Ing. Carlos Ormella Meyer y Asoc.
Seguridad de la Información, Redes y Telecomunicaciones
Tel: 54-11-4371-4638
E-mail: ciprio@ciudad.com.ar

ROSI, RETORNO SOBRE LA INVERSION DE SEGURIDAD ©

Abstract

Ing. Carlos Ormella Meyer

Justificar la inversión en seguridad de la información nunca ha sido nada fácil, constituyendo de hecho una problemática con diferentes enfoques y puntos de vista. ROSI -***Retorno Sobre la Inversión de Seguridad***- es una herramienta adecuada y simple para justificar tal inversión, sobre todo cuando se recurre a la simulación Monte Carlo para poder así establecer resultados razonables adecuadamente acotados.

ROSI deriva del conocido indicador financiero ROI, ***Retorno Sobre la Inversión***. ROI mide la relación porcentual entre el retorno que produce una inversión y dicha inversión. El retorno, por su parte, es la ganancia neta o ganancia incremental, es decir, la diferencia entre el beneficio o ingreso bruto y la inversión correspondiente.

Hay algunas diferencias entre ambos indicadores. ROI, como resultado de una inversión, apunta a determinar beneficios “positivos”, o sea, 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. De esta manera, la *reducción en las pérdidas* es de hecho un *beneficio o ingreso indirecto*, aunque no haya un ingreso efectivvo.

Las pérdidas por incidentes 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 de la información ISO 17799 y la metodología establecida por la ISO 27001 (anteriormente la BS 7799-2), para la implementación de un **Sistema de Gestión de Seguridad de la Información**, **SGSI**.

El resultado es que tendremos dos escenarios de pérdidas por incidentes. El primero referido a las pérdidas originales y el segundo al resultante luego de implementar las salvaguardas en cuestión. La diferencia entre el total de pérdidas de cada una de estas situaciones es el *ahorro o beneficio* mencionado antes. Puesto que tal ahorro se deberá a la aplicación de ciertas salvaguardas, podemos considerar que las mismas tienen un determinado **valor**, dado precisamente por dicho beneficio.

Por otra parte, la *inversión* que considera el ROI, resulta ser el **costo** de dichas salvaguardas en el ROSI.

Como por lo dicho anteriormente, el retorno que produce la implementación de una salvaguarda es el incremento respecto de su costo, será:
ROSI = Retorno/Costo = (Valor – Costo)/Costo.

Por cierto, si en esta expresión aplicamos el concepto genérico de “costo-beneficio” resulta que, para que un proyecto sea en principio aceptable, ROSI debe ser positivo, lo que ocurre cuando el *valor* de las salvaguardas es mayor que el *costo* de las mismas.

Cálculo básico detallado de ROSI

Como ya se dijo, el concepto de *valor* tiene su base de cálculo en las pérdidas por incidentes. Ahora bien, para calcular las pérdidas que puede producir un incidente de seguridad se emplea la métrica de gestión de riesgos conocida como **ALE** o ***Expectativa de Pérdidas Anualizadas***.

ALE es igual al producto de dos variables: el ***impacto*** causado por un incidente, y la ***frecuencia o probabilidad anual de ocurrencia*** de dicho impacto.

Tel: 54-11-4371-4638
E-mail: ciprio@ciudad.com.ar

El proceso para determinar ALE puede comenzar estableciendo para cada variable una serie de valores discretos para así cubrir diferentes niveles del espectro esperado de posibilidades correspondientes. Cada serie generalmente es de cinco o más valores.

Como ya se dijo tenemos dos escenarios; el original con los *incidentes sin tratar* y el resultante con los *incidentes tratados o mitigados*. Para cada escenario se prepara una tabla para calcular el ALE de cada uno de los incidentes. En ambos escenarios, una vez hechos los cálculos individuales por incidente, se suman los valores obtenidos para determinar las pérdidas anuales correspondientes.

Adicionalmente, en la tabla de incidentes mitigados, para cada uno de ellos se tabulan las diferentes contramedidas propuestas junto con sus costos iniciales y gastos recurrentes anuales. También aquí se suman los valores individuales por cada incidente para establecer los totales de los mismos.

La diferencia entre las pérdidas anuales totales del escenario original y las del correspondiente a los incidentes mitigados será el ***valor*** del total del conjunto de salvaguardas, mientras que el ***costo*** total correspondiente quedará también determinado en la segunda de dichas tablas. Con todo esto se puede determinar el ROSI correspondiente.

Indicadores financieros

Ahora bien, 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 anuales de ocurrencia. Y que, además, dichas estimaciones se manejan con sendas series de valores discretos para cada variable, de modo que los valores intermedios en realidad quedan sin cobertura o en todo caso sujetos a más apreciaciones, todo lo cual introduce 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 todo esto, una solución efectiva parte de recurrir a la teoría de la **toma de decisiones**, que para el caso 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, en lugar de trabajar con series de valores discretos, para cada variable se establecen rangos consecutivos de valores, asignando a su vez a cada variable una distribución estadística adecuada para el caso; por ejemplo, uniforme para las frecuencias de ocurrencia y triangular para los impactos.

Ahora buscamos aplicar dos teoremas de probabilidad estadística: la **Ley de los Grandes Números** y el **Teorema del Límite Central**. Estos teoremas indican que si a las variables de entrada se aplican una gran cantidad de veces diferentes valores independientes entre sí, los resultados tenderán a un valor "*central*" o *más probable* con una distribución que responde a la ***curva normal***, también conocida como ***campana de Gauss***.

Para la correcta aplicación del proceso mencionado, se necesita un mecanismo que simule la situación planteada y, de esta manera, proporcione resultados que tiendan a valores consistentes.

La **Simulación Monte Carlo** es el mecanismo adecuado para llevar adelante el proceso en cuestión. Monte Carlo es un método que consiste en generar una y otra vez *números aleatorios* independientes entre sí, 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 múltiples ***muestras*** de los resultados que conformen lo definido antes.

En nuestro caso, el proceso se aplicará sobre las dos variables tanto del escenario inicial sin tratar como del tratado con las salvaguardas.

En cada escenario, la visualización resultante del total de muestras es doble: un histograma de las distribuciones de frecuencias de probabilidades para los diferentes rangos de la variable de salida, y una curva segmentada de las frecuencias acumuladas correspondientes.

Lo más interesante de los resultados obtenidos será seguramente el *valor más probable* de los costos de los incidentes, tanto sin tratar como tratados.

Para analizar el ahorro o beneficio, hay que plantear un tercer escenario basado en variaciones estadísticas independientes entre ambos escenarios básicos. De esta manera el resultado correspondiente mostrará el comportamiento de dicho ahorro o beneficio.

Justamente en esta tercera gráfica es donde se observan los resultados más concluyentes. Por un lado, el histograma de las frecuencias de probabilidades mostrará el valor *numérico* más probable del ahorro o beneficio que nosotros denominamos ***valor*** de las salvaguardas. A su vez, observando en la curva acumulada por ejemplo los valores correspondientes al 10% y 90% de dicha curva, se podrán proyectar dos cotas en el valor numérico de las salvaguardas. Con estas cotas se puede establecer con el 90% de certidumbre que el valor de las salvaguardas será igual o mayor a la cota menor y, al mismo tiempo, menor o igual a la cota mayor.

Para una consistencia adecuada en todos esos resultados, la simulación Monte Carlo debe trabajar al menos con varios miles de muestras, tal como lo permiten los productos comerciales de simulación que trabajan como add-ins de Excel.

En otro aspecto de la problemática planteada, acotaremos que en realidad un proyecto de seguridad (que habitualmente se extiende a un período de no más de tres años) debiera encararse como cualquier otro *proyecto de negocios* que tiene 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 se apela al enfoque financiero del flujo de caja descontado, por el cual los ***valores futuros*** de cualquier índole se traen a ***valores presentes o actuales*** aplicando un *descuento* que podría ser un interés del tipo bancario. De esta manera todos los valores involucrados en un proyecto se consideran en el mismo momento del tiempo: el momento inicial en nuestro caso.

Con este concepto se pueden *traer* al presente los ahorros o beneficios de cada año del proyecto y establecer así el **valor** de las contramedidas. Lo mismo puede hacerse con los *gastos recurrentes* anuales correspondientes, para sumarlos directamente a la inversión o costo inicial de las contramedidas y determinar el **costo** de las mismas.

Gracias al mismo mecanismo, adicionalmente se pueden calcular otros indicadores financieros, como por ejemplo el **Valor Actual Neto, *VAN* o *NPV***, que en este caso resulta ser precisamente el *retorno* correspondiente del ROSI, y que de hecho establece un *valor monetario*. Esto puede ser muy importante como complemento del ROSI que hemos calculado, que por ser *porcentual*, al ser visto sólo como resultado nada nos dice en forma explícita de los montos de los beneficios de un plan de seguridad.

Justificación de las inversiones en seguridad – ROSI y el caso de negocio

ROSI puede resultar de gran utilidad como herramienta para que el responsable de seguridad pueda justificar un proyecto, así como para que el área de finanzas o administración de una empresa pueda analizar dicho proyecto con metodologías de finanzas que le son conocidas.

Además, mientras un análisis basado en ROSI puede ser suficiente por sí mismo, también puede tomárselo como el componente financiero del ***caso* de negocio** o ***business case*** que represente un proyecto de seguridad. De hecho, un caso de negocio es algo más adecuado que preferirían analizar los más altos niveles de decisión, el directorio o steering committee de una empresa, especialmente para proyectos mayores.