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

Preguntas y Respuestas
METRICAS DE SEGURIDAD DE LA INFORMACION

P: ¿Qué son las métricas?
R: Métricas de seguridad es la expresión usual con referencia a las Mediciones para la Gestión de Seguridad de la Información tratadas por la norma ISO 27004.

P: ¿Y qué dice la ISO 27004?
R: Esta norma establece un modelo aplicable a las métricas para medir la *eficiencia* y progreso del Sistema de Gestión de Seguridad de la Información (SGSI) y la *efectividad* de los controles implementados a partir de las normas ISO 27001 e ISO 27002 de Seguridad de la Información.

P: ¿Y cómo se mide eso?
R: Una herramienta efectiva para la gestión del desempeño de las medidas de seguridad es el Balanced Scorecard (BSC). El BSC es un modelo de gestión que traslada la estrategia en objetivos estratégicos interrelacionados y una herramienta que muestra el progreso hacia las metas estratégicas.

P: ¿Y qué características tiene ese modelo?
R: El BSC enfoca el negocio por medio de cuatro Perspectivas (Finanzas, Clientes, Procesos Internos, y Aprendizaje y Crecimiento) produciendo una propuesta de valor que balancea indicadores financieros con indicadores no financieros o intangibles.

P: ¿Y cómo se produce esa propuesta?
R: Siguiendo el proceso relacionado con las dos partes del BSC: **Mapa Estratégico y Tablero de Control o de Comando**.

P: ¿Qué es el Mapa Estratégico?
R: El Mapa Estratégico toma forma estableciendo diferentes Objetivos Estratégicos para cada una de las cuatro Perspectivas, de modo tal que los objetivos guarden *relaciones causa-efecto*.

P: ¿Y el Tablero de Control o Comando?
R: El Tablero de Control o Comando es la parte más conocida del BSC. Consiste en una tabla donde para cada Perspectiva se establecen los **Objetivos Estratégicos**, las **Iniciativas** para poderlos cumplir y los **Indicadores** con que se irá midiendo su evolución en diferentes hitos o **Metas** temporales conforme se proyecte.

P: ¿Indicadores es lo mismo que Métricas?
R: No exactamente. Ocurre que en realidad el término Métricas suele usarse con un sentido general; sin embargo es conveniente distinguir tres tipos de parámetros:
a) **Medidas:** Lo que realmente se mide.
b) **Métricas:** Resultado de relacionar diferentes Medidas. Muchas veces resulta un porcentaje.
c) **Indicador:** Evaluación de una o más Métricas. Puede constituir también un porcentaje.

P: ¿Y qué se hace con lo que se va midiendo según las Metas establecidas?
R: Es común que los valores medidos en las diferentes Metas temporales se comparen con los valores proyectados estableciendo así un nivel de logro o cumplimiento. Estos resultados pueden semaforizarse para destacarlos y facilitar la toma de decisiones de corrección que pudieren necesitarse incorporar.

P: ¿En qué consiste la semaforización?
R: Se puede usar la coloración automática de las celdas de resultados conforme ciertos umbrales que indiquen límites o rango, por ejemplo rojo, amarillo y verde para conformidad baja, media y alta respectivamente.

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

P: ¿Y todo esto se puede aplicar a la Seguridad de la Información?

R: Sí, efectivamente. La operativización de la estrategia traslada los *Objetivos Estratégicos* o de primer nivel a *Objetivos Operacionales* en las diferentes áreas de una organización. De esta manera se puede preparar un Tablero de Comando por ejemplo a nivel de Seguridad de la Información, donde los ***Objetivos operacionales*** pueden resultar ser sencillamente los ***Objetivos de Control*** de la norma ISO 27002 y las ***Iniciativas***, los ***Controles*** de la misma norma.

.