

Propuesta metodológica para la evaluación de la madurez del sistema de gestión de continuidad del negocio en el sector financiero bancario colombiano bajo el enfoque de la norma ISO 22301:2012*

Methodological proposal for evaluating maturity management
system business continuity in the colombian banking financial
sector under the approach of ISO 22301:2012

Recibido: 14 de marzo de 2016
Revisado: 28 de marzo de 2016
Aceptado: 27 de mayo de 2016

*Andrés Darío Olarte Rojas***
Universidad Santo Tomás - Icontec

* Artículo de resultado de investigación.

** Ingeniero industrial. Especialista en Gestión de Riesgos Financieros. Magíster en Calidad y Gestión Integral. Coordinador Continuidad del Negocio Credibanco. Correo electrónico: andres.olarte@credibanco.com

RESUMEN

El presente artículo busca comprender la necesidad de las entidades financieras bancarias de Colombia por tener una metodología integral que mida y evalúe la madurez del sistema de gestión de continuidad del negocio en cada una de ellas y del sector en particular. Se plantea una propuesta concreta de herramienta metodológica para ser aplicada en las diferentes entidades del sector, que se inicia con la definición del problema, encontrando que las entidades bancarias en alguna medida carecen de la herramienta y se identifica la ausencia y poca aplicación de un diagnóstico o evaluación gremial en general, con enfoque en las diferentes normas y metodologías aplicadas a la continuidad de los negocios. Por lo tanto, se analizan los antecedentes en contextos evaluados, destacando las organizaciones que han tenido impactos considerables por no tener definido un plan de continuidad del negocio y las repercusiones que ello ha generado, para justificar la necesidad del estudio. Se establecen unos objetivos enfocados a la construcción y entrega de la propuesta metodológica, para lo cual se elabora una encuesta que se aplica a las entidades con el fin de construir un diagnóstico estructurado de las mismas; junto con las metodologías de evaluación de madurez y la norma técnica ISO 22301:2012, se construye una herramienta metodológica práctica, de evaluación de la madurez del plan de continuidad de negocio de las entidades del sector bancario. Como resultado se obtiene la herramienta metodológica la cual describe los criterios y aspectos para evaluar mediante unos niveles definidos. Se concluye que las entidades tienen aspectos que deben fortalecer en la estructura y componentes de su plan de continuidad de negocio, para contar con la capacidad, respuesta, reacción y recursos necesarios para atender eventos de continuidad del negocio que se puedan presentar, ya que actualmente solo algunas entidades evalúan la madurez como factor crítico de evolución de su plan de continuidad del

negocio. Esta herramienta aporta direccionamiento y bases estructurales en el tema a las entidades, frente al cumplimiento de las mejores prácticas y a la evolución del plan de continuidad del negocio.

Palabras clave: evento, impacto, incidente, gestión de riesgos, madurez, manejo de la crisis, plan de continuidad del negocio, contingencia.

ABSTRACT

This project seeks to understand the need for banks in Colombia, to have a comprehensive methodology to measure and evaluate the maturity of Management System Business Continuity and each sector in particular. Therefore a concrete proposal for a methodological tool to be applied by the various entities in the sector arises. It starts with defining the problem, analyzing entities lack this tool, which has not been made a diagnosis or professional evaluation, with a focus on different standards and methodologies applied to business continuity. Therefore the background discussed in contexts evaluated, highlighting organizations that have had a significant impact, not having defined a business continuity planning, and the impact this has generated, in order to justify the need for the project. Subsequently general and specific objectives focused on the process for the construction and delivery of the methodological proposal, in which a survey that applies to entities to build a clear diagnosis of the same and which together with is made are set assessment methodologies maturity and ISO 22301:2012 sound methodology for assessing the maturity of the plan of continuity of institutions in the banking sector is built. As a result, the methodological tool which criteria and aspects are evident to assess through a defined levels is obtained. It is concluded that entities have aspects that should strengthen ahead to have the capacity,

responsiveness and resources to cater events business continuity that may arise, as only some of the entities currently evaluating maturity as a critical factor evolution of their business continuity planning.

Keywords: Event, impact, incident, risk management, maturity, crisis management, business continuity planning, contingency.

INTRODUCCIÓN

Colombia es un país muy diverso donde se encuentran organizaciones de todo tipo, las cuales están expuestas a riesgos y vulnerabilidades que pueden afectar sus operaciones principales, sus servicios y de tal manera su imagen y sus clientes. En el sector financiero bancario colombiano, el sistema de gestión de continuidad del negocio se ha convertido en una herramienta muy importante y vital para la mitigación y prevención de impactos y de reacción ante eventos adversos. En la actualidad falta más gestión puntual del sector en temas de continuidad que permita evaluarlo, así mismo tener un diagnóstico gremial para la toma de decisiones eficientes en el gremio, en caso de una situación de crisis generalizada de las entidades bancarias, o por un evento de contingencia que podría afectar considerablemente a todas las entidades.

Por lo anteriormente descrito, se da la necesidad por parte del sector financiero bancario de contar con una metodología básica estandarizada del sistema de gestión de contingencia y continuidad del negocio, que permita evaluar la madurez y determinar si realmente se está preparado de acuerdo a unos niveles definidos para hacer frente a una situación de emergencia, contingencia o crisis, pérdida de información crítica y sensible para las empresas y para proteger la infraestructura, tecnología, personas y los activos de las entidades, así mismo cumplir por normatividad con las

operaciones, actividades, productos y servicios a los cuales la entidad se compromete frente al cliente.

Según los referentes teóricos y conceptuales, en Colombia se puede dimensionar que el plan de continuidad de negocio se implementó y llegó a ser parte del sistema integral de la administración de riesgos, principalmente de las empresas del sector financiero bancario objeto de estudio, a partir del año 2006, por medio de la Asociación Bancaria y de Entidades Financieras de Colombia - Asobancaria (2006), la cual actualmente es la Superintendencia Financiera de Colombia. Como ente regulador y de control, vela por el buen funcionamiento y vigilancia del gremio bancario colombiano.

Adelantar esta investigación se justificó dado que toda organización tiene que enfrentar hechos o situaciones que afectaron y actualmente afectan sus operaciones y el sector en general, por no gestionar riesgos adecuadamente, aclarando que no contar con un adecuado, evaluado y maduro sistema de gestión de continuidad del negocio, puede tener consecuencias e impactos negativos para las diferentes organizaciones.

El concepto de madurez, según la Real Academia Española (2016), consiste en el estado de un elemento o sistema que ha alcanzado su pleno resultado o desarrollo final para obtener una calificación o distinción final. Para el caso del objeto de estudio, la evaluación de madurez se utiliza para dirigir a las organizaciones a que sean capaces de evaluar y mejorar su programa de continuidad de negocio, como un mecanismo de medición de la efectividad del mismo. De esta manera con la evaluación de la madurez se sacan conclusiones importantes sobre cómo están las entidades y en qué se debe mejorar o fortalecer para tener una mayor madurez, pero esto se da con el tiempo y con la implementación de planes de mejora.

La gestión y evaluación de la continuidad del negocio es una pieza clave dentro de los planes, ya que no

contar con estos preceptos hace que las organizaciones sean extremadamente vulnerables a incidentes graves. Según el Instituto Nacional de Tecnologías de la Comunicación (2010):

Carecer de la capacidad de recuperarse ante un evento de estas características, fuego, ataque terrorista, cortes de suministro, etc., puede tener consecuencias muy graves para la organización, pudiendo llegar a suponer la desaparición de la organización y su salida del mercado (p. 4).

Para la revisión de las metodologías de madurez aplicadas a este estudio, los referentes y teóricos más importantes son para el modelo BCMM Virtual Corporation, creado en el 2003 como un mecanismo globalmente aceptado para valorar la sostenibilidad de los programas de continuidad del negocio, donde varios estándares han sido creados para evaluar si una organización cumple con los requisitos acerca de un proceso y su documentación (Quevedo, 2012). Este modelo integra los requisitos de BSI BS 25999, NFPA1600 y ASIS SPC1 2009. Esta herramienta proporciona elementos para continuar mejorando el programa de continuidad del negocio en las organizaciones. El modelo Cobit 4.1 (IT Governance Institute, s.f) que integra la teoría de madurez asociada a la tecnología y soporte que será explicado en el marco conceptual, el cual permite tener una metodología básica para medir con base en atributos de madurez interrelacionados por cuatro dominios al interior de la organización por parte del IT Governance Institute (ITGITM, por sus siglas en inglés), para evolucionar el pensamiento y los estándares respecto a la dirección y control de una empresa con enfoque tecnológico. El modelo GTAG-10 (The Institute of Internal Auditors North America, s.f.) como parte de una guía mundial de auditoría de tecnología del instituto de auditores internos, con un método de logro y características de capacidad de las organizaciones, realizando una evaluación de la madurez mediante la integración de aspectos relevantes

de función y cumplimiento. Así mismo la integración dentro del marco teórico de la norma ISO 22301:2012 (2012), la cual se describe en el marco conceptual y que es un elemento fundamental para el desarrollo de la metodología de evaluación de la madurez.

De acuerdo a la revisión de hipótesis correspondientes a la relación y asociación entre las variables, se plantea que poco existe sobre una metodología integral de evaluación de madurez del sistema de gestión de continuidad del negocio en el sector financiero bancario. Las entidades del sector bancario deben fortalecer la práctica y la cultura de evaluar la madurez de su sistema de gestión de continuidad del negocio. La norma ISO 22301:2012 permite integrar las metodologías de evaluación de madurez del SGCN para medir la evolución de las entidades bancarias. Los eventos de continuidad del negocio en el sector bancario pueden convertirse en un riesgo sistémico que afecte a todo el sector. Así como también las metodologías de evaluación de madurez del sistema de gestión de continuidad del negocio evalúan la capacidad de preparación de las entidades ante un evento real.

Se construyó como objetivo general una metodología para la evaluación de la madurez del sistema de gestión de continuidad del negocio en el sector financiero bancario colombiano, bajo el enfoque de la norma ISO 22301:2012. Para lograr estos objetivos se identificaron las metodologías de evaluación de madurez del sistema de gestión de continuidad del negocio a nivel nacional e internacional, de manera paralela se realizó un diagnóstico del nivel de evaluación y madurez del sistema de gestión de continuidad del negocio de las entidades del sector financiero bancario colombiano. Posterior a ello se definieron los elementos y variables que se deben evaluar para medir la madurez del sistema de gestión de continuidad del negocio con base en la norma ISO 22301:2012 y otras metodologías integrales de gestión.

METODOLOGÍA

La metodología se desarrolló con base y en torno al paradigma empírico analítico, el cual según Gutiérrez Bonilla (2014), parte de la observación e investigación de estudios científicos establecidos para generar unos resultados, aplicando un estudio cuantitativo. Así mismo busca la explicación, la determinación de causas y efectos cuantitativamente comprobables y repetibles en contextos diversos con variables de control.

Por lo cual se desarrolló, según Hernández (2008), desde un énfasis de tendencia hipotético deductivo, método que combina la formación de hipótesis con la deducción para que por medio de observaciones y reflexión llegue a la solución de un problema, en consecuencia por ser un estudio cuantitativo tiende a ser un enfoque positivista. Correspondió a una investigación aplicada, ya que se propuso transformar el conocimiento puro en conocimiento útil, teniendo por finalidad la búsqueda y consolidación del saber y la aplicación de conocimientos para generar una idea o un resultado. La investigación se abordó desde un enfoque cuantitativo, ya que se realizó un análisis y esquematización de la información de metodologías y entendimiento de la norma 22301:2012 que hizo parte del objeto de estudio.

El alcance de la investigación correspondió a un nivel correlacional, ya que según lo descrito por Hernández, Fernández y Baptista (2010, p. 81), los estudios correlacionales responden a preguntas de investigación de diferente índole y se asocian con variables mediante un patrón predecible para un sector o una población, tiene como propósito conocer la relación de dos o más conceptos hablando de un contexto en particular, teniendo en cuenta que se investigó varios aspectos para estructurar la metodología de evaluación de madurez. El método utilizado fue correlacional descriptivo, ya que se tomaron las organizaciones del sector financiero

bancario colombiano para aplicar y revisar la metodología, así como la medición y evaluación que se hicieron de ellas en el transcurso del proyecto.

De acuerdo a lo anterior y según Hernández, Fernández y Baptista (2010, p. 204), luego de definido el problema de estudio, se realiza la revisión de la literatura para construir un marco teórico y derivar en unas hipótesis, las cuales son corroboradas con los resultados del estudio de investigación, con el fin de aportar evidencia o por el contrario descartarlas, de tal modo volver a replantear las hipótesis y definir la teoría. Las hipótesis correspondieron al tipo asociación y relación entre las variables, las cuales buscaban revisar y analizar si existe una metodología integral de evaluación de madurez del sistema de gestión de continuidad del negocio en el sector bancario.

Planteando que las entidades del sector bancario deben fortalecer la práctica y la cultura de evaluar la madurez de su sistema de gestión de continuidad del negocio, y que la norma ISO 22301:2012 permite integrar las metodologías de evaluación de madurez del SGCN para medir la evolución de las entidades bancarias. Adicionalmente se planteó que los eventos de continuidad del negocio en el sector bancario pueden convertirse en un riesgo sistémico que afecte a todo el sector, y que las metodologías de evaluación de madurez del sistema de gestión de continuidad del negocio, evalúan la capacidad de preparación de las entidades ante un evento real. Para estas hipótesis se hizo el análisis y se corroboró su resultado.

La población total para todo el proceso fueron las 25 entidades del sector financiero, “establecimientos bancarios” colombianos registrados según la Superfinanciera, de los cuales se realizó un muestreo probabilístico por medio de la herramienta *Decisión Analist STATS 2.0*, la cual con un margen de error del 10 % y un nivel de confiabilidad del 90 %, arrojó que

para el estudio se requería una muestra de 18 entidades, a las cuales se aplicó una encuesta por entidad a los cargos responsables de la continuidad del negocio en la entidad, en un nivel de coordinador hasta gerente, los cuales tienen una injerencia muy importante en temas de continuidad y riesgos, con el fin de tener más credibilidad y certeza, de este modo se hizo el respectivo procedimiento a fin de aplicar el instrumento. Como criterios de validez y confiabilidad, para el total de las encuestas aplicadas (18) se realizó

un análisis para determinar la validez, determinando que se realizaría validez de confiabilidad al 10 % de las encuestas (dos encuestas), por lo cual se concretó con dos expertos en el tema de continuidad del negocio, expertos en consultoría y con experiencia, la aplicación de la encuesta para validarla en forma y contenido. De acuerdo al desarrollo del instrumento se definieron las preguntas foco de revisión del nivel de madurez de las entidades. A continuación se describen las preguntas de la encuesta aplicada:

Tabla 1. Preguntas de la encuesta aplicada a las entidades.

1	¿Existe una política clara del SGCN al interior de su organización y es conocida por todos los funcionarios?
2	¿Cómo considera que la alta gerencia conoce y apoya el funcionamiento y mantenimiento del SGCN?
3	¿Realiza algún tipo de evaluación o medición a su SGCN?
4	¿Por quién es realizada la evaluación de su sistema de gestión de continuidad del negocio?
5	¿Con qué frecuencia se realiza una evaluación al sistema de gestión de continuidad del negocio?
6	¿Se ha realizado alguna vez una evaluación de la madurez al sistema de gestión de continuidad del negocio?
7	¿Qué orden le daría a los componentes del SGCN como prioridad para evaluar y trabajar de cara al buen funcionamiento y efectividad del sistema en un evento real?
8	Ordene los factores de riesgo según considere que más se han materializado en su organización y obligado a poner en funcionamiento el SGCN.
9	¿Realiza seguimiento y evaluación de sus terceros y proveedores críticos de cara a la continuidad del negocio?
10	¿Cómo considera que se encuentra su organización en evaluación, seguimiento y exigencia a terceros y proveedores críticos?
11	¿El Centro Alterno de Operaciones - CAO, como estrategia operativa de continuidad del negocio es propio o administrado por un tercero?
12	¿Cómo considera que se encuentra en nivel de preparación y alistamiento el Centro Alterno de Operaciones - CAO?
13	¿El Centro de Computo Alterno - CCA, como estrategia DRP de continuidad del negocio es propiedad de la empresa o administrado por un tercero?
14	¿Cómo considera que se encuentra en nivel de preparación y alistamiento el Centro de Computo Alterno - CCA?
15	¿Cómo considera que se encuentra en nivel de madurez cada uno de los componentes del sistema de gestión de continuidad del negocio en su organización?

Fuente: elaboración propia.

Se utilizaron como instrumentos y técnicas de investigación la observación, el análisis documental y la herramienta encuesta. Se utilizaron fuentes primarias correspondientes a las metodologías de evaluación de madurez de continuidad, normas como la ISO 22301:2012, otras normas técnicas ISO, libros, revistas,

documentos oficiales alusivos al tema. Como fuentes secundarias en la investigación se utilizó documentación existente de la continuidad del negocio de las entidades bancarias, información elaborada producto del análisis y organización de información primaria, en la cual están trabajos, artículos e investigaciones.

Con la aplicación del método de acuerdo a la investigación se obtuvo el diagnóstico de las entidades financieras bancarias, diseño de un instrumento para determinar la necesidad de aplicación en el sector financiero bancario y la propuesta del modelo de metodología de evaluación de madurez a aplicar.

RESULTADOS Y DISCUSIÓN

De acuerdo a la definición y aplicación de este proyecto, los resultados se dieron con base en la propuesta y aplicación de la metodología y toda la consecución de aspectos y actividades ejecutadas. Por lo anterior, los resultados se describen para cada uno de los objetivos específicos que llevaron al resultado final paso a paso con sus productos y entregables, la validación de cada una de las hipótesis planteadas de acuerdo con el método de estudio, y el resultado de lo anterior y propuesta final, la propuesta metodológica de evaluación de la madurez del sistema de gestión de continuidad del negocio del sector bancario colombiano. Con la aplicación de la metodología, y de acuerdo a la investigación, se obtuvieron los resultados asociados a los objetivos, las hipótesis planteadas, propuesta metodológica final y guía para diligenciar la propuesta.

Con el desarrollo y cumplimiento de cada uno de los objetivos planteados, se pudo llegar al resultado final, para cada uno de ellos se obtuvo un resultado que fue complementando y estructurando el resultado final del proyecto, producto de metodologías de evaluación de madurez del sistema de gestión de continuidad del negocio a nivel nacional e internacional. Se obtuvieron las principales metodologías de evaluación de madurez de planes de continuidad de negocios en términos técnicos y funcionales, como parte de los objetivos específicos.

Se realizó un diagnóstico del nivel de evaluación y madurez del sistema de gestión de continuidad del

negocio de las entidades del sector financiero bancario colombiano. Dicho diagnóstico concluye que las entidades están en un nivel básico medio de preparación y tienen un sistema de gestión de continuidad del negocio implementado y funcional, ninguna entidad se encuentra en un nivel básico y aislado, pero sí existen aspectos y componentes para mejorar desde el punto de vista individual y como gremio, con el fin de que alcancen un nivel de evaluación y madurez que atienda con total efectividad los eventos de continuidad del negocio y que eviten que un evento pueda afectar a todo el sector. Este diagnóstico es complementado con una metodología de evaluación de la madurez del sistema de gestión de continuidad del negocio, que puede ser aplicada por la entidad que lo considere necesario.

Otro producto del estudio son los elementos y variables que se deben evaluar para medir la madurez del sistema de gestión de continuidad del negocio con base en la norma ISO 22301 y otras metodologías. Con base en la revisión de modelos de evaluación descritos en el objetivo 1, la aplicación de la encuesta y diagnóstico del objetivo 2 y la revisión y análisis de la norma ISO 22301, se realizó la integración y relación de los modelos de evaluación de madurez del sistema de gestión de continuidad del negocio con la norma ISO 22301, con el fin de definir aspectos, variables y enfoques para la construcción de la metodología, tomando de la norma los 8 criterios o requisitos principales de evaluación para compararlos. Como producto de esto se obtuvo las similitudes y relación de la norma con los modelos de evaluación de la madurez.

Con base en los resultados de la investigación de metodologías, la aplicación de la encuesta y la revisión de la norma ISO 22301, se elaboró la propuesta metodológica de evaluación de madurez del sistema de gestión de continuidad del negocio, para las entidades del sector bancario colombiano y en las que participaron en el desarrollo del proyecto. La metodología busca evaluar

qué tan preparadas están las entidades con referencia a la norma ISO 22301 que es el referente actual más importante como requisito de un sistema, y unos niveles definidos de 1 a 5, para medir en qué nivel se encuentra la entidad con referencia a cada componente, y de tal modo obtener un resultado global final de calificación.

Según lo dicho por la teoría y los referentes y contrastado con la metodología, es acorde a los requerimientos y exigencias mínimas que debe tener un plan de continuidad del negocio, de acuerdo con el estudio.

Según los referentes e investigaciones conceptuales, las metodologías de evaluación reúnen una serie de requisitos y aspectos que deben tener las organizaciones para evolucionar en su sistema de gestión de continuidad del negocio. Estos requisitos tienen relación y correspondencia con la norma ISO 22301, esto permite que si las entidades lo aplican y tienen un nivel deseado, se puedan fácilmente certificar en el estándar que es certificable.

De acuerdo a la revisión de la literatura e investigación realizada, no se cuenta con una metodología de evaluación de madurez del SGCN que esté integrada con la norma ISO 22301:2012, por lo cual es algo novedoso,

adicionalmente porque se integran las diferentes metodologías de evaluación de madurez.

La norma ISO 22301:2012 de acuerdo a la revisión y análisis se puede integrar muy fácil con las metodologías de evaluación de la madurez, ya que dichas metodologías están construidas bajo anteriores estándares y normas de continuidad del negocio, por lo cual es muy aplicable para las entidades financieras en cada uno de sus aspectos y requerimientos. De acuerdo a la revisión de los resultados, tienen una coherencia con las hipótesis planteadas, debido a que lo planteado se pudo corroborar con el desarrollo de la investigación, apoyado en los objetivos específicos y en las herramientas e instrumentos utilizados en cada una de las etapas sin presentar contradicciones.

La investigación realizada brindó una solución al problema planteado, ya que se pudo evidenciar el nivel de madurez de las entidades que se encuentran en un nivel medio en promedio, se construyó una herramienta muy útil para ellas, con el fin de que encuentren oportunidades y mejoren, así mismo que las entidades estén atentas y reaccionen eficientemente ante un evento adverso o contingencia.

Tabla 2. Herramienta metodología de evaluación de la madurez del SGCN.

Metodología evaluación de la madurez sistema de gestión de continuidad del negocio Entidades sector financiero bancos en Colombia Universidad Santo Tomás - Icontec	
Nombre: _____ Cargo: _____ Entidad: _____ Fecha: _____	
La siguiente metodología está desarrollada bajo la norma ISO 22301:2012 integrada con los modelos de evaluación de madurez del SGCN (GTAG 10-COBIT 4.1-BCMM). Diligencie cada una de las preguntas escogiendo la opción que más se ajuste según su entidad y de acuerdo a las calificaciones. Al final obtendrá un resultado, por criterios y global, del nivel de madurez de su SGCN. Apóyese en la GUÍA METODOLÓGICA.	“CALIFICACIONES 1. En preparación 2. Básico 3. Establecido 4. Administrado 5. Optimizado”
1. CONTEXTO DE LA ORGANIZACIÓN	0,3
Establecimiento de aspectos y factores internos y externos del SGCN	5

Identificación y documentación de aspectos del SGCN (procesos, política, objetivos, criterios, propósito)	5
Definición y establecimiento de las necesidades y expectativas de partes interesadas	5
2. ALCANCE DEL SGCN	0.5
Se tienen determinados los límites, requisitos y aplicabilidad del SGCN	5
Partes a ser incluidas y definidas en el SGCN	5
Alcance del SGCN según productos, servicios, tamaño, partes interesadas, dominios y diseño organizacional	5
3. LIDERAZGO	1.5
Compromiso, apoyo, patrocinio y gestión, por parte de los ejecutivos y la alta gerencia al SGCN	5
Establecimiento y comunicación de la política de continuidad al interior de toda la organización	5
Asegurar la definición de roles, responsabilidad, autoridad y rendición de cuentas del SGCN	5
4. PLANIFICACIÓN	0.5
Identificación y determinación oportuna de riesgos y oportunidades	5
Alineación estratégica para prevenir efectos y evaluar acciones	5
Definición y claridad de los objetivos del SGCN alineados a los planes y estrategias	5
5. RECURSOS	1.0
Determinar y proporcionar los recursos necesarios para atender el SGCN	5
Recursos que cuentan con competencia, habilidades, experiencia y toma de conciencia para el SGCN	5
Dispone de mecanismos de comunicación interna y externa, quién, cuándo, dónde y procedimientos	5
Información documentada del SGCN (creación, actualización, control, mejora)	5
6. OPERACIÓN	0.750
Definición, evaluación y administración de riesgos y análisis de impacto al negocio RA-BIA	5
Diseño, determinación y administración de estrategias DRP y BCP para todo el SGCN	5
Diseño, determinación y administración de planes DRP y BCP para todo el SGCN	5
Procedimientos del SGCN y administración y respuesta a incidentes	5
Definición, ejecución y evaluación de ejercicios y pruebas al SGCN	5
7. EVALUACIÓN DE DESEMPEÑO	0.25
Evaluación y medición de todo el procedimiento de continuidad del negocio	5
Realización y cumplimiento de auditorías internas planificadas	5
Revisión y evaluación de los ejecutivos y la alta dirección o gerencia al SGCN	5
8. MEJORA	0.25
Identificación, monitoreo y solución de no conformidades y acciones correctivas	5
Mejora continua asociada al mantenimiento, actualización y conciencia sobre SGCN	5
CALIFICACIÓN GLOBAL	5.0
DESCRIPCIÓN CALIFICACIÓN GLOBAL	OPTIMIZADO

*SGCN: Sistema de gestión de continuidad del negocio

Fuente: elaboración propia adaptada de la norma ISO 22301:2012 y metodologías de evaluación de madurez del sistema de gestión de continuidad del negocio.

Guía para diligenciar la metodología de evaluación de la madurez del sistema de gestión de continuidad del negocio del sector bancario colombiano

La guía para diligenciar la metodología de evaluación de madurez del sistema de gestión de continuidad del negocio, es un instrumento que puede ser utilizado por las entidades que quieran realizar una evaluación de la evolución y madurez del sistema de gestión de continuidad del negocio de su organización. Esta metodología está construida bajo la integración de la norma ISO 22301 con otros modelos de evaluación de madurez de la continuidad. Debe ser diligenciada por la o las personas que administran, manejan y gestionan el plan de continuidad de las organizaciones. Se pueden establecer grupos focales para su revisión y diligenciamiento y que tengan interacción y relacionamiento con el sistema. Para realizarla deben apoyarse en la tabla “calificación de niveles” para

escoger la opción más acorde de acuerdo a su entidad. Se establecen dentro de la calificación 5 niveles (en preparación, básico, establecido, administrado, optimizado) dichos niveles están explicados en la respectiva tabla. A continuación se describen los pasos para que la metodología sea aplicada correctamente en su organización y le pueda entregar un resultado óptimo y adecuado:

1. Defina los profesionales o grupo focal que diligenciará la metodología y los cuales preferiblemente tengan trayectoria y conocimiento del sistema de gestión de continuidad del negocio de la organización.
2. Diligencie los datos iniciales del encabezado de la metodología (nombre, cargo, entidad, fecha).
3. La metodología consta de 26 aspectos agrupados en 8 criterios de la norma ISO 22301, de la siguiente forma:

Tabla 3. Criterios de calificación.

Criterio	Número aspectos	Ponderación	Calificación a escoger
1. Contexto organización	3	5 %	1. En preparación 2. Básico 3. Establecido 4. Optimizado 5. Administrado
2. Alcance del SGCN	3	10 %	
3. Liderazgo	3	30 %	
4. Planificación	3	10 %	
5. Recursos	4	20 %	
6. Operación	5	15 %	
7. Evaluación de desempeño	3	5 %	
8. Mejora	2	5 %	

Fuente: elaboración propia.

4. Escoja para cada aspecto de los 8 criterios la calificación que considere más apropiada de acuerdo a su organización. Para cada criterio se da una ponderación que va de acuerdo a criterio de expertos que es más indispensable y tiene más peso en la evaluación.
5. Cada calificación se va acumulando para obtener un ponderado al final de todos los aspectos. Revise con detalle cada una de las calificaciones escogidas.
6. Al final de los aspectos va a obtener una calificación global que le mostrará de manera cualitativa y cuantitativa el resultado de su evaluación, el cual se describe en la tabla 4.
7. Dicho resultado debe ser ubicado dentro de la pirámide de niveles de madurez del sistema de gestión de continuidad del negocio, descrita en la figura 1.
8. De acuerdo al resultado obtenido en la aplicación de la metodología la siguiente es la descripción de los resultados según cada nivel:

En preparación: la organización está en un nivel de solo alistamiento para cumplir con los requerimientos y aspectos de un sistema de gestión de continuidad, no cumple con los criterios de la norma ISO 22301. La organización debe definir un plan de trabajo que le permita evolucionar en su SGCN de manera inmediata.

Básico: la organización cumple con algunos de los criterios iniciales de un sistema de gestión de continuidad inicial. No cubre los requerimientos mínimos definidos en la norma ISO 22301.

Establecido: la organización ha definido en términos generales los aspectos y criterios principales de un sistema de gestión de continuidad del negocio de acuerdo a los requisitos de la norma ISO 22301. Tiene un sistema que puede responder de forma inicial ante eventos de continuidad del negocio.

Administrado: la organización tiene un sistema de gestión de continuidad de negocio integral que cumple con los requisitos de la norma ISO 22301. La organización se encuentra en un nivel que le puede permitir certificarse en la norma en el mediano plazo, ya que cumple con los requisitos necesarios.

Optimizado: la organización tiene un sistema de continuidad del negocio muy maduro que está integrado con los demás sistemas de gestión de la empresa. La alta gerencia tiene inherencia y apoyo total sobre el sistema y se genera evaluación y mejora continua planificada. Se puede la organización certificar en la norma ISO 22301 en el corto plazo.

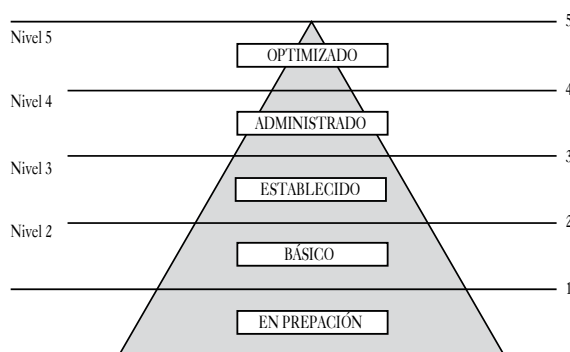
9. Posterior a la calificación y nivel de madurez de la organización, se pueden tomar las medidas pertinentes para poder mejorar el nivel en caso necesario, para revisar los aspectos a mejorar puede

Tabla 4. Resultados de calificación.

Resultado calificación	Descripción calificación madurez
Entre 0 y 1	En preparación
Entre 1,1 y 2	Básico
Entre 2,1 y 3	Establecido
Entre 3,1 y 4	Administrado
Entre 4,1 y 5	Optimizado

Fuente: elaboración propia.

Figura 1. Niveles de madurez del SGCN.



Fuente: elaboración propia.

apoyarse en la tabla calificación de niveles, con el fin de identificar con claridad qué aspectos mejorar o cambiar de cara a la evolución y capacidad del sistema.

10. Realice esta evaluación cuando lo considere necesario o cuando se realicen cambios o modificaciones representativos en la organización o en el sistema de gestión de continuidad del negocio en general. Puede apoyarse en la alta gerencia para realizar nuevamente la evaluación de madurez.

CONCLUSIONES

El sistema de gestión de continuidad del negocio es un tema de alta relevancia e importancia para las organizaciones, debido a que la no adecuada evaluación, medición y revisión del mismo, puede causar graves problemas e inconvenientes para las organizaciones, específicamente del sector bancario colombiano, afectándolas como sector.

Mediante este estudio se logró entender y analizar las diferentes metodologías existentes que evalúan la madurez del plan de continuidad del negocio a nivel nacional e internacional y su aplicabilidad en las diferentes organizaciones, adaptándolas a las organizaciones del sector bancario colombiano.

Por medio de la encuesta aplicada se obtuvo un diagnóstico que permitió evaluar y medir la actualidad de las entidades del sector bancario en temas relevantes asociados a la continuidad del negocio, encontrando debilidades y puntos fuertes, así como oportunidades para madurar en continuidad de negocio como gremio.

El diagnóstico como resultado de la herramienta de medición le aportó gran valor a las entidades, las cuales entendieron y contextualizaron el presente del sistema

de gestión de continuidad de negocio del sector, identificando fortalezas y debilidades.

La integración de la norma ISO 22301:2012 con las metodologías de evaluación de madurez, permitió identificar aspectos relacionados que se podían integrar en criterios aplicables para evaluar la madurez de forma transversal, apoyando el funcionamiento y la mejora de otros sistemas de gestión en las entidades, como calidad, riesgos, medio ambiente, entre otros.

Mediante el desarrollo de este trabajo se dio respuesta al problema que originó la investigación, ya que se diagnosticó y se elaboró una herramienta integral que no tenían las entidades, que ayudó al fortalecimiento, mejora del gremio e identificación de posibles impactos, corroborando las hipótesis planteadas al inicio de la investigación.

Para las entidades es de gran valor una metodología de evaluación de madurez de la continuidad del negocio integrada con la norma ISO 22301:2012, debido a que son exigencias de entes de vigilancia y control y exigencias de sus propios clientes. De tal manera la metodología construida fue una herramienta para que las entidades analizaran y mejoraran en su plan de continuidad de negocio y pensarán en pretender certificarse en la norma.

La investigación aportó al bienestar de la sociedad, en la medida que la aplicación de los elementos y fases de la evaluación de madurez del sistema de gestión de continuidad del negocio contribuyen a la protección del recurso humano tanto al interior de las organizaciones como fuera de ella.

Este tipo de investigaciones son muy interesantes y tienen muchos campos y temas por abarcar, sería recomendable hacer un instrumento de medición que pueda evaluar muchos más aspectos y que de alguna

manera se pueda integrar con otros sistemas de gestión existentes en las empresas.

Para este tipo de investigaciones, y según la descripción del proyecto, se recomienda incluir mínimo el 95 % de nivel de confianza con un margen de error del 5 %, o en su defecto hacerlo con el total de la población, que para el caso de este proyecto no fue posible.

Se presentaron algunas dificultades en la interpretación y análisis de los resultados de las encuestas debido a que se utilizaron algunas variables muy abiertas que no permitían concretamente tener un resultado y esto hacia que se sesgaran los resultados en algunos casos, específicamente para el encabezado de la encuesta.

Algunas de las preguntas de la encuesta no eran claras para quien la diligenciaba, por lo cual se hizo importante aplicar las encuestas presencialmente en las entidades ubicadas en Bogotá, para las entidades de otras ciudades se hizo de manera virtual, generando algunos retrasos en los tiempos del cronograma.

Se presentaron dificultades en la escogencia de las entidades, ya que al principio se iban a tomar todas las 25 entidades, pero algunas de ellas no participaban en el proyecto por confidencialidad de la información, ante lo cual se realizó una muestra probabilística por conveniencia, descartando a las entidades que no participaban en el proyecto, contando al final con 18 entidades que era la muestra requerida.

Se presentaron algunas dificultades y desviaciones en el proyecto reflejadas en el cronograma, correspondientes a demora en la aprobación del proyecto por las entidades debido a que el proyecto requirió de información confidencial de las entidades que participaron. Adicionalmente se presentó demora en el diligenciamiento de la encuesta debido a que en algunas entidades, por temas de seguridad de la información, era difícil diligenciar y responder algunas preguntas de la

encuesta, por lo cual se gestionó con áreas específicas a nivel gerencial para obtener la aprobación y el apoyo con el diligenciamiento de la encuesta.

En el presupuesto económico proyectado versus el ejecutado se presentó una diferencia que no afectó o impactó en términos generales el proyecto, ya que se contaba con una provisión adicional para atender estas situaciones.

Según el punto de vista de las entidades bancarias, sería conveniente realizar una evaluación mínimo una vez al año al plan de continuidad del negocio con la herramienta metodológica, tanto cada entidad como una aplicación en el gremio, para discutir los resultados y oportunidades de mejora de la evaluación en el comité de continuidad de Asobancaria.

REFERENCIAS

- Asociación Bancaria y Entidades Financieras de Colombia Asobancaria. (2006). *Guía para la elaboración de planes de contingencia*. Bogotá.
- Gutiérrez, M. (2014). *Investigación cualitativa aplicada*. Bogotá: Universidad Javeriana.
- Hernández, A. (2008). El método hipotético-deductivo como legado del positivismo lógico y el racionalismo crítico: su influencia en la economía. *Ciencias Económicas* 26(2), 183-195.
- Hernández, Fernández y Baptista. (2010). *Metodología de la investigación*. 5.ª edición. México: Mc Graw Hill.
- Instituto Nacional de Tecnologías de la Comunicación –INTECO-. (2010). Curso de sistemas de gestión de la seguridad de la información según la norma UNE-ISO/IEC27000. Recuperado de <https://es.scribd.com/document/33892096/>

Sgsi-La-Norma-Une-Iso-Iec-27000-Series-Gestion-de-la-Seguridad-de-la-Informacion.

ISO. (2012). ISO 22301, Societal Security - Business Continuity Management Systems-Requirements. Ginebra: ISO.

IT Governance Institute. (s.f). COBIT 4.0: Una Actualización Principal en el Estándar Internacional Permite a las Empresas Aumentar su Valor IT y Reducir los Riesgos. Recuperado de <https://www.isaca.org/About-ISACA/Press-room/News-Releases/Spanish/Pages/>

COBIT-4-0-Una-actualizacion-principal-en-el-estandar-internacional-permite-a-las-empresas-aumentar-s.aspx

Quevedo, J. (2012). Revisión de modelos de gestión de continuidad del negocio. *Revista de Investigación en Sistemas e Informática* 9 (1), 91-110.

The Institute of Internal Auditors North America. (s.f). Global Technology Audit Guide. Business Continuity Management. Recuperado de <https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG10.aspx>