Dificultades en la adopción de la Gestión de Seguridad de la Información en las organizaciones "Visión General"

Cifuentes Escobar, Nelly Maritze.
Universidad Piloto de Colombia, Bogotá, Colombia
maritzecif@hotmail.com

Abstract **- Companies and end users especially in the last decade are forced to use technology more secure, and protect your information is extremely important, market forces make it difficult for professionals from the sector to implement information security mechanisms; Latin America is no stranger to this phenomenon.**

Both private and Government sectors and the academic community have been and will continue carrying out significant efforts and improvements in favour of establishing mechanisms and standards that help users and organizations protect their information through the implementation of these guidelines apply within the information security management systems.

Resumen **- Las empresas y usuarios finales sobre todo en esta última década se ven obligados a utilizar tecnología cada vez más segura, y proteger su información es sumamente importante, las fuerzas de mercado hacen difícil para los profesionales del sector implementar mecanismos de seguridad de la información; Latinoamérica no es ajena a este fenómeno.**

La comunidad académica y sectores tanto privados como gubernamentales han realizado y continuaran llevando a cabo significativos esfuerzos y mejoras en pro de establecer mecanismos y estándares que ayuden a los usuarios y a las organizaciones proteger su información mediante la implementación de estas guías aplicables dentro de sistemas en gestión de la seguridad de la información

Índice de Términos – Ciberseguridad, Gestión del Riesgo, Ley de Metcalfe, Sistema de Información en Gestión de la Seguridad.

I. INTRODUCCIÓN

La adopción de la Seguridad de la Información al interior de las organizaciones ha evolucionado sustancialmente, una de las fuerzas que ha motivado este cambio precisamente ha sido el impacto económico y los mecanismos de oferta y demanda, que han obligado a las empresas y usuarios a hacer uso de tecnología cada vez más segura. El proceso no ha sido fácil, pero con el correr del tiempo, las compañías y los usuarios de recursos informáticos se han ido concientizando de la importancia de proteger su información y sus activos tecnológicos.

Con el mejoramiento continuo y dinámico de los procesos, las organizaciones han hecho uso de sistemas de información automatizados y tecnología aplicada, para dar apoyo a su misión. Dentro de sus metodologías clave deben considerar emplear de manera eficiente y eficaz la "Gestión del Riesgo" no meramente como un componente técnico sino concebido y ejecutado como uno de los pilares fundamentales para proteger la entidad.

La Gestión y Valoración del Riesgo son los principales componentes de los sistemas de Gestión de Seguridad de la información. Es generalmente aceptado por expertos en seguridad de la información, que la valoración del riesgo es parte de los procesos de Gestión del Riesgo. La Gestión del Riesgo es una actividad recurrente acorde con el análisis, planeación, implementación, control y monitoreo de medidas implementadas y políticas obligatorias de seguridad. [1]

II. ¿POR QUÉ ES DIFÍCIL LA IMPLEMENTACIÓN DE SEGURIDAD DE INFORMACIÓN EN LAS ORGANIZACIONES? – ASPECTOS ECONÓMICOS

En una encuesta realizada en 1993 sobre fraude contra cajeros automáticos ATM, fue encontrado que los modelos de fraude dependen sobre quien puede ser el responsable por ellos. En USA, si un cliente pone una queja debido a una transacción ATM, es el banco quien lleva a cabo los

mecanismos para probar que el cliente cometió un error o irresponsabilidad; esto daba a los bancos un motivo para proteger sus sistemas adecuadamente; pero en Gran Bretaña, Noruega y los países bajos, la carga de la prueba recaía sobre el cliente; el banco permanecía en lo correcto a menos que el cliente probara lo contrario. Desde esta perspectiva es casi imposible, que los bancos en estos últimos países fuesen cuidadosos. Debido al aumento de fraude excesivo por transacciones ATM en las últimas décadas se "echó por tierra" esta complacencia. Los bancos de USA, sufrieron mucho menos fraude, a la vez que ellos actualmente gastan menos dinero en seguridad que sus contrapartes europeas, quienes han tenido que invertir más dinero para dar solución a este problema. [2]

Hay muchos otros ejemplos: sistemas médicos que son pagados por aseguradoras en vez de por los proveedores de salud, fallas para proteger la privacidad del paciente cada vez que los conflictos con las aseguradoras hacen que se colecte información sobre sus clientes. Leyes de firma digital, transfieren el riesgo de firmas falsificadas desde el banco que envía la firma (y que construye el sistema) a la persona allegada que hace la firma, evaluaciones de criterios comunes no son hechas por auditores debidamente calificados**,** en vez de ello, por facilidad de pago comercial, son hechas por el vendedor, entre otros. [3]

Colombia no es ajena a esta situación, los usuarios y entidades tanto privadas como gubernamentales también han sufrido incidentes de seguridad en mayor o menor proporción, por ejemplo violación de datos personales como falsificación de información, acceso indebido a contraseñas, suplantación de identidad de los usuarios principalmente en los servicios financieros, y variadas situaciones que ponen en riesgo la seguridad de usuarios y empresas.

De acuerdo con el más reciente reporte sobre 'Tendencias de Ciberseguridad en América Latina y el Caribe' publicado por la Organización de Estados Americanos (OEA) y la empresa de seguridad Symantec, Colombia se posiciona como el sexto país en generar una mayor actividad maliciosa en línea, según los datos registrados en 2013. El reporte revela el panorama regional sobre las tendencias en materia de seguridad informática en la región y brinda algunas recomendaciones para incrementar la protección de los datos frente a estas amenazas. "En 2013, las estafas de redes sociales y la presencia de troyanos bancarios se multiplicaron en toda América Latina y el Caribe, aseguró Cheri McGuire, Vicepresidente de Asuntos Gubernamentales Globales y Políticas de Seguridad Cibernética en Symantec, durante la presentación del Reporte. Este aumento de la vulnerabilidad se debe, en parte, a la rápida adopción de Internet en la región, un hecho que genera mayores desafíos con relación a la seguridad en línea. [4]

Entre los ataques que presentaron un mayor crecimiento se encuentran los de 'ransomware', en los que un código malicioso cifra la información del equipo infectado y exige dinero al usuario para recuperarla. Estos casos, que tuvieron un crecimiento del 500 por ciento en 2013, estuvieron relacionados con atacantes que se hacían pasar por agentes de las fuerzas de seguridad locales, quienes exigían el pago de una multa falsa a cambio de la información. Con este engaño, lograban obtener entre 100 y 500 dólares por usuario. Debido a la alta rentabilidad de esta modalidad de ataque, los ciberdelincuentes desarrollaron un 'Cryptolocker', una evolución del 'ransomware', que exige directamente una suma de dinero para descifrar la información 'secuestrada' y no se hace pasar por ninguna entidad. El informe también destacó las estafas por correo electrónico, ataques de 'phising' o ingeniería social para robar información personal de la víctima y de códigos maliciosos dirigidos a instituciones financieras con motivo del Mundial de Fútbol. Adicionalmente, apunta que 15,4 por ciento de los ataques dirigidos registrados en América Latina en 2013 tuvieron como objetivo aquellas organizaciones con 501 hasta 1000 colaboradores. [5]

Es por ello que los usuarios y entidades deben incrementar sus medidas de seguridad, para protegerse individualmente y como organizaciones, se debe procurar estar un paso adelante del ciberdelincuente, porque día a día los ataques informáticos se vuelven más sofisticados y difíciles

de rastrear, y en muchas ocasiones, por descuido o negligencia podemos ser víctimas de una situación similar.

Consideremos los aspectos del porque es difícil la implantación de políticas y mecanismos de seguridad de la información, desde un matiz económico, entre ellos, tenemos:

A. Redes Externas

Los Economistas han dedicado mucho esfuerzo a las redes y a determinar cómo ellas son operadas por las compañías telefónicas, de aerolíneas y de tarjetas de crédito. La mayoría de personas utilizan una red típica, por ejemplo, emplean el sistema telefónico, o Internet para llamar porque así es más útil o cómodo para cada usuario. [6]

Este comportamiento algunas veces es referenciado como la *Ley de Metcalfe*: la cual dice que "el valor de una red de comunicaciones aumenta proporcionalmente al cuadrado del número de usuarios del sistema (n^2)". Formulada por primera vez en 1976 por **Robert Metcalfe** en relación con Ethernet, la ley de Metcalfe explica muchos de los efectos de red de las tecnologías y redes de comunicación, como Internet o la World Wide Web. La ley suele ilustrarse con el ejemplo de aparatos de fax: una única máquina de fax es inútil, pero su valor se incrementa con el número total de máquinas de fax de la red, debido a que aumenta el número de personas con las que se puede comunicar. [7]

Lo anterior no es limitado únicamente a sistemas de comunicación. La mayoría de comerciantes emplean tarjetas de crédito, es más útil si más clientes les compran, y la mayoría de clientes las tienen y si la mayoría de comerciantes las aceptan. El efecto es que las redes pueden crecer muy lentamente al principio, las tarjetas de crédito llevaron casi dos décadas para ser aceptadas, pero una vez la reacción fue positiva, hubo un posicionamiento, entonces el producto pudo crecer muy rápidamente. El telégrafo, el teléfono, la máquina de fax, el computador y más recientemente Internet han seguido este modelo. Con la masificación del uso de estos productos y para mantener el volumen de los clientes que los utilizan, en muchas ocasiones se obvia los diseños de seguridad que deben ser aplicados a los mismos, porque mayor seguridad podría implicar mayores costos, que inicialmente las compañías no deseaban asumir, y transferirle este costo al usuario podría significar perdidas de clientes. [8]

Sin embargo con el transcurrir del tiempo y debido al incremento sustancial de las aplicaciones informáticas y sus usuarios tanto a nivel individual como corporativo, y a las afectaciones en seguridad que aquejan más severamente, se ha hecho indispensable, la implementación de medidas de seguridad de la información, empezando por una concientización del usuario, la adopción de las organizaciones que ofrecen sus productos y el amparo de las entidades gubernamentales, en donde todos en conjunto, propenden por utilizar la tecnología de manera segura.

B. Aplicaciones competitivas y guerra corporativa

Las redes económicas tienen muchos otros efectos sobre la ingeniería de seguridad. Más que utilizar un estándar, o una solución bien analizada y probada, las compañías a menudo prefieren un propietario oscuro, que no ofrezca mayores garantías para incrementar clientes y aumentar la inversión que la competencia tiene que hacer para crear productos compatibles. Donde sea posible, ellos utilizarán algoritmos patentados (aun cuando no sean muy buenos), lo cual impone condiciones de licenciamiento sobre los manufacturadores. [9]

Este tipo de situaciones se presenta muy a menudo en sistemas propietarios, aplicaciones que ejercen una posición dominante en el mercado, no precisamente por su calidad, sino por los costos ofrecidos a sus usuarios, y en aras de ganar clientes e incrementar sus ganancias.

Un objetivo muy común es la diferencia de precios. Esto significa que el precio del producto o servicio no es el costo, pero si el valor al cliente. Un programa básico o servicio puede estar disponible gratuitamente, pero la versión completa solo estará disponible por suscripción. En muchos casos el programa es el mismo, excepto que algunas características son deshabilitadas dependiendo del presupuesto del usuario. Muchos mecanismos de protección y seguridad tienen su

funcionalidad real de mantenimiento en esta diferencia. [10]

Otro caso muy usual en la guerra corporativa, es la de las aplicaciones que utilizan métodos de autenticación como *single sign-on*, es decir un único conjunto de credenciales (usuario de ingreso y contraseña) con el cual el usuario puede acceder a todos los servicios que utilice dentro de la red interna y externa (servicios web), con los consiguientes riesgos que ello puede conllevar. Técnicamente los proveedores de estos servicios disponen de un repositorio central de autenticación en donde se almacena la información; los servidores utilizan esquemas de redireccionamiento web para conectar sus credenciales, la solicitud de autenticación y respuesta es pasada entre ellos por el navegador del usuario bajo ciframiento. Desde el punto de vista económico la funcionalidad de las aplicaciones *single sign – on,* puede ser más discreta, porque por ejemplo una empresa puede disponer de la información de todas las transacciones web de los sitios web a los cuales un usuario accede y puede comparar estos datos entre sí y mediante algoritmos estadísticos puede disponer de una gran cantidad de información de los clientes, como por ejemplo sus hábitos de compras online. Puede haber intercambio de información entre sitios, haciendo así que el valor de un sitio web se incremente considerablemente, llegando así a ser la red dominante del mercado. Microsoft es un claro ejemplo de este modelo. [11]

Cuando un sitio dispone de una inmensa cantidad de este tipo de información, puede convertirse en blanco de ataques informáticos para el robo de datos, y ser más atractivos para los ciberdelincuentes. El sector gobierno no es ajeno a esta realidad, la protección de la información es cada vez más importante y la utilización de procesos, mecanismos y herramientas para garantizar la seguridad es vital.

C. Guerra de Información: Ofensa y Defensa

En un ambiente globalizado como el que vivimos actualmente, en donde el mundo se ha convertido en una pequeña aldea, gracias a los avances tecnológicos y de comunicaciones, en donde una acción X llevada a cabo en el lejano Oriente, tiene su reacción Y en Latinoamérica, por ejemplo. Es sumamente importante para las naciones y los gobiernos determinar si los nuevos desarrollos tecnológicos protegen o amenazan sus naciones y si los favorecen o desfavorecen a nivel ofensivo y/o defensivo.

Supongamos que un producto grande y complejo tal como Windows tiene 1.000.000 bugs, tal vez sólo el 1% de ellos sean críticos en aspectos de seguridad. En segundo lugar, puede haber una sola alerta, para un gran número de fallos críticos para la seguridad. Por ejemplo, si la mitad de ellos son desbordamientos de pila, entonces tal vez estos puedan todos ser removidos por un nuevo compilador que los atrapa de alguna manera. En tercer lugar, se puede hacer la parte crítica de la seguridad del sistema lo suficientemente pequeña como para que los bugs se puedan encontrar. El ataque es simplemente más fácil que la defensa. Por ejemplo, un jefe de una agencia con tareas de inteligencia económica, y un informático que trabaja para el sector privado acaba de descubrir un nuevo exploit para Windows. Si se informa a Microsoft, se protegerá a 250 millones de americanos; si no se informa, se podrán llevar a cabo operaciones contra los 400 millones de europeos y 100 millones de japoneses, por ejemplo. Es más, se recibirá crédito por las operaciones que realizan con éxito contra los extranjeros, mientras que las probabilidades son que cualquier operación que se lleve a cabo con éxito contra objetivos de Estados Unidos seguirá siendo desconocida a los superiores. Esto acentúa aún más el motivo para el ataque en lugar de defensa. [12]

D. Distinguir lo bueno de lo malo

Otra visión es el 'mercado de limones', una explicación de por qué malos productos expulsan buenos productos de muchos mercados. Por ejemplo, considérese un mercado de autos usados, en la cual hay 100 autos buenos (las 'ciruelas'), por valor de $3000 cada uno y otros 100 en regular estado (el 'limón'), cada uno por valor de solo $1000. Los vendedores, por supuesto, saben cuál es cuál, pero los compradores no. Así que ¿cuál

será el precio de equilibrio de los coches usados? Si los clientes empiezan creyendo que la probabilidad de tener una ciruela es igual a la probabilidad de tener un limón, entonces el precio de mercado comenzará en $2000. Sin embargo, a ese precio sólo limones serán ofrecidos para la venta, y una vez que los compradores se den cuenta de esto, el precio caerá rápidamente a $1000, por lo tanto no se venderá la totalidad en absoluto. En otras palabras, cuando los clientes no tienen tanta información sobre la calidad de los productos como los vendedores, entonces habrá severa presión descendente sobre el precio y la calidad. Claramente esto sucede en los mercados para los productos de seguridad de la información y servicios. Puede ser el hecho aún peor cuando la gente que hace la evaluación de estos productos o servicios no son las personas que se ven afectadas cuando se presentan fallos. [13]

Esta es una buena comparación sobre como los gerentes, administradores y ejecutivos de las empresas y organizaciones, por obtener beneficios y comisiones al adquirir productos de seguridad en información de muy dudosa calidad, afectan el buen desarrollo de sus compañías, teniendo el conocimiento que pueden ser defectuosos, pero que pueden provenir de grandes proveedores o proveedores de su conveniencia; minimizando la probabilidad de obtener un buen soporte técnico cuando se lleguen a presentar las fallas, incrementando el riesgo de sus entidades. Por ello es bastante significativo que se cuenten con sistemas de evaluación de los productos que garanticen a las organizaciones y los usuarios la calidad y confiabilidad de los mismos.

III. SITUACIÓN EN AMÉRICA LATINA

Un reciente estudio presentado por McAfee, compañía de software especializada en seguridad informática, reveló que Colombia presenta serios problemas en esta área, con tendencia a crecer. De acuerdo con Juan Pablo Páez, gerente preventa para América Latina de la organización, "las razones están vinculadas con la falta de normas y exigencias por parte del Estado a las empresas y la ausencia de concientización de los directivos". El ejecutivo contó que los sectores que están mejor preparados para salvaguardar el problema de carácter mundial son el financiero y de telecomunicaciones, aunque hace falta crear una comunidad de apoyo externa, porque tienen logística internamente. Y mencionó que las instituciones de Gobierno aún están muy débiles en temas de seguridad de datos "lo que puede llegar a ocasionar incluso una crisis financiera o política". También mostró que las organizaciones débiles en este tema lo son porque: "En Colombia hay un modo reacción, hasta que no pasen las cosas no tomamos decisiones, y porque no han liderado esquemas que obliguen a cumplir con este requisito". Para Páez los beneficios que tienen las empresas armadas en seguridad informática se ven reflejados en "la permanencia en el negocio, la optimización de recursos, la eficiencia porque se toman decisiones en menores tiempos y la propia seguridad de la organización". [14]

Las inversiones en el ramo de tecnología y aseguramiento de la información, van en aumento a nivel mundial, incluyendo Latinoamérica, la cual tampoco es ajena a los principales factores de amenaza, como es el uso de correo electrónico, la red de datos para transferencia de información, y el entorno. El incremento de amenazas en seguridad informática es exponencial, debido al crecimiento constante de usuarios, aplicaciones y equipos que se adhieren al sistema, por ello es trascendental para las organizaciones entender que asegurando su información es base para la sostenibilidad de sus negocios, así como el entrenamiento y capacitación de los profesionales en el área.

Sin embargo, por muy difícil que sea la implementación de esquemas sólidos y confiables en seguridad de la información y el trabajo arduo de los profesionales en el ramo, es fundamental contar con sistemas de información en gestión de la seguridad, ISMS, por sus siglas en inglés.

IV. NECESIDAD DE UN SISTEMA DE INFORMACIÓN EN GESTIÓN DE LA SEGURIDAD (ISMS)

Como justificación para la implementación de un Sistema de Información en Gestión de la

Seguridad, los profesionales del sector, juicio de expertos y estudiosos de la materia, indican que:

- Los profesionales encargados de administrar la seguridad de la información, contarían con mejores tiempos pudiendo dedicar aproximadamente una tercera parte de su tiempo para direccionar aspectos técnicos. Las dos terceras partes restantes podrían utilizarse en desarrollar políticas y procedimientos, ejecutando revisiones en seguridad y analizando riesgos, direccionando planes de contingencia y promocionando conciencia en seguridad.[15]
- Las personas son fundamentales en la gestión y aplicación de la seguridad.
- Las amenazas internas en seguridad son mayores que las amenazas externas, debido a malas prácticas de los usuarios.
- La seguridad es tan fuerte como su eslabón más débil.
- El grado de seguridad depende de tres factores: el riesgo que se espera tomar, la funcionalidad del sistema, y los costos que se esté preparado a pagar [16]
- La seguridad es un ciclo continuo, no es una moda del momento.

Conforme a lo anterior se puede establecer que: "La Gestión de la seguridad exige administración y compromiso constante de todas las áreas de la organización y no es un problema meramente técnico a cargo de los profesionales de la seguridad".

Por ello el establecimiento, mantenimiento y continua actualización de un ISMS suministra un fuerte indicador de que una compañía está empleando una propuesta sistemática para la identificación, valoración y gestión de los riesgos en seguridad de la información. [17]

Es decir, cuando una organización ha logrado un nivel de madurez que le permite direccionar sus objetivos engranándolos con los objetivos fundamentales de la seguridad de la información, como son: la confidencialidad, la integridad y la disponibilidad, tendrá un efecto positivo en cuanto a:

- Soporte en sus procesos de continuidad del negocio.
- En caso de falló daños y pérdidas mínimas
- Alto nivel de competitividad
- Rendimientos financieros
- Posicionamiento estratégico e imagen organizacional
- Cumplimiento de normatividad y aspectos legales

V. OBJETIVO CLAVE

El objetivo clave de la Gestión de Seguridad de la Información es implementar las medidas apropiadas para eliminar o minimizar el impacto de varias amenazas y vulnerabilidades que pueda tener una organización relacionadas con la seguridad. [18]

Conforme se cumpla este objetivo, la compañía ofertara sus servicios con los criterios de calidad en seguridad anhelados y requeridos.

La misión y objetivos del negocio, son los que definen las necesidades de seguridad de la información, no es solo el tamaño de la misma; pero por lo general, compañías pequeñas se enfrentan a riesgos menores o riesgos de bajo impacto, cuando sus funciones no implican procesos relacionados con el manejo de información confidencial. Empresas de mayor tamaño como bancos, entidades de salud, compañías del sector gobierno, de telecomunicaciones, entre otras; requieren de un tratamiento más exigente en cuanto a la seguridad de su información, precisamente por el tipo de datos que administran, los cuales las obligan a garantizar su confidencialidad, integridad, disponibilidad, dando cumplimiento a aspectos legales y regulatorios, bien sea dentro del sector público y/o privado.

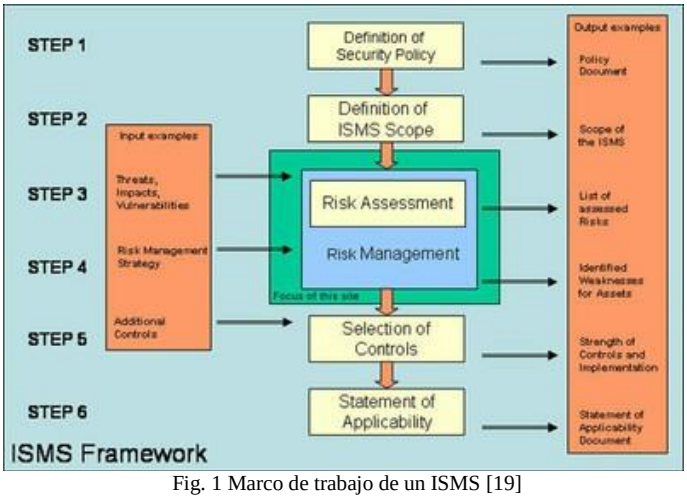

Fig. 1 Marco de trabajo de un ISMS [19]

Para desarrollar el objetivo clave es pertinente llevar a cabo un marco de trabajo o framework ISMS, el cual comprende los siguientes pasos: [20]

A. Definiciones de políticas de seguridad
B. Definición del alcance
C. Valoración del Riesgo (como parte de Gestión del Riesgo)
D. Gestión del Riesgo
E. Selección de Controles apropiados
F. Declaración de Aplicabilidad

La valoración y gestión del riesgo indicada en los literales C y D son el núcleo de un ISMS, ya que establecen las directivas y objetivos de seguridad, los otros se corresponden con el desarrollo e implementación de las medidas de control con el fin de mitigar y reducir amenazas y vulnerabilidades. La selección de controles y declaración de aplicabilidad especificada en los literales E y F hacen referencia a las tareas de carácter operativo necesarias para la gestión técnica, mantenimiento e inspección de las acciones de seguridad. Controles apropiados pueden ser derivados de conjuntos exhaustivos de controles o mecanismos, usualmente incluidos en estándares de información (ej. ISO 2700x) o guías, o ser la combinación o adaptación de controles propuestos para requerimientos específicos de la organización o características operacionales. [21]

Bien sea, aplicando un estándar o una guía propia de la compañía, o una combinación de ambas el literal F hace referencia al documento de hallazgos de los riesgos, así como los componentes técnicos y metodología que la organización haya decidido ejecutar.

Existen varios modelos en Gestión de la Seguridad de la Información, dada la importancia que tiene la valoración y gestión del riesgo al ser el núcleo de un ISMS, se cuenta con estándares que sirven de guía y apoyo para su implementación, entre los cuales contamos con:

VI. ESTÁNDARES PARA ADMINISTRAR EL RIESGO DE LAS TI

Desde hace años existen distintos estándares que intentan definir un modelo para administrar el riesgo de las Tecnologías de Información. Sin embargo, más de una vez hemos escuchado a los encargados y administradores de TI preguntar cómo se integran estas visiones y cuál debe ser aplicada a su organización. La problemática no es menor, sobre todo considerando que en muchas ocasiones se intenta desarrollar cada uno de los modelos como proyectos individuales, sin aprovechar las sinergias existentes en una implementación integrada, con un mayor esfuerzo de parte de las funciones operacionales. Para desarrollar este modelo de integración, se deben entender al menos los siguientes estándares: **COSO – Committee of Sponsoring Organizations of the Treadway Commission:** Es un modelo para entender el control interno y sirve como punto de partida para definir la administración de riesgo de manera transversal en una organización. COSO permite relacionar las necesidades de alto nivel -efectividad y eficiencia en la operación, confiabilidad de los reportes financieros y cumplimiento con leyes y regulaciones-, con requerimientos de administración de riesgo genéricos y específicos para los distintos procesos de negocio de una organización, incluyendo los procesos de apoyo como las Tecnologías de Información. **ISO/IEC 2700x:** La serie 27000 de estándares ISO es un conjunto de documentos ampliamente reconocido y globalmente aceptado para administrar la seguridad de la información, una de las principales áreas de administración de riesgo en TI. La serie incluye documentos específicos para definir un sistema de

gestión de seguridad de la información, buenas prácticas de control, métricas de seguridad y gestión de riesgo. **ISO 20000 (ITIL/ITSM):** Es el estándar más utilizado para administrar servicios TI. ITIL/ITSM define el modelo y los procesos clave para la entrega y soporte de servicios TI alineados con los objetivos del negocio y la necesidad de mejora continua, disponiendo de un módulo directamente relacionado con ISO/IEC 27000. **Cobit 4.1:** Cobit es un modelo de gobierno para administrar el riesgo y controlar las Tecnologías de Información. Este estándar ha sido ampliamente adoptado por las áreas TI en las organizaciones sujetas a requerimientos originados de la regulación Sarbanes-Oxley, siendo también un componente relevante a la hora de implementar mecanismos de medición de riesgo operacional (Basilea) y como herramienta para las funciones de auditoría interna y externa. [22]

La aceptación e implementación de uno de estos estándares o la combinación de ellos de forma integrada, depende de las necesidades de las organizaciones y de sus objetivos corporativos, sin embargo dentro de los factores comunes en pro de la aplicación de estos estándares, tenemos:

- Emplear un patrón comprobado y repetible en el tiempo.
- Generar resultados permanentes y coherentes.
- Obtención de métricas de control cuantificables y objetivas.
- Gobernabilidad e institucionalidad en los procesos de seguridad de información.
- Mayor claridad y comprensión de los riesgos a los que está expuesta la compañía.
- Punto de referencia para generar una cultura de seguridad.
- Garantía para las empresas al ofertar sus nuevos productos al mercado con mayor confianza para sí mismas y sus clientes.
- Posicionamiento de la imagen institucional.
- Cumplimiento de los aspectos regulatorios con mayor certeza y celeridad.

VII. CONCLUSIONES

Existe bastante y diversa literatura sobre el fracaso y las fallas de las medidas y herramientas en seguridad de la información para salvaguardar a los usuarios finales y empresas de fraude y violaciones de la privacidad y sus sistemas de información. Se pierde su enfoque cuando se analiza el tema desde un punto de vista de mercado; los gestores reales de diseños de sistemas de seguridad tienen en cuenta muy poco o nada que los objetivos altruistas y benévolos en seguridad de la información. Su meta primordial es económica, es el deseo de controlar un mercado en crecimiento, cobrar diferentes tarifas a diferentes usuarios tanto a nivel individual como corporativo por un mismo servicio y/o producto y eliminar a la competencia. Esto es lógico, en el mundo ideal, deshacerse de los siniestros estímulos económicos que crean sistemas inseguros podría solucionar y desburocratizar muchos problemas. La ingeniería en seguridad se enfocaría más a gestión de riesgos en vez de la eliminación del riesgo. Pero la realidad es muy diferente, la seguridad de la información es poder, es tendencia al monopolio; es poner obstáculos al comercio, es fragmentación de mercados y diferenciación de productos. Se aplican prácticas desleales y de riesgo moral. Cuando se elimina una de estas prácticas y es controlada por entes reguladores, las empresas, grupos asociados e inclusive gobiernos (de preferencia extranjera) generan o crean dos más.

En conclusión, la Gestión de Seguridad de la Información es un problema mucho más serio, delicado y político de lo que generalmente se cree y se percibe a simple vista; las soluciones pierden su enfoque y no abarcan todo el entorno. Este es el tiempo en que diferentes sectores de ingenieros, economistas, abogados, políticos y profesionales especialistas o no el ramo trabajen por un objetivo común.

REFERENCIAS

[1] (2014) Sitio web Enisa. Disponible: https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-isms

[2], [3] R. Anderson,“ Why Information Security is Hard - An Economic Perspective,” University of Cambridge Computer Laboratory, pp 1-2, Ene. 2001

[4], [5] (2014) Sitio web disponible: http://seguridadinformacioncolombia.blogspot.com/, http://www.symantec.com/page.jsp?id=cybersecurity-trends

[6], [8] R. Anderson,“ Why Information Security is Hard - An Economic Perspective,” University of Cambridge Computer Laboratory, pp 2, Ene. 2001

[7] (2013). Sitio web Wikipedia. Disponible: http://es.wikipedia.org/wiki/Ley_de_Metcalfe

[9], [10] R. Anderson,“ Why Information Security is Hard - An Economic Perspective,” University of Cambridge Computer Laboratory, pp 4, Ene. 2001

[11] R. Anderson,“ Why Information Security is Hard - An Economic Perspective,” University of Cambridge Computer Laboratory, pp 5, Ene. 2001

[12] R. Anderson,“ Why Information Security is Hard - An Economic Perspective,” University of Cambridge Computer Laboratory, pp 6-7, Ene. 2001

[13] R. Anderson,“ Why Information Security is Hard - An Economic Perspective,” University of Cambridge Computer Laboratory, pp 7-8, Ene. 2001

[14] (2014.) Sitio web El Espectador – Tecnología. Disponible: http://www.elespectador.com/tecnologia/colombia-lider-inseguridad-informatica-latina-articulo-482097 .

[15], [16], [17] (2014) Sitio web Enisa. Disponible: https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-isms/need

[18], [19], [20], [21] (2014.) Sitio web Enisa. Disponible: https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-isms/framework

[22] (2008.) Sitio web Noticias de Seguridad Informática. Disponible http://seguinfo.wordpress.com/2008/09/13/%C2%BFcual-es-el-mejor-estandar-de-administracion-de-riesgo-para-las-ti/