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: ingcomyasoc@gmail.com

INTRODUCCIÓN AL BOW-TIE PARA ANALISIS DE RIESGOS (*)

En la nota “Norma ISO 31000 de Riesgos Corporativos” que publicara hace un tiempo [1], se comentaron los diferentes aspectos de la norma ISO 31000 para Gestión de Riesgos Corporativos, es decir, para todo tipo de riesgos.

De hecho, especialmente la ISO 27001 así como la ISO 27005 responden al nuevo enfoque de la ISO 31000 en el que los riesgos responden a la **incertidumbre** que puede afectar a los objetivos que se busquen.

Este cambio hace que se consideren no sólo los tradicionales riesgos negativos, sino también a los riesgos positivos y las oportunidades como contrapartidas de las amenazas.

En dicho trabajo también se hizo una breve revisión de otra norma complementaria, la ISO 31010, referida a las Técnicas de Valuación de Riesgos y los diferentes criterios para la selección de las técnicas correspondientes.

Dicha norma incluye dos Anexos muy útiles.

En uno se tabula una serie de técnicas diferentes y su aplicación a las diferentes etapas del proceso de valuación de riesgos, de acuerdo con la respectiva relevancia respecto de recursos, incertidumbre, complejidad y posibilidad de resultados cuantitativos.

En el otro Anexo se analizan dichas técnicas en cuanto a su uso, requerimientos de entrada, proceso, resultados, y fortalezas y limitaciones.

Precisamente una de las técnicas revisadas en estos Anexos se refiere al llamado **Bow-tie**, un método de gestión de riesgos que se distingue por facilitar una interpretación simple de los riesgos más importantes por parte de personal no especializado y que, especialmente en la práctica de consultoría, nos ha resultado muy eficaz en la mayoría de los escenarios.

Esto obviamente es útil sobre todo cuando se gestiona un cierto presupuesto de seguridad, así como una suerte de “entrada” en el interés en la seguridad de la información por parte de la alta gerencia, como irá surgiendo en los próximos párrafos.

.

Bow-tie es un método visual que describe y analiza los caminos entre **causas** y **consecuencias** de un cierto riesgo; es decir, en nuestro caso entre **amenazas** e **impactos** ante la presencia de un riesgo puede ser activado por un incidente.

Bow-tie toma el nombre por la similitud del diagrama con una **corbata de lazo/moño o corbatín (bow-tie)**, y está formado por un centro circular y ambos costados radialmente abiertos hacia fuera **(Figura 1)**.

Por simplicidad en esta figura estamos representando las **amenazas (causas)** y los **impactos (consecuencias)** como sendos conjuntos.

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: ingcomyasoc@gmail.com

A su vez, las líneas radiales representan las relaciones entre amenazas y riesgos en la parte izquierda, y entre riesgos e impactos en la porción derecha del diagrama.

En los casos más simples una determinada amenaza se relaciona con el riesgo por medio de una de las líneas radiales hacia el centro, e incluso podría seguir por una única línea radial desde el riesgo hacia un determinado impacto.

Pero también puede darse el caso que una determinada amenaza provoque más de un impacto, así como también que más de una amenaza provoquen un cierto incidente con el impacto correspondiente.

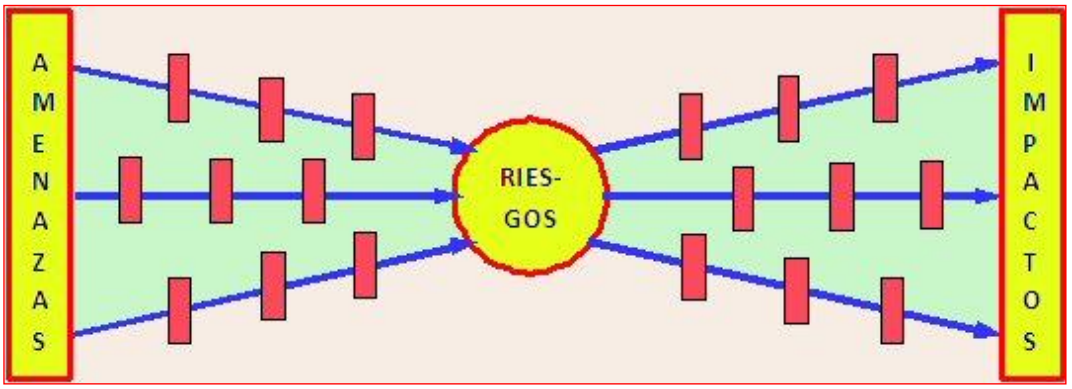

Figura 1

El análisis Bow-tie es un proceso ideal para comprender la dinámica de los mayores incidentes potenciales, gracias a facilitar una conceptualización de los riesgos de una manera muy clara y visual, facilitando la identificación y análisis de las variables involucradas.

De hecho, los diagramas Bow-tie constituyen una herramienta simple y efectiva para comunicar los resultados de un análisis de los riesgos más importantes al personal de todo nivel y que, de hecho, más importen a los ejecutivos de una empresa.

La elaboración del diagrama se inicia con la identificación de cada riesgo potencial que pueda ser aprovechado por una amenaza y causar un impacto que afecte los objetivos deseados de seguridad.

En la práctica es usual construir un diagrama bow-tie a partir de una sesión de *brainstorming* con los principales responsables de las operaciones de una empresa, incluyendo la alta gerencia especialmente en cuanto a los riesgos estratégicos del negocio.

En segundo término se dibujan líneas entre cada amenaza y el riesgo en cuestión.

El tercer paso consiste en establecer *barreras* en dichas líneas en forma de líneas verticales.

Se denominan *barreras* a los controles que se implementen y que en el tramo entre una amenaza y el riesgo representan los controles de prevención correspondientes en cada caso.

En la parte de la derecha del diagrama ya mencionamos que también tenemos líneas radiales que, en esta parte se ubican desde el riesgo hacia los impactos potenciales.

Además, también aquí se establecen *barreras* que en este caso representan las medidas reactivas de mitigación y recuperación.

Así las cosas, el Bow-tie ofrece una clara diferenciación entre la gestión de riesgos *preventivos* y *reactivos*.

Algo para destacar especialmente es que este método también puede usarse para consecuencias positivas donde los controles facilitan la generación o incremento de **Oportunidades**.

Efectivamente, el diagrama Bow-tie se puede usar también para los **riesgos positivos** (ver **Unidad de Estudio 5** del **Módulo de Estudio 2**), donde ahora las amenazas son las mencionadas Oportunidades.

Para ello hay que recordar que en realidad, conforme la **ISO 31000**, el riesgo del centro del diagrama es una expresión de la **incertidumbre** que puede afectar a los objetivos de seguridad que se buscan, de forma tal que se puede dar una situación de **riesgos positivos y negativos** (upside y downside risks).

En este enfoque, las *barreras* ahora reflejan las medidas que facilitan la generación de consecuencias favorables.

Efectivamente, en el caso de los riesgos positivos, los controles de la izquierda del diagrama trabajan para *optimizar y aumentar* el aprovechamiento de las **Oportunidades** donde los "controles" *preventivos* son ahora medidas habilitantes que facilitan el aprovechamiento de las **Oportunidades**.

A su vez, los "controles" de *mitigación o recuperación* ahora son medidas de mejoramiento en el aprovechamiento de dichas **Oportunidades**.

Todo esto implica que el *riesgo residual* (positivo) será, al revés de lo usual con los riesgos "tradicionales", *mayor* que el nivel del *riesgo inherente.*

Adicionalmente, puesto que las barreras nunca son perfectas, el esquema Bow-tie permite identificar las formas en que pueden fallar los controles.

Estos factores o condiciones se denominan **Factores de Escalado** que, por simplicidad, no hemos incluido en la Figura 1.

A partir de dichos factores pueden incorporarse controles especiales para controlar la efectividad de los controles/barreras.

Nosotros en este punto usamos directamente el Tablero de Control del BSC (Balanced Scorecard) [2] adaptado a los controles del Bow-tie.

Finalmente, como ya lo destacamos al principio, conviene destacar nuevamente que el diagrama Bow-tie no es precisamente lo más adecuado para todo nivel de riesgos, sino especialmente útil para los riesgos más importantes.

Además, para una claridad del esquema los riesgos estudiados no debieran pasar de 10 o aún menos.

De cualquier manera, como también se dijo, el esquema puede ser sumamente útil para niveles gerenciales no especialistas, sobre todo si se partió de un *brainstorming* donde esas mismas personas establecieron los riesgos más preocupantes para las operaciones y estrategias de la empresa.

(*) Extraído del Manual de Estudio del curso a distancia “Gestión de Riesgos de Seguridad de la Información” (Sección Cursos de la página Web www.angelfire.com/la2/revistalanandwan).

[1] “Norma ISO 31000 de Riesgos Corporativos”, www.angelfire.com/la2/revistalanandwan/iso_31000_riesgos_corp.pdf

[2] “Métricas de Seguridad de la Información y Gestión del Desempeño con el Balanced Scorecard”, www.angelfire.com/la2/revistalanandwan/articulos.html#bsc

* Ing. Carlos Ormella Meyer. Cursos y Soporte Digital - Asesoramiento - @meyerormella

Hecho el depósito en custodia bajo la Ley Nro. 11.723.