborda un tema que en muy poco tiempo se ha convertido en algo muy complejo y de especial importancia en el mundo entero: la seguridad de la información. Los países, las empresas e incluso las personas, a pesar de tener conocimientos de cada vez más asombrosos y perjudiciales sobre delitos informáticos y robos masivos de información, no toman conciencia ni gestionan los riesgos relacionados. De esta forma, aún muchas organizaciones públicas y privadas, no tienen la suficiente seguridad para garantizar los datos e información.

Índice de términos— seguridad informática, seguridad de la información, delitos informáticos, hackers, malware, defensa en profundidad, dato sensible.

I. INTRODUCCIÓN

Internet apareció como un proyecto de investigación de redes de conmutación de paquetes dentro del ámbito militar en la década de los 60, no obstante lo que surgió como un proyecto se convirtió rápidamente en un acceso a la información y las comunicaciones con la colaboración de universidades, empresas y organizaciones privadas que participaron en este desarrollo.

Años más tarde, la red global se volvió de uso público y los avances informáticos no pararon de crecer, llevando aceleradamente el desarrollo de la tecnología a niveles jamás imaginados. Sin embargo, con este importante logro de la humanidad llegan también nuevos retos, investigaciones y definiciones en el ámbito tecnológico que dan paso a la era digital y con ésta, a los denominados ataques informáticos, que siendo cada vez más frecuentes, han hecho que términos tales como hackers, crackers, virus, malware, y delitos en la red, no sean ajenos a una parte importante de la población y las organizaciones en el mundo.

Es aquí donde la seguridad de la información cobra gran importancia al minimizar la fuga o pérdida de información de las personas, las empresas y el gobierno, dándole el valor necesario a lo que hoy se posiciona como el activo más preciado: la información.

A primera vista la seguridad de la información y la seguridad informática pueden parecer lo mismo, sin embargo cada una tiene objetivos y alcances claramente diferenciados: la seguridad de la información *nos habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y esquemas normativos que nos exigen niveles de aseguramiento de procesos y tecnologías* [1], mientras que la seguridad informática *se encargaría de las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros* elementos [2].

De acuerdo con lo anterior, se puede concluir que hay una estrecha relación entre las dos prácticas que tienen alcances diferentes. En la siguiente gráfica se presenta con mayor claridad dicha relación dentro de una organización. Las áreas sombreadas con color azul hacen referencia a la seguridad de la información y las áreas de color amarillo a la seguridad informática.

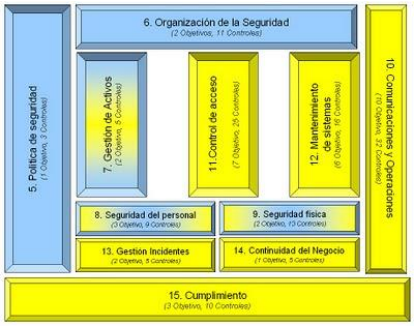

Figura 1. Seguridad de la información y seguridad informática

II. LA IMPORTANCIA DE LOS PILARES DE LA SEGURIDAD PARA PROTEGER LA INFORMACIÓN

Para las personas y organizaciones, la información es, ha sido y será el motor para su funcionamiento, uno de sus mayores activos con un valor incalculable para las mismas. La seguridad de la información se enfoca en preservar esencialmente la confidencialidad, integridad y disponibilidad de la información; además puede involucrar otras aristas tales como la autenticidad y no repudio, las cuales se definen a continuación:

Confidencialidad: la información solo puede ser acedada y utilizada por el personal de la empresa que tiene autorización para hacerlo [3].

Integridad: se refiere al momento que la información no ha sido borrada, copiada o modificada, es decir cuando se conserva tal como fue creada o enviada desde cualquier medio desde su origen hacia su destino [4].

Disponibilidad: se refiere a que la información facilitada en cualquier medio digital o software se encuentre disponible para su procesamiento [5].

Autenticidad: en este pilar se defina aquella información legítima, que al ser interceptada, puede ser copiada de su formato original a pesar de que la información sea idéntica [6].

No repudio: es el proceso que garantiza que el emisor no pueda negar lo que hizo. Equivale al término “aceptación” y es una de las características más difíciles de garantizar [7].

Las empresas u organizaciones deben garantizar al menos los tres primeros pilares para asegurar y proteger los datos e información que resguardan, demostrando así un excelente nivel de

seguridad de la información. La siguiente gráfica ilustra las interrelaciones de los tres pilares.

Figura 2. Tres pilares fundamentales de la información

El acelerado ritmo de cambio de las Tecnologías de la Información, que tienen un papel fundamental en un mundo globalizado y cada vez más competitivo, hace necesario avanzar en el despliegue de estrategias de seguridad de la información también cambiantes, que acompasadas con los más recientes avances y nuevas demandas de servicios, eviten crear falsas sensaciones de seguridad que lleven a una zona de confort.

En este sentido, debe ser una prioridad para toda organización incorporar en su modelo de negocio lo concerniente a la seguridad de la información, involucrando personas, procesos y tecnología en las tendientes dinámicas a garantizar los tres pilares citados anteriormente. Cabe anotar que el eslabón más débil de la cadena son las personas y por tal razón se hace necesaria la implementación de programas de sensibilización y capacitación en el uso y manejo de la información de acuerdo a su nivel de clasificación.

Por lo anterior expuesto y por no darle la importancia que realmente se merece el tema de seguridad de la información una de las grandes amenazas que consideran las compañías, es el ciber riesgo. Se ha convertido una verdadera preocupación en los últimos años el denominado riesgo cibernético que está en aumento gracias a los delitos informáticos que las empresas han sufrido a nivel mundial. Un informe realizado en el año 2015 revela que el ciber riesgo y la violación de datos son las principales preocupaciones de los empresarios [8].

Un ciber riesgo es un ataque que implica pérdida financiera, daño de la reputación de la empresa o interrupción del negocio resultado de una falla en sus sistemas de una información. Es claro que estos ataques son causados por ciber criminales o crackers y no solo impactan la productividad y reputación de una compañía, por no tener una infraestructura tecnológica y un excelente plan bien implementado de seguridad de la información, esto puede llegar a generar reclamos por parte de terceros que de una u otra forma se ven afectados por dichos ataques.

Conocido lo anterior ha dado lugar a un nuevo término en el ámbito tecnológico y de la seguridad en la información como lo son los denominados ciber seguros o CyberEdge que presta la aseguradora AIG y busca amparar el gasto asociado con la investigación por parte de autoridades reguladoras así como los relacionados con la restauración de datos electrónicos en caso de una infracción de seguridad [9].

Es significativo para las empresas estar al día con las amenazas informáticas y con ayudad de personal calificado y experto en estos temas puedan solucionar y más aún prevenir cualquier inconveniente causado por un ciber ataque, adquirir un ciber seguro de los hoy brindados por las empresas en el contorno tecnológico para minimizar la pérdida de información y asegurar los datos brindando más confianza a los cliente, podía ser una solución para los riesgos que corren las empresas al estar en el mundo del Internet.

Empresas líderes de antivirus informan un fuerte incrementos de hasta un 100% en el número de ataques cibernéticos frente al año pasado y estas lo han bautizado como el año de los delitos informáticos.

La compañía ha bloqueado 2.200 millones de ataques durante los primeros tres meses del 2015, el doble que el mismo trimestre del año anterior [10].

Se consideran varios retos a la hora de hablar de seguridad de la información. Uno de ellos puede ser el proteger la información privada, dado que demasiada información que se está generando en la web se da por acciones de las personas., por esto es se deben generar estrategias que permitan que dicha información sea protegida de manera adecuada. El manejo de la información se convierte en otro reto de seguridad ya que se debe continuar trabajando al interior para que las personas se enteren que de lo que están manejando y sepan el verdadero valor de la información. Es claro y muy importante que se debe volver un hábito en una empresa brindar entrenamiento y capacitación sobre el manejo que le debemos dar a los datos y la información ya que como ya se ha dicho anteriormente, este se convierte en activo valioso. Esto nos lleva a otro reto de igual importancia y que nos ayuda a proteger y hacer proteger los tres principios de la seguridad de la información. : Basta con tener alguno de estos principios comprometidos y las decisiones que se tomen desde la alta gerencia, basadas con esta información serán errados y podrán llevar a la entidad a perder mercado o incluso tener reveses de buena imagen, entre otros.

III. AVANCES TECNOLÓGICOS QUE CAMBIARON EL MUNDO

El mundo se ha ido convirtiendo en lo que se puede llamar "la sociedad del conocimiento", con sus grandes avances, inventos y descubrimientos hechos en materia de tecnología, ciencia e información.

Con la llegada de Internet también han llegado grandes desarrollos y tecnologías emergentes, como lo es el bien llamado Internet de las cosas. En la actualidad objetos personales y electrodomésticos como relojes, neveras, celulares, sistemas asistidos de automóviles, televisores, entre otros, ya son capaces de conectarse a Internet y nos brindan la posibilidad de estar más actualizados e informados de lo que pasa en el mundo; no obstante, estos avances tienen ventajas y desventajas para la humanidad ya que la creciente dependencia de la información y los mayores riesgos relacionados con la seguridad de la misma, pueden afectar el bienestar de las personas y la sostenibilidad de las organizaciones.

Los avances han sido de tal magnitud que hoy en día se diseñan y construyen robots que perfectamente pueden llegar a suplir necesidades en campos que hasta ahora eran exclusivos para las personas. Es aquí donde se muestra claramente que lo que años atrás era ciencia ficción hoy es una realidad en países como Japón, que desde hace ya un largo tiempo vienen investigando estos temas. Y vale la pena hacer mención especial de este país considerando que, con la universidad de Waseda y la empresa Tmsuk, ha desarrollado un robot llamado Kobian que es capaz de transmitir sentimientos de tristeza, felicidad, confusión, enfado u euforia [11].

Pero este no ha sido el único robot creado por los japoneses, dado que en años anteriores se han presentado más desarrollos como el humanoide Aiko Chihara, que es un androide hiperrealista

con apariencia de mujer que trabaja como recepcionista en los grandes almacenes Mitsukoshi, en Tokio [12].

IV. AVANCES TECNOLÓGICOS EN COLOMBIA

Colombia no es la excepción en temas de innovación y tecnología, al contrario quiere estar a la vanguardia *"En 2019, todos los colombianos conectados, todos los colombianos informados, haciendo uso eficiente y productivo de las TIC, para mejorar la inclusión social y la competitividad"* esto indica la visión del Plan Nacional de Tecnologías de la Información y las Comunicaciones 2008 – 2019 (PNTIC) y no podría ser al contrario cuando día a día Internet está hasta en la sopa: encender las luces del apartamento, tomar los signos vitales, solicitar al automóvil que se desplace, son algunas de las acciones que se pueden realizar desde un dispositivo móvil. El llamado 'Internet de las cosas' será una realidad.

Una reciente encuesta realizada en Colombia por el Instituto de Ingeniería Eléctrica y Electrónica (IEEE), relaciona alrededor de 23 tecnologías emergentes en el país, las cuales se listan a continuación:

1. Security cross-cutting issues
2. Open intelectual property movement
3. Sustainability
4. Massively online open couerse
5. Quantum computing
6. Device and nanotechnology
7. 3D integrated circuits
8. Multicore
9. Photonics
10. Universal mamory
11. Networking and interconnectivity
12. Software-defined networks
13. High-performance computing
14. Cloud compiuting
15. The Internet of Things
16. Natural user interfaces
17. 3D printing
18. Big data analytics
19. Machine learning and intelligent systems
20. Computer visión and patter recognition
21. Life sciences
22. Computational biology and bioinformatics
23. Robotics for medical care [13]

Por consiguiente, se genera una gran incógnita y es si el país está preparado para estas nuevas tecnologías.

Dar el salto a la industria TIC, implica muchos cambios que sin lugar a dudas causarán efectos ya sean positivos o negativos. Vale la pena preguntarnos, cuál será el rol del PNTIC y sí las personas son lo suficientemente consientes de los beneficios, responsabilidades y obligaciones que tenemos con la administración y buen uso de las tecnologías. Constituye un gran reto para nuestros dirigentes no solo la puesta en marcha, ejecución y sostenibilidad del plan sino también la generación de normas regulatorias que sobre la materia sean aplicables.

Las tecnologías de la información y la comunicación (TIC) están en constante desarrollo y más en este país que el auge del Internet en general y en dispositivos móviles cada día es más importante y acoge al ser humano. Colombia cada vez va más rápido en cuanto al uso de Tecnologías de Información, esto nos dice un estudio realizado por la multinacional consultora (EVERIS) y el IESE Business School de la Universidad de Navarra en España, estudio que muestra que Colombia se ubica en el grupo más avanzado en materia de Tecnologías de Información y Comunicación. Diego Molano, ex ministro de las

TIC dice "*esto demuestra que Colombia está acelerando cada vez más en materia del uso de tecnologías de y continuara haciéndolo este año*" [14].

V. CONCLUSIONES

El acceso a las nuevas tecnologías es una necesidad indiscutible para cualquier nación, pero ésta debe ir de la mano con la aplicación de una estrategia de interiorización de cultura para el buen uso de las TIC.

La seguridad de la información debe ser apoyada por la academia, el Estado y desde del interior de cada hogar; es aquí donde se debe sembrar la semilla de un futuro con tecnología pero haciendo un uso responsable de ella.

Es necesario identificar los obstáculos que tiene el PNTIC: la falta de recursos, la falta de confianza en la eficiencia, eficacia y efectividad de la administración del Estado, el cambio de mentalidad, una gran labor de concienciación y más aún cuando "Colombia utilizará activamente las TIC como herramienta para la reducción de las brechas económicas, sociales, digitales y de oportunidades" y "un dominio amplio de estas tecnologías en el sector público y privado, es una condición necesaria para reducir la pobreza" una afirmación que nos llevan a pensar si en realidad, se lograrán reducir estas brechas tan significativas en nuestra sociedad.

La información es definitivamente un activo que se debe proteger, desde cualquiera de los ángulos que se le observe.

REFERENCIAS

[1] Cano Jeimy J. ¿Seguridad informática o seguridad de la información? 2011 Octubre 06. [Online]. Available: http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html

[2] Ibid.

[3] [4] [5] [6] Pilares de la seguridad informática. Universidad Nacional Abierta y a Distancia. [Online] Available: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/11_leccin_1_pilares_de_la_seguridad_informtica.html

[7] Lección 14: No repudio. Universidad Nacional Abierta y a Distancia. [Online] Available: http://datateca.unad.edu.co/contenidos/233011/233011Exe/leccin_14_no_repudio.html

[8] Ciber riesgo, una de las principales preocupaciones para empresarios. 14 de Mayo de 2015. [Online] Available: http://www.elespectador.com/tecnologia/ciber-riesgo-una-de-principales-preocupaciones-empresar-articulo-560513

[9] Ibid.

[10] José Carlos García. El año en tomar en serio la seguridad/Análisis. 26 de Enero de 2015. Online] Available: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/2015-el-ano-de-tomar-en-serio-la-seguridad/15151578

[11] Presentan a Kobian, un robot con sentimientos. 24 de Junio de 2009. [Online] Available: http://www.hola.com/actualidad/200906249029/robot/japon/sentimientos/

[12] Cromo. Esta es Aiko, la recepcionista robot. 20 de Abril de 2015. [Online] Available:

http://www.cromo.com.uy/2015/04/esta-es-aiko-la-recepcionista-robot/

[13] Asociación Colombiana de Ingenieros de Sistemas. Nuevas tecnologías emergentes 2025, Revista ACIS. Enero – Marzo 2015.

[14] Colombia avanza en uso de tecnologías de información. 13 de Febrero de 2012. [Online] Available: http://www.portafolio.co/finanzas-personales/colombia-avanza-uso-tecnologias-la-informacion

FIGURAS

[1] Camelo, L. Seguridad de la información en Colombia. 2010 Febrero 18. [online] Available: http://seguridadinformacioncolombia.blogspot.com/2010/02/seguridad-de-la-informacion-y-seguridad.html

[2] Instituto nacional de ciberseguridad. ¿Te preocupas por la seguridad de la información de tu empresa? 23 de Julio de 2013. [online] Available: https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/preocupas_seguridad_informacion_empresa