La seguridad de la información en la actualidad y la incorporación del término CIBER, y derivados

Martínez Pava, Daniel Ricardo
Universidad Piloto de Colombina
Bogotá, Colombia
danielmpava@hotmail.com

Abstract- This document pretend to give to know a topic that in the actuality really affect seriously to enterprises as all the world and yet in some countries it is not as well known. It not necessary the physical attacks and wars between countries with bombs, rockets or military weapons, only takes a cyber attacks for doing enough damage on most value asset of the company such as information and personal data.

Resumen— Con este documento se pretende dar a conocer un tema que en la actualidad está afectando seriamente tanto a empresas como al mundo entero, y aún así, en algunos países no es tan conocido. Ya no son necesarios los ataques y guerras entre países con bombas, cohetes o armamento militar, basta con un ciber ataque para causar suficiente daño sobre lo que es el activo más valorado como es la información y los datos personales.

Índice de términos— ciber ataque, ciber guerra, ciber seguridad, ciber crimen, ciber acoso, seguridad informática, seguridad de la información, cifrado, defensa en profundidad.

I. INTRODUCCIÓN

Es un hecho innegable que ante la evolución constante del mundo actual, donde la globalización de la información, la proliferación de redes y nuevas tecnologías -la cual se dispara a gran escala-, surgen situaciones que se derivan directamente de esta realidad, y que traen consigo efectos poco deseables cuyas consecuencias presentan un impacto negativo muy alto sobre el patrimonio personal, económico, empresarial e informático para los protagonistas de este nuevo escenario virtual traído por las revoluciones tecnológicas; es precisamente, en la buena preparación que tengan dichos actores para enfrentar tales problemas donde radica no sólo el éxito en el desarrollo del espacio empresarial al que pertenecen, sino en el avance y evolución del mismo. Este escrito busca un acercamiento de las personas como recurso esencial para las organizaciones empresariales al conocimiento de los posibles ataques cibernéticos, vulnerabilidades o riesgos a los que pueden estar expuestos sus activos, información, usuarios o clientes en un ciber espacio o red de datos. Del mismo modo, hacer énfasis en la importancia de capacitar y concientizar a los empleados sobre el hecho de que ellos, a través de la información que manejan,

pueden ser el eslabón más débil, y vulnerable para la materialización de cualquier plan de ataque o persecución previsto en contra de la organización, que incluso generaran un impacto negativo, y un grave detrimento sobre el posible acceso a derechos inherentes a su ámbito personal, como el derecho constitucional fundamental de la intimidad y habbeas data consagrado en el artículo 15 de la carta política colombiana.

Es de resaltar que la seguridad cibernética de una empresa es tanto o más importante que la seguridad física y que el atacante puede entrar por donde menos se espera, para robar o estropear el sistema obteniendo información confidencial, sensible e importante de los miembros de la empresa.

II. LA SEGURIDAD DE LA INFORMACIÓN, UNA MEDIDA QUE SURGE DE LA TOMA DE CONCIENCIA EN LA ERA CIBER.

En la última década ha adquirido más fuerza un término que anteriormente no era muy sonado, se trata de la palabra "CIBER" que ha causado gran impacto en la nueva era tecnológica. Se conocen muchas derivaciones de este término que combinadas con la informática y los avances de Internet en la actualidad han generado gran discordia entre las personas, empresas, organizaciones, empleados y usuarios.

Términos como *ciber seguridad, ciber crimen, ciber terrorismo, ciber espacio, ciber nautas, ciber guerra, ciber acoso, ciber ataques, ciber defensa, ciber secuestro,* entre otras definiciones, han tenido al mundo entero en una constante inquietud. Esto da paso a la siguiente frase: la seguridad de la información es y será siempre un producto en desarrollo. Con la creciente situación de ataques a través de la web, las personas encargadas del área de sistemas tienen que estar en continuo desarrollo e implementación para asegurar el activo que hoy por hoy se cataloga como el más importante para una compañía: "la información".

Para que la información y los datos de una empresa sean seguros, deben cumplir los siguientes requisitos:

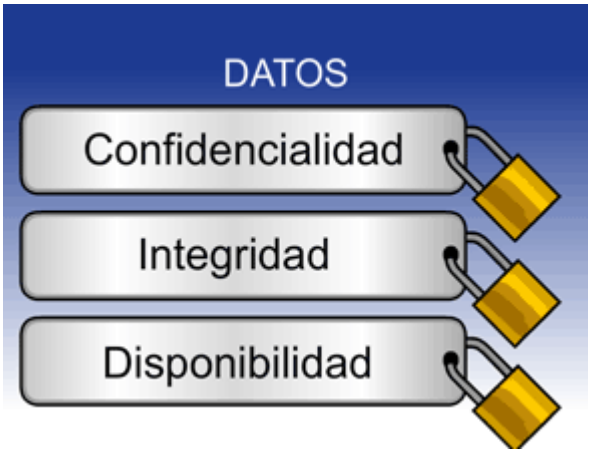

Figura 1. Los tres pilares de la seguridad de la información

Alguna vez un docente de Ingeniería de Sistemas dijo *–hablar de seguridad es hablar de inseguridad-* refiriéndose a seguridad en sistemas de cómputo. Esta pequeña frase no dice ni más ni menos que algunas veces entre más seguridad se implemente para resguardar la información, crece más el deseo que provoca en los ciber delincuentes de entrar al sistema, escudriñar, modificar o robar información con el único fin de hacer algún daño, bien sea para llevar a cabo planes de persecución empresarial o muchas veces para beneficio propio. Por esto y para evitar esta clase de ataques o ciber ataques se debe tener en claro la importancia de que las empresas cifren los datos sensibles y tengan una buena y estructurada defensa en profundidad. *"El cifrado adecuadamente implementado es cada vez más importante*[1], son reflexiones escritas por la

presidente de la comisión federal de comercio, Edith Ramirez.

Es de igual importancia mantener buenos hábitos y tener en cuenta algunos tipos en las organizaciones para protegerse de intrusos, hacker o personas con malas intenciones para que a estas les sea cada vez más complicado entrar o cometer cualquier delito en contra de los sistemas organizacionales.

Es de resaltar lo que hoy es el boom del momento, "las redes sociales". Mucha gente en el mundo hace uso de alguna red social y por ende disfrutan publicando estados, subiendo fotos, videos, diciendo el lugar donde se encuentran o suministrando información que realmente debería ser confidencial, privada; sin tener en cuenta que precisamente las redes sociales son eso, "sociales y públicas" y no se sabe en que momento un ciber atacante o ciber delincuente al otro lado de la pantalla puede estar viendo toda su información. Al respecto cabe citar al periodista Brian Krebs con su frase, *"Estar a salvo y seguro en línea requiere fundamentalmente de un cambio de mentalidad"*[2], el criterio de este periodista resulta bastante acertado, ya que realmente se requiere de un cambio de perspectiva y concientización de todos los actores de los espacios virtuales y tecnológicos para hacer un buen uso de las herramientas tecnológicas, debido a que todos conocemos que existen virus, robos en línea, formas de obtener información personal a través de Internet pero no muchos toman las precauciones necesarias para evitar el secuestro de información.

Con el inicio de la nueva tecnología: las computadoras y las redes, infortunadamente se atraen ciber criminales, cuyas acciones son principalmente destructivas. Aquí juega un papel muy interesante el saber o aprender a entender la mentalidad de las personas (principalmente de los delincuentes cibernéticos) e integrar información clave del comportamiento humano en cuanto a las tecnologías, para así ir siempre varios pasos delante de sus malintencionados planes en contra de la información y dejarlos desarmados a la hora de su inesperada arremetida.

Con el desarrollo tecnológico y el aumento del uso de ordenadores por el que el mundo está atravesando desde hace algunos años, los temas de la seguridad de la información, la seguridad informática y la protección de datos personales se han convertido en algo trascendental, más para las empresas u organizaciones debido a la privacidad de la información de sus clientes con el fin de mantener la confianza, imagen y estatus de los mismos; protegiendo la reputación y su responsabilidad legal; pues es innegable el hecho de que se ha dado gran importancia a las leyes que hacen referencia a la intimidad, incluyendo la ley de protección de datos personales, la cual salvaguarda la integridad de las personas en el ámbito de la red global (Internet). Actualmente las organizaciones dan un manejo cauteloso a este tema, debido al riesgo de responsabilidad legal y promulgación de leyes estatales e internacionales que protegen el núcleo esencial de derechos inherentes al ser humano como el de la intimidad en sus datos.

Como bien lo afirma Daniel Suárez para la revista Forbes *"Internet no fue pensado para ser una red segura"*[3], pero sin embargo la red ha sido puesta a disposición y servicio de importantes organizaciones como la banca en línea, el comercio de acciones, los procesos industriales, el comercio electrónico, entre algunas otras más; las organizaciones están en el deber de tener una infraestructura suficientemente robusta y segura, implementado una excelente defensa en

profundidad a la vez que garantiza los tres niveles de la seguridad; confidencialidad, integridad y disponibilidad de la información, para así brindar el mejor servicio a sus clientes mitigando los riesgos que puedan llegar a presentarse. *Cuando las tecnologías centrales de Internet están bien mantenidas, Internet funciona. Cuando no es así los planes de seguridad mejor establecidos fallan*[4] dice Joe Sullivan, responsable de seguridad en Facebook.

Con el desarrollo de los SmartPhone y los dispositivos inteligentes, los ciber criminales y/o ciber delincuentes están a la vanguardia concentrándose en los sistemas operativos de estos móviles, tanto así que estudios e informes han revelado que han aumentado las infecciones a dichos dispositivos, siendo Android el sistema operativo que ha presentado más incidentes con un 79%, Symbian 19%, Apple 0.7% y por último Windows Mobile y Blackberry ocupando el último lugar con el 0.3% [5].

III. EL CIFRADO UNA ALTERNATIVA EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN EL CIBER ESPACIO.

Con la llegada de Internet y la creación de las bases de datos, empresas, compañías y hasta personas naturales comenzaron a entrar en un mundo diferente y adquirir lo que hoy se conoce como *identidad digital*, con ella se empiezan a conocer en el mundo virtual. Datos privados, datos que solo importan a las compañías o a terceros involucrados, información en la cual se puede llegar a exponer a un individuo, son algunos temas que se consideran confidenciales y deberían estar bajo llave o seguros, pero con el mundo del Internet, esta información (muchas veces sensible) está a disposición de hackers y otras personas que pueden llegar a robarla, no obstante como lo afirma J. C. García en su artículo: "*todo parece indicar que a quien menos importa nuestros datos personales es a nosotros mismos"* [6]. Toda vez que en la actualidad brindamos datos personales simplemente por abrir un correo, tener una tarjeta para acumular puntos, abrir cuenta en redes sociales, porque ofrecen gigas de almacenamiento, jugar en línea o sencillamente haciendo uso del chat brindamos datos personales que como se dijo anteriormente, no se sabe quien esté detrás de la pantalla y sin ser conscientes del trato que se le va a dar a nuestra información.

Para ahondar más sobre este tema, se puede hablar de los robots de recolección de datos que son los que algunas compañías utilizan para conocer más a sus clientes y usuarios, con esto pueden saber gustos, hobbies, actividades, etc., de personas para así poder llegar más fácil a cada uno. Claramente se puede decir que los robots de recolección de datos, *son la gasolina de grandes corporaciones en el comercio de nuestros datos para efecto de publicidad* [7]. Esto da paso para que aparezcan los ciber delincuentes a robar o secuestrar los datos e información de las empresas recolectoras y como comenta Pablo Tejeira, director general de Sophos-Iberia, *"la información confidencial de las empresas es uno de los grandes activos con los que cuentan y por ello, deben maximizar su protección. El robo de datos está a la orden del día, por ello debemos impulsar el cifrado de la información, de tal forma que aunque los ciber delincuentes consigan acceder a datos sensibles de nuestros clientes, les sea imposible hacer mal uso de ellos*."[8]

Desde hace pocos años han venido llegando grandes cambios a nivel de tecnología e Internet, uno muy nombrado y que ha causado noticia en muchos sectores es el famoso Internet de las

cosas. Relojes, automóviles, casas, electrodomésticos, televisores inteligentes, entre muchos otros dispositivos… cada vez más cosas con las que interactuamos en la vida cotidiana están avanzando tecnológicamente asumiendo los peligros y riesgos que esto puede llegar a ocasionar. Es un hecho que los fabricantes de este tipo de dispositivos no se han preocupado en exceso por la seguridad, lo que puede hacer de ellos un objetivo muy jugoso y altamente atractivo para los ciber delincuentes o un ciber ataque.

IV. ¿REALMENTE VALORAMOS NUESTROS DATOS PERSONALES?

A partir del auge de las redes sociales, teléfonos móviles, electrodomésticos inteligentes y otros dispositivos o aplicaciones donde guardamos nuestra información y datos personales, se podrían formular preguntas como: ¿las redes sociales hacen parte de nuestras vidas ó nosotros hacemos parte de las redes sociales?, ¿tenemos teléfono móvil ó el teléfono móvil nos tiene a nosotros?, Vivimos cargando todos los días datos y más datos personales a Internet, tabletas, celulares y cuanto dispositivo se conecte a la web sin tener el mínimo detalle de seguridad o tomarse el tiempo de configurar los mismos y sin saber que estos datos podrían ser interesantes para otras personas y sus mal intencionados planes de ataque.

Un estudio de la empresa japonesa de antivirus y seguridad que se enfoca en el precio que le damos a nuestra información y donde se tratan temas como: [9]

- ¿Cuánto cuestan nuestras fotos?
- ¿Qué precio tienen los recibos, tu historial de cuenta bancaria?
- Historiales médicos y contraseñas.
- Direcciones físicas y de email
- Datos de hijos, familiares y pareja
- Condición saludable

Dicho estudio revela estos y otros datos. La siguiente gráfica muestra algunos de ellos.

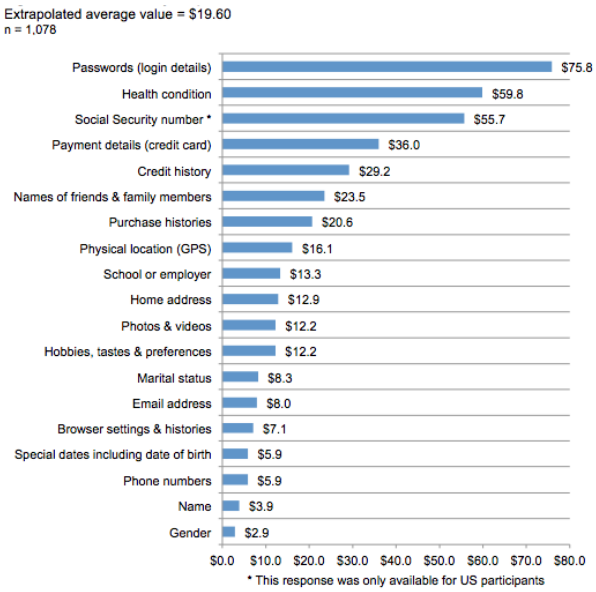

Figura 2. ¿Cuánto valen nuestros datos personales?

El estudio concluye que los usuarios dan mayor valor a sus claves, pero olvidan la importancia de información confidencial como su nombre, su ubicación y aún el sitio de trabajo, dalos que revelan sin cuidado alguno y que al caer en manos inescrupulosas les hacen víctimas potenciales de la ciber delincuencia.

V. ¿CÓMO SE PODRÍA DISEÑAR UNA ESTRATEGIA DE DEFENSA FRENTE A UN CIBER ATAQUE?

En muchas partes del mundo desde hace bastante tiempo la seguridad informática es muy importante. En Colombia con leyes como habeas data, la ley de protección de datos, la circular 042 de 2012, entre otras, se ha comenzado a prestar importancia a este tema y se ha convertido en algo más que necesario. Existen reglas y normas que exigen a empresas diseñar, implementar y tener

una defensa ante cualquier ataque o vulnerabilidad que pueda llegar a suceder.

Para una compañía es de vital importancia y de ahí que debe tener un excelente sistema de protección con el fin de que su información este a salvo, buena seguridad física-lógica, y una robusta estrategia de defensa para sus sistemas de información. Rafael Gómez –responsable legal y de auditorías en España- recomienda que las empresas realicen regularmente controles de seguridad en sus procesos para evitar brechas de seguridad, *cada semana, somos testigos de las continuas vulnerabilidades y problemas de seguridad que padecen tiendas online* [10].

No ha bastado con las noticias que se han visto en los últimos días, donde hacker o cracker han realizado ciber ataques contra reconocidas compañías como Sony, Twitter, Facebook, Target, Vodafone Egipto, Fox News, Cadillac, entre muchas más, para que personas y compañías tomen una conciencia real del riesgo al cual están expuestos, y presten más atención a la protección y seguridad de datos e información sensible. Muestra de lo mucho que le falta recorrer y reforzar tratándose de seguridad de la información a los miembros de la comunidad cibernética actual, es lo acontecido recientemente con el caso de los hacker rusos sobre la red de información del presidente de los Estados Unidos, Barack Obama, pues es inconcebible el hecho de cómo, ni las redes del dirigente de una de las principales potencias del mundo y con mayor evolución tecnológica se han salvado de las artimañas extremas de los ciber delincuentes, para lograr penetrar en la información que cualquiera creería está sujeta a protecciones rigurosas; sin embargo, el suceso deja entrever que no es así, que realmente la preparación y la capacitación en armas, y herramientas efectivas de seguridad de la información es un campo muy incipiente necesita ser reforzado y difundido masivamente, pues tal parece que las habilidades ociosas de los ciber terroristas van más allá que cualquier plan de seguridad que se esté implementando actualmente por lo que desde el mismo momento en que falla por su precariedad o falta de efectiva planificación, entran en sumo riesgo múltiples factores que van desde la información y reserva de datos de organizaciones empresariales, derechos inalienables de los individuos, seguridad personal (en caso de los múltiples secuestros planeados a través de estos medios), patrimonios económicos y hasta la misma seguridad pública o la soberanía de un estado como hubiese pasado en caso de que la información entrada en el caso de Obama hubiese sido relativa a planes de seguridad nacional.

Según una publicación de la revista semana, cada año se pierden más de 113 billones de dólares por cuenta del ciber crimen y de acuerdo con cifras entregadas por Microsoft, cada segundo 12 personas son víctimas de ataques informáticos[11].

Debido a los ataques que han servido como espejo para algunas compañías, estas han comprendido que la seguridad informática se ha convertido en un punto crítico dentro del modelo de negocio y muchas veces las mismas son conscientes de esto pero no saben cómo reaccionar ante este tipo de ataques de piratas informáticos, por la falta de conocimiento en el campo de seguridad de la información y de inversión en la capacitación de sus plantas de personal sobre este tema que tal parece, se convertirá a corto plazo en el único y verdadero escudo valido, y eficiente para obtener un blindaje efectivo de los activos empresariales y organizacionales.

La empresa Este Latinoamérica ha entregado una importante serie de sugerencias con el fin de tenerlas en cuenta para minimizar y enfrentar este tipo de riesgos.

- *Determine el alcance del ataque informático.*
- *Alerte a los empleados.*
- *Contenga el alcance del ataque.*
- *Elimine el virus que llegó a sus sistemas.*
- *Aprenda de los errores.* [12]

Por lo anteriormente expuesto es de vital importancia que empresas y organizaciones tengan en cuenta el cifrado debidamente implementado como una estrategia frente a hacker o cracker ya que si logran robar la información les va ser difícil poder saber que dice esta, puesto que se ha aplicado una técnica de cifrado. Por otro lado cada día las corporaciones se ven obligadas a que los empleados usen su propio teléfono móvil o tabletas para trabajar y utilizan la red, esto abre puertos que proporciona una entrada para software malintencionado o personas que pueden tener acceso a la red, por lo anterior se deben implementar técnicas y estrategias como, tener uno o más firewalls, utilizar proxy, tener subredes identificadas en la red y tener otra red para los usuarios de la oficina que desean conectarse con dispositivos ajenos. Otras estrategias que son importantes tener en cuenta ya que son decisivas a la hora de obtener verdadera protección, se refieren a capacitar a jefes y junta directiva para sensibilizarlos sobre los riesgos, vulnerabilidades y amenazas a los cuales está expuesto su activo más importante, la información. No obstante también se debe concientizar a empleados y toda persona de la organización que use su red, ya que en demasiadas ocasiones son estos el eslabón más débil de la seguridad, hacerles saber cuáles son los riesgos de los que se puede ser víctimas en Internet y como se debe llegar a evitar.

Aplicar estrategias de seguridad para resguardar los datos personales o los de las empresas, ha tomado un nivel de importancia muy alto, sólo basta con echar un vistazo a todo lo que está sucediendo en la actualidad, ver día tras día las noticias donde personas o compañías han sido atacadas por cracker o hacker con el fin de robar información o husmear en la red.

A medida que se masifique el acceso a Internet más serán los afectados por el ciber crimen [13].

VI. CONCLUSIONES

- Es de gran relevancia implementar un sistema fortalecido y consolidado de herramientas de protección a la seguridad de la información que apunten a una verdadera defensa de los activos empresariales, haciendo cada vez más difícil la actuación de los atacantes y desarmarlos en sus mal intencionadas maniobras.

- Se debe dejar en claro, bien configuradas además de resaltadas las reglas de exclusión y seguridad escritas en firewalls, switches o router.

- La primera gran herramienta para obtención de verdadera protección consiste en la debida capacitación y concientización de altos directivos, plantas de personal y usuarios en general, para que hagan un correcto uso de la tecnología, una rigurosa selección de los datos que ingresan en la red y de la manera en que pretenderán el blindaje de los mismos.

- Ser cautelosos con el tipo de información a suministrar en red, excluyendo totalmente el aporte de datos sensibles sin antes tener en claro las políticas de privacidad y seguridad de donde se están suministrando.
- Empresas, organizaciones, usuarios, personas naturales y en general cualquier actor dentro del creciente escenario de las nuevas redes tecnológicas, deberán usar claves fuertes y tener al menos la información sensible con un nivel aceptable de cifrado.
- Es indispensable aprender a diseñar, implementar y poner en marcha estrategias de seguridad, que vayan desde niveles micro como las redes de información instaladas en los ordenadores personales y domésticos, hasta los niveles macro como las redes propias de grandes, medianas y pequeñas entidades empresariales (públicas o privadas), organizaciones gubernamentales y/o estatales; en aras de minimizar y excluir al máximo cualquier riesgo o vulneración provenientes de ciber ataques, que pongan en detrimento valores personales, empresariales, económicos, públicos, estatales y que se deben derivar de una efectiva y eficiente seguridad de la información.

REFERENCIAS

[1] Ramírez E. (2014, Junio 23). . Presidente de la comisión federal de comercio. [Online] Available: http://www.forbes.com.mx/10-ideas-para-solucionar-las-fallas-de-ciberseguridad/.

[2] Krebs, B. (2014, junio 23). Periodista de investigación y autor del libro próximo a publicarse *Spam Nation*. [online] Available: http://www. forbes.com.mx/10-ideas-para-solucionar-las-fallas-de-ciberseguridad/. .

[3] Suárez D. (2014, junio 23). Escritor de ciencia ficción. [online] Available: http://www.forbes.com.mx/10-ideas-para-solucionar-las-fallas-de-ciberseguridad/.

[4] Sullivan, J. (2014, marzo 16). Responsable de seguridad en jefe de Facebook. Revista Forbes México. 10 ideas para reforzar las fallas de ciberseguridad. [online] Available: http://www.forbes.com.mx/10-ideas-para-solucionar-las-fallas-de-ciberseguridad/.

[5] Periódico El Espectador (2014, noviembre 14). Cibercriminales le apuestan al secuestro de información. [online] Available: http://www.elespectador.com/tecnologia/cibercriminales-le-apuestan-al-secuestro-de-informacion-articulo-527121.

[6] [7] J.C García. (2014, Diciembre 2). Editor Tecnosfera. Periódico el tiempo. ¿Qué tanto protegemos nuestra privacidad? [online] Available: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/como-proteger-y-reforzar-la-privacidad-en-internet-analisis/14917183. .

[8] Guilarte, M. (2014, Noviembre 26). En el 2015, las empresas deberán preocuparse por el robo de información. [online] Available: http://www .muycomputerpro.com/2014/12/26/robo-de-informacion.

[9] Pérez, D. (2015, abril 6). El androide libre por google. ¿Cuánto valen nuestros datos personales? [online] Available: http://www.elandroide

libre.com/2015/04/cuanto-valen-nuestros-datos-personales.html.

[10] Gómez, R. (2013, marzo 22). Los datos sensibles deben estar cifrados para evitar su robo por terceros. [online] Available: http://www.ticpymes.es/comercio/noticias/1066469025404/datos-sensibles-deben-cifrados.1.html. .

[11] [12] Revista Semana (2015, marzo 30), sección tecnología. ¿Qué hacer si su empresa sufre un ataque informático? [online] Available: http://www.semana.com/tecnologia/articulo/que-hacer-si-su-empresa-sufre-un-ataque-informatico/422687-3.

[13] García, J.C. (2015, Enero 26). El año en tomar en serio la seguridad/Análisis. [online] Available: http://www.eltiempo.com/ tecnosfera /novedades-tecnologia/2015-el-ano-de-tomar-en-serio-la-seguridad/15151578.

FIGURAS

[1] Eset Guías de seguridad III Empleado seguro. Los tres pilares de la seguridad de la información. 14 de Junio de 2013. [online] Available: http://www.estacion-informatica.com/2013/06/eset-guias-de-seguridad-iii-empleado.html

[2] El androide libre. ¿Cuánto valen nuestros datos personales?. 6 de Abril de 2015 [online] Available: http://www.elandroidelibre.com/2015/04/cuanto-valen-nuestros-datos-personales.html