MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

MARCO DE REFERENCIA PARA EL DESARROLLO E IMPLEMENTACIÓN DE PLANES DE CONTINUIDAD DE NEGOCIO EN PYMES DEL SECTOR INMOBILIARIO DEL ECUADOR.

Propuesta de artículo presentado como requisito para la obtención del título:

Magíster en Auditoría de Tecnologías de la Información

Por el estudiante: SOLIS OROBIO Juan Carlos

Bajo la dirección de: GONZALEZ CARRIÓN Raúl Vicente

Universidad Espíritu Santo
Maestría en Auditoría de Tecnología de la Información
Samborondón - Ecuador
Agosto del 2018

Marco de referencia para el desarrollo e implementación de planes de continuidad de negocio en pymes del sector inmobiliario del ecuador.

Frame of reference for the development and implementation of business continuity plans in SMEs of the real estate sector of Ecuador.

Resumen

El sector inmobiliario del Ecuador se ha visto afectado por eventos disruptivos de diferente naturaleza en los últimos años, los niveles de afectación de estos eventos han sido medidos desde diversas perspectivas por parte de entes gubernamentales y privados; a esto se suman la progresiva competencia entre organizaciones del sector, demandas cada vez más exigentes de los clientes y partes interesadas y elevados costos operativos de varias de estas organizaciones. Estos factores, comprometen a las empresas a tener firmeza en la operatividad de sus procesos claves, de manera que, independiente de su tamaño, éstas puedan continuar operando en caso que eventos disruptivos se presenten. El presente trabajo de investigación es el compendio de una profunda revisión de literatura y el análisis e interpretación de una investigación cualitativa que ha buscado estudiar esta problemática particular del sector; con los resultados obtenidos, se ha podido desarrollar un marco de referencia metodológico para la implementación de planes de continuidad en éstas compañías, el cual se adapta a la realidad y limitaciones observadas en estas empresas y utiliza como base las directrices del estándar ISO 22301:2012. Finalmente, el trabajo de investigación deja las puertas abiertas a nuevas investigaciones posterior a la implementación del marco de referencia propuesto, tales como la medición de resultados posterior mediante la utilización de herramientas administrativas.

Palabras clave:	Tecnologías de la información, seguridad informática; continuidad de negocios; PCN; PRD

Abstract

The real estate industry of Ecuador has been affected by disruptive events of different nature in recent years, the levels of impact of these events have been measured from different perspectives by governmental and private entities; this is compounded by the progressive competition among organizations in the industry, increasingly demanding demands from customers and interested parties and high operating costs of several of these organizations. These factors commit companies to be firm in the operation of their key processes, so that, regardless of their size, they can continue to operate in the event of disruptive events. The present research work is the compendium of a thorough literature review and the analysis and interpretation of a qualitative research that has sought to study this particular problem of the sector; With the results obtained, it has been possible to develop a methodological reference framework for the implementation of continuity plans in these companies, which is adapted to the reality and limitations observed in these companies and uses the guidelines of the ISO 22301: 2012 standard as a basis . Finally, the research work leaves open doors to new researches after the implementation of the proposed reference framework, such as the subsequent measurement of results through the use of administrative tools.

Key words	Information technology; informatics security; business continuity; BCP; DRP

INTRODUCCIÓN

De acuerdo con (Loyola, 2011) el nacimiento de la recuperación de desastres se dio en los años setenta, cuando Norman L. Harris, Edward S. Devlin y Judith Robey buscaban un método de planificación y gestión que evitara la continua atención de problemas de forma improvisada. Las primeras conceptualizaciones se desarrollaron a partir de que los administradores de centros de cómputo empezaran a reconocer la dependencia de sus organizaciones con sus sistemas computarizados.

Durante los ochentas y los noventas, la recuperación tecnológica ante desastres y la industria de la recuperación ante desastres crecieron rápidamente, esto, ante la conciencia por parte de las organizaciones de que las interrupciones de tecnología (en adelante TI) podrían tener impactos significativos en la continuidad de sus operaciones. Con el rápido crecimiento de internet las organizaciones de todos los tamaños se volvieron más dependientes de la disponibilidad de sus sistemas informáticos; este incremento de dependencia a los sistemas de TI así como la conciencia de posibles desastres a gran escala como el "11 de septiembre del 2001", el terremoto del océano índico del año 2004, accidente nuclear de Fukushima y otros eventos disruptivos de este orden aportaron al crecimiento de diversas industrias relacionadas a la recuperación de desastres.

En la actualidad, la gestión de la continuidad abarca todas las funciones y recursos de las organizaciones a nivel mundial; por ello, la necesidad de continuidad en varias empresas y sectores se han convertido en propósito de regulación gubernamental en diversas economías. En el Ecuador, varias empresas comenzaron con la incorporación de la gestión de la continuidad a partir de la publicación de la norma INEN 2900, la cual entró en vigencia a partir del año 2014 y luego, con la implementación de la ISO 22301 a partir del año 2015, la cual fue publicada en el año 2012.

A lo antecedido, se anexan eventos disruptivos suscitados en nuestro país como el proceso eruptivo del volcán Tungurahua en el año 2006, la activación del volcán Cotopaxi en el 2015, el terremoto de Manabí y Esmeraldas del 2016 y las inundaciones en la provincia de Napo del año 2017, los cuales han dejado evidencia de la necesidad de gestionar la continuidad operativa de pequeñas y medianas empresas en el Ecuador, las cuales, de acuerdo con (Instituto Nacional de Estadísticas y Censos, 2017) tienen una participación del 76,59% del mercado empresarial ecuatoriano, reflejando así la importancia de estas organizaciones para el desarrollo económico y tributario del país.

Adicional al riesgo de que puedan suscitarse nuevos eventos catastróficos; cambios políticos, tributarios y legales podrían materializarse, lo cual podría lograr que diversos mercados nacionales limiten la inversión, y, que varios sectores productivos entren en recesión, así como sucedió con el sector Inmobiliario posterior al terremoto del 2016 mediante la publicación de la ahora derogada ley de plusvalía, la cual generó inseguridad en las inversiones inmobiliarias provocando una decaída en las ventas y construcción de proyectos de construcción.

Disrupciones como las expuestas, podrían representar la salida del mercado de varias organizaciones del sector inmobiliario en particular, en especial de aquellas cuyos presupuestos operativos no consideran la inversión necesaria para el desarrollo de un plan de continuidad de negocio, si la misma depende de recursos no tecnológicos; un plan de recuperación de desastres, si se depende de un sistema de información; o un sistema de gestión de continuidad integral, si se depende de factores tecnológicos y no tecnológicos para su operatividad.

Por otro lado, en el Ecuador las PYMES deben cumplir con varios requisitos gubernamentales, como los establecidos por (Asamblea Nacional de la República del Ecuador, 2018) que indica que una pequeña empresa debe contar con entre 10 y 49 empleados y un ingreso de hasta 1 millón de dólares anual; mientras que una mediana empresa debe estar formada por entre 50 y 199 empleados y registrar un ingreso anual de hasta 5 millones de dólares; pero, adicionalmente, las pymes del sector inmobiliario deben sobreponerse también a limitaciones inherentes a su actividad, tales como la falta de recursos tecnológicos y humanos, competencia, o,

condiciones de complejidad y alta disponibilidad de servicios para sus operaciones.

Estos antecedentes demuestran que varias compañías del sector inmobiliario en el Ecuador no se encuentran preparadas para gestionar la continuidad de sus actividades en caso de que eventos disruptivos se presenten, lo cual representa una amenaza directa a la inversión del pequeño y mediano empresario, a la estabilidad laboral de los trabajadores directos e indirectos de estas compañías y a la economía del país en general.

El presente marco de referencia permite a pequeñas y medianas empresas del sector inmobiliario diseñar e implementar un plan de continuidad de negocio a un bajo costo ajustable a sus necesidades particulares, el mismo que preparará a la compañía implementadora para responder de manera apropiada a incidentes de diversas naturalezas y poder continuar operando a medianos plazos, esto, dentro de un marco adaptable y ajustable a la realidad del entorno socioeconómico de cada organización y del país.

MARCO TEÓRICO

1.1 Administración y Planificación Estratégica

1.1.1 Generalidades

El éxito de una organización depende principalmente de una buena gestión administrativa, ya que es a través de ella que se hace la correcta distribución de los recursos con los que se cuenta. El origen de la teoría administrativa estuvo establecido con la revolución industrial, pero no fue sino hasta el final de la revolución industrial y el inicio del siglo XX que no se pudo observar un concepto completo de administración. Dentro de este periodo se destacan los autores Taylor y Fayol, quienes coinciden en todos los aspectos primordiales para una buena gestión, con la diferencia en que Taylor sostiene un énfasis superior en la capacitación y ayuda que deben recibir de forma permanente y constante quienes actúan como jefes. Esta y otras acotaciones son evidentes en lo que (Taylor, 1911) llamó *Estado Mayor de una Empresa*.

Por otro lado, las investigaciones de Henry Fayol en esta misma área se basaron en un enfoque sintético, global y universal de la empresa. Uno de los resultados fue la creación de los conocidos *14 principios de Fayol*, que muchas empresas han aplicado para lograr altos índices de eficiencia, donde destacan la disciplina, autoridad y correcta delimitación de funciones (Fayol, 1916).

En la actualidad, luego de más de un siglo de evolución de las teorías administrativas, y a pesar de que se considera al recurso humano como el más valioso en la gerencia de empresas; la toma de decisiones se ven seriamente influenciadas por el factor económico, lo cual en la práctica resulta en ocasiones ser un obstáculo para los procesos modernización de las empresas, es decir, su capacidad de evolucionar y adaptarse a los cambios de los cuales dependen su productividad y posicionamiento en el mercado. Dentro de este ámbito uno de los factores más importante es la conservación y administración de la información para cuyo propósito, las tecnologías de la información brindan las herramientas necesarias. Esta realidad puede generar que la toma de decisiones sea favorable o no para el propósito del negocio, sobre esta temática (Organ, 1968) sostiene que las organizaciones pueden tender a *modernizar* sin tomar en cuenta estudios reales de los costos y productividad; esto, debido a las ventajas que se pueden obtener a corto plazo.

El acceso a las tecnologías de la información es necesario, pero debe ir acompañado de inversiones características con un propósito claro

para que ésta pueda ser absorbida, adoptada y aprendida (Lall, 2001). Es por esto que, los directivos de las organizaciones están denotando crecimiento y nuevas funciones para los departamentos de tecnología informática, esto a razón de la importancia de la información; según un estudio realizado por la revista WeWeek, la mayoría de las 500 empresas que forman parte de Fortune cuentan con un departamento de tecnología conformado por entre 2 hasta 5 personas, sin embargo, el 12% de estos departamentos tienen entre 20 o más personas.

De acuerdo con (Arribas, 2000) esta es la razón por la cual la administración de recursos tecnológicos se ha convertido en una figura primaria en los perfiles de los profesionales de la tecnología; adicional, afirma también que "el papel de los directivos de tecnologías de la información es el de asegurar que los directivos conozcan el potencial y los recursos de utilización de la TI, así como proporcionar asesoría y conocimientos técnicos para el funcionamiento de las estrategias empresariales".

1.1.2 Gestión Estratégica y Gobierno Corporativo

La planificación estratégica es una herramienta de gestión que apoya a la toma de decisiones de las organizaciones en torno a su situación actual y al camino que deben recorrer en el futuro para adaptarse a los cambios y demandas impuestas por el entorno, logrando la mayor eficiencia, eficacia y calidad en los bienes y servicios que éstas proveen (Armijo, 2009).

De acuerdo con (Casadesus-Masanell & Ricart, 2011), los actuales factores socioeconómicos a nivel mundial han generado que las organizaciones se enfoquen en la elaboración e implementación de cambiantes modelos de negocios, los cuales constituyen la lógica de la compañía, la forma en la que opera y cómo crea valor para sus inversionistas. Para estos autores, la forma en la que las actividades y recursos son usados para asegurar sustentabilidad y crecimiento diferenciándose de la competencia y satisfaciendo las necesidades del consumidor es lo que constituye un exitoso modelo de negocio.

En concordancia, un gobierno corporativo, plantea el manejo del modelo de negocio organizacional ofreciendo un conjunto de condiciones que garanticen a los diferentes inversionistas que podrán recuperar su inversión, más alguna remuneración por ella, dando un efecto importante a la gestión estratégica haciendo que la asignación de recursos sea eficiente (Giraldo, 2017).

1.1.3 Gobierno de TI

La gestión estratégica de una organización que aprovecha el factor tecnológico para el alcance de sus objetivos, debe buscar alinear tecnología y negocio mediante una apropiada gestión de TI. Autores como (Webb, Pollard, & Ridley, 2006) hablan de una evolución de la gestión de TI hacia gobierno de TI, concepto que integra gobierno corporativo y los sistemas de información estratégicos como una disciplina de investigación.

El objetivo de la implementación de un gobierno de TI es que la organización asegure que las metas sean alcanzables, los riesgos debidamente considerados y los recursos organizacionales debidamente utilizados (IT Governance Institute - ITGI, 2005). El gobierno de TI busca entre otras cosas la alineación estratégica entre tecnología y negocio, visualizar oportunidades de negocio generadas por la TI en el futuro, promover ciclos

de procesos que incluyan la gestión del cambio y responder a las exigencias de los agentes de la empresa y a la sociedad (Giraldo, 2017).

1.2 Continuidad del Negocio

1.2.1 Generalidades

Las empresas, al igual que otros elementos de la sociedad, están en riesgo de un gran número de amenazas naturales, tecnológicas y humanas. El crecimiento de regulaciones específicas para algunas industrias, requisitos de gobierno corporativo, presión de inversionistas, medios de comunicación y escrutinio público exigen un enfoque de gestión del riesgo de los negocios y gestión de la continuidad (Shawn & Harrald, 2004). Por ello, planificar la continuidad del negocio es parte esencial para que funcione cualquier organización moderna que tome su negocio y clientes seriamente (Disaster Recovery, 2014).

Dentro de los últimos años, el mundo ha sido testigo de muerte, devastación y destrucción en una escala de ocurrencia y ferocidad cada vez incrementada. El tsunami de Sumatra del 2004, el huracán Katrina del 2005, el tsunami en Japón del 2011 son ejemplos de eventos que seriamente han impactado las operaciones de los sectores público y privado (Kennedy, 2011).

La gestión de continuidad de negocio es un proceso holístico que identifica amenazas potenciales y el impacto a las operaciones del negocio que esas amenazas, si se materializan, pueden causar (Aronis & Stratopoulos, 2016). Por ello, organizaciones de varias industrias buscan desarrollar e implementar un sistema de gestión de continuidad de negocio (en adelante “SGCN”).

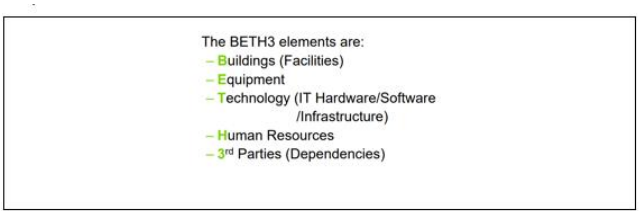


Gráfico 1 - Elementos de BETH3 - Fuente: BETH3 - Simplifying the BCM Strategy Selection Process

En este contexto, la Organización Internacional de Normalización (ISO) ha publicado la norma ISO 22301:2012, la cual especifica los requisitos para planificar, establecer, implementar, operar, monitorear, revisar, mantener y continuamente mejorar un sistema de gestión documentado que protege contra, reduce la probabilidad de ocurrencia, prepara para, da respuesta y recupera una organización de incidentes disruptivos cuando estos suceden (ISO, 2012).

1.2.2 Continuidad de Negocios

La continuidad de negocio se puede definir como el proceso impulsado por el negocio el cual establece un marco estratégico y táctico de ajuste para mejorar la organización y hacerla resistente contra la interrupción de sus objetivos claves, proporcionar un método ensayado para restaurar la capacidad de una organización para garantizar el suministro de sus productos y servicios clave después de una interrupción y proporcionar la capacidad de gestionar una interrupción del negocio y proteger la reputación de la organización y de la marca (Gonzalez, 2017).

En la actualidad, estudios como *Horizon Scan* (BCI, 2017), muestran que el 72% de disrupciones de negocios responden a incidentes relacionados con la caída no planificada de tecnologías de la información (TI) y telecomunicaciones (BCI, 2017), por este motivo, el establecimiento del Plan de Continuidad de Negocio (BCP) y Plan de Recuperación de Desastres (DRP) permiten planificar la disponibilidad de tecnología. El gráfico 2 muestra los 10 mayores causantes de interrupción en el año pasado:

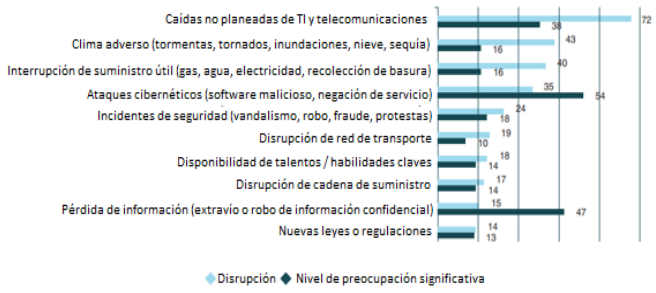


Gráfico 2 - Disrupciones de Negocios de Acuerdo a Horizon Scan - Fuente: Horizon Scan Report 2017, BCI

De acuerdo con (Sarabacha, 2008), la no disponibilidad de un proceso de negocio se genera por la pérdida parcial o total de los elementos definidos en el enfoque BETH3, el cual integra, por sus siglas en inglés, edificios, equipos, tecnología, recursos humanos y terceras partes interesadas. De acuerdo con este autor, la utilización de este enfoque permite a una compañía evaluar los requerimientos alrededor de cada elemento crítico en cada uno de los procesos de la empresa y utilizarlos para impulsar la identificación y selección de estrategias de recuperación.

El enfoque planteado por (Sarabacha, 2008), establece tres etapas que permiten la simplificación de la selección de la estrategia de continuidad que puede ser adoptada por una organización dentro del marco de desarrollo e implementación de un SGCN, estas son: análisis, desarrollo e implementación. Otros autores como (Aronis & Stratopoulos, 2016) coinciden con este enfoque en sus estudios, mientras que otros autores, tal como (Asgary, 2016), hablan de un enfoque orientado a la selección de la estrategia de continuidad basado en parámetros administrativos de la organización que aporten al cumplimiento de los objetivos empresariales.

1.2.3 Análisis de Riesgo y Análisis de Impacto al Negocio

La evaluación del estado actual de una organización y la evaluación del riesgo al cual ésta se encuentre expuesta, producto de las diferentes amenazas, van de la mano y se realizan en conjunto (Sarabacha, 2008). Dentro de este proceso misional, se desarrollan, el análisis de riesgo (RA por sus siglas en inglés), el cual identifica los riesgos potenciales a los cuales la organización se expone, y, el análisis de impacto al negocio (BIA por sus siglas en inglés), el cual identifica el impacto de la materialización de un riesgo, así como el tiempo de recuperación objetivo (RTO por sus siglas en inglés), el punto de recuperación objetivo (RPO por sus siglas en inglés) y los recursos mínimos que requiere la empresa (Gonzalez, 2017). Una vez identificados los elementos descritos, se establece los planes de continuidad de negocio (BCP por sus siglas en inglés) y los planes de recuperación de desastres (DRP por sus siglas en inglés).

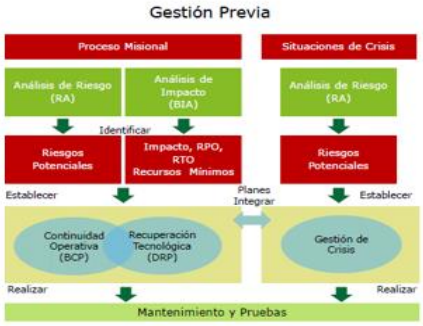


Gráfico 3 - Gestión Previa - Fuente: Clases Magistrales Continuidad de Negocio, Raúl González

Por otro lado, se realiza un análisis de situaciones de crisis, el cual, luego de la identificación de riesgos potenciales permite establecer un plan de gestión de crisis, el mismo se integra al BCP y al DRP (Gonzalez, 2017).

En su estudio, nuevos enfoques al análisis de impacto al negocio, (Sikdar, 2011), dando importancia al desarrollo del BIA, afirma:

"El Análisis de Impacto Empresarial (BIA) es un proceso importante que investiga los procesos de negocio para determinar y listar los procesos críticos que son vitales para mantener el negocio en marcha. Es necesario entender los entornos empresariales, recopilar datos e información, identificar los procesos críticos necesarios para llevar a cabo las operaciones vitales del negocio y, finalmente, preparar un informe BIA alistando sus conclusiones para ser presentado a la alta dirección. Deben considerarse los esfuerzos por considerar los ambientes internos y externos y los riesgos que afectan la posición financiera, así como la reputación de la organización."

Por otro lado, el análisis de riesgo comprende una etapa en la cual se determinan las amenazas a las cuales se encuentra expuesta una organización y el riesgo que implica la materialización de las mismas. Sobre esta afirmación, el mismo autor recalca:

"El análisis de los datos prevé una recopilación de la información reunida en un formato significativo para obtener los datos necesarios para llegar al impacto de la interrupción en los procesos del negocio".

Sin embargo, dentro de un marco de definición del análisis de impacto al negocio, autores más empoderados en el tema, como (Kennedy, 2011) definen de una manera más clara el BIA:

"Un análisis de impacto resulta en la diferenciación entre las funciones / actividades de la organización críticas (urgentes) y no críticas (no urgentes). Una función puede ser considerada crítica si las implicaciones para las partes interesadas de los daños a la organización resultantes se consideran inaceptables. Las percepciones sobre la aceptabilidad de la interrupción pueden ser modificadas por el costo de establecer y mantener soluciones empresariales o de técnicas de recuperación apropiadas. Una función también puede ser considerada crítica si es dictada por la ley o las regulaciones."

Según (Kennedy, 2011) y (Sikdar, 2011), los principales objetivos del BIA son la recopilación y el análisis de información para presentar un informe tabulado a la alta dirección, como justificación de la provisión de la adquisición necesaria para el programa BCP, así como los recursos necesarios para su implementación. Hay tres fases principales para completar el BIA: recolección de datos, análisis de datos y reportes de BIA. Con esta definición coincide (Sarabacha,

2008), quien adicional a la recopilación y análisis de información, expresa que otros objetivos clave del BIA son: revisión de procesos de negocio, interdependencias y prioridades; enmarcamiento de aplicaciones críticas; determinación del tiempo de recuperación objetivo (RTO) y del punto de recuperación objetivo (RPO); y, de los requisitos mínimos de operación.

Para estos autores, se requiere para alcanzar el objetivo del BIA, es relevante obtener la siguiente información de la organización:

- Número de clientes, transacciones, ingresos totales, propósito de las unidades del negocio y operaciones críticas que se ejecutan.
- Costos financieros e intangibles asociados con las interrupciones del negocio en términos diarios y cómo éste cambia cuando se proyecta sobre un periodo de tiempo.
- Personal clave que se requiere para soportar el funcionamiento de las unidades de negocio después de un evento disruptivo.
- Lista de sistemas y aplicaciones críticas, incluyendo plataformas informáticas y software.
- Tiempo de recuperación objetivo (RTO), que es, el tiempo en el cual los sistemas, actividades, aplicaciones o funciones deben ser recuperados después de una interrupción para reactivar las funciones críticas.
- Punto de recuperación objetivo (RPO), que es, la cantidad máxima de pérdida información que una unidad de negocio puede sostener durante un evento.
- Plazos críticos asociados con diversas unidades de negocio y funciones empresariales.
- Alternar contingencias de procesamiento, como basarse en procesamientos manuales hasta que los sistemas estén en funcionamiento.
- Temporada o periodo del año para el procesamiento de urgencias de trabajo que deben ser documentadas.
- Numero de contacto del personal clave, administradores e involucrados claves que deben ser contactados en caso de emergencia.
- Espacio físico, equipo y personal que debe ser acomodado durante una emergencia.
- Documentación tal como SLA’s o contratos legales que deben ser mantenidos.
- Opciones de sitios alternos en caso de una interrupción prolongada.
- Flujos de dependencias externas e interdepartamentales.
- MBCO u objetivo mínimo para la continuidad de negocio, que es el nivel mínimo de servicios o productos que necesita suministrar o producir una organización una vez que restablece sus operaciones comerciales.
- MTPD, es la cantidad máxima de tiempo que puede estar interrumpida una actividad sin incurrir en un daño inaceptable.

Una vez que se ha logrado identificar y documentar cada una de las variables intervinientes en el análisis de riesgo y el análisis de impacto al negocio, posterior a la elaboración del informe BIA, se puede continuar con la elaboración de los BCP y DRP (Gonzalez, 2017). Sin embargo, el BIA es un proceso continuo que debe realizarse periódicamente para que los nuevos impactos, que pueden ser introducidos por cambios internos o externos en el entorno empresarial, sean capturados, listados y llevados a la atención de la dirección ejecutiva. Las actualizaciones pueden planificarse mensualmente o anualmente según los requerimientos de la industria y se puede configurar un sistema para supervisar que se producen las actualizaciones y se conserva un seguimiento de auditoría para actualizaciones y un programa de retención de registros (Sikdar, 2011).

1.2.4 BCP y DRP

Es la actividad realizada por una organización para asegurar que todas las funciones críticas del negocio estarán disponibles para los clientes, proveedores, reguladores y otras entidades que deben tener acceso o confiar en esas funciones (Kennedy, 2011). Acerca de su función principal, (Bautista, 2014) expone:

> "El propósito de un Plan de Continuidad de Negocio (Business Continuity Plan, BCP por sus siglas en inglés) es proporcionar procedimientos para mantener en funcionamiento los servicios críticos de la organización a causa de una interrupción de los mismos mientras se realiza la recuperación, en caso de un desastre natural o causado por humanos."

El desarrollo de un BCP, comúnmente, se realiza mediante el cumplimiento de las siguientes etapas:

Fase 1 – Evaluación de impacto al negocio

Sin importar el estándar de continuidad del negocio con el cuál se decida trabajar como guía, es fundamental evaluar el impacto de la materialización de una amenaza de forma numérica o económica para desarrollar exitosamente un BCP o DRP (Gonzalez, 2017). Por ello, a pesar de que se conoce que existen recursos limitados (humanos, tiempo, económicos) dentro de todas las empresas, éstas buscan proteger sus activos y proveer continuidad de negocio y protección en eventos de tiempos adversos a sus funciones críticas, sin las cuales los objetivos organizaciones no se podrían cumplir (Kennedy, 2011). Como resultado, un establecimiento formal del BIA, es la primera etapa del desarrollo del BCP.

Fase 2 – Desarrollo de las estrategias de mitigación

Durante esta fase se desarrollan las estrategias de recuperación que satisfagan los requisitos de recuperación del negocio (RTO, RPO y MTPD) identificados en la fase BIA. En esta fase es donde los líderes del negocio tomarán la decisión de la cantidad de recursos que se gastarán para direccionar los requisitos de recuperación (personas, dinero y tiempo). La regla de proporcionalidad entra en efecto aquí, es decir, la cantidad de recursos comprometidos con la implementación de la estrategia de mitigación deben ser inferiores o igual al costo actual de impacto si unas paralizaciones de las operaciones del negocio llegan a ocurrir. La frecuencia de potencial caída y el impacto financiero y operativo deben ser tomadas en cuenta. Todas las opciones tienen diferentes tiempos de recuperación, costos y capacidades asociadas a ellas. La dirección del negocio presentará varias opciones y costos de recuperación de las cuales se seleccionarán las estrategias apropiadas que se ajusten a los requisitos de la organización (Kennedy, 2011).

Fase 3 – Planificación

Tanto (Bautista, 2014) como (Kennedy, 2011) coindicen en el desarrollo de la planificación, ambos establecen que una vez que las estrategias de recuperación han sido identificadas y seleccionadas, el proceso continúa con la fase de planificación. Usualmente existen los siguientes tipos de planes requeridos en las mayorías de organizaciones:

- BCP integral
- BCP de una unidad de negocio
- DRP

BCP Integral

Se utiliza para evaluar y gestionar los efectos de una interrupción de emergencia significativa en las operaciones del negocio en un esfuerzo para proporcionar continuidad de las funciones críticas de la empresa. Estas funciones críticas del negocio incluyen la entrada de órdenes de clientes, completar transacciones reguladas y proporcionar a empleados y clientes acceso a procesos y funciones de misión crítica (Kennedy, 2011). Este BCP empieza con la evaluación de cada una de las unidades de negocio y su riesgo de continuidad. Este proceso abarca todos los aspectos claves del negocio, la evaluación define, para cada proceso empresarial, su criticidad y un método de recuperación. Los planes individuales de cada unidad de negocio se revisan y se actualizan anualmente, o cuando suceden cambios significativos en la organización.

BCP de unidad de negocio

Los planes de unidad se enfocan en lo requerido para restaurar la misión crítica de actividades, funciones y procesos de una particular operación de negocio. Por ende, las personas que desarrollan este plan necesitan estar íntimamente informadas en el funcionamiento interno de una unidad de negocio o función empresarial. Muchas empresas incorrectamente entregan esta tarea al área de TI para ser desarrollado junto al DRP, pero la historia ha demostrado que un plan desarrollado de esta manera más a menudo falla. Este plan debe ser asignado, desarrollado, revisado, ejercido y firmado por las personas en el área funcional a ser recuperada (Kennedy, 2011).

DRP

El DRP es el proceso que enfrenta una organización, para luego desarrollar, documentar, implementar, probar y mantener procedimientos que ayudan a la organización a retornar rápidamente a las operaciones normales y reducir al mínimo las pérdidas después de un desastre (Erbschloe, 2003). Un DRP está enfocado a los sistemas de información, diseñado para restablecer la operación de los servicios informáticos críticos específicos (hardware y software), con instalaciones, infraestructura y procedimientos alternos, en caso de una emergencia; el responsable del DRP es el departamento de TI de la organización (Bautista, 2014). El DRP cubre la restauración de las funciones técnicas que la empresa necesita para operar apropiadamente, no más, no menos.

1.3 ISO 22301

1.3.1 Generalidades

Varias normas y marcos de referencia se han diseñado para orientar a las empresas en el desarrollo e implementación de planes o sistemas de continuidad de negocio; entre ellos, DRI, ISO, BSI, NIST, COBIT5, BCI.

En el año 2007 se publicó el primer estándar internacional auditable y certificable, BS 25999-2:2007, el cual tenía la misión de definir los requisitos para un enfoque de sistemas de gestión para la continuidad de negocios basado en buenas prácticas, y en años posteriores, luego de la publicación de varios estándares similares,

se publicó finalmente en el año 2012 la norma ISO 22301, la cual se encuentra apostada en el ciclo PDCA para la planificación, establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora continua de sistemas de gestión para la continuidad de negocios (ISOTools Excellence, 2014).

ISO 22301 es una norma internacional de gestión de continuidad de negocio creada en respuesta a la fuerte demanda internacional que obtuvo la norma británica original, BS 25999-2 y otras normas. Esta norma, identifica los fundamentos de un SGCN, estableciendo el proceso, los principios y la terminología de gestión de continuidad de negocio; proporciona una base de entendimiento, desarrollo e implantación de continuidad de negocio dentro de una organización. La norma proporciona a las organizaciones un marco que asegura que éstas pueden continuar trabajando durante las circunstancias más difíciles e inesperadas, siempre protegiendo a sus empleados, manteniendo su reputación y proporcionando la capacidad de continuar operando y comercializando (ISOTools, 2017).

1.3.2 PDCA y Estructura de ISO 22301

El ciclo de Deming, o circulo "*plan, do, check, act" (*PDCA por sus siglas en inglés), es una estrategia de mejora continua de la calidad en cuatro pasos, que permite a las empresas, mediante su implementación, obtener una mejora integral de la competitividad, de productos o servicios, mejorando continuamente la calidad, reduciendo costos, optimizando la productividad, incrementando la participación de mercado y aumentando la rentabilidad de la organización (Deming, 1989).

La estrategia de la calidad de Deming se representa de forma habitual por un círculo que representa la evolución continua del ciclo PDCA. El círculo siempre debe estar en movimiento y cada uno de los pasos alimenta el siguiente, de forma que cada vez sea más sencillo avanzar y más natural (SBQ Consultores, 2013).

Las etapas del ciclo de Deming son: *Plan*, en la cual se planifican los cambios y los objetivos a alcanzar valorando los pasos a seguir y planificando lo que se debe utilizar para conseguir los objetivos; *Do*, donde se lleva a cabo lo paneado, siguiente lo estipulado en la etapa anterior en el mismo orden y proporción de lo planificado; *Check*, en la cual se verifica que se ha actuado conforme a lo planeado así como que los efectos son los correctos y se corresponden a lo que inicialmente se diseñó; *Act*, en esta etapa se recopila lo aprendido y se pone en marcha, en esta etapa suelen aparecer recomendaciones y observaciones que sirven para volver a la planificación y de esa manera, el circulo no deja de fluir (SBQ Consultores, 2013).

La norma se encuentra estructurada por diez cláusulas que especifican los requerimientos para implementar y administrar de forma efectiva un SGCN, el cual, enfatiza la importancia del entendimiento de las necesidades de continuidad la organización, implementa y opera controles y medidas para administrar la capacidad total de manejar eventos disruptivos, monitoreando y mejorando continuamente (ISO, 2012).

La estructura de norma está dada de la siguiente manera:

1. Ámbito
2. Referencias Normativas
3. Términos y Definiciones

4. Contexto de la Organización
5. Liderazgo
6. Planificación
7. Soporte
8. Operación
9. Evaluación de Desempeño
10. Mejora

Dentro de la estructura expuesta, el ciclo de Deming también se ve representado en forma circular, tomando cada una de cláusulas de la norma y adaptándolas a las diferentes etapas del ciclo:

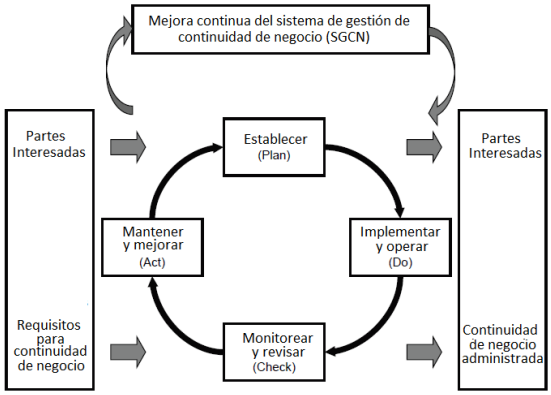


Gráfico 4 - Ciclo PDCA en ISO 22301 - Fuente: Norma ISO 22301:2012

De esta manera, podemos observar que de las diez cláusulas que conforman la norma, siete se ven representadas en el ciclo. Las cláusulas cuatro, cinco, seis y siete forman parte de 'Plan'; la cláusula ocho conforma el 'Do' del ciclo; la cláusula nueve del 'Check' y la cláusula diez constituye el 'Act' (ISO, 2012).

1.3.3 Implementación

El proceso de implementación de un SGCN basado en la norma ISO 222301 inicia mediante el entendimiento de la organización y su entorno, comprendiendo las necesidades y expectativas de las partes interesadas, y, finalmente, determinando el alcance del SGCN (Gonzalez, 2017).

Para el proceso de implementación, el grupo (ISOTools Excellence, 2014), ha publicado el diagrama del proceso de implementación de la norma desarrollado por la consultora EPPS Services, el cual, se considera ajustable a cualquier entorno organizacional; el diagrama propuesto, se encuentra presentado en el gráfico numero cinco:

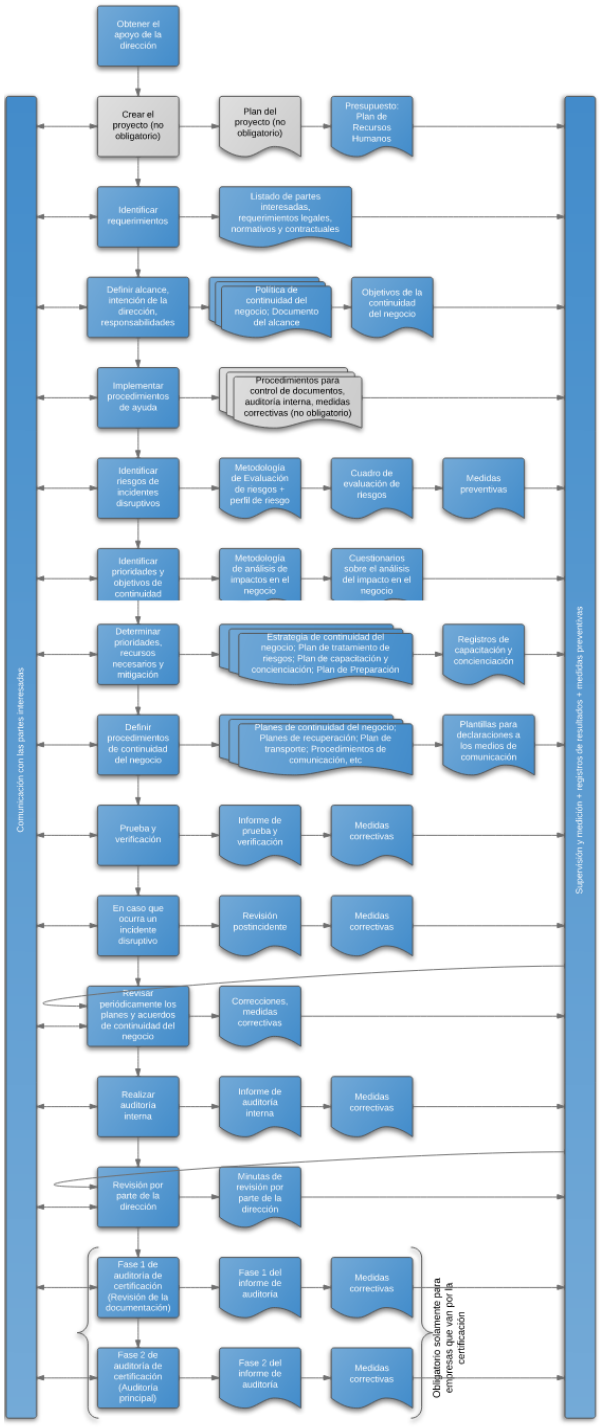


Gráfico 5 - Flujo Proceso Implementación ISO 22301

Como se puede observar, el diagrama abarca todas las etapas y análisis delimitados en el proceso de desarrollo de un BCP, integrando el ciclo de Deming en cada una de sus etapas y finalizando con las auditorías de certificación necesarias.

METODOLOGÍA.

Tipo y Alcance de Investigación

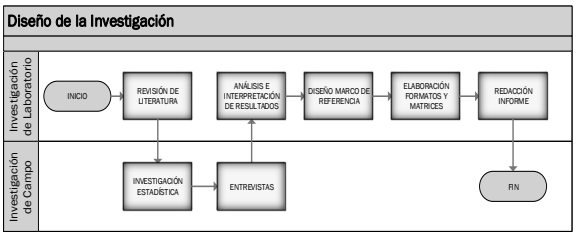
Para el desarrollo del presente trabajo se utilizó investigación de tipo cualitativo estudiando la problemática en su contexto natural y cómo sucede, sacando e interpretando el fenómeno de acuerdo a los resultados obtenidos con la técnica de la observación.

Dado que, dentro del diseño de la investigación se contempló una profunda revisión de literatura, la presente investigación tiene un alcance descriptivo, siendo útil para mostrar con precisión los ángulos o dimensiones de la situación de continuidad en las empresas a las que puede adaptarse al marco de referencia propuesto; adicional, se ha buscado mostrar con precisión las dimensiones de la implementación del marco de referencia, el cual ha sido desarrollado a la medida de las realidades de las pequeñas y mediadas inmobiliarias del Ecuador, tomando como punto de partida los criterios obtenidos mediante la utilización de técnicas de investigación como observación y entrevistas a diferentes actores del sector. Finalmente, la investigación especifica características, sujetos y objetos involucrados, variables que han sido medidas y concluye con precisión el fenómeno estudiado.

METODOLOGÍA	
Enfoque de la investigación	Cualitativo
Diseño de la investigación	• Revisión de literatura • Investigación estadística • Entrevistas • Análisis e interpretación de resultados • Diseño de marco de referencia en base a resultados obtenidos • Elaboración de formatos y matrices • Redacción de informe
Alcance de la investigación	Descriptivo
Unidad de análisis	Empresa inmobiliaria del Ecuador que reúnes las características necesarias para la investigación.

Tabla 1 - Metodología

Diseño de la Investigación



Revisión de literatura

La etapa inicial, revisión de literatura, se centró en la búsqueda de fuentes bibliográficas apropiadas para el desarrollo del trabajo de investigación; entre las fuentes investigadas se pudo recopilar artículos de revistas científicas, estudios estadísticos, investigaciones previas, libros y registros oficiales. En total se obtuvieron alrededor de 130 fuentes relevantes a la investigación y, adicional, se obtuvieron estudios previos dentro del mismo ámbito de los cuales se ha tomado lo que aplicable a la presente investigación. Adicional, se consultaron tres metodologías de continuidad de negocios de las diversas existentes a nivel mundial.

Investigación Estadística

Posterior a la recopilación y revisión de literatura, se procedió con el diseño de instrumentos que se aplicaron para obtener datos e información de la unidad de análisis establecida para la investigación. Además, se realizó la extracción de datos estadísticos contenidos en la literatura revisada en la etapa anterior, los cuales sirvieron como refuerzo a los instrumentos diseñados y brindaron soporte al desarrollo del informe final de investigación.

Entrevistas

Una vez diseñados los instrumentos de obtención de datos se procedió con la aplicación de los mismos en la unidad de análisis y otras entidades de relevancia a la investigación. Los resultados de estas entrevistas se pueden evidenciar en la sección consiguiente del presente artículo y el detalle de entes e instrumentos utilizados se detalla en la tabla a continuación:

Entidad Empresa	Experto Entrevistado Fuente	Instrumento
Inmobiliaria XIMA	Ing. Klever Sigüenza – presidente directorio	Entrevista presencial y grabada de 20 preguntas dentro del contexto riesgos e inversión del sector inmobiliario
Inmobiliaria Approach	Arq. Nohora Granados – C.E.O.	Entrevista presencial de 10 preguntas dentro del contexto comercial del sector inmobiliario
Ciudad Celeste	Ing. Jaime Rumbea – director APIVE	Entrevista telefónica de 5 preguntas dentro del contexto “eventos disruptivos del sector inmobiliario”
APIVE	Publicaciones oficiales	Matriz de recopilación de datos – Eventos disruptivos – Datos estadísticos sector inmobiliario
Cámara de la industria de la construcción	Publicaciones oficiales	Matriz de recopilación de datos – Eventos disruptivos
INEC	Publicaciones oficiales	Matriz de recopilación de datos – Eventos disruptivos – Datos estadísticos sector inmobiliario.

Tabla 2 - Actores e instrumentos aplicados en la etapa "Entrevistas" de la investigación

Análisis e interpretación de resultados

Posterior a la obtención de datos de diferentes fuentes, y, luego de haber entrevistado a personas y entes relevantes para la presente investigación, se ejecutó la etapa “análisis e interpretación de los datos e información recabada”; este trabajo de laboratorio, permitió plantear el desarrollo del marco de referencia propuesto más adelante ajustado a las expectativas y necesidades plasmadas por los entes y actores del sector inmobiliario del Ecuador. Adicional, con el análisis, se pudieron realizar matrices y formatos que ayudaron a una tabulación de datos sencilla y eficaz.

Los resultados de la investigación se encuentran plasmados en la sección consiguiente del presente artículo.

ANÁLISIS DE RESULTADOS

De acuerdo con datos del (Instituto Nacional de Estadísticas y Censos, 2016) el sector inmobiliario ha mantenido un crecimiento sostenido del 0,01% anual aproximado desde el año 2013; como resultado, las empresas inmobiliarias ocupan actualmente el 2.5% del mercado corporativo ecuatoriano, superando en presencia a otros sectores claves para el desarrollo nacional tales como minas y canteras, información y comunicación, salud, y, actividades financieras.

La elevada presencia de empresas inmobiliarias en el Ecuador podría estar justificada con la alta rentabilidad de inversión que ofrece este sector en el país; de acuerdo con el (Instituto Nacional de Estadísticas y Censos, 2017), la actividad inmobiliaria es la tercera actividad que genera más valor de producción por hora trabajada en el país, debajo únicamente de actividades financieras y de seguros; y, explotación de minas y canteras. De acuerdo con la Arq. Granados, C.E.O. de Inmobiliaria Approach, por este motivo el sector inmobiliario es atractivo para los inversionistas en el Ecuador.

Adicional, el sector inmobiliario constituye soporte directo de gestión para el sector de la construcción, el cual ocupa el 3.4% del mercado empresarial del país, logrando que ambos sectores se posicionen dentro de las 10 industrias más grandes del Ecuador.

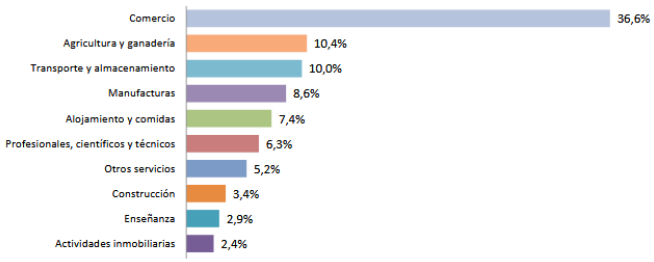


Gráfico 6 - Diez primeras actividades económicas empresariales del Ecuador año 2016 - Fuente: INEC

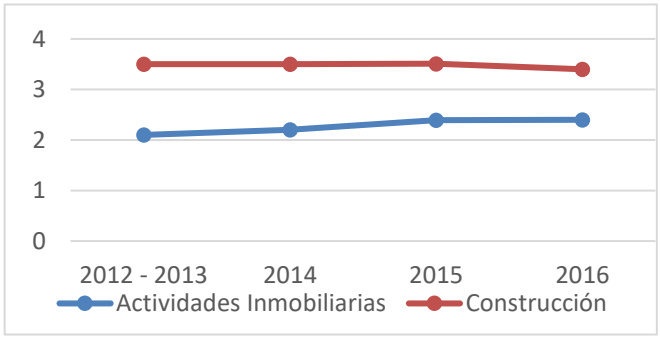


Gráfico 7- Crecimiento de Sectores Inmobiliario y Construcción en los últimos 5 años - Fuente: INEC

Durante la etapa de investigación estadística se pudieron obtener datos relevantes acerca del efecto de diversos eventos disruptivos en el sector inmobiliario. De acuerdo con datos de la Asociación de Promotores Inmobiliarios de Vivienda del Ecuador (APIVE) el evento disruptivo de mayor impacto al sector inmobiliario durante los últimos 4 años ha sido la publicación de la ley de plusvalía en diciembre del año 2016, el cual, adicional a paralizar las operaciones de empresas y construcción en curso de varios proyectos inmobiliarios, logró que las reservas bajaran hasta en un 35.2% en el primer semestre del año 2017 en comparación al mismo periodo del año anterior, el cual ya había sido impactado en un 3.1% por otro evento disruptivo, el terremoto de 7.8 grados en abril del año 2016, el mismo que por otro lado, fue beneficioso en cierta medida para el sector de la construcción.

La información obtenida permite analizar que, si bien el sector inmobiliario fue impactado por diferentes eventos disruptivos, ha tenido un crecimiento sostenido durante los últimos años, esto debido al soporte que brinda este sector al sector de la construcción, la rentabilidad sobre la inversión y la complejidad de las regulaciones legales a las que deben regirse las construcciones de proyectos inmobiliarios en nuestro país.

Posterior, durante la etapa de entrevistas, estos datos fueron expuestos al Ing. Klever Sigüenza, presidente de Inmobiliaria XIMA, importante inmobiliaria de la ciudad de Guayaquil; de acuerdo con el Ing. Sigüenza, los datos obtenidos reflejan la sensibilidad del sector inmobiliario frente a la presencia de eventos disruptivos de cualquier índole y de ahí la necesidad de contar con planes de continuidad de negocio adaptables

a las realidades de las pequeñas y medianas empresas del sector, ya que, inmobiliarias como la de él pudieron continuar operando sin ventas únicamente gracias al aporte de capital de socios y capacidad de ahorro de la compañía.

En un sondeo de opinión realizado a tres sujetos claves de tres inmobiliarias de Guayaquil, se pudo determinar que los factores que debe considerar un plan de continuidad de negocios para PYMES del sector son los descritos en la tabla tres, los cuales se encuentran analizados en base a las entrevistas utilizadas en la tabla cuatro y resumidos en el gráfico ocho.

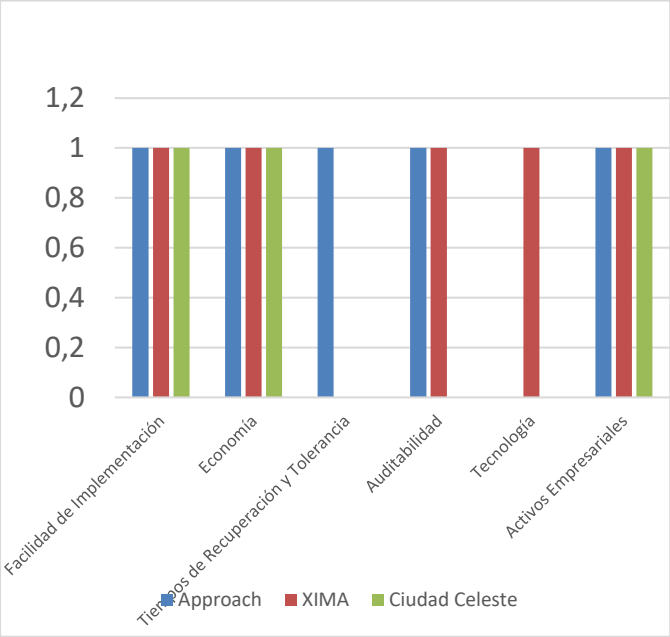


Gráfico 8- Factores a considerar para el desarrollo de planes de continuidad en PYMES del sector inmobiliario - Criterio de Expertos

Finalmente, se pudo observar que los procesos claves de las PYMES del sector inmobiliario, en mayoría, se ajustan a los descritos en gráfico nueve, y, en base a ellos y los criterios obtenidos, se procedió con el desarrollo de la propuesta planteada en la parte consiguiente del artículo. Esta propuesta toma como base los elementos y procesos de los estándares ISO 22301, ITIL y BS25999, ya que no busca sustituir ninguna norma existente sino tomar lo mejor de cada una y adaptarlas a medida de los alcances y limitaciones de las PYMES del sector inmobiliario del Ecuador.

Criterio	Facilidad de implementación			Economía			Tiempos de recuperación y tolerancia			Auditabilidad			Tecnología			Activos Empresariales		
Sujeto / Entidad	Importancia			Importancia			Importancia			Importancia			Importancia			Importancia		
	Alto	Medio	Bajo	Alto	Medio	Bajo	Alto	Medio	Bajo	Alto	Medio	Bajo	Alto	Medio	Bajo	Alto	Medio	Bajo
XIMA	x			x					x	x			x			x		
Approach	x			x			x			x					x	x		
Ciudad Celeste	x			x					x			x			x	x		
Investigador	x				x		x			x			x				x	
SUMA	4	0	0	3	1	0	2	0	2	3	0	1	2	0	2	3	1	0

Tabla 3 - Importancia de criterios expuestos a entes entrevistados

Criterio	Análisis
Facilidad de implementación	De acuerdo con los entrevistados la facilidad de implementación de la metodología propuesta es un factor determinante; ya que, al no contar con personal especializado o capacitado en temas de continuidad de negocios, el desarrollo de un BCP se ve limitada a su facilidad de implementación.
Economía	Otro factor determinante para los entrevistados es el costo de implementación, o inversión. Esto supone una limitante fuerte para las PYMES del sector inmobiliario ya que, de acuerdo con los expertos entrevistados, muchas de estas empresas no poseen presupuestos para inversión tecnológica, mucho menos para el desarrollo de un plan de continuidad que busque la recuperación de los procesos tecnológicos y no tecnológicos de una organización.
Tiempos de recuperación y tolerancia	Dos de tres expertos entrevistados consideran que la gestión inmobiliaria no demanda cortos tiempos de recuperación, debido a la naturaleza de su actividad. Han considerado que más allá de la gestión inmobiliaria, es la construcción de un proyecto lo que demanda tiempos rápidos de recuperación; sin embargo, al estar condicionada la construcción de un proyecto inmobiliario por la adecuada y oportuna gestión inmobiliaria, el investigador y uno de los entrevistados consideran importante un adecuado manejo de tiempos de recuperación y tolerancia.
Auditabilidad	Se ha podido analizar que las dos compañías que aseguran haber realizado altas inversiones en tecnología demandan que la metodología propuesta sea auditable, y de esa manera poder medir la eficacia de las medidas adoptadas, y, de igual manera, justificar la inversión que un BCP demanda. Para uno de los entrevistados, tiene baja importancia ya que las PYMES del sector inmobiliario rara vez hacen cambios en sus procesos críticos o estructura de negocios.
Tecnología	La organización entrevistada que asevera haber realizado una fuerte inversión en tecnología es la única que considera indispensable la recuperación de tecnología; al estar fuertemente tecnificada, los procesos claves de la organización dependen de la continuidad tecnológica. Sin embargo, los demás entrevistados indican que aún no han tecnificado sus procesos en totalidad, por ende, no consideran indispensable este criterio.
Activos Empresariales	Un criterio que consideran importante todos los entes entrevistados es la recuperación de los diversos activos empresariales, sobre todo de aquellos que soporten la operación organizacional; entre estos activos detallan: equipos y suministros, documentación legal y contable, y, edificios u oficinas para operación organizacional.

Tabla 4 - Análisis de criterios expuestos a los entes entrevistados

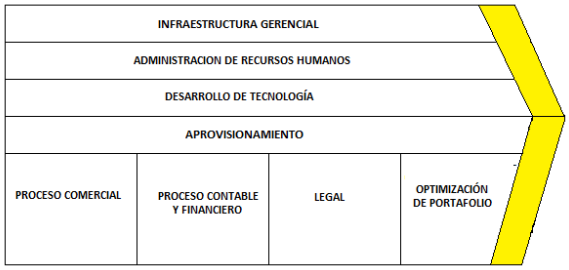


Gráfico 9 - Cadena de valor estándar del sector inmobiliario - Fuente: Pérez, R. (2012) Análisis del sector inmobiliario.

PROPUESTA

En base a los criterios analizados en el apartado anterior, y a las directrices y mejores prácticas de las diferentes normas, se propone que las pequeñas y medianas empresas del sector inmobiliario del Ecuador implementen un plan de continuidad de negocios que tome como base la metodología a continuación descrita, la cual tiene como base el ciclo PDCA, actividades establecidas en las metodologías BS25999 e ITIL, y, considera las limitaciones tecnológicas, logísticas, administrativas y presupuestarias que las organizaciones de este sector y tamaño podrían tener. Para el desarrollo de la propuesta se ha realizado un análisis de las metodologías mencionadas y se han tomado los elementos más relevantes de cada una de ellas. Este análisis puede ser observado en la tabla cinco.

La metodología propuesta se encuentra sintetizada en el gráfico diez, el cual detalla sistemáticamente las diferentes etapas que se deberán seguir en el sector estudiado para una adecuada implementación. Se debe considerar, que cada organización es única, por consiguiente, las etapas de la metodología propuesta podrían ajustarse a cada una de estas realidades sin que esto implique la modificación de la metodología como tal.

ANALISIS DE METODOLOGÍAS			
Elemento	**ISO 22301**	**BS25999**	**ITIL**
Administración BCP	X	X	
Análisis de Riesgos	X	X	X
Entendimiento de la organización	X	X	X
Estrategia para continuidad de negocio	X	X	
Administración de incidentes	X	X	X
Planificación para recuperación de T.I.			X
Plan de pruebas		X	X
Plan de mantenimiento BCP	X	X	
Desarrollar cultura de continuidad de negocios	X	X	
Política de continuidad de negocios	X	X	
Desarrollar programa de capacitación	X	X	
SLA's	X	X	X
Política de seguridad de la información	X		X

Tabla 5 - análisis de metodologías existentes.

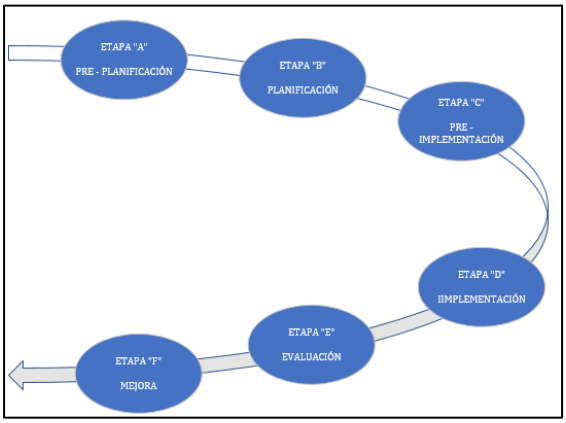


Gráfico 10 - Metodología Propuesta

La metodología comprende seis etapas: (A) Pre – Planificación, (B) Planificación, (C) Pre – Implementación, (D) Implementación, (E) Evaluación y (F) Mejora; cada una de las etapas contiene actividades claves a desarrollar dentro de la organización. Las etapas de la metodología se encuentran detalladas a continuación:

ETAPA “A”: PRE-PLANIFICACIÓN

Esta etapa, busca analizar la factibilidad de la implementación del plan de continuidad en la organización a nivel económico y administrativo previo el análisis tradicional sugerido por la norma ISO 22301, el cual busca entender la organización, su contexto y las expectativas de las partes interesadas.

Este análisis, se sugiere que sea realizado mediante la utilización de una matriz de interesados, la cual permita identificar las personas y organizaciones que participarán de forma activa en el proyecto o cuyos intereses puedan verse afectados como resultado de la implementación del plan de continuidad.

Una actividad clave de esta etapa es la designación de responsabilidades de cada uno de los interesados y la elaboración de un cronograma de implementación adaptado a las expectativas de los interesados; para esto, se sugiere la elaboración de una matriz EDT cuyas actividades posteriormente se plasmen en un diagrama de Gantt.

Finalmente, esta etapa culmina con el diseño de la política de continuidad de negocio de la organización, la cual debe ir en concordancia con otras políticas de calidad, seguridad de la información, gestión o administración existentes.

El grafico diez detalla las actividades a realizar en la etapa “A”:

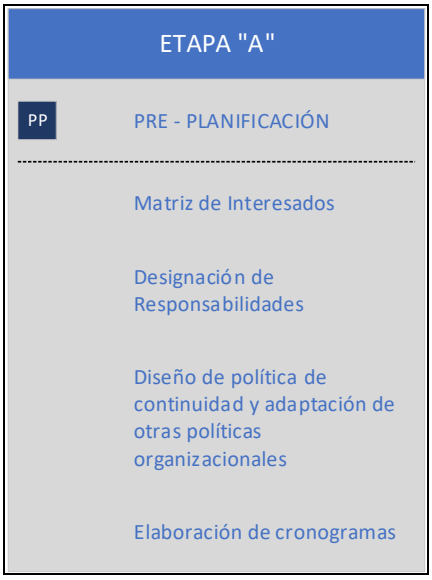


Gráfico 11 - Actividades de la Etapa "A"

ETAPA “B”: PLANIFICACIÓN

En esta etapa, y tras haber obtenido soporte y las inversiones necesarias por parte de los interesados, la organización toma la decisión de abordar el plan de continuidad mediante la utilización de la metodología propuesta; para esto, se debe identificar qué actividades se van a realizar y los motivos para hacerlo.

La primera actividad de esta etapa busca identificar el contexto de la organización mediante la utilización de la metodología planteada en la norma ISO 22301, la cual hace enfoque principal en la determinación del ámbito del plan de continuidad, los requisitos legales y regulatorios, y, la identificación de las necesidades y expectativas de las partes interesadas. Dentro de esta actividad es indispensable obtener el compromiso de la dirección, definiendo las responsabilidades y obligaciones que ésta adquiere en el desarrollo e implementación del plan de continuidad.

La segunda actividad consiste en la identificación de servicios y productos que la organización tiene

comprometido entregar a sus clientes; este análisis debe tomar en consideración la infraestructura tecnológica y las cadenas de dependencias de la misma; así como la cadena de valor de la empresa y los procesos claves de la misma. Para esta actividad se sugiere utilizar la matriz expuesta en el gráfico once, la cual permite identificar las dependencias y criticidad de los procesos claves, los cuales fueron previamente definidos en la cadena de valor organizacional.

ID	PROCESO	MANUAL / AUTOMATIZADO	DEPENDE DE					CRITICIDAD			IMPACTO NO DISP.			RIESGO CALCULADO EN MATRIZ DE RIESGOS
			Otro Proceso	Tecnología	Recurso Humano	Terceros	Otros factores	ALTO	MEDIO	BAJO	Financiero	Operativo	Legal	

Gráfico 12 - Matriz sugerida para identificación de criticidad de procesos claves

Posterior a la identificación de todos los elementos descritos, se procede con el análisis de impacto al negocio y el análisis de riesgos; se sugiere la utilización de matrices simples que identifiquen plenamente las vulnerabilidades de la compañía, las amenazas a las que se encuentra expuesta y que cuantifiquen el nivel de riesgo al que ésta se expone si hubiese una materialización de los mismos.

Finalmente, esta etapa considera el levantamiento de una planificación de recursos necesarios para la implementación del plan, un esquema de comunicación y la validación de documentos existentes que la organización podría tener como evidencia según lo establecido por los estándares ISO22301 y BS 25999:

- Política de continuidad de negocio
- Documento de términos claves
- Análisis de riesgos de la compañía
- Análisis de impacto a negocios de áreas claves
- Identificación de recursos
- Programa de capacitación
- Programa de concientización
- Plan de administración de incidentes
- Contratos con terceras partes
- DRP

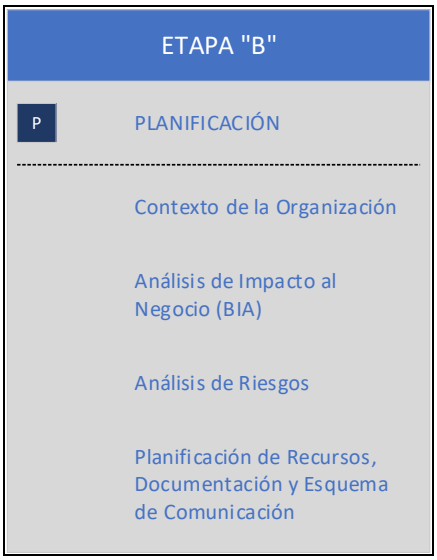


Gráfico 13 - Actividades de la Etapa "B"

ETAPA "C" – PRE-IMPLEMENTACIÓN

La etapa de pre-implementación tiene como objetivo principal asegurar la compañía mediante la adoptación de medidas de seguridad que eviten que se requieran activar los planes de contingencia o que se produzcan incidentes dentro de la misma. Estas actividades deben ser diseñadas por el equipo implementador acorde a las necesidades y expectativas levantadas en las etapas anteriores.

Por otro lado, se debe buscar asegurar la infraestructura general de la organización; se recomienda asegurar los elementos descritos en BETH3 (Buildings, Equipment, Technology, Human Resources, 3rd Parties – por sus siglas en inglés). Una actividad recomendada para este propósito es la adopción de políticas que busquen

mitigar la existencia de grandes cadenas de dependencias en cada uno de los objetos de BETH3; por ejemplo, la adopción de sistemas de información basados en tecnología en nube, eliminación de estaciones de trabajo fijas, adopción de tendencias actuales como BYOD (Bring Your Own Device - por sus siglas en inglés); todo, dentro de entornos que consideren políticas de seguridad y calidad. De esta manera se puede mitigar la dependencia de oficinas, equipos y terceras partes.

Posterior, se recomienda buscar el aseguramiento de procesos claves de las organizaciones mediante la adopción de políticas de calidad, levantamiento de documentación relevante en cuanto a manuales de procesos y procedimientos, capacitación de procesos generales al personal, entre otras.

Finalmente, una vez adoptadas las actividades necesarias para asegurar la organización, infraestructura y procesos, y, derivado de los resultados del BIA, se debe proceder con la definición de alternativas de recuperación de las actividades críticas en el caso que eventos disruptivos puedan presentarse; para esto, la organización debe tener en cuenta los posibles daños potenciales a la hora de seleccionar las diferentes soluciones o alternativas de recuperación de sus procesos claves tomando en cuenta, entre otros, los siguientes factores:

- Costo de adopción de la estrategia (recursos humanos, técnicos, otros)
- Beneficios de la estrategia
- MTPD
- RTO
- RPO

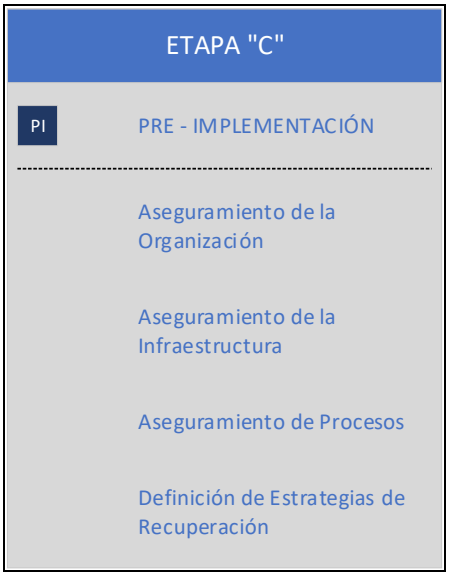


Gráfico 14 - Actividades de la Etapa "C"

ETAPA “D” – IMPLEMENTACIÓN

La cuarta etapa de la metodología propuesta busca definir los diferentes requisitos para activar el plan de contingencia mediante la aplicación de las estrategias de recuperación definidas en la etapa anterior, gestionando la respuesta a incidentes y asegurando la continuidad de los procesos críticos.

La primera actividad consiste en la definición de requisitos para la activación del plan de contingencia; esto, se puede realizar mediante la composición de equipos de personas que intervengan en la ejecución del plan, los cuales pueden variar en función del tamaño de la compañía y su estrategia de recuperación. Las organizaciones del sector deberán definir la persona o grupo que cumplan con las funciones que usualmente se asignan a los siguientes equipos: (1) equipo de respuesta a incidentes, (2) comité de crisis, (3) equipo de alera, (4) logística, (5) recuperación, (6) relaciones públicas.

Finalmente, los equipos definidos en la primera actividad, son los encargados de poner en

práctica las medidas de recuperación; entre las diferentes actividades se pueden ejecutar: gestión de alertas, gestión de alarmas, coordinación y cooperación de equipos de emergencia. En el caso de que la contingencia implique la recuperación de tecnologías de la información, se debe utilizar las directrices del DRP para recuperar aplicaciones y servicios críticos, permitiendo así la continuidad de operaciones tecnológicas.

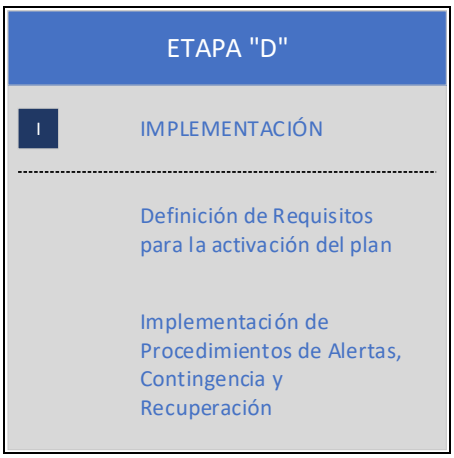


Gráfico 15 - Actividades de la Etapa "D"

ETAPA “E” – EVALUACIÓN

En esta etapa se especifican los ejercicios que ayudarán a verificar la efectividad del plan de continuidad; por ende, la organización deberá diseñar un plan de prueba para cada actividad crítica.

La primera etapa, pruebas y ejercicios del plan, se ejecuta con la finalidad de garantizar que la documentación prevista para ser usada durante eventos disruptivos sea validada en práctica y evaluación; adicionalmente, permite asegurar que las estrategias y planes se ajustan a la realidad de la organización y que son viables para el alcance de los objetivos de la misma. Las pruebas sugeridas, al igual que en la mayoría de metodologías y estándares, son pruebas de escritorio, funcional y ejercicio completo.

La segunda actividad, de medición y auditoría al plan, sugiere la utilización de indicadores claves para la detección de errores y la medición de eficiencia, para esto, se sugiere la utilización de herramientas como cuadros de mando integral.

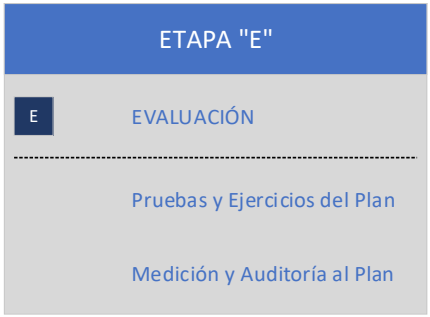


Gráfico 16 - Actividades de la Etapa "E"

ETAPA “F” – MEJORA

Esta etapa busca que el plan de continuidad de negocio implementado sea mantenido, cumpliendo con el ciclo de mejora continua, propuesto en la norma ISO 22301; se debe considerar que cualquier cambio organizacional tanto a nivel estratégico u operacional puede impactar al negocio y por ende al plan de continuidad.

Por lo descrito, la compañía debe buscar la mejora continua del plan de continuidad de manera que las capacidades, la eficacia e idoneidad del mismo se mantenga. Para esto, se sugiere seguir las tres actividades de esta etapa: (1) Análisis de resultados de evaluación, (2) actualizar el plan de continuidad en base a los cambios presentados en la estructura de la organización, sus servicios, esquemas de negocios u otros, y, (3) actualizar las políticas, acorde a las actualizaciones del plan de continuidad.

Para lograr una completa eficacia de la etapa de mejora, se sugiere implementar programas educativos que sean de fácil asimilación en la organización.

Gráfico 17 - Actividades de la Etapa "F"

CONCLUSIONES

El desarrollo e implementación de un plan de continuidad de negocios que se enfoque de forma particular en los procesos críticos o claves de una organización, resulta un aseguramiento que garantiza la continuidad de las operaciones y prolongación de la vida de cualquier compañía. Debido a los diferentes eventos disruptivos que impactaron al sector inmobiliario del Ecuador en los últimos años se planteó el presente estudio, el mismo que recabó diferentes criterios otorgados por profesionales e inversionistas del sector.

Para el desarrollo de la investigación se encontraron varias limitaciones, entre ellas se destacaron la falta de desarrollo de investigaciones previas sobre este sector productivo del país, la dificultad de acceso a información estadísticas en entes gubernamentales y privados, la no existencia de datos estadísticos del impacto de eventos disruptivos desde otros puntos de vista diferente al económico; y, la seguridad y confidencialidad que las empresas inmobiliarias mantienen sobre sus datos, estadísticas e información en general.

Con los resultados obtenidos durante la investigación, se ha podido diseñar una metodología para la implementación de planes de continuidad de negocios en empresas de este sector, particularmente, en aquellas con limitaciones de recursos tecnológicos, económicos y humanos.

El marco de referencia propuesto una vez adoptado e implementado en las pequeñas y medianas empresas del sector inmobiliario del Ecuador permitirá a estas organizaciones obtener capacidad de resiliencia frente a la posible presentación de eventos disruptivos, sean estos, de tipo natural, político, social o económico.

La metodología propuesta está conformada de seis etapas, las cuales toman como base el ciclo de Deming y las directrices generales de la norma ISO 22301:2012 adaptándolas a las necesidades particulares de las empresas del sector inmobiliario del ecuador, necesidades que fueron observadas durante la investigación. Adicionalmente, se han tomado en cuenta prácticas y elementos de las metodologías BS25999 e ITIL.

La práctica más propicia para complementar la metodología propuesta es la adecuada adopción de tecnologías, mejores prácticas y tendencias tecnológicas actuales, tales como utilización de software como servicio o infraestructura como servicio, las cuales permitirán reducir costos operativos en las compañías de este sensible sector, además de brindarles integridad, disponibilidad, confidencialidad y registros

necesarios de la información corporativa, de esta manera garantizando también su seguridad.

Para comenzar con la implementación de la metodología propuesta, es fundamental contar con el apoyo de la alta dirección de la organización y regirse a los marcos normativos planteados; por ello, las actividades de las etapas de "pre-planificación" y "planificación" deben desarrollarse de forma meticulosa y supervisadas por el líder de proyecto. Se espera que, luego de haber desarrollado las seis etapas de la metodología propuesta, las organizaciones del sector estudiado hayan desarrollado sus capacidades de recuperación y continuidad de sus procesos claves en el caso que eventos disruptivos de cualquier índole se presenten.

Es recomendable durante la etapa de "planificación" que para realizar un adecuado análisis de impacto a negocio se consideren las cadenas de dependencia de los procesos claves, al igual que la infraestructura que los soportan; ya que, una de las limitantes obtenidas durante la investigación ha sido la capacidad de identificación de dependencias en las organizaciones estudiadas, al igual que las limitadas capacidades tecnológicas de la infraestructura de soporte. De igual manera, la etapa de mejora debe poner especial atención en el análisis de resultados de evaluación para que de esa forma la actualización del plan resulte óptima.

Finalmente, se propone que posterior a la implementación y cumplimiento del ciclo de la metodología propuesta, las compañías puedan realizar la medición de resultados mediante la utilización de herramientas administrativas, tales como cuadros de mando integral e indicadores de gestión tácticos, estratégicos u operativos medidos con la adopción de técnicas como el pensamiento lean o canvas; y, de esa manera poder evidenciar el impacto de las medidas aplicadas desde una perspectiva administrativa y económica; estos resultados, podrían derivar en la aceptación de la metodología propuesta en otros sectores productivos del Ecuador, los cuales podrían ajustarle a sus necesidades y complejidades particulares.

REFERENCIAS BIBLIOGRÁFICAS

Agrawal, H. K. (2014). A Review on Optical Ethernet and its Evolution. *International Journal of Applied Engineering Research, Amity University, Noida, UP, India*.

Alair Consultores. (2005). *La Elaboración del Plan Estratégico.* ECO3 Colecciones.

Alonso, M. (2005). La gestión de los recursos humanos en la administración pública y empresarial. *Folletos Gerenciales*.

Alvarez Medina, M. T., Chavez Rivera, M. Y., & Moreno Velarde, S. A. (2006). El balanced scorecard, una herramienta para la planeación estratégica. *Revista ITSON*.

Alveiro Montoya, C. (2011). El balanced scorecard como herramienta de evaluación en la gestión administrativa. *Vision de Futuro*. doi:1668 – 8708

Armijo, M. (2009). Manual de Planificación Estratégica e Indicadores de Desempeño en el sector público. *Políticas Presupuestaria y Gestión Publica ILPES / CEPAL 2009* (pp. 1 -103). ILPES.

Aronis , S., & Stratopoulos, G. (2016). Implementing business continuity

management systems and sharing best practices at a European bank. *Journal of Business Continuity & Emergency Planning*, 203 - 217.

Arribas, A. (2000). ¿Centralizar o descentralizar los sistemas de información en la empresa? *Universidad del País Vasco*.

ASAMBLEA LEGISLATIVA DEL DISTRITO FEDERAL. (18 de diciembre de 2014.). *Ley de prestación de servicios inmobiliarios del distrito federal .* México DF.

Asamblea Nacional de la República del Ecuador. (2018, Agosto 21). Ley orgánica para el fomento productivo, atracción de inversiones, generación de empleo, y estabilidad y equilibrio fiscal. Quito, Pichincha, Ecuador: Registro Oficial N°309.

Asgary, A. (2016). Continuidad de negocio y gestión del riesgo de desastres en la educación de negocios: El Caso York University . *AD-minister*, 49 - 72.

Baldecchi, R. (2014, Septiembre). Implementación efectiva de un SGSI ISO 27001. Santiago, Chile: SONDA.

Bautista, M. A. (2014). Marco de Referencia para la Formulación de un Plan de Continuidad de Negocios, caso de estudio. *Revista Técnica Energía*.

BCI. (2017). *Horizon Scan Report.* Caversham, UK: BSI.

Beckers, K., Cote, I., & Goeke, L. (2014). A catalog of security patterns for the domain of cloud computing systems. *ITESYS Institut für technische Systeme GmbH*. doi:10.1145/2554850.2554921

Beebe, N. (2009). Digital forensics research: the good, the bad, and the unddressed. *Fifth IFIP WG 11.9 International Conference on Digital Forensics.* Orlando.

Bernal, D. (2013). Análisis de volcado de memoria en investigaciones forenses computacionales. .*Seguridad* , Número 17.

Breier, J., & Hudec, L. (2011). Risk analysis supported by information security metrics. *CompSysTech.*

C.H.Meyer. (1989). Cryptography a state of the art review. *CompEuro'89* (pp. 4/150-4/154). Hamburg: IEEE.

Cano, J. (2004). Inseguridad informática: un concepto dual en seguridad informática. *Revista de Ingeniería*, 40-44.

Carrier, B. (2006). Categories of digital investigation analysis techniques based on the computer history model. *Digital Investigation*, 121-130.

CAS Chile. (2005). *Sistema de Gestion de Seguridad de la Información CAS Chile.* Santiago: CAS.

Casadesus-Masanell, R., & Ricart, J. (2011). How to Design A Winning Business Model. *Harvard Business Review.*, Vol. 89 Issue 1/2, p100-107. 8p.

Casey, E. (2011). *Digital evidence and Computer Crime.* Baltimore: Elsevier.

Casey, E. (2008). The impact of full Disk Encryption on Digital Forensics. *ACM SIGOPS Operating System Review*, 93-98.

CISCO. (2016). *Informe anual de seguridad de Cisco 2016.* San José.

Correa García, J., Arango Serna, M., & Castaño Rios, C. (2011). Metodologías de valoración de los activos tecnológicos. Una revisión . *Pensamiento y gestión N°31*.

Costa, C. J., & Aparicio, M. (2005). Visualization of Balanced Scorecard on PDAs. *SIGDOC*. doi:10.1145/1085313.1085339

Deming, W. (1989). *Calidad, productividad y competitividad: la salida de la crisis.* Madrid, España: Ediciones Díaz de Santos.

Disaster Recovery. (2014). *Benefits of Business Continuity Planning*. Retrieved from http://www.disasterrecovery.org/business_continuity.html

Dolan-Gavitt, B. (2007). The VAD Tree: A process-eye view of physical memory. *Digital Investigation*, S62-S64.

Dolins, S. B. (2006). Using the Balanced Scorecard Process to Compute the Value of Software Applications. *ICSE*.

EC-Council. (2010). *Introduction to Disaster Recovery & Business Continuity.* EEUU.

Erbschloe, M. (2003). *Guide to disaster recovery.* Boston, Massachusetts: Thomson.

Ernst & Young. (2014). *The cyber threat landscape.*

ESET Security Report. (2015). *ESET Security Report, Latinoamérica 2015.*

EY. (2013). EY: Los delitos informáticos son la mayor amenaza mundial para la supervivencia de las empresas en la actualidad. *Business Wire*.

Fayol, H. (1916). *Administration industrielle et générale.* Paris.

Flantrmsky, H. (2012). La computación en nube y el cambio del universo informático. *Pensamiento y Cultura*, Vol 15 Pag. 88-93.

Flores, D. A. (2012). El futuro de los ataques por desbordamiento de pila. *Redifis*, 1-5.

Foster, J., Osipov, V., Bhalia, N., & Heinen, N. (2004). *Buffer Overflow Attacks.* Massachusetts: Syngress.

Ganga Contreras, F., Vera Garnica, J., & Araya Moreno, J. E. (2009). Diagnóstico y prospectiva de la administración de recursos humanos. *Revista Gaceta Laboral*, Vol 15 53 - 73.

García, D. (2014, Abril). Metodología basada en el cómputo forense para la investigación de delitos informáticos. Distrito Federal, México.

Garfinkel, S. (2010). Digital forensics research: the next 10 years. *ScienceDirect*, S64-S73.

Gartner, I. (2012). *Gartner's 2012 Hype Cycle for Emerging Technologies,.* Stamford, Connecticut, USA: Gartner.

Giraldo, L. (2017). *Gestión y Gobierno de T.I.* Samborondón, Ecuador: Clase Magistral UEES MATI.

Gómez Baryolo, O., Bauta Camejo, R. R., & Estrada Sentí, V. (2014). Modelo para la compartimentación de la información en las organizaciones. *Ciencias de la información Vol. 45*, 11-17.

González, L. (1997). Aprender a trabajar en equipo: clave de las organizaciones que aprenden, en . *Alta Dirección, núm. 191*.

Gonzalez, R. V. (2017). *Continuidad del Negocio.* Samborondón, Ecuador: Clase Magistral UEES MATI.

Granados Paredes, G. (2006). Introducción a la criptografía. *Revista Digital Universitaria*, 2-17.

Halderman, J., Schoen, S., Heninger, N., Clarkson, W., Paul, W., Calandrino, J., . . . Felten, E. (2008). Lest we Remember:

Cold Boot Attacks on Encription Keys. *ACM*, 1-15.

Hargreaves, C., & Chivers, H. (2008). Recovery of Encryption Key from Memory using a Linear Scan. *Conference on Availability, Reliability and Security.* Barcelona: Technical University of Catalonia.

Hawkey, K., Gagne, A., Botta, D., Beznosov, K., Werlinger, R., & Muldner, K. (2008). Human, Organizational, and Technological Factors of IT Security. *CHI*.

IEEE. (2007). A Study of Volatile Information Collection of Computer Forensics System for Computer Emergency Based on Ubiquitous Computing. *Third International Conference on Natural Computation (ICNC 2007)* (pp. 690-697). Haikou: IEEE Xplore Digital Library.

inCite . (2013, Noviembre 1). I.T. Disaster Recovery. *Australian Library & Information Association*, pp. 14-15.

Instituto español de estudios estratégicos. (2011). *ciberseguridad,restos y amenazas a la seguridad nacional en el ciberespacio.* Barcelona: Ministerio de Defensa.

Instituto Nacional de Estadisticas y Censos. (2012 - 2013). *Directorio de Empresas y Establecimientos.* Quito, Ecuador: INEC.

Instituto Nacional de Estadisticas y Censos. (2014). *Directorio de Empresas y Establecimientos.* Quito - Ecuador: INEC.

Instituto Nacional de Estadísticas y Censos. (2015). *Directorio de Empresas y Establecimientos.* Quito - Ecuador: INEC.

Instituto Nacional de Estadísticas y Censos. (2016). *Directorio de Empresas y Establecimientos.* Quito, Ecuador: INEC.

Instituto Nacional de Estadísticas y Censos. (2017). *Encuesta Estructural Empresarial.* Quito, Ecuador: INEC.

IONESCU, A. (2014). Security of computer networks implemented in universities and business eviroment. *Hyperion University from Bucharest*.

ISACA. (2015). *State of Cybersecurity: Implications for 2015.*

ISO. (2008). *ISO 38500:2008.*

ISO. (2012). *ISO 22301:2012.* Ginebra, Suiza: ISO.

ISO27002.es. (2013). *Sistema de Gestión de Seguridad de la Información.* Retrieved from http://iso27002.es/

ISOTools. (2017, 08 20). *Software ISO Riesgos y Seguridad*. Retrieved from https://www.isotools.org/normas/riesgos-y-seguridad/iso-22301

ISOTools Excellence. (2014, Enero 22). *PMG-SSI*. Retrieved from Blog Espacializado en Sistemas de Gestión de Seguridad de la Información: https://www.pmg-ssi.com/2014/01/iso-22301-como-surge-la-norma/

IT Governance Institute -ITGI. (2005). *IT Governance: Developing a successful governance strategy.* London : IMPACT.

Jadhav, H. (2017). Futures in the sky. *California CPA*.

Jimenez Ortiz, Y. (2003). *Aplicación del proceso de planeación para una empresa de transporte de materia y residuos peligrosos.* Monterey.

Kaplan, B., & Geiger, M. (2007). *Ram is key.* Pennsylvania.

Kendrick, R. (2010). *Cyber Risks for Business Professionals: A Management Guide* . IT Governance Publishing.

Kennedy, J. (2011, 08 17). *BUSINESS CONTINUITY AND DISASTER RECOVERY: MAKING A START*. Retrieved from Continuity Central Archive: http://www.continuitycentral.com/feature0905.html

Kern, A., Kuhlmann, M., Schaad, A., & Moffett, J. (2002). Observations on the Role Life-Cycle in the Context of Enterprise Security Management. *SACMAT*.

Korkin, I., & Nesterov, I. (2015). Applying Memory Forensics to Rootkit Detection. *ArXiv preprint*, 2-20.

Lall, S. (2001). National strategies for technology adoption in the industrial sector. *Human Development Report 2001: Harnessing Technology for Human Development*.

Leal, G. (1997, Octubre). La Explotación Sexual de Niños. *Boletin del Instituto Interamericano del Niño "INFANCIA" Tomo 67*, 234. Montevideo, Uruguay.

Loyola, R. (2011). *Propuesta de plan de contingencia de negocio en el área de informática de Enami.* Paipote, Chile: Universidad de Atacama.

Lucena, M. (1999). *Criptografía y Seguridad en Computadores.* Jaen, España: Departamento de Informática - Escuela Politécnica Superior Universidad de Jaen.

Lucena, M. (2010). *Criptografía y Seguridad en Computadores.* Barcelona.

Lucena, M. (2010). *Criptografía y Seguridad en Computadores.* Jaen, España: Universidad de Jaen.

Maartmann-Moe, C., Thorkildsen, S., & Arnes, A. (2009). The persistence of memory: Forensic identification and extraction of cryptographic keys. *Digital Investigarion*, S133-S140.

MacLeod, A. (2015). Effective information management and assurance for a modern organisation during a crisis. *Journal of Business Continuity & Emergency Planning*, 52-59.

Marrero, Y. (2003). La Criptografía como elemento de la seguridad informática. *ACIMED*.

Martinez, A. (2014). *Guía de toma de evidencias.* Barcelona: Instituto Nacional de Ciberseguridad.

Microsoft. (2016, Enero). *Developer Network*. Retrieved from https://privacy.microsoft.com/en-us/privacystatement

Moingeon, B., & Lehmann-Ortega, L. (2006). STRATEGIC INNOVATION: HOW TO GROW IN MATURE MARKETS. . *European Business Forum. Spring2006, Issue 24*, p50-54. 5p.

Okolica, J., & Peterson, G. (2010). Windows Operating Sistems agnostic memory analysis. *ScienceDirect*, S48-S56.

Organ, W. (1968). Social Construction of Technology. *the Academy of Management Review, Vol. 11*, 3.

Paar, C. (2014). *Introduction to Cryptography.* Retrieved from https://www.youtube.com/watch?v=2aHkqB2-46k

Paar, C., & Pelzl, J. (2010). *Understanding Cryptography.* Berlin: Springer-Verlag.

Panchal, E. (2013). Extraction of persistence and volatile Forensic Evidences from Computer System. *International Journal of computer trends and Technology (IJCTT)*, 964-968.

Pao, E., & Taplin, J. (2015, 9 21). Should We Let Ourselves Be Anonymous Online? *Time, 186*(11), 66.

Perez Castillo, J. N. (2014). Soporte Computacional para Administración Integrada de Redes y Servicios. *Ingeniería e Investigación*.

Perez, H. (1985). Impacto de la informática en la administración. *Monetaria*.

Pérez, H. (1985). Impacto de la informática en la administración. *Centro de estudios monetarios Latinoamericanos.*

Pérez, J. N. (n.d.). Soporte computacional para administración integrada de redes y servicios. *Ingeniería e Investigación*.

Perez, R. (2012, 10 24). *SlideShare - Análisis del sector inmobiliario.* Retrieved from https://es.slideshare.net/rperezllanes/analisis-del-sector-inmobiliario

Plata Cheje, R. (2009). DES/Encriptación en la Informática Forense . *Revista de Información Tecnológica y Sociedad*, 41-44.

Ramirez, A. (2009). El Malware en las organizaciones. *Sistemas Telemáticos y las Organizaciones Inteligentes en la Sociedad del Conocimiento*, 3-100.

Rodriguez, A., Utrera, M., Panzi, M., & Cabrera, G. (2007). Problemas que afectan la administración adecuada de los recursos tecnologicos en las pequeñas y medianas empresas. *Revista de la Ingenieria Industrial*.

Rodriguez, E. (2008). *Manual de Implementacion: Modelo estandar de control interno para el estado Colombiano.* Bogota, Colombia: Departamento Administrativo de la Funcion Publica.

Ruskov, P., & Todorova, Y. (2008). Building the Academic Strategy Program. *CompSysTech.*

Sachin, J., Choudary, D., & Pandey, Y. (2013). Buffer Overflow Attack Blocking using MCAIDS. *IJETAE*, 281-287.

Saecker, M. E. (2011). Marie Curie in JCE Resources and Modern Media. *Journal of Chemical Education, 88*(6), 690-692. Retrieved 11 7, 2017, from https://dialnet.unirioja.es/servlet/articulo?codigo=5106205

SANS Institute. (2002). Introduction to Business Continuity Planning. *InfoSec Reading Room*.

Saphiro, J. (2005). *Planificación Estratégica.* Johannesburg: CIVICUS.

Sarabacha, D. (2008). *BETH3 - Simplifying the BCM Strategy Selection Process .* Deloitte & Touche LLP.

SBQ Consultores. (2013, Junio 25). *El ciclo de Deming o círculo PDCA*. Retrieved from https://www.sbqconsultores.es/el-ciclo-de-deming-o-circulo-pdca/

Scaramussa, S. A., Reisdorfer, V. K., & Ribeiro, A. A. (2010). La contribución del balanced scorecard como instrumento de gestión estratégica en el apoyo a la gerencia. *Vision de Futuro*.

Seddon, P. B., Graeser, V., & Willcocks, L. P. (2002). Measuring Organizational IS Effectiveness: An overview and update of senior management perspectives. *The*

DATA BASE for Advances in Information Systems, Vol. 33, No. 2.

Shawn, G., & Harrald, J. R. (2004). Identification of the Core Competencies Required of Executive Level Business Crisis and Continuity Manager. *Journal of Homeland Security and Emergency Management 1*, 1547-7355.

Sikdar, P. (2011). Alternate Approaches to Business Impact Analysis. *Information Security Journal: A Global Perspective*, 20:128–134.

Simonsson, M., & Johnson, P. (2006). Assessment of IT Governance - A Prioritization of Cobit. *KTH, Royal Institute of Technology*, 151-161.

Syverson, P. (2011). A Peel of Onion. *Center for High Assurance Computer Systems U.S. Naval Research Laboratory*.

Tarín, P. (2015, Abril 16). *Infotecarios*. Retrieved from La Deep Web y el Proyecto Tor por el derecho a la información: http://www.infotecarios.com/deep-web-y-proyecto-tor/

Taylor, F. W. (1911). *Estado Mayor de Una Empresa.* Filadelfia, Pensilvania.

Trend Micro. (2008). *Web Application Security: Trend Micro.* . Retrieved from http:// es.trendmicro.com/imperia/ md/content/es/products/datasheets/ds 01was_081111es.pdf

van Baar, R., Alink, W., & van Ballegooij, A. (2008). Forensic memory analysis: Files mapped en memory. *Digital Investigation*, s53-s57.

van Cleeff, A. (2010). A risk management process for consumers: the next step in information security. *NSPW'10*.

Vargas, A., & Castro, A. (2011). *SGSI ISO 27000.*

Velitchkov, I. (2008). Integration of IT Strategy and Enterprise Architecture Models. *CompSysTech.*

Vera, C. (2010). Lo que esconde mi ordenador. *Reflexiones y Experiencias Innovadoras en el Aula*.

Volti, R. (2006). Society and Technological Change. *Worth Publishers*, 5e.

Vomel, S., & Freiling, F. (2011). A survey of main memory acquisition and analysis techniques for the windows operating system. *ScienceDirect*, 11-22.

Vostokov, D. (2008). *Memory Dump Analysis Anthology.* Republic of Ireland: Opentask.

Voutssas, J. (2010). Preservación documental digital y seguridad informática. *Investigación Bibliotecológica*, 127-155.

Waterfield, D. (2015). *The Real Estate Law Review.* London, UK: Encompass Print Solutions.

Webb, P., Pollard, C., & Ridley, G. (2006). Attempting to Define IT Governance: Wisdom or Folly? *Proceedings of the 39th Hawaii International Conference on System Sciences - 2006*.

Weill, P., & Ross, J. (2005). IT Governance: How Top Performers Manage IT Decision Rights for Superior Results. *International Journal of Electronic Government Research*, 63-67.

Wessels, E., & van Loggerenberg, J. (2006). IT Governance: Theory and Practice. *Proceedings of the Conference on Information Technology in Tertiary Education*.

Wlosinski, L. G. (2014). *Continuity Planning: Components, Process, & Resources.* ISACA.

Wolfe, H. (2002). Encountering Encrypted Evidence. *Informing Science*, 1603-1607.

Wright, A. (2008). Searching the Deep Web. *Communications of the ACM*, Vol. 51, p-14 - 15.

Zawada, B. (2014). The practical application of ISO 22301. *Journal of Business Continuity & Emergency Planning*, 83-90.