

ROSI, RETORNO SOBRE LA INVERSION DE SEGURIDAD ©

Abstract

Ing. Carlos Ormella Meyer

ROSI es el Retorno Sobre la Inversión de Seguridad, derivado del conocido indicador financiero ROI, Retorno Sobre la Inversión, donde dicho retorno es la ganancia neta, es decir, la diferencia entre el beneficio o ingreso bruto y la inversión. En tal sentido ROSI también busca relacionar los *beneficios* y *costos* de una inversión, en este caso respecto a la seguridad de la información.

Sin embargo el ambiente de análisis no es tan similar al de un ROI que como resultado de una inversión apunta directamente a determinar beneficios “positivos”, es decir, ingresos monetarios efectivos en el flujo de caja de una empresa.

En el caso de ROSI la situación es algo diferente. Efectivamente, frente a las *pérdidas* que pueden producirse como consecuencia de incidentes de seguridad tales como ataques, fallas o errores, ROSI se aplica para identificar cuánto ahorraría o dejaría de perder una empresa, gracias a un sistema o proyecto de seguridad que mitigue los efectos correspondientes a tales incidentes.

Esto nos dice que la *reducción en las pérdidas* es de hecho un *beneficio*, por lo que por comparación con el ROI aquí podríamos decir que ROSI relaciona la reducción en las pérdidas ocasionadas por incidentes de seguridad con los *costos* que demande tal reducción.

Las pérdidas se mitigan gracias a la implementación de salvaguardas o contramedidas de seguridad. La determinación de tales salvaguardas puede hacerse trabajando, por ejemplo, dentro del marco de trabajo de la norma de seguridad ISO 17799 y la metodología establecida por la ISO 27001, anteriormente la BS 7799-2) para la implementación del SGSI (Sistema de Gestión de Seguridad de la Información), en base al análisis gap entre los resultados de una valuación de riesgos y los controles de seguridad de las normas.

La diferencia entre las pérdidas originales y las resultantes luego de implementar las salvaguardas en cuestión es el *ahorro o beneficio* mencionado antes, una suerte de ingreso o beneficio indirecto, con lo que adquiere características del **valor** de las salvaguardas aplicadas. Estas salvaguardas, a su vez, tienen su **costo**.

Yendo al cálculo específico del ROSI, siempre en base al ROI, resulta ser igual a la relación entre el *retorno* y el *costo* de las salvaguardas (la inversión en el ROI). El retorno, por su parte, puede verse como la ganancia incremental sobre el costo (la inversión en ROI) y, por lo tanto, resulta en este caso igual al *valor* de las salvaguardas menos el *costo* de las mismas. En definitiva tendremos:

ROSI = Retorno/Costo = (Valor – Costo)/Costo.

Para que un proyecto sea en principio aceptable, ROSI debe ser positivo, lo que ocurre cuando el *valor* es mayor que el *costo*.

Para determinar ROSI tenemos entonces que trabajar con dos variables: *Valor* y *Costo* de las salvaguardas. El cálculo de dichas variables resulta de definir que:

- a) El *Valor de las Salvaguardas* es igual a las pérdidas totales originales por incidentes sin tratar menos las pérdidas totales con los incidentes mitigados por las salvaguardas.
- b) El *Costo de las Salvaguardas* es igual a la Inversión Inicial más los Gastos Recurrentes. Estos gastos son los que se repiten periódicamente a lo largo del ciclo de vida del proyecto tales como licencias, mantenimiento, actualización, etc.

Para calcular las posibles pérdidas que puede producir *cada* incidente, se emplea la métrica de gestión de riesgos conocida como **ALE** (Expectativa de Pérdidas Anualizadas) que responde a un modelo *cuantitativo*.

ALE es igual al producto de dos variables: el valor probable del **impacto** monetario de un incidente, y el de la **frecuencia anual de ocurrencia** de dicho impacto.

Para cada variable se establece una serie de posibles valores discretos con el objeto de cubrir el espectro esperado completo. Para las frecuencias de ocurrencia, desde una muy baja frecuencia (por ejemplo, una vez cada diez años) hasta una elevada frecuencia (por ejemplo, una vez por día). Para los impactos, desde un valor pequeño hasta uno de gran magnitud. Las series generalmente son de cinco o más valores, y no necesariamente la cantidad de valores tiene que ser igual en ambas variables.

Ahora bien, ALE es un concepto típico de gestión de riesgos y fue estipulado hace casi 30 años. No contempla en forma explícita el efecto de las **vulnerabilidades**, componente que junto con las **amenazas** y los **activos** constituyen los tres factores determinantes de los *riesgos de seguridad de la información*. Efectivamente, hoy en día está claro que los **activos** pueden tener **vulnerabilidades** que pueden facilitar la acción de las **amenazas** sobre dichos activos.

Sin embargo, el impacto del ALE puede tomarse como un porcentaje del valor del activo en cuestión; es el llamado *Factor de Exposición*, que en nuestro caso puede verse como el efecto de las vulnerabilidades de dicho activo. Si el nivel de vulnerabilidades de un activo es alto, mayor será dicho factor y el impacto tenderá al valor del activo; si en cambio el nivel de vulnerabilidades es bajo, el factor disminuirá y el impacto será consecuentemente menor que el valor del activo; y finalmente si el activo no ofrece vulnerabilidades, el factor valdrá cero y no habrá impacto posible.

Aclarado el concepto extendido del ALE, resta su cálculo para cada uno de los incidentes en una tabla para cada escenario, el original sin tratar y el tratado o mitigado. En cada caso se determinan las pérdidas anuales totales, sumando los ALEs de todos los incidentes considerados.

Adicionalmente, en el escenario de incidentes mitigados se tabulan también las contramedidas propuestas junto con sus costos iniciales y gastos recurrentes anuales. También aquí se suman al final para establecer los totales de costos iniciales y gastos recurrentes de las salvaguardas.

La diferencia entre las pérdidas de las tablas de ambos escenarios será el *valor* de las salvaguardas totales, mientras que su *costo* total quedará también determinado en la tabla de incidentes mitigados. Con todo esto se puede determinar el ROSI correspondiente.

Sin embargo, hay que tener muy en cuenta que todo el proceso de cálculo surge de *estimaciones de expectativas* tanto de valores de impacto como de frecuencias de ocurrencia. Y que, además, dichas estimaciones se manejan con series de valores discretos, de modo que los valores intermedios en realidad quedan sin cobertura o sujetos a más apreciaciones, todo lo cual guarda un margen importante de incertidumbre.

El resultado es que esta situación generalmente no es muy aceptada, e incluso cuestionada, por parte del área financiera/administrativa de una empresa, precisamente por la volatilidad de los datos, y la imprecisión y errores en su determinación.

Frente a esta situación, una solución efectiva a estas disyuntivas parte de recurrir a la teoría de la *toma de decisiones*, que nos dice que en condiciones de riesgo los problemas que se plantean pueden analizarse por medio de la *teoría estadística y de probabilidades*.

A partir de este enfoque corresponde asignar a cada variable:

- a) Una serie de *rangos* de valores, cada uno con un *mínimo* y *máximo* por debajo y arriba respectivamente de los valores usados originalmente como valores discretos.
- b) Un tipo de *distribución estadística* (o sea la forma en que se distribuyen las probabilidades en un rango de valores). En general para este tipo de trabajos se asume una distribución *uniforme* para las frecuencias de ocurrencia, y una distribución *triangular* para los impactos. La distribución uniforme asigna igual probabilidad a todo un rango. La distribución triangular, en cambio, tiene en cuenta que el

valor “central” o *más probable* no caerá en el medio de la distribución puesto que en general los impactos (recordar que son valores monetarios) si bien podrían resultar algo menores de cada estimación, pueden llegar a ser bastante mayores. El resultado es un triángulo escaleno, lo que se conoce como una distribución asimétrica sesgada a la derecha, o sea hacia los valores mayores. Para aplicar la distribución triangular hace falta establecer no sólo el mínimo y máximo como se dijo antes, sino también el valor más probable mencionado.

Pero el modelo así establecido sigue siendo estático. Habría que estar haciendo a mano múltiples cálculos dentro de cada distribución y considerar los resultados en conjunto. En consecuencia, se necesita un mecanismo que, a partir de las variables de entrada y sus distribuciones, realice automáticamente dichos cálculos en forma independiente entre sí para que los resultados tiendan a un valor consistente.

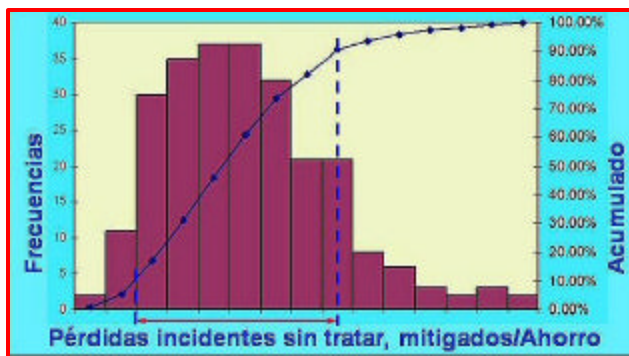
Esta consistencia es factible conforme dos teoremas de probabilidad estadística: la **Ley de los Grandes Números** y el **Teorema del Límite Central**. Estos teoremas indican que los resultados finales tenderán a un valor “central” o más probable con una distribución que responde a la **curva normal**, también conocida como **campana de Gauss**.

La simulación Monte Carlo puede ser el mecanismo adecuado para llevar adelante este proceso. La simulación Monte Carlo es un método que consiste en generar una y otra vez *números aleatorios* que para el caso se aplican a cada variable de entrada en base a la distribución estadística de cada una de ellas, y así producir *muestras* de los resultados que conformen lo definido en el párrafo anterior.

En nuestro caso, el proceso en cuestión se aplicará sobre los datos del escenario inicial sin tratar, así como al tratado con las salvaguardas para determinar así el ahorro que se produzca.

Cada uno de estos resultados se presenta, tal como se ve en la figura, como un histograma de las distribuciones de frecuencias de probabilidades para diferentes rangos de la variable de salida, así como las frecuencias acumuladas correspondientes.

A modo de ejemplo, analizando la gráfica acumulada del ahorro, se podría concluir por caso que hay un 90 % de certidumbre que el *valor* de las salvaguardas estará entre un mínimo y máximo adecuadamente acotados.



Los resultados presentados en la figura corresponden a una simulación limitada en el número de muestras. Para mayor precisión, las muestras debieran ser al menos de varios miles, como lo permiten los productos comerciales de simulación que trabajan como add-ins de Excel. Incluso de esta manera la respuesta se aproximará a la prevista por los teoremas mencionados.

Adicionalmente la simulación Monte Carlo puede facilitar el trabajo con un modelo *cualitativo* a nivel de las variables de entrada. Esto puede ser muy útil en situaciones en que es bastante difícil o complicado establecer valores numéricos para los impactos y frecuencias de ocurrencia de los diferentes incidentes.

La base de un proceso como el planteado reside en la valuación de riesgos, a partir de criterios precisamente cualitativos por ejemplo del tipo Bajo-Medio-Alto de impactos y frecuencias de ocurrencia del ALE. Este tipo de estimaciones, pese a no ser preciso en valores, puede ser más certero en los resultados puesto que a quien hace la estimación no se le estipulan niveles numéricos. Será luego tarea del analista, el mapear cada nivel (en la práctica generalmente se usan más de tres) a los rangos cuantitativos usados en el ALE.

Gracias a todo esto se pueden derivar estimados *cuantitativos* razonables de beneficio-costos a partir de criterios *cualitativos* de impactos y frecuencias de ocurrencia. Además, la determinación de las

contramedidas necesarias puede analizarse con mayor facilidad por medio de una matriz de riesgos, a partir de niveles cualitativos de los factores que los determinan.

En otro aspecto, acotaremos que un proyecto de seguridad debiera encararse como cualquier otro proyecto de negocios que tenga en cuenta el valor del dinero en el tiempo, es decir lo que diferencia una misma cantidad hoy, de aquí un año, dos, etc. Para ello los *valores futuros* de beneficios se traen a *valores presentes o actuales* aplicando un descuento que podría ser un interés del tipo bancario.

De esta manera se pueden calcular otros indicadores financieros, como por ejemplo el Valor Actual Neto (VAN o NPV) que puede verse precisamente como el *retorno* correspondiente del ROSI, y que establece un *valor monetario*. Esto puede ser muy importante como complemento del ROSI que hemos calculado, que por ser *porcentual* nada nos dice en forma explícita de los montos de los beneficios de un plan de seguridad.

ROSI puede resultar de gran utilidad especialmente en el análisis de un proyecto de seguridad que realice el área de finanzas o administración de una empresa. Aquí es donde ROI es conocido, por lo que un plan de seguridad debiera aportar algo similar a cualquier otro proyecto presentado a estas gerencias. De hecho se trata no sólo de convencer a los decisores sino incluso competir por recursos especialmente financieros con proyectos de otras áreas de la empresa.

Mientras un análisis basado en ROSI puede ser suficiente por sí mismo, también podría llegar a constituir el componente financiero del **caso de negocio** que representa un proyecto de seguridad. De hecho, un *caso de negocio* es algo que preferirían escuchar niveles de decisión gerenciales, no precisamente técnicos, como los mencionados antes.

© 2007 - Carlos Ormella Meyer