Modelo para medir el retorno sobre la inversión en seguridad informática y de la información – ROSI

Model to measure return on investment in computer and information security - ROSI

[1]Christian Angulo Rivera

[1]Universidad Nacional Abierta y a Distancia

Recibido: 19/09/20 Aprobado 10/10/20

Resumen

La presente ponencia pretende proponer, a través de una investigación cuantitativa correlacional, un modelo para medir el retorno sobre la inversión en seguridad informática y de la información ROSI en las pymes de Colombia, permitiendo de esta manera que los gerentes, líderes de tecnología y seguridad, tengan las herramientas necesarias para determinar de manera objetiva como priorizar las inversiones, pensando siempre en el bienestar económico y operativo de la organización.

Una variable importante de esta investigación es el entendimiento de estado en el cual se encuentran las pymes de Colombia en temas de seguridad informática y de la información, ya que estos temas son nuevos debido a que apenas están empezando a escuchar estos términos, gracias a la cantidad de noticias que hacen referencia a "hackeos" o pérdidas de información corporativa.

De igual manera se pretende visibilizar los modelos de seguridad que las pymes pueden utilizar teniendo en cuenta las ventajas y desventajas de su aplicación. Aunque no es obligatorio para las organizaciones legalmente constituidas, implementar controles de seguridad de la información, existe una responsabilidad corporativa para entregar siempre un excelente producto o servicio, lo cual solo se garantiza si los activos de información están correctamente salvaguardados.

También se presentan los costos ocultos e intangibles que se generan debido a la falta de inversión o planeación en las inversiones de seguridad. Esto permite que las pymes estén conscientes de que pueden ser víctimas de los delincuentes informáticos o que se pueden generar pérdidas debido a la falta de capacitación de su personal y todo esto debido a la falta de implementación de controles, que garanticen la adecuada gestión en temas tecnológicos.

Citación: Angulo Rivera , C. (2021). Modelo para medir el retorno sobre la inversión en seguridad informática y de la información - ROSI. Publicaciones E Investigación, 14(3). https://doi.org/10.22490/25394088.4487

[1]Correo: christian.angulo@unad.edu.co, Especialización en seguridad informática, UNAD, Colombia. https://orcid.org/0000-0001-6510-7245,

https://doi.org/10.22490/25394088.4487

Palabras clave: ciberseguridad, seguridad de la información, retorno sobre inversión en seguridad, seguridad informática, ROSI.

Abstract

The following work tries to propose across a quantitative correlation investigation, a model to measure the return on the investment in IT security ROSI in the SMEs of Colombia, allowing hereby that the managers, leaders of technology and security, should have the necessary tools to determine in an objective way how to prioritize the investments, thinking always about the economic and operative well-being of the organization.

An important variable of this investigation is the understanding of the state in which they find the SMEs of Colombia in topics of IT security and of the information, since these topics are new due to the fact that scarcely they are starting listening to these terms, thanks to the quantity of news that relates to "Hackers" or losses of corporate information. In the city of Cali there is a great quantity of SMEs that are very focused on the development of their service or main function and do not have inside their radar a topic so delicate as it is that of the IT security and of the information.

Likewise, the aim is to make visible the security models that SMEs can use into account the advantages and disadvantages of their application. Although it is not mandatory for legally constituted organizations to implement security controls, there is a corporate responsibility for the delivery of an excellent product or service, which is only guaranteed if the information assets are correctly safeguarded.

Hidden and intangible costs generated due to lack of investment or planning in security investments are also presented. This allows SMEs to be aware that they can be victims of computer criminals or that losses can be generated due to the lack of training of their staff and all this due to the lack of implementation of controls, which ensure proper management on issues technological.

Key words: *Cybersecurity, Information Security, Information Security, Return on Investment in Security.*

1. Introducción

El término TIC (Tecnología de Información y Comunicaciones) se ha vuelto de uso cotidiano para las organizaciones, ya que las tecnologías son el soporte de las operaciones de las empresas. Sería impensable una empresa que no funcione con servicios conectados a redes informáticas como el correo electrónico, sistemas contables, servicios web entre otros. Ese desarrollo organizacional encaminado a la obtención de sistemas de información robustos y autosuficientes no debe estar aislado de la protección de este, ya que toda la información está siendo almacenada en dispositivos informáticos que son accedidos por medio de redes internas y externas, que a su vez está siendo compartida con facilidad cada día. De ahí surge la necesidad de determinar de qué manera las inversiones realizadas en seguridad informática y de la información, impactan en la rentabilidad de las organizaciones.

Es necesario que las pymes entiendan que se debe generar una cultura de seguridad informática y de la información, porque a diario se están generando millones de intentos de ataques cibernéticos a las compañías con un porcentaje alto de acierto. Las organizaciones indistintamente de su tamaño o procedencia están siendo vulneradas por delincuentes informáticos, que aprovechan la falta de conocimiento en temas

de seguridad, para obtener información confidencial y afectarlas de manera económica u operación.

En la mayoría de las organizaciones, las decisiones de inversión deben tener un soporte financiero que le de viabilidad al proyecto, solución o dispositivo de seguridad con el cual se pretende minimizar o los riesgos de seguridad informática y de la información. Es ahí donde empiezan las complicaciones para los directores de TI o de seguridad a la hora de sustentar su presupuesto de inversión, ya que, en su mayoría, estas soluciones no generan un retorno sobre la inversión tangible.

En esta investigación se pretende generar precisamente un modelo que les permita a las pymes identificar fácilmente cual va a ser el retorno que van a tener con relación a las inversiones realizadas en materia de seguridad informática y de la información, ROSI. De esta manera se genera una conciencia organizacional alrededor de temas como el tratamiento de riesgos de seguridad, identificación de activos, aplicación de controles, cuantificación de variables, entre otras, para el correcto cálculo del ROSI.

2. Desarrollo del artículo

El problema identificado, consiste en la dificultad que tienen las pymes de Colombia para calcular el retorno sobre la inversión realizada en todas las soluciones de seguridad informática y de la información, ya que se desconoce si dichas inversiones son beneficiosas y rentables. Adicionalmente las compañías están bajo amenaza tecnológica, poniendo en riesgo su activo principal como lo es la información. Sumado a esto existen brechas humanas, tecnológicas, políticas y ambientales que se deben identificar para generar estrategias de protección adecuadas y evitar que se comprometa la disponibilidad, integridad y/o confidencialidad de la información.

En la actualidad existen metodologías, como los modelos Gordon-Loeb (Gedesco, 2016), Sonnenreich (Gordon & Loeb, 2002) estándares, normas y de más que permiten medir cuantitativamente el retorno sobre la inversión en seguridad informática, pero mucha de esta información es totalmente desconocida para las pymes del país, ya que en muchos casos nuestros empresarios piensan que el tema de los "Hackers" solo pasa en las películas. De ahí que la medición del retorno sobre la inversión en seguridad informática y de la información proporcionara una hoja de ruta para poder escoger de una manera correcta las soluciones de seguridad que son ofrecidas en el mercado. Este insumo será de gran ayuda tanto para directores de infraestructura tecnológica, como encargados de seguridad y la dirección general de la organización.

Por tal razón el aseguramiento de la información se ha convertido en un punto de referencia en las organizaciones (Sonnenreich, 2006). De ahí que existan empresas especializadas en la seguridad informática, así como metodologías y estudios encaminados solo a la preservación de dicho activo que se ve amenazado por diferentes factores. Es por esto que poder medir el retorno sobre las inversiones en seguridad informática y de la información en las organizaciones, permitirá realizar mejores y mayores inversiones en soluciones de seguridad ajustadas a las necesidades reales de las pymes.

De esta manera se propone un modelo óptimo de medición sobre las inversiones de seguridad informática y de la información, que se puede adoptar en organizaciones de cualquier tamaño.

3. Modelo ROSI propuesto

3.1 ROI – Retorno sobre la inversión

En las organizaciones, los gerentes financieros o quienes toman las decisiones económicas deben garantizar que todas las inversiones tengan una adecuada justificación financiera. Es por esto por lo que en buena medida esperan que se tenga un *Retorno sobre la inversión* (ROI) adecuado. El ROI (Phillips & Phillips, 2009) compara el costo de una compra

de una solución con los rendimientos esperados durante la vida útil del mismo. Este se calcula de la siguiente manera:

ROI=(Ingresos-Inversión)/Inversión x 100

3.2 Modelo ROSI Gordon y Loeb

En este modelo se explica que la inversión para proteger datos de empresa implica un costo que, a diferencia de otras inversiones, por lo general no genera el beneficio. Esta inversión sirve para prevenir los posibles gastos en que incurriría la organización tratando de recuperar los datos o activos de información del negocio, ya sea porque estos sean robados, dañados, corrompidos o se pierda la información. Para estructurar este modelo, la empresa debe poseer el conocimiento de tres parámetros: 1. Cuál es el valor de los datos; 2. Cuál es la exposición al riesgo y 3. Cuál es la probabilidad un ataque efectivo sobre los datos. A este último parámetro, Gordon & Loeb (2002) lo han definido como vulnerabilidad. El producto de estos tres parámetros proporciona la pérdida aproximada de dinero si no se llevase a cabo la inversión de seguridad.

Por ejemplo, si el valor de datos estimado es de $US 3.000.000, con una probabilidad de ataque o exposición al riesgo del 20%, y una posibilidad del 85% que un ataque fuera acertado. En este caso, el producto de la pérdida potencial es:

Valor Estimada de Perdida=Valor Datos x Exposición al riesgo x Posibilidad de acierto del Ataque

Valor Estimada de Perdida=US$ 3.000.000 x 0,20 x 0,85=US$510.000

Según Gordon & Loeb (2002), la inversión de la empresa en la seguridad no debería exceder el 37% del valor estimado de pérdida para considerarla una inversión rentable en seguridad, es decir:

US$500.000 x 0.37=US$ 188.700

3.3 Modelo ROSI Böhme

Otro de los modelos importantes para el cálculo del ROSI es el modelo de Böhme (2010) desarrollado en el Instituto Internacional de Ciencias de la Computación en Berkeley, California, por Rainer Böhme, quien indica que el modelo propuesto por Gordon y Loeb presenta algunos inconvenientes debido a que no se puede ver todo el panorama de seguridad solo midiendo las entradas de inversión en seguridad y probabilidad de pérdida, ya que hay más elementos que se deben contemplar. Por su parte Böhme indica que su modelo tiene en consideración elementos como el costo de la seguridad (en términos monetarios) el cual se asigna al nivel de seguridad y a su vez, el nivel de seguridad determina los beneficios de la seguridad.

ROSI = (Beneficios de seguridad-Costo de seguridad)/(Costo de seguridad)

Böhme, durante su investigación, corrobora que se han venido haciendo inversiones significativas en seguridad, pero no se trata de las inversiones realizadas, sino más bien la calidad de dichas inversiones, ya que todos los modelos de ROSI se construyen sobre métricas de seguridad las cuales definen las entradas, salidas, procesos y parámetros, y esta información es desconocida por las organizaciones.

3.4 Modelo ROSI Sonnenreich, Albanese y Stout

En el modelo Sonnenreich, Albanese y Stout, los autores proponen una medición del ROSI teniendo en cuenta variables, como exposición al riego, porcentaje del riesgo mitigado y costo de la solución. De este modo la ecuación del ROSI queda de la siguiente manera:

ROSI = ((Exposición al riesgo x % Riesgo mitigado)-Costo de la solución)/ (Costo de la Solución) x 100

Por ejemplo, si una pyme estima que un ataque de Ramsonware le significaría pérdidas anuales por US$ 20.000 aproximadamente, y tiene la posibilidad de adquirir una solución de protección contra este tipo de ataques que garantiza una mitigación del 90% por

US$15.000 durante 2 años, el retorno sobre la inversión se calcularía de la siguiente manera:

Exposición al riesgo=US$20.000 x 2 años=US$40.000

Riesgo mitigado del 90% Costo de la solución US$15.000

ROSI = ((US$40.000 x 90%)-US$15.000)/US$15.000 x 100=140%

La ecuación es sencilla pero tal cual y como está, le hace falta un poco de precisión en el cálculo de la exposición al riesgo y el costo de la solución, ya que el cálculo de la cuantificación de la exposición al riesgo debe ser una tarea con mayor dedicación, por ejemplo si una solución para una pyme cuesta $100.000.000 pero la implementación de esta representa una improductividad de 5 minutos para los 1.000 trabajadores de la compañía que en promedio ganan $50.000 al día lo que significa esos 5 minutos equivalen a una pérdida diaria de $694, que por año en costos de improductividad se traducen en

$254.472.222 aproximadamente, sumados a los $100.000.000 del costo de la solución, lo que nos daría $354.472.222 como valor real de la solución.

3.5 Modelo ROSI propuesto

A continuación, se presenta la manera en que vamos a calcular el ROSI, una vez ya se tiene claro de dónde se obtuvieron los datos de cada una de sus variables. Posteriormente se realizará la evaluación del ROSI para el año 2 en adelante, ya que existen una serie de cambios en su evaluación debido a que en el costo de la solución se genera una disminución significativa en la inversión y mitigación del riesgo.

1) Ampliación del modelo de Sonnenreich, Albanese y Stout

ROSI = ((Exposición riesgo anual x % Riesgo mitigado)-Costo mitigación)/(Costo mitigación) x 100

Exposición al Riesgo anual = Costo de impacto x Tasa de ocurrencia Anual

% Riesgo Mitigado = Porcentaje que la solución mitiga del riesgo. Esta información sale de estadísticas del fabricante o base de datos de conocimiento propio.

Costo de la Solución = Valor Solución + Valor Tiempo Improductivo + Gasto Operacional

Para ejemplificar el cálculo del ROSI vamos a tomar como referencia los valores calculados anteriormente y los pondremos en contexto.

Para mitigar el riesgo denegación del servicio que afecta el activo SAP se pretende adquirir un firewall para brindar aseguramiento perimetral. A continuación, se presenta el cálculo y en la tabla 34 se ejemplifica de manera más visual.

ROSI = (((($28.000.000 x 12) x 0,95)-$170.200.000)/$170.200.000 x 100=88%

Para esta labor lo que debemos realizar es listar los riegos catalogados como críticos para la organización y validar los controles que hemos definido para su mitigación. Una vez tenemos los controles, se debe verificar si estos son transversales a varios de los riesgos identificados para proceder al costeo de las soluciones apropiadas. Con esto se obtiene el insumo fundamental para el plan de inversiones en seguridad al cual se le validara el ROSI.

Costo mitigación = Valor solución + Valor tiempo improductivo + Gasto operacional

Valor de la solución: hace referencia al costo inicial que la pyme debe pagar para poder obtener dicha solución. Si se llegase a necesitar algún tipo de licenciamiento adicional, este valor debe ir al gasto operacional. También es importante tener en cuenta el valor del tiempo de improductividad que puede llegar a generar dicha solución, por ejemplo, si se adquiere una solución de seguridad perimetral como un firewall, y que debido

a la configuración que se debe aplicar ralentiza la operación en la red en 3 minutos al día, estos minutos sumados diariamente por la cantidad total de trabajadores, arrojan un valor que no podemos dejar pasar por alto.

Valor de solución de seguridad perimetral = $90.000.000

Valor tiempo improductivo: un trabajador que gana $6.000 la hora, significa que gana $100 el minuto y si dicha solución genera 3 minutos de ralentización de la red, significa $300 de pérdida al día. Visto de manera rápida no parece muy significativo, pero si este valor lo multiplicamos por los 22 días en los cuales se encuentra el trabajador en la oficina y también lo multiplicamos por los 12 meses del año y a su vez multiplicamos esto por la cantidad total de trabajadores, que para este ejemplo serán 1.000, el panorama cambia drásticamente.

Valor tiempo improductivo = $300 x 22(días) x 12(meses) x 1.000(trabajadores)

Valor tiempo improductivo = $79.200.000 Gasto operacional: si la solución requiere la

adquisición para dispositivos adicionales o existe un costo de mantenimiento anual o se requiere la contratación de un ingeniero o empresa de seguridad para su operación, estos gastos deben ser incluidos en esta variable. Por lo general este gasto operacional no se ve reflejado en el primer año del servicio de la solución, pero al pasar este tiempo se requiere renovar la solución, lo cual genera costos de licenciamiento a partir del año 2 en adelante.

Gasto operacional = $1.000.000 (mantenimiento)

De esta manera podemos decir que el costo de mitigación del riesgo asociado a esta solución es el siguiente:

Costo mitigación = Valor solución + Valor tiempo improductivo + Gasto operacional
Costo mitigación = $90.000.000 + $79.200.000 + $1.000.000
Costo mitigación = $170.200.000

4. Conclusiones

La seguridad informática sigue siendo un tema desconocido para las pymes de Colombia, debido a que estas dedican parte de sus recursos a las actividades generadoras de valor, dejando a un lado todas las actividades que no representan significancia económica para ellas.

Una vez se identifica que la seguridad informática no genera un retorno económico sino más bien un beneficio para la organización y que la no aplicación de controles para los riesgos puede ocasionar cuantiosas pérdidas, es justo en ese momento que las pymes realzan la importancia de la seguridad informática.

El desconocimiento de los modelos y estándares en seguridad informática y de la información hacen que las pymes determinen que esto puede ser un costo muy alto para ellas, pero esta investigación dejó claro que existe un modelo de consulta gratuita generado por el MinTic denominado MSPI, Modelo de Seguridad y Privacidad de la Información, que puede ser utilizado sin mayor complicación por cualquier organización.

A través de una herramienta conformada por una serie de pasos sencillos de seguir, se puede calcular de manera correcta el Retorno Sobre la Inversión en Seguridad, teniendo en cuenta valores tangibles e intangibles que permiten una aproximación más exacta al cálculo del ROSI.

El cálculo y presentación efectiva del ROSI es un insumo muy poderoso a la hora de sustentar proyectos de inversión en seguridad a directores administrativos y financieros, así como a juntas directivas.

Agradecimientos

Agradezco a Dios y mi familia por brindarme la oportunidad de adquirir estos nuevos conocimientos para poder transmitirlos y darlos a conocer a toda la comunidad académica.

Referencias

Böhme R. (2010) Security Metrics and Security Investment Models. En: Echizen I., Kunihiro N., Sasaki R. (Eds.). *Advances in Information and Computer Security. IWSEC 2010. Lecture Notes in Computer Science*, vol 6434. Berlin: Springer. https://doi.org/10.1007/978-3-642-16825-3_2

Gedesco (2016). Consejos para proteger los datos de tu empresa. *Gedesco* [en línea]. https://www.gedesco.es/blog/consejos-proteger-datos- empresa/

Gordon, L. A. & Loeb, M. P. The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC*), *5*(4), 440. https://dl.acm.org/citation.cfm?id=581274

Phillips, P. P.; Phillips, J. J. (2009). Return on investment. *Handbook of Improving Performance in the Workplace.* Volumes 1-3, (pp. 823-846). https://doi.org/10.1002/9780470592663.ch53

Sonnenreich, W. (2006). Return on security investment (ROSI)-a practical quantitative model. *Journal of Research and practice in Information Technology*, *38*(1), http://infosecwriters.com/text_resources/pdf/ROSI-Practical_Model.pdf