

# Presentando el ROSI a la Alta Gerencia

Gabriel Marcos, Product Manager - Datacenter, Security & Outsourcing,  
Global Crossing Latin America & Caribbean.

Originalmente publicado por la revista [CXO Community](#)

*¿Qué es eso de lo que todo el mundo habla, pero tan poco se ha visto en concreto? ¿Es posible justificar económicamente las inversiones en seguridad de la información?*

Es un hecho que cada vez encontramos más perfiles asociados a la seguridad de la información en las organizaciones, tanto en América Latina como en el mundo.

La creación de la figura del **CISO** (Chief Information Security Officer) está dando lugar a la aparición de ciertas necesidades no cubiertas respecto a la seguridad de la información en las empresas, llevando al CISO a responder una serie de preguntas que pueden definir el éxito o el fracaso de su gestión: ¿Estamos invirtiendo lo suficiente?, ¿Cuánto deberíamos invertir de acuerdo a nuestros objetivos de negocio?, ¿Cómo distribuir las inversiones de la mejor forma?

Gracias al surgimiento de estas (y muchas otras) preguntas, es que suena cada vez más fuerte la necesidad de contar con un adecuado cálculo de ROSI (Return On Security Investments - Retorno de la Inversión en Seguridad), que permita justificar inversiones y proyectos frente a la Alta Dirección y el Departamento de Finanzas.

Es un hecho que a medida que en las organizaciones crece la conciencia respecto a la relación entre la seguridad de la información y el cumplimiento de los objetivos del negocio, las inversiones en recursos asociados a seguridad se posicionan para competir por el presupuesto con los proyectos más significativos en cuanto costos y recursos.

Es en este escenario donde resulta fundamental presentar los beneficios de las inversiones más allá del dominio técnico, y utilizando un lenguaje común a los niveles de decisión más altos de la organización.

El cálculo del ROSI deriva de la forma genérica de “Retorno de la Inversión” (ROI), que es un indicador bien conocido y ampliamente utilizado por las Gerencias de Finanzas y Administración en general:

$$\text{ROI} = (\text{Beneficio} - \text{Costo}) / \text{Costo}$$

De forma general: si el ROI es positivo, estamos frente a una inversión que conviene considerar; sino, los costos superarán el beneficio, por lo cual no es recomendable.

Cabe aclarar que cuando nos referimos a beneficio, significa “Beneficio Económico”: una de las principales ventajas que presentan este tipo de indicadores, es que no analiza los detalles técnicos particulares de cada

inversión, sino solamente el impacto que ésta tendrá sobre la rentabilidad de la organización, tanto en los ingresos como en los costos.

### ***Interpretación del ROSI***

En el caso del ROSI, si bien la fórmula conserva la forma del cálculo del ROI, los indicadores son diferentes:

$$\text{ROSI} = (\text{Riesgo Disminuido} - \text{Costo}) / \text{Costo}$$

Esto es así porque cuando analizamos una inversión en seguridad, no buscamos un aumento en los ingresos, sino más bien una disminución del riesgo al que están expuestos los principales procesos del negocio.

Antes de continuar con los detalles inherentes al cálculo del ROSI, es fundamental comprender esta diferencia en cuanto a los indicadores: aún cuando estemos frente a un proyecto que vaya a aumentar los ingresos de la organización y que dependa fuertemente de controles asociados a la seguridad de la información (por ejemplo: la implementación de una nueva plataforma de comercio electrónico), los análisis de ROI y ROSI se realizan necesariamente por separado, ya que el "ROI" estaría representando la inversión "imprescindible" para el desarrollo del negocio, mientras que el "ROSI" representa la inversión más adecuada de acuerdo al "Nivel de Riesgo" que estamos dispuestos a asumir.

Y ésta es la primera clave a considerar en el desarrollo de un cálculo de ROSI representativo de la organización y del negocio; ya que garantizar un determinado nivel de seguridad de la información es imposible (menos aún, el ideal del "100%"), lo que se busca no es justificar la implementación de "la mejor solución", sino encontrar cuál es "la más adecuada" de acuerdo al nivel de riesgo tolerable para el negocio.

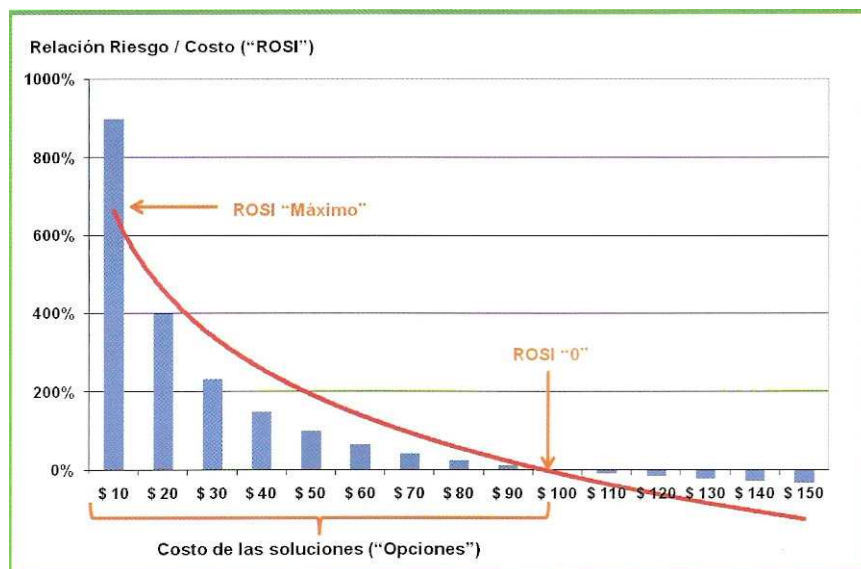
Por supuesto, siempre que tenemos que elegir, necesitamos opciones, y en esto se basa nuestra metodología para el cálculo de ROSI: una herramienta de decisión, que nos permite elegir la mejor entre las diferentes opciones que tenemos disponibles.

Adicionalmente, si bien todo cálculo del riesgo tiene asociados componentes "subjetivos" o no demostrables, nuestra metodología nos permitirá utilizar un modelo de fórmula aceptado ampliamente en los niveles más altos de la organización, con un conjunto de técnicas matemáticas que disminuirán los componentes subjetivos del análisis a los niveles más bajos posibles.

### ***Tres enfoques para el cálculo del ROSI***

Habiendo aclarado las cuestiones de base, es momento de pasar a la acción: ¿Cómo se calcula el ROSI? ¿Cómo llegamos a obtener "un número"?

En principio, y en función de la necesidad de analizar diferentes opciones y tomar una decisión, el resultado de nuestros cálculos no será "un número", sino "una curva" que tendrá una forma similar la siguiente:



Para un mismo nivel de "Riesgo Aceptable", podremos encontrar:

- ¿Cuál es el rango de "costo de las soluciones" que representan las opciones entre las cuales podemos elegir?
- ¿A partir de qué punto ("ROSI = 0") las soluciones comienzan a ser contraproducentes para el negocio, ya que el costo supera el beneficio?

Alcanzar esta curva es un proceso no trivial, pudiendo ser enfocado desde tres puntos de vista:

#### **1. Enfoque Cualitativo**

Esta metodología es la que, en el mejor de los casos, más frecuentemente aparece en el mercado como la más utilizada. Es, también, la menos representativa y la más imprecisa de las tres que presentamos aquí. Se basa, principalmente, en "supuestos", por lo tanto implica un elevado nivel de subjetividad, y no resulta útil para justificar las inversiones frente a los niveles de la Alta Dirección.

Por sus características, la construcción de un modelo bajo este enfoque es relativamente rápida, tomando en promedio entre 1 y 2 semanas. La aplicación ideal es la priorización de tareas en el área de IT para el desarrollo de los planes de acción. Forma parte también del inicio de los procesos del análisis de las diferencias (Gap Analysis), tanto respecto al estándar ISO 27001 como a ITIL.

## 2. Enfoque Estadístico

Este enfoque es el puntapié inicial para desarrollos más avanzados de seguridad de la información, ya que advierte sobre "lo puede pasar", sin resultar representativo de la organización en particular. Es una herramienta para generar preguntas, más que para proveer las respuestas.

Siempre hablando en forma general, el desarrollo de un modelo para este enfoque debería tomar entre 4 y 8 semanas, de acuerdo a la organización, la complejidad y el tipo de procesos de negocio que se analicen. La aplicación ideal es la concientización para todos los niveles de la organización. El desarrollo de un modelo bajo este enfoque requiere de apoyo externo, que complemente la tarea de los recursos internos aportando información, estadísticas, relevamientos de mercado, y know-how específico sobre los riesgos inherentes a determinadas tecnologías.

## 3. Enfoque Probabilístico

Este es el método más preciso para el cálculo de ROSI, y el más representativo de la organización en particular. Por el mismo motivo, análisis realizado para una empresa y en un momento determinado, no puede extenderse a otras organizaciones, por el contrario, los modelos no son genéricos sino individuales y específicos. Este es el enfoque que nos permite "hablar de igual a igual" con los Departamentos de Finanzas Planeamiento Estratégico de la organización.

Se combinan distintas herramientas: "Consultivas" (Análisis de Riesgo, GAP Analysis) y "Probabilísticas" (Método Montecarlo, Matrices de Markov).

Por su complejidad, el desarrollo de un modelo de ROSI de acuerdo a esta metodología podrá tomar entre 8 Y 12 semanas, aunque según el grado de desarrollo de la seguridad de la información en la organización, este tiempo podría extenderse en un máximo de 4 semanas, en forma genérica. Este enfoque requiere de un apoyo externo significativo para la elaboración de los modelos probabilísticos, como también, para el desarrollo detallado del análisis de riesgo de la organización y los procesos de negocio que se están considerando.



## ***Recomendaciones***

Si bien la extensión y el objetivo de esta nota no alcanzan para profundizar en el desarrollo detallado de las metodologías que presentamos, mencionaremos algunas de las recomendaciones importantes a la hora de encarar el desarrollo de un modelo de ROSI:

### **Representatividad**

Debe ser el máximo objetivo del análisis, ya que los modelos genéricos no sirven para justificar inversiones, y tomar decisiones en base a análisis desarrollados para otras organizaciones y/u otros contextos, eleva aún más el nivel de riesgo.

### **Impacto en el Negocio**

Las inversiones deben analizarse en función de los procesos de negocio de la organización, descartando aquello que no tiene un impacto real en la rentabilidad, que es uno de los principales indicadores de una organización.

### **Reconocimiento**

Un análisis de ROSI válido, es reconocido por las áreas de Finanzas, Planeamiento Estratégico, IT, y la Alta Dirección. Por eso debemos mantener al mínimo los componentes "subjetivos", y concentrarnos en los datos "objetivos" relacionados al negocio y en herramientas matemáticas, financieras y estadísticas.

En este sentido, contar con apoyo externo especializado es de una gran ayuda para disminuir la subjetividad en los análisis y generar confianza entre las distintas áreas de la organización.