EFICIENCIA GERENCIAL Y PRODUCTIVIDAD S.A.
Calle Pedro Irigoyen # 116, Miraflores, Lima, Perú
Tfl.: (511) 434 3528 fax: (511) 436 6144
www.eficienciagerencial.com

Gestión del Riesgo en el Business Continuity Planning

Por

Alberto G. Alexander, Ph.D. CBRP
Auditor SGSI Certificado IRCA
alexander@eficienciagerencial.com

Es muy importante entender que un programa de business continuity planning (BCP) no sólo debe atender la recuperación de las instalaciones frente a un desastre. El BCP, también debe contemplar las acciones preventivas de lugar. Para dicho efecto en todo programa de BCP se debe de manera regular efectuar un cálculo del riesgo que no sólo contemple la identificación de amenazas significativas que afecten las operaciones de la empresa, las vulnerabilidades y el grado de exposición al riesgo. Es importante también identificar los controles a instaurar para minimizar el daño en la empresa del impacto de un posible desastre. Un resultado esperado del cálculo del riesgo en la metodología del BCP, es determinar los distintos tipos de escenarios de amenazas que pueden presentársele a una empresa, los cuales serán usados para la elaboración de las estrategias de continuidad y desarrollo de los planes.

Introducción.-

La gestión del riesgo tradicionalmente contempla el "cálculo del riesgo, la apreciación de su impacto en el negocio y la posibilidad de ocurrencia." (Hiles, 2004) Seguidamente se derivan pasos para reducir la frecuencia a un nivel considerado aceptable. Para entender la gestión del riesgo, es importante clarificar algunos conceptos. En primera instancia, ¿que es riesgo? Riesgo se define como "la probabilidad que una amenaza pueda explotar una vulnerabilidad y causar daño a los activos de una organización." (Barnes, 2001) Una amenaza es "el intento de hacer daño" (von Roessing, 2002). Las amenazas pueden clasificarse de varias maneras según su naturaleza. Pueden ser: (1) naturales, (2) físicas, (3) humanas, (4) tecnológicas, (5) operacionales, (6) sociales. Las vulnerabilidades son "condiciones de la organización que pueden hacer que una amenaza se manifieste" (Meredith, 1999). Una vulnerabilidad "es una combinación de la posibilidad de una alteración y su potencial severidad" (Sheffi, 2005) Los activos de una organización "son todas aquellas cosas a las que la empresa les da valor". (O´Hehir, 2001) En segunda instancia es importante entender que una amenaza por si sola no causa daño, es una simple intención de producir daño. El riesgo se presenta cuando la amenaza y la vulnerabilidad se juntan y la amenaza la puede explotar. La gestión del riesgo en el contexto del BCP trata los conceptos presentados, para determinar luego, la exposición al riesgo que tiene la empresa e identificar los escenarios de amenazas a los que la organización esta sujeta.

Es relevante mencionar que en las últimas décadas se ha observado un crecimiento de una serie de requerimientos legales y regulatorios para una gama de industrias exigiendo que las empresas desarrollen un sistema de gestión del riesgo, dándole cada vez más importancia al BCP. Así tenemos en el Reino Unido el denominado "Turnbull Report", el cual pone exigencias muy puntuales para las empresas que coticen en la bolsa de valores de Londres. En esencia se exige que las empresas que coticen tengan un sistema de control interno para poder facilitar la gestión de los riesgos del negocio. En los Estados Unidos, aparece el llamado "Sarbanes-Oxley Act" conocido como el "SOX 404". Esta ley desde Julio del 2002, requiere que toda empresa que cotice en la bolsa de valores estadounidense, tenga instaurado un sistema de análisis del riesgo y controles para mitigarlos. A nivel mundial tenemos las regulaciones de BASILEA II con una serie de exigencias para la Banca internacional en relación al manejo del riesgo operativo. En la industria alimentaria en muchos países existe un requerimiento para realizar el análisis del riesgo el cual es exigido por el denominado Hazardous Analysis Critical Control Point (HACCP), convertido recientemente en el ISO 22000. En los Estados Unidos el organismo "Federal Deposit Insurance Corporation" (FDIC) encargado específicamente de supervisar a los Bancos con el fin de asegurar un adecuado sistema bancario, le exige a cada entidad bancaria y a todas sus sucursales que tengan un BCP implantado y ensayado.
Como se puede observar, el requerimiento para que las empresas realicen una gestión del riesgo esta popularizándose en distintas industrias a nivel mundial La exigencia en las empresas es que la gestión del riesgo sea una herramienta gerencial y los gobiernos corporativos la puedan utilizar como medio de control de las operaciones.

En la figura Nº 1 se presentan los pasos metodológicos que se debieran seguir al construir un business continuity plan. El primer paso, en el método clásico es la denominada "gestión del riesgo". En esta etapa se persiguen, usualmente los siguientes objetivos: (1) Identificación de las distintas amenazas que podrían impedir el normal desenvolvimiento de las operaciones en la empresa. (2) Evaluar la vulnerabilidad organizacional de cada amenaza y que tan severamente podrían ser afectadas las operaciones en la empresa. (3) Revisión de los controles actuales para reducir el riesgo o mitigar pérdidas. (4) Cálculo del nivel de exposición al riesgo (5) Determinar los escenarios de amenazas para los cuales deben ser desarrolladas las estrategias de continuidad y los planes respectivos.

Metodología del Cálculo del Riesgo.-

En la figura Nº 2 se tienen los pasos metodológicos que se recomiendan para el cálculo de la exposición del riesgo y posteriormente poder determinar los escenarios de amenazas que afectan a la empresa o al área a la que se le realiza el estudio.
A continuación se hará una descripción de los pasos de la metodología.
(1) Identificación de Amenazas.- Un paso fundamental en la metodología es la identificación de las amenazas. Todas esas condiciones que pueden generar daño a la organización deben ser definidas. Las amenazas al explotar las vulnerabilidades pueden ocasionar el riesgo. Un riesgo que afecta las operaciones y las puede paralizar se define como "desastre". Un desastre es "un evento que altera los procesos críticos de la organización que afectan su misión y degrada su servicio a un punto donde el impacto financiero y operacional se convierte en inaceptable" (Hiles, Barnes, 2002).

Figura Nº 1 Proceso de Elaboración de un Business Continuity Plan

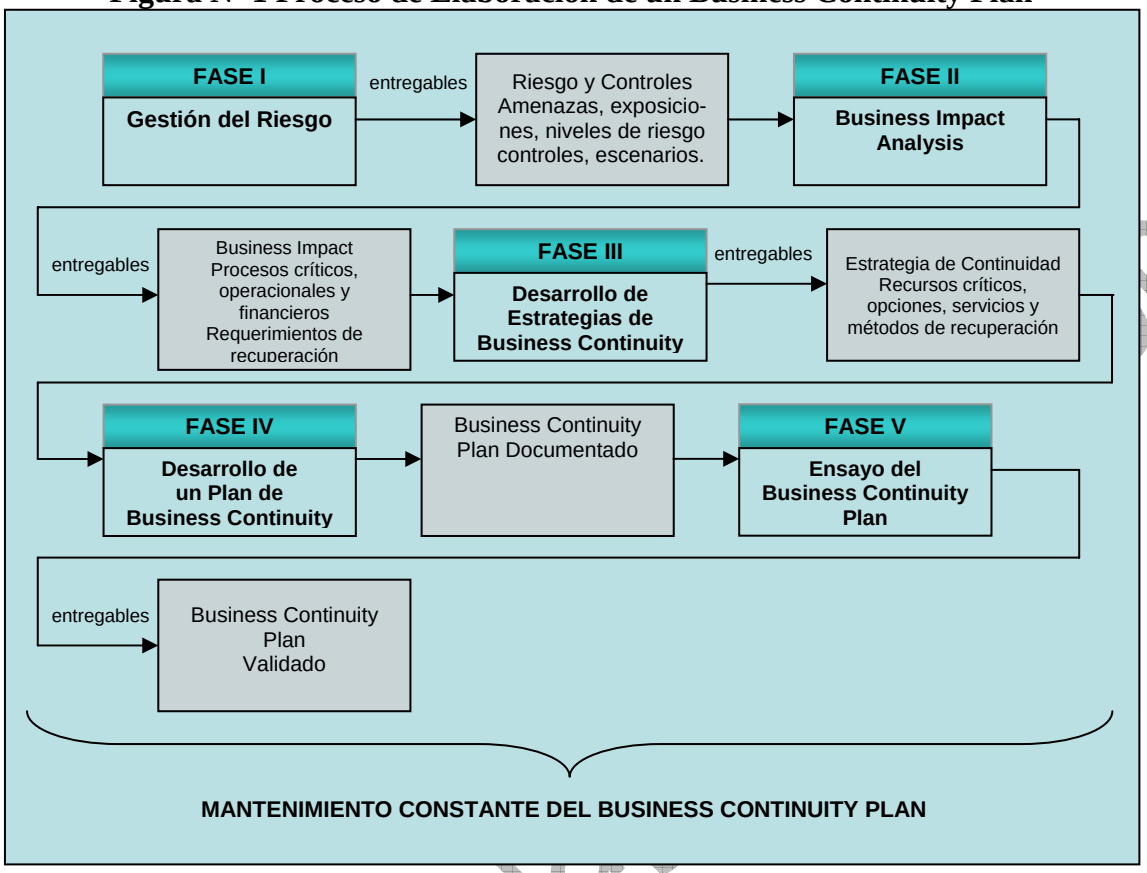
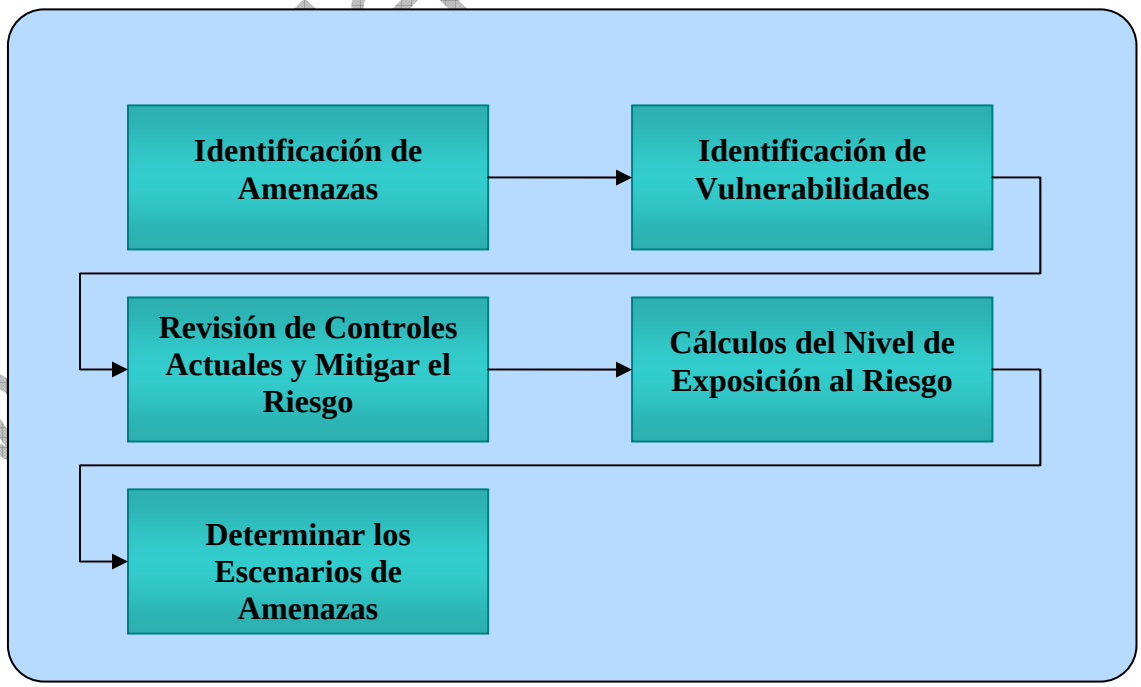


Figura Nº 2 Metodología del Cálculo del Riesgo



Las amenazas que se desean identificar son aquellas que afectan a los activos de las funciones organizacionales. El método recomendado para buscar las amenazas tiene dos etapas: **(a)** Análisis General de Amenazas. Aquí se revisan las distintas potenciales amenazas que pueden afectar a la organización. Uno de los objetivos de esta etapa es la de identificar exposiciones específicas que puedan requerir medidas protectoras y así minimizar la probabilidad que las amenazas pudiesen causar daño a la organización. Este tipo de análisis es conducido en las instalaciones de la empresa y puede usualmente atender los siguientes aspectos: ubicación de instalaciones, seguridad interna y externa, ambiente físico, protección de activos, protección del personal, protección de información y análisis de la cobertura de pólizas. **(b)** Análisis Departamental.- Aquí en este tipo de investigación se hace especial hincapié en las interrupciones a las que las funciones organizacionales departamentales están expuestas por la pérdida de recursos esenciales tales como: instalaciones, sistemas de cómputo, registros vitales, sistemas telefónicos, personal clave, conectividad de la red, equipo especializado, materias primas y material de empaque. En este nivel de análisis el objetivo es el de identificar las funciones organizacionales que tienen la mayor exposición a la interrupción, y poder identificar los recursos de los que dependen las funciones organizacionales.

A cada amenaza identificada se le debe calcular su posibilidad de ocurrencia y el impacto económico que pudiese ocasionar en la organización. La empresa debe tomar en esta etapa decisiones sobre las opciones de tratamiento del riesgo. Decidir que amenazas se reducirán con controles, cuáles se aceptarán y se decidirá vivir con ellas, cuáles se transferirán (por ejemplo a una aseguradora.) y cuales se evitarán. El resultado final de esta etapa es un listado de amenazas consideradas vitales y un listado de funciones organizacionales mostrando su dependencia con determinados recursos.

(2) Identificación de Vulnerabilidades.- Por cada amenaza identificada en el paso anterior se deben identificar sus vulnerabilidades. Es importante recalcar, que una vulnerabilidad no causa daño, es simplemente una condición o conjunto de condiciones que pueden hacer que una amenaza afecte un activo. Una vez identificadas las distintas vulnerabilidades por cada amenaza, se debe hallar el grado en que la amenaza puede explotar cada vulnerabilidad. Se termina con un listado de aquellas vulnerabilidades consideradas importantes, ya que pueden ser explotadas por las amenazas.

(3) Revisión de Controles Actuales.- Al haber identificado las distintas amenazas y las respectivas vulnerabilidades organizacionales, se debe en esta etapa analizar con la debida profundidad las distintas salvaguardas existentes en la empresa. Si una amenaza explota una vulnerabilidad podría generarse un desastre. Se debe poner hincapié en cerciorarse que las salvaguardas están trabajando correctamente. Una salvaguarda en la cual se confía en su eficacia, pero en la práctica no opera bien, es una fuente de posibles vulnerabilidades y se aumentan las probabilidades que las amenazas penetren y hagan daño.

El resultado de esta etapa es una lista de todos aquellos controles, su estado de funcionamiento y detalle de aquellos controles que deben instaurarse para reforzar las vulnerabilidades y minimizar las consecuencias en la empresa si el desastre se presentara.

(4) Cálculo del Nivel de Exposición al Riesgo.- Una vez detectadas las amenazas, la dependencia de recursos de cada función organizacional y sus vulnerabilidades, se debe proceder a precisar el grado de severidad de cada potencial amenaza identificada y la cobertura. La cobertura es el grado de protección que tiene la empresa frente a una amenaza en particular. En la figura Nº 3 denominada Cálculo de la Exposición del

Figura Nº 3: Cálculo de la Exposición del Riesgo

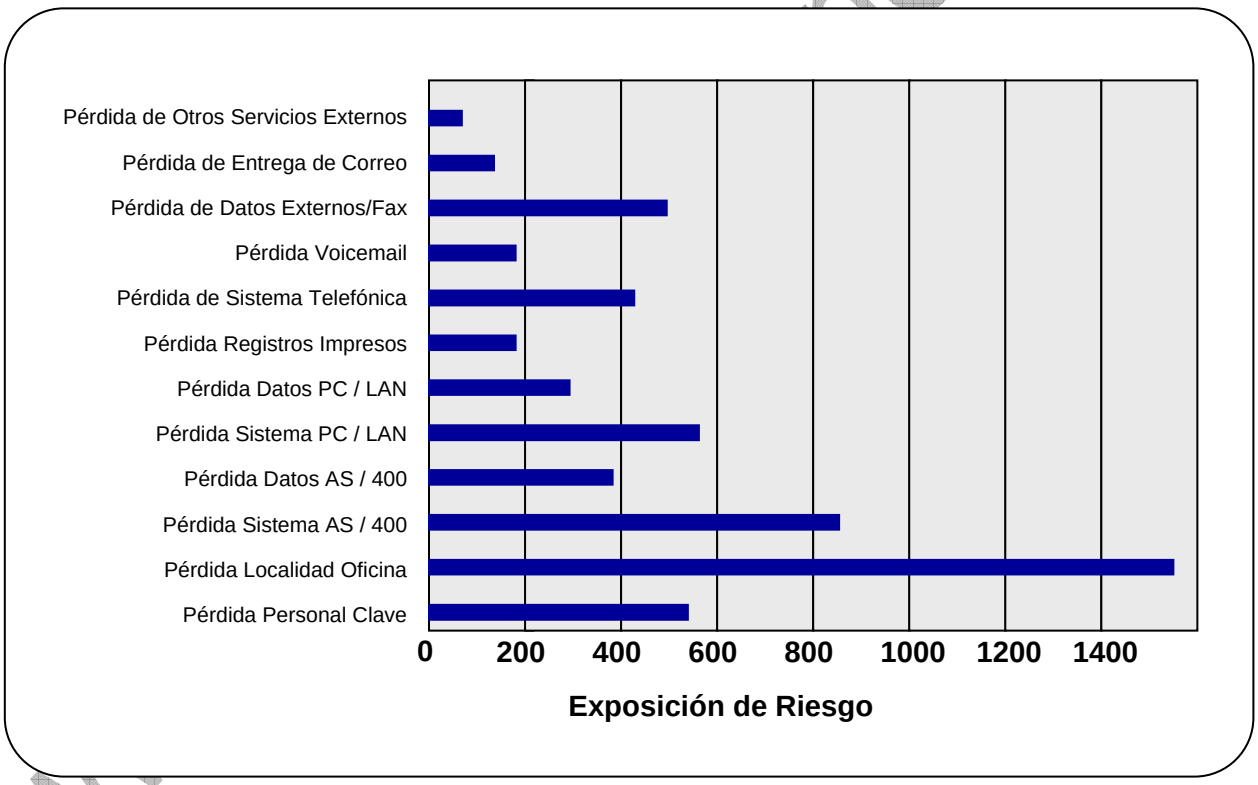
POTENCIALES AMENAZAS	SEVERIDAD				COBERTURA						EXPO-SICIÓN DEL RIESGO
	N/A	B	M	A	0-19%	20-39%	40-59%	60-79%	80-99%	100%	
1. PÉRDIDA DE PERSONAL CLAVE				✓				✓			40
2. PÉRDIDA DE INSTALACIONES				✓	✓						100
3. PÉRDIDA SISTEMA AS/400				✓			✓				60
4. PÉRDIDA DATOS AS/400				✓				✓			40
5. PÉRDIDA PC/LAN		✓							✓		2
6. PÉRDIDA PC/LAN DATOS		✓							✓		2
7. PÉRDIDA DE SISTEMA TELEFÓNICOS (VOZ)			✓		✓						50

NIVELES DE SEVERIDAD:
Alta = 100, Moderada = 50, Baja = 10

EXPOSICIÓN DEL RIESGO:
NIVEL DE SEVERIDAD x (100% - %COBERTURA)

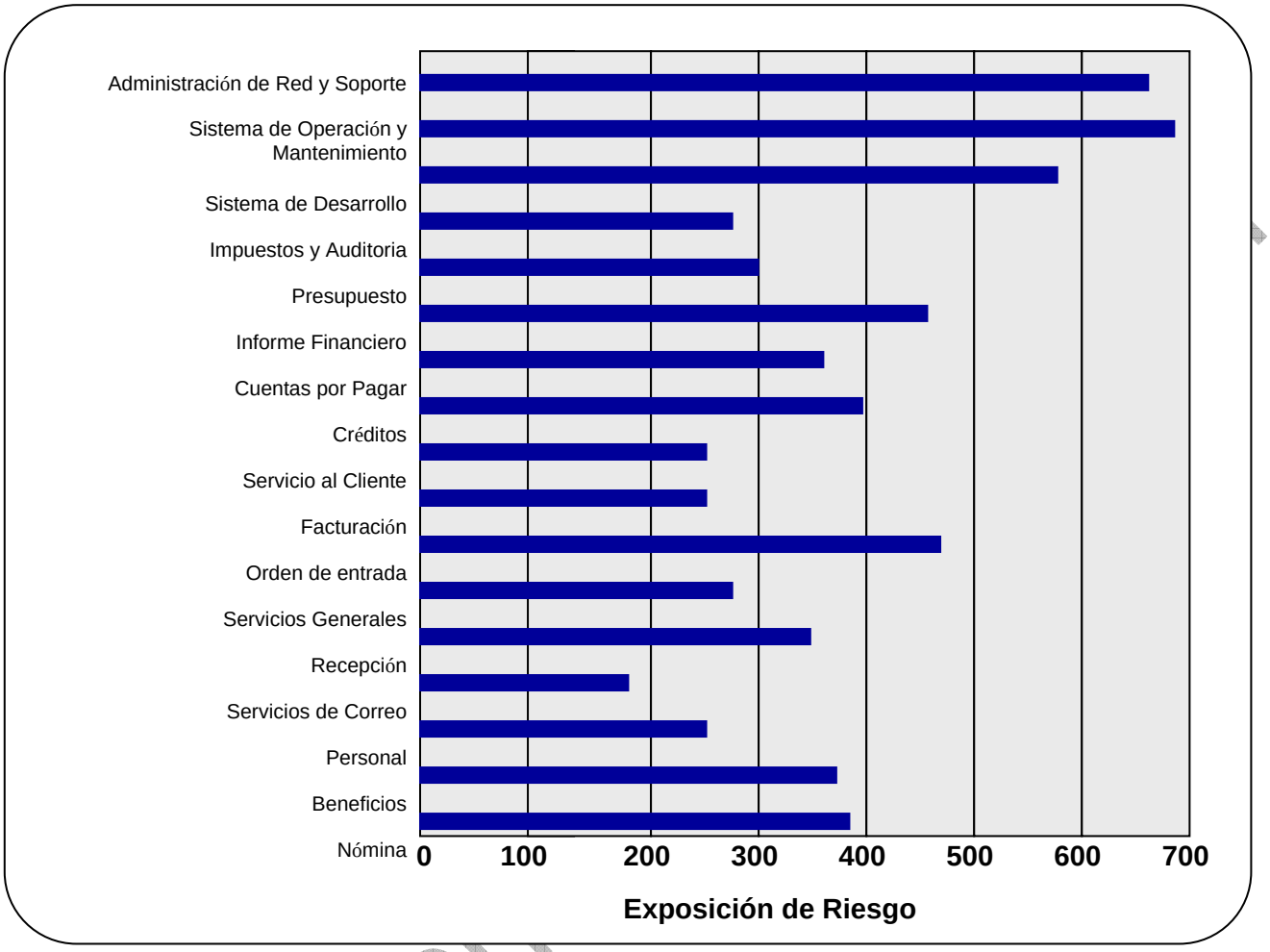
Riesgo, se tiene a nivel de ilustración como se procede para una empresa en particular a identificar la exposición al riesgo.
Los niveles de severidad se estiman en una escala de cuatro puntos. Empieza con **N/A**= No Aplica, **B**=Bueno, **M**=Moderada y **A**=Alta. Luego tenemos los grados de cobertura, los cuales van de un rango de 0 hasta 100, clasificados en seis categorías. Como se puede observar en la figura Nº 3, la exposición al riesgo se calcula de la siguiente manera: Nivel de severidad x (100% - % cobertura). Así tenemos en la figura Nº 3 que para la potencial amenaza de pérdida de personal, se estimó un grado de severidad Alto (100) y una cobertura de (60-79). Aquí siempre se escoge el valor más bajo (60). En este caso la exposición al riesgo es de 40. Una vez calculada la exposición al riesgo, los datos se pueden graficar y comunicarlos a grupos específicos para tomar decisiones sobre acciones. En la Figura Nº 4 tenemos a nivel de ilustración las exposiciones al riesgo de amenazas potenciales.

Figura Nº 4: Exposición al Riesgo por Amenazas Potenciales



En la figura Nº 5 tenemos graficada la exposición al riesgo por procesos en una empresa determinada.

Figura Nº 5: Exposición al Riesgo por Función Departamental



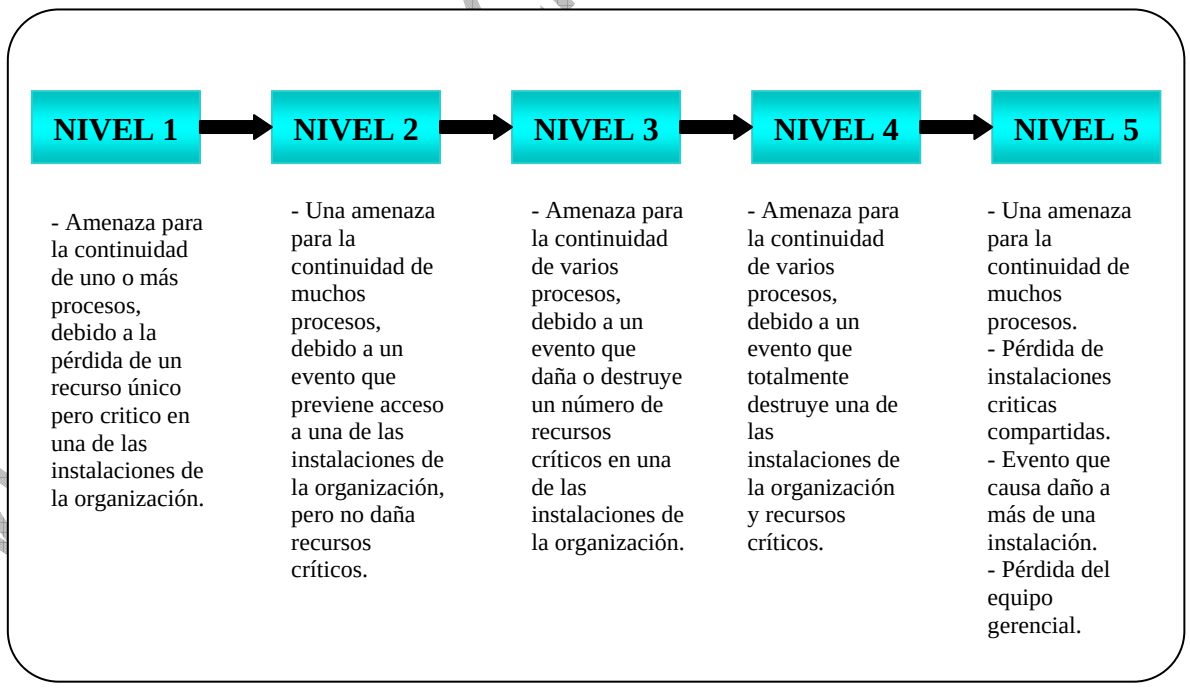
Una vez calculada la exposición al riesgo por cada amenaza potencial y por cada función organizacional en la empresa, se empieza a pensar en escenarios particulares de amenazas que la empresa pudiera tener y que pudiesen causar daño a las operaciones de la empresa.

(5) Determinar Escenarios de Amenazas.- Una vez calculada la exposición al riesgo por cada amenaza potencial y por funciones organizacionales en la empresa, se elaboran escenarios particulares de riesgos que la empresa pudiera tener y el daño que pudiesen causar a las operaciones de la empresa.

En la Figura Nº 6 se tiene la gráfica en la cual se han identificado para una empresa en particular, los distintos escenarios de amenazas que pudiesen presentarse. Los escenarios, que en este caso para la empresa han sido cinco, se han elaborado después de haber analizado los cálculos de exposición al riesgo.
Los escenarios de amenazas son clasificados desde los menos graves, que en este caso son el escenario 1, y hasta los más complejos que son el escenario 5. Es importante recalcar que para cada escenario identificado, se deben de elaborar según la

metodología del BCP, presentada en la Figura Nº 1 las fases III, IV y V. Vale decir para cada escenario hay que desarrollar las respectivas estrategias de business continuity, los planes de business continuity y los ensayos respectivos para cada plan.
A continuación se hará una breve descripción de cada uno de los escenarios de amenazas identificadas en la Figura Nº 6.
(a) Amenaza Nivel 1.- Aquí se identifica una amenaza para la continuación de una o mas funciones organizacionales en la empresa. Esta amenaza se debe a la pérdida de un recurso único pero crítico en una de las instalaciones de la organización (energía, sistemas de computación, archivos electrónicos, personal clave) **(b) Amenaza Nivel 2**.- En este escenario se identifica una amenaza para la continuidad de muchas funciones organizacionales, debido a un evento que previene acceso a una de las instalaciones de la organización, pero no daña ningún recurso crítico. **(c) Amenaza Nivel 3.-** Una amenaza para la continuidad de varias funciones organizacionales, debido a un evento que daña o destruye un número de recursos críticos en una de las instalaciones de la organización. Este escenario es una combinación de los niveles 1 y 2. **(d) Amenaza Nivel 4.-** Una amenaza para la continuidad de varias funciones organizacionales en la empresa, debido a un evento que totalmente destruye una de las instalaciones de la organización y sus respectivos recursos críticos. Esto podrían ser cosas como incendios o explosiones. **(e) Amenaza Nivel 5.-** Una amenaza para la continuidad de muchas funciones organizacionales e instalaciones múltiples debido a la pérdida de instalaciones críticas compartidas (energía, telecomunicaciones, sistemas centralizados) El evento causa daño y/o acceso restringido a más de una instalación en la organización (sismo, huracán, incidente ambiental). Se puede generar pérdida del equipo gerencial (accidente aéreo, bomba, terrorismo biológico).

FIGURA Nº 6: Escenario de Riesgos en la Organización



Conclusiones

La gestión del riesgo en la metodología del BCP es muy importante para, en base a la información recolectada, poder con bastante precisión identificar los varios escenarios de amenazas que pudiesen seriamente afectar las operaciones de la organización. La empresa debe invertir el tiempo necesario para jerarquizar los escenarios por “niveles de amenazas”. Esta evaluación de los escenarios se sustenta basados en el punto de qué operaciones serían interrumpidas, dado el grado de seriedad de las amenazas. El principal objetivo es entender, a un alto nivel, qué podría salir mal y qué funciones podrían ser afectadas.

Otro aspecto importante es entender que una vez identificadas las amenazas y las respectivas vulnerabilidades organizacionales, es fundamental establecer los respectivos controles para fortalecer las vulnerabilidades y minimizar la posibilidad de que el desastre penetre en la empresa y cause daño.

A lo largo del ensayo se ha hecho hincapié en que los escenarios de amenazas y su respectiva evaluación por su nivel de complejidad, son el insumo para poder desarrollar las fases III, IV y V dentro de la metodología del BCP. Por cada escenario se deben establecer estrategias de continuidad del negocio, los planes de continuidad requeridos y los ensayos.

Referencias Bibliográficas

(1) Hiles, Andrew, Barnes, Peter. Business Continuity Management. Wiley. 2002.

(2) Meredith,William "Business Impact Analysis" Business Continuity Management. Wiley. 2002.

(3) O´Hehir, Michael. "What is Business Continuity Planning Strategy?" Business Continuity Management, 2002.

(4) The Institute of Chartered Accountants in England & Wales. "Internal Control Guidance for Directors on the Combined Code", London, 1999.

(5) Leech, Tim. "Sarbanes-Oxley Sections 302 & 404. A White Paper Proposing Practical, Cost Effective Compliance Strategies" 2003, New York.

(6) Sheffi, Yossi. The Resilient Enterprise. M.I.T Press, 2005 Cambridge, Mass.

(7) Hiles, Andrew. Business Continuity: Best Practices. Rothstein Associates, Inc. 2004 Connecticut.

(8) Von Roessing, Rolf. Auditing Business Continuity: Global Best Practices Rothstein Associates, Inc.2002

(9) Barnes, James. A Guide to Business Continuity Planning. Wiley, London. 2001