TESIS DE POSTGRADO

Modelo de Evaluación de Gestión de Continuidad del Negocio basado en la norma ISO 22301:2012

Propuesta de artículo presentado como requisito parcial para optar al título de:

Magíster en Auditoría de Tecnologías de la Información

Por el estudiante:

Ernesto Max LOJÁN GRANDA

Bajo la dirección de:

Raúl GONZÁLEZ CARRIÓN

Universidad de Especialidades Espíritu Santo
PostGrado Online.
Guayaquil - Ecuador
Febrero de 2017

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 Max LOJÁN GRANDA[1]
Raúl V. GONZÁLEZ CARRIÓN [2]

Resumen

El propósito de este paper 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, dimensionado a nivel organizacional y departamental. El modelo propuesto ha sido construido con base a referencias de modelos relevantes de evaluación de gestión de continuidad del negocio combinando aspectos tales como niveles de madurez, estándares de gestión de continuidad del negocio e indicadores clave de desempeño. El modelo resultante ha sido validado por expertos mediante grupo focal virtual y puede servir además como guía metodológica para la implementación ágil de sistemas de gestión de continuidad del negocio en organizaciones de cualquier tipo o tamaño, enfatizando la resiliencia organizacional y efectividad de procesos de continuidad como pilares fundamentales de la estrategia de recuperación de la cadena de suministro de bienes y servicios. Este estudio muestra que la norma ISO 22301:2012 es un excelente marco referencial de implementación de continuidad del negocio, sin embargo, debe complementarse con un sistema de indicadores clave de desempeño, agrupados coordinadamente, a fin de lograr una organización resiliente ante eventos catastróficos.

Palabras clave:	ISO 22301:2012; BCMS, Continuidad del Negocio; KPI; modelos de madurez, resilencia.

Abstract

The purpose of this paper is to present a new qualitative and quantitative evaluation model of the Business Continuity Management System according to ISO 22301: 2012, dimensioned at organizational and departmental level. The proposed model has been constructed based on references from relevant business continuity management assessment models combining aspects such as maturity levels, business continuity management standards and key performance indicators. The resulting model has been validated by experts through a virtual focus group and can also serve as a methodological guide for the agile implementation of business continuity management systems in organizations of any type or size, emphasizing the organizational resilience and effectiveness of continuity processes Fundamental pillars of the strategy of recovery of the supply chain of goods and services This study shows that ISO 22301: 2012 is an excellent frame of reference for business continuity implementation, however, it should be complemented by a system of key performance indicators, coordinated in order to achieve a resilient organization in the face of catastrophic events

Key words	ISO 22301: 2012; BCMS, Business Continuity; KPI; maturity models, resilience
Clasificación JEL JEL Classification	M15

[1] Estudiante de la Maestría en Auditoría Tecnologías de la Información en Universidad Espíritu Santo – Ecuador. E-mail elojan@uees.edu.ec
[2] CISA, CBCP, CICA, ISO 22301 LI, ISO 22301 LA, ISO 27001 IA, COBIT, MSc. Docente de la Maestría en Auditoría en Tecnologías de la Información Universidad Espíritu Santo- Ecuador

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) (ISO 22301:2012, 2012). 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 la BS 25999, ambas basan su estructura y lineamientos de buenas prácticas en el ciclo de Control de Deming[3] PHVA (Planear, Hacer, Verificar y Actuar), el cual postula que los sistemas siempre estarán en estado de imperfección, por lo tanto, es necesario un proceso de mejoramiento continuo.

La Figura 1 muestra la relación de las cláusulas generales de la norma ISO 22301:2012 y el ciclo PHVA. Por ejemplo, si el requisito de evaluación del desempeño (Verificar) detecta inconsistencias o deficiencias en el cumplimiento de los objetivos, entonces el requisito mejoramiento continuo (Actuar) resuelve tales discrepancias mediante las correcciones respectivas. Así también, las acciones de mejoramiento deben ser validadas y planificadas (Planear) antes de ser puestas en marcha en el requisito de operación (Hacer), para nuevamente ser verificadas.

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, predecibles o no, que impactan negativamente en la normal provisión de productos y servicios mediante la implementación de planes de acción eficaces, 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 de la organización.

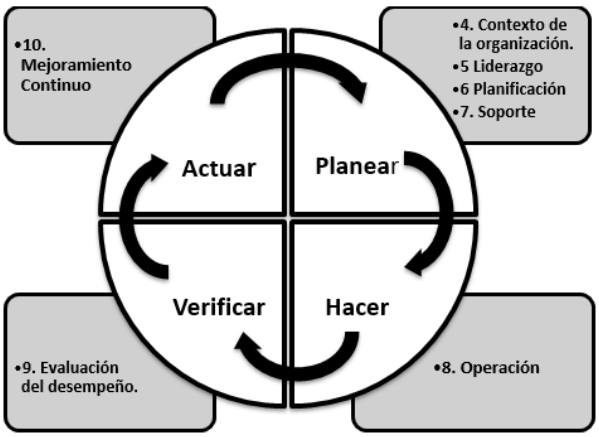

Figura 1: El ciclo PHVA y la ISO 22301.

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 producirse ésta, 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 BCP y que de aquellas que si hicieron tales pruebas, la mayoría no las pasó satisfactoriamente. Adicionalmente, los BCP dependen directamente del BCMS, el cual también debe ser evaluado.

Surge entonces la necesidad de contar con una herramienta metodológica que permita emitir una

[3] William Edwards Deming estadístico estadounidense, profesor universitario, autor de textos, consultor y difusor del concepto de calidad total

declaración concluyente sobre el grado de eficacia de los BCP, 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 una visión cuantitativa y cualitativa de la eficacia del BCMS. Este paper está dividido en cinco secciones, seguidamente hará una revisión y síntesis de literatura relacionada con la presente temática. En la tercera sección se desarrolla la metodología empleada, en la cuarta sección se presentan los resultados obtenidos y finalmente las conclusiones y trabajo futuro se exponen en la quinta sección.

MARCO TEÓRICO.

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). Sin embargo, Castillo (2005), afirma que se debe involucrar a todas las funciones de la organización en el BCMS de manera que se prioricen tareas que permitan una eficaz recuperación del negocio ante desastres, por lo tanto, el BCMS debe ser un trabajo de toda la organización.

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 (ver Figura 1).

No obstante el beneficio aportado por la normalización del BCM, 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 BCM se traslada ahora a la cuestión de elegir una normativa dentro un amplio conjunto de estándares disponibles. Adicionalmente, las organizaciones desarrollan sistemas de calidad, medio ambiente, salud y la seguridad, finanzas, recursos humanos, tecnologías de la información y protección, lo cuales componen el ecosistema de la gestión organizacional; el desafío entonces es lograr la sinergia de tal ecosistema (Stoichev, 2014).

En consecuencia, un BCMS requiere de un enfoque integral, holístico e integrado a otros sistemas de gestión (Bajgoric, 2014; Horvath, 2013). El estándar ISO 22301:2012, como se señala en la parte introductoria del presente artículo, basa su estructura en el ciclo **PHVA**, la cual también es estructura del conjunto de normas del ecosistema ISO de estándares de gestión organizacional, por lo tanto, se integran perfectamente (Cortina , Mayer , Renault , & Barafort, 2014).

Fundamentos de catástrofe y recuperación.

Primeramente, se debe tener claro que un BCP no es igual que un 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. En síntesis, 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 organización podría desaparecer del mercado (Boehmer, 2009; Faertes, 2015; Zambon, Bolzoni, Etalle, & Salvato, 2007).

Como parte del BIA, se tiene 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).

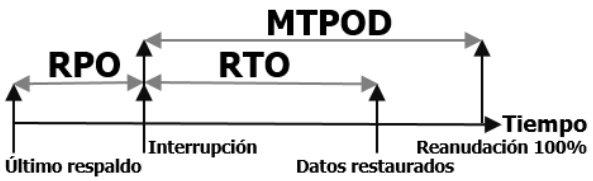

Figura 2: RPO y RTO vs tiempo.

Además del MTPOD, RTO y RPO otro factor resultante del BIA es 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 $RTO \leq MTPOD$.

Resiliencia Organizacional.

La Figura 3 muestra la ubicación del MTPOD dentro de un escenario típico de interrupción catastrófica, MTPOD expresa el tiempo de inactividad máximo aceptable para garantizar la continuidad del negocio (Zambon, Bolzoni, Etalle, & Salvato, 2007), por encima de este tiempo el negocio podría ser inviable y desaparecer (Bajgoric, 2014; Watters, 2014) por lo tanto, es objetivo crucial para una organización no sobrepasar el MTPOD dado un evento que le impida la provisión normal de bienes o servicios.

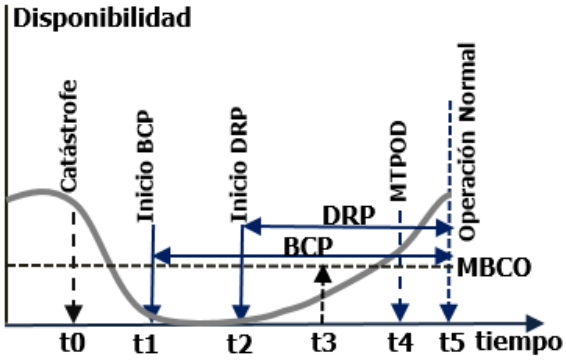

Figura 3: Recreación de tiempos t0 a t4 en la recuperación de continuidad.

En consecuencia, 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 se puede mejorar aumentando la capacidad de adaptación del sistema (Dalziell & McManus, 2004). Esta capacidad adaptativa según Dalziell & McManus (2004) depende de la estructura organizativa, los

sistemas de gestión y sistemas operacionales, los requisitos para lograrla son:

- El desarrollo de metodologías simples pero efectivas que las organizaciones pueden utilizar para evaluar su resiliencia y estrategias.
- Una terminología común para facilitar el diálogo y el debate dentro de las organizaciones sobre sus prioridades de resiliencia.
- Métricas para evaluar la resiliencia.

Adicionalmente, 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 (como se visualiza en la figura 4).

Respecto del grado de resiliencia de la organización contra las fluctuaciones causadas por eventos de interrupción, Dalziell & McManus (2004) y Hémond & Benoît (2014) consideran imprescindible evaluarla a través de indicadores clave de desempeño KPI ya que ésta medición puede dar alguna indicación en cuanto a la probabilidad de éxito de la adaptación o recuperación después de una catástrofe.

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 indicador clave de desempeño 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).

Otro aspecto fundamental respecto a KPI es su carácter comparativo contra objetivos internos y externos, ya sea de forma cualitativa o cuantitativa (Alemanni, Grimaldi, Tornincasa, & Vezzetti, 2008; Hémond & Benoît , 2014) lo cual proporciona información crucial acerca del rendimiento y efectividad de la estrategia de continuidad del negocio. 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).

Indudablemente, RTO es un KPI crítico de continuidad del negocio (Yang, Yuan, & Huang, 2015), en tal sentido, las nuevas estrategias empresariales se basan en KPIs específicos para evaluar su rendimiento; una desviación importante en un KPI conlleva acciones correctivas inmediatas (Calabrò, Lonetti, & Marchetti, 2015), sin embargo, se debe tener en cuenta que detrás de un KPI crítico se encuentran otros KPIs que coadyuvan en la consecución del KPI óptimo.

De esta manera, 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 solamente.

Es así que, Boehmer propone medir el desempeño de un BCMS mediante la siguiente ecuación:

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

Donde $\boldsymbol{Efk}$ es la eficacia del BCMS representada por el producto de los siguientes KPIs:

$\boldsymbol{Iex}$: Existencia de controles de cumplimiento de la norma BS 25999.

$\boldsymbol{Iop}(\boldsymbol{BCP})$: Grado de cumplimiento de los BCP.

$\boldsymbol{Iop}(\boldsymbol{DRP})$: Grado de cumplimiento de los DRP.

$\boldsymbol{Ico}$: Grado de cobertura de BIA y Análisis de Riesgos (AR) en recursos críticos.

La ecuación (1) mide cuan desviado está el objetivo de continuidad del negocio, los valores entregados por esta ecuación están en un rango entre 0 a 1. Si $\boldsymbol{Efk}$ 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.

Modelos de Madurez.

Los primeros modelos de madurez se aplican a dominios relacionados con la ingeniería de software; sin embargo conceptualmente, estos modelos 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 mejores 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 permitiría 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, por lo tanto, un modelo genérico de madurez y el BCMS se comportan análogamente.

Así, 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 final resultante se puede observar en la Figura 4.

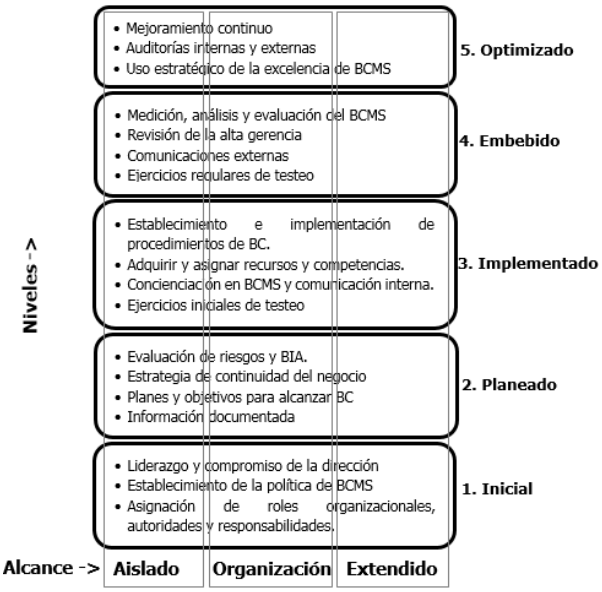

Figura 4: Modelo de madurez de BCM propuesto por Junttila,(2014).

El modelo de madurez de Junttila cubre dos dimensiones: el nivel y alcance de la madurez, este último indica el grado de cobertura de BCM que 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. Se puede apreciar que en la base se encuentran los requerimientos iniciales de la norma, tales como Contexto Organizacional y Liderazgo, hasta llegar al nivel 5 que corresponde a Mejoramiento Continuo. 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.

Ahora bien, el modelo de Junttila no prescribe cómo hacer la medición, análisis y evaluación del BCMS, tampoco la norma ISO 22301:2012 lo da. 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 la metodología de

implementación de un BCMS debería ser capaz de adaptarse a cualquier tipo o tamaño de organización, en otras palabras, tanto la implementación como la evaluación de madurez del BCMS debe ser ágil.

Consecuentemente, 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 de la BCM (Aislado, Organización y Extendido).

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 Organizacional 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.

METODOLOGÍA

El presente artículo es de corte exploratorio, por lo tanto, es netamente cualitativo y pretende generalización teórica en lugar de generalización empírica. 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 e indicadores clave de desempeño KPI.
2) Análisis exhaustivo de la norma ISO 22301:2012.
3) Construcción de modelo prototipo de evaluación de BCMS basado en los resultados de 1) y 2).
4) Validación de modelo prototipo resultado de 3) mediante la técnica Grupo Focal Virtual.
5) Presentación de resultados.

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.

Análisis exhaustivo de la norma ISO22301:2012

Se revisó la primera edición, versión en idioma inglés corregida al 2012-06-15 de la norma ISO 22301:2012, Societal security — Business continuity management systems — Requirements, y del Draft International Standard ISO/DIS 22313 Societal security — Business continuity management systems — Guidance, en este último documento se analizó con el objetivo de indagar posibles métricas de desempeño.

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?
- ¿Sirve como marco de implementación del BCMS enfocando el aumento de capacidad de los procesos?
- ¿Permite evaluar la resiliencia organizacional?

A continuación, la Figura 5 expone el modelo prototipo resultante.

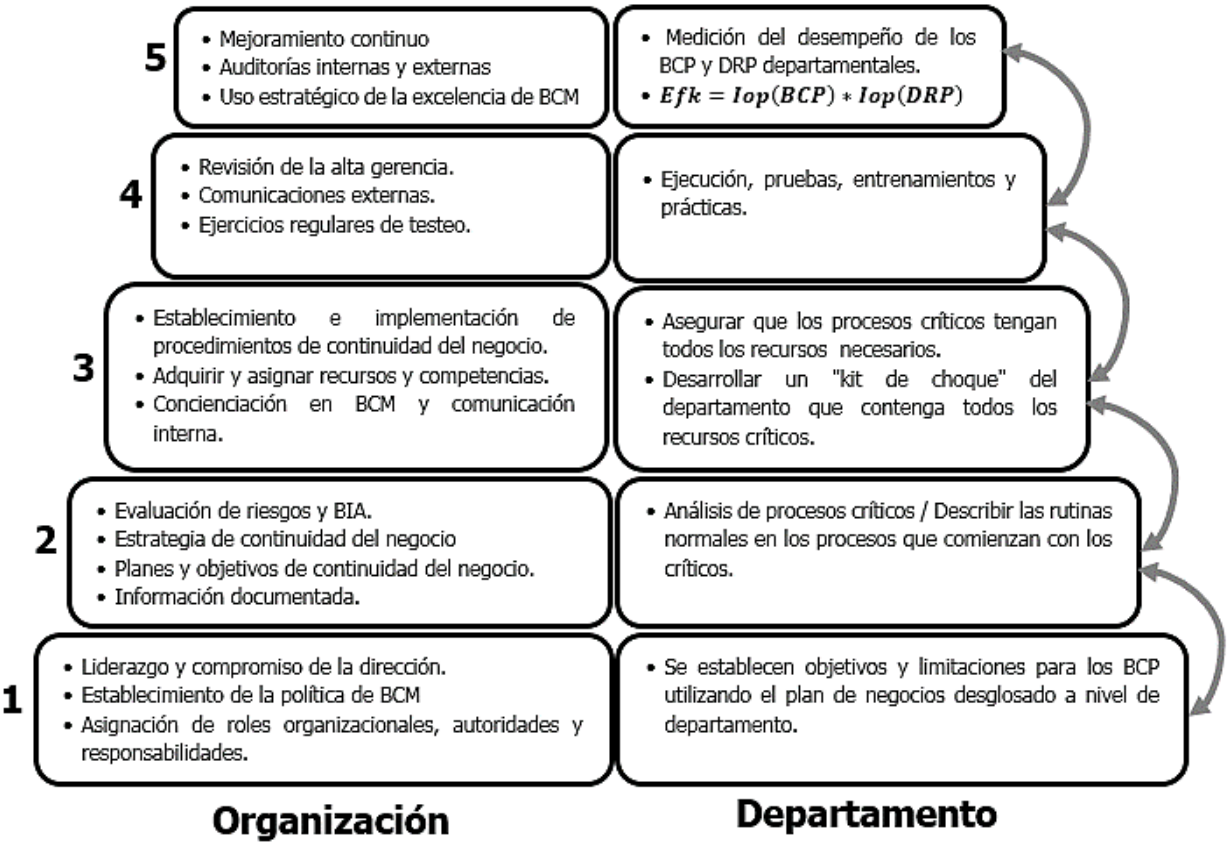

Figura 5: Modelo prototipo propuesto de evaluación del BCMS.

El modelo 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 maneje la BCM como un proyecto, en el cual se delega su realización a la alta dirección y mandos gerenciales; sin embargo, 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 calificarlo 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).

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, $\boldsymbol{Iex}$ y $\boldsymbol{Ico}$ no son necesarios ya que son considerados dentro de la etapa de proyecto del modelo propuesto, por lo tanto, el indicador de eficacia $\boldsymbol{Efk}$ se redefine como:

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

$\boldsymbol{Iop}$ representa el grado de cumplimiento de BCPs y DRPs basados en los resultados de evaluaciones de ejercicios prácticos y desviaciones en los controles planificados, para hallar $\boldsymbol{Iop(BCP)}$ usar:

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

$\sum_{i=1}^{n} C\lambda i(BCP)$ 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 resultara. Cada medida adoptada o faltante

agrega un 1 en su sumatoria respectiva. Análogamente, $\boldsymbol{Iop(DRP)}$ se calcula:

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

En conclusión, un $\boldsymbol{Efk}$ calculado mediante (2), (3) y (4) 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 $\boldsymbol{Efk}$ 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 prototipo expuesto. La razón fundamental es que requerir detalles sobre BCP a las partes interesadas externas podría ser un trabajo complicado y demorado. Adicionalmente, no hay garantía que la información suministrada ofrezca un conocimiento fidedigno de su nivel de madurez (Tucker, 2014). En este caso, la certificación de requisitos normativos a través de un tercero es lo recomendado.

Validación de modelo prototipo

Con el objetivo de validar el modelo prototipo expuesto en esta sección, se emplea la técnica de recopilación de información Grupo Focal, la cual se define como una entrevista grupal semi-estructurada centrada en un tema específico y 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 BCM 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 anterior apartado 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 en este caso, no es necesario.

Para efectos de validar el modelo propuesto se convoca a los expertos: Master Carlos Garcés quien cuenta con las siguientes certificaciones PMP, CISA, CISM, CGEIT, CRISC, MBCP, CICA, ISO 22301 LI, ISO27001 LA, ITIL, COBIT 5, ISO9001 LA – con 20 años de experiencia y de nacionalidad colombiano, Master Oswaldo Bravo quien cuenta con las siguientes certificaciones CRISC, CICA, LA ISO 27000, CBCP, Cobit 5 – con 25 años de experiencia y de nacionalidad ecuatoriano y Master Raúl González quien cuenta con las siguientes certificaciones CISA, CBCP, CICA, ISO 22301 LI, ISO 22301 LA, ISO 27001 IA, COBIT – con 10 años de experiencia y de nacionalidad ecuatoriano. Los expertos convocados son profesionales certificados con amplia 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 así como los detalles del desarrollo del Grupo Focal Virtual y el compendio de opiniones se agregan en la sección anexos de este paper.

RESULTADOS.

El modelo propuesto ha tenido aceptación general por parte de los participantes al grupo focal virtual. No obstante, luego de la reducción y categorización de opiniones, técnica empleada para el análisis de datos recopilados (Escobar & Bonilla-Jimenez, 2011) se determinaron tres macro categorías:

1) Necesidad de contar con un mapa de ruta en la ejecución del modelo de evaluación del BCMS.

2) Describir y detallar cada caja descrita en los niveles del modelo propuesto.

3) Detallar KPIs intervinientes en la ecuación de eficacia del BCMS.

En síntesis, estas macro categorías buscan responder la siguiente cuestión fundamental respecto del modelo propuesto:

¿Sirve como marco de implementación del BCMS enfocando el aumento de capacidad de los procesos?

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:

ALCANCE ORGANIZACIONAL		
NIVEL DE MADUREZ	**DESCRIPCIÓN**	**ACTIVIDADES**
1	Se establecen políticas, roles, responsabilidades y alcances del BCM. La alta administración demuestra su compromiso y liderazgo en la ejecución del programa BCMS.	Creación del comité ejecutivo y 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.

La tabla 1 detalla actividades del BCMS desde la perspectiva de proyecto de certificación, por lo tanto un mayor detalle se puede encontrar en el Draft International Standard ISO/DIS 22313 Societal security Business continuity management systems Guidance. La tabla 2 detalla las actividades desde la perspectiva de procesos departamentales. Al respecto, hay que remarcar el hecho de que el alcance Departamental no está divorciado del alcance Organizacional sino todo lo contrario, están estrechamente vinculados y coordinados en cada nivel. En efecto, los hallazgos de Baba, Watanabe, Nagaishi, & Matsumoto (2014); Lindström, Samuelsson, & Hägerfors (2010) y Hémond & Benoît (2014) en el sentido que cada área o unidad de negocio maneje su

propio ciclo de vida de gestión de continuidad, demuestran que la organización no queda inhabilitada para lograr el objetivo de continuidad de modo integral, por el contrario, vuelve la gestión de procesos de continuidad más ágil y eficaz. Las tablas 1 y 2 son la repuesta a las macro categorías 1 y 2.

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 contexto organizativo.	Establecimiento de roles y propietarios de procesos de continuidad. Creación del comité de continuidad.
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.

La tabla 3 responde a la macro categoría 3 y se vincula al nivel 5 del modelo de alcance departamental, es decir, a la aplicación de las ecuaciones (3) y (4). Por ejemplo, un KPI cumplido agrega 1 a la sumatoria de Ci (BCP) o Ci (DRP), caso contrario, agrega 1 a la sumatoria de NoCi (BCP) o NoCi (DRP).

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[4] (Acuerdo de Nivel de Servicio) cumplido.
	OLA[5] (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] Acuerdo entre un proveedor de servicio de TI y la organización.

[5] Acuerdo entre un proveedor de servicio de TI y un departamento de la organización.

Para entender mejor el ejemplo anterior, suponer que se ha realizado la prueba de un DRP arrojando como resultado los valores observados en la tabla 4. Si se aplica la ecuación (4), el KPI obtenido es 0.50. Este valor es una medida de la eficacia del DRP probado. Siguiendo un proceso análogo se puede evaluar el BCP departamental, en este caso usando la ecuación (3); suponiendo que el valor obtenido sea 0.70, entonces al aplicar la ecuación (2), se obtiene el KPI general del departamento: 0.50*0.70 = 0.35.

Consiguientemente, el KPI general obtenido es un dato cuantitativo ya que ofrece la magnitud de resiliencia departamental y por otro lado es un dato cualitativo ya que muestra qué acciones están faltando para mejorarlo. Lo esperado es que en sucesivas evaluaciones, el KPI general vaya mejorando de tal manera que se tenga una mayor capacidad de respuesta ante eventos catastróficos de interrupción.

Así mismo, 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.

KPIs específicos	Ci (DRP)	NoCi (DRP).
Cumplimiento de programas de concienciación		1
Cumplimiento de programas de capacitación	1	
Entrenamiento DRP	1	
Entrenamiento a intervalos regulares	1	
RTO <= MTPOD	1	
RPO al 100%	1	
MBCO alcanzado por debajo del 50% del MTPOD	1	
SLA cumplido	1	
OLA cumplido		1
Ejercicio basado en escenarios.		1
Producción de reportes post-ejercicios para mejoras.		1
Ejercicios realizados a intervalos planificados.	1	
Suma total	**8**	**4**

Tabla 4: Prueba simulada de KPIs específicos aplicados a un DRP.

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 normalización juega un papel crucial en la orientación de la gestión del proyecto de continuidad del negocio de la organización. No se puede afirmar que un BCMS se ha implantado correctamente sin haberlo sometido a un riguroso proceso de estandarización en buenas prácticas para la continuidad del negocio bajo el aval de una normativa reconocida internacionalmente, en este caso, la norma ISO 22301:2012, la cual es el resultado de la evolución del lineamiento BS 25999, primer estándar de continuidad del negocio auditable y certificable, que incorpora el ciclo PHVA en su estructura funcional.

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.

Por lo tanto, la estrategia de continuidad del negocio para ser exitosa, debe integrar tanto la normalización de sus prácticas de continuidad del negocio como el uso de KPIs para evaluar su efectividad. De este modo, si complementaria y paralelamente a la gestión del proyecto de certificación del BCMS se realiza la medición periódica de efectividad de BCPs y DRPs mediante el uso KPIs, entonces se abre un camino iterativo para el mejoramiento continuo del BCMS ya que el uso de KPIs viabiliza la adopción de acciones

concretas para la determinación de correctivos inmediatos.

Así pues, el modelo de evaluación del BCMS presentado en este paper se construyó sobre la base de los modelos de Junttila (2014) y Lindström, Samuelsson, & Hägerfors (2010) diseñados bajo estricto rigor sistemático como la metodología de la Ciencia del Diseño como base teórica de fundamentación, y de Boehmer (2009) que demostró que es posible medir cuantitativamente la efectividad instantánea del BCMS, usando KPIs.

En efecto, el modelo aquí expuesto es en realidad una iteración de los modelos anteriormente indicados, 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, y la medición de eficacia de procesos de continuidad del negocio mediante el uso de KPIs con el objetivo de evaluar cualitativa y cuantitativamente los BCPs y DRPs de la organización, independientemente de su tipo o tamaño.

Con respecto a su utilidad como marco guía de implantación del BCMS empresarial, se anexaron al modelo original las descripciones y actividades vinculadas a cada nivel de madurez de modo que quede clara cada etapa de implementación, no obstante, las especificaciones de requerimientos para la certificación pueden ser halladas en la documentación formal relacionada a la norma ISO 22301:2013, así como las normas ISO 31000 para la gestión de riesgos y la ISO 22317 para la realización del BIA.

Es importante recalcar que cada nivel tanto en el alcance organizacional como en el departamental, se encuentra estrechamente vinculados, de este modo:

- El nivel 1 organizacional corresponde al contexto de la organización y liderazgo, cuyos resultados componen el insumo que el nivel 1 departamental procesa para conocer los alcances y limitaciones de sus procesos de continuidad.
- El nivel 2 organizacional desarrolla el BIA el cuál sirve como base para el mapeo de procesos críticos del nivel 2 departamental.
- En el nivel 3 departamental se elaboran los primeros BCP y DRP determinando los recursos necesarios para el entrenamiento y ejecución, este apoyo se deriva de la determinación y asignación de recursos del nivel 3 organizacional.
- El nivel 4 de ambos alcances, desarrolla pruebas departamentales independientes y luego se hacen pruebas en conjunto de acuerdo a escenarios variados.
- Finalmente, el nivel 5 corresponde al mejoramiento continuo; para este efecto, en el ámbito departamental se mide el desempeño de los planes de continuidad y en el ámbito organizacional se realizan auditorías internas y externas.

El modelo propuesto se validó mediante un panel de expertos, sin embargo, no fue posible exponer el mismo a un grupo más amplio y variado de practicantes de la continuidad del negocio debido a que el desarrollo de la BCM aún se encuentra en un proceso de crecimiento en nuestro medio.

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, así como también para adicionar KPIs que permitan medir la eficiencia de los procesos de continuidad del negocio de la empresa.

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 22301:2012. *GESTIÓN*.

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.

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

Castillo, C. (2005). Disaster preparedness and Business Continuity Planning at Boeing: An integrated model. *Journal of Facilities Management,*, 8-26.

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.* 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. *International Conference "Risk in Contemporary Economy"*, (págs. 71-74). Galati.

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.

Watters, J. (2014). *Disaster Recovery, Crisis Response, and Business Continuity: A Management Desk Reference.* New York: Apress.

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.

Yang, C.-L., Yuan, B., & Huang, C.-Y. (2015). Key Determinant Derivations for Information Technology Disaster Recovery Site Selection by the Multi-Criterion Decision Making Method. *Sustainability*, 6149-6188.

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.

ANEXO 1: Detalles de realización de Grupo Focal Virtual.

El día 28 de diciembre 2016 se realiza el Grupo Focal Virtual de 08:00 a 10:00.

Participantes:

Ing. Carlos Garcés MBA, PMP, CISA, CISM, CGEIT, CRISC, MBCP, CICA, ISO 22301 LI, ISO27001 LA, ITIL, COBIT 5, ISO9001 LA.

Ing. Raúl González CISA, CBCP, CICA, ISO 22301 LI, ISO 22301 LA, ISO 27001 LA, COBIT.

Ing. Oswaldo Bravo CRISC, CICA, LA ISO 27000, CBCP, Cobit 5

Pormenores:

Con la anticipación debida se envió a los correos electrónicos de los participantes la invitación al grupo focal virtual así como el material de presentación que incluyó el modelo prototipo a evaluar y las preguntas (ver Anexo 2) a desarrollar en la sesión virtual. Cabe destacar que el Ing. Garcés se ha conectado desde Bogotá - Colombia, el Ing. Bravo desde Lima - Perú y el Ing. Gonzalez desde Guayaquil – Ecuador.

El grupo focal se desarrolla en ambiente virtual síncrono, en la plataforma ***Google Hang-Outs,*** la sesión es grabada mediante ***Apowersoft Free Online Screen Recorder*** a fin de facilitar la transcripción de los datos obtenidos.

El moderador, en este caso el autor de este paper, lee cada pregunta en voz alta, luego de esto, otorga la palabra a cada integrante, en el siguiente orden: C. Garcés, O. Bravo y R. González.

Cada vez que un participante emite su opinión, cualquiera de los demás participantes puede solicitar al moderador la palabra ya sea para rebatir o complementar.

Todos los participantes intervienen en las 21 preguntas programadas (ver Anexo 2), que abarcan 4 temáticas: Utilidad, Aplicabilidad, Cobertura ISO 22301:2012 y KPIs.

Cada participante tiene un tiempo máximo de participación de 2 minutos, controlado por el moderador.

Se mantendrá en confidencialidad la organización o empresa donde labore el participante, únicamente se citará su nombre en la transcripción de datos.

El evento se desarrolla en perfecta calma y armonía. Todos los participantes acuden de manera puntual. Primeramente se hacen pruebas de audio, optando por cortar video ya que además de no aportar datos significativos a la temática, permite conservar ancho de banda.

Seguidamente se lee la agenda de trabajo. Posteriormente se realiza una breve descripción del modelo propuesto por parte del moderador.

Finalmente se comienza la ronda de preguntas y debate. El resumen de la transcripción del debate se muestra en el anexo 3.

ANEXO 2: 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?

ANEXO 3: Compendio opiniones debate Grupo Focal Virtual.

Temática: Utilidad del modelo propuesto.

1) **¿Está Ud. de acuerdo con la terminología empleada en el modelo propuesto?**
   Los expertos están de acuerdo con la terminología empleada.

2) **¿Considera Ud. que el modelo propuesto puede ser implantado en una organización, independientemente de su tamaño, misión y visión?**
   Los expertos consideran que el modelo propuesto tiene una estructura estándar y adaptable, por lo tanto puede ser implantado en cualquier organización.

3) **¿A su juicio, el número de niveles propuesto es el indicado? ¿O quizá deban aumentarse o disminuirse?**
   El número de niveles es correcto a juicio de los expertos.

4) **¿A su juicio, la dimensión ALCANCE, se justifica? ¿Quizá vuelve más complicado el modelo incluir esta dimensión?**
   A criterio de los consultados y por unanimidad, es correcto considerar la dimensión **alcance**, sin embargo, se aclara que no todas las unidades de negocio deben tener un BCP, sino que únicamente aquellas que cuya criticidad de sus procesos afecten la continuidad de la organización. O. Bravo manifiesta que el alcance **DEPARTAMENTO** puede ser visto como el conjunto de responsabilidades que de la implementación de la norma 22301 se deriven.

5) **¿Cree Ud. que el presente modelo podría servir como marco guía para la implementación del BCMS?**
   C. Garcés opina que el modelo puede servir como marco guía de implementación siempre y cuando los niveles del modelo propuesto se detallen y expliquen mejor en una estructura aparte. De la misma manera, los demás consultados están de acuerdo en la realización de una guía anexa al modelo propuesto.

6) **¿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?**
   Los consultados son enfáticos en declarar que la organización debe trabajar en conjunto, no es recomendable que cada unidad de negocio trabaje de manera aislada o separada.

Temática: Aplicabilidad del modelo propuesto.

7) **¿Cuál es el obstáculo más importante que Ud. considera podría aparecer al aplicar el modelo propuesto?**
   C. Garcés manifiesta que la **no claridad** para tomar mediciones podría ser el principal obstáculo. O. Bravo estima que los conceptos de cada uno de los niveles deben estar **perfectamente claros** para evitar la confusión. Mientras R. González considera que tener el **apoyo de la alta gerencia** es uno los principales obstáculos a vencer.

8) **¿Es posible simplificar aún más el modelo propuesto, cómo?**
   Tener claro los objetivos de cada nivel es crucial para que el modelo sea simple de aplicar (C. Garcés), los demás consultados opinan que ya no es factible simplificarlo más.

9) **¿Es posible volver más ágil el modelo propuesto? ¿Que se podría agregar o quitar con tal finalidad?**
   Agregar como detalle un flujo-grama que guie el inicio, desarrollo y finalización de cada una de las etapas o niveles sería una buena idea para volver más ágil la ejecución del modelo propuesto (C. Garcés). La automatización a través de una herramienta tecnológica ayudaría mucho en darle agilidad a la implementación del modelo propuesto (O. Bravo).

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

Aspectos como el **soporte de la alta gerencia** y del **tipo de empresa** donde se aplique el modelo depende la complejidad, de ahí en más, no hay nivel o alcance más complicado que otro (C. Garcés).

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?

Los consultados no aplican modelos conocidos o estándares de BCM sino que usan modelos propietarios de las firmas donde trabajan adaptados de modelos genéricos de gestión. Sin embargo, R. González estima que el modelo propuesto en la presentación compendia todo lo sugerido para un modelo BCM.

Temática: Cobertura ISO 22301:2012 del modelo propuesto.

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

La norma es clara, sin embargo los consultados reiteran que debe explicarse y detallarse mejor los conceptos señalados en cada nivel.

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

A juicio de los expertos se cubren todos los puntos de la norma.

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

Los consultados opinan que no es necesario mover ni cambiar niveles ya que eso no agregaría valor. "El conjunto de todo es lo que daría el resultado final esperado" (C. Garcés). El detalle de cada caja del modelo propuesto es lo realmente importante (R. González).

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?

Los consultados estiman que la cantidad de niveles propuesta es adecuada.

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

Según los consultados, está clara la relación entre ambas columnas.

Temática: Indicadores clave de desempeño del modelo propuesto.

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

Los consultados coinciden en la necesidad de detallar la lista de KPIs necesarios que intervienen en la ecuación de eficacia. Otra recomendación dada es la necesidad de saber el grado de cumplimiento de los requisitos a modo de porcentaje.

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

Se reitera la necesidad, por parte de los consultados, de detallar los KPIs necesarios para completar la ecuación de medición del desempeño del BCP departamental.

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?

Los consultados se manifiestan contrarios a la proliferación excesiva de KPIs. Tener 100 o 200 KPIs no es un indicativo de que el modelo de gestión sea exitoso, más bien lo puede entorpecer (C. Garcés, R. González). Están de acuerdo que el modelo propuesto ofrece un conjunto de métricas válidas para medir la resiliencia organizacional, siempre que se tenga cuidado en elegir los KPIs adecuados.

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

Los consultados coinciden en que conocer cuándo es necesaria la actualización de estos análisis (BIA y RA) es lo realmente importante.

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

(C. Garcés): Flujo-grama o mapa de ruta en la ejecución del modelo de evaluación del BCM.
(O. Bravo): Detallar KPIs intervinientes en la ecuación de eficacia del BCM.

(R Gonzalez): Describir y detallar cada caja descrita en los niveles del modelo.