ISSN 0798 1015

REVISTA ESPACIOS

HOME Revista ESPACIOS ÍNDICES A LOS AUTORES

Vol. 38 (Nº 54) Año 2017. Pág. 3

Modelo de evaluación de gestión de continuidad del negocio basado en la norma ISO 22301:2012

Assessment model business continuity management based on ISO 22301: 2012

Ernesto LOJÁN Granda 1; Johanna NAVARRO Espinosa 2; Christian CAGUA Vásquez 3

Recibido: 09/07/2017 • Aprobado: 01/08/2017

Contenido

RESUMEN:
El propósito de este artículo es exponer un nuevo modelo de evaluación cualitativa y cuantitativa del Sistema de Gestión de Continuidad del Negocio de acuerdo a la norma ISO 22301:2012, combinando niveles de madurez e indicadores clave de desempeño. El modelo resultante ha sido validado por expertos mediante grupo focal virtual, los resultados muestran que la norma ISO 22301:2012 debe complementarse con medición de efectividad de procesos de continuidad, enfocando al negocio como un conjunto de partes.
Palabras clave: ISO 22301:2012, Continuidad del Negocio, KPI

ABSTRACT:
The purpose of this article is to present a new qualitative and quantitative evaluation model of the Business Continuity Management System according to ISO 22301: 2012, combining maturity levels and key performance indicators. The resulting model has been validated by experts through a virtual focus group, the results show that ISO 22301: 2012 should be complemented by measures of effectiveness of continuity processes, focusing on the business as a set of parts.
Keywords: ISO 22301:2012, Business Continuity, KPI

1. Introducción

La norma internacional ISO 22301:2012 "Seguridad de la sociedad – Sistemas de gestión de la continuidad del negocio – Requisitos", establece el código de un conjunto de buenas prácticas para la Gestión de Continuidad del Negocio (Business Continuity Management, BCM por sus siglas en inglés). El estándar ISO 22301:2012 es la evolución de la norma internacional BS 25999 publicada en noviembre del 2007 por el British Standard Institution BSI, la cual estuvo

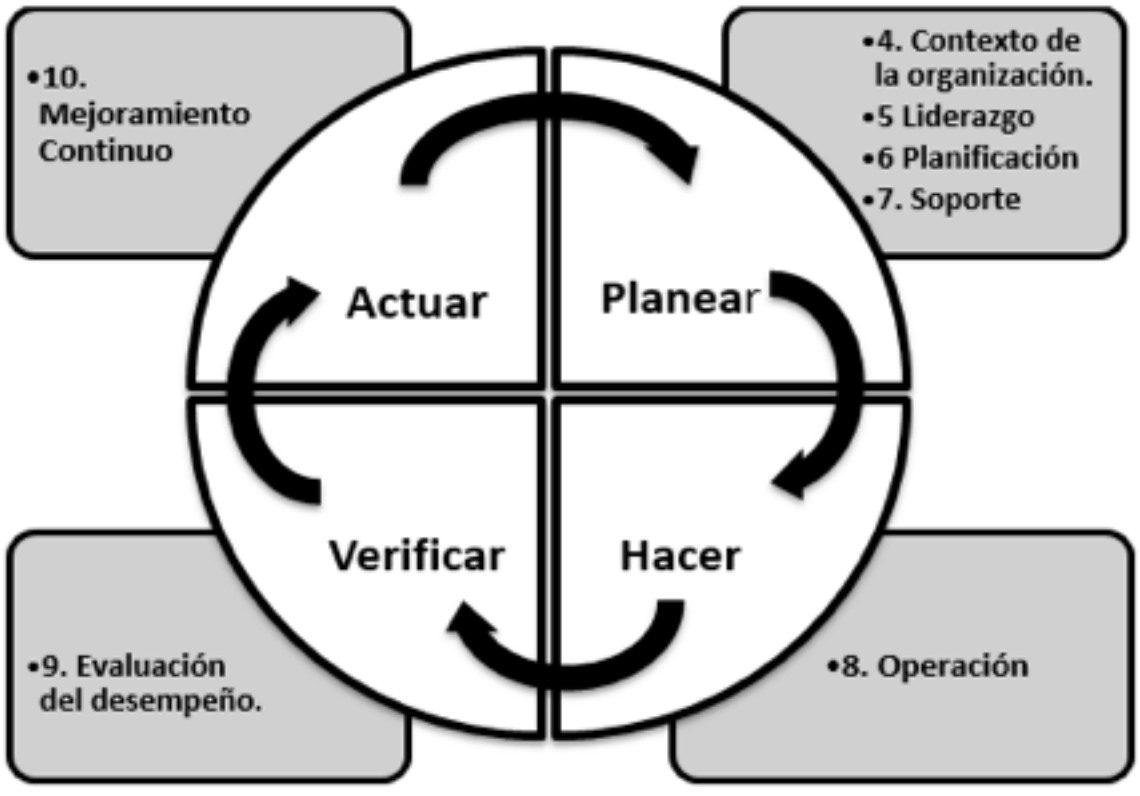
vigente para certificación hasta noviembre del año 2012 (Alexander, 2012; Sharp, 2012).

Los nuevos conceptos introducidos en la norma ISO 22301:2012 hacen énfasis en el liderazgo de la alta dirección mediante el aseguramiento de la compatibilidad del BCM con la dirección estratégica del negocio, la integración de los requerimientos de la norma en el plan de negocios y la comunicación de la importancia de una eficaz gestión de la continuidad del negocio. Así también, se han adicionado requerimientos y redefinido términos con el objetivo de simplificar y facilitar su interpretación.

No obstante las posibles diferencias entre las normas ISO 22301:2012 y BS 25999, ambas basan su estructura y lineamientos de buenas prácticas en el ciclo de Control de Deming PHVA (Planear, Hacer, Verificar y Actuar), el cual postula que los sistemas siempre están en estado de imperfección, por tanto, es necesario un proceso de mejoramiento continuo.

La Figura 1 muestra la relación entre las cláusulas generales de la norma ISO 22301:2012 y el ciclo PHVA. La idea central de un Sistema de Gestión de Continuidad del Negocio (Business Continuity Management System, BCMS por sus siglas en inglés) es potenciar la capacidad de respuesta organizacional frente a eventos catastróficos que interrumpan la normal provisión de productos y servicios, mediante la implementación de planes de acción denominados Planes de Continuidad del Negocio (Business Continuity Plan, BCP por sus siglas en inglés), salvaguardando el bienestar personal en primer lugar, la rentabilidad económica, imagen, reputación y las actividades de creación de valor.

Figura 1: El ciclo PHVA y la ISO 22301.



En virtud de lo antes expuesto, las organizaciones compiten por tener operativa su cadena de suministro, considerando todos los aspectos y recursos necesarios para evitar su paralización y en caso de ocurrir, lograr su oportuno restablecimiento.

Ahora bien, una organización podría asegurar que su BCP sea realmente eficaz mediante la realización periódica de simulacros en vivo; sin embargo, no es técnica ni económicamente factible realizar este tipo de pruebas con la frecuencia necesaria. Una encuesta realizada a empresas en EEUU (The Disaster Recovery Preparedness Council, 2014) revela que una gran parte de ellas no ha realizado pruebas a sus BCPs y que de aquellas que si las hicieron, la mayoría no las pasó satisfactoriamente.

Surge entonces la necesidad de contar con una herramienta metodológica que permita emitir una declaración concluyente sobre el grado de eficacia de los BCPs, en cualquier tipo y tamaño de organización, con la mayor exactitud posible y sin tener que recurrir a excesivas pruebas de

campo. La literatura describe dos métodos esenciales para medir el desempeño de eficacia y eficiencia de una estrategia o ciclo de vida: Un método se basa en la determinación y medición de Indicadores Claves de Desempeño (Key Performance Indicator, KPI por sus siglas en inglés) (Alemanni, Grimaldi, Tornincasa, & Vezzetti, 2008; Chorfi, Berrado, & Benabbou, 2015), y el otro se basa en la evaluación de la madurez de procesos.

El presente trabajo investigativo propone un nuevo modelo de evaluación del BCMS, combinando los métodos arriba descritos, esto es, KPIs integrados en un modelo de madurez basado en requisitos de cumplimiento del estándar ISO 22301:2012 y que ofrezca además una visión cuantitativa y cualitativa de la eficacia del BCMS.

1.1. Gestión de continuidad del negocio y estándares relacionados

Los primeros códigos formales relacionados con la preparación ante desastres datan de los años 50’s en Estados Unidos como Ley de Defensa Civil, la cual contempla medidas de acción en caso de ataque nuclear. Actualmente, y con el aporte de la investigación científica, el enfoque de defensa nuclear se traslada al de capacidad de respuesta organizacional contra todo tipo de riesgo (Tucker, 2014). Como derivación de este proceso de madurez se estandarizan procedimientos dirigidos a la prevención y recuperación de desastres.

Así también, el concepto de gestión de continuidad del negocio surge junto a los primeros centros de datos que programan los respaldos a cargo del departamento de TI; este antecedente explica porque aún hoy muchas organizaciones delegan el BCMS al área de TI (Tucker, 2014).

En tal sentido, Urbancová & Venclová (2013) señalan como áreas de aplicación del BCMS, no solamente la parte tecnológica sino también a la seguridad de los empleados, comunicaciones internas, renovación y mantenimiento de los procesos / funciones críticos y la gestión eficaz de la análisis de riesgos y crisis; justamente estas áreas son consideradas en las cláusulas 4, 5, 6 y 7 del estándar ISO 22301:2012 y corresponden a la fase planear del ciclo PHVA.

Adicionalmente, y sin embargo del beneficio aportado por la estandarización del BCMS en razón de proporcionar a las organizaciones una orientación para su desarrollo, medición y evaluación (Faertes, 2015; Stanciu, Stanciuc, Dumitrascu, Nistor, & Sirbu, 2012; Urbancová & Venclová, 2013), el problema de los gestores de la BCMS se traslada a la cuestión de elegir una normativa dentro un amplio conjunto de estándares disponibles, considerando además que las organizaciones desarrollan sistemas de calidad, medio ambiente, salud y la seguridad, finanzas, recursos humanos, tecnologías de la información y protección, así pues, el desafío consiste en lograr sinergia entre ellos (Stoichev, 2014).

En síntesis, un BCMS requiere de un enfoque holístico e integrado a otros sistemas de gestión (Bajgoric, 2014; Horvath, 2013). El estándar ISO 22301:2012 basa su estructura en el ciclo PHVA al igual que otros estándares de diverso propósito de gestión organizacional, por lo tanto, pueden integrarse sinérgicamente (Cortina, Mayer, Renault, & Barafort, 2014).

1.2. Fundamentos de catástrofe y recuperación.

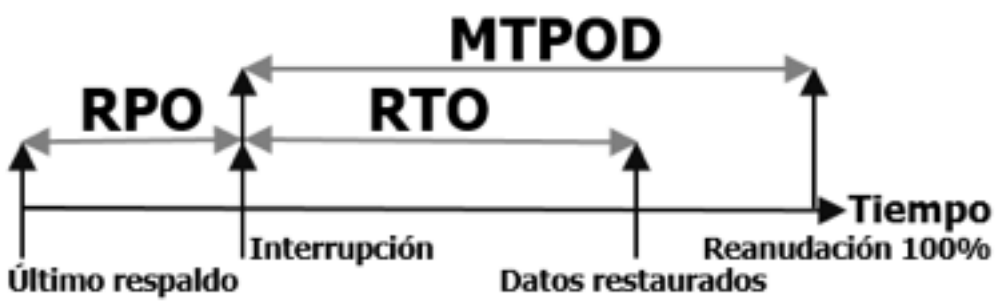
En primer lugar, se debe tener claro que BCP no es igual que Plan de Recuperación de Desastres (Disaster Recovery Plan, DRP por sus siglas en inglés), un BCP es una estrategia de mitigación, en otras palabras, un BCP facilita la recuperación rápida de las operaciones de negocio críticas e incluye a todas las partes o funciones de la organización (Gordon , 2013); el DRP en cambio, es un grupo de procedimientos de respuesta de emergencia relativos a la infraestructura tecnológica de información de la organización, DRP es un subconjunto del BCP. Concretamente, BCP proporciona a la organización el plan de negocios estratégico a largo plazo para la continuación después de una interrupción, mientras que un DRP es más táctico y proporciona un plan de corto plazo para hacer frente a las interrupciones específicas orientadas

a TI (Zhang & McMurray, 2013).

Así, un BCP es un plan de mitigación que utiliza el Análisis de Impacto del Negocio, (Business Impact Analysis, BIA por sus siglas en inglés) el cual determina procesos críticos que deben ser tomados en cuenta y la rapidez con que éstos deben recuperarse a fin de estar dentro del Tiempo Máximo Tolerable de Interrupción (Maximum Tolerable Period of Disruption, MTPOD por sus siglas en inglés), si este límite es sobrepasado, la empresa podría desaparecer del mercado (Boehmer, 2009; Faertes, 2015; Zambon, Bolzoni, Etalle, & Salvato, 2007).

Un factor del BIA, es el Tiempo Objetivo de Recuperación (Recovery Time Objective, RTO por sus siglas en inglés) el cual establece los límites temporales de toda la estrategia de gestión de continuidad de negocio, esto quiere decir que todas las unidades de negocio necesitan alinear la sensibilidad temporal de sus aplicaciones y procesos críticos dentro del RTO (Gordon, 2013). Por otra parte, el Punto de Recuperación Objetivo (Recovery Point Objective, RPO por sus siglas en ingles), se limita a la frecuencia de los respaldos de datos, es un elemento específico de la estrategia de continuidad del negocio (ver Figura2).

Figura 2: RPO y RTO vs tiempo.



Además de MTPOD, RTO y RPO otro factor resultante del BIA es el Objetivo Mínimo de Continuidad del Negocio (Minimum Business Continuity Objective, MBCO por sus siglas en inglés) es decir, un mínimo funcional en el suministro de bienes y servicios para alcanzar los objetivos de negocio (ISO 22301:2012, 2012).

En la Figura 3 se recrean los momentos t0 hasta t5 en un escenario de interrupción catastrófica. La curva representa la variación de la disponibilidad de productos o servicios. En t0 ocurre el evento de interrupción y la curva cae dramáticamente hasta t1, luego se activa el BCP. En t2 se invoca al DRP logrando que para t3 se alcance el MBCO. En el momento t5 las operaciones han retornado a su estado normal y la curva retoma la disponibilidad esperada.

Notar que un BCP tiene un alcance y duración mayor que el DRP, así como también el inicio de ambos no es simultáneo. Entre t0 y t4 se cumple que $RTO \leq MTPOD$.

1.3 Resiliencia Organizacional

La Figura 3 también muestra la ubicación del MTPOD dentro de un escenario típico de interrupción catastrófica, como ya se mencionó, MTPOD expresa el tiempo de inactividad máximo aceptable para garantizar la continuidad del negocio, indudablemente es un objetivo crucial para una organización no sobrepasar el MTPOD. Así, una organización debe tener el potencial para mantener y/o recuperar su capacidad funcional después de una interrupción (Hémond & Benoît, 2014); a esta habilidad organizacional se la denomina resiliencia. La resiliencia de un sistema puede mejorar aumentando la capacidad de adaptación del sistema (Dalziell & McManus, 2004). Esta capacidad adaptativa depende de:

1) El desarrollo de metodologías simples pero efectivas que las organizaciones pueden utilizar para evaluar su estrategia de resiliencia.

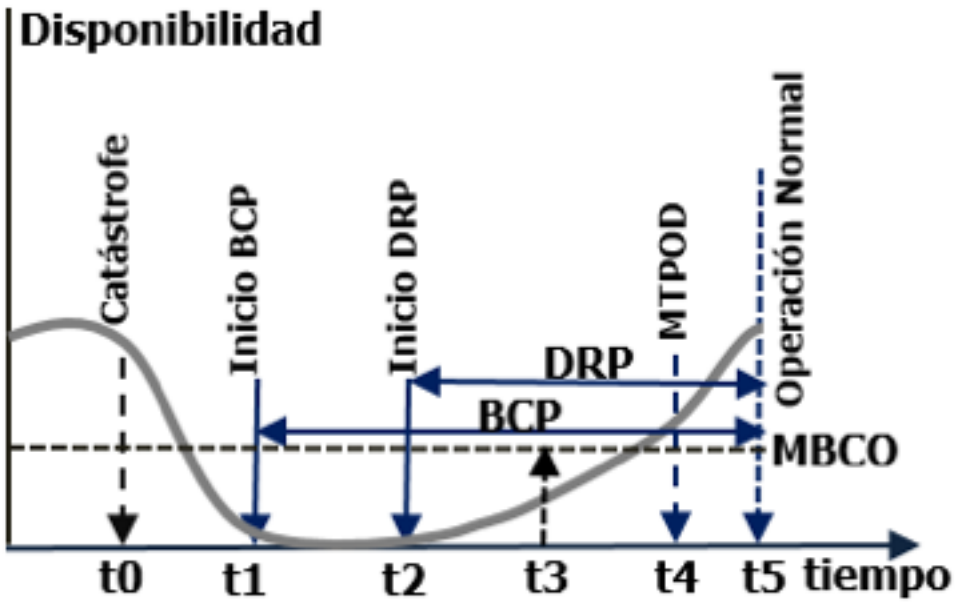
2) Una terminología común para facilitar el diálogo y el debate dentro de las organizaciones sobre procesos que demanden prioridad de recuperación.

3) Métricas para evaluar la resiliencia.

Además, Baba, Watanabe, Nagaishi, & Matsumoto (2014), consideran que a fin de fortalecer la resiliencia se deben crear BCP basados en áreas de aplicación. Cada área conforma un alcance y cuenta con su ciclo de gestión de continuidad propio, de esta manera, mejora la capacidad coordinada de manejo de desastres dentro de cada área objetivo.

Respecto al grado de resiliencia de la organización contra fluctuaciones causadas por eventos de interrupción, Dalziell & McManus (2004) y Hémond & Benoît (2014) consideran imprescindible evaluarla a través de KPI ya que dicha medición cuantifica su probabilidad de éxito.

Figura 3: Recreación de tiempos t0 a t4
en la recuperación de continuidad.



1.4 Indicadores Clave de Desempeño KPI

Un sistema de gestión puede ser medido por indicadores de eficacia y eficiencia. Un indicador es una variable sujeta a métrica, a su vez, un KPI está formado por un conjunto de indicadores generales que proporcionan una declaración cuantitativa importante sobre la capacidad de un sistema (Boehmer, 2009). Sin embargo, el conjunto de KPI debe ser el apropiado, ya que de otro modo la instantánea ofrecida puede mostrar una irrealidad (Alemanni, Grimaldi, Tornincasa, & Vezzetti, 2008). Si un KPI se desvía de su valor óptimo, pone en estado de vulnerabilidad al sistema; el tiempo que tarde en retomar su normalidad es función de resiliencia de la organización (Dalziell & McManus, 2004); por consiguiente, una desviación importante en un KPI conlleva acciones correctivas inmediatas (Calabró, Lonetti, & Marchetti, 2015),

Asimismo, Boehmer (2009), en su trabajo "Survivability and Business Continuity Management System According to BS 25999" construyó un modelo de evaluación de continuidad del negocio basado en la norma BS 25999 para predecir en un instante dado la probabilidad de supervivencia de una organización luego de una catástrofe, mediante un conjunto de ecuaciones estructurales involucrando KPIs generales y específicos. El modelo de Boehmer es una interesante e innovadora propuesta en cuánto a la incorporación de KPIs dentro de modelos de evaluación de gestión enmarcados en buenas prácticas, no obstante, el modelo de Boehmer no da una declaración cualitativa del BCMS o aspectos a mejorar, es decir, se limita a cuantificarlo únicamente.

Boehmer propone medir el desempeño de un BCMS mediante la siguiente ecuación:

$$Efk = Iex * Iop(BCP) * Iop(DRP) * Ico \quad (1)$$

Donde ***Efk***es la eficacia del BCMS representada por el producto de los siguientes KPIs: ***Iex,*** Existencia de controles de cumplimiento de la norma BS 25999, ***Iop(BCP)*** Grado de

cumplimiento de los BCP, ***Iop(DRP):*** Grado de cumplimiento de los DRP e ***Ico:*** Grado de cobertura del BIA y Análisis de Riesgos (AR) en recursos críticos.

La ecuación (1) mide cuan desviado está el objetivo de continuidad del negocio. Si ***Efk*** está muy cercano a 1, es un indicativo de alto grado de eficacia del BCMS, por el contrario, valores muy bajos o cercanos a 0 son un indicativo de necesidad urgente de mejora del BCMS. Para tener una explicación más detallada se sugiere revisar el artículo "Survivability and Business Continuity Management System According to BS 25999" de Wolfgang Boehmer (2009).

1.5 Modelos de Madurez

Los primeros modelos de madurez se aplican a dominios relacionados con la ingeniería de software; sin embargo, estos modelos también se relacionan con la gestión de la calidad aplicada a una amplia variedad de dominios, no solo de desarrollo de software (Wendler, 2012). Un modelo de madurez está formado por niveles jerárquicos y su propósito es brindar un marco de referencia cualitativo acerca del estado, importancia, potencialidades, requerimientos, y complejidad del objeto analizado (Wendler, 2012).

Posteriormente, modelos de madurez clásicos como CMMI o Spice (ISO/IEC15504) sirvieron como disparadores de un vasto proceso investigativo sobre desarrollo y validación de modelos de madurez, sin embargo, los trabajos investigativos se han limitado en gran mayoría a proponer modelos descriptivos o prescriptivos. Existe una carencia latente de modelos teóricamente reflexivos (Junttila, 2014; Wendler, 2012), un modelo reflexivo además de hacer el diagnóstico del sistema actual, se compara con las buenas prácticas y otras organizaciones.

Así mismo, un modelo de madurez puede ser enfocado desde dos perspectivas: por alcance de etapas y por desempeño de procesos; éste último enfoque permite una evolución continua e incremental de los mismos (Junttila, 2014; Koehler, Woodtly, & Hofstetter, 2015), la naturaleza iterativa de un modelo viabiliza mediciones de su progreso en el tiempo y no solamente su calidad en un instante específico (Woodhouse, 2008). De la misma manera, Lindström, Samuelsson, & Hägerfors (2010) y Randeree, Mahal, & Narwani (2012) coinciden en el hecho de que un BCMS está conformado por un conjunto de procesos iterativos, esto es, un modelo de madurez y un BCMS se comportan análogamente.

De ahí que, el modelo presentado por Junttila (2014) en "A Business Continuity Management Maturity Model" está construido mediante un riguroso proceso de desarrollo, reflexivo, iterativo, evaluado y validado, en el marco de la norma ISO 22301:2012. Junttila evaluó varios modelos de madurez de continuidad del negocio en cuanto a sus niveles, dimensiones y cobertura BCM de la norma ISO 22301:2012, seguidamente, mejoró el modelo seleccionado mediante la aplicación de la metodología de Ciencia del Diseño para la elaboración de modelos de madurez propuesto por Becker et al. (2009) en "Developing Maturity Models for IT Management – A Procedure Model and its Application".

El modelo de madurez de Junttila cubre dos dimensiones: el nivel y alcance de la madurez, este último indica el grado de cobertura del BCMS el cual podría comprender una unidad de negocio (Aislado), todas las unidades de negocio (Organización) y adicionalmente cubrir a las partes externas interesadas (Extendido). Así mismo, cada nivel de madurez cubre los requerimientos de norma ISO 22301:2012 en orden ascendente. Es importante notar que es posible tener un nivel de madurez por alcance, es decir, un departamento o unidad de negocio podría estar en nivel de madurez distinto a otras unidades de negocio dentro de la misma organización. El modelo final resultante se puede observar en la Figura 4.

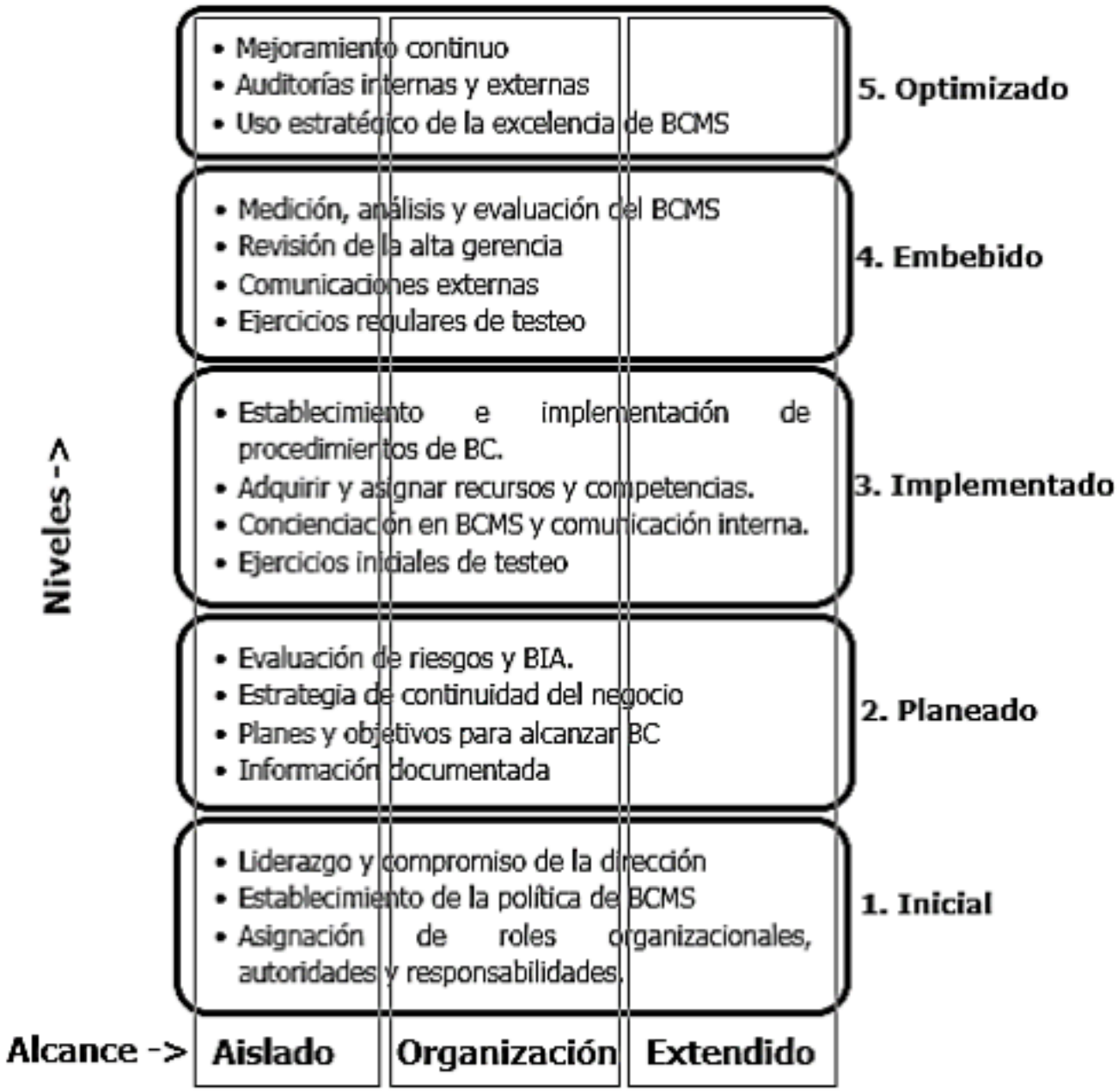


Figura 4: Modelo de madurez de BCM propuesto por Junttila, (2014).

Ahora bien, el modelo de Junttila no describe cómo hacer la medición, análisis y evaluación del BCMS, tampoco la norma ISO 22301:2012. En tal sentido, Lindström, Samuelsson, & Hägerfors (2010) critican al hecho de que las organizaciones confían demasiado en listas de verificación proporcionadas por los estándares. Otro punto a considerar es que tanto la implementación como la evaluación de madurez del BCMS deben ser ágiles.

Por estas razones, Lindström, Samuelsson, & Hägerfors (2010) proponen un modelo de madurez de capacidades o en escalera, el cual postula que cada nivel de madurez debe adaptarse al ambiente donde éste se aplica, esto es, los procesos de gestión de una unidad departamental difieren de los procesos de gestión de la organización como tal, por lo tanto, no es recomendable usar el mismo modelo de evaluación de madurez en todos los alcances del BCMS.

De hecho, el modelo de Lindström, Samuelsson, & Hägerfors (2010) avala la aseveración de autores como Baba, Watanabe, Nagaishi, & Matsumoto (2014); Dalziell & McManus (2004) y Hémond & Benoît (2014) quienes estiman que la resiliencia depende directamente de la capacidad adaptativa de las unidades departamentales o funciones de la organización, donde cada una de ellas actúa por separado pero de manera coordinada con su propio ciclo de gestión de continuidad.

2. Metodología

El objetivo del presente artículo es exponer un nuevo modelo de evaluación del BCMS, de carácter reflexivo, basado en la norma 22301:2012, para lo cual se seguirán los siguientes pasos:

1) Revisión de literatura relevante sobre modelos existentes de madurez de sistemas y KPI.
2) Construcción de modelo prototipo de evaluación de BCMS basado en los resultados de 1)
3) Validación de modelo prototipo resultado de 2) mediante la técnica Grupo Focal Virtual.
4) Presentación de resultados.

2.1 Revisión de literatura relevante.

Con el fin de otorgar validez de contenido al presente trabajo investigativo, se realizó la búsqueda de publicaciones relevantes sobre modelos de madurez de evaluación de BCMS que incorporen la norma ISO 22301 o al menos algún estándar de buenas prácticas, así como también artículos relacionados con la implementación de KPIs.

2.2 Construcción de modelo prototipo de evaluación de BCMS

La construcción del modelo prototipo se basa en los trabajos de Boehmer (2009); Junttila (2014) y Lindström, Samuelsson, & Hägerfors (2010). Luego, el modelo prototipo resultante debe responder las siguientes cuestiones fundamentales:

> ¿Se adapta a la organización, independientemente de su tipo y tamaño
>
> ¿Se enmarca dentro de un estándar reconocido internacionalmente de buenas prácticas?
>
> ¿Permite evaluar la resiliencia organizacional?

El modelo resultante, descrito en la Figura 5 separa en 2 columnas el BCMS de modo que a nivel departamental se desarrollen planes de continuidad de manera ágil enfocados en procesos que mejoren la capacidad de respuesta (Kit de choque) a eventos específicos y propios de su ámbito operativo; mientras, a nivel organizacional se maneja el BCMS como un proyecto, en el cual se delega su realización a la alta dirección y mandos gerenciales, no obstante, esto no supone un aislamiento comunicacional, es vital que ambas columnas trabajen coordinadamente.

Un aspecto a resaltar de este modelo es cómo se identifica a cada nivel, estos se enumeran ordinalmente, sin calificarle como mejor o menos bueno. Esta designación se fundamenta en una realidad inobjetable: declarar un nivel más alto de madurez no implica necesariamente tener mejores procesos, es necesaria su evolución incremental y continua ya que finalmente, procesos con capacidades fortalecidas harán más resiliente a la organización (Koehler, Woodtly, & Hofstetter, 2015); de ahí la necesidad de métricas para evaluar su desempeño (Dalziell & McManus, 2004).

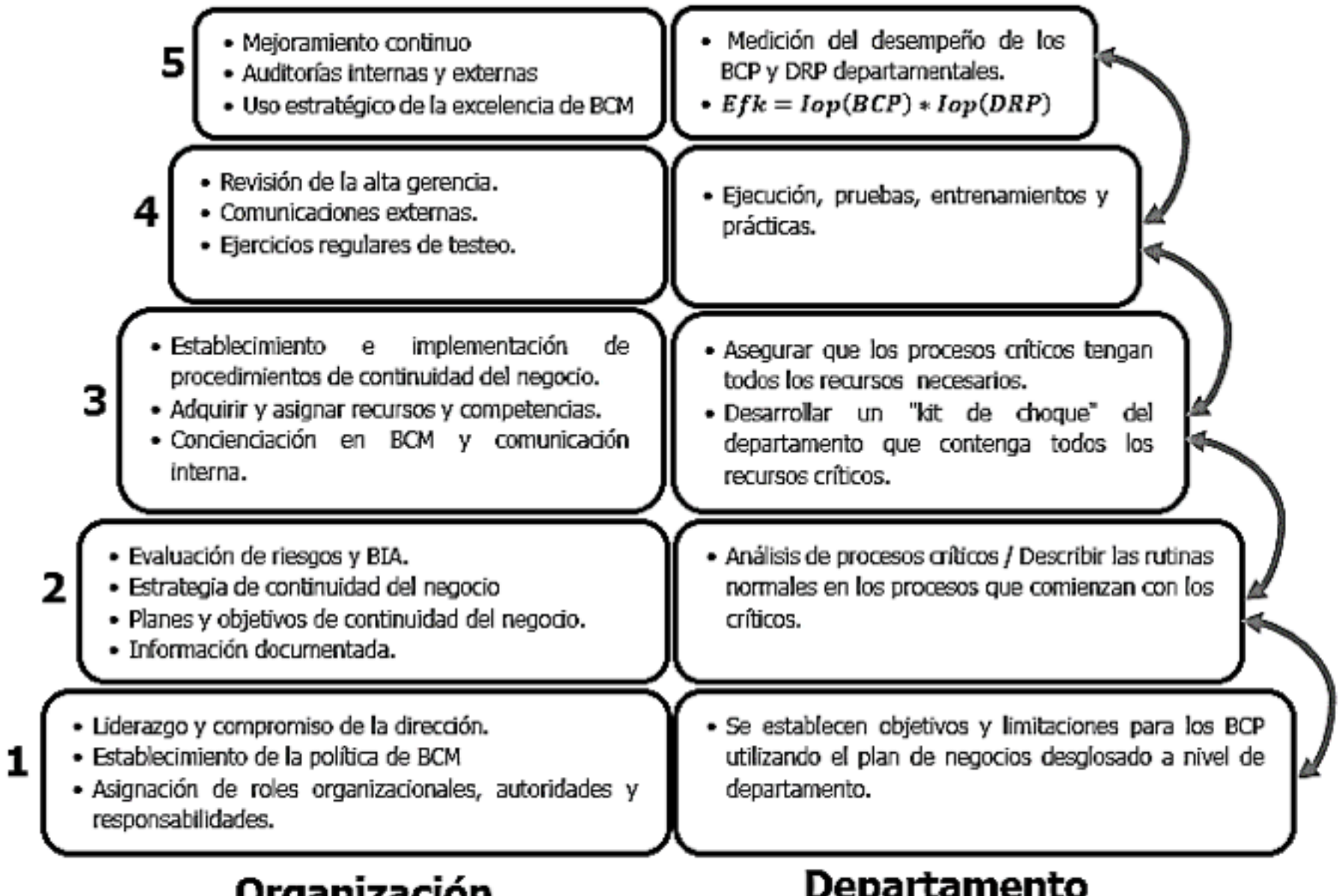


Figura 5: Modelo prototipo propuesto de evaluación del BCMS.

Luego, en el nivel "Medición del desempeño de los BCP y DRP departamentales", se usan KPIs que con base en la idea de Boehmer (2009), vienen definidos por la ecuación (1), sin embargo, ***Iex*** y ***Ico*** no son necesarios ya que son considerados dentro de la etapa de proyecto del modelo propuesto, por lo tanto, el indicador de eficacia ***Efk*** se redefine como:

$$Efk = Iop(BCP) * Iop(DRP) \quad (2)$$

$$\text{Donde } Iop(BCP) = \frac{\sum_{i=1}^{n} C\lambda i(BCP) - \sum_{j=1}^{m} NoCj(BCP)}{\sum_{i=1}^{n} C\lambda i(BCP)} \quad (3)$$

$\sum_{i=1}^{n} C\lambda i(BCP)$ Representa la sumatoria de medidas adoptadas y $\sum_{j=1}^{m} NoCj(BCP)$ representa la sumatoria de medidas faltantes o inexistentes tomando como referencia la evidencia documental que de la ejecución, pruebas, entrenamientos y prácticas del BCP resultaran.

Análogamente, $Iop(DRP)$ se calcula:

$$Iop(DRP) = \frac{\sum_{i=1}^{n} C\lambda i(DRP) - \sum_{j=1}^{m} NoCj(DRP)}{\sum_{i=1}^{n} C\lambda i(DRP)} \quad (4)$$

Por ejemplo, un ***Efk*** calculado mediante (2) muy cercano o igual a 1 es un indicativo de procesos de continuidad de alto grado de eficacia y por ende de resiliencia organizacional. Por el contrario, un ***Efk*** cercano a 0 indica desviaciones en los objetivos de los planes de continuidad en cuyo caso, es necesario adoptar acciones correctivas inmediatas, o dicho de otra forma: es necesario iterar los procesos críticos de negocio.

Con respecto al alcance Extendido (ver Figura 4) no se ha incluido en el modelo propuesto. La razón fundamental es que requerir detalles sobre BCPs a las partes interesadas externas

podría ser un trabajo complejo o no factible. En este caso, la certificación de requisitos normativos a través de un tercero es lo recomendado.

2.3 Validación de modelo prototipo

Con el objetivo de validar el modelo expuesto en esta sección, se emplea la técnica de recopilación de información de Grupo Focal, la cual se define como una entrevista grupal semi-estructurada centrada en un tema específico, facilitada y coordinada por un moderador para generar datos cualitativos (Escobar & Bonilla-Jimenez, 2011; Sim, 1998).

La idea central es categorizar las experiencias de practicantes de la BCMS para canalizarlas en favor de un modelo mejorado y validado. Sin embargo, la técnica de Grupo Focal cara a cara de acuerdo a Sim (1998); Sweet (2001) y Turney & Pocknee (2005), tiene los siguientes puntos en contra:

Clasificar la información, la cual se toma de la grabación de audio y notas tomadas a mano, se torna complicada el momento de identificar al autor, ya que es necesario citar las intervenciones.

Derivado de lo anterior, la transcripción de datos es lenta.

Si el entrevistado vive en otra localidad geográfica impide su participación.

Por otra parte, existe el riesgo de que los entrevistados se sientan intimidados al emitir su criterio debido a la presencia de un entrevistado dominador

Una técnica alternativa al Grupo Focal y que soluciona los problemas mencionados en el apartado anterior es el Grupo Focal Virtual, la cual se realiza mediante plataformas web de aprendizaje colaborativo virtual tales como Blackboard, WebEx, Google Hang-Outs o Jigsaw por mencionar algunas. Ciertamente, habrá situaciones donde es necesaria la interacción cara a cara con los participantes, en especial donde es fundamental para el investigador observar gestos o actitudes, no obstante, para el propósito de este estudio no es necesario.

Para efectos de validar el modelo propuesto se convoca a expertos que cuentan con certificaciones PMP, CISA, CISM, CGEIT, CRISC, MBCP, CICA, ISO 22301 LI, ISO27001 LA, ITIL, COBIT 5, ISO9001 LA, con vastos años de experiencia en desarrollos, implementación y auditorías a sistemas de gestión de continuidad de negocio y recuperación de desastres en firmas reconocidas internacionalmente. El foro de discusión en línea se realiza de manera síncrona utilizando Google Hang-Outs y Apowersoft Free Online Screen Recorder para registrar el audio. Las preguntas realizadas se agregan en la sección anexos de este paper. La identidad de los participantes se omite por asuntos de confidencialidad.

---

3. Resultados

El modelo propuesto tuvo aprobación general por parte de los expertos. No obstante, luego de la reducción y categorización de opiniones, se identificaron dos aspectos a mejorar:

1) Es necesario describir y detallar cada uno de los niveles del modelo propuesto.

2) Se debe detallar KPIs intervinientes en la ecuación de eficacia del BCMS.

Por lo tanto, al modelo final de evaluación de BCM basado en la norma ISO 22301:2012 agrega al modelo prototipo original, las tablas 1 y 2 como respuesta al punto 1:

ALCANCE ORGANIZACIONAL		
NIVEL DE MADUREZ	**DESCRIPCIÓN**	**ACTIVIDADES**
1	Se establecen políticas, roles,	Creación del comité ejecutivo y

	responsabilidades y alcances del BCMS. La alta administración demuestra su compromiso y liderazgo en la ejecución del programa BCMS.	administrativo para la BCM. Reconocimientos de los primeros procesos empresariales. Determinación del apetito de riesgo de la organización y requerimientos legales y regulatorios.
2	Se realizan los estudios BIA y RA. Sus resultados se utilizan para la estrategia y objetivos de continuidad del negocio que se plasman en planes para alcanzar esos objetivos, sin embargo, estos planes son provisionales ya que deben ser refinados posteriormente.	Realización de RA y BIA. Realización de BCPs preliminares.
3	En este punto la organización ha establecido e implementado BCPs, se han adquirido y asignado los recursos y competencias necesarios para implementar la estrategia seleccionada en el nivel anterior. Todo el personal de la organización toma conciencia del BCMS.	Asignación de recursos. Establecimiento del plan de comunicación, entrenamiento y concienciación de empleados. Pruebas preliminares de BCPs
4	En este nivel el programa de BCM se enfoca más como proceso que como proyecto. La alta dirección realiza la revisión de la consistencia de los BCPs con los objetivos de continuidad del negocio. Se realizan las primeras pruebas y testeos de los BCPs.	Pruebas integrales de BCMS.
5	En este nivel se determinan oportunidades de mejora a los BCPs existentes. En este nivel la organización puede usar su mejorada capacidad resiliente como ventaja competitiva y comercial.	Realización de auditorías internas y externas a intervalos planificados.

Tabla 1: Descripción del alcance Organizacional

ALCANCE DEPARTAMENTO		
NIVEL DE MADUREZ	**DESCRIPCIÓN**	**ACTIVIDADES**
1	La alta administración y la jefatura de departamento establecen objetivos y limitaciones para las medidas de continuidad del negocio de acuerdo al	Establecimiento de roles y propietarios de procesos de continuidad. Creación del comité de continuidad.

	contexto organizativo.	
2	En este nivel se analizan los procesos críticos que resultan del BIA.	Creación de mapas de procesos detallados para reconocer las rutinas de los procesos que componen el alcance del BCMS.
3	El "kit de choque" consiste en establecer las estrategias de continuidad (BCP y DRP departamental) y asegurar que para cada proceso crítico detectado en el nivel anterior existan los recursos necesarios.	Determinar el personal de gestión, sistemas de TI / herramientas utilizadas y lista de proveedores, socios de negocios, toda la información de contacto necesaria. Ejecución de plan de entrenamiento y concienciación.
4	Ejecución, pruebas, entrenamientos y prácticas	Pruebas de escritorio y de campo programadas de aplicación de DRP y BCP.
5	El valor resultante de Efk es un indicativo del grado de efectividad de los BCP y DRP. Ahora el departamento ha establecido las medidas de continuidad del negocio necesarias y necesita mantenerlas.	Aplicación de ecuaciones (2), (3) y (4).

Tabla 2: Descripción del alcance Departamental.

Finalmente, La tabla 3 responde al punto 2 (Se debe detallar KPIs intervinientes en la ecuación de eficacia del BCMS) el cual está vinculado al nivel 5 del modelo de alcance departamental, es decir, a la aplicación de las ecuaciones (3) y (4). Es importante mencionar que los KPIs de tabla 3 son referenciales, esto es, cada organización debe definir los KPIs que considere apropiados y alineados con sus objetivos de continuidad del negocio.

CLASE	KPIs específicos
ENTRENAMIENTO Y CAPACITACIÓN	Cumplimiento de programas de concienciación.
	Cumplimiento de programas de capacitación.
	Entrenamiento DRP y BCP.
	Entrenamiento a intervalos regulares.
EJECUCIÓN	RTO <= MTPOD
	RPO al 100%
	MBCO alcanzado por debajo del 50% del MTPOD
	SLA (Acuerdo de Nivel de Servicio) cumplido.

	OLA (Acuerdo de Nivel Operacional) cumplido.
	Ejercicios basados en escenarios.
	Producción de reportes post-ejercicios para mejoras.
	Ejercicios realizados a intervalos planificados.

Tabla 3: KPIs específicos sugeridos.

4. Conclusiones

Los hallazgos de Boehmer (2009), Junttila (2014) y Lindström, Samuelsson, & Hägerfors (2010) establecen que la eficacia de la estrategia de continuidad del negocio no depende únicamente de una lista de verificación proporcionada por un estándar, sino que también se debe medir el desempeño de los procesos de continuidad dimensionándolos por alcance a fin de garantizar la resiliencia y mejoramiento continuo.

Sin embargo, la estandarización juega un papel crucial en la orientación de la gestión del proyecto de continuidad del negocio. No se puede afirmar que un BCMS se ha implantado correctamente sin haberlo sometido a un riguroso proceso de normalización de buenas prácticas bajo el aval de una normativa internacionalmente reconocida, en este caso, la norma ISO 22301:2012.

Consiguientemente, la estrategia de continuidad del negocio debe integrar tanto la normalización de sus prácticas de continuidad del negocio como el uso de KPIs para evaluar su efectividad. De tal modo, para la gestión del proyecto de certificación del BCMS se deben realizar mediciones de efectividad de BCPs y DRPs mediante el uso KPIs, lo cual garantiza mejoramiento continuo y por ende un mejor factor de resiliencia.

Por otro lado, la división de la organización en silos o unidades de negocio procura una ágil implementación y evaluación de desempeño de los BCP y DRP, sin que esto afecte la cohesión del BCMS empresarial.

El modelo de evaluación del BCMS presentado en este trabajo investigativo se construyó iterativamente sobre la base de los modelos de Junttila (2014), Lindström, Samuelsson, & Hägerfors (2010) y Boehmer (2009), reuniendo en un solo producto lo mejor de cada uno y demostrando que es posible juntar las potencialidades de la gestión de proyectos de continuidad del negocio en el marco de la norma ISO 22301:2012.

Finalmente, debido al nivel exploratorio del presente artículo, el modelo resultante es conceptual y por tanto su validez es teórica. Un siguiente momento dentro de esta línea investigativa sugiere la implementación y prueba del modelo propuesto en una organización real bajo la modalidad de la investigación-acción, cuyos resultados pueden arrojar insumos para una siguiente iteración del modelo actual.

Referencias bibliográficas

Alemanni, M., Grimaldi, A., Tornincasa, S., & Vezzetti, E. (2008). Key performance indicators for plm benefits evaluation: The alcatel alenia space case study. *Computers in Industry*, 833–841.

Alexander, A. (2012). Nuevo estándar internacional en continuidad del negocio ISO. *Gestión*, 1-23.

Baba, H., Watanabe, T., Nagaishi, M., & Matsumoto, H. (2014). Area Business Continuity Management, a new opportunity for building economic resilience. *ScienceDirect*, 296 – 303.

Bajgoric, N. (2014). Business continuity management: a systemic framework for

implementation. *Kybernetes*, 156-177.

Boehmer, W. (2009). Survivability and Business Continuity Management System According to BS 25999. *IEEE*, 142-147.

Calabró, A., Lonetti, F., & Marchetti, E. (2015). KPI Evaluation of the Business Process Execution through Event Monitoring Activity. *IEEE*, 169-176.

Chorfi, Z., Berrado, A., & Benabbou, L. (2015). Selection of Key Performance Indicators for Supply Chain Monitoring using MCDA. *IEEE Explore*, 1-6.

Cortina , S., Mayer , N., Renault , A., & Barafort, B. (2014). Towards a Process Assessment Model for Management System Standards. En A. Mitasiunas , T. Rout, R. O'Connor , & A. Dorling, *Software Process Improvement and Capability Determination* (págs. 36-47). Luxemburgo: Springer International Publishing.

Dalziell, E., & McManus, S. (2004). Resilience, Vulnerability, and Adaptive Capacity: Implications for System Performance. *International Forum for Engineering Decision Making (IFED)*, 1-17.

Escobar, J., & Bonilla-Jimenez, F. (2011). Grupos Focales: Una Guía Conceptual Y Metodológica. *Cuadernos Hispanoamericanos de Psicología*, 51-67.

Faertes, D. (2015). Reliability of Supply Chains and Business Continuity Management. *Procedia Computer Science*, 1400 – 1409.

Gordon , A. (2013). *Official (ISC)2® Guide to the ISSAP® CBK, Second Edition.* New York: Auerbach Publications.

Hémond, Y., & Benoît , R. (2014). Assessment process of the resilience potential ofcritical infrastructures. *Int. J. Critical Infrastructures*, 200-217.

Horvath, G. K. (2013). Information Security Management for SMEs: Implementating and Operating a Business Continuity Management System (BCMS) Using PDCA Cycle. *FIKUSZ*, 133-141.

ISO 22301:2012. (2012). Societal security — Business continuity management systems — Requirements. Switzerland.

Junttila, J. (2014). A Business Continuity Management Maturity Model The Search for an ISO 22301 Compliant BCM Maturity Model. *Master´s Thesis in Information Systems Science*. Turku, Finlandia.

Koehler, J., Woodtly, R., & Hofstetter, J. (2015). An impact oriented maturity model for IT-based case management. *Information Systems ELSEVIER*, 278–291.

Lindström, J., Samuelsson, S., & Hägerfors, A. (2010). Business continuity planning methodology. *Disaster Prevention and Management: An International Journal*, 243 - 255.

Randeree, K., Mahal, A., & Narwani, A. (2012). A business continuity management maturity model for the UAE banking sector. *Business Process Management Journal*, 472 - 492.

Sharp, J. (24 de Agosto de 2012). *www.bsigroup.com.* Obtenido de https://www.bsigroup.com/Documents/iso-22301/resources/BSI-BS25999-to-ISO22301-Transition-UK-EN.pdf

Sim , J. (1998). Collecting and analysing qualitative data: issues raised by the focus group. *Journal of Advanced Nursing*, 345-352.

Stanciu, S., Stanciuc, N., Dumitrascu, L., Nistor, C., & Sirbu, R. (2012). Modern Approach to Business Continuity Management in Food. *Risk in Contemporary Economy*, 71-74.

Stoichev, K. (2014). The role of business continuity management in the business management system. *Science Journal of Business and Management*, 97-102.

Sweet, C. (2001). Designing and conducting virtual focus groups. *Qualitative Market Research: An International Journal*, 130 - 135.

The Disaster Recovery Preparedness Council. (2014). *Disaster Recovery Preparedness Benchmark Survey.* Obtenido de https://drbenchmark.org/wp-content/uploads/2014/02/ANNUAL_REPORT-DRPBenchmark_Survey_Results_2014_report.pdf

Tucker, E. (2014). *Business Continuity from Preparedness to Recovery: A Standards-Based Approach.* Oxford: Butterworth-Heinemann.

Turney, L., & Pocknee, C. (2005). Virtual Focus Groups: New Frontiers in Research. *International Journal of Qualitative Methods*, 32-43.

Urbancová, H., & Venclová, K. (2013). Importance of Knowledge Continuity in Business Continuity Management. *Acta Univ. Bohem. Merid.*, 3-13.

Wendler, R. (2012). The maturity of maturity model research: A systematic mapping study. *Information and Software Technology ELSEVIER*, 1317–1339.

Woodhouse, S. (2008). An ISMS (Im)-Maturity Capability Model. *IEEE 8th International Conference on Computer and Information Technology Workshops*, 242-274.

Zambon, E., Bolzoni, D., Etalle, S., & Salvato, M. (2007). A Model Supporting Business Continuity Auditing & Planning in Information Systems. *Second International Conference on Internet Monitoring and Protection (ICIMP 2007)*, 1-9.

Zhang, X., & McMurray, A. (2013). Embedding Business Continuity and Disaster Recovery within Risk Management. *World Journal of Social Sciences*, 61 – 70.

Anexos

ANEXO 1: Preguntas Grupo Focal Virtual.

Temática: Utilidad del modelo propuesto.

1. ¿Está Ud. de acuerdo con la terminología empleada en el modelo propuesto?

2. ¿A su juicio, el número de niveles propuesto es el indicado? ¿O quizá deban aumentarse o disminuirse?

3. ¿A su juicio, la dimensión ALCANCE, se justifica? ¿Quizá vuelve más complicado el modelo incluir esta dimensión?

4. ¿Cree Ud. que el presente modelo podría servir como marco guía para la implementación del BCMS?

5. ¿A su juicio, es acertado que cada unidad de negocio maneje un ciclo de gestión de continuidad propio en lugar del ciclo de toda la organización?

6. ¿Considera Ud. que el modelo propuesto puede ser implantado en una organización, independientemente de su tamaño, misión y visión?

Temática: Aplicabilidad del modelo propuesto.

7. ¿Cuál es el obstáculo más importante que Ud. considera podría aparecer al aplicar el modelo propuesto?

8. ¿Es posible simplificar aún más el modelo propuesto, cómo?

9. ¿Es posible volver más ágil el modelo propuesto? ¿Que se podría agregar o quitar con tal finalidad?

10. ¿Del modelo propuesto, qué nivel o alcance es el más complicado de aplicar?

11. ¿Podría hacer una comparativa general del modelo de evaluación de continuidad del negocio usado por Ud. en su organización y el modelo propuesto en esta presentación?

Temática: Cobertura ISO 22301:2012 del modelo propuesto.

12. ¿La descripción de la norma es clara en el modelo propuesto?

13. ¿Se cubre la totalidad de la norma en el modelo propuesto?

14. ¿De acuerdo a su criterio, movería o agruparía de un modo distinto los ítems de la norma dentro del modelo propuesto?

15. ¿La norma está repartida en 5 niveles de madurez, considera Ud. necesario disminuir o quizá aumentar la cantidad de niveles de manera que la norma se cubra de la mejor manera?

16. ¿La relación entre las columnas ORGANIZACIONAL y DEPARTAMENTO respecto de la norma es clara?

Temática: Indicadores clave de desempeño del modelo propuesto.

17. ¿Considera UD. que el conjunto de KPI seleccionado es el apropiado?

18. ¿Agregaría Ud. algún KPI adicional en algún otro nivel o alcance del modelo propuesto?

19. ¿El KPI del modelo propuesto ofrece una medida de la eficacia de procesos de continuidad del SGCN, a su juicio, considera esto como una métrica válida para evaluar la resiliencia organizacional?

20. ¿La cobertura de aspectos normativos como análisis de riesgos y BIA debería evaluarse también mediante KPIs también?

21. ¿Alguna sugerencia en particular respecto del modelo propuesto?

---

1. Ingeniero en Sistemas, Magister en Auditoria de Tecnologías de la Información UEES-ESAI Business School. Consultor de TI. Guayaquil, Ecuador. elojan@uees.edu.ec

2. Ingeniero en Sistemas , Magister en Auditoria de Tecnologías de la Información. Coordinadora de la USG y Docente a tiempo completo de la Universidad ECOTEC. Guayaquil, Ecuador. jnavarro@ecotec.edu.ec

3. Ingeniero en Sistemas Computacionales. Magíster en Auditoría de Tecnologías de la Información. IT Manager Grupo Citikold christian.cagua@uees.edu.ec

---

Revista ESPACIOS. ISSN 0798 1015
Vol. 38 (Nº 54) Año 2017

[Index]