

EL ROI DE LA SEGURIDAD Y LAS PRIMAS DE SEGUROS ©

Ing. Carlos Ormella Meyer

Introducción

Los temas de seguridad de la información se están volviendo cada vez más importantes en los intereses de una organización, en cierta medida por las leyes y regulaciones que vienen apareciendo, y también especialmente cuando se visualiza su contribución a los números financieros (1).

Incluso desde hace relativamente poco se está dando la “extensión” del concepto de *seguridad informática* al de *seguridad de la información*. Ya no basta hablar exclusivamente de riesgos de carácter técnico o sea de TIC o ICT (IT y Comunicaciones), sino que también hay que incorporar especialmente los *riesgos operacionales*. Si bien este tema siempre existió, viene teniendo mayor presencia e influencia en parte debido a la implementación del Nuevo Acuerdo de Capitales Basilea II para bancos internacionales. Ocurre que precisamente un tratamiento adecuado de los riesgos operacionales permite reducir las exigencias en los encajes bancarios ajustados a las directrices de Basilea II.

Las normas internacionales de seguridad juegan un papel crucial en estas nuevas problemáticas. La norma ISO 27002 (anteriormente ISO 17799) ofrece una visión holística de la seguridad de la información a nivel corporativo. Las *recomendaciones* de esta norma se extienden en forma integral a todas las funcionalidades de una organización, no sólo a las correspondientes a cada área sino también a las interacciones entre las mismas. Esta norma por cierto se complementa con la ISO 27001 que establece los *requisitos* para la implementación de un **sistema de gestión de seguridad de la información (SGSI)**, contando además con toda una serie de normas llamada a veces 27k, de las cuales ya hay varias publicadas.

Con estas normas puede usarse la metodología del mapeo de requisitos de diferentes regulaciones, tales como Basilea II, Sarbanes-Oxley y Continuidad de Negocios, a controles de seguridad de dichas normas. En Argentina incluso tal criterio se usa con las disposiciones de la Dirección Nacional de Protección de Datos Personales en el ámbito del cumplimiento a la Ley 25.326 de Habeas Data. Cualquiera de estas implementaciones con la adecuada definición de su alcance podrían llegar a certificarse conforme las especificaciones de la ISO 27001 que, por cierto, usa un marco de trabajo común al de la ISO 9001 de Calidad y otras normas similares.

Todo este panorama, desde la extensión de los escenarios de riesgos hasta las obligaciones legales, implica de hecho un incremento en los costos relacionados con la seguridad. Por tal motivo, cada vez es más importante su análisis para justificar tales costos como *inversiones*, frente al concepto clásico de que dichos costos son simplemente *gastos* a los efectos contables de las empresas.

Si queremos que un proyecto de seguridad sea considerado como una inversión y no como un gasto (y facilitar así su aprobación), habrá que presentarlo como cualquier otro proyecto especialmente desde el punto de vista de las finanzas. Acá es donde pueden comenzar algunas complicaciones para especialistas técnicos sin suficientes conocimientos del área de economía y finanzas, y también lamentablemente el porqué surgen algunas observaciones y opiniones poco fundadas que suelen escucharse y leerse.

Los mecanismos más tradicionales en los ambientes de negocios para analizar inversiones son los *indicadores financieros* tales como el ROI, TIR y VAN, entre otros. El primero, sobre todo, ofrece un enfoque muy adecuado para el análisis de las inversiones en seguridad de la información.

ROI y Seguridad

La forma más conocida para encarar los desafíos correspondientes al análisis de una inversión es determinar el **ROI**, *Retorno Sobre la Inversión*.

El ROI se expresa básicamente como el cociente entre el **retorno** y el **costo** de una inversión, donde el **retorno o beneficio neto** está dado por la diferencia entre lo que se obtiene por una inversión y el costo correspondiente a la misma.

En su forma más simple el ROI se ejemplifica con la compra de un bien, por ejemplo una acción bursátil, que al tiempo (quizás a los pocos días) se vende. En este caso, el retorno es simplemente la diferencia entre el precio de venta y el de compra (o sea la inversión). Y el ROI, a su vez, la relación entre dicho retorno y el precio de compra.

Si bien estrictamente ROI se basa en el capital invertido y su recupero, hoy día la mayoría de la gente de negocios lo considera, en forma genérica, como el retorno de una inversión financiera logrado a lo largo del ciclo de vida de un proyecto dividido por el costo total a lo largo de dicho ciclo, incluyendo la inversión inicial.

El concepto de *Flujo de Caja* se aplica a un proyecto como el resultado combinado de ingresos y egresos debidos al proyecto en cuestión para cada período de su ciclo de vida, generalmente de un año cada uno. Además, en un proyecto que se extienda a un año o más, habrá que considerar la diferencia entre el *valor futuro* y el *valor presente* del dinero, y la aplicación de cierto *descuento* para “traer” los Flujos de Caja de cada año a valores presentes y tratarlos con la inversión inicial para determinar así el resultado final del proyecto.

Pasemos ahora al ROI de Seguridad, mejor conocido como **ROSI** o *Retorno Sobre la Inversión en Seguridad*.

Obviamente ROSI tiene su antecedente directo en ROI. En consecuencia, tendremos que considerar los principios de cálculo de ROI y las derivaciones que surgen para su aplicación en ROSI, especialmente en cuanto a las condiciones y características que debe reunir para negociar una prima de seguro.

Debido a cierta complejidad del escenario planteado lo estudiaremos desde una perspectiva reduccionista, que nos permita formar una idea concreta de los diferentes factores básicos que intervienen en la concepción, cálculo y verificación de una solución a esta problemática. Para ello hay que reconocer y encadenar la serie de temas que se enumeran a continuación:

- a) Metodología de cálculo: ALE, LDA, Bayes, Efecto de las colas.
- b) Los conceptos de un ROSI integral.
- c) ROSI y los valores de entrada.
- d) Manejo de la Incertidumbre y la Simulación Monte Carlo.
- e) Métricas.
- f) ROSI y las Primas de Seguro.

ALE

Hace casi 30 años NIST (entonces NBS) fue quien introdujo el concepto de **ALE**, como *Expectativa de Pérdidas Anuales*. ALE es la sumatoria del producto de cada uno de los **impactos** de incidentes por la **probabilidad anual de ocurrencia** de los mismos (2).

De esta manera, ALE puede verse como un *indicador de riesgos* y, de hecho, como base fundacional de la **valuación de riesgos**, de modo tal que su uso se extiende a los diferentes métodos y aproximaciones que analizamos en este trabajo.

Los riesgos pueden ser específicos de los negocios, pero también de todo lo que pueda afectarlos, como precisamente ocurre con los inherentes a la seguridad de la información.

Por todo lo dicho hasta acá podemos considerar que ALE responde a un modelo **cuantitativo** para el análisis de riesgos, en nuestro caso el cálculo de las pérdidas producidas por incidentes de seguridad. Además, que ALE requiere *valores discretos* para su cálculo, así como que se presupone que dichos datos están basados en la historia de eventos ya ocurridos.

Si tales valores discretos no son completamente exactos y/o no muy confiables, se puede circundar en parte esta limitación aplicando la expresión semicuantitativa de Courtney. Courtney trabaja tanto para los **impactos** como para las **frecuencias de ocurrencia anual** con ocho rangos escalonados en forma decimalizada.

LDA

Es frecuente que los resultados correspondientes al ALE de cada uno de los posibles incidentes se repitan, por tener iguales ambos factores, o bien diferentes pero produciendo igual producto. Cuando los resultados agrupados de esta manera se grafican en función de la cantidad de veces o frecuencia a lo largo de un año de un mismo resultado, se obtienen las **pérdidas agregadas** o **pérdidas acumuladas**.

En la práctica los valores así obtenidos se vuelven a agrupar ahora en rangos de menor a mayor, con lo que el resultado es un histograma de barras.

Generalmente un histograma puede aproximarse con una curva continua que señala la forma en que varían los resultados. Se trata de una curva de *distribución estadística*, denominada específicamente **función de densidad de probabilidades**. Una distribución de probabilidades muy conocida es la llamada **campana de Gauss o curva normal**.

En el caso de ALE, tendremos una curva representativa de la distribución de las pérdidas por incidentes. El resultado obtenido se denomina **Aproximación de Distribución de Pérdidas LDA**.

La principal característica de LDA, y como vimos antes también del propio ALE, es que enfatiza el uso de datos internos históricos y supuestamente confiables.

Pero además, bajo el esquema LDA se puede obtener el **Valor en Riesgo, VaR**, un conocido indicador en las áreas financieras así como las de riesgos de crédito y mercado, y también presente en los cálculos de riesgos operacionales conforme Basilea II.

El VaR cuantifica la *máxima pérdida potencial* para un determinado **nivel de confianza**, un número que señala el percentil para dicha pérdida y que se expresa en forma porcentual, por ejemplo 98% para el percentil 98. En la práctica el VaR se toma en no menos del 95% y en algunos casos hasta fracciones por arriba del 99%.

Para precisar la importancia del VaR, recordemos que las funciones de distribución generalmente se reconocen por un indicador tradicional como lo es su **valor medio**. Este valor medio en nuestro caso señala las **Pérdidas Esperadas** especialmente en el contexto de Basilea II. Ahora bien, el valor medio puede ser mayor que el **valor más probable** (o sea un pico máximo en la curva de distribución), ya que en los casos que analizamos, *las curvas de distribución no son simétricas* como la curva normal sino asimétricas sesgadas a la derecha, lo que implica una cola más ancha en el extremo mayor de la distribución.

De cualquier manera, en los ambientes de finanzas e incluso en nuestro caso es mucho más usual trabajar sobre condiciones extremas, con lo que el VaR es más adecuado que los indicadores anteriores.

Finalmente, cuando no se dispongan de suficientes datos históricos, se puede seguir usando LDA con el mejor ajuste posible de los datos existentes a una curva de distribución adecuada.

Bayes

Sin embargo para un escenario como el recién planteado es preferible emplear métodos estocásticos, es decir aleatorios, tales como la **Aproximación de Bayes** o especialmente la **Simulación Monte Carlo**. Veamos Bayes en este punto dejando Monte Carlo para más adelante.

Bayes es un método de inferencia que se basa en una aproximación que combina datos **cuantitativos y cualitativos**. Los datos cuantitativos, como antes, son datos históricos internos o externos a la organización. Los cualitativos se corresponden con información subjetiva surgida de opiniones (generalmente de expertos), conformadas por medio de algún método de investigación prospectiva como Delphi. La incorporación de este tipo de datos cualitativos constituye una significativa ventaja propia de esta aproximación.

La clave de Bayes está en poner a prueba información anterior de datos opinables en función de las probabilidades de datos históricos. La distribución resultante o *posterior* es función de la distribución de las opiniones de expertos y de las observaciones o muestras de datos a partir de dicho conocimiento *anterior*.

El uso de esta aproximación es habitual en las áreas de ciencias básicas como la Física y Química, y especializadas como Meteorología y Paleontología, así como también precisamente en Seguros.

Efecto de las colas

Pero hay otra cuestión importante a considerar. ¿Qué pasa con los eventos de seguridad a los que ALE prácticamente no aporta nada más allá del nivel de confianza del VaR?

Tales tipos de eventos se corresponden con incidentes que se dan con una frecuencia anual de ocurrencia cercana a cero (por ejemplo una vez cada 50 años), de modo que aunque puedan ser de alto impacto producen un ALE muy pequeño..

Este tipo de incidentes, entonces, se ponen de manifiesto en la cola superior, incluyendo especialmente la porción de la curva de distribución por arriba del VaR estipulado.

Situaciones como éstas implican una curva de distribución con una **cola ancha** (*fat-tail*) en los percentiles más elevados de la distribución, lo que hace a la asimetría y al sesgo a la derecha ya mencionados.

Todo esto nos dice que en lo posible hay que considerar el histograma en su totalidad y no sólo la curva ajustada de distribución que puede representarla bastante bien en su mayor parte, aunque no lo suficiente precisamente en el extremo superior.

Ahora bien, sabemos que VaR mide hasta cierto percentil de una distribución y no tiene en cuenta las pérdidas extremas más allá del nivel de confianza fijado. Sin embargo, las pérdidas en cuestión podrían llegar a ser trascendentes.

Hay dos formas de estudiar dichas pérdidas: o como una extensión o complemento de la curva de distribución general, o bien exclusivamente sobre la propia cola sin considerar la forma de la distribución del cuerpo principal.

La primera considera las pérdidas más allá del VaR por medio del **ES (Shortfall o Deficit Esperado)**, un indicador usado en finanzas para medir riesgos financieros. El Shortfall Esperado es simplemente el promedio de las pérdidas en la porción entre el VaR y el 100% de la cola.

La otra forma de considerar las colas se basa en la **Teoría del Valor Extremo** o **EVT**, desde hace cierto tiempo usada en el campo actuarial y últimamente también en el campo financiero, sobre todo en lo relativo a la **gestión de riesgos**

El mecanismo más usual para aplicar la EVT es por medio del **POT**, una técnica que considera los picos en los percentiles más elevados de la curva o histograma de la distribución, a partir de un percentil que podría o no ser el del VaR.

POT también es un promedio, pero en este caso de los *picos* de pérdidas con probabilidades mayores a cierto *umbral* que generalmente está dado por el promedio de las probabilidades en los percentiles extremos considerados.

Este método permite la determinación de una adecuada distribución estadística en la cola superior, por ejemplo por medio de una curva de distribución Pareto. Incluso hasta podría establecerse una distribución que se adapte no sólo a los valores del cuerpo principal sino también a los de la cola. Para esto se puede recurrir a una combinación adecuada en base a Pareto o Weibull. De esta manera también se podría establecer una aproximación más realística del VaR.

Los conceptos de un ROSI integral

Si bien ROSI deriva del ROI, nos encontramos con algunas diferencias que es necesario aclarar y tener en cuenta.

En primer lugar, por lo general ROSI no produce ingresos contables directos. Sin embargo, lo que en realidad ocurre es que gracias a un proyecto de seguridad y las medidas correspondientes *se reducirán las pérdidas* que por incidentes de seguridad podrían existir con anterioridad.

Para ello en primer término se establecerán las pérdidas debidas a cada uno de los incidentes de seguridad *antes y después* de aplicar dichas medidas de seguridad, para luego totalizar cada circunstancia por separado y determinar el ahorro total correspondiente.

Dichas medidas de seguridad o **salvaguardas** pueden ser de diferentes tipos. Algunas son para **prevenir** incidentes, produciendo una reducción en las *probabilidades de ocurrencia* de los mismos. Otras son para **remediar** los efectos de tales incidentes, reduciendo la magnitud o monto de los *impactos* correspondientes. Finalmente hay salvaguardas que producen ambos efectos. De una u otra forma el objetivo es siempre el mismo: reducir o mitigar las pérdidas, lo que equivale a un ahorro o ganancia indirecta.

Tal reducción de pérdidas es un beneficio perfectamente aceptable, de manera similar a lo que ocurre en la práctica con ROI al considerar por ejemplo las ganancias por aumento de la productividad y de la calidad, la disminución del esfuerzo, así como los beneficios derivados de la concientización y capacitación del personal.

Adicionalmente se puede considerar la reducción de ciertos costos indirectos, como los resultantes de procesos ineficientes, las pérdidas de oportunidad, e incluso en circunstancias especiales los costos intangibles como la pérdida de imagen pública. O sea que en definitiva, no todo es un ingreso monetario efectivo en un libro contable.

Ahora definimos el **valor** de las salvaguardas como igual a las pérdidas totales por incidentes sin tratar menos las pérdidas totales con los incidentes mitigados por las salvaguardas. Por lo dicho antes, el concepto ampliado de *pérdidas* incluye también los costos indirectos comentados.

A su vez consideramos al **costo** de las salvaguardas como los costos totales de las mismas, que incluyen no sólo la inversión inicial sino cualquier otro costo variable o recurrente (como la renovación anual de licencias).

De esta manera, la diferencia entre el valor y el costo de las salvaguardas resulta ser el **retorno** propio del proyecto.

En definitiva, a semejanza de ROI, ahora tendremos:

$$\text{ROSI} = \text{Retorno/Costo} = (\text{Valor} - \text{Costo})/\text{Costo}$$

Para los cálculos correspondientes nos basaremos en ALE, ya que es el método usado históricamente para calcular las pérdidas en forma cuantitativa por lo que su uso es directamente aplicable a ROSI (3).

Además, ROSI no debe considerarse como una estrategia para períodos cortos de tiempo. Entonces, puesto que un proyecto de seguridad puede extenderse a 2 o 3 años, un cálculo adecuado debe seguir también los lineamientos del flujo de caja descontado, tal como se comentara antes, por lo que habrá que manejar valores futuros y traerlos a valores presentes con el correspondiente descuento aplicado a los flujos de caja de cada año.

Por otra parte, para dar más fuerza en la práctica a un proyecto de seguridad, es conveniente que ROSI se complemente con otros indicadores financieros, que se calculan directamente a partir del mismo análisis de flujo de caja. Tales indicadores pueden ser:

a) El **IIR** o **TIR** (**Tasa Interna de Retorno**) que establece el máximo interés de descuento de los valores futuros para un proyecto en equilibrio (o sea sin pérdidas ni ganancias) permitiendo su comparación con otros proyectos.

b) El **Payback** o **PRI** (**Período de Recuperación de la Inversión**), generalmente también descontado, que determina el momento del ciclo de vida del proyecto en que los flujos de caja traídos al presente igualan a la inversión inicial.

c) El **NPV** o **VAN (Valor Actual Neto)** que proporciona el valor monetario del beneficio neto de todo el proyecto y es, por lo tanto, un complemento muy importante a la relación porcentual que expresa ROSI (4).

ROSI y los valores de entrada

Analizada la metodología así como la concepción integral de ROSI conforme todo lo visto hasta ahora, hay que considerar, yendo un poco hacia atrás, la verosimilitud de los datos de entrada con que se realicen tales cálculos.

Porque después de todo, y de hecho un argumento de la compañía de seguros, ¿cómo se demuestra la validez de los valores de entrada para el cálculo de ROSI especialmente cuando hay escasos datos históricos? Y, por lo tanto, si efectivamente las medidas de seguridad harán que se reduzcan las pérdidas en los valores que se consignan.

Conseguir un ROSI plenamente tangible no es fácil, y no precisamente porque generalmente no haya un ingreso contable en la organización.

Se ha escrito bastante sobre algunos aspectos opinables de ROSI. Algunos lo hacen desde puntos de vista exclusivamente técnicos, con lo cual obviamente el enfoque no es total sino parcial. En este punto aparecen influencias más bien negativas como el ROSI preparado por algunos proveedores de productos de seguridad, que suele adolecer de fallas u omisiones en pos de presentar dichos productos en mejores condiciones competitivas.

Lamentablemente muchos especialistas técnicos (y no sólo los propios de una empresa sino externos que con notas periodísticas pueden confundir más aún) no poseen conocimientos adecuados de finanzas, estadísticas y a veces hasta de riesgos a nivel corporativo, es decir más allá de los específicamente técnicos. Entonces, por ejemplo, mal se puede explicar así al personal decisor de administración/finanzas de la propia empresa la problemática integral de las cuestiones que estamos analizando. A su vez, dicho personal lo que menos quiere escuchar es sobre cuestiones técnicas como virus, hackers y esas cosas, perdiéndose la posibilidad de su propio aporte a todo este análisis.

Estos enfoques limitados hacen que quienes no estén bien informados, puedan adquirir y/o mantener una actitud crítica respecto a ROSI, sobre todo si se hace un enfoque parcial de los riesgos, es decir, sin considerar la totalidad de la gama de riesgos del ambiente integral de la seguridad corporativa.

Efectivamente, cuando se analizan los riesgos no hay que olvidar que no son sólo los riesgos de carácter técnico, con vulnerabilidades de a lo sumo 2 o 3 niveles. En la actualidad, como se comentara al principio, los **riesgos operacionales** son cada vez más cruciales en los escenarios de seguridad de la información. Y las vulnerabilidades correspondientes a este tipo de riesgos se extienden a lo largo de una amplia gama de grises, muy relacionada con el comportamiento humano y las opiniones subjetivas de las personas.

En consecuencia, el análisis y cálculo puede y debe incluir todo tipo de riesgos, no sólo los del área tecnológica sino también los riesgos físicos, organizacionales y sobre todo operacionales. Un ROSI que no lo haga seguramente será cuestionable.

Manejo de la Incertidumbre y Simulación Monte Carlo

En base a todo lo revisado hasta aquí, puede considerarse que el cálculo de ROSI tiene suficientes fundamentos para su aceptación. Sin embargo, especialmente tanto si sólo hay escasos datos históricos, así como si no se trabaja con valores y probabilidades discretas y puntuales sino en forma de rangos, los resultados mantienen una condición de incertidumbre de cierta consideración. Este panorama seguramente entorpece y complica la evaluación y aprobación de un proyecto cualquiera, en nuestro caso de seguridad de la información, así como su consideración frente a una posible reducción de las primas de seguro.

El problema que así se presenta se puede tratar apelando a la **teoría de las decisiones** en condiciones de **riesgo e incertidumbre**.

Como en nuestro caso el grado de incertidumbre no es absoluto, las condiciones de riesgo pueden considerarse estadísticamente. Esto es similar a los seguros, aunque en este caso las presunciones se

basan en probabilidades bastante definidas gracias a la experiencia acumulada con el tiempo. La mejor solución para enfrentar dichas condiciones es complementar las metodologías comentadas antes con la **simulación Monte Carlo**.

La simulación Monte Carlo es un método estocástico para simulación por computadora que permite estudiar el rol de la **incertidumbre** sobre las variables bajo **condiciones de riesgo**. Con este mecanismo se pueden generar una y otra vez muestras aleatorias en base a distribuciones estadísticas conocidas.

De esta manera con la simulación Monte Carlo se pueden obtener estimaciones cuantitativas razonables y consistentes aplicando probabilidades y estadísticas adecuadas para una mejor entropía.

Concretamente, por diferencia entre las pérdidas anteriores y posteriores luego de la aplicación de las salvaguardas correspondientes se pueden establecer:

- a) El *valor medio* resultante de la aplicación de la *Ley de los Grandes Números*, gracias a que este mecanismo de simulación justamente posibilita que trabajen las leyes de las probabilidades.
- b) El *valor más probable* del ahorro o beneficio de un plan de seguridad.
- c) Un nivel aceptable de certidumbre para el monto del ahorro a obtener acotado por un *margen de confianza* dado por ejemplo por un 10% de probabilidades para un *valor mínimo* y un 90% para un *máximo*.
- d) El *VaR* para un 95% o más de nivel de confianza y casi siempre mejor determinado que con el LDA solamente.
- e) Los efectos de la cola superior debido a los incidentes de bajas probabilidades de ocurrencia anual pero alto impacto, por medio del *Expected Shortfall* o del *POT*.

La experiencia indica que cuando se ponen en práctica las consideraciones comentadas hasta aquí, el ROSI obtenido puede ser suficiente para un análisis fundado con el área administrativa/financiera de la organización, o de la compañía de seguros (5).

Incluso internamente aún mejores resultados pueden lograrse haciendo que tal análisis de ROSI constituya el componente financiero de un Business Case o Caso de Negocios de Seguridad de la Información. Por cierto, nada mejor para un CISO o Leader de Seguridad que hablar al personal de finanzas en su idioma: cómo aumentar la eficiencia, reducir las pérdidas, etc. manejando y usando conceptos como cash flow, valor presente, valor futuro, valor actual neto, etc. Y mejor aún, hablarles lo menos posible de virus, malware, etc.

Métricas

Además de todo lo visto, con el proyecto ya en marcha hay una cuestión más a considerar y que se refiere a los resultados obtenidos, cuyas verificaciones se realizan por medio de mediciones, también denominadas métricas.

Las métricas sirven principalmente para establecer, entre otros detalles, qué controles realmente se han implementado, así como el porcentaje de eficiencia y eficacia de los mismos en la reducción de las pérdidas de seguridad.

Ya el draft de la norma ISO 27004, próxima a ser finalizada, aporta sin duda la estructura adecuada para estas tareas. Mientras tanto hay buenos trabajos relacionados especialmente con las métricas a nivel de los 39 *objetivos de control* de la ISO 27002.

Además, la publicación 800-55v1 del NIST puede proporcionar una ayuda aún más granular en algunos casos. Si bien las medidas de seguridad del NIST no son las mismas de la ISO 27002, el NIST 800-53 ofrece un mapeado entre unas y otras.

Finalmente, en los últimos tiempos se han venido desarrollando interesantes modelos de **Balanced-Scorecard**, **BSC** (también conocido como *Tablero de Comando* o bien *Mando Integral Balaceado*), aplicados al desempeño de la seguridad de la información. Con BSC se pueden identificar indicadores de riesgos que incluso pueden facilitar su gestión al indicar la causa de dichos riesgos, especialmente los de carácter operacional. Por otra parte, la importancia de estos desarrollos radica en la mayor trascendencia dada últimamente al BSC en los ambientes de negocios. Y sin duda es una forma de llevar la seguridad de

la información a los niveles más altos de una organización no sólo a modo de concientización sino a su reconocimiento efectivo en el área de negocios.

ROSI y las Primas de seguros

¿Es todo lo anterior suficiente para renegociar una prima de seguros? En primer lugar y aunque parezca elemental, un análisis completo de ROSI es mejor que nada, con seguridad. En segundo término, no hay que olvidarse que las compañías de seguro también trabajan con estadísticas, no tan estáticas como se podría imaginar. Por ejemplo, ¿qué tal con los eventos de seguridad que seguramente surgen en organizaciones afectadas directa o indirectamente por los cracks financieros actuales?

Una cuestión inicial a considerar es qué se contrata específicamente que pueda ser afectado por la seguridad de la información. Para el caso habrá que ver la forma en que la compañía de seguros calcula este tipo de primas, algo que podría basarse en cuestionarios o investigaciones que quizás contengan cuestiones que justamente se tratan en una implementación ISO 27001, con lo cual ya habría una base común para negociar.

En cuanto a la renegociación misma, habrá que tener en cuenta que una prima menor implica una menor comisión para el vendedor, por lo que puede retacear su apoyo. Pero también por el otro lado, siempre la empresa contratante podrá considerar la aplicación de acciones estratégicas como el posible cambio de compañías.

Y para terminar, además de todos los aspectos propios de la *seguridad de la información*: ¿no sería más amplio un análisis que incluya la *continuidad de negocios* basado principalmente en la disponibilidad operacional de una empresa? Es muy probable, pero esto ya es otra historia.

Notas

(1) Este trabajo fue preparado para especialistas tanto de Tecnología como de Economía y Finanzas. Algunos conceptos serán conocidos por unos pero no por otros, y viceversa.

(2) ALE no se debe confundir con ROI. ALE es un valor monetario de *pérdidas* anuales. ROI es la relación (cociente) entre el *beneficio* neto de una inversión y el *costo* de la misma.

(3) ALE es un indicador conocido y de utilidad comprobada durante muchos años. Cuando se introdujo su uso en el tema de seguridad hubo lamentablemente quienes procuraron modificar su sentido demostrando quizás poco conocimiento de sus verdaderas implicancias. Por ejemplo, una redefinición hablando de un nuevo ALE al que al original se agrega el costo de las salvaguardas. Esta acción obviamente colisiona con la propia definición de ALE que habla de “pérdidas” con lo cual el parámetro de costos no es precisamente un ítem coherente. También se quiso modificar el ALE incorporando un supuesto porcentaje de reducción en base a la aplicación de las medidas de seguridad. Este mecanismo viene siendo usado por algunos proveedores para concluir que su producto podría reducir en un determinado porcentaje el ALE producido por ciertos incidentes. En realidad, tal criterio tampoco es aceptable puesto que aunque se acepte un porcentaje en la reducción de las pérdidas, esto no puede aplicarse directamente al *producto* ALE, sino individual e independientemente a sus *factores*, la **frecuencia anual de ocurrencia** o el **impacto**. Esto se debe a que generalmente los efectos específicos de las salvaguardas son para **prevenir** o para **remediar** respectivamente dichos factores.

(4) Justamente, a veces ROSI se encuentra expresado simplemente sólo por el *numerador* de su expresión original. Sin embargo, un simple análisis indica que tal numerador no es ni más ni menos que el NPV o VAN (Valor Actual Neto) correspondiente a todos los ingresos y egresos producidos en el período considerado de validez de la inversión con los valores futuros traídos a valores presentes.

(5) Se ha dicho que ROI en el contexto de seguridad no es exacto. En realidad tampoco un ROI es exacto cuando se lo estima a priori, salvo luego de hecha la inversión y medidos sus verdaderos resultados. Esto no impide su utilidad. No debemos olvidar que la certeza y precisión absolutas, felizmente, no son necesarias para tomar decisiones.