Universidad de Buenos Aires
Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Maestría en Seguridad Informática

Tesis

Evaluación de la seguridad de la información desde la perspectiva económica

Autora: María Patricia Prandini

Director de Tesis: Doctor Raúl Saroka

Año: 2012
Cohorte 2009

Declaración Jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADO
Nombres y Apellidos: María Patricia Prandini
Número de documento: 13.530.756

RESUMEN

La visión de la seguridad de la información que brinda la Economía habilita una mirada imprescindible para insertar esta función en la organización. Así, los responsables de áreas de seguridad deben justificar los costos y beneficios de sus iniciativas, utilizando para ello una serie de métricas económico-financieras.

Sin embargo, una encuesta realizada a especialistas demostró que estas herramientas son poco conocidas y su uso es limitado.

Desde una perspectiva más global, otros indicadores permiten también estimar el valor que la seguridad informática aporta a una organización. Entre ellos se encuentran el comportamiento de la cotización de las acciones frente a la difusión de fallas o ataques, los ciberseguros, el mercado de compra-venta de vulnerabilidades y el de contratos a futuro. El trabajo desarrolla las características de estos indicadores, sus fortalezas, debilidades y su confiabilidad para reflejar el valor de la seguridad informática.

Finalmente, sobre la base de la encuesta, se analiza si la seguridad informática puede ser expresada en términos de beneficios y no solo como una forma de evitar pérdidas potenciales.

Se concluye que deben emplearse métricas e indicadores económicos para alcanzar una gestión exitosa de la seguridad informática, optimizando así los niveles de protección de la información.

Palabras Clave

Métricas económicas, inversión, seguridad informática, economía, beneficio

INDICE

PROLOGO

La presentación de este trabajo de tesis representa para mí la realización de un deseo largamente esperado. En este proceso, han sido muchas las personas que han hecho posible esta gran satisfacción personal. Entre ellos, quiero agradecer especialmente a los Docentes de la Maestría en Seguridad Informática. Todos y cada uno de ellos me han ayudado a construir este bagaje de conocimientos que me ha permitido llegar a este punto. En particular, quiero destacar a mi Director de Tesis, Dr. Raúl Saroka, por guiarme sabiamente en la elaboración de este trabajo. Deseo mencionar también al Dr. Hugo Scolnik, cuya oportuna invitación a postularme en la Maestría borró en el acto cualquier duda que hubiera tenido hasta ese momento. Para ambos, mi admiración y reconocimiento.

Quiero agradecer asimismo a Marcia Maggiore, con quien he tenido el privilegio de transitar estos años de estudio. Su acompañamiento y permanente apoyo han hecho gratos todos los momentos vividos durante el Posgrado.

No puedo dejar de mencionar también a mi papá, que ya no está físicamente conmigo, y a mi mamá. Ambos me enseñaron a disfrutar del aprendizaje permanente y la superación personal. A mis hijos Natalia y Martín, les agradezco que me hayan alentado en estos años de estudio y que hayan soportado sin quejas, tener una “mamá estudiante”. A mi esposo Rodolfo, le agradezco infinitamente su apoyo incondicional y su paciencia y que haya sido mi mentor para hacer realidad este deseo.

Finalmente, quiero dejar expresado mi orgullo por haber concluido mis estudios de Posgrado en la prestigiosa Universidad de Buenos Aires, a la que me siento honrada de pertenecer.

GLOSARIO

Las siguientes definiciones han sido adaptadas del libro “Cuestiones contables fundamentales” de Enrique Fowler Newton [10], excepto cuando expresamente se indica otra fuente.

Beneficio [18]	Ingreso total menos costo total incluidos tanto los costos implícitos como los explícitos.
Beneficio marginal	Beneficio adicional (o disminución del costo total) que se obtiene de generar una unidad adicional de producción.
Costo	Es el sacrificio que demanda o demandaría: a) La compra o producción de un bien, un servicio o un conjunto de bienes o servicios. b) El desarrollo de una actividad.
Costo marginal	Costo adicional (o aumento del costo total) necesario para producir una unidad adicional de producción (o sea, la reducción del costo total derivada de la producción de una unidad menos).
Costo de Oportunidad	Dadas varias alternativas de acción, el costo de oportunidad de una de ellas es lo que se pierde por elegirla, que es la diferencia entre lo que se habría obtenido si se hubiera optado por la mejor alternativa y lo logrado como consecuencia de la elección.
Ganancia	Aumento o variación positiva del patrimonio registrado en un período. También denominada superávit.
Gasto	Salida o consumo de activos o la asunción de pasivos, a cambio de un bien o servicio.

Ingreso	Aumento de los activos y disminución de pasivos originados en la producción o entrega de bienes, en la prestación de servicios o en otros hechos que hacen a las actividades del ente.
Ingreso marginal	Ingreso adicional que obtendría una empresa si vendiera una unidad adicional de producción.
Inversión [18]	Gasto en equipo de capital, existencia y estructuras.
Mercado [18]	Mecanismo en el que los compradores y los vendedores determinan conjuntamente los precios y las cantidades de las mercancías.
Pérdida	Disminución o variación negativa del patrimonio registrada en un período. También denominada déficit.
Riesgo [8]	La combinación de la probabilidad de ocurrencia de un evento y sus consecuencias.
Tasa de descuento	Es una medida financiera que permite determinar el valor actual de una erogación futura.
Teoría de los juegos[18]	Análisis de situaciones en las que participan dos o más personas que tienen intereses opuestos, al menos en parte.

INTRODUCCIÓN

No es sencillo tomar decisiones a la hora de decidir cuánto invertir en materia de seguridad de la información (en adelante, SI). Cuál debería ser el volumen de fondos a asignar a la protección de la información, cómo justificar la necesidad de obtener fondos para implementar determinados controles o cómo estimar el valor económico que la seguridad le aporta la organización, constituyen interrogantes que se comportan como verdaderos desafíos para quienes deben adoptar decisiones en esta materia.

Este hecho fue reconocido por una rama de la investigación en SI hace ya una década, además de desvelar cotidianamente a los responsables de áreas de Tecnología de Información (en adelante, TI) y SI en todo el mundo. En efecto, determinar el nivel óptimo de inversión en seguridad o ponderar en términos económicos cuánto le aporta a una organización requiere, además del necesario conocimiento técnico, de un análisis no trivial de costos, ingresos y beneficios esperados, para fundamentar las decisiones que se adopten.

Influyen en este proceso distintos factores vinculados a la incertidumbre, a las dificultades para determinar especialmente los ingresos atribuibles a una inversión en seguridad, a la ausencia de datos concretos respecto a la frecuencia e impacto de determinadas fallas o ataques informáticos o a las percepciones de quienes deben decidir, entre otras motivaciones. El propio proceso de evaluación del riesgo al que se expone la organización, base de la implementación de medidas concretas de mitigación y control, es un análisis complejo que también incide en la ponderación económica de la SI.

Una primera aproximación al tema indicaría que los aspectos técnicos, operativos y de exigencia legal son los que prevalecen en el proceso de toma de decisiones a la hora de decidir cómo invertir, y que los mecanismos económicos de medición de la SI no son utilizados en todo su potencial.

Ante esta problemática, este trabajo de investigación tiene por objetivo determinar cuán útiles son las métricas y otros indicadores económicos para ponderar el valor que la SI le aporta a una organización, tomando como base una serie de indicadores utilizados internamente en las organizaciones o surgidos de la observación del comportamiento de distintos agentes en el mercado, tales como accionistas, aseguradoras o potenciales compradores, entre otros.

Adicionalmente, se buscará determinar en qué medida la SI es percibida hoy en términos de beneficio para la organización, bajo la hipótesis de que al menos en ciertos escenarios, existen derivaciones positivas de la implementación de medidas de seguridad que, al ser percibidas por distintos actores, provocan la preferencia por aquellas entidades que promueven una activa protección de su información.

El estudio se nutrirá de los resultados de una encuesta realizada a especialistas, con el fin de echar luz sobre algunos de los aspectos señalados anteriormente.

EVALUACIÓN ECONÓMICA DE LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información tiene por objetivo la preservación de su integridad (asegurando su precisión, completitud y validez), confidencialidad (que se encuentre habilitada solo para quienes deben accederla en razón de su actividad o derecho) y disponibilidad (que pueda ser accedida cuando y desde donde sea requerida). Su presencia reviste cada vez mayor criticidad, tanto a nivel de las organizaciones como de las personas y es considerada actualmente como un atributo esencial de la calidad de la información.

Inclusive los países han empezado a considerar que la protección de sus infraestructuras críticas de información, es decir el conjunto de instalaciones, equipos físicos y de tecnologías de la información, redes, servicios y activos que se utilizan en sus ámbitos, es una actividad esencial para la preservación de la salud, la seguridad o el bienestar económico de los ciudadanos y para el buen funcionamiento del gobierno.

La propia integración en la vida cotidiana de las TI tiene como contracara, un nivel cada vez mayor de exposición frente a fallas y ataques en un escenario de mayor complejidad de los sistemas y plataformas que gestionan la información. Esto lleva a preguntarse si se destinan suficientes recursos a su protección o si la inversión es excesiva para los resultados obtenidos. En otras palabras, surgen interrogantes respecto a la efectividad de la inversión en mecanismos de aseguramiento de la información. Efectivamente, se ingresa en un terreno complejo cuando se intenta determinar el valor que su presencia o ausencia implican para una entidad. Las respuestas a estas preguntas provienen de un análisis económico de la SI.

Tanto desde la perspectiva técnica u operativa como económica, existen impedimentos para garantizar un nivel absoluto de seguridad, que proteja en un cien por ciento a la información y a los sistemas que la gestionan. En efecto, todas las organizaciones, cualquiera sea su tipo y dimensión, se enfrentan a la realidad de contar con presupuestos limitados. Por lo tanto, los responsables de las áreas de SI deben asignar prioridades

en la afectación de partidas determinadas y convencer a los niveles directivos de que le asignen mayores fondos para robustecer los mecanismos de protección de la información.

En los últimos años, las organizaciones se han visto en la necesidad de determinar los costos y beneficios de la inversión en SI. Esto obedece a diversos factores, tales como la necesidad de cumplir con requerimientos regulatorios, la aparición de nuevas amenazas y una dependencia cada vez mayor de las organizaciones respecto a las TI.

Métricas de la seguridad de la información

La palabra métrica proviene del latín "*metrĭcus*" y se refiere a aquello perteneciente o relativo al metro. El Diccionario de la Real Academia Española la define como "la medida o estructura de los versos" y sólo como adjetivo, lo considera como perteneciente o relativo al metro (unidad de longitud). No contiene una acepción que como sustantivo, lo relacione con medida o indicador de una determina medición. Sin embargo, debido a su amplio uso entre los profesionales de la ingeniería y la informática, la palabra "métrica" se utilizará en este trabajo bajo la siguiente definición, extraída de la norma ISO 27004:2005 [16]: "Una forma definida de medición (método de medición, función del cálculo o modelo analítico) y la escala correspondiente, utilizada para medir uno o varios atributos".

En el campo de la SI, las métricas constituyen valiosas herramientas utilizadas por los niveles directivos y por la línea para determinar la eficacia y eficiencia de sus programas de seguridad, el nivel de riesgo al que se expone la organización, aspectos específicos de un determinado sistema, producto o proceso o la habilidad del personal para comprender y llevar adelante distintas actividades vinculadas a la protección de la información y sus recursos asociados.

En particular, las métricas económicas de la SI, subconjunto de las métricas utilizadas en ese campo, representan una forma de justificar en términos de flujo de fondos, las inversiones y el valor que la SI le aporta a

una organización. Se expresan generalmente en base a moneda corriente o como porcentaje de ingresos o egresos financieros.

Por que utilizar métricas económicas

La necesidad de efectuar inversiones cada vez más importantes en este campo, que viene de la mano de un uso cada vez más generalizado de las tecnologías en actividades centrales de los negocios, han llevado a los niveles directivos a exigir que los responsables de TI y de SI deban explicar los ingresos potenciales de la inversión a realizar. Compiten en este sentido con otras áreas de la organización, más acostumbradas a realizar este tipo de análisis.

Efectivamente, antes bastaban el miedo, la incertidumbre y la duda (FUD, por las siglas en inglés de la expresión *"Fear, Uncertainty and Doubt*") para obtener los fondos requeridos. Al aumentar la frecuencia y el impacto de las ciberamenazas, los responsables de SI han empezado a valorar los métodos más racionales de la Economía para presentar sus requerimientos de fondos. En este sentido, Stanley [23] citando a Ekman y Hoyt, explica que el cuento del "pastorcito y el lobo" puede ayudar a conseguir el primer firewall pero en el largo plazo, se requiere una perspectiva más acabada.

Distintas perspectivas de las métricas económicas de la seguridad de la información

Böhme y Nowey [3] distinguen dos áreas de investigación en el campo del análisis económico de la seguridad de la información y de la utilización de métricas e indicadores de seguridad. La primera de ellas toma la visión financiera vinculada a la administración del negocio y basa el análisis en una serie de métricas cuantitativas que se emplean tanto como base para las decisiones en materia de inversiones futuras como para la evaluación de las medidas de seguridad ya implementadas.

El segundo campo identificado por los autores, utiliza el análisis del comportamiento de distintos actores que interactúan en el mercado, tales como los accionistas, las empresas proveedoras de tecnología, las

consultoras que brindan servicio de seguridad, las aseguradoras o quienes encuentran vulnerabilidades y las ofrecen al “mejor postor”. Este comportamiento y la manera en que se fijan los precios, permiten reunir información relevante para ponderar la SI desde una perspectiva económica. A partir del comportamiento de actores se derivan conclusiones, ya que al interactuar entre sí, sea en mercados genéricos como específicos a los bienes de SI, brindan indicios del valor atribuible a la SI.

*E*l presupuesto en seguridad de la información

La determinación de la inversión y los gastos vinculados a la protección de la información, así como los ingresos o menores egresos, tienen como objetivo primordial la protección de su confidencialidad, disponibilidad e integridad.

En el marco de un proceso de formulación presupuestaria, los egresos asociados a la SI surgen de inversiones de capital bajo la forma de activos, así como de costos operativos atribuibles a un período específico. En el primer grupo se ubican bienes tales como el hardware que por sus características forma parte del activo de una organización, constituyendo bienes amortizables. En el segundo grupo se incluyen por ejemplo, los sueldos y honorarios del personal dedicado a funciones de SI, ya sea interno o externo, los insumos específicos, las contrataciones de servicios, etc.

Dada la magnitud que ha alcanzado la utilización de las TI para funciones centrales de la actividad de la mayoría de las organizaciones, requiere de un adecuado reflejo en el presupuesto, con relación a la identificación de los ítems que se aplicarán para garantizar una adecuada protección de los activos de información y los datos. En efecto, siendo el presupuesto parte del ciclo administrativo que consiste en planear, gestionar y controlar, constituye un cálculo anticipado de los ingresos y gastos de la actividad que desarrollará una organización. Es una formulación que integra y coordina la actividad de la entidad y que expresa en términos monetarios para un período determinado, formulado con el fin de lograr los objetivos

fijados por la dirección. Constituye un valioso instrumento sobre el que se formulan sus planes, programas e instancias de control y medición.

Una encuesta realizada entre 167 especialistas en tecnologías de la información ubicados en Argentina y en otros países de Latinoamérica (ver descripción del perfil de los participantes en la sección A del Anexo I) entre octubre de 2010 y marzo de 2011 mostró que un tercio de los participantes en la muestra señala que en los presupuesto de las organizaciones donde se desempeñan no se distinguen rubros específicos para la SI (ver pregunta 7). La misma encuesta indica que un 39,6% se encuentra a cargo de su determinación o ha participado en el proceso de su elaboración.

A quienes respondieron que había participado en la formulación del presupuesto, o bien conocían su contenido, se les solicitó indicar a partir de una lista dada, los tres ítems que consumían un mayor presupuesto en sus respectivas organizaciones. Los más seleccionados fueron la seguridad en las comunicaciones (26,7%), la adquisición y el mantenimiento de hardware de seguridad (25,6%) y el control de acceso (23,3%).

Ampliando a los 10 elementos más seleccionados aparecen una variedad de temas como lo son la capacitación, la generación de un marco normativo y procedimental para la seguridad de la información así como la incorporación de elementos de hardware, software y comunicaciones.

Costos y beneficios de la seguridad de la información

Gordon y Loeb [12] afirman que desde una perspectiva económica, las organizaciones deben invertir en SI hasta el punto en el que una unidad monetaria de inversión produce mayor o igual unidad de ahorro al generar un efecto positivo en la minimización del riesgo asociado. Esto plantea una visión de la SI en términos de un análisis costo-beneficio.

En su trabajo, los autores analizaron el comportamiento de los decisores que en un contexto organizacional deben formular el presupuesto en SI y encontraron que éstos adoptaban distintos enfoques para este proceso. Entre estos enfoques, pueden citarse:

- La comparación en términos monetarios de los ingresos o ahorros esperados, una vez evaluados los riesgos, respecto a la inversión a realizar en SI. En este esquema, siempre que el valor monetario de los ingresos o ahorros esperados supere el valor de la inversión, las medidas a adoptar deben ser aprobadas.
- La adopción de un escenario simplificado respecto al anterior, en el que los decisores estiman los beneficios potenciales desde una perspectiva cualitativa y no cuantitativa. En este caso, el enfoque es menos complejo pero más intuitivo y por ende, menos preciso. Generalmente, se le asigna una categorización de “Alto”, “Medio” o “Bajo” al beneficio esperado de la adopción de determinada medida, tomando como base el impacto potencial que se estaría evitando.
- La consideración del impacto de una posible amenaza pero no de su probabilidad o viceversa. Este enfoque incompleto surge cuando no se obtienen datos suficientes para formular una estimación razonable y se caracteriza por la imposibilidad de estimar el riesgo en forma precisa. La problemática de la ausencia de datos confiables constituye un verdadero dilema para el campo de la SI. En efecto, los mismos decisores que evitan comunicar datos sobre fallas o ataques sufridos por temor a un perjuicio en la reputación de la organización o a posibles consecuencias laborales, luego no confían en las iniciativas para cuantificar los riesgos a las que se encuentra expuesta la información, justamente por la escasez de datos que las justifiquen.

Los autores antes señalados [11] indican que otras estrategias menos elaboradas para la formulación del presupuesto se limitan a ajustar el de años anteriores, aplicando algún tipo de incremento más ligado a cuestiones financieras, como el índice de inflación o los mayores o menores ingresos de la empresa.

En definitiva, la bibliografía existente coincide en que la determinación del presupuesto de SI es un proceso que debe partir de una efectiva evaluación de riesgos, ya sea cuantitativa o cualitativa. En el primer caso, se busca asignar valores numéricos a la probabilidad de ocurrencia y al impacto

de cada uno de los riesgos a los que se expone la organización, así como a los costos relacionados con la implementación de las medidas de seguridad correspondientes.

Bojanc y Jerman-Blazic [4] señalan que el propósito de un control de seguridad sobre un recurso es mitigar un riesgo, siendo la cota superior para la inversión que demande su implementación, el punto en el que el costo marginal de implementarlo se iguale al valor de los ahorros que surgen de evitar la materialización de una amenaza sobre dicho recurso.

Un problema de las técnicas cuantitativas de evaluación de riesgos es la ausencia de un método estándar, preciso y efectivo para el cálculo del valor de los activos y del costo de los controles que se deben implementar. Mucho más complejo es determinar el ahorro estimado a partir de la adopción de una determinada medida de control.

En contraposición, los métodos de evaluación cualitativos buscan determinar valores relativos y son conducidos en base a una combinación de cuestionarios y reuniones de evaluación. Suelen requerir un menor nivel de calificación del personal, ya que no demandan cálculos precisos. Su uso se recomienda para organizaciones más pequeñas. Sin embargo este tipo de evaluaciones suelen ofrecer resultados vagos e imprecisos y, por lo tanto, insatisfactorios desde la perspectiva de los niveles directivos.

Desde el punto de vista cuantitativo, como resultado de las investigaciones mencionadas, aparecen varias propuestas de modelos de medición para justificar la inversión en seguridad de la información, entre las que se encuentran: ROSI (Return on Security Investment), ALE (Annual Loss Expectancy), NPV (Net Present Value), IRR (Internal Rate of Return, [27]) o SEAM (Security Atribute Evaluation Model, [5]), e inclusive mediciones más sofisticadas, como la aplicación de la Teoría de los Juegos, [12] y [13]. Algunas de estas técnicas se analizan más adelante.

En la encuesta realizada se buscó determinar si las organizaciones formulaban presupuestos específicos en SI o si al menos, identificaban rubros específicos en los presupuestos de área de TI (ver pregunta 7). Al respecto, pudo determinarse que sobre 167 respuestas obtenidas, un 67,8% indicó que se confeccionaban presupuestos específicos. Este valor si bien

dista de ser el ideal, mostraría una preocupación considerable por establecer asignaciones específicas para este campo. Un 39,6% de quienes respondieron indicó haber participado en la elaboración del presupuesto.

A continuación se invitó a quienes había contestado favorablemente a la pregunta de si participaban en la elaboración del presupuesto, a identificar los ítems que consumían un mayor porcentaje de la asignación presupuestaria. En este sentido, la selección recayó sobre las erogaciones vinculadas a la seguridad de las comunicaciones, la adquisición y el mantenimiento de hardware de seguridad y el control de accesos. A estos elementos, de carácter eminentemente técnico, siguen la adquisición, mantenimiento y desarrollo de software de seguridad y la protección de datos críticos. Finalmente, la generación del marco normativo de la seguridad (políticas, normas y procedimientos) y la capacitación y concientización en SI del personal, ocupan el 6° y 7° lugar, ingresando como primeros temas vinculados a la gestión de la seguridad.

Un análisis más detallado revisando solo las respuestas de los responsables de TI o SI lleva a la siguiente lista de prioridades: seguridad de las comunicaciones, protección de datos críticos, control de acceso, seguridad en las aplicaciones y capacitación y concientización del personal. En esta población, los temas de gestión reciben una categorización inferior a la que se obtiene tomando a todos los encuestados. Se mantiene en consiguiente la tendencia a la selección de aspectos técnicos sobre los de gestión.

MÉTRICAS DE LA SEGURIDAD DE LA INFORMACIÓN

La utilización de métricas económicas tiene como propósito dimensionar la influencia del monto invertido o a invertir en SI en el logro de los objetivos de una organización. En otras palabras buscan determinar los egresos e ingresos, y por lo tanto los beneficios, de diferentes soluciones disponibles a los efectos de la protección de la información y sus recursos asociados. Apuntan a determinar el valor agregado de la SI a la organización para establecer en términos de flujos de fondos, el nivel de eficiencia con que una determinada medida puede influir en la reducción de:

- La probabilidad de ocurrencia de un evento negativo y/o
- La pérdida potencial que traería aparejada.

Las métricas económicas tienen los siguientes objetivos:

- Medir la influencia de la inversión en seguridad en el éxito de la organización.
- Determinar los costos y los ingresos generados por las soluciones implementadas.
- Permitir la comparación y evaluación entre distintas alternativas de inversión.
- Habilitar la comparación con otras organizaciones.

Como cualquier métrica, aquellas de índole económica también pierden valor si se las piensa como valores estáticos. Su importancia se asienta en la posibilidad que da compararlas con otros indicadores similares y en un rango temporal.

En este contexto, Böhme y Nowey [3] señalan que las métricas de la inversión en SI pueden ser empleadas en dos momentos diferentes:

- Ex-ante, buscando determinar los costos y los ingresos producidos por futuras inversiones y facilitando las decisiones en cuanto a la rentabilidad potencial de los proyectos de SI. Esta perspectiva permite decidir si conviene invertir en una determinada medida de seguridad, o bien identificar la mejor frente a varias posibles alternativas.

Responde a la pregunta “¿Cuáles son las medidas que deben implementarse?”.

- Ex-post, con el objetivo de determinar si una inversión realizada ha sido rentable, permitiendo comparar lo planificado vs lo realmente implementado, para evaluar si los recursos de la organización fueron invertidos en forma eficiente. En este caso, el interrogante a responder es “¿Se hicieron bien las cosas?”.

Los autores avanzan al afirmar que la ley de los rendimientos decrecientes puede ser aplicada también a la inversión en SI. El enunciado de esta ley afirma que se obtendrá una producción adicional cada vez menor a medida que se vaya incrementando la cantidad agregada de un factor, manteniendo constantes los restantes. Por lo tanto a partir de determinado punto, ésta puede ser excesiva para los beneficios obtenidos. En otras palabras, debe invertirse en SI solo hasta el punto en el cual los beneficios marginales igualan los costos marginales. A esta realidad se le agregan las exigencias normativas que hoy se manifiestan sobre las organizaciones, cuya satisfacción no necesariamente se ajusta a la ecuación antes señalada.

Si bien las métricas utilizadas son adaptaciones de aquellas que surgen de la teoría clásica de la inversión, deben reconocerse algunas diferencias que caracterizan al campo de la SI. Una de las primeras es que el cálculo de la utilidad económica no resulta trivial en este caso, debido a su naturaleza vinculada a la eventual ocurrencia de fallas. En efecto, invertir en procesos o productos vinculados a la SI pocas veces produce un flujo positivo de fondos directo. Esto complica las posibilidades de determinar la utilidad económica de dichas inversiones ya que ésta radica fundamentalmente en la reducción de riesgos potenciales. Adicionalmente, la determinación de los costos de las medidas de seguridad resulta complicada ya que deben computarse no solo los costos directos (instalación, capacitación o mantenimiento, por ejemplo), sino los indirectos (afectación de la reputación de la organización, ineficiencia operativa, desmotivación del personal, excesiva resistencia al cambio, etc.).

Otros factores que diferencian a la SI son los siguientes:

- No suele ser efectiva en forma absoluta.
- En general, condiciona la agilidad de la operatoria.
- No siempre se está seguro de necesitarla.
- Se conoce el resultado de su implementación con posterioridad.
- Su efectividad se mide en función de la ausencia de fallas.

La aplicación de metodologías de evaluación de riesgo apunta a determinar el grado de exposición, que surge de determinar la probabilidad de ocurrencia de un evento determinado y su impacto en los activos afectados, buscando reducir las pérdidas potenciales. En este sentido, Böhme y Nowey [3] afirman que las métricas de la inversión en seguridad tienen por objetivo determinar cuan eficiente es una medida determinada al momento de ejercer una influencia en dicha probabilidad y dicho impacto.

Desde la perspectiva del profesional especializado en SI y en el marco del proceso decisorio que busca determinar el impacto financiero que la falta de un adecuado marco de protección de la información tendrá en la organización, éste deberá estar en condiciones de determinar:

- El costo de la falta de seguridad para la organización.
- El impacto en la operatoria por una falla en su plataforma tecnológica.
- Las soluciones efectivas en términos de costo-beneficio.
- La estimación de en cuánto se acota la exposición.
- La valorización del riesgo residual que es razonable enfrentar.

Para ello deberá utilizar métricas que le permitan mostrar, en forma clara al nivel directivo, los beneficios en términos financieros, ya sea como ahorros o ingresos potenciales, aunque estos últimos son más difíciles de demostrar.

El siguiente cuadro es una adaptación del presentado en la tesis de Maestría de Cardholm [6]. Muestra distintos tipos de métricas financieras que podrían ser aplicadas al evaluar proyectos o inversiones vinculadas a la SI. Algunas de ellas se desarrollan en mayor profundidad más adelante. Como Anexo II se incluye un ejercicio práctico que muestra cómo se calculan las métricas más importantes presentadas a continuación.

Métrica	Descripción
ROI	El Retorno sobre la Inversión (ROI, por sus siglas en inglés de "*Return of Investment*") se define como la diferencia entre los ingresos esperados y los egresos vinculados a la inversión. Se presenta bajo la forma de múltiples ecuaciones en función de las distintas interpretaciones y aplicaciones de cada sector o el área de la organización. Puede considerarse por lo tanto, un término genérico. Sin embargo, si no se sigue un criterio uniforme, esta falta de consistencia en la forma en que se lo define puede llevar a confusiones cuando se la utiliza para comparar varios proyectos. Más adelante se plantea una derivación de esta métrica para los proyectos de seguridad, denominada ROSI.
NPV	El Valor Presente Neto (NPV, por sus siglas en inglés de "*Net Present Value*") de un proyecto o de una determinada inversión, se define como la suma del valor presente de los flujos anuales de caja, menos la inversión inicial y las periódicas que deban realizarse para su concreción. NPV es considerada una de las herramientas de medición financiera más robustas a la hora de evaluar una determinada inversión.
IRR	La Tasa Interna de Retorno (IRR, por sus siglas en inglés de "*Internal Rate of Return*") se define como la tasa de descuento que hace que el proyecto tenga un NPV igual a cero. Representa un método de evaluación de inversiones alternativo, que no requiere la estimación de la tasa de descuento. Otra forma de definirla es como el promedio de los rendimientos futuros esperados para una determinada inversión.

ALE	La Pérdida Anual Esperada (ALE, por sus siglas en inglés "*Anual Loss Expectancy*") es una forma de expresar el grado de exposición al riesgo, que se obtiene multiplicando el costo proyectado de un incidente de seguridad por la cantidad estimada de ocurrencias, durante un lapso determinado, que suele ser de un año. Esta métrica se encuentra fuertemente asociada a la definición de riesgo y se expresa en moneda corriente.
DCF	El Flujo de Caja Descontado (DCF, por sus siglas en inglés de "*Discounted Cash Flow*") es un método utilizado para valorar un proyecto o una determinada inversión, sobre la base del valor actual de los flujos de fondos futuros, descontados a una tasa que refleja el costo del capital aportado. Permite evaluar el potencial de una inversión.
Payback Period	El Período de Desembolso (del inglés "*Payback Period*") es una técnica utilizada por las organizaciones para determinar el tiempo que tardarán en recuperar el desembolso inicial realizado para una determina inversión. El proyecto con el menor tiempo de recuperación es el que debería resultar seleccionado, siempre que se mantengan estables el resto de las variables. Presenta como desventaja que no tiene en cuenta cualquier ingreso posterior al desembolso inicial ni considera el valor actual de los egresos futuros.
TCO	El Costo Total de Propiedad (TCO, por sus siglas en inglés de "*Total Cost of Ownership*") tiene por objetivo determinar el valor que refleja el costo total de la inversión, incluyendo los costos iniciales y los recurrentes. No considera los ingresos o beneficios esperados.
TBO	El Beneficio Total de Propiedad (TBO, por sus siglas in

	inglés de "*Total Benefits Ownership*") es utilizado para dar énfasis en que los beneficios de una determinada implementación serán mayores si se incluyen aquellos de carácter indirecto, tales como la satisfacción de los clientes o el incremento de las ventas. Esta métrica se obtiene al sumar los efectos positivos de una inversión, sin considerar los costos.
EVA	El Valor Económico Agregado (EVA, por sus siglas en inglés de "*Economic Value Added*") es una manera de determinar el valor de las ganancias de un determinado proyecto para la organización. Se lo define como el valor residual luego de deducidos de los ingresos la totalidad de los gastos, incluidos el costo de oportunidad del capital y otros gastos. Se obtiene luego de haber cubierto todos los gastos y de haber satisfecho una rentabilidad mínima esperada por los accionistas.
ROSI	El Retorno sobre la Inversión en SI (ROSI, por sus siglas en inglés de "*Return of Security Investment*") es una adaptación del ROI, que muestra los ingresos de una inversión realizada con el objetivo de fortalecer la SI. Representa los ahorros netos obtenidos a partir de la mitigación de uno o más riesgos, al evitar o minimizar una eventual pérdida financiera.

Estas y otras herramientas de medición financiera de la SI han sido cubiertas ampliamente en la bibliografía, destacando su importancia a la hora de estimar la inversión necesaria. En efecto, existe unidad de criterio en la bibliografía respecto a que las mediciones que permiten cuantificar los costos e ingresos directos o mayores ahorros asociados a la SI, aplicadas adecuadamente, fortalecen los procesos decisorios al permitir la anticipación de los ingresos y egresos, la formulación presupuestaria y el control de los costos directos e indirectos asociados a una efectiva protección de la información.

En este sentido, existe coincidencia entre los especialistas en que sólo a través de herramientas objetivas de medición, se podrán ponderar las ramificaciones financieras de los problemas de seguridad, de manera de poder dirigir adecuadamente los recursos para la provisión de un marco adecuado de protección de la información. Concretamente, para justificar la implementación de un control determinado, se debería estar en condiciones de asegurar que la inversión que dicho control requiere no es superior a las pérdidas provocadas por el impacto probable del riesgo que se busca mitigar.

Por otra parte, en un contexto organizacional, fuera del ambiente específico de las áreas de TI, será necesario interactuar con otros decisores, tales como los gerentes financieros, quienes más allá de la efectividad técnica de las medidas a implementar, requerirán justificaciones sólidas en cuando al valor económico que un determinado proyecto le aporta a la organización. En otras palabras, deberá vincularse las ganancias de la organización con la inversión que se promueve realizar.

En este sentido, dado que los presupuestos son limitados en su alcance, será necesario competir con otras áreas funcionales de la organización, más acostumbradas o más cercanas por su propia actividad, a expresar en valores monetarios los objetivos a los que se quiere llegar con un proyecto en particular. Por lo tanto, se hace imprescindible que se tomen en cuenta una o varias de las métricas antes citadas, con el fin de lograr una adecuada protección de la información de la organización. En la sección siguiente se describen en mayor detalle las métricas más utilizadas.

Sin embargo, no escasean las reservas en cuanto a su efectividad, reflejadas en publicaciones de distintos autores, como por ejemplo Wood y Parker [18] y Xiaomeng [29]. Las dificultades para estimar los ingresos o eventuales ahorros asociados a la implementación de medidas de SI resultan uno de los obstáculos más importantes. A esto se agrega que los procesos de evaluación de riesgos sobre los que se basan estas métricas, son complejos por la falta de datos respecto a fallas o incidentes ocurridos. Por otra parte, los profesionales responsables de las áreas de TI o de SI no

cuentan muchas veces con la preparación para realizar este tipo de estimaciones y tienden a subestimar su importancia.

Por todo ello, el uso de estas herramientas no se encuentra completamente instalado aún en las áreas de TI y de SI. En este sentido, en la encuesta referida anteriormente, se preguntó a los especialistas consultados cuál era la percepción respecto a la utilidad de estas herramientas (ver pregunta 11). Solo un 17,5% respondió que las consideraba muy útiles, mientras que un 14,3% las consideró parcialmente útiles y un 15,6%, como difíciles de aplicar. Por otro lado, el 26% de los encuestados indicó que le interesaría utilizarlas pero que consideraban que no las conocían lo suficientemente bien y el 23,4% restante manifestó no tener opinión al respecto. Tomando estos dos últimos grupos de respuestas, puede concluirse que aproximadamente un 50% desconoce estas herramientas.

Para determinar si efectivamente se estaban utilizando, la encuesta preguntó si habían utilizado alguna de las siguientes métricas: ROSI, ALE, NPV o IRR (ver pregunta 12). Del total de respuestas, ROSI resultó la más utilizada (18,1%), seguida por IRR (15,5%), ALE (14,2%) y NPV (11,6%). Un 63% indicó no haber utilizado nunca este tipo de herramientas.

A continuación y sobre la base de las 57 respuestas afirmativas en cuanto a la efectiva utilización de al menos una de las métricas citadas, se buscó determinar cuál había sido el resultado de esta experiencia (ver pregunta 13). Se encontró que una amplia mayoría (61,4%) las encontraba parcialmente útiles, un 7% las empleó solo por exigencias legales, casi un 9% las juzgó útiles solo para grandes organizaciones y 15,8% las encontró realmente útiles. Solo un 3,5% manifestó que no servían y otro tanto indicó no tener opinión al respecto.

Por otro lado, se analizó cuáles eran los ítems de mayor peso en el presupuesto destinado a SI, indicados por quienes usaban métricas y seguidamente, por quienes no las empleaban. Esto se plasmó cruzando las preguntas 8 y 12. Al respecto se encontró lo siguiente:

Ítems más seleccionados por quienes usaban cualquiera de las métricas	Ítems más seleccionados por quienes no usaban métricas
• Seguridad en las comunicaciones (26,8%). • Control de accesos (26,8%). • Seguridad en las aplicaciones (19,5%). • Capacitación y concientización en Seguridad Informática del personal de TI y de los usuarios (17,1%). • Monitoreo de la seguridad (14,6%). • Protección de datos críticos (14,6%).	• Adquisición y mantenimiento de hardware de seguridad (31,1%). • Seguridad en las comunicaciones (24,4%). • Atención y respuesta a incidentes de seguridad (24,4%). • Protección de datos críticos (24,4%). • Generación del marco normativo de seguridad (22,2%). • Control de accesos (22,2%).

Del cuadro anterior se desprende que ambos grupos analizados no seleccionan mayormente los mismos ítems y cuando lo hacen (seguridad de las comunicaciones y control de acceso), no le asignan la misma prioridad. Podría concluirse que la utilización de métricas influye en los procesos de decisión en cuanto a la formulación presupuestaria de la SI, sin desconocer por ello que otros factores, tales como la real necesidad de realizar algunas acciones concretas, también pueden condicionar tal selección.

Finalmente, se buscó identificar cuáles eran las métricas más utilizadas por quienes participaban en la elaboración del presupuesto, ya sea porque se encontraba bajo su responsabilidad o porque colaboraba en esta tarea (cruce de preguntas 7 y 12 y resultados, en pregunta 12). Se observó que la más utilizada es ROSI (42,3%), seguida de ALE (26,9%), IRR (21,2%) y NPV (9,6%). El orden en que se presentan las métricas de acuerdo a su uso es similar al registrado para la totalidad de los encuestados.

MÉTRICAS FINANCIERAS

Pérdida Anual Esperada

El cálculo de la pérdida anual esperada o ALE es una forma de expresar el grado de exposición al riesgo. Se obtiene multiplicando el costo proyectado de un incidente de seguridad por la cantidad estimada de ocurrencias durante el lapso de un año y se expresa en moneda corriente.

Esta métrica es una de las bases del cálculo de otros esquemas cuantitativos de medición de la SI. Se la ha utilizado desde la década de los 70 y fue adoptada por el NIST a través de la publicación FIPS # 65 [19]. Si bien fue considerada por algún tiempo como demasiado complicada, en su artículo Böhme y Norwey [3] indican que en la última década ha ganado popularidad, habiendo sido incorporada a otros estimadores, como por ejemplo, ROSI.

Para un evento determinado, ALE resulta del producto de dos factores:

- Pérdida unitaria esperada (Single Loss Expectancy – SLE): consecuencias financieras indeseadas de un evento.
- Tasa anual de ocurrencia (Annual Rate of Occurence – ARO): cantidad de ocurrencias de dicho evento en un año.

$$ALE = SLE \times ARO$$

Este valor también puede ser expresado como la sumatoria de todas las ALE de varios eventos no deseados:

$$\mathrm{ALE} = \sum_{i=1}^{n} S(O_i)\ F_n$$

Donde:

- O_i= evento indeseado i
- S (O_i) = severidad del evento i
- F_n = frecuencia de ocurrencia del evento i

Kitteringham y McQuate, citados por Lucas [17] expresaban en el año 2003 que el factor más significativo para obtener fondos es el retorno sobre la inversión. Agregaban que "… los lazos del monedero no se soltarán hasta que la empresa no sepa cuánto está obteniendo por cada peso invertido".[1]

El retorno sobre la inversión, como su nombre lo indica, representa cuánto se recibirá por lo invertido o gastado.

En este escenario, el cálculo de ROSI es un indicador clave para medir la eficiencia de la inversión en SI. Esta métrica permite comparar estrategias o proyectos alternativos. Para su obtención, el monto de la inversión se compara con las ganancias esperadas, las que reflejan el ahorro en las pérdidas que se evitaron durante la vida útil de los bienes o servicios objeto del cálculo, de acuerdo a lo indicado por Sonnenreich [25].

Su cálculo reconoce tres fases que incluyen la identificación de los activos de información, la determinación de las amenazas y vulnerabilidades a las que se encuentran expuestos y el cálculo de su valor y el de las salvaguardas que deben adoptarse para su protección. Estos dos últimos valores son luego comparados para determinar el retorno sobre la inversión que debe realizarse.

Básicamente, el objetivo principal del cálculo de ROSI es la comparación de los costos asociados a la implementación de controles, con los ahorros que significa la adopción de medidas preventivas o correctivas que buscan minimizar la probabilidad de ocurrencia o el impacto de una determinada amenaza, evitando así posibles pérdidas.

Una primera aproximación al cálculo de ROSI puede resumirse en la siguiente fórmula:

ROSI = (Ingresos esperados - Costos de la inversión)/costos de la inversión

[1] Traducción de la autora de: "The purse strings will not be loosened until the company knows what is getting in return of its cash". Extraída de "Economic Evaluation of a Company´s Information Security Expenditures", de Kelly Lucas, Network Administrator, Morgan Stanley, citando a Kitteringham y McQuate.

Téngase en cuenta que, como se dijo anteriormente, los ingresos esperados representan en realidad el ahorro que surge de las pérdidas que se evitaron por la inversión realizada para mitigar la exposición.

Si bien se trata de una fórmula relativamente sencilla, se presentan algunas dificultades a la hora de realizar el cálculo. Tomando los costos de la inversión, su cálculo no parece complejo ya que se obtendría sumando los fondos invertidos, como por ejemplo, el costo del equipamiento o el software, el valor horario o mensual de los recursos humanos afectados y otros costos indirectos, como la luz. Pueden ser bienes tangibles (equipamiento) o intangibles (software).

Las dificultades se plantean a la hora de calcular los ingresos o ahorros esperados a partir de la inversión en SI, ya que en general surgen de estimaciones subjetivas, especialmente cuando se trata de estimar los ingresos devenidos de acciones preventivas.

Una forma más precisa de cálculo es la siguiente:

$$ROSI = R – ALE/R$$

Donde:

R: Costo de la recuperación ante una intrusión o falla

ALE: Pérdida Anual esperada

Cabe acotar en este punto que la inversión en controles busca la mitigación del riesgo, su transferencia (por ejemplo, a través de una póliza de seguros), su aceptación o una combinación de las tres.

Finalmente, se aclara que todos los montos que se utilizan para el cálculo de ROSI son valores corrientes.

Valor Presente Neto

Ya en 1994 Somerson [24], citado por Morgan Stanley [23], afirmaba que “un modelo de valor agregado que compute el valor presente neto puede dar a los especialistas en seguridad lo que necesitan para competir en forma efectiva”.

En efecto, esta herramienta aplicada al área de la SI en particular, representa el valor presente neto en moneda corriente de los flujos de caja vinculados a la inversión en bienes o servicios asociados a la seguridad de la información. Se trata de la estimación y comparación de valor presente de la inversión en SI, descontado y ajustado en función del riesgo, con los costos esperados.

Se aplica a proyectos que se prolongan por varios períodos y se obtiene descontando los ingresos o ahorros y costos anticipados a su valor actual. Se expresa en valores monetarios.

Es calculado como la diferencia entre el valor presente de ingresos futuros y el valor presente de los egresos de un proyecto de inversión en SI. Si el NPV es mayor que cero, el proyecto es rentable.

Para calcularlo, se utiliza la siguiente ecuación:

$$\mathrm{NPV} = \sum_{i=0}^{n} \frac{B_i - C_i}{(1+t)^i}$$

Donde:

- B_i es el valor presente de los ingresos netos del período i
- C_i son todos los costos
- t es la tasa de descuento

Si:

- NPV ≥ 0 → el proyecto es rentable
- NPV < 0 → el proyecto genera pérdidas

Gordon y Loeb [12] indican que el uso del NPV se ve dificultado por la necesidad de estimar los eventuales ahorros que surgen a partir de una determinada inversión, a realizarse o realizada con el fin de fortalecer la SI, siendo éste un factor clave para el uso de esta métrica en las organizaciones.

INDICADORES BASADOS EN MECANISMOS DEL MERCADO

Existe unanimidad en la bibliografía en considerar a Anderson [1] como el iniciador de las investigaciones en este campo. En efecto, Anderson fue el primero en aplicar en forma exhaustiva el análisis económico en el campo de la SI. En sus estudios, se animó a desafiar la idea de que los problemas de seguridad de Internet y de las redes en general debían atribuirse únicamente a la falta de dispositivos o implementaciones técnicas como la criptografía, los firewall o los mecanismos de control de acceso, entre otros. Anderson [1] demostró que los sistemas eran a menudo inseguros porque quienes eran responsables de su implementación, custodia o utilización, carecían de los incentivos necesarios para protegerlos. De esta manera se puso en evidencia que la seguridad de la información no era una cuestión meramente técnica.

Entre otros beneficios, este enfoque facilitó la comprensión de estos temas en los planos directivos y gerenciales y mejoró la interacción de las áreas del TI y SI con el resto de la organización, ya que las fallas de seguridad empezaron a ser expresadas en términos de limitación de eventuales pérdidas económicas y no únicamente a través de sus características técnicas.

A partir de los estudios de Anderson [1], la seguridad o más precisamente, la inseguridad de la información empezó a ser percibida como una externalidad negativa, es decir como un efecto secundario y adverso de las implementaciones de las TI, similar a la contaminación ambiental respecto del avance industrial. El especialista también demostró que la imposibilidad que tienen la mayoría de los compradores para percibir y determinar las características de seguridad de los productos o servicios de TI que adquieren, era un factor condicionante para la incorporación de medidas de seguridad. En otras palabras, frente a dos productos informáticos de similar propósito (por ejemplo, dos antivirus), resulta sumamente complejo para un usuario no especializado determinar cuál de ellos presenta una mejor relación “precio/beneficio”. Como inevitable

consecuencia, disminuyen los incentivos para agregar componentes de seguridad en los productos y servicios que se ofrecen.

Tomando como ejemplo el mercado de productos de software, puede observarse que esta asimetría en la información disponible para los usuarios o compradores potenciales, tiene un fuerte impacto sobre el nivel de seguridad de los productos. En efecto, garantizar la seguridad de un software determinado es un proceso muy complejo y difícil de apreciar por un usuario común cuando trata de comparar distintos productos. Por otro lado, para un desarrollador, agregar seguridad presenta siempre un costo adicional generalmente alto, mientras que las consecuencias de ignorar la seguridad suelen ser menores, eventuales y no apreciadas por los potenciales compradores, al menos al momento de la adquisición. Por lo tanto, en este escenario quienes comercializan software no tienen incentivos para aumentar los valores de venta de sus productos por la incorporación de mayor seguridad, ya que esto significaría un incremento en los precios que a priori, los usuarios no querrían pagar. En otras palabras, los incentivos para agregar seguridad a sus productos son bajos o inclusive, inexistentes.

A partir de los estudios de Anderson [1], Gordon y Loeb [11] de la Universidad de Maryland (EEUU), analizaron este escenario desde el punto de vista de una organización y crearon uno de los primeros modelos para determinar el nivel óptimo de inversión para alcanzar una adecuada protección de un conjunto determinado de datos. Desde esta perspectiva, reconocieron y fundamentaron el hecho de que si bien es necesario invertir en SI, una mayor protección no siempre se encuentra justificada desde el punto de vista económico. En sus trabajos, establecieron la diferencia entre una seguridad perfecta y una seguridad eficaz, en términos de costos y beneficios. Para ello tomaron en cuenta el nivel de vulnerabilidad de la información frente a una falla eventual y las pérdidas potenciales en caso que tal evento ocurra. Los autores demostraron que una organización no necesariamente debe concentrar su inversión en aquellos recursos de información más vulnerables, ya que estos pueden ser demasiado costosos para proteger. En su lugar, sugieren que la organización debe concentrarse en aquellos activos con vulnerabilidades de nivel medio, como una forma de

"*triage*" que descarta los extremos: aquellas medidas o mecanismos excesivamente costosos en su implementación y aquellos riesgos sin consecuencias significativas. Cabe aclarar que la palabra "*triage*" proviene del término en francés "*trier*", que significa clasificar o escoger. Su uso se origina en los campos de batalla y describe el proceso mediante el cual los soldados con heridas mortales eran dejados a un lado para morir mientras eran atendidos aquellos con lesiones menores y mejores posibilidades de recuperación para regresar al campo de batalla. Del análisis realizado, los autores infieren que para maximizar el beneficio esperado de la inversión en seguridad, debe gastarse solo una fracción del monto de la pérdida esperada ante la materialización de una amenaza. Efectivamente, en su modelo los autores especifican en base a los estudios realizados que en ciertos casos, el nivel óptimo de inversión en SI no debe exceder el 37% de las pérdidas esperadas como resultado de una falla de seguridad.

Rosenfeld, Rus y Cucker [21] por su parte, presentaron un modelo basado en la "Tragedia de los comunes" como arquetipo en el cual, los esfuerzos realizados para mejorar la SI en una organización son limitados si se ignora el hecho de que se está utilizando o consumiendo un recurso compartido con otros usuarios. Este trabajo presenta varios escenarios que sugieren cómo se pueden resolver los problemas, atendiendo a la maximización de las ganancias a partir de los esfuerzos realizados.

En línea con los trabajos de Anderson [1], más recientemente Grossklags, Johnson y Christin [14] plantearon que la cantidad de información disponible para que los usuarios puedan tomar una decisión racional a la hora de invertir en un mecanismo de seguridad, es insuficiente. En otras palabras, se ven superados por el nivel de complejidad de los sistemas que utilizan y no pueden obtener la información necesaria para formular un análisis de costo-beneficio que les permita adoptar o bien rechazar, una medida de seguridad determinada.

Esta suerte de asimetría de información entre consumidores y productores de bienes y servicios de TI, se ve reforzada por los trabajos de Rosenberg, Rus y Cucker, quienes señalan que el nivel de interdependencias que hoy se registran entre las acciones de distintos

usuarios provoca que ciertas iniciativas individuales causen efectos no deseados en otros usuarios o en el resto de la red. Pueden citarse como ejemplo, las infecciones causadas por la transmisión o copia de archivos infectados, el SPAM o la elección de contraseñas débiles para una red corporativa. En la mayoría de los casos, estas interdependencias son ignoradas por los usuarios comunes, quienes no perciben ni entienden que el resultado de sus acciones inseguras puede afectar a otros en la red, sea esta corporativa o pública.

Por otro lado, los autores antes citados reconocen que si bien este tipo de comportamiento no se manifiesta en usuarios expertos, éstos no suelen tener en cuenta en sus decisiones la situación de la mayoría de los que utilizan las redes, quienes como ya fue expresado, carecen de los conocimientos necesarios para adoptar decisiones críticas en materia de SI.

A estos especialistas les siguieron otros que buscaron tipificar costos, plantear nuevos modelos para justificar la inversión y relevar casos de éxito o fracaso en la medición de la SI desde la perspectiva económica, tomando como base distintos mercados.

Todos estos estudios permiten concluir que las organizaciones que priorizan la protección de su información y de los elementos que las soportan y adoptan una política seria de prevención de fallas o incidentes, deben invertir en SI en función de la optimización de los recursos, en lugar de focalizarse exclusivamente en las soluciones técnicas posibles. Deben considerar en sus marcos estratégicos de SI el nivel de comprensión de los usuarios involucrados y estimar las medidas que acoten la cantidad y complejidad de las decisiones que éstos deben tomar, proveyendo herramientas y capacitación para que puedan adoptar decisiones fundadas en los casos que correspondan.

Entre los indicadores económicos de la SI, se distinguen aquellos basadas en mercados genéricos y los que toman sus valores a partir de mercados que en los que se realizan transacciones productos específicos vinculados al aseguramiento de la información. Este tipo de indicadores no se utilizan en el contexto de una organización en particular y su cálculo se realiza a partir de una serie de observaciones económicas formuladas a

partir del comportamiento de determinados actores racionales en el mercado. Entre estos actores se encuentran las empresas, las personas y los gobiernos. Sus decisiones proveen una valiosa información que puede ser empleada para construir indicadores respecto de la SI.

El concepto de mercado consiste en una plataforma de negociación para el intercambio de bienes físicos o intangibles, como por ejemplo la información, o servicios. En su ámbito interactúan los distintos agentes económicos, bajo un denominador común que constituye un precio expresado en términos de moneda corriente.

Tal como lo indican Böhme y Norwey [3], si bien los precios que se fijan en el mercado no siempre son precisos, proveen herramientas valiosas para medir la SI.

Indicadores basados en mercados genéricos

Los indicadores basados en mercados genéricos buscan evaluar el impacto que tiene sobre la cotización de las acciones, la difusión de noticias vinculadas a compromisos de la seguridad de la información de las organizaciones. Típicamente se analiza el comportamiento del valor de las acciones con el fin de identificar los efectos anormales producidos por el público conocimiento de un hecho que impacta sobre la seguridad de su información. En otras palabras, mide el impacto del evento negativo sobre la valoración que los inversionistas hacen de la empresa.

Numerosas publicaciones han analizado el efecto de la difusión al público de ataques informáticos sobre el valor de las acciones de una entidad.

Böhme y Nowey [3] explican que estos efectos no esperados surgen de la comparación del escenario que se presenta una vez conocido el evento, con estimaciones respecto al que debería haberse presentado de no haberse producido el hecho. Para analizar estas situaciones, analistas e investigadores utilizan diferentes métodos estadísticos, buscando determinar la real magnitud del impacto. En consiguiente, a la hora de compararlos, importa más el signo y la profundidad del efecto, que su valor específico.

En su trabajo, los autores antes citados referencian a Ettredge y Richardson [9], quienes en el año 2003, realizaron uno de los primeros estudios del efecto que causa la publicación de un incidente de seguridad en los medios de difusión masiva, sobre la cotización de las acciones de varias empresas. Las circunstancias fueron consideradas ideales ya que el ataque fue inesperado y repentino y afectó a organizaciones conocidas por el público por su trayectoria. Los autores analizaron el contexto en el que se produjo el ataque de denegación de servicios (en adelante, DoS) que sufrieron en febrero del 2001 las firmas Yahoo, eBay y Amazon y la manera en que esto afectó a otras empresas. Lo interesante del trabajo es que estos autores encontraron que un importante número de organizaciones sufrieron un impacto negativo en la cotización de sus acciones, aún cuando no había sido blanco del ataque. El estudio abarcó a 287 empresas dedicadas al comercio electrónico, sin incluir a las tres que fueron afectadas en forma directa. Como resultado del ataque se produjo un efecto contagio en los inversores, que entendieron que estas entidades podían verse expuestas a un ataque similar.

En sus conclusiones, los autores estimaron que los efectos negativos sobre estas empresas afectadas indirectamente, fueron significativos en magnitud y no se revirtieron en el corto plazo.

Según citan Böhme y Nowey [3], dos estudios posteriores, realizados por Campbell et al (2003) y Cavusoglu et al [7], presentaron las siguientes conclusiones:

- Cuando se difundían en los medios masivos de comunicación noticias respecto a incidentes de seguridad que afectaban a determinadas empresas, éstas veían afectados negativamente el valor de sus acciones.
- Estos efectos eran mayores cuando el incidente afectaba la confidencialidad de la información, con lo cual los inversionistas demuestran tener la capacidad para distinguir distintos tipos de impacto.

- Las empresas más pequeñas sufren un impacto mayor, justificado en el hecho de que disponen de menores recursos para realizar una adecuada evaluación y gestión de riesgos.
- Los precios de las acciones de empresas dedicadas a la SI en cambio, mostraban un efecto positivo en su cotización.

Telang y Wattal (2005), según Böhme y Nowey [3], también analizaron el efecto del reporte público de incidentes sobre el valor de cotización de las acciones, y encontraron que la empresa Microsoft se veía más afectada que el promedio. Esto puede explicarse por la mayor exposición producto de su posición dominante en el mercado.

El trabajo de Anthony et al [2] también concluyó que los anuncios públicos de ataques a sitios web mostraban un efecto negativo sobre el valor de las acciones de la compañía.

Sin embargo, Hovav y D'Arcy's [15] en un estudio realizado en el año 2003 en el que analizaron ataques de DoS en un período de cuatro años y medio, concluyeron que en general, el mercado no penalizaba a las empresas que sufrían un ataque. En efecto, los autores afirman que si bien existe un efecto negativo sobre el valor de las acciones en los primeros cinco días, éste no es significativo ni se extiende considerablemente en el tiempo. Los resultados obtenidos sugieren que los inversionistas interpretan que las empresas con mayor utilización de Internet, se encuentran expuestas a mayores riesgos y que aquellas que simplemente la utilizan sin ser parte de su objeto de negocio, no se ven afectadas significativamente. Consecuentemente estas últimas podrían estar sobrevaluando las consecuencias de la difusión pública de los incidentes, al invertir recursos para prevenir problemas que tienen en realidad, un efecto marginal sobre el valor de sus acciones.

Más recientemente en el año 2011, la empresa Sony sufrió un ataque simultáneo de DoS y sobre su red de "*Play Station*" que provocó la salida de servicio de su plataforma por veintitrés días y el robo de datos de millones de usuarios. Según la publicación "The Register" [26], el valor de las acciones de Sony cayó más del 50% a raíz del ataque, que le habría costado

a la empresa casi 200 millones de dólares, sin contar los gastos judiciales. Sin embargo, ese efecto no se mantuvo en el tiempo y no existen estudios conclusivos que permitan determinar si las mermas en la cotización pueden ser atribuidas exclusivamente al ataque informático sufrido por la empresa.

Como conclusión, puede afirmarse que cuando una falla de seguridad o un ataque informático que compromete la seguridad de la información de una empresa llega al conocimiento público, el valor de sus acciones se ve afectado. Sin embargo, este valor no puede ser considerado realmente una métrica directa debido a varios motivos:

- La dificultosa estimación del impacto en la cotización de las acciones en el mediano y largo plazo.
- La escasez de casos que pueden ser analizados.
- La circunstancia de que el valor de cotización de una acción representa el valor agregado de mucha información, por lo que es imposible desagregar el impacto atribuido exclusivamente a un compromiso de la seguridad de la información.

Finalmente, debido a que este tipo de indicadores muestran los efectos posteriores, no pueden ser considerados como métrica, sin por esto dejar de reconocer su valor como medida del valor que la seguridad le aporta a la organización.

Indicadores basados en mercados específicos

Como fuera expresado con anterioridad, diversos autores demostraron que en el escenario actual de compra-venta de bienes y servicios informáticos, los vendedores no tienen incentivos para agregar seguridad a los productos que comercializan, ni los compradores quieren pagar un costo adicional por estas mejoras. Esta situación que no puede explicarse desde la perspectiva técnica sino económica, ha generado distintas respuestas que buscan contrarrestar esta falla del mercado y que adicionalmente producen indicadores sobre el nivel de la seguridad en las organizaciones. A continuación se analizan cuatro de estas soluciones:

- Las recompensas.
- La compra-venta de vulnerabilidades.
- Los ciberseguros.
- El mercado de los “exploits”.

Recompensas

Una efectiva inversión en seguridad de la información requiere disponer de información precisa sobre las vulnerabilidades de los productos o servicios a incorporar. En este sentido, se han desarrollado una serie de mecanismos para aumentar la disponibilidad de esta información. La identificación de las vulnerabilidades y el proceso de difusión que sigue a su descubrimiento, constituyen dos factores claves a la hora de garantizar dicha disponibilidad. Uno de estos mecanismos o soluciones que se han desarrollado para generar el reporte y la difusión, es el de las recompensas bajo la forma de desafíos para encontrar y reportar fallas.

En esta solución el vendedor o desarrollador de un producto o servicio ofrece una cantidad de dinero, como premio o recompensa, para quien reporte una vulnerabilidad en su producto o servicio. Este concepto, que también es utilizado en otras áreas, viene siendo empleado desde hace varios años. Una de las primeras recompensas fue ofrecida en 1995 por la empresa Netscape. Posteriormente, RSA a través de concursos de factoreo y de obtención de claves privadas; Mozilla, mediante un programa de Bugs de Seguridad y Argus, con desafíos a la seguridad, también incorporaron esta modalidad.

En el caso de Mozilla el desafío premiaba a quienes reportaran vulnerabilidades de productos de la empresa que reunieran las condiciones de ser originales, no reportadas previamente y remotas. Quienes realizaran el reporte no debían ser los autores o tener vinculación laboral o de cualquier otro tipo con la firma. La recompensa ofrecida estaba entre los 500 y 3.000 dólares estadounidenses.

Más recientemente, Facebook y Google ofrecieron una serie de recompensas a quienes reportaran vulnerabilidades en sus sitios web. En el primer caso, en el año 2011 la empresa reveló que su iniciativa de recompensa por el reporte de vulnerabilidades pagó más de 40.000 dólares estadounidenses en tres semanas. El pago mínimo era de 500 dólares si bien en algunos casos se llegó a pagar 5.000. La firma no reveló la cantidad de vulnerabilidades reportadas. En el caso de Google, la entidad ofreció en

el año 2010 entre 500 y 3.137 dólares estadounidenses a quienes reportaran vulnerabilidades en sus sitios web.

En términos teóricos, para garantizar el éxito de estos programas, el valor de la recompensa debe ser superior al que obtendría quien identificó la vulnerabilidad, si decidiera explotarla directamente o bien venderla a otra entidad. En consiguiente su monto, conocido también como el valor de mercado de la vulnerabilidad (del inglés “Market price of a Vulnerability – MPV”) es el límite inferior del costo de vulnerar un sistema y podría considerarse como el valor mínimo de la fortaleza de un producto o servicio. Desde otra perspectiva, el bien o servicio, por cuya vulnerabilidad se ofrece un premio, debería ser usado para gestionar o proteger uno o varios activos, cuyo valor total no supere el monto de esa recompensa. De lo contrario, quien detecta la vulnerabilidad podría verse tentado a aprovecharla para apoderarse del o los activos, en lugar de reportarla y cobrar la recompensa.

Un problema que se manifiesta entonces es la dificultad para determinar el valor de la recompensa. Las experiencias antes citadas demostraron que el valor ofrecido no siempre compensaba otras alternativas de obtención de beneficios a partir de las vulnerabilidades encontradas. Ocurre también que muchas veces los vendedores que ofrecen este tipo de recompensas mantienen acuerdos de confidencialidad para evitar efectos adversos en los medios de prensa y por lo tanto, no difunden el monto real de las recompensas. Por otra parte cuando se analiza este tipo de mecanismos, deben considerarse los costos y los riesgos que asume quien detecta la vulnerabilidad si decide reportarla a una entidad distinta del proveedor o desarrollador (por ejemplo, una organización criminal). A manera de ejemplo de las dificultades para fijar los montos de las retribuciones, la propia RSA indicaba en su sitio web que dado el volumen de capacidad computacional requerida para realizar la factorización que motivaba la recompensa, éstas eran meramente simbólicas.

Cabe destacar asimismo, que para funcionar adecuadamente, se necesitan muchos participantes de los desafíos y una actualización permanente de los valores ofrecidos a manera de recompensa.

No obstante las dificultades antes citadas, el desarrollo de programas de recompensas para impulsar el hallazgo y reporte de vulnerabilidades ha demostrado tener algunas consecuencias positivas. Entre ellas se encuentran la posibilidad de ofrecer una alternativa legal a la opción de venta en el mercado negro y un alto grado de economía para las empresas, en comparación con el costo de programas de seguridad internos o la contratación de servicios de terceros para hallar dichas fallas.

Sin embargo, las recompensas no constituyen métricas confiables de la seguridad de un producto o servicio ya que han demostrado contener una serie de imperfecciones, que les restan valor como indicadores económicos del nivel de seguridad de la información de bienes o servicios.

Compra-venta de vulnerabilidades

En este caso, el mercado específico se conforma por empresas privadas generalmente dedicadas a la Seguridad, como Verisign® iDefense® Security Intelligence Services o TippingPoint DVLabs, que pagan por información relativa a vulnerabilidades de productos y servicios y luego las venden a sus clientes a través de servicios, generalmente suscripciones. Entre estos clientes se encuentran los propietarios de grandes redes, el público en general o inclusive, hackers. Un efecto adverso de esta actividad es que en el último caso, la difusión temprana de una vulnerabilidad puede provocar que ésta sea explotada más rápidamente. Algunos inclusive entienden que este tipo de servicio podría ser considerado extorsivo ya que quien no se suscribe estaría perdiendo información importante.

Desde el punto de vista de las métricas, el valor que se pagan por las vulnerabilidades podría ser considerado un indicador de la seguridad de un determinado producto o servicio. A mayor valor pagado, mayor es el grado de exposición al que se verían sometidos los activos protegidos. Sin embargo, los precios que se pagan son confidenciales con lo cual este indicador pierde accesibilidad. Adicionalmente, con el surgimiento de los Equipos de Respuesta a Incidentes (CSIRTs o CERTs por sus siglas en inglés), este tipo de mercados va perdiendo vigencia.

Ciberseguros

Otra solución desarrollada por el mercado para compensar las fallas de seguridad de los activos informáticos son los seguros cibernéticos o “ciberseguros”. Se trata de una forma de proteger a la organización de aquellos riesgos vinculados a la infraestructura tecnológica y a las actividades relacionadas con las TI. La cobertura de estos seguros alcanza, entre otras, a las pérdidas relacionadas con la destrucción de datos, la extorción por medios electrónicos, el robo de información o de propiedad intelectual, el hackeo o los ataques de denegación de servicio. Pueden también comprender la protección contra terceros originada en las indemnizaciones que pudieran ser reclamadas por eventuales errores u omisiones, fallas en el resguardo de información, indisponibilidad de un servicio informático, etc.

La contratación de seguros representa una instancia de transferencia del riesgo, frente a las distintas posturas que pueden adoptarse. Los seguros son contratados para cubrirse de eventualidades cuyo impacto financiero podría dejar a la organización fuera del negocio. A cambio de ello, las empresas de seguro cobran un valor fijo, denominado prima. A su vez, el conjunto de primas vendidas por una aseguradora le permiten hacer frente a las pérdidas que deben cubrir ante un siniestro y a los costos administrativos de su gestión y además, generar ganancias. Quienes contratan seguros, obtienen a cambio un mecanismo de flujo de fondos más estable y repartido en el tiempo.

Cuando una organización adquiere un ciberseguro, el costo de la prima es ajustado según el entorno de seguridad, teniendo en cuenta la tecnología y las prácticas que se encuentran implementadas. Cada póliza es diseñada según la situación y las necesidades de la entidad asegurada, incluyendo la tecnología implementada y el nivel de riesgo al que está expuesta. Influyen entre otros factores, el tamaño de la organización (a mayor tamaño, mayores pérdidas y por lo tanto, mayor prima), el tipo de datos que maneja (a mayor criticidad, mayor prima), el nivel de regulación (a mayor regulación, mayor exposición a sanciones, y por lo tanto mayor prima)

y el nivel de dependencia de las actividades centrales del negocio respecto de la tecnología (a mayor dependencia, mayor riesgo y por ende, mayor prima).

De esta forma, los ciberseguros permiten mitigar riesgos pero también pueden transformarse en métricas ya que al ajustarse el monto de las primas a la situación de cada organización en materia de seguridad, se convierten en un indicador de la fortaleza del sistema de protección implementado. En efecto, las empresas aseguradoras requerirán un nivel mínimo de seguridad como precondición para dar la cobertura y luego ajustarán el valor de la prima a las condiciones que encuentren en revisiones sucesivas. En este contexto, es esperable que las empresas que tengan un mejor nivel de seguridad tengan primas menores y viceversa, cuando las condiciones no son las deseables. Del mismo modo, en la medida en que se fortalezca la seguridad, por ejemplo, instalando mejores sistemas de detección de incendios, mecanismos de acceso más confiables o sistemas de detección de intrusiones, podrán solicitarse mermas en las primas.

La frecuencia con la que se efectúen este tipo de ajustes, sean estos positivos o negativos, la publicación de estadísticas y el acceso a los valores de las primas son la base para la conformación de la este tipo de indicadores.

Sin embargo y a pesar de sus múltiples beneficios, el mercado de los seguros no se ha desarrollado completamente. En el año 2002 el economista Robert Hartwig, entonces Presidente de Instituto de Seguros de la Información (en inglés, "*Insurance Information Institute"*), en un reportaje realizado por el periódico WashingtonPost.com, manifestó que el mercado de las primas de seguro alcanzaría en empresas de los Estados Unidos los 2.500 millones de dólares estadounidenses en el año 2005. Sin embargo, en el año 2010, el valor del Mercado recién había alcanzado los 500 millones de dólares, según lo indicado por Robert Parisi, Vicepresidente Senior en la empresa de seguros Marsh [20].

Existen varios motivos para esta falta de desarrollo. Entre ellos se encuentra el temor de las empresas aseguradoras a un escenario de "huracán cibernético" que afecte a un alto número de empresas y sea motivo

de un volumen de reclamos tan elevado que no pueda ser afrontado por ellas. Este escenario se apoya en la gran interdependencia y estandarización de los sistemas informáticos, caracterizados por la falta de diversidad en las plataformas instaladas, lo que hace posible que una determinada vulnerabilidad pueda tener un efecto dominó sobre un importante número de plataformas y organizaciones. Esta concentración del riesgo atenta contra un principio básico del mercado de las aseguradoras, que busca un portafolio equilibrado de pólizas para repartir el riesgo. Para protegerse, las empresas aseguradoras incrementan sus primas, pensando en el peor escenario y buscando un equilibrio financiero para sus empresas.

Otro problema que dificulta el desarrollo de este mercado es la falta de datos actuariales para calcular las primas. Esta carencia condiciona el análisis de riesgo tanto desde el punto de vista de las empresas, que deben decidir si toman o no un seguro, como de las aseguradoras, que deben determinar las primas en función de las amenazas y los riesgos relacionados.

Por otro lado, la falta de exigencias legales para contratar seguros, hace que muchas empresas pospongan la decisión de contratarlos. Finalmente, influye también negativamente en esta solución de mercado la naturaleza intangible de los activos y las dificultades para sustanciar los reclamos.

La contratación de ciberseguros es más común en EEUU, Canadá y Europa. Sin embargo diversas publicaciones señalan que está creciendo en los países en desarrollo.

Finalmente cabe mencionar que a partir de la encuesta realizada, entre los elementos que eran considerados como las principales consecuencias negativas de una falla de seguridad (ver pregunta 9), se encontraban las pérdidas de información (20,5%) y dinero (11,1%) y las sanciones eventuales por incumplimiento de leyes, normas y contratos aplicables (10,3%). Cabe acotar que este tipo de riesgos pueden ser mitigados mediante su transferencia, a través de la contratación de ciberseguros específicos.

En conclusión, ya que el negocio de los seguros se encuentra organizado como un mercado específico, el nivel de las primas que se contraten puede constituir un indicador de la fortaleza del sistema de seguridad de una o varias organizaciones, a partir del cual pueden conformarse métricas valiosas tanto para los sistemas como para las organizaciones. Sin embargo, hasta tanto este mercado no adquiera un mayor nivel de desarrollo y un volumen significativo, estas métricas no serán lo suficientemente confiables.

El mercado de los "*exploits*"

Esta solución fue desarrollada por Böhme a partir de la aplicación de las opciones binarias a las vulnerabilidades, en un hipotético mercado en el que se transarían contratos vinculados a su materialización, normalmente conocidos como "*exploits*". La opción binaria es un concepto que proviene de las finanzas y consiste en un tipo de opción por la que un contrato transfiere a su tenedor el derecho, pero no la obligación, de comprar o vender una determinada acción por un precio específico (precio de ejercicio), en un plazo dado establecido de antemano (fecha de expiración o vencimiento). Las opciones binarias u opciones digitales son opciones de tipo "todo o nada" y brindan a los inversores un retorno fijo si se cumple el criterio de la opción. En efecto, este escenario plantea la existencia de contratos que se pagarían en una fecha determinada siempre y cuando, ocurran determinados eventos o bien, su contracara que supone un "contrato espejo", considerando un pago si dicho suceso no ocurre.

Böhme [3] desarrolla la idea de la existencia de un mercado en el que a través de una plataforma de intercambio, las partes pueden comprar contratos que pagan una determinada suma si una vulnerabilidad tiene lugar. Así, un determinado contrato, denominado "de vulnerabilidad", paga $100 si esa falla se manifiesta en un cierto producto para una fecha determinada. Por otro lado, aparece la figura de un contrato inverso, denominado "de seguridad", que paga igual suma si esa falla no tiene lugar antes de un día y una hora predeterminados. Se encomienda a una tercera parte confiable la

confirmación de que el evento tuvo o no lugar. Estos dos contratos son por su parte, comprados y vendidos en forma individual sucesivas veces en el mercado antes de la fecha fijada.

Un aspecto interesante de esta solución teórica desarrollada por Böhme [3], es la existencia de varios grupos de interés que podrían participar en este mercado. Por ejemplo, los usuarios de un determinado producto de software demandarían aquellos contratos, que el autor antes citado denomina C, que plantean la existencia de la vulnerabilidad, de manera de equilibrar los riesgos a los que se encuentran expuestos, minimizando posibles pérdidas. Lo mismo se aplicaría a las empresas que comercializan los productos que podrían verse afectados, dando una señal a sus clientes de que son seguros ya que se influiría negativamente sobre el precio al aumentar la demanda. Ocurriría algo similar con las empresas aseguradoras de las firmas que han implementado dicho producto.

En el otro extremo, algunos inversores no incluidos en los grupos anteriores, podrían adquirir los contratos C´, es decir aquellos que apuestan a que esa vulnerabilidad no ocurra, para diversificar su portafolio. Los competidores de las firmas dueñas de los productos eventualmente afectados, también tenderían a adquirir contratos C´ de estas últimas, apostando a demostrar un entorno de bajo nivel de seguridad en la competencia. Este esquema ideado por Böhme [3] podría ser también pensado, en palabras del mismo autor, como un incentivo a los desarrolladores para asegurar sus productos.

Finalmente, el autor considera la situación de los expertos en seguridad, que luego de evaluar el producto, podrían adquirir contratos C o C´ en función del resultado de sus revisiones.

Ya que ambos tipos de contratos se negocian en moneda corriente, todo el proceso de sucesivas compra-ventas tendrá necesariamente una influencia en el precio, a lo largo del tiempo, ese valor tendería a reflejar la probabilidad real de que las vulnerabilidades tengan lugar. Así el precio podría convertirse en métricas económicas de la fortaleza de los productos, a los que la vulnerabilidad podría o no afectar.

Sin embargo, además de su carácter hipotético a la fecha, se plantean algunos cuestionamientos a este modelo desarrollado por Böhme [3]. Entre ellos se encuentran la falta de una taxonomía de las vulnerabilidades que atomiza el eje de la contratación, la resistencia de los vendedores o desarrolladores a que se conozcan las vulnerabilidades que afectan sus productos, así como los precios que eventualmente serían pagados por los contratos y el desafío de motivar a los eventuales participantes en este mercado, de manera de contar con un alto número de participantes que garantice un precio que pueda ser utilizado efectivamente como métrica de la seguridad.

BENEFICIOS DE LA SEGURIDAD DE LA INFORMACIÓN

La SI, como ocurre con la aplicación de la seguridad en cualquier otra disciplina, se implementa con la intención de minimizar los riesgos que necesariamente trae la utilización malintencionada o errónea de uno o varios recursos.

En ese contexto, la SI suele ser expresada únicamente en función de la reducción de pérdidas esperadas, según lo expresa Wouter de Buijn [29]. Sin embargo, cabe preguntarse si ésta también puede ser pensada en términos del valor agregado que le aporta a una organización.

Esta cuestión no parece haber sido tratada adecuadamente aún en la bibliografía, quizás por tratarse de un área relativamente nueva. Sin embargo, algunos autores la proponen como un área de desarrollo futuro a medida que la SI sea considerada en mayor medida como un área estratégica de la organización.

La pregunta a responder es si el fortalecimiento de los procesos de gestión de la información en términos de la preservación de su confidencialidad, integridad y disponibilidad, así como de otros atributos que hacen a su confiabilidad, podría ser también expresado cuantitativa o cualitativamente en función de los beneficios esperados. Así, una organización que implementa una cultura de la seguridad acompañada de estrategias, políticas y procedimientos apropiados para la protección de la información y sistemas que utiliza, podría ser reconocida por sus empleados, clientes, usuarios, socios potenciales y otras partes interesadas, como una entidad responsable y robusta y en consiguiente, ser seleccionada frente a otras opciones, alternativas o competidores. A manera de ejemplo, una institución bancaria podría perder clientes si estos perciben que no genera mecanismos robustos de acceso lógico a sus bases de datos o no protege adecuadamente el acceso físico a sus cajeros automáticos.

En el mismo sentido, una organización podría ver depreciado su valor de venta si se demostrara que su SI es inadecuada. Steven Ross [22] especula que en una situación como la descripta, si la protección de los activos de información no alcanzara un nivel básico esperado, no habría

directamente adquisición, aduciendo que la inseguridad plantea dudas respecto a la estabilidad del negocio y de su habilidad para la supervivencia en el largo plazo. El citado autor agrega que la ausencia parcial o total de seguridad haría pensar que la gerencia ha ignorado los riesgos potenciales y por lo tanto, no ha adoptado las medidas de control para enfrentarlo. Concretamente, sostiene que se esperaría que la empresa cuente con una política de seguridad, basada en estándares, controles de acceso, protección a la privacidad y una estrategia de recuperación frente a desastres. El autor avanza en su análisis especulando que tal vez la compra podría llegar a realizarse, pero que la falta de seguridad podría ser utilizada como argumento para reducir el precio a pagar.

En el mismo sentido, la escasez de información relativa a los incidentes informáticos que sufren las organizaciones, por ejemplo los bancos, llevan a pensar que éstos no se difunden ante el riesgo que de los clientes opten por otra institución de similar propósito, al sentir que sus datos no se encuentran debidamente protegidos. La contracara de esta situación probaría que la SI le aporta valor a la organización en términos de clientes, visibilidad, etc.

Ahondando en su análisis, Ross [22] sugiere la utilización del concepto de “suficiencia de la SI”, denotando la importancia de un adecuado proceso de gestión de riesgos para determinar el grado en que los recursos y la información se encuentran adecuadamente protegidos.

También destaca que en la actualidad, el concepto de propiedad intelectual está directamente ligado al nivel de SI que se utiliza para protegerla, con lo cual también en este caso, la seguridad podría ser expresada como un porcentaje del valor total de este concepto.

Así aparecen diversos elementos que llevan a suponer que ante una tendencia creciente e inexorable de dependencia de las organizaciones de cualquier naturaleza respecto de las TI, la SI se convertirá a un valor distintivo y vital a la hora de evaluar la eficiencia de una entidad y determinar su valor de mercado. Será necesario en consiguiente, valorizar su influencia en el mantenimiento de las ventajas competitivas de la organización, al tener como objetivos la protección adecuada de los servicios que presta y la

información que gestiona, garantizar un flujo de fondos y una rentabilidad acorde con las expectativas de los propietarios y otras partes interesadas y asegurar el cumplimiento de las leyes, todo esto en la dirección de mantener la imagen y reputación de la organización.

Para determinar la percepción que se tiene de la SI, una de las preguntas de la encuesta citada precedentemente apuntó a establecer si ésta era pensada en sí misma como portadora de beneficios para la organización o sólo como una herramienta para disminuir los costos (ver pregunta 14). En este sentido, se obtuvo una mayoritaria respuesta (97,4%) respecto a que los efectos eran siempre beneficiosos.

A continuación (ver pregunta 15) buscó determinar cuáles eran esos beneficios que la SI le aportaba a la organización. Esta pregunta se formuló solo a aquellos especialistas que había considerado que la SI aportaba valor a la organización y no una mera minimización de costos. Sin embargo, la respuesta más votada fue “Ahorros al evitar pérdidas de información o de recursos”, seguida de “Mayor calidad de los productos o servicios”, “Mayor confianza de los usuarios al utilizar los sistemas” y “Mejor imagen en clientes y proveedores” y “ante la opinión pública”. Si bien la primera selección parece contradecir la elección de la pregunta anterior, las siguientes muestran a la SI como vehículo para una mayor calidad y mayor confianza en usuarios y como elemento contribuyente a la mejor imagen de la organización.

Profundizando el análisis, se segmentó la respuesta a la pregunta en función de las funciones desempeñadas por los especialistas consultados (cruce de preguntas 5 y 15), tratando de determinar cuáles eran los mayores beneficios asociados según las responsabilidades y tareas que se desempañaban. El resultado de esta estratificación se muestra en el siguiente cuadro, donde la primera columna denota el orden respecto al beneficio más votado y la primera fila distingue el rol de los encuestados en la organización. Se destacan los puntos coincidentes.

	Gerentes no informáticos	Gerentes o Personal de TI	Gerentes o Personal de SI
1	Mejores condiciones de trabajo para los empleados	Reconocimiento de la corporación/sede central	Reconocimiento de la corporación/sede central
2	Mayor confianza de los usuarios al usar los sistemas	Informes satisfactorios de los auditores	Informes satisfactorios de los auditores
3	Procesos eficientes de toma de decisiones	Procesos eficientes de toma de decisiones	Menor exposición a litigios o sanciones de organismos de contralor

A partir del cuadro, podrían formularse las siguientes conclusiones:

- Que los gerentes no informáticos priorizan a los empleados y la confiabilidad de los usuarios, posiblemente explicado en el hecho de que no se interesan en aspectos técnicos y son usuarios calificados de las TI.
- Que las área de TI y SI priorizan el reconocimiento de la organización y los informes de los auditores.
- Que los gerentes no informáticos y los gerentes y el personal de TI entienden que la SI contribuye a mejorar el proceso de toma de decisiones.
- Que únicamente el personal de SI tuvo en cuenta el aspecto vinculado al cumplimiento del marco normativo.

CONCLUSIÓN

La centralidad de la SI en los procesos de negocios ha alcanzado tal magnitud en términos económicos, que ha generado que los responsables de las áreas de competencia se vean en la necesidad de utilizar los mecanismos y el lenguaje del resto de organización, a la hora de competir por los fondos disponibles y demostrar la eficacia de sus inversiones.

Esta realidad obliga a los especialistas en SI a proveer justificaciones fundamentadas para obtener los recursos que necesitan y a formalizar sus presentaciones ante los niveles directivos, utilizando métodos y métricas económico-financieras largamente empleados en otras áreas de la organización. Así, deben demostrar la viabilidad de sus proyectos, combinando detalles técnicos de la actividad con un adecuado análisis económico-financiero.

La bibliografía ha ofrecido en los últimos años una variedad de métricas aplicables a la SI, que permiten evaluar y comparar proyectos de SI, tanto en forma previa a su implementación como en cuanto a sus resultados. Entre ellas, pueden citarse ROSI, IRR, ALE y NPV.

Sin embargo, en coincidencia con otros estudios realizados, la encuesta llevada a cabo como parte del trabajo, demostró que estas métricas no parecen ser suficientemente conocidas ni utilizadas. Efectivamente, más de la mitad de los especialistas encuestados manifestó no saber lo suficiente sobre ellas, descreer de su utilidad o no tener opinión al respecto. Al analizar los motivos para esta posición, aparecen entre otros, las dificultades para calcularlas, que devienen principalmente de las complejidades que acarrea la estimación de los ingresos vinculados a la SI y de la falta de datos históricos sobre la ocurrencia de fallas o ataques. La insuficiente preparación de los responsables del área de seguridad respecto a la utilización de métricas económicas es también un motivo, que puede ser parcialmente explicado por la vertiginosidad con que la SI pasó a ocupar un rol central en la organización.

Acompañando lo indicado en la bibliografía, los resultados de la encuesta demostraron que ROSI es la métrica más empleada, posiblemente

por reflejar para la SI el uso extendido del ROI en el resto de la organización. Le siguen IRR y ALE.

Sin dejar de reconocer las dificultades que plantea el cálculo de este tipo de métricas en el campo de la SI y las imprecisiones que pueden generarse, los especialistas deben reconocer que es necesario justificar frente a los niveles gerenciales, la eficiencia y efectividad en términos utilidad económica de sus iniciativas. En este sentido, las características de cada proyecto determinarán el tipo de métrica a aplicar en función del grado de dificultad que deviene de cada caso en particular. En consecuencia, deben incrementar sus esfuerzos para expresar su actividad en términos monetarios, respondiendo a los requerimientos de la organización. Por otro lado, es esperable que con el tiempo estas dificultades se vean superadas, especialmente en lo que respecta a contar con un mayor volumen de datos históricos y a mejorar la formación de los responsables de SI en el campo del uso de mecanismos económicos para justificar su actividad.

El trabajo también analizó otras lecturas que las herramientas de la Economía permiten realizar respecto de la SI. En efecto, el mercado ofrece algunas instancias que pueden ser utilizadas para mostrar el valor que un adecuado marco de protección de la información le aporta a la organización. Es el caso de los ciberseguros, cuyo desarrollo muestra una evolución inferior a la estimada inicialmente pero de crecimiento constante. A medida que su uso se extienda, es esperable que el valor de las primas se convierta en un indicador de la robustez de los esquemas de SI de una organización.

Otros mecanismos, tales como las recompensas por la denuncia de fallas o la compra-venta de vulnerabilidades, han sido cuestionados por diversos motivos y no son consideradas como representativas del verdadero valor que la explotación de dicha vulnerabilidad significaría para una organización. En cuanto a la influencia de la difusión al público de una falla de seguridad en el valor de las acciones de la organización afectada, los estudios realizados por varios autores han demostrado que en la mayoría de los casos, se registra algún tipo de impacto. Sin embargo, dicha afectación suele ser reflejo de múltiples factores, no siendo posible aislar las consecuencias debidas exclusivamente a un compromiso de la seguridad.

Por último, el trabajo buscó responder si la SI podía ser pensada en términos de beneficio para la organización, trascendiendo la mera disminución de las pérdidas potenciales. Las escasas publicaciones que han intentado responder a este interrogante parecen demostrar que esto es así, ya que una SI poco robusta puede alejar clientes, socios y otras partes interesadas e inclusive, influir negativamente en una eventual venta de una organización, reduciendo su valor de adquisición. En este sentido, los especialistas consultados en la encuesta adhirieron en forma casi unánime a considerar que la SI representa un beneficio para la organización. Si bien a la hora de precisar los beneficios, la opción más seleccionada fue “Ahorros al evitar pérdidas de información o de recursos”, le siguieron, con valores cercanos, “Mayor calidad de los productos y servicios” y “Mayor confianza de los usuarios al utilizar los sistemas”. Estos resultados permiten inferir que, en la opinión de los especialistas consultados, la SI le aporta valor a la organización, además de implicar una minimización de efectos negativos.

Se concluye entonces que el herramental, ya sea bajo la forma de métricas o indicadores de mercado, que brinda la Economía permite fortalecer la SI en una organización y apreciar su nivel de robustez. Esta afirmación es aplicable tanto desde una perspectiva interna enfocada a la gestión, como respecto al valor que le otorga a la entidad. En consecuencia, para alcanzar una gestión exitosa, los responsables de SI deben ampliar el espectro de su análisis para incluir la perspectiva económica, mejorando de esta manera sus posibilidades de obtener y aplicar los fondos en las implementaciones que llevan adelante. Cuanto antes lo concreten, mejores serán las oportunidades que tendrán para fortalecer el marco de protección de la información, demostrando de esta manera el valor que la SI puede aportarle a la organización.

Anexo I – Análisis de la encuesta

Metodología

Con el objeto de analizar los factores que influyen en el proceso de toma de decisiones a la hora de determinar la inversión en SI, entre los meses de octubre y diciembre del año 2010 se realizó una encuesta dirigida a profesionales vinculados a las TI y a la SI. En particular, se buscó conocer la visión desde la perspectiva del análisis costo-beneficio de aquellos involucrados cotidianamente en la implementación de controles y en la adopción de medidas de seguridad de las acciones. Los resultados recopilados constituyeron la fuente primaria de datos para las conclusiones que se incorporan al final de la presente sección.

Específicamente, la encuesta tuvo los siguientes objetivos:

1. Conocer los puntos de vista y las percepciones que perfilan el proceso de presupuestación de la inversión en SI y la manera en que se determinan los costos de las medidas a implementar.
2. Estimar el nivel de uso de las metodologías cuantitativas de evaluación de costos y beneficios de la SI y la percepción que se tiene de ellas.
3. Determinar si la SI puede ser promovida a partir de los beneficios que le aporta a la organización y no meramente por la disminución de costos o por la neutralización de otros efectos negativos que su falta acarrea.

La encuesta se basó en 15 preguntas, de tipo “multiple choice” y fue realizada a nivel local y regional, cubriendo organizaciones tanto públicas como privadas. En total, se obtuvieron 167 respuestas. Cabe acotar que en 13 casos no se llegó a completar todo el cuestionario. En algunos casos, estas respuestas parciales fueron tomadas en cuenta ya que aportaban información a la encuesta.

Para el desarrollo de la encuesta se utilizó la herramienta disponible en el sitio web www.surveymonkey.com, que ofrece una interface gráfica sencilla y amigable y que permite incorporar una serie de controles para facilitar la recolección de respuestas y su posterior análisis. Adicionalmente se incorporó un canal seguro para garantizar la privacidad de los datos, si bien se evitó recopilar información que pudiera ser catalogada como crítica o personal. La publicación de la versión definitiva de la encuesta fue precedida por un periodo de prueba, para validar la

redacción de las preguntas, asegurar su comprensión en función de los objetivos buscados.

Las respuestas obtenidas provinieron de expertos de la Argentina, y en menor número, de Paraguay, Colombia, Uruguay, Guatemala, México, Perú, Chile, Brasil, Venezuela, España, EEUU, Costa Rica y Panamá. Asimismo, se cubrieron diversos ámbitos de la economía tales como lo son el sector público, el académico, el de consultoría, el productivo, etc.

Análisis de datos

Sección A: Perfil de los participantes

Las primeras cinco preguntas se orientaron a determinar las características principales de la organización en la que se desempeña el encuestado, buscando determinar:

- El país en el que desarrolla su actividad.
- El sector en el que trabaja.
- El alcance geográfico de la organización.
- La cantidad de empleados.
- El cargo o función del especialista.

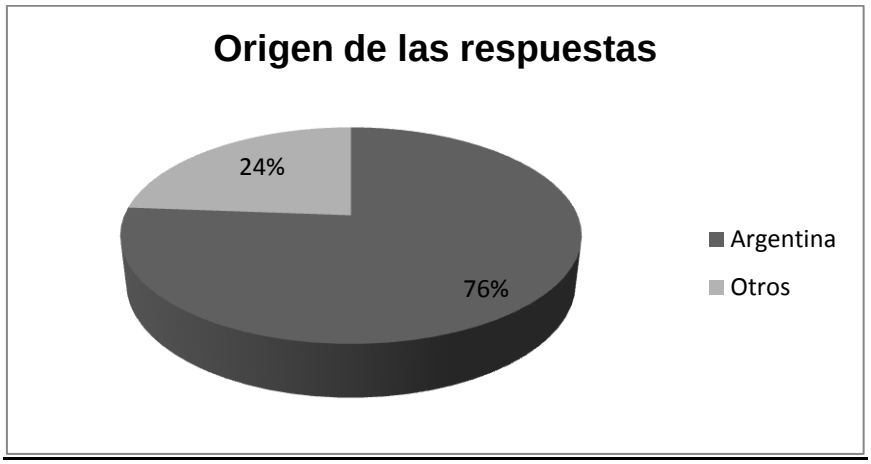
Los resultados recopilados permiten afirmar que la muestra presenta características regionales, con representatividad de diversos sectores y organizaciones nacionales y multinacionales. Aproximadamente la mitad de los consultados trabaja en organizaciones de más de mil empleados. Un tercio se desempeña en el área de SI y otro tanto en TI. A continuación se desglosan los datos recopilados.

País de origen

Un 76,2% de las respuestas provinieron de Argentina y el resto de otros países de la región latinoamericana, EEUU, España y Francia. Con esto se logró regionalizar el universo de especialistas.

Señale su país de residencia.		
Países	**Porcentaje**	**Total**
Argentina	76,2%	128
Colombia	7,1%	12
Brasil	3,6%	6
Uruguay	2,4%	4
México	1,8%	3
Guatemala	1,8%	3
Paraguay	1,2%	2
Chile	1,2%	2
Costa Rica	1,2%	2
España	0,6%	1
Perú	0,6%	1
Venezuela	0,6%	1
EEUU	0,6%	1
Panamá	0,6%	1
Francia	0,6%	1
	Total respuestas	**168**

Tabla 1: País de residencia de los especialistas que respondieron la encuesta



Cuadro 1: El gráfico muestra la proporción de respuestas recibidas de expertos de Argentina y de otros países.

Sector de la industria

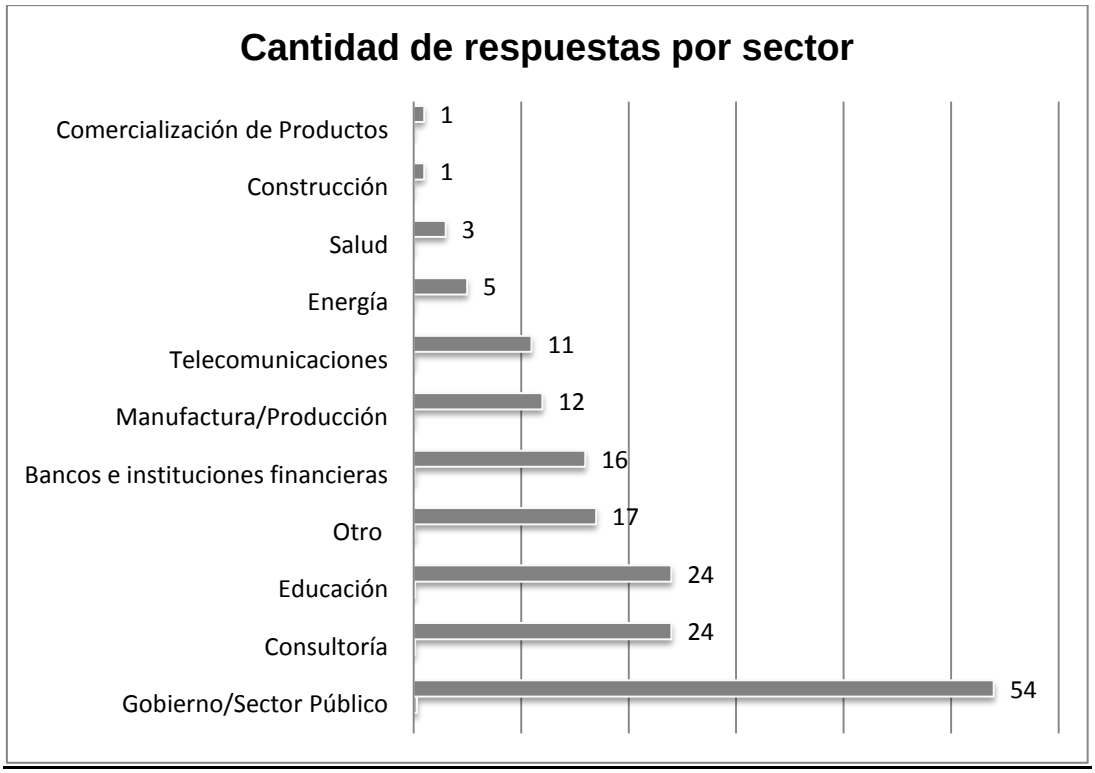
Aproximadamente un tercio de las respuestas (32%) provinieron de especialistas del sector público, mientras que del resto, los rubros con mayor volumen de respuestas fueron los de consultoría (14%) y educación (14%).

Señale el sector al que pertenece la organización en la que se desempeña.		
Sector	**Porcentaje**	**Total**
Gobierno/Sector Público	32,1%	54
Consultoría	14,3%	24
Educación	14,3%	24
Otro	10,1%	17
Bancos e instituciones financieras	9,5%	16
Manufactura/Producción	7,1%	12
Telecomunicaciones	6,5%	11
Energía	3,0%	5
Salud	1,8%	3
Construcción	0,6%	1
Comercialización de productos	0,6%	1
	Total respuestas	**168**

Tabla 2: Sector en el que se desempeña el especialista

Dentro del grupo “Otro”, se encuadraron un total de 17 especialistas de, entre otras, las siguientes áreas:

- Organismo internacional.
- Televisión y espectáculos.
- Aeronavegación.
- Medios.
- ONG.



Cuadro 2: El eje vertical muestra los sectores en los que desarrollan su actividad los participantes de la encuesta, mientras que las barras presentan la cantidad de respuestas obtenidas en cada caso.

Tipo de organización

Un 74.4% de los que respondieron desempeñan funciones en empresas de alcance nacional mientras que el 25,6% restante trabaja en empresas multinacionales.

Alcance territorial de la Organización en la que se desempeña el especialista		
Alcance	**Porcentaje**	**Total**
Nacional	74,4%	125
Multinacional	25,6%	43
	Total respuestas	**168**

Tabla 3: Alcance geográfico de la organización

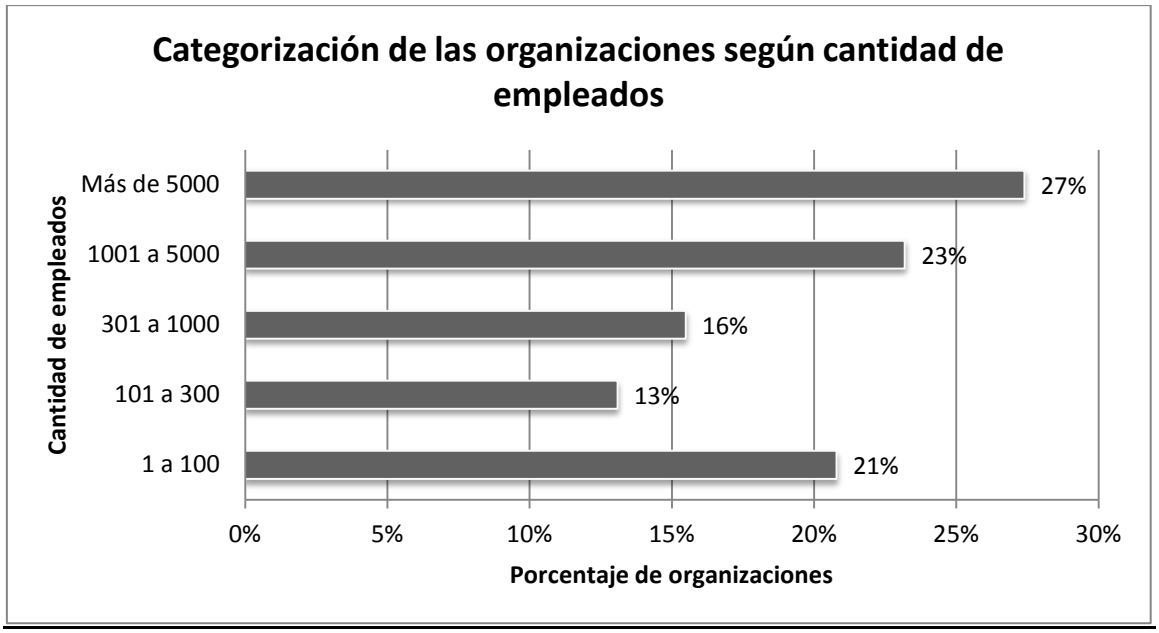
Cuadro 3: El gráfico presenta en porcentajes, la pertenencia de los encuestados a una organización del alcance nacional o internacional.

Tamaño de la planta de personal de la organización

De los datos recopilados se desprende que algo más de la mitad de los especialistas consultados se desempeñan en organizaciones de más de 1000 empleados, alcanzando un total de 50,6%. Por su parte un 33,9% desarrolla sus funciones en empresas caracterizadas como PyMES a nivel nacional, con hasta 300 empleados.

Indique la cantidad de empleados de la organización en la que se desempeña		
Cantidad de empleados	**Porcentaje**	**Total**
1 a 100	20,8%	35
101 a 300	13,1%	22
301 a 1000	15,5%	26
1001 a 5000	23,2%	39
Más de 5000	27,4%	46
	Total respuestas	**168**

Tabla 4: Cantidad de empleados en la organización



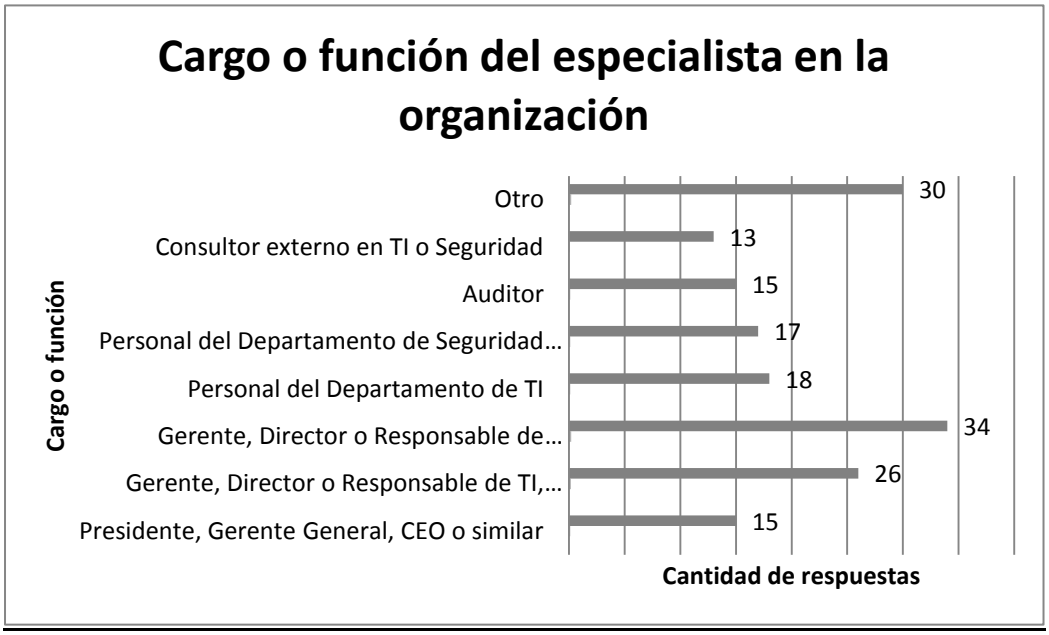
Cuadro 4: El eje vertical estratifica las respuestas en función de la cantidad de empleados de las organizaciones en las que se desempeñan los encuestados. El eje horizontal por su parte, refleja la cantidad de respuestas en porcentaje. Estos valores se muestran también junto a cada barra.

Función de los participantes

Un 8,9% de los especialistas consultados ocupaban cargos directivos en la organización, mientras que un 26,2% trabajaba en el área de TI y un porcentaje levemente superior (30,3%) se desempeñaba directamente en el área de SI. Del 34,6% restante, un 7,7% trabajaba como consultor independiente y un 8,9% en el rol de auditor. En la categoría de otros se ubicaron investigadores, docentes y gerentes de otras áreas de la organización.

Cargo o función del especialista en la organización		
Cargo o función	**Porcentaje**	**Total**
Presidente, Gerente General, CEO o similar	8,9%	15
Gerente, Director o Responsable de TI, CIO o similar	15,5%	26
Gerente, Director o Responsable de Seguridad, CISO o similar	20,2%	34
Personal del Departamento de TI	10,7%	18
Personal del Departamento de Seguridad de la información	10,1%	17
Auditor	8,9%	15
Consultor externo en TI o Seguridad	7,7%	13
Otro (especifique a continuación)	17,9%	30
	Total respuestas	**168**

Tabla 5: Cargo o Función del especialista encuestado



Cuadro 5: Distribuye a los encuestados según su cargo o función en la organización. Presenta la cantidad de respuestas para cada categoría junto a cada barra.

Sección B: Importancia de la seguridad de la información en la organización

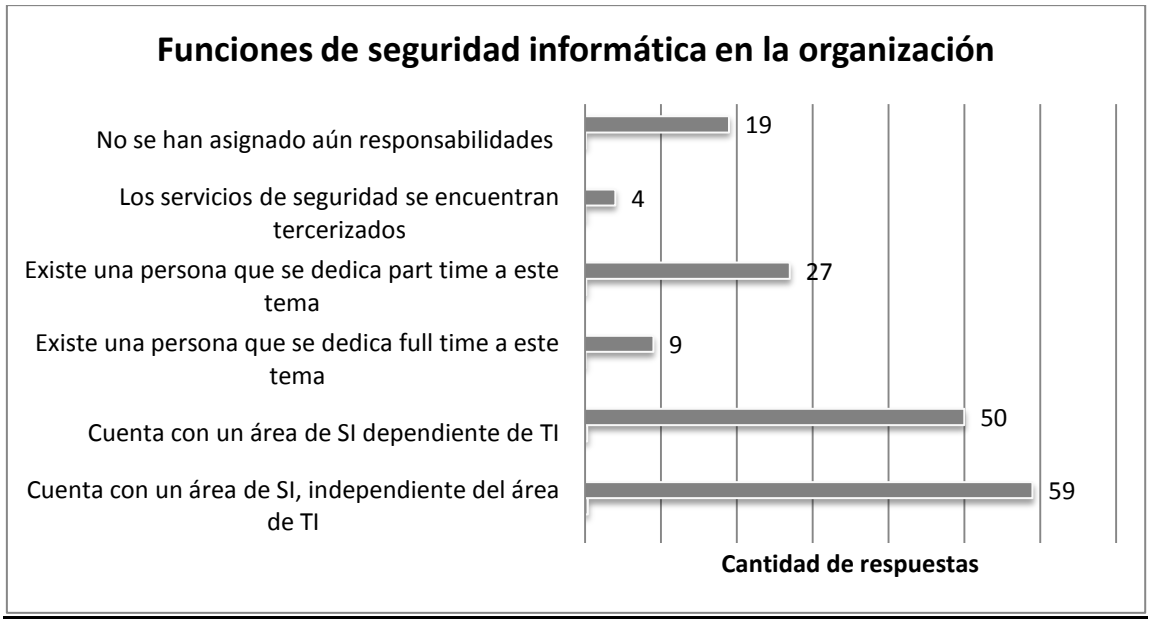
Esta sección se orientó a determinar el nivel de formalización de las funciones de SI en la organización y a la existencia de un presupuesto específico para los elementos vinculados.

Formalización del área de seguridad de la información en la estructura

Como puede observarse en el cuadro que sigue, solo algo más de un tercio de los participantes declara que su organización cuenta con un área independiente de TI dedicada específicamente a SI. Un 30% manifiesta que si bien cuentan con una unidad dedicada a la temática, ésta depende de Sistemas. Debe tenerse en cuenta que esta dependencia es desaconsejada en la mejores prácticas por comprometer la objetividad y libertad de acción de quienes se dedican a la protección de los recursos tecnológicos. Finalmente, un tercios cuenta solo con una persona dedicada part-time a la SI o directamente, carece de un recurso dedicado a tal fin.

¿En qué etapa se encuentra su organización en cuanto a la seguridad de la información?		
Existencia de un área de seguridad	**Porcentaje**	**Total**
Cuenta con un área de Seguridad de la información independiente del área de TI	35,1%	59
Cuenta con un área de Seguridad de la información dependiente del área de TI	29,8%	50
No cuenta con un área de SI pero existe una persona que se dedica full time a este tema	5,4%	9
No cuenta con un área de SI pero existe una persona que se dedica part-time a este tema	16,1%	27
Los servicios de seguridad se encuentran tercer-izados en una empresa o consultora externa	2,4%	4
No se han asignado responsabilidades en materia de Seguridad de la información	11,3%	19
	Respuestas totales	**168**

Tabla 6: Muestra la importancia que le da la organización en su estructura a las funciones de seguridad de la información



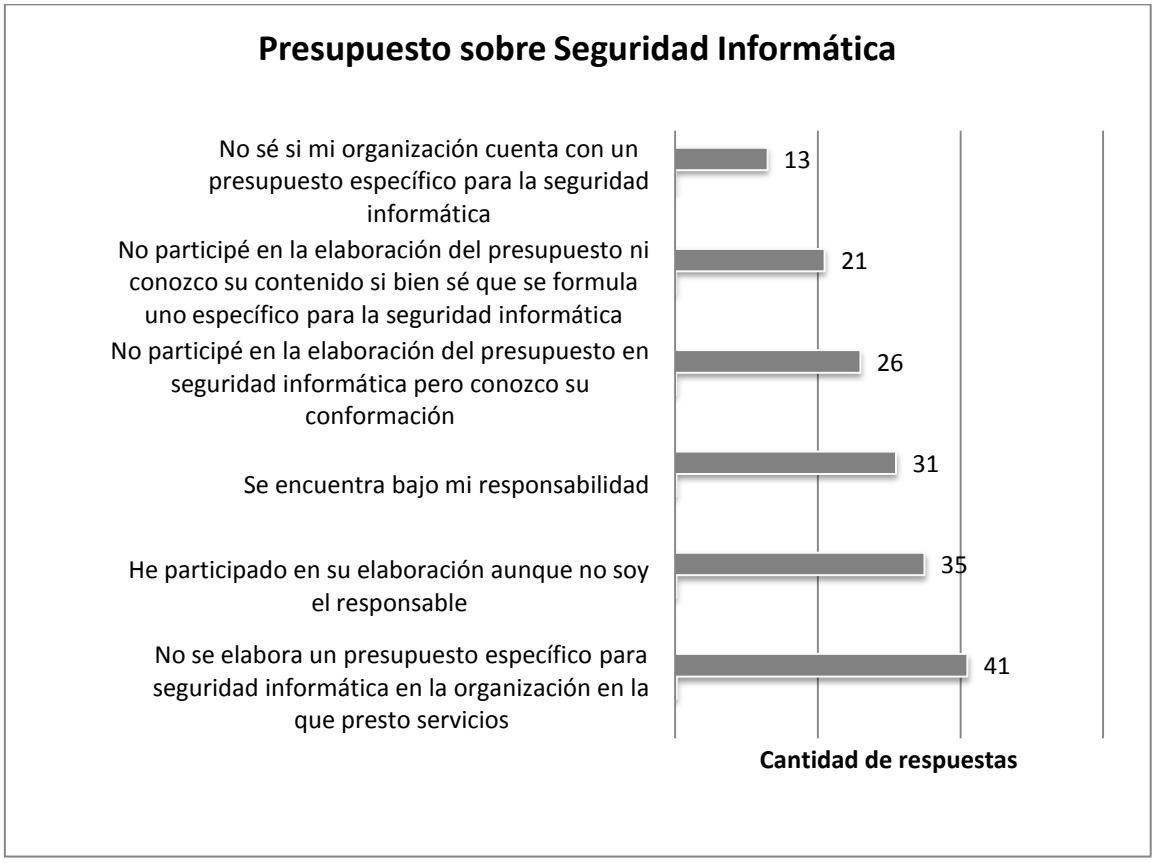
Cuadro 6: Presenta en función de la cantidad de respuestas el grado de formalidad que la organización en la que se desempeña el especialista le da al área de SI. El eje horizontal muestra la cantidad de respuestas recibidas.

Participación en la elaboración del presupuesto

Como puede observarse en el cuadro que sigue, solo un tercio de los participantes en la muestra señala que en su presupuesto no se distinguen rubros específicos para la SI, mientras que del resto, un 39,6% indica estar a cargo de su determinación o bien que ha participado en el proceso de su elaboración.

¿Ha participado en la elaboración del presupuesto de seguridad de la información de su organización, o bien conoce su conformación?		
Responsabilidad en la elaboración del presupuesto de SI	**Porcentaje**	**Total**
No se elabora un presupuesto específico para seguridad de la información en la organización en la que prestó servicios	24,6%	41
He participado en su elaboración aunque no soy el responsable	21,0%	35
Se encuentra bajo mi responsabilidad	18,6%	31
No participé en la elaboración del presupuesto en seguridad de la información pero conozco su conformación	15,6%	26
No participé en la elaboración del presupuesto ni conozco su contenido si bien sé que se formula uno específico para la seguridad de la información	12,6%	21
No sé si mi organización cuenta con un presupuesto específico para la seguridad de la información	7,8%	13
	Respuestas totales	**167**

Cuadro 7: Presenta el nivel de responsabilidad del especialista encuestado respecto a la formulación del presupuesto de Seguridad de la información de su organización



Cuadro 7: Presenta la cantidad de respuestas respecto a la participación en la elaboración del presupuesto: si la organización formula un presupuesto para seguridad de la información y el nivel de participación de los encuestados en su formulación.

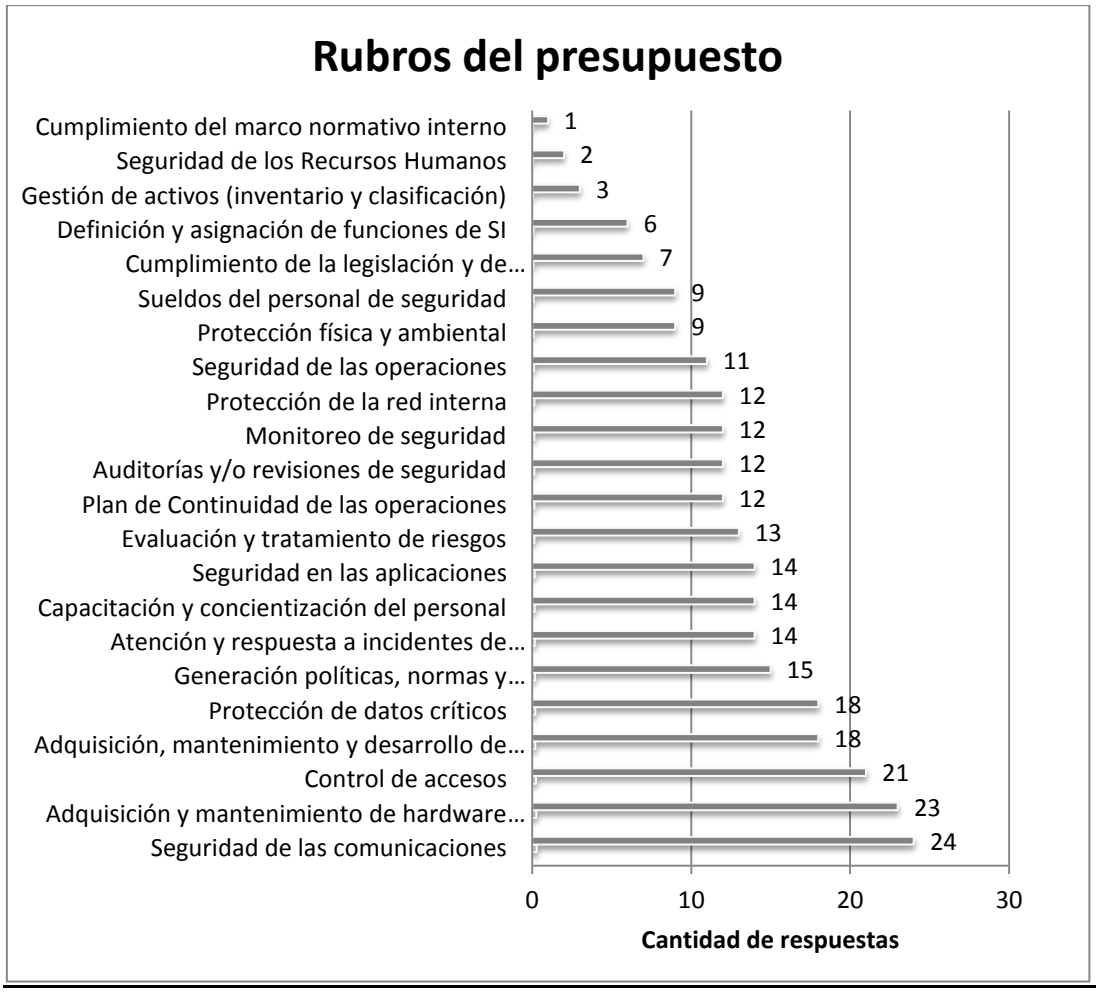
Conformación del presupuesto

Esta pregunta estuvo orientada a determinar los rubros del presupuesto en seguridad de la información a los que se destinan mayores fondos. Fue presentada solo a aquellos que en la pregunta anterior, habían marcado una de la primeras tres opciones, es decir que tenían el presupuesto bajo su responsabilidad, que habían participado en su elaboración o que conocían su contenido. A ellos se les solicitó indicar los tres ítems que consumían un mayor presupuesto en sus respectivas organizaciones.

Como se desprende del resumen de respuestas que sigue, los más seleccionados fueron la seguridad en las comunicaciones (26,7%), la adquisición y el mantenimiento de hardware de seguridad (25,6%) y el control de acceso (23,3%).

Señale los tres temas o áreas que consumen un mayor porcentaje de los fondos disponibles para seguridad de la información en su organización.		
Rubros del presupuesto	**Porcentaje**	**Total**
Seguridad de las comunicaciones	26,7%	24
Adquisición y mantenimiento de hardware de seguridad	25,6%	23
Control de accesos	23,3%	21
Adquisición, mantenimiento y desarrollo de software de seguridad	20,0%	18
Protección de datos críticos	20,0%	18
Generación políticas, normas y procedimientos	16,7%	15
Atención y respuesta a incidentes de seguridad	15,6%	14
Capacitación y concientización del personal	15,6%	14
Seguridad en las aplicaciones	15,6%	14
Evaluación y tratamiento de riesgos	14,4%	13
Plan de Continuidad de las operaciones	13,3%	12
Auditorías y/o revisiones de seguridad	13,3%	12
Monitoreo de seguridad	13,3%	12
Protección de la red interna	13,3%	12
Seguridad de las operaciones	12,2%	11
Protección física y ambiental	10,0%	9
Sueldos del personal de seguridad	10,0%	9
Cumplimiento de la legislación y de contratos con terceros	7,8%	7
Definición y asignación de funciones de SI	6,7%	6
Gestión de activos (inventario y clasificación)	3,3%	3
Seguridad de los Recursos Humanos	2,2%	2
Cumplimiento del marco normativo interno	1,1%	1
	Total respuestas	**90**

Tabla 8: Ranking de clasificación por monto de los ítems que conforman el presupuesto en Seguridad de la información.



Cuadro 8-A: El cuadro muestra la priorización de los ítems que conforman el presupuesto en seguridad de la información, de acuerdo al monto, en la percepción de los especialistas consultados

Focalizando en los 10 elementos más seleccionados y como puede apreciarse del cuadro que sigue, se presenta una variedad de temas como lo son la capacitación, la generación de un marco normativo y procedimental para la seguridad de la información así como la incorporación de elementos de hardware, software y comunicaciones.

Cuadro 8-B: El cuadro muestra los diez ítems más seleccionados en cuanto a su participación en el presupuesto de seguridad de la información, de acuerdo al monto.

Sección C: Percepción de los encuestados respecto a la seguridad de la información

Al analizar los daños que puede sufrir una organización cuando se enfrenta con una falla o incidente de seguridad, las pérdidas pueden ser inmediatas o indirectas. En el primer caso, se trata de pérdida de ingresos, de productividad o un aumento en los costos de seguros, horas extras, etc.). Las pérdidas indirectas suelen ser más serias ya que sus efectos negativos perduran mayor tiempo sobre terceros, tales como clientes, proveedores, socios, fuentes de crédito, etc. Los costos indirectos afectan la reputación de la organización, causan la interrupción de procesos de negocios, responsabilidades legales y daños en la confianza de los clientes.

Los daños causados por un incidente de seguridad se focalizan generalmente en la confidencialidad, integridad y disponibilidad de los activos de información. Entre ellas, el impacto sobre la confidencialidad suele ser considerado el que reviste mayor gravedad.

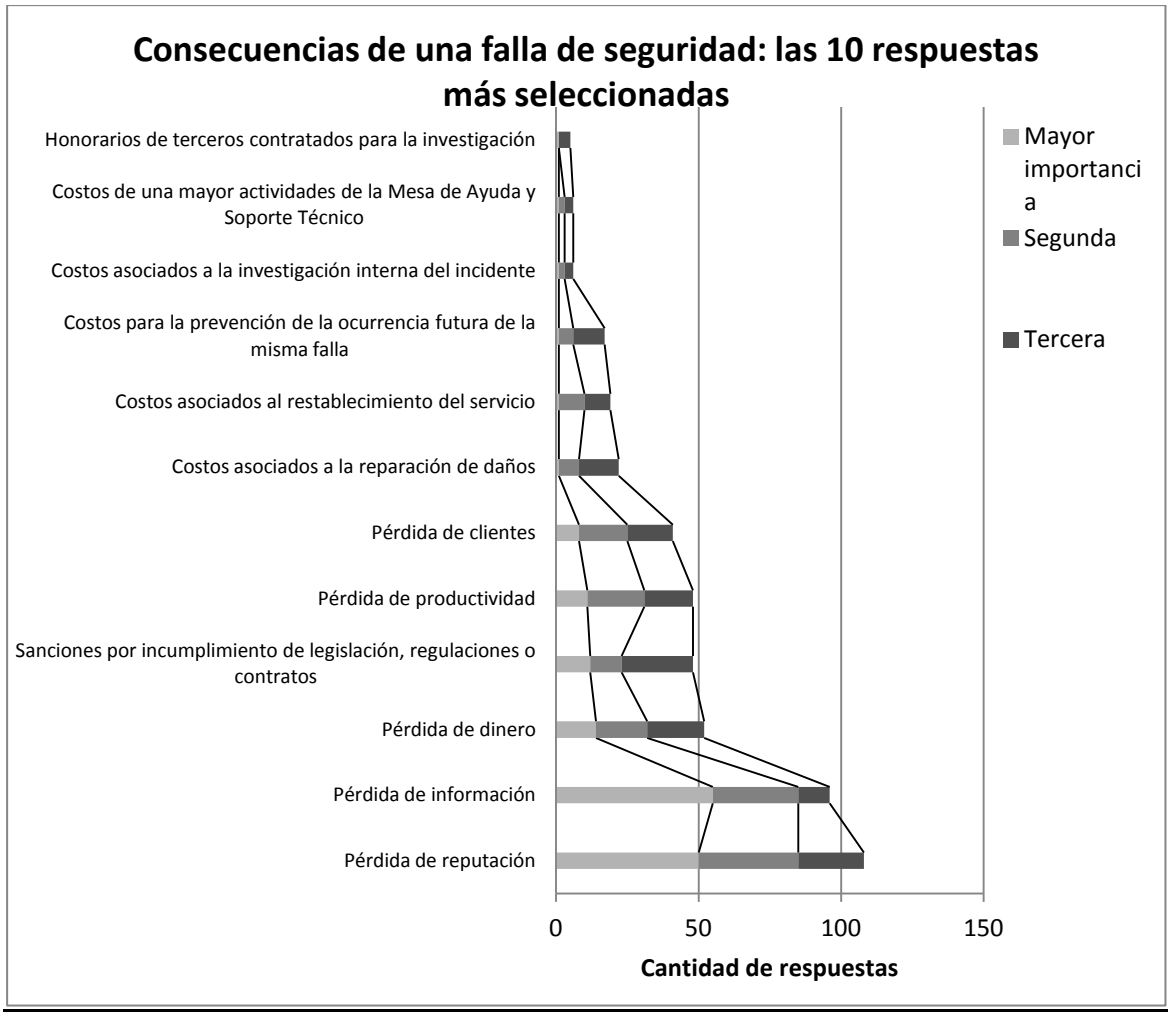
Sin embargo, los costos reales de un incidente de seguridad son difíciles de determinar, ya que las organizaciones no hacen un seguimiento sistemático ni documentan su ocurrencia y no comparten información con otras por temor a los efectos en la opinión pública.

Costos potenciales de una falla de seguridad

En esta pregunta se buscó determinar cuáles eran a juicio de los entrevistados, las principales consecuencias negativas de la falta de seguridad. En este sentido, la pérdida de información fue la más votada, seguida de la afectación de la reputación y la pérdida financieras.

A la hora de estimar los costos potenciales de una eventual falla de seguridad, señale los tres elementos más significativos a tener en cuenta, priorizándolos según su importancia.				
Elementos más significativos	**Mayor importancia**	**Segunda en orden de importancia**	**Tercera en orden de importancia**	**Total**
Pérdida de reputación	50	35	23	108
Pérdida de información	55	30	11	96
Pérdida de dinero	14	18	20	52
Sanciones por incumplimiento de legislación, regulaciones o contratos	12	11	25	48
Pérdida de productividad	11	20	17	48
Pérdida de clientes	8	17	16	41
Costos asociados a la reparación de daños	1	7	14	22
Costos asociados al restablecimiento del servicio	1	9	9	19
Costos para la prevención de la ocurrencia futura de la misma falla	1	5	11	17
Costos asociados a la investigación interna del incidente	1	2	3	6
Costos de una mayor actividades de la Mesa de Ayuda y Soporte Técnico	1	2	3	6
Honorarios de terceros contratados para la investigación	1	0	4	5
			Respuestas totales	**156**

Tabla 9: Muestra la percepción de los participantes respecto a las consecuencias de una falla en la seguridad.



Cuadro 9-A: Muestra la percepción de los participantes respecto a las diez consecuencias de una falla en la seguridad con mayor impacto, indicando las seleccionadas como las de mayor importancia.

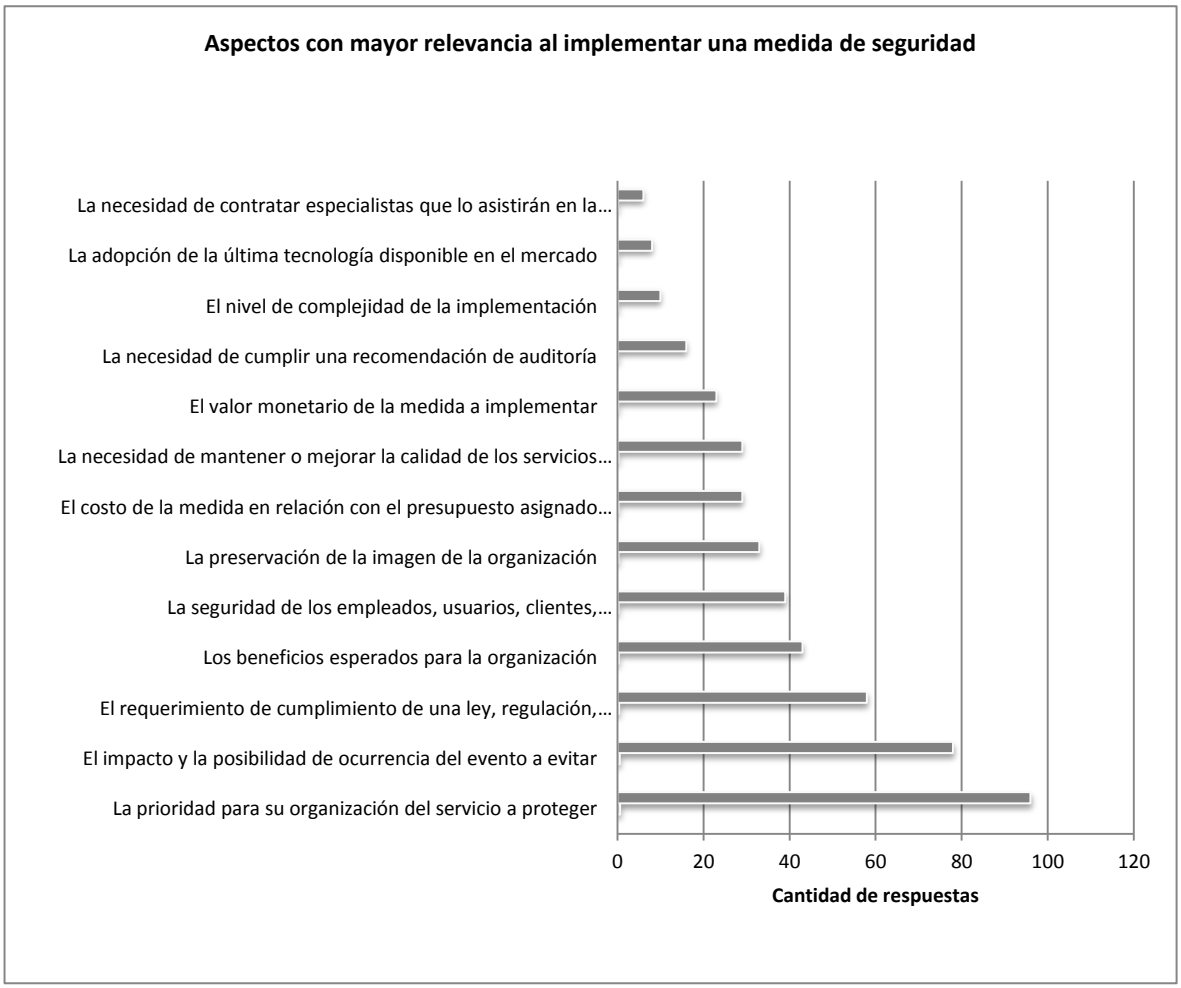
Tabla 9-B: Muestra la percepción de los participantes en la encuesta respecto a las consecuencias de una falla en la seguridad, con valores promedio de respuesta.

Aspectos de mayor incidencia en las decisiones de implementación de controles

El objetivo de esta pregunta fue determinar los factores en los que los especialistas consultados tendían a focalizarse frente a la necesidad de recomendar o implementar medidas de seguridad. En este sentido, se observa que la prioridad que le da la organización al servicio a proteger, el nivel de riesgo, determinado por el impacto y el cumplimiento de normas y reglamentaciones, son los factores determinantes a la hora de sopesar las medidas de seguridad.

Si tuviera que recomendar, o directamente implementar, una medida de seguridad para proteger un recurso o dato crítico de su organización, señale los tres aspectos que más pesarían en su decisión.		
Respuestas	**Porcentaje**	**Total**
La prioridad para su organización del servicio a proteger	61,5%	96
El impacto y la posibilidad de ocurrencia del evento a evitar	50,0%	78
El requerimiento de cumplimiento de una ley, regulación, estándar o norma corporativa	37,2%	58
Los beneficios esperados para la organización	27,6%	43
La seguridad de los empleados, usuarios, clientes, proveedores, terceros en general	25,0%	39
La preservación de la imagen de la organización	21,2%	33
El costo de la medida en relación con el presupuesto asignado al área de seguridad de la información	18,6%	29
La necesidad de mantener o mejorar la calidad de los servicios que se brindan	18,6%	29
El valor monetario de la medida a implementar	14,7%	23
La necesidad de cumplir una recomendación de auditoría	10,3%	16
El nivel de complejidad de la implementación	6,4%	10
La adopción de la última tecnología disponible en el mercado	5,1%	8
La necesidad de contratar especialistas que lo asistirán en la medida	3,8%	6
	Total Respuestas	**156**

Tabla 10: Aspectos con mayor peso a la hora de recomendar o implementar una medida de seguridad o un control.



Cuadro 10: Aspectos con mayor peso a la hora de recomendar o implementar una medida de seguridad o un control, expresados en función de los promedios de respuesta.

Sección D: Herramientas de medición de la seguridad de la información

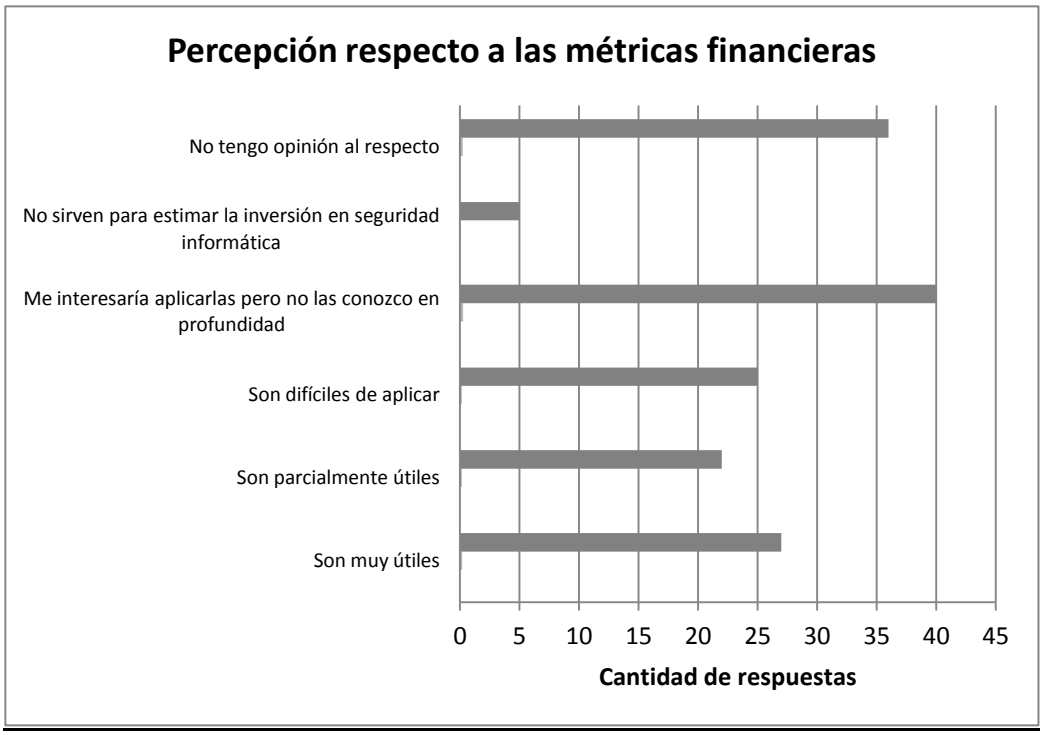
Las preguntas correspondientes a esta sección se orientaron a relevar la opinión de los participantes respecto a las metodologías de medición económica de la seguridad de la información, tales como ROSI, NPV, etc. y a determinar si se estaban utilizando y en ese caso, con qué resultados.

Percepción sobre herramientas de medición económica de la seguridad de la información

Ante la pregunta de cuál era la percepción sobre las herramientas, la cantidad más significativa de encuestados (25.8%) indicó que le interesaría utilizarlos pero que no las conocían mientras que una cantidad similar (23,4%) manifestó no tener opinión al respecto. Tomando estos dos grupos de respuestas puede concluirse que aproximadamente un 50% no conoce cómo utilizar estas herramientas. El resto de los participantes se divide prácticamente en partes iguales entre quienes las consideran muy útiles (17,5%), parcialmente útiles (14,3%) y difíciles de aplicar (15,6%).

Valorización	**Porcentaje**	**Total**
Son muy útiles	17,4%	27
Son parcialmente útiles	14,2%	22
Son difíciles de aplicar	16,1%	25
Me interesaría aplicarlas pero no las conozco en profundidad	25,8%	40
No sirven para estimar la inversión en seguridad de la información	3,2%	5
No tengo opinión al respecto	23,2%	36
	Total respuestas	**155**

Tabla 11: Percepción de los especialistas sobre las herramientas más conocidas de medición de la seguridad de la información.



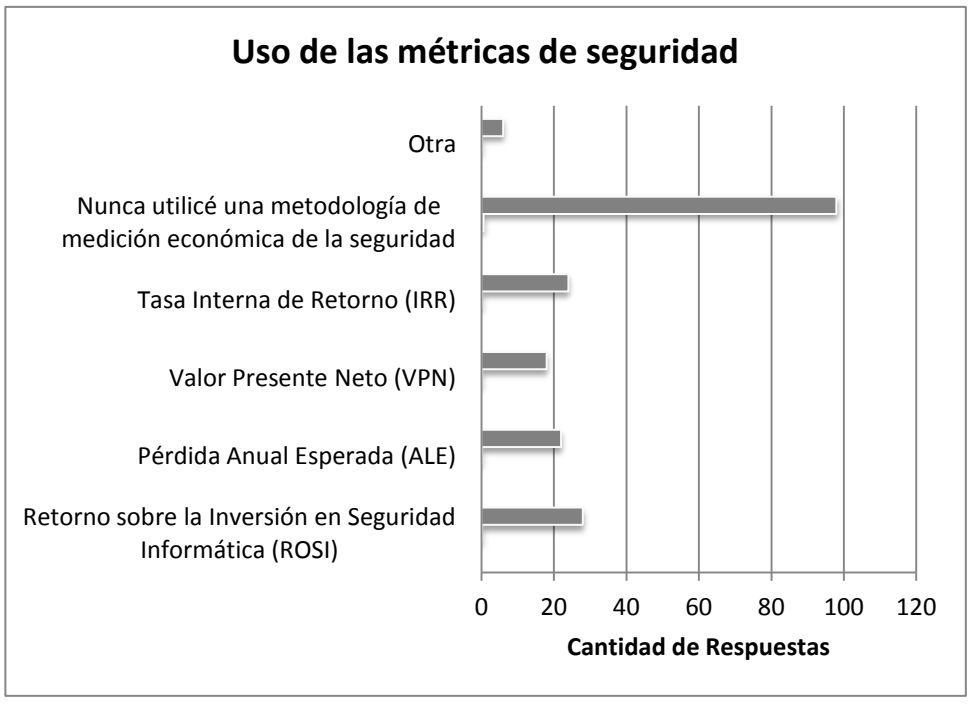
Cuadro 11: Percepción de los especialistas sobre las herramientas más conocidas de medición de la seguridad de la información.

Nivel de utilización de las herramientas de medición económica

Esta pregunta se enfocó a determinar si efectivamente se había utilizado una herramienta de medición económica de la seguridad. Del total de respuestas, un 63% manifestó no haber utilizado nunca una herramienta de esta naturaleza. Del resto, la más utilizada es ROSI, seguida de IRR y ALE.

¿Ha utilizado alguna o varias de las siguientes herramientas para estimar el presupuesto o la inversión en seguridad de la información? (puede señalar más de una)		
Métrica	**Porcentaje**	**Total**
Retorno sobre la Inversión en Seguridad de la información (ROSI)	18,1%	28
Pérdida Anual Esperada (ALE)	14,2%	22
Valor Presente Neto (VPN)	11,6%	18
Tasa Interna de Retorno (IRR)	15,5%	24
Nunca utilicé una metodología de medición económica de la seguridad	63,2%	98
Otra	3,9%	6
	Total Respuestas	**155**

Tabla 12 A: Nivel de utilización de las herramientas más conocidas de medición de la seguridad de la información.



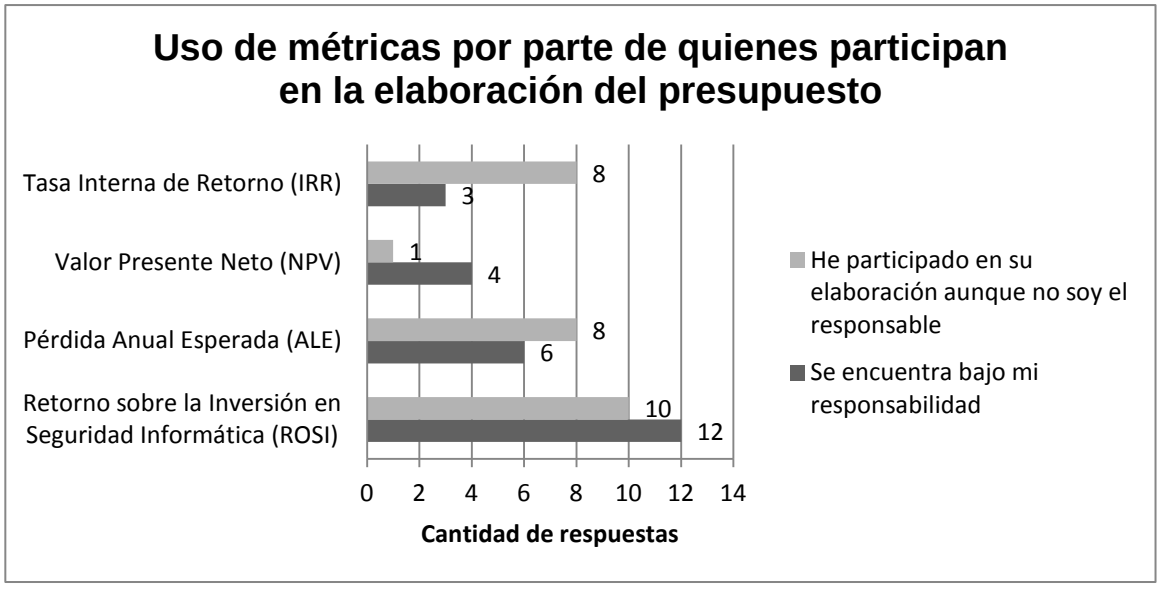
Cuadro 12 A: Nivel de utilización de las herramientas más conocidas de medición de la seguridad de la información.

En esta pregunta en particular, se buscó identificar cuáles eran las métricas más utilizadas por quienes participaban en la elaboración del presupuesto, ya sea porque se encontraba bajo su responsabilidad o simplemente porque colaboraba en esta tarea.

Se observó que la más utilizada es ROSI (42,3%), seguida de ALE (26,9%), IRR (21,2%) y NPV (9,6%). Estas observaciones se exponen en la tabla y el cuadro que siguen.

	Participación en la elaboración del presupuesto			
Uso de métricas	**Se encuentra bajo mi responsabilidad**	**He participado pero no soy el responsable**	**Porcentaje**	**Cantidad de respuestas**
Retorno sobre la Inversión en Seguridad Informática (ROSI)	12	10	42,3%	22
Pérdida Anual Esperada (ALE)	6	8	26,9%	14
Valor Presente Neto (NPV)	4	1	9,6%	5
Tasa Interna de Retorno (IRR)	3	8	21,2%	11
			Total respuestas	52

Tabla 12 B: Uso de métricas por parte de quienes participan en el proceso de elaboración del presupuesto.



Cuadro 12 B: Nivel de utilización de las métricas entre quienes participan en la elaboración del presupuesto.

Para esta pregunta, también se buscó identificar cuáles eran los ítems más seleccionados por quienes usaban o no métricas de seguridad. Los resultados obtenidos se muestran en el cuadro siguiente. En su análisis se debe tener en cuenta que la pregunta original ofrecía tres opciones de selección, de acuerdo a la importancia asignada.

	Utiliza métricas de seguridad		No utiliza métricas de seguridad	
Items del presupuesto	**Porcentaje**	**Cantidad de respuestas**	**Porcentaje**	**Cantidad de respuestas**
Evaluación y tratamiento de riesgos	11,1%	5	19,5%	8
Generación del marco normativo de seguridad	22,2%	10	12,2%	5
Organización de la seguridad	4,4%	2	9,8%	4
Gestión de activos (inventario y clasificación)	2,2%	1	4,9%	2
Seguridad de los Recursos Humanos	4,4%	2	0,0%	0
Protección física y ambiental	6,7%	3	14,6%	6
Seguridad de las comunicaciones	24,4%	11	26,8%	11
Seguridad de las operaciones	13,3%	6	12,2%	5
Control de accesos	22,2%	10	26,8%	11
Adquisición, mantenimiento y desarrollo de softw de seguridad	17,8%	8	22,0%	9
Adquisición y mantenimiento de hardware de seguridad	31,1%	14	19,5%	8
Atención y respuesta a incidentes de seguridad	24,4%	11	7,3%	3
Plan de Contingencias para la continuidad de las operaciones	6,7%	3	19,5%	8
Cumplimiento del marco normativo interno	2,2%	1	0,0%	0
Cumplimiento de la legislación y de los contratos con terceros	6,7%	3	9,8%	4
Capacitación y concientiz. en SI del personal de TI y usuarios	15,6%	7	17,1%	7
Protección de datos críticos	24,4%	11	14,6%	6
Sueldos del personal de seguridad	11,1%	5	9,8%	4
Auditorías y/o revisiones de seguridad	11,1%	5	9,8%	4
Monitoreo de seguridad	11,1%	5	14,6%	6
Protección de la red interna	17,8%	8	9,8%	4
Seguridad en las aplicaciones	8,9%	4	19,5%	8
Total respuestas		**45**		**41**

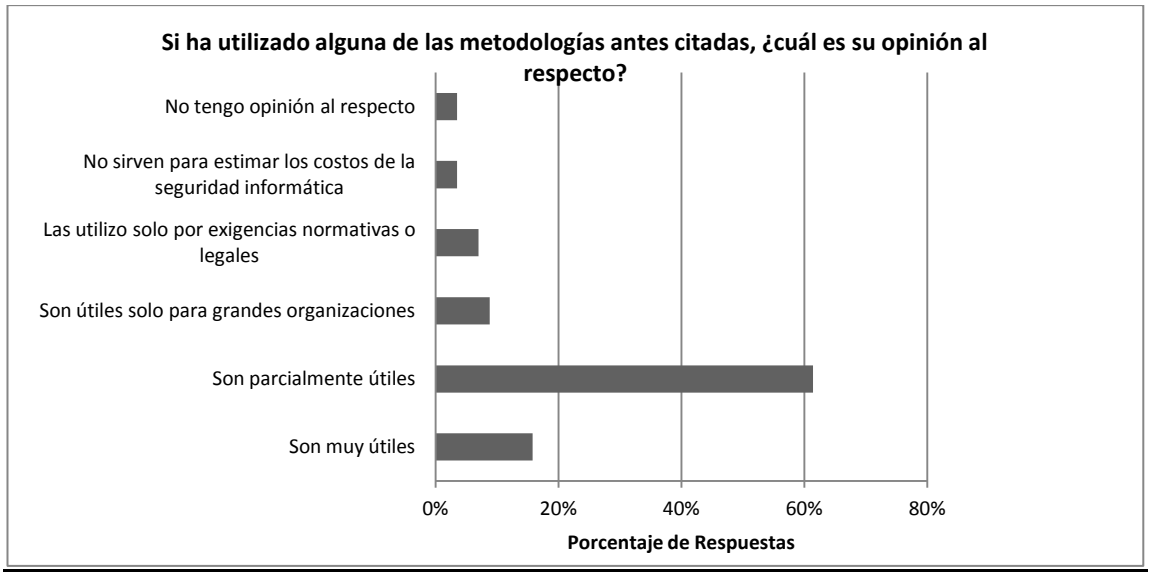
Cuadro 12 C: Selección de ítems del presupuesto según su importancia, elegidas por quienes usan métricas y por quienes no las utilizan.

Percepción sobre las herramientas de valorización en base a su uso

En este caso, se presentó esta pregunta solo a quienes en la pregunta anterior habían respondido que habían utilizado algunas de las metodologías, es decir a 57 participantes, tomando como base el cuadro correspondiente a la sección anterior. De este total una amplia mayoría (61,4%) las encontró parcialmente útiles, una 7 % las empleó solo por exigencias legales, casi un 9% las juzgó útiles solo para grandes organizaciones y 15% las encontró útiles. Solo un 3.5% manifestó que no servían y otro tanto indicó no tener opinión al respecto.

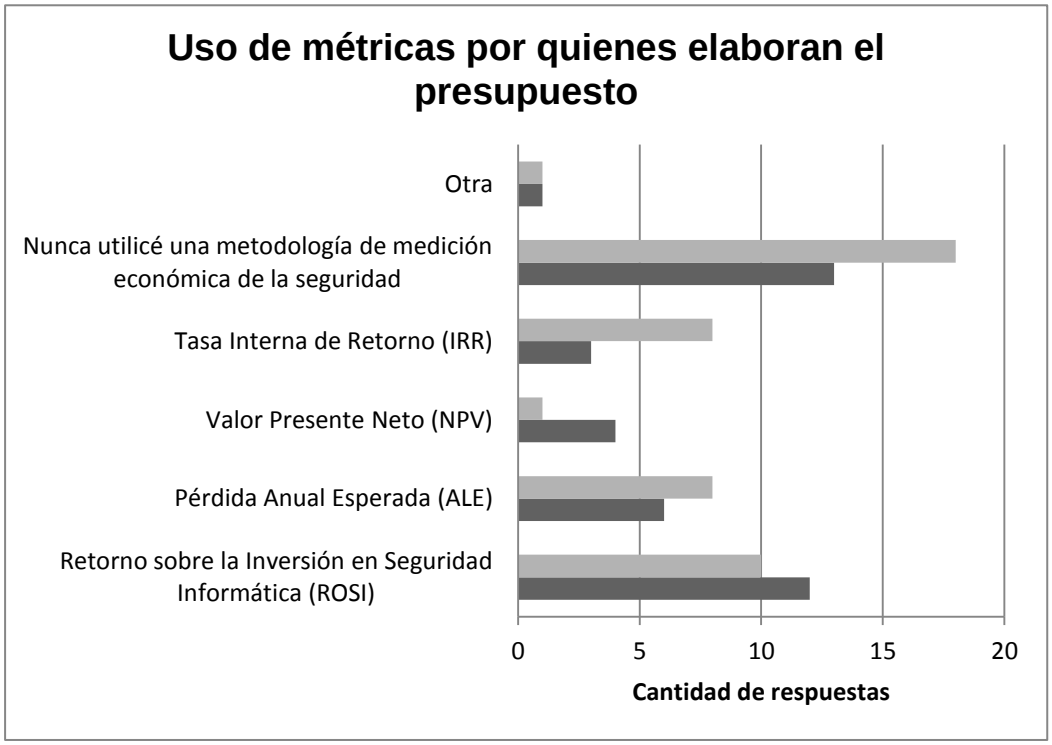
Percepción sobre las metodologías	**Porcentaje**	**Total**
Son muy útiles	15,8%	9
Son parcialmente útiles	61,4%	35
Son útiles solo para grandes organizaciones	8,8%	5
Las utilizo solo por exigencias normativas o legales	7,0%	4
No sirven para estimar los costos de la seguridad de la información	3,5%	2
No tengo opinión al respecto	3,5%	2
	Respuestas Totales	**57**

Tabla 13: Opinión respecto a las metodologías de medición de la seguridad de la información.



Cuadro 13: Opinión respecto a las metodologías de medición de la seguridad de la información.

Si se toman del cuadro 7, referido a la participación en la elaboración del presupuesto en seguridad de la información, aquellos participantes que manifestaron tenerlo bajo su responsabilidad o haber participado en su elaboración, se obtienen los resultados que se presentan en el siguiente cuadro. Puede observarse que una amplia mayoría percibe estas herramientas como parcialmente útiles o bien aplicables solo a grandes organizaciones. Solo un 19% de quienes tienen a su cargo el presupuesto y un 27% de quienes participan en su generación las consideraron útiles.



Cuadro 13: Opinión respecto a las metodologías de medición de la seguridad de la información, filtrado por aquellos que han participado en su elaboración o que lo tienen bajo su responsabilidad.

Sección E: Beneficios de la seguridad de la información

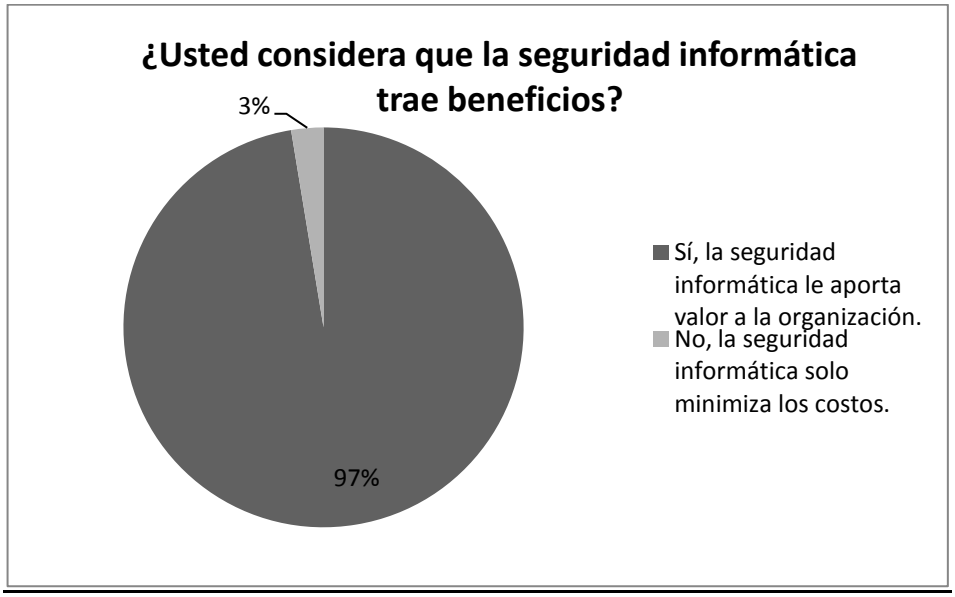
Estas dos últimas preguntas buscaron determinar si la seguridad era entendida en términos de beneficios para la organización o solo como un costo y las características de esta percepción.

Percepción sobre la Seguridad de la información como beneficio para la organización

Como puede observarse, una amplia mayoría opinó que la seguridad de la información trae beneficios a la organización.

Respuestas	Porcentaje	Total
Sí, la seguridad de la información le aporta valor a la organización.	97,4%	151
No, la seguridad de la información solo minimiza los costos.	2,6%	4
	Respuestas Totales	**155**

Tabla 14: Percepción de los encuestados respecto a la seguridad de la información como fuente de Beneficios para la organización.



Cuadro 14: Percepción de los encuestados respecto a la seguridad de la información como fuente de Beneficios para la organización.

Mayores beneficios asociados a la seguridad de la información

Esta pregunta se presentó solo a aquellos que en la anterior habían reconocido que la seguridad podía ser expresada en términos de beneficios. La consulta en este caso requirió la señalización de tres beneficios de la seguridad de la información, categorizados según su nivel de importancia. Llama la atención que más de la mitad de las respuestas totales la interpreta como un ahorro de costos y una manera de evitar pérdidas. Sigue en el nivel de respuestas, la mayor calidad que aporta a los productos y servicios, siendo este un atributo que permitiría, a diferencia del anterior, expresar la seguridad en términos de beneficios. En tercer y cuarto puesto, aparecen una mejor imagen en clientes y proveedores y una mayor confianza de los usuarios al utilizar los sistemas, respuestas ambas que también, parecen catalogar a la seguridad como portadora de beneficios y no como un mero depresor de pérdidas.

Si ha respondido afirmativamente la pregunta anterior, señale los tres mayores beneficios que la seguridad de la información le aporta a su organización.				
Beneficios	**Mayor beneficio**	**Segundo mayor beneficio**	**Tercer mayor beneficio**	**Total**
Ahorros al evitar pérdidas de información o de recursos	49	31	15	95
Mayor calidad de los productos o servicios	36	19	15	70
Mayor confianza de los usuarios al utilizar los sistemas	15	18	24	57
Mejor imagen en clientes y proveedores	12	21	20	53
Mejor imagen ante la opinión pública	13	11	15	39
Menor exposición a litigios/sanciones de organismos de contralor	3	15	17	35
Mayor eficacia en el logro de los objetivos	10	13	12	35
Procesos eficientes de toma de decisiones	6	13	9	28
Informes satisfactorios de los auditores	0	5	9	14
Mayores ganancias	6	1	4	11
Reconocimiento de la corporación/sede central	1	1	6	8
Mejores condiciones de trabajo para los empleados	0	2	4	6
Menor costo de seguros	0	1	1	2
		Respuestas Totales		**151**

Cuadro 15: La seguridad de la información como beneficio para la organización

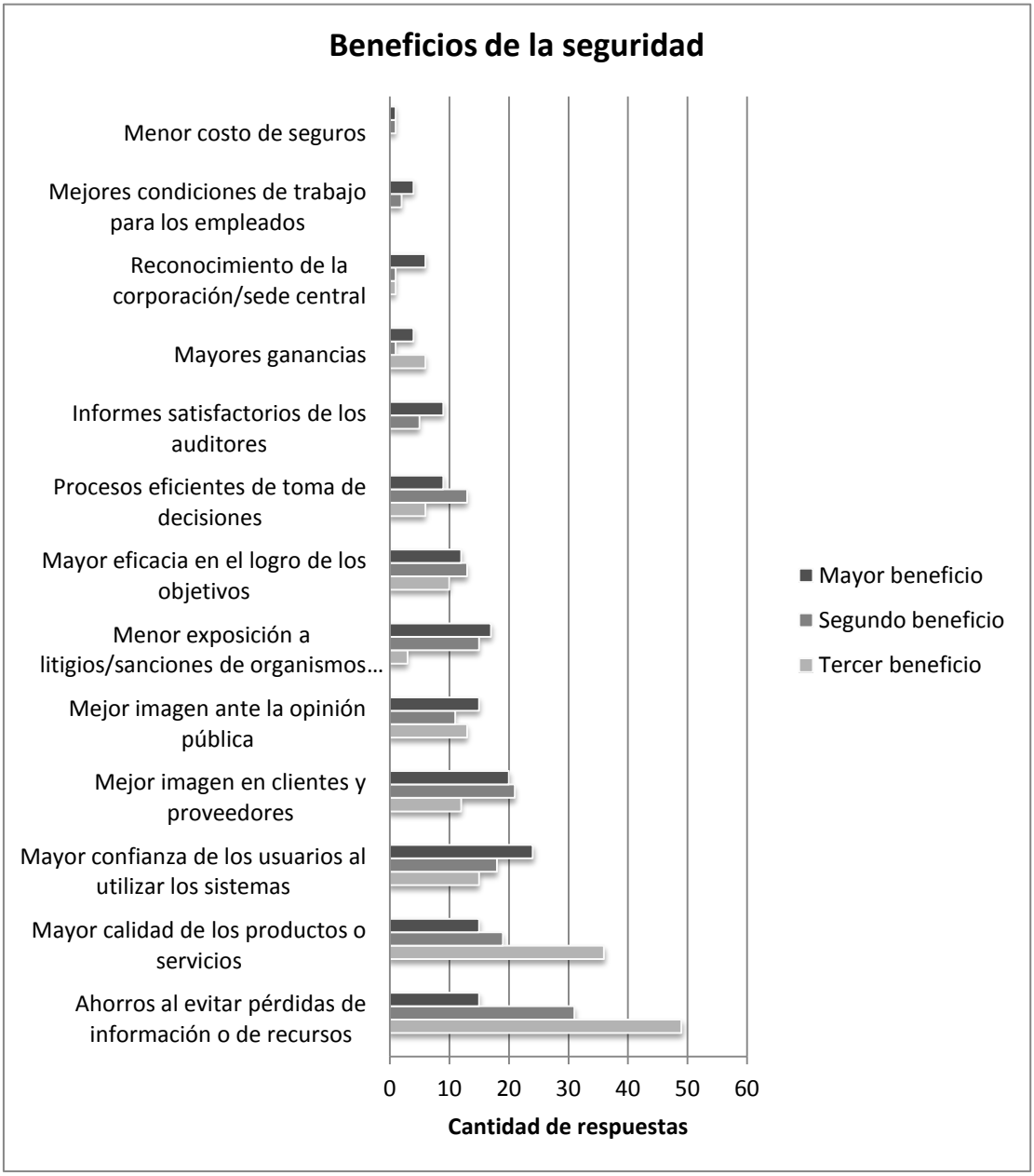


Tabla 15: El gráfico muestra los principales beneficios que los especialistas asignan a la seguridad de la información, categorizados en función de su importancia teniendo en cuanta las tres alternativas de respuesta (mayor beneficio, segundo mayor beneficio y tercer mayor beneficio).

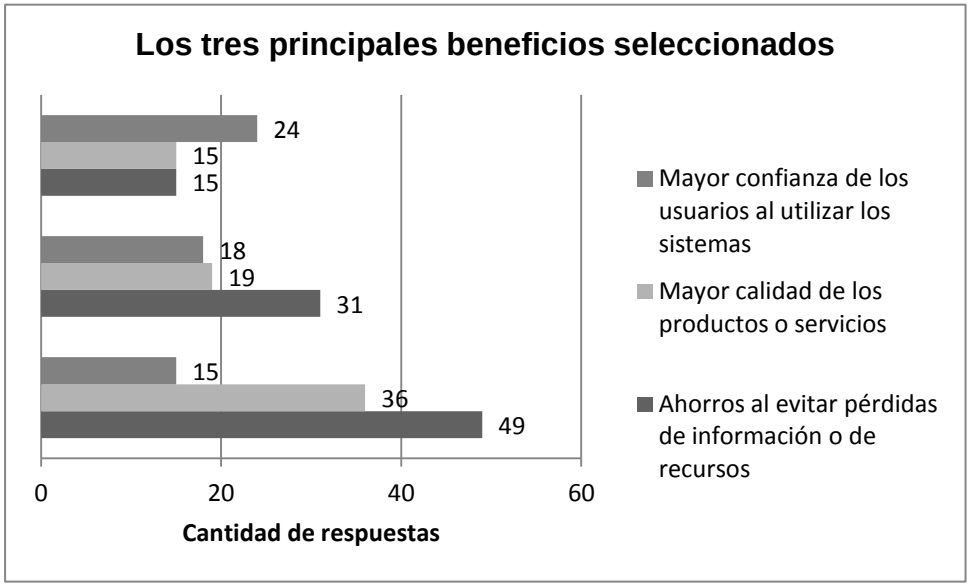


Tabla 15 - 1: El gráfico muestra los 3 principales beneficios que los especialistas asignan a la SI, categorizados por la importancia que le asignaron. Cada barra muestra la cantidad de respuestas obtenidas.

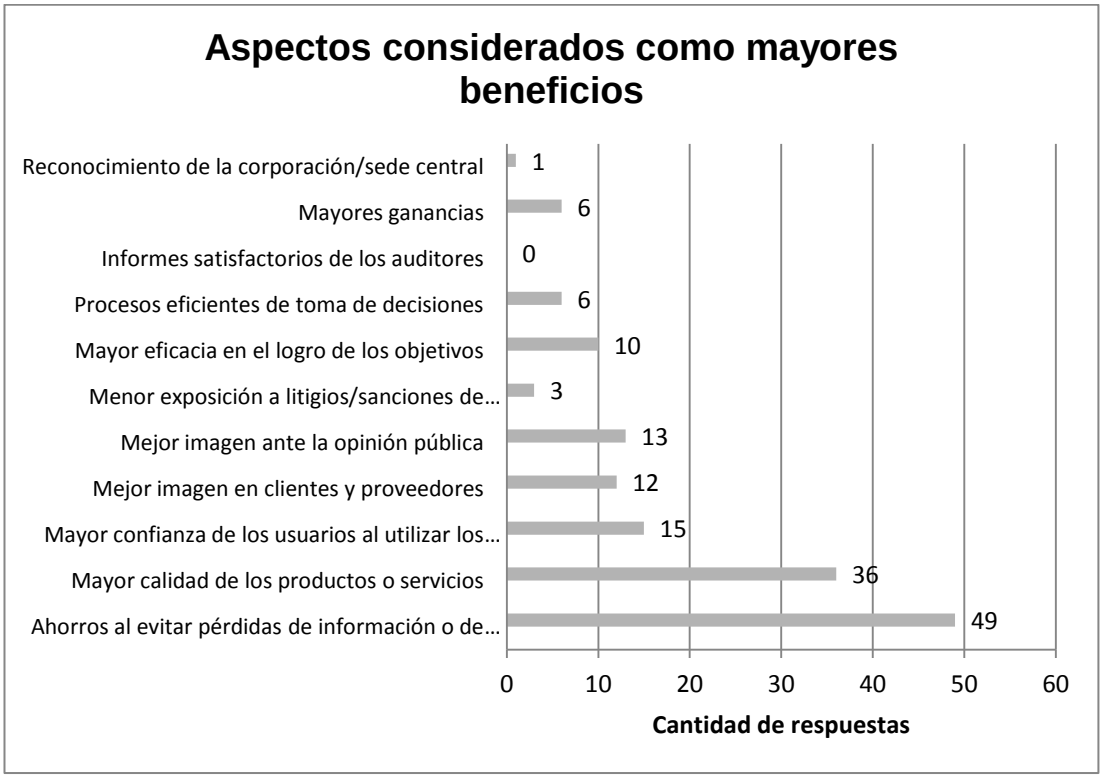


Tabla 15 - 2: El gráfico muestra los aspectos a los que los especialistas asignan a la mayor prioridad al considerarlos como beneficios de la seguridad de la información. El eje horizontal muestra la cantidad de respuestas.

ANEXO II

Caso práctico de uso de métricas

El siguiente caso es una adaptación del artículo de Bojanc y Jeman-Blazic [4].

Usted trabaja en la Gerencia de Seguridad de una importante empresa que aprovecha en forma intensiva las TI. Luego de haber realizado un proceso intensivo de evaluación de riesgos y presentado el informe a la Gerencia General, ésta ha aceptado la recomendación de disminuir la cota superior del nivel aceptable de riesgo a un 10%. Esto representa una reducción significativa de riesgo para la organización.

La situación es la siguiente:

- La empresa cuenta con un parque informático de 500 computadoras
- Una potencial falla de seguridad representaría hoy una pérdida anual estimada en un millón de pesos
- El sistema de controles de seguridad implementado actualmente le permite reducir el riesgo en un 80%
- La inversión para disminuir el nivel de riesgo debe realizarse en 4 años, luego de lo cual el estado de la seguridad será evaluado nuevamente
- La tasa de interés es del 5% anual

El Gerente de Seguridad propone tres alternativas para alcanzar el objetivo de reducir el riesgo a un 10% como máximo:

- Solución 1 – Bajo costo (BC): consiste en una renovación parcial del equipamiento y un reemplazo de algunos de los aplicativos. Reduce el riesgo total producto de posibles fallas de seguridad a un 10%, justo en el límite fijado como objetivo. El precio de adquisición de esta solución es de $60.000 y el costo estimado de mantenimiento anual, vinculado a actualizaciones y monitoreo, es de $20.000

- Solución 2 - Profesional (PR): virtualiza parte de los dispositivos de red y los puestos de trabajo de los usuarios comunes. Reduce la probabilidad de una falla de seguridad al 1%, siendo el valor de incorporación de la solución de $100.000 y el costo de renovación anual de $30.000, mientras que los costos de mantenimiento son de $5.000 por cada uno de los cuatro años subsiguientes.
- Solución 3 – Outsourcing (OU): la empresa que provee los servicios de tercerización asegura que el riesgo no superará el 7%. El cargo inicial es de $150.000, seguido de un costo anual de $25.000, por el mantenimiento y soporte técnico.

El Gerente de Seguridad se propone señalar las ventajas y desventajas de cada una de las soluciones propuestas y le encarga que provea la información necesaria para justificar la conveniencia de seleccionar una solución, desde la perspectiva financiera. Calcule los siguientes indicadores para facilitar la toma de decisiones:

1. TCO – Costo total de Propiedad
2. TBO – Beneficio total de la Propiedad
3. ALE – Pérdida Anual Esperada
4. ROSI – Retorno sobre la inversión en Seguridad Informática
5. NPV – Valor Presente Neto
6. IRR – Tasa Interna de Retorno

Tabla I – Beneficios y Cálculos para cada una de las alternativas

Año	Tasa	Alternativa Bajo Costo			Alternativa Virtualización			Alternativa Outsourcing		
		Beneficios	Compra y Actualizac	Mantenimiento	Beneficios	Compra y Actualizac	Mantenimiento	Beneficios	Compra y Actualizac	Mantenimiento
0	0,05		60.000			100.000			150.000	
1	0,05	100.000		20.000	190.000	30.000	40.000	130.000	25.000	
2	0,05	100.000		20.000	190.000	30.000	5.000	130.000	25.000	
3	0,05	100.000		20.000	190.000	30.000	5.000	130.000	25.000	
4	0,05	100.000		20.000	190.000	30.000	5.000	130.000	25.000	

Solución:

Cálculo del TCO

- TCO(BC) = $140.000
- TCO(VI) = $275.000
- TCO(OU) = $250.000

Cálculo del TBO (considerando un período de 4 años)

- TBO(BC) = $400.000
- TBO(VI) = $670.000
- TBO(OU) = $520.000

Cálculo de ALE (considerando una frecuencia de una ocurrencia al año)

- ALE(BC) = $100.000
- ALE(VI) = $10.000
- ALE(OU) = $70.000

Cálculo del Beneficios en términos de reducción de la pérdida anual esperada (ALE):

- Beneficios(BC) = 1.000.000 x (90 - 80) / 100 = $100.000
- Beneficios(VI) = 1.000.000 x (99 - 80) / 100 = $190.000
- Beneficios(OU) = 1.000.000 x (93 - 80) / 100 = $130.000

Cálculo de ROI:

$$\text{ROI} = \frac{\text{Beneficio} - \text{Costo de la Inversión}}{\text{Costo de la Inversión}} \times 100$$

1. Solución 1: Bajo Costo

$$\mathrm{ROI_{BC}} = \frac{400.000 - 140.000}{140.000} \times 100 = 186\%$$

2. Solución 2: Virtualización

$$\mathrm{ROI_{VI}} = \frac{760.000 - 275.000}{275.000} \times 100 = 176\%$$

3. Solución 3: Outsourcing

$$\mathrm{ROI_{OU}} = \frac{520.000 - 250.000}{250.000} \times 100 = 108\%$$

Cálculo del NPV:

$$\mathrm{NPV} = \sum_{t=0}^{n} \frac{B_t - C_t}{(1+i)^t}$$

1. Solución 1: Bajo Costo

$$\mathrm{NPV_{BC}} = 76.190 + 72.562 + 69.107 + 65.816 - 60.000 = \$223.675$$

2. Solución 2: Virtualización

$$\mathrm{NPV_{VI}} = 114.285 + 140.589 + 133.894 + 127.519 - 100.000 = \$416.286$$

3. Solución 3: Ourtsourcing

$$\mathrm{NPV_{OU}} = 100.000 + 95.238 + 90.702 + 86.383 - 150.000 = \$222.323$$

Cálculo del IRR:

$$\mathrm{NPV} = \sum_{t=0}^{n} \frac{B_t - C_t}{(1+i)^t} = 0$$

1. Solución 1: Bajo Costo
   Para IRR_{BC}

$$0 = -60.000 + \frac{80.000}{1 + \text{IRR}} + \frac{80.000}{(1 + \text{IRR})^2} + \frac{80.000}{(1 + \text{IRR})^3} + \frac{80.000}{(1 + \text{IRR})^4}$$

$$\text{IRR}_{\text{BC}} = 128\%$$

2. Solución 2: Virtualización
   Para IRR_{VI}

$$0 = -100.000 + \frac{120.000}{1 + \text{IRR}} + \frac{155.000}{(1 + \text{IRR})^2} + \frac{155.000}{(1 + \text{IRR})^3} + \frac{155.000}{(1 + \text{IRR})^4}$$

$$\text{IRR}_{\text{VI}} = 130\%$$

3. Solución 3: Ourtsourcing
   Para IRR_{OU}

$$0 = -150.000 + \frac{105.000}{1 + \text{IRR}} + \frac{105.000}{(1 + \text{IRR})^2} + \frac{105.000}{(1 + \text{IRR})^3} + \frac{105.000}{(1 + \text{IRR})^4}$$

$$\text{IRR}_{\text{OU}} = 59\%$$

BIBLIOGRAFÍA

[1] Anderson, R. “Why Information Security is Hard – An Economic Perspective”. Proceedings of the 17th Annual Computer Security Applications Conference, 2001. Disponible en: http://www.cl.cam.ac.uk/~rja14/Papers/econ.pdf. (Consultada el 20 de junio de 2010).

[2] Anthony, J., W. Choi & S. Grabski. “Market Reaction to E-Commerce Impairments and Web-site Outages”. International Journal of Accounting Information Systems 7, (2): 60-78, 2006. Disponible en: http://accounting.uwaterloo.ca/uwcisa/symposiums/symposium_2005/Grabski%20et%20al.pdf. (Consultada el 24 de noviembre de 2011).

[3] Böhme, Rainer y Nowey, Thomas. “Economic Security Metrics”. Capítulo del libro “Dependebility Metrics”. LNCS 4909, Berlin Hilderberg, Springer Verla, pp 176-187, 2008. Disponible en: http://www1.inf.tu-dresden.de/~rb21/publications/BN2008_Economic_Security_Metrics.pdf. (Consultada el 2 de septiembre de 2011).

[4] Bojanc, Rok and Jerman-Blazic, Borka. “An economic modelling approach to information security risk management”. Faculty of Economics, Ljubljana University and Josef Stefan Institute, Slovenia. International Journal of Information Management 28 (2008) 413-422.

[5] Butler, Shawn A. “Security Attribute Evaluation Method”. PhD. Thesis. Carnegie Mellon University, 2003. Disponible en: http://www.cs.cmu.edu/~shawnb/SAEM-ICSE2002.pdf. (Consultada el 20 de junio de 2010).

[6] Cardholm, Lucas. “Adding value to business performance through cost benefit analyses of information security investments” – Tesis de Maestría de la Universidad de Gävle, Departamento de Business Administration. 2006. Disponible en: http://hig.diva-portal.org/smash/record.jsf?pid=diva2:119787. (Consultada el 22 de septiembre de 2011).

[7] Cavusoglu, Huseyin; Mishra, Birendra and Raghunathan Srinivasan. “A Model for Evaluating IT Security Investments”. Communications of the ACM, vol. 47, Nro. 7. 2004. Disponible en: http://utd.edu/~huseyin/paper/investment.pdf. (Consultada el 20 de junio de 2010).

[8] COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT – ISACA, 2012.

[9] Ettredge, Michael y Richardson, Vernon. “Assessing the Risk in E-Commerce”. University of Kansas - Proceedings of the 35th Hawaii International Conference on System Sciences – 2002 – Disponible en: http://www.hicss.hawaii.edu/HICSS_35/HICSSpapers/PDFdocuments/INISC03.pdf. (Consultada el 3 de noviembre de 2011).

[10] Fowler Newton, Enrique. “Cuestiones Contables Fundamentales” – La Ley – 4ta. Edición, 2005.

[11] Gordon, L.A. and Loeb, M.P. “The Economics of Information Security Investment”. ACM Transactions on Information and System Security, vol. 5 (4), 2002. Disponible en: http://delivery.acm.org/10.1145/590000/581274/p438-a_gordon.pdf?key1=581274&key2=8342318511&coll=&dl=acm&CFID=15151515&CFTOKEN=6184618. (Consultada el 20 de junio de 2010).
[12] Gordon, Lawrence A. and Loeb, Martin P. “Budgeting Process for Information Security Expenditures”. Communication of the ACM. Vol. 49, N° 1, enero de 2006. Disponible en: http://iris.nyit.edu/~kkhoo/Spring2008/Topics/Topic10/BudgetingInfoSecExpenditure_CACM2006.pdf. (Consultada el 10 de junio de 2011).
[13] Grossklags, Jens; Christin, Nicolas and Chuang, John. “Secure of insecure? A game-theoretic analysis of information security games”. 17th International World Wide Web Conference (WWW2008). Internet Monetization track, Beijing, China. 2008. Disponible en: http://www.andrew.cmu.edu/user/nicolasc/publications/GCC-WWW08.pdf. (Consultada el 20 de junio de 2010).
[14] Grossklags, Jens, Johnson, Benjamin and Christin, Nicolas. “When Information Improves Information Security (Extended version)”. CyLab Carnegie Mellon University, Pittsburg, EEUU. Carnegie Mellon CyLab Technical Report, marzo de 2009. (Consultada el 17 de abril de 2009).
[15] Hovav, A, & J. D'Arcy - “The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms. Risk Management and Insurance Review” 6 (2): 97-121, 2003. Disponible en: http://biz.korea.ac.kr/~anat/RMIR_Hovav.pdf. (Consultada el 15 de octubre de 2011).
[16] ISO 27004:2005 - “Information technology -- Security techniques - Information security management – Measurement”. International Organization for Standarization – www.iso.org.
[17] Lucas, Kelly. “Economic Evaluation of a Company´s Information Security Expenditures”. 2005. Disponible en http://www.infosecwriters.com/text_resources/pdf/Economic_Evaluation.pdf. (Consultada el 30 de agosto de 2010).
[18] Mankiw, Gregory – “Principios de Economía” –– Segunda Edición – Editoral Mc Graw Hill, 2002.
[19] NIST Special Publication 800 – 65. “Integrating IT Security into the Capital Planning and Investment Control Process”. Enero 2005. Disponible en: http://csrc.nist.gov/publications/nistpubs/800-65/SP-800-65-Final.pdf. (Consultada el 25 de agosto de 2010).
[20] Risen, Tom. “Can insurers protect the US from cyber attacks”. National Journal. November 2010. Disponible en: http://www.nationaljournal.com/njonline/no_20100208_9513.php. (Consultada el 23 de abril de 2011).
[21] Rosenfeld, Shalom, Russ, Ioana and Cukier, Michel. “Modeling the “Tragedy of the Commons” Archetype in Enterprise Computer Security”. En: Journal of Information Assurance and Security 4, 2009.

Disponible en: http://www.softcomputing.net/jias/rosenfeld.pdf. (Consultada el 21 de junio de 2010).
[22] Ross, Steven J. “What is the Value of Security”. ISACA Journal, Volume 2, 4-5, 2011.
[23] Stanley, Morgan. “Economic Evaluation of a Company´s Information Security Expenditures”. Disponible en: http://www.infosecwriters.com/text_resources/pdf/Economic_Evaluation.pdf, 2005. (Consultada el 26 de mayo de 2011).
[24] Somerson, I. “Information: What it costs when it´s lost”. Security Management 38 – pag. 61-65. 1994.
[25] Sonnenreich, Wes, “Return On Security Investment (ROSI): A Practical Quantitative Model”. SageSecure Research. Disponible en: http://www.infosecwriters.com/text_resources/pdf/ROSI-Practical_Model.pdf, 2002. (Consultada el 1 de julio de 2010).
[26] The Register - http://www.theregister.co.uk/. (Consultada el 20 de noviembre de 2010).
[27] Xiaomeng Su. “An overview of Economic Approaches to Information Security Management”. Techincal Report TR-CTIT-06-30. University of Twente, 2006. Disponible en: http://www.notablesoftware.com/Papers/SecCost.html. (Consultada el 20 de junio de 2010).
[28] Wood, Charles Cresson and Parker, Donn B. “Why ROI and Similar Financial Tools Are Not Advisable For Evaluating The Merits Of Information Security Projects”. Computer, Fraud and Security, volume 2004, Issue 5, 2004.
[29] Wouter de Buijn, Marco R. Spruit and Maurits van den Heuvel. “Identifying the Cost of Security”. Journal of Information Assurance and Security 5, 2010. Disponible en: http://74.125.155.132/scholar?q=cache:ltLwotI4naUJ:scholar.google.com/+Identifying+the+Cost+of+Security&hl=es&as_sdt=2000. (Consultada el 20 de junio de 2010).