Ing. Carlos Ormella Meyer y Asoc.
Gestión y Auditoría de Riesgos y Seguridad de la Información
Tel: +54-11-4371-4638 – Cel: +54-911-6513-2751
E-mail: ciprio@ingcomyasoc.com.ar

MÉTRICAS DE SEGURIDAD DE LA INFORMACION Y GESTION DEL DESEMPEÑO CON EL BALANCED SCORECARD

Hay dos temas en seguridad de la información que pese a su limitada difusión se proyectan a todas las áreas de protección de datos corporativos, adquiriendo así una trascendencia que es necesario considerar.

Uno de estos temas es el de la justificación de las inversiones en seguridad. El otro es cómo medir el desempeño de las medidas de seguridad y realizar la gestión correspondiente en la búsqueda de mejores resultados.

El primer tema hace ya varios años que ha sido analizado, dando origen al **ROSI** (ver recuadro **ROSI**) como aplicación en seguridad de la información del indicador financiero **ROI**, es decir, el *Retorno Sobre la Inversión*.

Diferente ha sido hasta hace poco tratar con la segunda cuestión planteada antes. Desde hace un tiempo lo más completo han sido las métricas del **NIST** [1], aunque con un mayor enfoque en lo técnico. Nosotros hemos venido trabajando con el mapeo de los controles NIST a los controles de las normas ISO [2] para determinar así las métricas NIST adecuadas, además de agregar algunas otras que resultan del análisis del texto de los propios controles de seguridad ISO 27002 con apoyo de la aproximación **GQM** (*Métricas por Cuestionarios de Metas*).

Adicionalmente también corresponde verificar la efectividad de los planes de concientización en cuanto por ejemplo a diferentes políticas sobre las que se ha trabajado. El cumplimiento de tales *políticas* por parte de las personas se puede verificar según diferentes *criterios*.

Como habrá un cierto número de políticas con diferente importancia o prioridad (con lo cual la suma de tales prioridades se iguala a uno), la situación puede analizarse recurriendo a la **Función de Valor** como método más empleado del **MCDA** (*Análisis de Decisiones con Múltiples Criterios*). También los criterios con que se consideren las políticas tendrán su importancia relativa o prioridad entre ellos, de modo que también se puede aplicar la Función de Valor correspondiente.

ROSI

El ***Retorno Sobre la Inversión en Seguridad*** trabaja con el mecanismo **ALE**, es decir la *Expectativa de Pérdidas Anualizadas*, basado en el *impacto* de cada incidente de seguridad y su *probabilidad de ocurrencia* a lo largo de un año.

Este mecanismo funciona adecuadamente cuando se disponen de suficientes datos históricos de dichos incidentes. Ante la ausencia de datos históricos propios, se puede recurrir a fuentes externas aunque, generalmente no son completas y pueden estar referidas a ambientes de negocios diferentes al que se analiza.

Además, tampoco es seguro que lo ocurrido se repita de la misma manera, ya que hay incidentes que declinan en su aparición por la acción de salvaguardas o de las propias amenazas, así como incidentes nuevos que antes no aparecían.

En este escenario de incertidumbre se puede usar la aproximación de Bayes que combina los datos históricos que se dispongan con datos cualitativos surgidos de las opiniones del personal clave involucrado. O mejor aún, aplicar la *simulación Monte Carlo* a partir de distribuciones estadísticas adecuadas, lo que permite acotar resultados como para volverlos más aceptables, incluso las inversiones correspondientes, por parte de los gerentes administrativos y otros ejecutivos que por sus actividades conocen las aplicaciones del ROI.

Para la aplicación de la Función de Valor veamos el caso del análisis de las diferentes políticas en cuanto a su conformidad con cada uno de los criterios establecidos.

En primer lugar la Función de Valor para una política cualquiera respecto de cierto criterio estará dada por el Nivel de Cumplimiento verificado de la misma (en valores porcentuales) para el criterio en cuestión y el factor de importancia/prioridad o Peso relativo (de 0 a 1) del mismo criterio.

A su vez, la Función de Valor particular para *una política* respecto de *todos los criterios* es la sumatoria de los resultados obtenidos para cada uno de los criterios del producto del Nivel de Cumplimiento verificado de dicha política respecto de un criterio en particular y el Peso relativo de dicho criterio.

Finalmente, la Función de Valor total para *todas las políticas* analizadas será igual a la sumatoria de la Función de Valor particular de cada una de las políticas por el Peso relativo (de 0 a 1) de la política considerada en cada caso.

Un análisis similar puede hacerse con los diferentes criterios simplemente permutando “política” por “criterio” y viceversa en los conceptos de los cuatro párrafos anteriores.

Para llevar adelante todo el proceso mencionado antes se requiere establecer las *políticas*, los *criterios* con que se analizarán el cumplimiento de las mismas, y los *pesos relativos* de cada una de las políticas y de cada uno de los criterios.

En primer lugar las *políticas* responden a los temas tratados en el plan de concientización, como por ejemplo nivel de atención a las políticas, manejo y gestión de contraseñas, uso de equipamiento móvil, manejo de documentación en papel, uso del email, reacción ante incidentes, etc.

Ahora bien, para establecer el nivel de cumplimiento de dichas *políticas* se puede recurrir a técnicas propias de la Psicología Social tales como cuestionarios cerrados de dos o tres respuestas posibles, enfocados por separado en *criterios* como el aporte a dicho cumplimiento en cuanto, por ejemplo, al ***conocimiento, actitud y comportamiento*** [3] del personal correspondiente.

Y finalmente, los *pesos relativos* de cada una de las políticas y de cada uno de los criterios se pueden establecer mediante la aplicación del ***AHP*** *(Proceso de Análisis Jerárquico*) incluyendo las comparaciones de a pares.

Más allá de todos los enfoques específicos mencionados, el panorama normativo se amplió con la aparición en diciembre de 2009 de la ISO 27004 de Métricas de Seguridad. Esta norma establece un marco de referencia para medir la *eficiencia* del SGSI y la *efectividad* de los controles de seguridad implementados conforme la ISO 27001, así como también un modelo de mediciones incluyendo las condiciones sobre qué medir y cómo, y que proporcione resultados adecuados para analizar y mejorar el tratamiento de los riesgos.

Sin embargo, hasta aquí no surge un mecanismo que pudiere servir como control y medio de gestión efectivo para las medidas de seguridad implementadas, y que incluso facilite la toma de decisiones para las mejoras correspondientes. En este caso, como con ROSI, se puede recurrir a una herramienta de otra área de negocios.

Se trata del **Balanced Scorecard (*BSC*)** o **Cuadro de Mando Integral (*CMI*)** que, si bien se presentó hace casi 20 años como una herramienta para medir el desempeño de procesos, hoy día tiene su principal aplicación en la implementación de los objetivos estratégicos de una empresa.

Esto último es importante para la seguridad porque permite una comunicación directa con las áreas de negocio de la empresa, con las ventajas que irán surgiendo en lo que sigue.

Para poder aplicar el BSC a la seguridad de la información es conveniente tener claro algunos conceptos básicos a nivel empresarial. Ellos son principalmente la *Misión, Visión, Estrategia, Objetivos Estratégicos y Activos*.

En forma resumida pero concreta estos conceptos implican lo siguiente:

- La **Misión** se enfoca en el presente de la empresa.
- La **Visión** expresa lo que la empresa aspira ser en el futuro, en general las metas que se quieren lograr.
- La **Estrategia** consiste en establecer **objetivos estratégicos** para lograr a partir de las condiciones definidas en la Misión, concretar las metas expresadas en la Visión.
- Los **Activos** son los bienes con que cuenta una empresa. Hay dos tipos de activos: *Financieros* e *Intangibles*.
  a) Los **Activos Financieros** son los únicos que tradicionalmente se han considerado, ya que expresan los valores físicos y contables con que cuenta una empresa.
  b) Los **Activos intangibles**, un moderno paradigma, incluyen los conocimientos, la información, la cultura corporativa, el liderazgo, y otros.

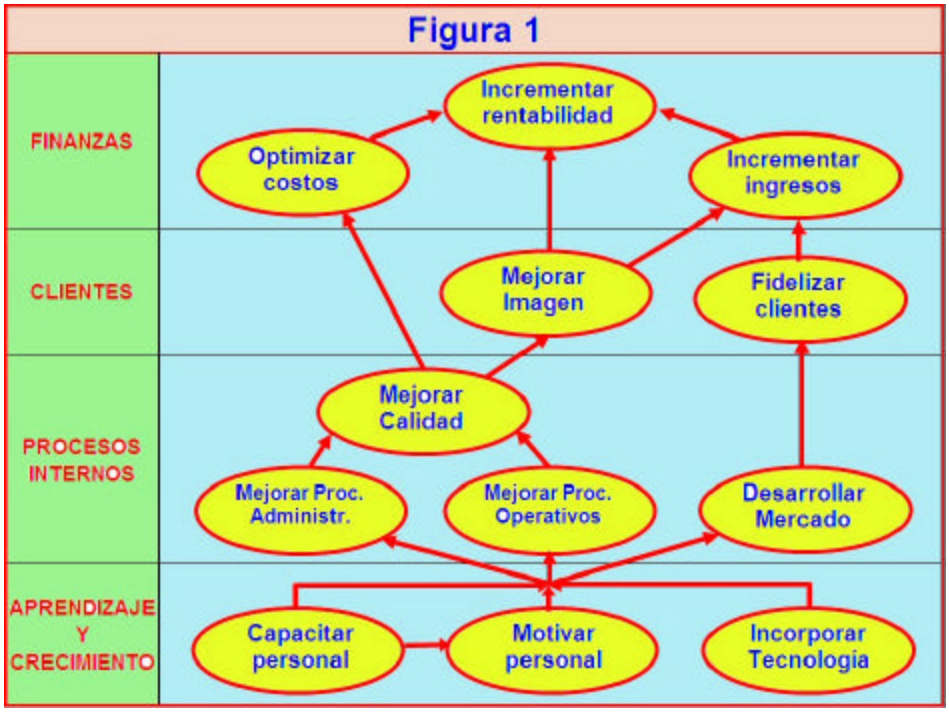
El BSC incorpora los Activos Intangibles además de los Activos Financieros, con lo cual adquiere una mucho mayor relevancia gracias a un enfoque integral de la problemática de una organización. A partir de estas bases el BSC traslada la Estrategia a la acción y monitorea su ejecución, facilitando la toma de decisiones para cumplir las metas y objetivos.

El enfoque del BSC se basa en **cuatro perspectivas: *Financiera, Clientes, Procesos Internos y Aprendizaje y Crecimiento***. Este último suele referírselo también como ***Investigación y Desarrollo***.

Breve pero concretamente tales perspectivas pueden describirse de la siguiente manera:
- **Financiera:** Punto de vista de los socios.
- **Clientes:** Punto de vista de los clientes.
- **Procesos Internos:** Se relaciona con la gestión de las operaciones en general.
- **Aprendizaje y Crecimiento:** Define cómo se aprende a crecer y soportar la estrategia por medio de sus procesos y a entregar la respuesta adecuada a los clientes.

El BSC tiene dos partes: ***Mapa Estratégico*** y ***Tablero de Comando*** que se aplican a las cuatro perspectivas.

El **Mapa Estratégico** (Figura 1) es la imagen gráfica que muestra la representación de la hipótesis en la que se basa la estrategia. Surge de los Objetivos Estratégicos determinados en la Estrategia y las cuatro perspectivas con que se enfocan los negocios.



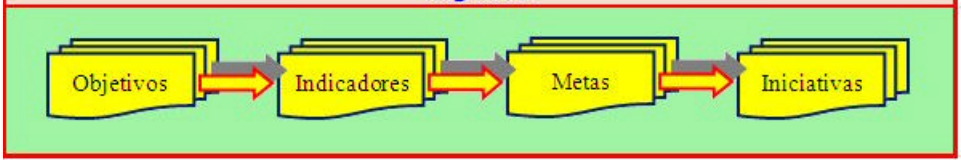
El resultado es una dependencia entre objetivos manifestada por una cadena de **relaciones *causa-efecto*** entre los mismos tanto en una misma como diferente perspectiva.

Estas relaciones son importantes porque de los resultados que se obtengan luego en el Tablero de Comando, puede surgir la necesidad de cambios o mejoras en

uno o más objetivos, lo que implica una toma de decisiones respecto de los objetivos de los cuales dependen.

Por su parte, el **Tablero de Comando** se forma con cuatro elementos (Figura 2): ***Objetivos, Indicadores, Metas e Iniciativas***.

Figura 2



Estos cuatro elementos se aplican a cada una de las cuatro perspectivas y en forma resumida pueden describirse así:

- **Objetivos:** Lo que se quiere conseguir. Generalmente de 3 a 5 por cada perspectiva.
- **Indicadores:** Parámetros para monitorear el progreso hacia el alcance de cada objetivo. Usualmente entre 1 y 5 por cada Objetivo. Es conveniente distinguir los conceptos de *indicadores, métricas y medidas*. Las **medidas** son las *mediciones* realizadas, las **métricas** son *relaciones entre medidas* y los **indicadores** son *evaluaciones de métricas*.
- **Metas (targets) o hitos:** Lo que se quiere ir logrando a lo largo del tiempo, y que se mide por medio de los indicadores.
- **Iniciativas:** Planes de acción o programas para lograr los objetivos y las metas correspondientes.

Hasta acá el análisis se refiere a lo puramente estratégico de una empresa. Ahora bien, las estrategias establecidas derivan siempre en procesos operacionales, de modo que los ***Objetivos Estratégicos*** determinan ***Objetivos Operacionales*** que se aplican a distintas áreas y/o funciones de una organización.

En nuestro caso, dichos Objetivos Estratégicos establecen Objetivos Operacionales relacionados con la Seguridad de la Información. Una vez establecido un Objetivo Operacional de este tipo, del mismo se derivarán como antes los *Indicadores* para verificar su cumplimiento, las *Metas* correspondientes deseadas y las *Iniciativas* a tomar para lograr tal cumplimiento.

Este proceso de "mapeo" de los objetivos estratégicos de negocios a objetivos de seguridad es muy importante, puesto que de esta manera las métricas de seguridad se ponen en un contexto entendible y con sentido para ejecutivos y gerentes, como resultado de cuantificar la eficiencia del SGSI en su proyección a las actividades de toda la empresa, como de hecho lo pide la ISO 27004.

El resultado es que de esta manera el BSC permite establecer un diálogo con ejecutivos en base a aspectos de la seguridad de interés para la alta gerencia, lo que facilita romper esa suerte de falso paradigma que *la seguridad es un problema técnico* solamente, es decir propio del área IT [4], tan común en las demás áreas de una empresa así como en los niveles gerenciales medios y superiores.

Más aún, en estas condiciones el BSC cumple un rol estratégico en relación con la seguridad de la información. Efectivamente, al *generar* ***valor*** dentro del desarrollo de los negocios el BSC actúa como puente entre el área de negocios y el de seguridad de la información.

Ahora bien, una cuestión que surge a continuación es cómo definir los Indicadores y las Iniciativas correspondientes a los Objetivos Operacionales de Seguridad. Pues bien, los Objetivos de Seguridad pueden ser en la práctica ni más ni menos que los propios **Objetivos de Control** de las normas ISO 27001/27002. Y, por su parte, las Iniciativas de Seguridad pueden ser precisamente los propios **Controles** de estas normas.

Lo anterior no quiere decir precisamente que *todos* los Objetivos del Tablero de Comando sean Objetivos de Control y/o que *todas* las Iniciativas sean Controles de las normas. En realidad el Tablero de Comando no pretende ser una imagen completa de la seguridad de la información a nivel normativo, sino más bien correlacionar los aspectos más críticos de la seguridad con los procesos de negocios de la empresa.

Ing. Carlos Ormella Meyer y Asoc.
Gestión y Auditoría de Riesgos y Seguridad de la Información
Tel: +54-11-4371-4638 – Cel: +54-911-6513-2751
E-mail: ciprio@ingcomyasoc.com.ar

En la Figura 3 se puede visualizar un fragmento de un Tablero de Comando preparado en Excel que gracias al formato condicional permite una semaforización automática de tres niveles (que en los productos comerciales pueden ser más). Para estos niveles se pueden usar diferentes criterios. En la tabla que se presenta se establecieron como umbrales diferenciadores:

- Verde: 75% o más.
- Amarillo: De 45% a menos de 75%.
- Rojo: Menos de 45%.

Figura 3

Perspectivas	Objetivos Control	Indicadores	Metas			Iniciativas
			2010	Cumpl Meta	Nivel Cumpl	
Finanzas	10.1 - Asegurar operación segura	Reducción pérdidas x vulnerabil.	30%	8%	27%	Control 10.1.2 - Gestión de cambios
	.....	.....	.....	.....	.....	.....
Clientes	6.2 - Mantener segurid. con terceros	Accesos controlados clientes	90%	48%	53%	Control 6.2.2 - Tratamiento segur. c/clientes
	.....	.....	.....	.....	.....	.....
Procesos internos	12.6 - Reducir riesgos por vulner.	Vulnerab. verificadas y tratadas	70%	45%	64%	Control 12.6.1 - Control de vulnerabilidades
	.....	.....	.....	.....	.....	.....
Aprendizaje y Crecimiento	8.2 - Asegurar conocim. normas	Nivel de concientización	60 horas	50 horas	83%	Control 8.2.2 - Plan de concientización
	.....	.....	.....	.....	.....	.....

A modo de ejemplo, en el caso del Objetivo "Asegurar una operación segura" se estableció que para el año 2010 las *pérdidas por vulnerabilidades* debían reducirse en un 30%. Sin embargo las mediciones verificadas indican que sólo se redujeron en un 8% lo que implica un 27% de cumplimiento de la meta prevista. Como el nivel de cumplimiento del 27% está por debajo del 45%, el color que toma la celda correspondiente será el rojo.

Del análisis de un tablero de comando puede surgir la necesidad de tomar decisiones adecuadas para proporcionar mayor fuerza a las Iniciativas (controles) relacionadas con las metas en rojo y amarillo, en este orden de prioridades, o incluso adicionar nuevas Iniciativas para lograr el cumplimiento de la meta en cuestión.

Los datos que alimenten los valores verificados de un Tablero de Comando pueden lograrse por medio de interfaces a otros programas que ofrecen los productos comerciales, o bien simplemente ingresando en forma manual los datos correspondientes.

Referencias

[1] NIST 800-55 - Performance Measurement Guide for Information Security.
http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/sp800-55-rev1.pdf
[2] NIST 800-53 - Recommended Security Controls for Federal Information Systems.
http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf
[3] El Factor Gente y la Seguridad de la Información, Ing. Carlos Ormella Meyer.
http://ictnet.es/system/files/factor_gente_segu_info.pdf -
http://www.criptored.upm.es/descarga/FactorGenteSeguInfo.zip -
www.iso27000.es/download/Carlos_Ormella-factor-gente-segu-info.pdf
[4] Seguridad Informática vs. Seguridad de la Información, Ing. Carlos Ormella Meyer.
http://www.angelfire.com/la2/revistalanandwan/articulos.html#si2