Ing. Carlos Ormella Meyer y Asoc.
Seguridad de la Información, Redes y Telecomunicaciones
Tel: 54-11-4371-4638 – Cel: (011) 15-6513-2751
E-mail: ciprio@ciudad.com.ar

¿Análisis de Impactos o Valuación de Riesgos?

En algunos medios se ha planteado una suerte de disyuntiva sobre qué mecanismo es mejor o más adecuado para iniciar un plan de seguridad de la información. Y en tal sentido se menciona el **BIA** (Análisis de Impacto en los Negocios) y **RA** (Valuación de Riesgos).

La verdad es que ya de las propias palabras que los caracterizan, surge evidente que BIA y RA son cosas distintas, por lo que su comparación no puede hacerse directamente. Incluso hasta se podría decir que RA no se relaciona directamente con el BIA.

BIA, Análisis de Impacto en los Negocios

El análisis de impacto en los negocios BIA es un paso clave en el proceso de un **BCP** (Plan de Continuidad de Negocios).

Esto se debe a que BIA está básicamente relacionado con eventos indeseados que provoquen una interrupción o degradación de las operaciones de una empresa, es decir, afectando la ***disponibilidad*** de los recursos críticos para mantener operando adecuadamente los procesos de negocio correspondientes. Incluso en este contexto no se necesita conocer la razón y/o la probabilidad de tales eventos para poder determinar el impacto de una falla en dichos procesos.

El BIA por definición se refiere a ***impactos***, un concepto muy atado al **ALE** (Expectativa de Pérdidas Anuales) para la determinación de riesgos. De cualquier manera, el impacto es uno de los dos factores de riesgos, donde el otro es la frecuencia anual de ocurrencia de los eventos indeseados, para determinar entre los dos la expectativa de pérdidas a lo largo de un año.

Por otra parte, el BIA sirve para valuar el impacto a lo largo del tiempo en un ***proceso de negocios*** no disponible o con un desempeño diferente al previsto, así como para priorizar las funciones que lo relaciona con otros procesos.

La función de tiempo se identifica con el **RTO** (Objetivo del Tiempo de Recuperación) de los procesos de negocios lo que conlleva el RTO de los componentes correspondientes, es decir las funciones de negocio y los recursos/activos que las sustentan. A su vez, las necesidades de disponibilidad de los procesos en cuestión implican el establecimiento de una frontera temporal crítica dada por el **RPO** (Objetivo del Punto de Recuperación).

RA, Valuación de Riesgos

Por el otro lado, la valuación de riesgos (risk assessment) se refiere obviamente a los riesgos como entidad, es decir los resultantes de los diversos componentes que se usen: los dos factores mencionados de ***impactos*** y ***probabilidad anual de ocurrencia*** en el caso de trabajar con ALE, o bien **activos, vulnerabilidades y amenazas** en el caso más usual en los proyectos de seguridad de la información.

Además, lo importante a tener en cuenta es que el RA no se refiere sólo a los aspectos de **continuidad/disponibilidad** propios del BIA sino también al resto de los factores que afectan la seguridad de la información, tales como la **confidencialidad, integridad, responsabilidades, autenticidad y confiabilidad.**

Por otra parte, el RA es el mecanismo idóneo para determinar cómo mitigar el efecto de esos eventos o incluso previendo que ocurran, trabajando sobre los componentes del riesgo por medio de salvaguardas o contramedidas de seguridad.

RA y BIA

De todo lo anterior podría decirse que RA es más completo que BIA, aunque en realidad no incluye todas las prestaciones del BIA, como los parámetros temporales mencionados. Además, en todo caso se puede decir que la tasa de criticidad o importancia de los procesos determinados con BIA se puede traspasar a

la RA, con lo que para procesos de un mismo nivel de riesgo el tratamiento sería más inmediato para los de mayor tasa y menor o postergable para los otros.

En realidad los dos mecanismos que se comparan surgen de metodologías diferentes, aunque en todo caso con algunos aspectos en común. Estas metodologías son el **BCP** ya mencionado y el **SGSI** (Sistema de Gestión de Seguridad de la Información) resultante de la aplicación de las normas de seguridad de la información ISO 27002 e ISO 27001.

Cuando se revisan ambos tipos de prestaciones en un proyecto común, hay quienes dicen que el RA debiera anteceder al BIA, ya que provee suficiente justificación para embarcarse en el desarrollo de un BCP que por supuesto incluye el BIA. Sin embargo de esta manera se corre el riesgo de encontrar que algunos procesos no están en riesgo y entonces algunas funciones críticas podrían pasarse por alto.

En realidad, si se trata de un proyecto de BCP exclusivamente, el BIA irá primero y luego el RA, aunque enfocado exclusivamente a los procesos que el BIA determinó como críticos para la continuidad de los negocios.

En cambio, la situación es distinta en un proyecto específico de seguridad de la información basado en un SGSI. En primer lugar un proyecto de este tipo incluye los controles específicos relacionados con el BCP, entre ellos el 14.1.2 de la ISO 27002 referido al BIA. Además, conforme lo estipulado por la ISO 27001, el RA como análisis de riesgos es anterior a la implementación del propio SGSI, aunque de cualquier manera el BIA realizado luego pueda complementarlo.

Por otra parte, en un proyecto BCP específico se puede trabajar directamente con la **BS 25999**, una muy buena norma británica sobre **BCM** (Gestión de Continuidad de Negocios) que, por cierto, puede considerarse "descendiente" de la BS 7799 (precursora también de las normas de seguridad ISO 17799, hoy 27002, y de la ISO 27001).

BS 25999 se usa para planificar, implementar/operar, monitorear/revisar, y mantener/mejorar un **BCMS** (Sistema de Gestión de Continuidad de Negocios, **SGCN** en español), similar bajo el ciclo ***PDCA*** de mejoramiento continuo, al **SGSI** de la ISO 27001 así como a otros sistemas de gestión tales como **SGC**, **SGA** y **SGSSL** de las normas ISO 9001, ISO 14001 y OHSAS 18001 de Calidad, Ambiental, y Seguridad y Salud Laboral respectivamente.