

¿Existe un retorno de inversión en seguridad?

1era parte: <http://bsecure.com.mx/articulo-66-6557-375.html>

2da parte <http://bsecure.com.mx/articulo-66-6583-376.html>

3era Parte: <http://bsecure.com.mx/articulo-66-6581-377.html>

Adrián Palma es licenciado en informática, cuenta con más de 22 años de experiencia en IT y seguridad de la información, está certificado como: CISSP, CISA, CISM y BSA. Ha sido conferencista a nivel internacional y catedrático del diplomado de seguridad en el ITESM, es ex presidente de la ALAPSI Internacional y actualmente funge como director de educación de la misma. educacion@alapsi.org

Tradicionalmente los montos destinados a seguridad se han identificado como un gasto, pero lo cierto es que esto es una inversión, cuyo retorno puede medirse.

En un mundo donde hackers, virus de computadoras y cyber-terroristas son un asunto cotidiano, la seguridad se ha vuelto prioritaria. Pero, ¿Cómo es que una organización llega a ser segura? ¿Cuánta seguridad es suficiente? ¿Cómo una compañía puede saber si su nivel de protección es adecuado? Y lo más importante, ¿Cuál es el retorno de invertir en esto y cómo se mide?

Esta última cuestión resulta especialmente difícil de responder, sobre todo si se considera que a la alta dirección no le interesa si los firewalls o los detectores y preventores de intrusos realmente protegen la red y los servidores de su organización.

Para poder determinar cuánto deben gastar en seguridad ellos quieren saber:

1. ¿Qué tan insegura es la empresa (vulnerabilidades) y cuánto le cuesta esto a la organización?
2. ¿Qué impacto está teniendo la falta de seguridad en la productividad?
3. ¿Qué impacto tendría un incidente catastrófico?
4. ¿Cuáles son las soluciones más rentables?
5. ¿Qué impacto tendrán las soluciones en la productividad?

Y es que antes de gastar dinero en cualquier producto, herramienta, dispositivo o solución, quienes toman las decisiones necesitan que esa inversión esté financieramente justificada.

Con la seguridad no es diferente, por lo tanto lo que se requiere es contar con métricas que muestren cómo los gastos ligados a esto van a impactar realmente a la organización, porque no hay razón ni justificación en implementar una solución si su costo verdadero es mayor que la exposición al riesgo.

De manera que conviene buscar un modelo para el cálculo del valor financiero de los gastos de seguridad, y ubicar técnicas que permitan obtener los datos necesarios para completarlo. Sólo que, como se supondrá, llevarlo a la práctica no es complejo, es complejísimo.

¿Cuál de las opciones genera el mayor valor?

Esa es la pregunta fundamental que se debe responder cuando se busca ubicar el Retorno en la Inversión (ROI). Este concepto es frecuentemente usado para comparar estrategias alternativas de inversión. Por ejemplo, una compañía puede usar el ROI como factor al momento de decidir si invertir en el desarrollo de una nueva tecnología o si ampliar las capacidades de la que ya tiene.

$$\text{ROI} = \frac{\text{Ganancias Esperadas} - \text{Costo de la Inversión}}{\text{Costo de la Inversión}} \quad (1)$$

Para calcular el ROI, el costo de una compra se compara con las ganancias previstas sobre la vida del artículo (1). Un ejemplo simple: si una nueva facilidad de producción costara \$1 millón de dólares y se espera que retorne \$5 millones en el curso de tres años, el ROI para el periodo de tres años es 400% (4x es la inversión inicial de las ganancias netas).

Una simple ecuación para calcular el Retorno de la Inversión de Seguridad (ROSI) es la siguiente:

$$\text{ROI} = \frac{(\text{Exposición del Riesgo, \% Riesgo mitigado}) - \text{Costo de la Solución}}{\text{Costo de la Solución}} \quad (2)$$

En un producto de scanner de virus, esta ecuación opera de la siguiente forma: la organización Patito S.A. de C.V. ha tenido varias infecciones por virus. Se estima que el costo promedio en daños y pérdida de productividad ocasionados por un incidente de este tipo es de \$25,000 pesos. Actualmente, Patito tiene cuatro infecciones de virus por año, pero espera contener por lo menos tres implementando un scanner de virus de \$25,000 pesos.

Exposición del riesgo: \$25,000 x 4x por año = \$100,000

Riesgo mitigado: 75%

Costo de la solución: \$25,000

$$\text{ROSI} = \frac{(\$100,000 * 75\%) - \$25,000}{\$25,000} = 200\% \quad (3)$$

Puesto así, la inversión del antivirus parece valer la pena, pero sólo porque se asume que el costo de un desastre es de \$25,000 pesos, que el scanner contendrá el 75% de los virus y que su costo es de \$25,000 pesos. Sin embargo, ninguno de estos números es exacto. ¿Qué pasaría si los ataques de tres de los cuatro virus costaran \$5,000 pesos en daños pero uno costara \$85,000? El costo promedio de pérdida sería aun de \$25,000. Pero aquí se presenta una cuestión interesante: ¿Cuál de esos cuatro virus lograría pasar o vulnerar el scanner? Si es uno cuyo impacto sea de \$5,000 pesos, el ROSI incrementaría cerca de 300% pero si es el de \$85,000 pesos, el ROSI se vuelve totalmente negativo.

Jugar con valores significativos para los factores en la ecuación del ROSI no es una tarea sencilla, al contrario es realmente compleja. Uno de los problemas más importantes es saber realmente el valor de las pérdidas por no tener seguridad. Otro es poder determinar qué porcentaje de riesgo será mitigado al implementarla.

A tales complicaciones se suma que muchas compañías no hacen este tipo de ejercicios simple y sencillamente porque de verían en la necesidad de realizar un análisis de riesgos, ligado a un manejo de los mismos, a lo cual se le conoce como Risk Management y desafortunadamente lo que se hace hoy en la mayoría de las empresas es un análisis de vulnerabilidades, que es una sola etapa del análisis de riesgos.

Además, no hay un modelo estándar para determinar el riesgo financiero asociado con los incidentes de seguridad, ni métodos estandarizados para establecer el riesgo si la efectividad de las soluciones de protección no es la esperada. Incluso los métodos para calcular el costo de éstas pueden variar gradualmente. Algunos incluyen solamente hardware, software y costos de servicio, mientras que otros incluyen factores de costos internos, incluyendo overheads indirectos e impactos a largo plazo en la productividad.

Asimismo, existen técnicas para medir la cantidad de exposición al riesgo, pero los resultados tienden a variar en exactitud. En la mayoría de los tipos de riesgo, la exposición puede determinarse si se consultan tablas actuariales creadas a partir de décadas de demandas y de estadísticas demográficas. Desafortunadamente en nuestro país y en América Latina no existen.

Por otra parte, la variabilidad en costos de la exposición puede conducir a resultados engañosos al intentar predecirlos basándose en datos actuariales que son mucho muy difíciles de conseguir.

En el ejemplo de Patito S.A de C.V., el costo de la exposición es engañoso, el promedio de \$25,000 pesos no refleja el hecho de que la mayoría de los incidentes cuestan muy poco mientras que otros cuestan mucho más.

¿Hay algún punto para calcular el ROSI si los datos subyacentes son imprecisos? Aparentemente sí, desde que algunas industrias han estado usando exitosamente, por décadas, métricas inexactas de ROI.

La publicidad, por ejemplo, se evalúa en base al número de espectadores potenciales, que continuamente es extrapolado de los datos de circulación y demográficos. Los compradores de anuncios asumen que el verdadero número de espectadores está directamente correlacionado al número de espectadores potenciales.

Si el método para determinar el ROSI produce resultados repetitivos y consistentes, puede funcionar como una herramienta útil para comparar soluciones de seguridad, basándose en valores relativos.

En ausencia de una exactitud pura, la alternativa es encontrar medidas consistentes para los factores de ROSI, las cuales devuelvan

resultados comparables. Esta tarea es mucho más fácil, y rompe la barrera de la exactitud que se ha mantenido en el ámbito de los libros.

Cuantificando la exposición del riesgo

Un método analítico simple para calcular la exposición al riesgo es multiplicar el costo proyectado de un incidente de seguridad (Single Loss Exposure o SLE) con su valor anual, estimado, de ocurrencia (Annual Rate Occurrence o ARO). El resultado de esto se conoce como: Exposición Anual de Perdida (ALE).

Mientras no existan métodos reales para estimar SLE o ARO, hay tablas actuariales que dan valores estadísticos promedio, basados en reportes de daño del “mundo real”. Estas tablas se crean a partir de los datos de demandas de seguros, investigaciones académicas o encuestas independientes.

$$\text{Exposición del Riesgo} = \text{ALE} = \text{SLE} * \text{ARO}$$

Es muy difícil obtener datos acerca del verdadero costo de un incidente de seguridad (SLE), porque muy pocas organizaciones los evalúan con éxito. De hecho, los que no tienen un impacto inmediato en una organización ocurren sin que nadie se dé cuenta.

Por lo regular, cuando se declara un incidente, la organización está ocupada arreglando el problema y no se preocupa por saber el valor de su impacto. Después del desastre, el apuro interno y las preocupaciones por la pérdida de imagen pública vuelven invisible a tal suceso. Como resultado de esta “respuesta avestruz”, el volumen de datos en las pocas tablas actuariales que existen es por demás deficiente.

Hasta hoy, el mejor dato actuarial se ha generado de esfuerzos tales como el estudio del Instituto de Seguridad en Computo (CSI) y el FBI, en el que a las organizaciones se les pide estimar el costo de incidentes seguros para varias categorías, durante el curso del año. Desafortunadamente, los métodos usados para calcular estos costos, varían de organización en organización.

Afortunadamente para obtener el ROSI la exactitud del costo del incidente no es tan importante como una buena metodología para calcularlo y reportarlo. Sería bastante complejo lograr que las compañías estuvieran de acuerdo sobre una técnica estándar para tabular el costo interno de un incidente de seguridad. Además, el foco debe estar en los factores que son medibles y que están correlacionados directamente a la criticidad del evento.

Valorar la pérdida de productividad y los tiempos muertos en los incidentes de seguridad brinda un nuevo significado al retorno de inversión en las estrategias de protección.

En la primera de las tres partes de esta serie de artículos en los que se identificará como puede medirse el retorno de inversión en seguridad de IT se hablaba de la necesidad de ubicar métricas que muestren cómo los gastos ligados a esto impactan realmente a la organización. A los ejemplos anteriormente dados se agrega ésta otra serie de opciones.

Un costo significativamente potencial para cualquier compañía es la pérdida de información sensible. En las organizaciones valuadas por su información crítica y su propiedad intelectual, una violación a la seguridad, resultado del robo de datos sensibles puede generar un impacto alto, incluso si no trastoca la productividad.

En este caso, el costo de un incidente de seguridad está en función del valor estimado de la información sensible y de la propiedad intelectual bajo riesgo. Por lo que aplicaría utilizar estándares contables y modelos de valuación de los datos. Sin embargo, estos son extremadamente complejos y muy poco prácticos.

Otro costo representativo es la pérdida de la productividad asociada con un incidente de seguridad. Para muchas organizaciones esto es mucho más importante que el costo de recuperación de datos o de reparación de un sistema.

La seguridad puede estar directamente alineada a la salud financiera de una empresa, a través de la inclusión de la pérdida de productividad en el costo de un incidente o un desastre. Dicha inclusión forzaría automáticamente a que los proyectos de seguridad mejoren la eficiencia de la organización y eliminará aquellos que son justificados sólo por miedo.

Y es que la pérdida de productividad puede tener un alto impacto económico en la organización. Tan solo 10 minutos de tiempo muerto por día, por empleado, puede agregar una cantidad significativa de pérdida, tal como se muestra en la tabla 1:

Tabla 1

1000	empleados
* 40	horas / año, por tiempo muerto ocasionado por incidentes de seguridad
* \$90	por hora salario promedio
=3, 600,000 pesos	por año en pérdida de productividad

La conveniencia de adoptar la pérdida de productividad o el valor de la información sensible o la combinación de ambas como una medida de exposición al riesgo dependerá de la naturaleza de la organización y de cuál sea su preocupación mayor: robo, divulgación, modificación o disponibilidad de los datos o una combinación de estos.

Especialistas en seguridad pueden utilizar técnicas para poder valorar la información, aun con la complejidad y dificultad para llevarlas a la práctica, pero una pregunta interesante es ¿Cómo se puede medir la pérdida de productividad?

Algunas organizaciones miden la productividad usando una combinación de pérdidas y ganancias financieras y la evaluación del performance. El problema con este enfoque es que resulta imposible aislar el impacto de la seguridad de otros factores en la productividad (tales como un rendimiento bajo). Las técnicas de medir el tiempo muerto tampoco son adecuadas desde el punto de vista de que sólo previenen a alguien para que haga su trabajo.

Una hora de tiempo muerto de un servidor a las 3 A.M. usualmente no tiene un impacto significativo en la productividad. Es mucho más importante medir la percepción de un usuario final con respecto a tiempos muertos que impacten directamente su jornada laboral.

Una medida para conocer la percepción del empleado respecto a esto se logra con un estudio, diseñado correctamente, para ubicar la correlación entre su resultado y la evaluación financiera. Por ejemplo: si un departamento muestra una disminución en la percepción de tiempo muerto, deberá mostrar también un incremento en la productividad.

Un buen estudio hará preguntas cuyas respuestas impliquen un valor cuantitativo, como, ¿Cuánto spam recibe al día? Menos de 10, entre 10 y 30, 30 y 50 o más de 50. Los minutos promedio de tiempo muerto pueden estar asociados con cada respuesta. Por ejemplo: lidiar con entre 30 y 50 mensajes de spam por día puede causar hasta 10 minutos de tiempo muerto, especialmente si el usuario desconoce la diferencia entre spam y correos deseados.

La clave entonces para conseguir resultados consistentes de un estudio que mide la percepción del usuario es asegurarse de que las preguntas son cuantitativas, claras y que se puedan contestar sin pensar mucho. Un mal planteamiento sería: “Estime la cantidad de tiempo muerto que tuvo este mes”. Pocas personas podrían responder esto sin llevar un registro de las veces que les ha sucedido.

Así que la alternativa adecuada es, ¿Qué tan frecuentemente su servidor de archivos no está disponible por más de diez minutos. Y las siguientes opciones: diariamente, semanalmente, mensualmente o rara vez.

Una vez que las respuestas son evaluadas, los resultados serán un indicador del tiempo muerto mensual. Esto se puede convertir a una cantidad en pesos, usando los salarios como cuotas por hora.

Si el salario promedio de un departamento es de \$90 pesos por hora y el promedio de tiempo muerto es de 30 horas por mes, entonces la compañía está perdiendo \$2,700 pesos en tiempo de no productividad por empleado debido a los incidentes de seguridad relacionados.

Además, una valoración del tiempo muerto puede proporcionar un análisis post-mortem de la pérdida de productividad durante un segundo

incidente y este monto puede ser usado al calcular el ROI de las soluciones de seguridad, para prevenir problemas similares en un futuro.

El problema es que en la vida real tendría que existir un estudio combinando este tipo de análisis en una tabla estadística, donde se asocie la pérdida de productividad con incidentes particulares de seguridad.

Si esto se quisiera hacer, es posible usar la valoración del tiempo muerto para estimar ese desfaldo con un incidente que aún no ha ocurrido. Por ejemplo: si una organización quisiera predecir el impacto de un virus, podría realizar una valoración de tiempo muerto para contar con medidas generales de productividad. Por lo que se podrían tomar los resultados de la valoración y variar las respuestas de preguntas realizadas para pérdida de datos, no disponibilidad de la red etc.

El resultado podría ser un rango potencial, utilizable para calcular el ROI máximo y mínimo de una solución preventiva de un brote de virus. Una herramienta útil para este tipo de análisis es Monte Carlo Simulation, que automatiza el proceso de variar un número de factores en el mismo tiempo y devuelve un rango de resultados potenciales.

Otra alternativa para valorar el tiempo muerto es examinar el impacto general de la seguridad en la productividad de la organización. Las violaciones de seguridad y fallas de tecnología pueden causar significativas pérdidas de productividad cuando hay cierto overtime. La tabla 2 muestra sólo un pequeño número de factores que pueden hacer perder minutos de un lado y de otro. Una organización promedio generalmente tendrá por lo menos cinco de estos problemas que representarán por lo menos una hora de tiempo muerto por día.

El ROSI toma un nuevo significado si cada día de pérdida de productividad es usado como la figura de exposición al riesgo. La implicación es que una organización con un nivel de riesgo aceptable es decir con el nivel de seguridad que requiere tendrá menos violaciones de seguridad y menos fallas tecnológicas, por lo tanto tendrá menos pérdida de productividad.

Sin embargo, el riesgo que se corre con este enfoque es que las violaciones severas serán ignoradas, porque el foco se pone en problemas recurrentes y menores. Esto evade completamente el problema del cálculo de ROSI para un evento que probablemente no ocurra o uno de grandes dimensiones.

Pero aun así, si una solución de seguridad puede mejorarse por completo mientras se eliminan algunos de estos problemas se tendrá un ROSI positivo, incluso si no se calculó para un incidente serio o mayor.

Tabla 2 Causas Diarias Potenciales de Pérdida de Productividad

Problema	Tiempo muerto promedio en minutos
Caídas del sistema y aplicaciones	10
Filtrado de contenido	15
Ancho de banda y rendimiento	10
Políticas de seguridad inadecuadas	10
Cumplimiento de políticas de seguridad	10
Implantación y upgrades de sistemas de IT	10
Parches de seguridad para sistemas operativos y aplicaciones	10
Topologías de red inadecuadas	15
Virus, scanner de virus	10
Gusanos	10
Troyanos, key logging	10
Spyware	10
Popup Ads	10
Problemas de compatibilidad - hardware y software	15
Permisos basados en problemas de seguridad (usuarios/passwords)	15
Desorganización del sistema de archivos	10
Datos corruptos	15
Robo de datos o penetración de sistemas	15
Respaldos, Recuperación	15
Problemas de aplicaciones de usuario final	15
Tiempo total 240 minutos	

Los beneficios de contar con una estrategia de seguridad pueden cuantificarse a través de diversos factores, entre estos: el riesgo mitigado en la organización.

Determinar los beneficios de mitigar el riesgo es tan complicado como definir la exposición a éste. La mayoría de los problemas surgen del hecho de que la seguridad no crea directamente algo tangible, más bien, previene una pérdida.

Por ejemplo, el sistema de detección de intrusos de una organización mostró que contuvo 10 ataques el año pasado, pero en este año sólo cinco. La gran pregunta sería, ¿ese decremento fue debido a este dispositivo de seguridad o hubo cinco hackers menos atacando el sistema?

En realidad, una solución de seguridad es diseñada para mitigar ciertos riesgos. Si está funcionando adecuadamente, mitigará cerca del 100% de estos (85% para ser conservadores, recordemos que no hay control 100% efectivo). Por lo tanto, la cantidad de mitigación del riesgo es 85%.

Desafortunadamente, hay un número de serios problemas con este “enfoque”: una puerta bien cerrada es incapaz de mitigar el riesgo si la ventana de a lado está abierta; las soluciones de seguridad no trabajan solas, la existencia y efectividad de otras tendrán un efecto mayor si trabajan holísticamente; las barreras de protección raramente son implementadas para ser tan efectivas como sea posible, esto debido al impacto que tienen sobre la productividad; los controles llegan a ser menos efectivos con el tiempo, de modo que los atacantes siempre encontraran maneras de poder violarlos.

Así que un mejor enfoque es conducir una evaluación de seguridad basada en un análisis de vulnerabilidades. Ésta puede representar en cierta parte el riesgo que está siendo mitigado actualmente.

Evaluando la mitigación del riesgo dentro del contexto de la seguridad, en este caso para la red de la organización, los problemas de aislamiento mencionados anteriormente se evitan. Una buena evaluación tendrá también el nivel de impacto de seguridad en la implementación de las soluciones hechas, ya sea por motivos de uso y/o productividad.

La evaluación de una solución de seguridad puede realizarse como si ésta ya estuviera implantada. La diferencia entre el resultado de ese ejercicio y el estado actual de la seguridad es la cantidad de riesgo mitigado por la solución.

Para calcular el ROSI, el resultado pronosticado (no la diferencia) deberá usarse como toda la mitigación del riesgo, recordando en todo momento el enfoque simplista.

Pero la exactitud de los resultados dependerá de la calidad de la evaluación, que puede hacerse siguiendo los lineamientos publicados por grupos de estándares tales como: el Foro Internacional de Seguridad (ISF), el Instituto Nacional de Estándares en Tecnología (NIST), y la Organización Internacional de Estándares (ISO).

Cuantificando el costo de la solución

Sin embargo, en este punto, debemos de visualizar que el costo de una solución no es sólo el precio que tiene en su etiqueta. Hay que considerar también el costo asociado con la implementación y el entrenamiento del personal involucrado en su uso, así como el mantenimiento y el soporte. Pero esto tampoco es suficiente, una vez más, la productividad y la funcionalidad aparecen en escena.

La productividad es importante porque la seguridad casi siempre se asocia con el costo del beneficio, recordemos que hoy día la seguridad es vista como un mal necesario y algo que no aporta un real valor a la organización.

Incluso, la mayoría de las soluciones de seguridad terminan creando barreras que los empleados necesitan saltar para poder hacer su trabajo. Dependiendo del tamaño y frecuencia de estas barreras, el costo de la pérdida de productividad puede aumentar muy seriamente.

La tabla 3 muestra como con relativa facilidad se pierde el tiempo, debido a los “retrasos” creados por las soluciones implantadas para corregir problemas de seguridad:

Tabla 3: Pérdida de productividad causada por las soluciones de seguridad. *

Problema	Tiempo muerto promedio
Caídas del sistema y aplicaciones	10 mins
Eficiencia de ancho de banda y procesamiento	10 mins
Políticas de seguridad restrictivas	10 mins
Mejoras en el sistema de IT	10 mins
Parches de seguridad para Sistemas Operativos	10 mins
Problemas de descarga de archivos debido al Scaneo de virus	10 mins
Issues de compatibilidad - hardware y software	15 mins
Demasiados passwords / Permisos de problemas relacionados con seguridad	15 mins

* Datos reales de una organización en México

Claro que también tenemos el otro lado de la moneda, también es posible que una solución de seguridad incremente la productividad. Esto sucede cuando un efecto secundario de la solución llega a eliminar otros problemas significativos que la obstaculizaban. Por ejemplo, la implementación de un firewall puede requerir la reestructuración de la

red. La nueva estructura puede resolver serios problemas de ancho de banda, que previamente generaban mucho tiempo muerto.

Este tipo de impacto puede medirse a través de estudios de productividad, usados para estimar la exposición al riesgo (artículo anterior). Las respuestas dadas son ajustadas para asumir que la solución se ha implementado y la diferencia entre la productividad actual y la proyectada es el factor de impacto que necesita ser incluido en este cálculo.

Factoricemos la productividad dentro de nuestro reciente ejemplo con el scanner de virus de ViriCorp's. Podemos ver que si el costo de la solución excede los \$60,000 pesos, el ROI es del 0%, y, por lo tanto, no es sujeto de compra. Pero si el costo total del sistema permanece en \$30,000 pesos, hay un margen de \$30,000 pesos. Por 100 empleados ganando en promedio \$20 pesos por hora, ese margen se compara a 3.5 minutos de pérdida de tiempo muerto por día.

Si al implementar el scanner de virus se crean mas de 3.5 minutos de tiempo muerto cada día, resulta más efectivo no comprar el scanner. Por otro lado, si éste puede eliminar el tiempo muerto, nulificando el impacto del código malicioso, podría hacer al scanner menos atractivo en términos de ROSI.

Visión de largo plazo

Para las inversiones a largo plazo, la mayoría de los ejecutivos financieros querrán factorizar el valor del dinero en el tiempo. Después de todo, el dinero gastado en seguridad es dinero que pudieron haber invertido en otros lugares. Por ejemplo, imagine que usted debe elegir entre dos soluciones de protección, una cuesta \$100,000 pesos y la otra \$50,000 pesos, al año, por dos años.

Ambas soluciones cuestan al final \$100,000 pesos. Pero la segunda solución se vuelve más atractiva ya que deja la opción de invertir los otros \$50,000 pesos en algo más por un año. El verdadero costo de la segunda solución es en realidad menos de \$100,000 pesos, cuando la inversión potencial está factorizada. Este costo de "ajuste" se llama: Valor Presente Neto (VPN o NPV, en inglés).

Uno de los factores más importantes al calcular el Valor Presente Neto es el porcentaje de descuento, es decir la cifra que se podría obtener al colocar el dinero en alguna otra forma de inversión. Otro elemento interesante de información puede obtenerse al imaginar que porcentaje de descuento es necesario para que el resultado de un VPN sea cero. A esto se le conoce como: Porcentaje de Ganancias Internas (PGI o IRR, en inglés), y básicamente indica que porcentaje ha ganado la inversión. En general, tener PGI arriba del porcentaje de descuento es una buena señal.

En la mayoría de los casos, el VPN y el PGI son mejores indicadores que un simple calculo de Ganancias de la Inversión. Pero si usted no puede pronosticar exactamente el tiempo o magnitud de los costos y los

beneficios sobre el tiempo de vida de la inversión, obtendrá resultados engañosos.

Para ilustrar el problema veamos el VPN y el PGI de un dispositivo de seguridad con un costo de \$10,000 pesos. En un primer ejemplo, el dispositivo previene un incidente de \$50,000 pesos, en el quinto año después de su instalación. En el segundo ejemplo, lo hace durante el primer año.

	%	Xosto	Y1	Y2	Y3	Y4	Y5	VPN	PGI	ROSI
#1	0.05	-10000	0	0	0	0	5000	\$27,786	38%	400%
#2	0.05	10000	- 50000	0	0	0	0	\$35,827	400%	400%

Desafortunadamente, nadie puede predecir cuando un dispositivo de seguridad va a prevenir un incidente. Como resultado, una solución es para garantizar los ahorros a través del ciclo de vida del equipo. Aunque se podría también asumir que el dispositivo será más efectivo al inicio de su vida, y perderá efectividad con el paso de los años:

	%	Costo	Y1	Y2	Y3	Y4	Y5	VPN	PGI	ROSI
#3	0.05	-10000	10000	10000	10000	10000	10000	\$31,709	97%	400%
#4	0.05	-10000	17500	15000	10000	5000	2500	\$33,316	153%	400%

El problema al usar el Valor Presente Neto para inversiones de seguridad es que la exactitud es crítica si se quieren obtener resultados comparativamente significativos. En cuanto al ROSI, éste no factoriza sobre el valor del dinero en el tiempo, pero puede proveer figuras comparables y consistentes aun con datos inexactos. Así que habrá que elegir si se quiere ser significativo o preciso.