Ing. Carlos Ormella Meyer y Asoc.
Gestión y Auditoría de Riesgos y Seguridad de la Información
Tel: +54-11-3979-7220 – Cel: +54-911-6513-2751
E-mail: ingcomyasoc@gmail.com

¿Análisis de Impactos o Valuación de Riesgos?

En algunas ocasiones se ha venido planteado una 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 caracterizan dichas siglas surge evidente que BIA y RA son cosas distintas, por lo que su comparación no puede hacerse directamente.

BIA, Análisis de Impacto en los Negocios

El análisis de impacto en los negocios es un paso clave en el proceso de un **BCP** (Plan de Continuidad de Negocios) como parte de un **BCM** (Gestión 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 necesarios para mantener operando adecuadamente los procesos críticos de negocio correspondientes. Incluso en ese contexto no se necesitan conocer las causas 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 usado para la determinación de riesgos enfocados en los **incidentes** incluso medidos cuantitativamente como el **ALE** (Expectativa de Pérdidas Anuales). 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 permite 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.

El BIA permite identificar los lapsos de tiempo y el alcance del impacto de una interrupción en las operaciones críticas de una organización, proporcionando los datos para determinar las estrategias para tratar con ellos. De esta manera está muy relacionado con la disponibilidad. Los lapsos de tiempo se establecen con indicadores como **RTO, RPO y MTPD**. Estos indicadores establecen ventanas “críticas”, "recuperación del pasado” y “fatal” respectivamente. En todos los casos, los componentes de los procesos, es decir funciones y recursos/activos de los procesos que los soportan, heredan los correspondientes lapsos de tiempo.

RA, Valuación de Riesgos

Por el otro lado, la valuación de riesgos (risk assessment) se refiere también a los riesgos como entidad, es decir los resultantes de los diversos componentes que los provocan: 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 de determinar los i>riesgos enfocados en los **activos**

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.

Ing. Carlos Ormella Meyer y Asoc.
Gestión y Auditoría de Riesgos y Seguridad de la Información
Tel: +54-11-3979-7220 – Cel: +54-911-6513-2751
E-mail: ingcomyasoc@gmail.com

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.

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/BCM** de la norma BS 25999 y el **SGSI** (Sistema de Gestión de Seguridad de la Información) según lo establecido por las normas de Seguridad de la Información ISO 27002 e ISO 27001.

En un proyecto de BCP / BCM, RA es posterior al BIA. Un Análisis de Impactos en los Negocios debe completarse antes de realizar la Valuación de Riesgos, para identificar así primero las funciones críticas en las que debe concentrarse dicha valuación.

Como resultado, esta forma de RA se refiere solamente a los procesos críticos para la continuidad de negocios identificados por el BIA, bajo el enfoque de la disponibilidad necesaria para asegurar la continuidad de negocios.

Por otra parte, en cualquier caso, podemos decir que el índice de criticidad / importancia de los procesos establecidos en el BIA puede utilizarse en la RA, con lo que para procesos de un mismo nivel de riesgo el tratamiento sería más inmediato para los de mayor tasa de criticidad y menor o postergable para los otros.

Pero las cosas no son tan simples en algunas situaciones. Una de ellas en la que hemos trabajado aparece cuando las empresas ya habían implementado un BCP y estaban planeando establecer un plan de seguridad bajo SGSI.

Efectivamente, la valuación de riesgos implica la valuación de todas los riesgos existentes (no sólo los críticos) tanto TIC como los organizacionales, operacionales y físicos, en el contexto del valor de los activos de la organización. En este sentido, la valuación de riesgos en forma integral requiere identificar las vulnerabilidades de los activos de la organización que las amenazas podrían explotar.

Además, RA no se refiere sólo al aspecto de **disponibilidad** propio del BIA sino también al resto de los factores que afectan la seguridad de la información, tales como la **confidencialidad e integridad, más la responsabilidad, autenticidad y confiabilidad**. Como se puede apreciar, el RA en un escenario SGSI es más amplio que en el caso de un BCP, por lo cual si existe un BCP/BCM antes de implementar el SGSI de la ISO 27001, habrá que ampliar el RA correspondiente.

La situación es diferente cuando no hay una implementación BCP/BCM previa antes de implementar un SGSI. En este caso el RA se realiza antes que el BIA resultante de aplicar el Capítulo 14, Gestión de Continuidad del Negocios, de la ISO 27002. De esta manera, se tiene que esta forma de RA es lo suficientemente amplia como para permitir extraer un subconjunto del RA para el tratamiento de la porción Continuidad de Negocios de un proyecto de seguridad de la información.

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

Hecho el depósito en custodia bajo la Ley Nro. 11.723

