FACULTAD DE POSGRADOS

PROPUESTA DE UN PLAN DE CONTINUIDAD DE NEGOCIO PARA UNA INSTITUCIÓN FINANCIERA DEL SECTOR PRIVADO BANCARIO DEL ECUADOR

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Magister en Gerencia de Sistemas y Tecnologías de la Información

Profesora Guía

MSc. Katalina del Rocío Coronel Hoyos

Autor

Jairo David Rojas Bustamante

Año

2017

DECLARACIÓN DEL PROFESOR GUÍA

Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los trabajos de Titulación.

_____

Katalina del Rocío Coronel Hoyos
Magíster en Gerencia de Sistemas y Tecnologías de la Información
CI.: 1711000016

DECLARACIÓN DEL PROFESOR CORRECTOR

Declaro haber revisado este trabajo, dando cumplimiento a todas las disposiciones vigentes que regulan los trabajos de Titulación.

_____

Luis Patricio Moreno Buitrón
Magíster en Gerencia de Sistemas y Tecnologías de la Información
CI.: 1705511051

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.

_____

Jairo David Rojas Bustamante
CI.: 1721671087

AGRADECIMIENTOS

A mis queridos padres Manuel Rojas y Livia Bustamante, por dejarme la mayor herencia que los padres pueden dejar a sus hijos, la educación, y por inculcarme siempre valores y las ganas de ser mejor y superarme día a día.

A mi hermana Gabriela Rojas por cada día ser mi soporte y ayuda incondicional, por estar siempre a mi lado y demostrarme un amor puro y sincero.

A toda mi familia Gracias.

DEDICATORIA

A mis padres a mi hermana con mucho cariño, porque este trabajo representa mi esfuerzo y dedicación, para obtener una de mis metas trazadas.

A mi primo Orlando Procel, que a pesar de no estar presente para celebrar juntos mi logro, me dejó un gran ejemplo de lucha constante, demostrando que no existen barreras que no se pueden derrumbar y sueños que no se puedan cumplir.

A mi Dios porque siempre guía mis pasos y pensamientos, para actuar de manera adecuada y vencer todo obstáculo.

RESUMEN

La preocupación de los directivos en el logro de mejores resultados en la eficiencia de los negocios, es una cuestión de suma importancia y ha sido presentada desde diversas aristas, en la administración de empresas; la forma en que deben ser tratados los riesgos de todo tipo, son un punto en común en los métodos que se implementen para lograr un fin determinado. El trabajo titulado “Propuesta de un Plan de Continuidad de negocio para una Institución Financiera del Sector Privado Bancario del Ecuador”, en específico en el Banco ABC, es un ejemplo de la afirmación anterior; el manejo de ahorros, préstamos e inversiones de los clientes, se exponen constantemente a contingencias o eventos que pueden afectar notoriamente el normal desempeño de la organización objeto de estudio, algunos de los riesgos más comunes es la presencia de terremotos, inundaciones, robos, desorganización y mala administración de los recursos. Por todos estos argumentos la investigación presentada tuvo como objetivo fundamental proponer de un plan de continuidad de negocios, donde se identificaron las principales amenazas y riesgos tecnológicos, así como la evaluación de los mismos. En el trabajo se analizaron varios estándares internacionales como las normas de calidad. Posteriormente se diseñó una metodología de continuidad de negocios, que consta de cuatro fases, análisis del contexto, proyección, desarrollo, verificación y control y por último la fase de mejoramiento; en esta última etapa, se propone un plan de mantenimiento, la propuesta de mejora y el informe de los resultados expuestos detalladamente en la presente investigación.

Descriptores: Plan de continuidad de negocio, riesgos, amenazas, calidad, administración, procesos.

ABSTRACT

The concern of the executives in the achievement of better results in the efficiency of the business, is an issue of many importance and has been presented from various edges in the administration of companies; the way all types of risks should be treated, is a common point in the methods that are applied to achieve a specific purpose. The paper titled "Proposal for a business continuity plan for a financial institution of the Ecuador's private banking sector", specifically for Bank "ABC", is an example of the above statement; the management of savings, loans and investments of customers, are constantly exposed to contingencies or events that can significantly affect the normal work of the organization being studied; some of the most common risks are earthquakes, floods, robbery, disorganization and bad administration of the resources. For all these issues is that this research has as a fundamental objective to propose a business continuity plan, which identified the main threats and technological risks, as well as the evaluation of them. The work analyzed different international standards as quality standards. Subsequently, a business continuity plan was designed, consisting of four phases: context analysis, projection, development, verification and control, and finally the improvement phase; in this last stage, a maintenance plan is proposed, the proposal of improvement and the report of the results are exposed in detail in the present investigation.

Descriptors: Business continuity plan, risks, threats, quality, administration, processes.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1. DESCRIPCIÓN Y OBJETIVOS DE LA INVESTIGACIÓN

1.1. Objetivos

1.1.1. Objetivo general

Proponer un plan de continuidad del negocio para una institución financiera del sector privado bancario del Ecuador.

1.1.2. Objetivos específicos

- Describir las características más relevantes de las instituciones financieras del sector privado bancario del Ecuador a efectos de la elaboración de la propuesta del plan de continuidad del negocio.
- Identificar las principales amenazas y riesgos tecnológicos que pueden interrumpir la continuidad de los negocios de las instituciones financieras del sector privado bancario en el Ecuador.
- Evaluar los riesgos en función de la magnitud de los daños, período de recuperación y tiempo máximo de interrupción que pueden ocasionar.
- Analizar las principales metodologías y estándares internacionales para la implementación de un plan de continuidad del negocio y extraer sus fortalezas.
- Diseñar un modelo de plan de continuidad del negocio para adaptarlo a la empresa caso de estudio.

1.2 Antecedentes

Toda empresa, cualquiera sea la actividad que desempeñe, está expuesta a contingencias que pueden afectar su funcionamiento, tales como, terremotos, inundaciones, robos, desorganización, mala administración, entre otros. Estas situaciones pueden obedecer tanto a factores internos como externos; y mientras mayor sea su probabilidad y la pérdida potencial, mayor será el riesgo (Hogarth, 2006). Así como ocurrió en el atentado del 11 de septiembre de 2001 a las Torres Gemelas, en donde empresas de todo tipo sufrieron pérdidas insalvables, quedando imposibilitadas para volver a funcionar.

En este sentido, Estupiñán (2007) afirma que el riesgo existe “cuando hay una probabilidad de que algo negativo suceda o que algo positivo no suceda, la ventaja de una empresa es que conozca claramente los riesgos oportunamente y tenga la capacidad para afrontarlos” (p.101).

Ahora bien, las instituciones financieras del sector privado bancario del Ecuador, donde se genera gran volumen de información de importancia a fines de canalizar los ahorros, préstamos e inversiones de muchos clientes, empresas y otros entes; tienen el deber de establecer medidas que garanticen la continuidad de operaciones en caso de ocurrencia de cualquier amenaza contra su normal funcionamiento.

Para restablecer las actividades ante este tipo de situaciones, es preciso contar con un plan de continuidad del negocio, también conocido como BCP, del inglés *Bussines Continuity Plan*. Este último es conceptualizado por BSI Group (2007), como la capacidad estratégica y táctica para planificar y responder ante incidentes e interrupciones del negocio con el fin de permitir la continuidad de las actividades con un nivel aceptable previamente definido.

El BCP sirve para identificar, evaluar y administrar los riesgos para permitir continuar con las operaciones del negocio en caso de cualquier eventualidad. En este sentido, la Resolución JB-2014-3066 emanada de la Junta Bancaria (2014), ente rector de la actividad bancaria del Ecuador; señala que el plan de continuidad:

> “Está orientado a asegurar la continuidad del negocio, la satisfacción del cliente y la productividad a pesar de eventos inesperados. Se ejecuta permanentemente como parte de la administración de riesgos. Un plan de continuidad debe contener procedimientos que se ajusten a la realidad del negocio de cada institución” (p.2).

Así que, el BCP debe proteger los procesos críticos del negocio contra contingencias naturales, humanas o tecnológicas, y evitar las pérdidas causadas por la falta de disponibilidad de los recursos de la organización.

También tiene que establecer cómo prepararse, responder y recuperarse ante eventos que provocan interrupciones, constituyendo una metodología interdisciplinaria, basada en procedimientos y medidas de seguridad, para recuperar sus funciones críticas parcial o totalmente después de una interrupción o desastre (ITEAM, 2014).

Entre los beneficios de implementar un plan de continuidad, resaltan los siguientes: (a) aseguramiento de la continuidad de las actividades, (b) prevención o minimización de las pérdidas en caso de desastres, (c) ventaja competitiva frente a otras organizaciones, y (d) asignación más eficiente de las inversiones en materia de seguridad gracias al análisis de riesgos (Béjar R, 2013).

Cabe destacar que, la norma internacional para la gestión de la continuidad del negocio, denominada ISO 22301:2012, establece cómo identificar las amenazas potenciales de una organización y los impactos en las operaciones de negocio a fin de contar con capacidad de respuesta para salvaguardar sus intereses. Además, explica las fases del BCP: (a) descripción del negocio y análisis de riesgos, (b) estrategias o mitigación del riesgo, (c) desarrollo de implantación del plan, y (d) mantenimiento del plan (ISO, 2012).

Por su parte, la norma ISO/IEC 27005:2011, establece las directrices para la gestión del riesgo de seguridad en la información para todo tipo de organización. Procura preservar la confidencialidad, integridad y disponibilidad de la información, mediante los siguientes pasos: (a) establecimiento del contexto, (b) evaluación del riesgo, (c) tratamiento del riesgo, (d) aceptación del riesgo, (e) comunicación del riesgo, y (f) seguimiento del riesgo (ISO, 2011).

El marco de trabajo para el gobierno de la TI, desarrollado por la Information Systems Audit and Control Association (ISACA), denominado COBIT 5, tiene por objeto organizar y optimizar los estándares internacionales relacionados con la tecnología de la información en las organizaciones, presentando un conjunto de prácticas enfocadas al control, con base en criterios de calidad, confianza y seguridad. COBIT 5 se fundamenta en cinco principios: (a)

satisfacer las necesidades de las partes interesadas, (b) cubrir la empresa de extremo a extremo, (c) aplicar un marco de referencia único integrado, (d) hacer posible un enfoque holístico, y (e) separar el gobierno de la gestión (ISACA, 2012).

Asimismo, la guía elaborada por el Business Continuity Institute (BCI), denominada *Good Practice Guidelines* (GPG), que en español se traduce: Buenas prácticas para la continuidad del negocio, explica el cómo y el porqué de los principios de la disciplina de continuidad del negocio, incluyendo la terminología de la norma ISO 22301, para asegurar los más altos estándares en su ejecución. Está integrada por seis secciones: (a) política de BCM y programa de administración, (b) entendimiento de la organización, (c) determinando la estrategia de continuidad del negocio, (d) desarrollo e implementación de responsabilidades, (e) probar, dar mantenimiento y revisión del programa de continuidad del negocio, y (f) desarrollando una cultura de continuidad del negocio en la organización (BCI, 2013).

De manera que, el presente trabajo plantea una propuesta de BCP para una institución financiera del sector privado bancario del Ecuador, que permita una recuperación ágil y ordenada frente a cualquier incidente e interrupción que amenace su normal funcionamiento; garantizando así la calidad del servicio y rentabilidad de la empresa. A tales fines, se recurre a cuatro referentes fundamentales: (a) ISO 22301:2012, (b) ISO/IEC 27005:2011, (c) COBIT 5, y (d) *Good Practice Guidelines* (GPG). Con base en estos, se confeccionará un BCP sólido, acorde con la realidad de las instituciones bancarias del sector privado en el Ecuador.

Es preciso señalar que, si bien los planes de continuidad del negocio atienden a tres tipos de riesgos: (a) naturales, (b) humanos y (c) tecnológicos; la presente investigación se enfoca en los riesgos tecnológicos.

El aporte de este trabajo, consiste en recopilar las mejores prácticas en función a los principales referentes para la confección de BCP, investigar y sintetizar esas herramientas para generar una propuesta del plan de continuidad del

negocio en una empresa privada del sector financiero bancario del Ecuador, cuya identificación se realizará mediante las siglas ABC a fin de mantener la confidencialidad de su información.

1.3. Justificación de la investigación

Las instituciones financieras del sector privado bancario del Ecuador, responsables de una función tan importante como es el manejo de ahorros, préstamos e inversiones de muchos clientes, empresas y otros entes, están expuestas a contingencias que pueden afectar su normal funcionamiento, como por ejemplo, terremotos, inundaciones, robos, desorganización, mala administración, entre otros.

Además, la Superintendencia de Bancos del Ecuador, exige que las referidas entidades, cuenten con un sistema tecnológico seguro, que garantice la continuidad de sus operaciones en todo momento.

Por lo tanto, la presente investigación está dirigida a dar respuesta a esta necesidad de seguridad y continuidad frente a riesgos tecnológicos, mediante la recopilación de las mejores prácticas o referentes para la confección de un BCP, que permitan generar una propuesta del plan de continuidad del negocio para la empresa privada del sector financiero bancario del Ecuador que para efectos de este estudio se ha denominado ABC.

1.4. Alcance

Se plantea como alcance, recopilar las mejores prácticas en función a cuatro referentes fundamentales para la confección de BCP: (a) ISO 22301:2012, (b) ISO/IEC 27005:2011, (c) COBIT 5, y (d) *Good Practice Guidelines* (GPG). Con la investigación y síntesis de esas herramientas se podrá generar una propuesta del plan de continuidad del negocio para la institución financiera ABC, enfocada en los riesgos tecnológicos de esta.

2. MARCO TEÓRICO APLICADO

2.1. Plan de Continuidad del Negocio (BCP)

2.1.1. Definición de BCP

El plan de continuidad del negocio, o BCP como también se le conoce por sus siglas en inglés (*Bussines Continuity Plan),* constituye básicamente "un plan de emergencia con el objetivo de mantener la funcionalidad de la organización a un nivel mínimo aceptable durante una contingencia", además, el BCP debe centrarse en "las medidas preventivas y de recuperación para cuando se produzca una contingencia que afecte al negocio." (Meza, 2009).

Por otra parte, Serrano R. (2013) expresa que el BCP *"*busca amortiguar en lo posible el riesgo mediante un plan global permitiendo la pronta recuperación de la operación y de la información, en caso de presentarse algún evento que afecte el flujo normal de las actividades de una organización"(p.5).

Es válido mencionar que, para el caso específico de instituciones financieras, en Ecuador se tiene la Resolución JB-2014-3066 de la Junta Bancaria (2014), en cuyo Artículo 1, numeral 2.29, define el BCP como:

> "Está orientado a asegurar la continuidad del negocio, la satisfacción del cliente y la productividad a pesar de eventos inesperados. Se ejecuta permanentemente como parte de la administración de riesgos. Un plan de continuidad debe contener procedimientos que se ajusten a la realidad del negocio de cada institución" (p. 2).

Teniendo en cuenta los criterios anteriores, así como otras definiciones dadas por organizaciones reconocidas como BSI GROUP (2007) e ITEAM (2014), se resume el concepto de BCP como la capacidad que tienen las organizaciones de planificar las acciones preventivas y circunstanciales al momento de un siniestro, para garantizar que la organización pueda continuar sus operaciones de manera aceptable, en base a la identificación de riesgos reales y potenciales que podrían interrumpir, de manera breve o indefinida, las

actividades regulares de una empresa; debido a afectaciones causadas por entes naturales, humanos o tecnológicos.

2.1.2 Evolución del BCP

La vulnerabilidad ante diferentes fenómenos naturales, ha formado parte permanente del ser humano; sin embargo, en la medida en que ha evolucionado, ha mejorado su manera de planificar acciones preventivas que posibilitan la supervivencia y disminución del efecto negativo de dichos eventos sobre sí mismo y sus medios.

Sin embargo, en la medida en que se desarrollan las sociedades, también han surgido nuevos riesgos, más que todo los que están relacionado con acciones del propio hombre, y la aparición de nuevos recursos como la información.

Ciertamente, la información se ha convertido en uno de los recursos más importantes con que cuentan las organizaciones, de ello depende en gran medida la operatividad de muchos de los procesos que en éstas se realizan. Fue por ello que en los años 60 del siglo pasado, ciertos bancos de Estados Unidos se vieron en la necesidad de tomar medidas que le permitiesen garantizar en todo momento el contenido y flujo de información como parte esencial para garantizar la continuidad de sus operaciones a modo de evitar retrasos y pérdidas económicas por la falta de información al momento justo; lo cual, poco tiempo después, se concibió como una norma legislativa a nivel mundial para este tipo de instituciones (Sun Gard Availability Services (SGAS), 2005).

Diez años después aparecen los primeros planes de contingencias, conocidos bajo el nombre de Disaster Recovery Plan (DRP), en los cuales se establecían las medidas y métodos para el resguardo de la información en los casos de desastres naturales o ataques terroristas. Seguidamente, en los 80, se implementan aplicaciones informáticas (software) y medios que garantizaran la disponibilidad de información de manera constante; lo que años después se complementó con medidas asociadas a todos los procesos operativos de las

organizaciones. A continuación se puede ver el esquema de una parte de la evolución antes mencionada:

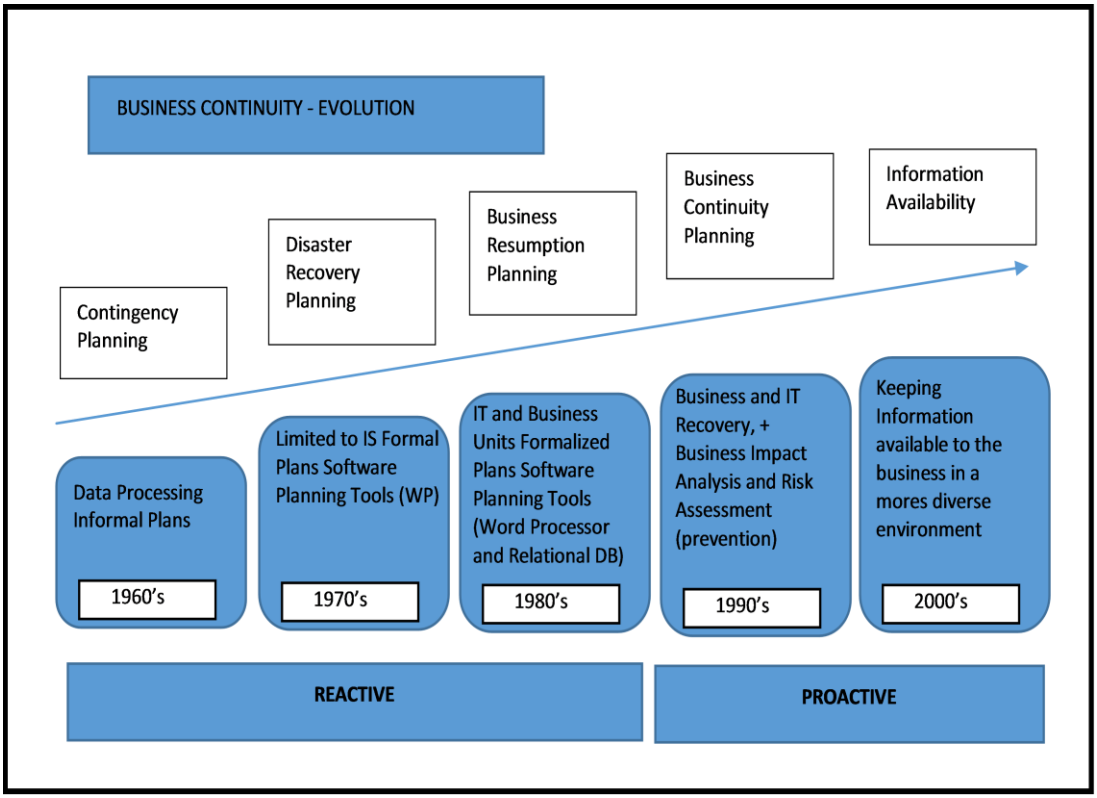


Figura 1. Evolución del BCP.
Tomado de (SGAS, 2005)

Luego de los acontecimientos que marcaron historia el 11 de septiembre de 2001, las empresas comenzaron a valorar aún más los BCP como una necesidad, más que un protocolo de acciones, a tal punto sucedió esto que, sin importar la actividad o tamaño de la organización, los BCPs se convirtieron en norma obligatoria para todos.

Fue de esta manera que los BCPs del momento cambiaron su enfoque de reactivo a proactivo; donde previamente se analizan los riesgos y posteriormente se toman medidas y se crean procedimientos para que las organizaciones puedan enfrentar los incidentes de manera oportuna

garantizando la continuidad de sus operaciones y la conservación de sus recursos (Shahrawat, 2004).

2.1.3 Beneficios del BCP

Entre los principales beneficios que ofrece el implementar un plan de continuidad, resaltan los siguientes (Meza, 2009):

- Identifica los disímiles incidentes que podrían atentar contra la continuidad de las operaciones del negocio.
- Posibilita la identificación de los tiempos críticos de recuperación para volver a la situación anterior a la catástrofe sin comprometer al negocio.
- Previene o minimiza las pérdidas para el negocio en caso de desastre.
- Garantiza la asignación de inversiones en materia de seguridad de manera eficiente.
- Representa una ventaja competitiva para las organizaciones.

2.1.4 BCP en el mundo y Ecuador

A nivel mundial, sin importar la actividad, ubicación o tamaño de la empresa, siempre estará expuesta a riesgos potenciales que podrían impactar negativamente sobre el funcionamiento de las mismas, ejemplo de ello son los desastres naturales como: sismos, tifones, tsunamis, inundaciones, etc.; y las catástrofes generadas por el hombre como: incendios, ataques terroristas, robos, etc. En este sentido, como bien se había mencionado anteriormente, luego del desastre del 11 de septiembre, tanto las empresas como los países, han tomado conciencia de la importancia que tiene el hecho de contar con un BCP eficiente, sin embargo, a pesar de ello, son muchos los que reconocen sus beneficios, pero no aplican esfuerzos en su realización e implementación.

Esta última idea se respalda en dos fuentes principales, la primera hace referencia al Chartered Management Institute, el cual aplicó una encuesta a 1257 gerentes de empresas del Reino Unido, para conocer tanto la implementación como la opinión de éstos sobre los BCP, cuyos resultados

indicaron que: “sólo la mitad tienen un BCP, a pesar de que más del 94% estuvo de acuerdo con su importancia” (Woodman, 2007, p. 20)

Por otra parte, la segunda fuente reafirma la necesidad de los BCP y las implicaciones que tiene el no contar con dichos planes, en este sentido se tienen los estudios realizados por ITEAM (2014), donde se ha podido demostrar que: “de cada 100 organizaciones sin BCP que sufren una contingencia, 43% nunca reabren, 51% a lo sumo sobreviven 2 años, y sólo 6% logran sobrevivir a largo plazo” (p.1).

De manera que es imprescindible contar con un BCP. Por esta razón, existen organizaciones y normativas internacionales que certifican los aspectos de seguridad esenciales para preservar la continuidad ante cualquier contingencia. De acuerdo con ITEAM (2014), las más destacadas en consultoría son: “Deloitte, KPMG, Risk México, Price Water House Coopers y AON”; en cuanto a servicios de apoyo: “Sungard, IBM, EMC, Symantec, Veritas, CITRIX y CISCO”; y, sobre la disciplina como tal: “Business Continuity Institute (BCI), Business Standard Institute (BSI), Disaster Recovery Institute Internacional (DRII), Internacional Organización for Standarization (ISO), Information Systems Audit and Control Association (ISACA) y NFPA”.

Ahora bien, en el caso específico del Ecuador, se pudo identificar que existen sectores como los de servicio público, de salud, de la producción industrial, como fábricas de producción de alimentos y proveedoras de piezas o partes esenciales para maquinarias, así como, las instituciones financieras; que cuentan con BCP por normativa, sin embargo; es reconocible que en las pequeñas y medianas empresas privadas no sucede de la misma forma, dígase por falta de normativa gubernamental o legislativa, o por imprudencia de los dueños de negocio, lo cual fue notable al momento de cuantificar las pérdidas ocasionadas por el pasado terremoto el 16 de abril, donde los cálculos ascienden a 3 millones de dólares (El Comercio, 2016).

Por otra parte, en el caso de las instituciones financieras ecuatorianas, teniendo en cuenta el gran volumen de información que manejan, y la

importancia que tiene para éstas garantizar, no solo la continuidad del servicio sino la preservación de sus medios y recursos, este sector cuenta con un soporte normativo en las Resoluciones de la Superintendencia de Bancos y Seguros, y los marcos de referencia y certificaciones efectuados por organizaciones internacionales especializadas en la continuidad del negocio, que obligan a las empresas del sector a diseñar, elaborar e implementar el BCP.

2.2. Riesgos y amenazas contra la continuidad

2.2.1. Riesgo

2.2.1.1. Definición de riesgo

En el Diccionario de la Lengua Española (Espasa Calpe, 1995), define la palabra riesgo proveniente del "vocablo *resgar*, cortar, cuyo origen en el latín es *resecare*, cortar"; conceptualizado como: "contingencia o proximidad de un daño."

Son varios los autores que hacen referencia a este término como la probabilidad de ocurrencia de un evento dado (Junta de Andalucía. Consejería de salud, 2010).

Este término también se vincula con:

> "La variedad de medidas de probabilidad de un resultado generalmente no favorable, al número esperado de pérdidas humanas, personas heridas, propiedad dañada e interrupción de actividades económicas, producto de fenómenos naturales particulares y, por consiguiente, de riesgos específicos y elementos de riesgo." (Echemendía, 2010, p. 5)

Ahora bien, aplicando esta noción al plano empresarial, Estupiñán (2006), explica que "se produce un riesgo cuando hay una probabilidad de que algo negativo suceda o que algo positivo no suceda, la ventaja de una empresa es

que conozca claramente los riesgos oportunamente y tenga la capacidad para afrontarlos” (p.101).

A modo de resumen, se entiende por riesgo a las probabilidades de ocurrencia o no de un evento negativo que podría traducirse en pérdidas de todo tipo de recursos, ya sean humanos, materiales, monetarios o de información, y cuya identificación es fundamental para poder definir las medidas de mitigación.

2.2.1.2. Tipos de riesgos en instituciones financieras

Las organizaciones están expuestas a contingencias de diferente índole: operacionales, ambientales, financieras, tecnológicos, entre otras. No obstante, en el caso particular de las entidades financieras ecuatorianas, de acuerdo con el Artículo 2 de la Resolución N° JB-2004-631 de la Superintendencia de Bancos y Seguros (2004), los tipos de riesgos que se pueden presentar en estas instituciones son los siguientes:

- Riesgo de crédito.- Es la posibilidad de pérdida debido al incumplimiento del prestatario o la contraparte en operaciones directas, indirectas o de derivados que conlleva el no pago, el pago parcial o la falta de oportunidad en el pago de las obligaciones pactadas.
- Riesgo de mercado.- Es la contingencia de que una institución del sistema financiero incurra en pérdidas debido a variaciones en el precio de mercado de un activo financiero, como resultado de las posiciones que mantenga dentro y fuera de balance.
- Riesgo de tasa de interés.- Es la posibilidad de que las instituciones del sistema financiero asuman pérdidas como consecuencia de movimientos adversos en las tasas de interés pactadas, cuyo efecto dependerá de la estructura de activos, pasivos y contingentes.
- Riesgo de tipo de cambio. - Es el impacto sobre las utilidades y el patrimonio de la institución controlada por variaciones en el tipo de cambio y cuyo impacto dependerá de las posiciones netas que mantenga una institución controlada, en cada una de las monedas con las que opera.

- Riesgo de liquidez. - Es la contingencia de pérdida que se manifiesta por la incapacidad de la institución del sistema financiero para enfrentar una escasez de fondos y cumplir sus obligaciones, y que determina la necesidad de conseguir recursos alternativos, o de realizar activos en condiciones desfavorables.
- Riesgo operativo.- Es la posibilidad de que se produzcan pérdidas debido a eventos originados en fallas o insuficiencia de procesos, personas, sistemas internos, tecnología, y en la presencia de eventos externos imprevistos. Incluye el riesgo legal, pero excluye los riesgos sistémico y de reputación. Agrupa una variedad de riesgos relacionados con deficiencias de control interno; sistemas, procesos y procedimientos inadecuados; errores humanos y fraudes; fallas en los sistemas informáticos; ocurrencia de eventos externos o internos adversos, es decir, aquellos que afectan la capacidad de la institución para responder por sus compromisos de manera oportuna, o comprometen sus intereses.
- Riesgo legal.- Es la probabilidad de que una institución del sistema financiero sufra pérdidas directas o indirectas; de que sus activos se encuentren expuestos a situaciones de mayor vulnerabilidad; de que sus pasivos y contingentes puedan verse incrementados más allá de los niveles esperados, o de que el desarrollo de sus operaciones enfrente la eventualidad de ser afectado negativamente, debido a error, negligencia, impericia, imprudencia o dolo. Todo esto puede derivarse de la inobservancia, incorrecta inoportuna aplicación de disposiciones legales o normativas, así como de instrucciones de carácter general o particular emanadas de los organismos de control, dentro de sus respectivas competencias; o, en sentencias o resoluciones jurisdiccionales o administrativas adversas; o de la deficiente redacción de los textos, formalización o ejecución de actos, contratos o transacciones, inclusive distintos a los de su giro ordinario de negocio, o porque los derechos de las partes contratantes no han sido claramente estipuladas; (sustituido con resolución No. JB-2008-1202 de 23 de octubre del 2008).

- Riesgo de reputación.- Es la posibilidad de afectación del prestigio de una institución del sistema financiero por cualquier evento externo, fallas internas hechas públicas, o al estar involucrada en transacciones o relaciones con negocios ilícitos, que puedan generar pérdidas y ocasionar un deterioro de la situación de la entidad" (p. 560).

2.2.2. Riesgos tecnológicos

Según González (2012), el riesgo tecnológico en instituciones bancarias se define como: "la posibilidad de que se produzca pérdida por daños, interrupción, alteración o fallas derivadas del uso o dependencia de tecnologías de la información en la prestación de servicios bancarios" (p. 7).

Entiéndase este concepto como las amenazas que pudiesen incidir directamente sobre los medios tecnológicos, ya sean físicos o informáticos (hardware y software), y que por supuesto, de cualquier manera afectarían la continuidad de los procesos si se tiene en cuenta que la mayoría de las operaciones bancarias dependen de estos recursos para funcionar.

2.2.2.1. Origen del riesgo tecnológico

Las principales fuentes generadoras del riesgo tecnológico se definen desde tres elementos esenciales, dígase: el físico, desde la infraestructura tecnológica; el lógico, que se refiere a los sistemas y aplicaciones informáticos o de la información; y por último, el error humano, que deriva de las acciones conscientes o inconscientes del factor humano (Montenegro, 2013).

Según Hidalgo (2004), las principales fuentes generadoras del riesgo tecnológico derivan de eventos tales como:

- El proceso en el que se adquiere o transfiere la tecnología, donde podrían ocurrir pérdidas de información o roturas de los medios por mala gestión u organización; o también por deficiencias por parte de los recursos humanos en el manejo de la tecnología, de ambos sentidos de la transacción, ya sea el emisor o el receptor.

- El proceso de constantes cambios de la tecnología utilizada; lo cual se da fundamentalmente por el desarrollo que vuelven obsoletas e inutilizables a las tecnologías empleadas.
- Fuentes externas a la institución, ejemplo de ello es el desarrollo del mercado y los cambios en las políticas macroeconómicas o legales que podrían limitar o impedir no solo la adquisición de la tecnología, sino también su posterior mantenimiento.

En esencia, cada una de estas fuentes no actúan por sí solas, todas ellas de una manera u otra se encuentran relacionadas, por lo que la diferenciación e identificación del origen del riesgo tecnológico se puede percibir de mejor manera si se analiza desde un enfoque sistémico. A continuación se representa la relación entre las fuentes anteriormente mencionadas:

Figura 2. Fuentes de origen del riesgo tecnológico.
Tomado de (Hidalgo, 2004)

2.2.2.2. Clasificación del riesgo tecnológico

Respecto a la clasificación del riesgo tecnológico, puede decirse en primer lugar que, ciertamente, ninguno es igual a otro sobre todo porque depende de las circunstancias y el entorno de origen, asimismo, la importancia de cada uno de ellos es distinta, lo mismo sucede con la probabilidad de ocurrencia y el impacto que estos pudiesen tener sobre diferentes áreas o procesos.

Sin embargo, teniendo en cuenta lo anterior, se pueden clasificar los riesgos tecnológicos siguiendo los criterios de Gualim (2014), quien los categoriza atendiendo al elemento en los que estos podrían impactar; a continuación se describen dichos elementos:

- Riesgos tecnológicos sobre la seguridad de acceso: acceso y manejo de información por personal de la entidad o individuos ajenos a la institución, que no cuentan con la autorización necesaria.
- Riesgos tecnológicos sobre la calidad de medios y la información: las infraestructuras tecnológicas no son eficientes para el procesamiento de la información, y a su vez, estos datos se ven comprometidos porque carecen de la calidad necesaria o se encuentran tergiversados, incompletos o inexactos.
- Riesgos tecnológicos sobre la disponibilidad de recursos e información: Los medios tecnológicos y la información no se encuentran disponibles de manera oportuna. (p.4).

2.2.2.3. Escenarios de los riesgos tecnológicos

Sánchez (2013) define los peores escenarios que tendrían lugar producto a riesgos tecnológicos, los cuales son agrupados por el autor de la manera siguiente:

1. “Escenarios generados por riesgos que imposibilitan que la entidad mantenga la continuidad de sus operaciones.
    - Falta de disponibilidad de los sistemas informáticos producto de una inadecuada gestión de medios, error de proveedores en el abastecimiento, fallas en el suministro de energía eléctrica.
    - Sabotaje interno de los medios tecnológicos.
    - Errores propios de los sistemas tecnológicos, ya sea en el hardware o el software de los sistemas.
    - Colapsos provocados por exceso de cargas en los sistemas, o por deficiente tecnología utilizada.
    - Eventos catastróficos.

2. Pérdida de confidencialidad de información sensible para el negocio.
    - Hurto de información clasificada por trabajadores internos, hackers, o personas externas.
    - Confidencialidad de información comprometida por mal manejo o gestión, ocasionadas por errores humanos de trabajadores internos o de las aplicaciones informáticas.
3. Fraude online o interno.
    - Fraudes realizados por criminales que reemplazan identidades o números de tarjetas que son objeto de robo.
    - Fraudes realizados por trabajadores internos sobre la manipulación de la información y los sistemas, en función de beneficios propios.
4. Objetivos del negocio afectados como consecuencia de una mala adopción de la tecnología.
    - Incapacidad para cumplir con nuevos requerimientos de cliente o pérdidas excesivas generadas por altos costos derivados de retrasos, donde la satisfacción del cliente se ve comprometida, debido a limitaciones en la tecnología utilizada” (p.35).

2.2.2.4. Gestión de riesgos tecnológicos

Teniendo en cuenta las normas internacionales ISO 31000 e ISO 27005, y la relación que éstas tienen con la continuidad del negocio, se establecen los procesos necesarios para la gestión de riesgos tecnológicos, los cuales a su vez deben estar alineados con los procesos que plantea la gestión de mejora continua en las organizaciones como parte fundamental de la gestión de la calidad. A continuación se muestra dicha alineación en función de la gestión del riesgo tecnológico:

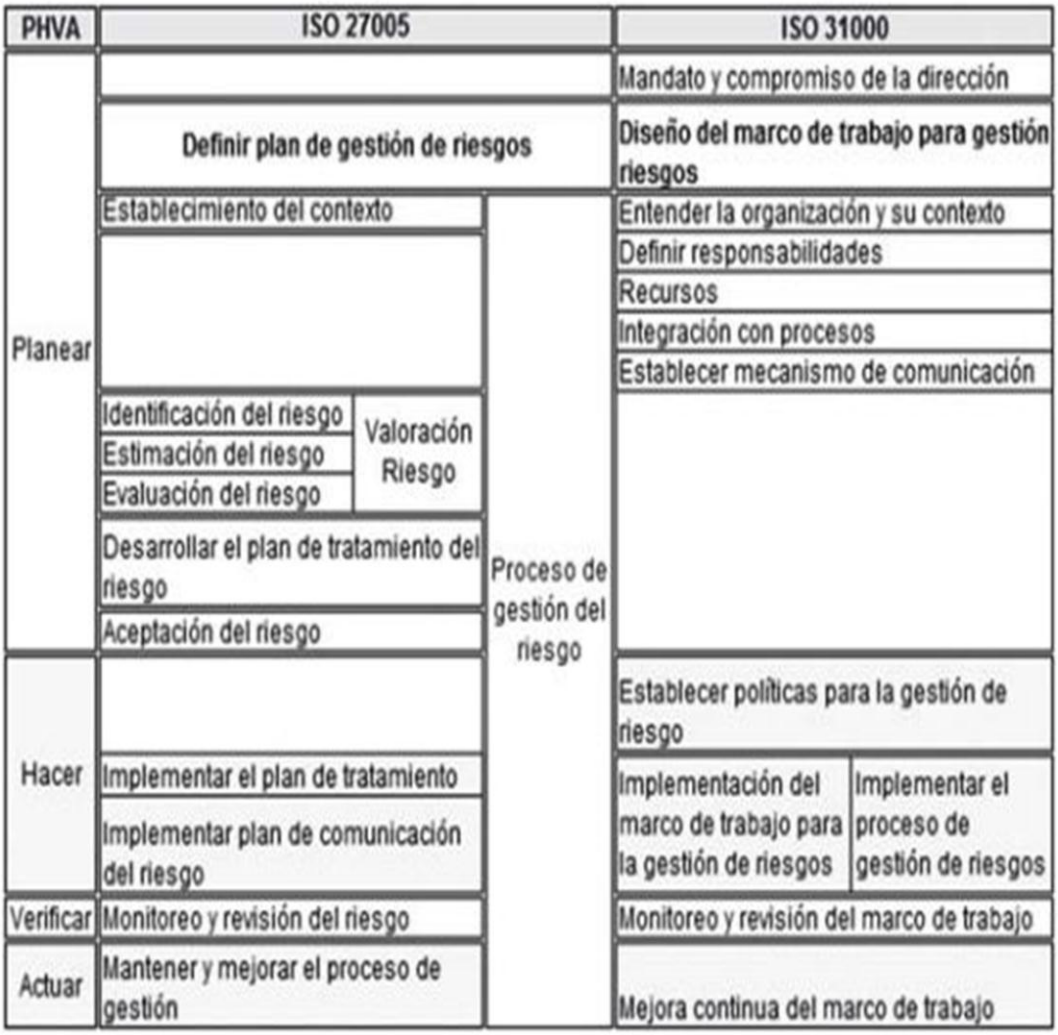


Figura 3. Alineación de estándares ISO 31000 e ISO 27005 con modelo PHVA.

Tomado de (Ramirez & Ortiz, 2011)

Teniendo en cuenta los procesos anteriormente mencionados y la importancia que tienen; es necesario gestionar los riesgos tecnológicos, para lo cual Ramírez y Ortiz (2011) plantean la siguiente metodología:

Figura 4. Metodología para la gestión de riesgos tecnológicos.
Tomado de (Ramirez & Ortiz, 2011)

Donde los pasos a seguir se describen como:

- Identificar: se refiere al levantamiento de la información con la finalidad de conocer los activos a evaluar. Así como también, determinar las amenazas y vulnerabilidades potenciales a las cuales están expuestos.
- Estimar: consiste en medir el impacto y probabilidad de los riesgos identificados con sus respectivos escenarios. Esta fase es sumamente compleja por su carácter subjetivo, y suele incluir controles preventivos y correctivos.

- Evaluar o priorizar: una vez identificados y analizados los riesgos, se procede a clasificarlos para determinar cómo canalizar cada riesgo en consideración de los recursos de la empresa, criticidad y costos de los mismos.
- Plan de tratamiento de riesgo o mitigación: establecimiento de un plan contentivo de las diferentes medidas preventivas o correctivas, que pueden implementarse en la empresa para mitigar el riesgo, indicando los costos y tiempos relacionados con cada alternativa propuesta. Se deben tomar en cuenta también, los criterios de aceptación de tolerancia al riesgo, previamente definidos.
- Comunicación y cultura de riesgo: existe cultura de riesgo cuando todos los niveles de una organización saben cómo y por qué responder ante los riesgos tecnológicos que pueden presentarse.

2.3. Análisis del impacto sobre el negocio (BIA)

El análisis de impacto sobre el negocio (Business Impact Analysis o BIA por sus siglas en inglés), es otra de las herramientas empleadas para evaluar las consecuencias que podría sufrir una organización producto de alguna eventualidad o un desastre que tenga lugar en el entorno de la misma. (Mendoza, 2014).

El BIA constituye un proceso más especializado que se basa específicamente en el “cómo” las organizaciones serían afectadas por las amenazas que atentan contra la seguridad de las mismas, atendiendo a la determinación, al análisis y a la evaluación de los impactos económicos, probabilidad de ocurrencia y consecuencias que tendrían los riesgos sobre las operaciones y activos del negocio.

Este análisis se considera como parte fundamental para poder elaborar los planes de recuperación ante desastre (DRP), y por consiguiente, es inherente a los BCP, ya que mediante el BIA se pueden identificar y valorar las afectaciones económicas y funcionales que implicarían un obstáculo en la continuidad del negocio.

Dentro del BIA según Mendoza (2014) existen varios conceptos importantes, tales como:

- Punto de recuperación objetivo (Recovery Point Objective – RPO): hace alusión a “la antigüedad máxima de los datos para su restauración, es decir, la tolerancia que el negocio puede permitir para operar con datos de respaldo, por lo que el RPO estará en función de las actividades primordiales de una organización” (p. 4).
- Tiempo de recuperación objetivo (Recovery Point Objective - RTO): indica “el período permitido para la recuperación de una función o recurso de negocio a un nivel aceptable luego de una interrupción o desastre” (p. 7).
- Período máximo tolerable de tiempo de inactividad (Maximum Tolerable Period Of Down time - MTPOD): refiere “el período máximo de no disponibilidad para las actividades, activos o procesos, antes de que la organización deje de operar” (p. 4).

2.4. Metodologías y estándares internacionales para la continuidad del negocio

En la actualidad existen varias referencias que desarrollan metodologías en función de la elaboración e implementación de BCP en las organizaciones. La mayoría procede de organizaciones internacionales especializadas en la continuidad del negocio. A continuación se mencionan algunas de las más importantes:

2.4.1. BS 25999:2007

La norma fue elaborada por el Instituto Británico de Normas; básicamente consiste en una ampliación de la noción del plan de continuidad del negocio para abarcar toda la organización. Se divide en dos partes: (a) BS 25999-1: Contiene un código de práctica con el propósito de la norma y recomendaciones; y (b) BS 25999-2: Los requisitos para un sistema de gestión de continuidad (Bello, 2008).

Según este marco de referencia, un plan de continuidad del negocio consta del siguiente ciclo de vida (Bello, 2008):

- Plan de Administración de Continuidad del Negocio.
- Conocimiento sobre la organización.
- Determinación de las estrategias de continuidad del negocio.
- Implementación de un programa de responsabilidad para la continuidad del negocio.
- Pruebas y mantenimiento del plan de continuidad del negocio.
- Desarrollo de una cultura de continuidad del negocio.

2.4.2. BS 25777:2008

Proporciona apoyo para la implementación de servicios de información y tecnología de comunicaciones. Según Hamidovic (2011) se compone de los siguientes principios:

- Protección
- Detección
- Reacción
- Recuperación
- Operación
- Regreso
- Personal
- Localidades
- Tecnología

Se utiliza generalmente en complementación con el BS 25999-1 para lograr resultados más efectivos en el área de tecnología de la información.

2.4.3. ISO/IEC 27005: 2011

La norma ISO/IEC 27005:2011 es el estándar internacional encargado de la gestión de riesgos de seguridad de la información. Esta norma es aplicable a

todas las organizaciones que desean gestionar los riesgos que pueden poner en peligro la seguridad de la información.

Es importante destacar que la presente norma no recomienda una metodología estricta y concreta puesto que su aplicación dependerá de una serie de factores, presentes en el sector comercial de la propia industria o dependientes del verdadero alcance del sistema de gestión de seguridad de la información. (Castro, 2011).

2.4.3.1. Enfoques de la ISO/IEC 27005:2011

Se presentan los enfoques que la norma presenta como los adecuados:

Establecimiento del contexto: esta etapa tiene como objetivo principal conocer a fondo la organización y de este modo identificar cuáles son las amenazas tanto a nivel interno como externo y determinar los alcances y limitaciones.

Identificación y Estimación del riesgo: en esta etapa es imprescindible identificar los activos realmente relevantes para la empresa, bien sea procesos, datos y activos de soporte. Luego se deben tener en cuenta los tipos de amenazas ya sean físicas, estratégicas, naturales, técnica, accidental o intencionales. El resto permitirá determinar los controles y priorizar los riesgos. Es importante tener en cuenta la dependencia entre activos y procesos ya que estos últimos deben ser priorizados con la finalidad de conocer los niveles más críticos a los que puede enfrentarse.

Evaluación y tratamiento del riesgo: con la presente etapa se establecen las acciones necesarias para enfrentar los riesgos encontrados y deben llevarse a cabo acciones de reducción, aceptación, eliminación y trasferencia. De este modo se procede a realizar los controles recomendables en los cuales deberá incluirse un análisis detallado del costo- beneficio. Es importante destacar que el plan de tratamiento tiene que tener definidos los pasos para la gestión de riesgos, así se evitarían otros por error de implementación (SGSI, 2015).

Aceptación y comunicación del riesgo: después de tener claros los riesgos que enfrenta la institución es importante confeccionar el plan de comunicación que se realizará teniendo en cuenta las definiciones sobre la existencia del riesgo en la empresa, así como los objetivos de la gestión y el debido informe tanto de los avances del proceso como de todo lo que se considere pertinente. El diseño de dicho plan debe crear una conciencia sobre la existencia de los riesgos tecnológicos y permitir la obtención de la información que facilite colaborar en la planificación del proceso de gestión de riesgos. Esta propuesta contiene tres etapas:

- Comunicación inicial: aspectos generales sobre los riesgos y sus implicaciones y ventajas.
- Comunicación sobre la marcha: se muestran los avances del proceso para conseguir el apoyo y participación de los involucrados.
- Comunicación de resultados: Difundir los resultados teniendo siempre en cuenta los filtros de información.

Monitoreo y revisión del riesgo: En esta fase es necesario tener en cuenta que el elemento principal es el control de cambios, por lo cual la supervisión deberá ser realizada sobre los procesos, vulnerabilidades, activos, controles, amenazas, etc. Se tiene por finalidad predeterminar acciones a seguir ante cambios de cualquier índole y mantener la gestión continuamente actualizada. Con esto se busca evaluar el cumplimiento de los planes.

2.4.4. ISO 22301:2012

La norma ISO 22301: 2012 es en sí la primera norma de tipo internacional creada como sistema de gestión de la continuidad del negocio. Su creación se fundamenta en la necesidad de minimizar el riesgo de interrupciones en las empresas.

Entre sus especificaciones se presentan los requisitos necesarios que permiten a las organizaciones responder y recuperarse lo más pronto posible de las interrupciones en el momento que sucedan. Para ello se especifica en los

siguientes procesos: establecer, planificar, modelar, implantar, revisar, monitorear y mantener y mejorar el sistema de gestión. Estos requisitos pueden ser aplicados a todas las empresas, sin importar la naturaleza o tamaño de la misma, puesto que la aplicación de estos depende de la complejidad de la empresa y el ambiente operativo en que se desarrolla.

La norma internacional para la gestión de la continuidad del negocio, denominada ISO 22301:2012, establece cómo identificar las amenazas potenciales de una organización y los impactos en las operaciones de negocio a fin de contar con capacidad de respuesta para salvaguardar sus intereses; además, explica las fases del BCP de la siguiente manera (ISO, 2012).

- Descripción del negocio y análisis de riesgos.
- Estrategias o mitigación del riesgo.
- Desarrollo de implantación del plan.
- Mantenimiento del plan.

2.4.4.1. Modelo de gestión que plantea la ISO 22301

La norma está organizada en diferentes cláusulas, las cuales facilitan la aplicación de la misma, entre las más importantes se pueden encontrar las siguientes:

Contexto de la organización: se enfoca a temas tanto internos como externos con el propósito de alcanzar las metas de la empresa y conseguir los resultados esperados en el sistema de gestión de continuidad del negocio.

Entre los temas principales abarcados por esta cláusula se encuentran:

- Las actividades desarrolladas por la empresa, bien sean servicios productos, cadenas de suministros o cualquier impacto potencial que pueda provocar la interrupción.
- La creación de los vínculos necesarios entre los objetivos planteados por la organización y la política de continuidad del negocio.

- Priorizar las expectativas y necesidades que tienen las partes interesadas y que puedan afectar de algún modo a la organización.

Liderazgo: Es imprescindible que la dirección de la empresa muestre un compromiso continuo, puesto que por medio del liderazgo la empresa tiene que mantener el ambiente adecuado en el que se involucre a los trabajadores y supervisar que el sistema de gestión de continuidad del negocio funcione eficientemente.

Es importante resaltar que entre las principales responsabilidades de la dirección se encuentran:

- Supervisar que la estrategia seguida por la institución sea compatible con el sistema de gestión de continuidad del negocio e integrar los requisitos de dicho sistema a los procesos de negociación de la empresa.
- Asegurar el debido cumplimiento de los objetivos y los planes del sistema de gestión de continuidad del negocio y del mismo modo facilitar los recursos que se necesitan, priorizando la dirección, apoyo y mejora continua del mismo. Con ello se pretende conseguir los resultados esperados y de este modo proceder al establecimiento de las políticas de continuidad del negocio.

Planificación: En esta etapa se procede al establecimiento de los principios y objetivos estratégicos que contribuyen a la orientación del sistema de gestión de continuidad del negocio, debido a que los mismos tratan los riesgos ya identificados y cumplen con las necesidades que posee la institución (SGSI, 2015).

Puede afirmarse entonces que los objetivos de la continuidad del negocio deben estar dirigidos a:

- Conocimiento preciso de la política de continuidad de la empresa para de este modo utilizar los productos y servicios en sus niveles mínimos, porque deben ser medibles.

- Conocer a profundidad los requisitos aplicables para que puedan ser actualizados y controlados en el tiempo que se estime conveniente.

Soporte: La gestión diaria del sistema que se aborda está basada en la utilización de los recursos apropiados para las más disímiles actividades realizadas por la empresa, aunque cabe destacar que la utilización de estos recursos incluye al personal, pues el mismo necesita capacitación y esto puede ser apoyado con la información documentada, siempre considerando como un eslabón primordial a la comunicación tanto interna como externa.

Operación: Luego de ser planificado el sistema de gestión de continuidad del negocio, la organización tiene que implementarlo, por lo que esta cláusula incluye:

- El análisis del impacto causado por el funcionamiento del sistema de gestión de continuidad del negocio y la evaluación de los riesgos que puedan presentarse, así como las estrategias para la continuidad del negocio.
- La aplicación de procedimientos de continuidad del negocio, entre las que se destacan el establecimiento de un protocolo de comunicación que tenga flexibilidad para responder ante las amenazas y minimizar las consecuencias con el establecimiento de estrategias de mitigación.
- Ejercicios de aplicación y pruebas de seguimiento.

Evaluación del desempeño: Cuando ya el sistema se encuentra implementado, la norma establece que se realice un seguimiento, mediante la revisión periódica para lograr la mejora. Esto se puede conseguir a través de:

- El seguimiento a las políticas de continuidad, así como a sus objetivos y metas. Además, se ha de verificar el desempeño de los procesos, funciones y procedimientos para la protección de las actividades.
- Realizar auditorías internas a intervalos, las cuales deben ser previamente planificados. También se ha de comprobar su relación con la norma para evaluar la revisión de la dirección.

Mejora: La mejora continua se realiza a lo largo de toda la institución con la finalidad de lograr un incremento en la eficiencia y eficacia de las actividades y los controles de las mismas, lo cual aportará sin duda, beneficios para la empresa. Dicha mejora se realizará mediante la utilización de la debida política de continuidad del negocio.

2.4.4.2. Procedimiento que plantea la ISO 22301 para el desarrollo del BCP

La empresa debe ser capaz de establecer, implementar y mantener los procedimientos necesarios para la continuidad del negocio, los cuales facilitarán la gestión ante un evento diferente. Así la organización podrá continuar sus actividades partiendo de la recuperación ante tal situación, por lo cual es vital poseer documentados los procesos que aseguran la continuidad de dichas actividades.

Estos procesos deben incluir:

1. El establecimiento de los respectivos protocolos de comunicación tanto internos como externos.
2. Ser específicos en relación a los pasos que se deben seguir durante la interrupción.
3. Ser flexibles para responder a un escenario de amenazas y cambios, bien sean internos o externos.
4. Focalización en el impacto de eventos que potencialmente puedan interrumpir las operaciones.
5. Desarrollar bases de presuposiciones y análisis de interdependencia.
6. Ser efectivos en minimizar las consecuencias sobre la implementación de estrategias de mitigación apropiadas (Estandar Internacional ISO 22301, 2012).

Estructura de respuesta

Por otro lado es importante resaltar que la organización debe tener establecida una estructura de respuesta y contar con el personal y la autoridad necesaria para poder preparar, mitigar y responder a un evento alterado.

Esta estructura debe estar dirigida a :

1. Identificar los impactos que pudieran justificar el inicio de una respuesta formal.
2. Evaluar tanto la naturaleza y extensión de un evento diferente, como su potencial impacto.
3. Iniciar la respuesta apropiada a la continuidad del negocio.
4. Prever los procesos y procedimientos necesarios para la activación, coordinación, operación y comunicación de la respuesta.
5. Tener disponibles lo recursos necesarios para el apoyo de los procesos y la gestión de eventos alterados, así como el trabajo para minimizar el impacto apropiadas (Estandar Internacional ISO 22301, 2012).

Comunicación y Avisos

Otro de los procedimientos necesarios ante una situación de riesgo es el aviso y la comunicación, los cuales deben ser ejercitados de manera regular y deben contener:

1. La detección de un incidente.
2. El continuo monitoreo del incidente.
3. La comunicación interna en la organización, así como la recepción de documentos y la respuesta a las partes interesadas.
4. La recepción, comunicación y respuesta de cualquier sistema de riesgo consultivo nacional o regional.
5. Asegurar la disponibilidad de los medios de comunicación durante el incidente.
6. Facilitar una comunicación estructurada a organizaciones de emergencia.
7. Registrar la información vital sobre el incidente, así como las acciones y decisiones tomadas apropiadas (Estandar Internacional ISO 22301, 2012).

Plan de Continuidad del negocio

La empresa debe contar con procedimientos documentados para los planes de continuidad del negocio que faciliten la recuperación de las actividades en un tiempo predeterminado. Dichos procedimientos deben contener:

1. Los roles y responsabilidades definidas para las personas y equipos que tienen autoridad durante y después de un incidente.
2. Contar con un proceso de activación de respuesta.
3. Poseer los detalles para gestionar la inmediata consecuencia de un incidente, considerando el bienestar de las personas; las opciones, estrategias y tácticas para responder a una alteración y la prevención de futuras pérdidas o no disponibilidad de actividades priorizadas.
4. Los detalles de cómo se comunicará la organización con los empleados y sus familiares, partes interesadas claves y los contactos de emergencia.
5. Definir cómo continuar o recuperar las actividades priorizadas en un tiempo predeterminado.
6. Dar detalles de la respuesta organizacional a los medios después del incidente, incluyendo la estrategia de comunicación, el interfaz preferido con los medios y el guion e interlocutor apropiado.
7. Contar con un proceso para la recuperación después que termine el incidente apropiado (Estandar Internacional ISO 22301, 2012), el cual debe contener:

- Propósito y alcance
- Objetivos
- Criterio de activación y procedimientos
- Procedimientos de implementación
- Roles, responsabilidades y autoridades
- Requerimientos y procedimientos
- Interdependencia e interacción interna y externa
- Requerimiento de recursos
- Flujo de información y proceso documental

Recuperación

La empresa debe tener documentados los procedimientos para el restablecimiento y el retorno de las actividades del negocio, luego de las medidas temporalmente adoptadas. Además, se han de apoyar los requerimientos del mismo, luego del incidente.

Ejercicios y Ensayos

Deben ser ensayados y ejercitados todos los procedimientos de continuidad con la finalidad de asegurar su consistencia con los objetivos del Sistema de Gestión de Continuidad del Negocios (SGCN) y de este modo permitir:

1. Consistencia con el alcance y objetivos del SGCN.
2. Estar basados en escenarios apropiados, con la debida planificación.
3. Que el tiempo valide todos los arreglos de continuidad del negocio, incluyendo a las partes interesadas más relevantes.
4. Minimizar el riesgo de una alteración a las operaciones.
5. Producir informes después de cada ejercicio que contenga resultados y definir recomendaciones e implementación de mejoras apropiadas (Estandar Internacional ISO 22301, 2012).

2.4.4.3. Documentación oficial para la certificación

El modelo ISO22301:2012 exige una serie de documentos de tipo obligatorio que la empresa debe desarrollar Alexander (2012).

A continuación se listan los mismos:

1. Lista de requisitos legales, normativos y de otra índole.
2. Alcance del SGCN. Política de la continuidad del negocio.
3. Objetivos de la continuidad del negocio.
4. Evidencia de competencias del personal.
5. Registros de comunicación con las partes interesadas.
6. Análisis del impacto en el negocio.
7. Evaluación de riesgos, incluido un perfil del riesgo.

8. Estructura de respuesta a incidentes.
9. Planes de continuidad del negocio.
10. Procedimientos de recuperación.
11. Resultados de acciones preventivas.
12. Resultados de supervisión y medición.
13. Resultados de la auditoría interna.
14. Resultados de la revisión por parte de la dirección.
15. Resultados de acciones correctivas.

Esta documentación es necesaria para la certificación, sin embargo, las organizaciones no necesariamente deben estar certificadas para garantizar la efectividad de la respuesta ante situaciones de crisis. Las instituciones pueden poseer los procedimientos adecuadamente definidos en función de la administración de la continuidad del negocio, de manera tal que se considere preparada para enfrentar cualquier riesgo que se presente por complicado que sea.

2.4.5. COBIT 5

Este marco de trabajo para el gobierno de la TI, desarrollado por la Information Systems Audit and Control Association (ISACA), tiene por objeto organizar y optimizar los estándares internacionales relacionados con la tecnología de la información en las organizaciones. Presenta un conjunto de prácticas enfocadas al control, con base en criterios de calidad, confianza y seguridad. COBIT 5 se fundamenta en cinco principios (ISACA, 2012):

- Satisfacer las necesidades de las partes interesadas.
- Cubrir la empresa de extremo a extremo.
- Aplicar un marco de referencia único integrado.
- Hacer posible un enfoque holístico.
- Separar el gobierno de la gestión.

A continuación se detalla la perspectiva que COBIT 5 ofrece sobre cada uno de los principios anteriormente mencionados.

Satisfacer las necesidades de los colaboradores: se basa en la definición de los objetivos que tiene la organización y los objetivos que están estrechamente relacionados con la tecnología de la información.

Cubrir la empresa de extremo a extremo: se enfoca en el cambio de visión de las compañías, con la finalidad de que las mismas consideren a las tecnologías de la información como un activo para su entidad y no como un costo. Por tanto, se propone que los directivos incluyan dentro de sus funciones la gestión de dichos activos.

Aplicar un solo marco integrado: este principio propone a las organizaciones el uso de un solo marco de gobierno más integrado con la finalidad de brindar el mayor valor posible a sus activos y recursos de la tecnología de la información.

Separar al gobierno de la gestión: este principio parte del criterio de que el gobierno se encarga de que se logren los objetivos empresariales, siempre evaluando las necesidades de los accionistas, así como sus opciones y condiciones, además prioriza la toma de decisiones, monitoreo, desempeño y cumplimiento para el establecimiento de la dirección.

La gestión en cambio se encarga de la planificación, construcción, ejecución y supervisión de las actividades presentadas por la dirección previamente establecida por el gobierno.

Habilitar un enfoque holístico: en este principio propone que se tomen en cuenta varios componentes o habilitadores, los cuales influyen en el funcionamiento o no de cualquier actividad propuesta (Osores, 2014).

Entre los habilitadores COBIT 5 propone analizar lo siguiente:

- Principios, políticas y modelos de referencia: son el vehículo para trasladar el comportamiento deseado en guías prácticas para la gestión diaria.

- Procesos: describen un conjunto de prácticas y actividades organizadas para cumplir con ciertos objetivos y producir un conjunto de salidas para alcanzar los objetivos generales relacionados con TI.
- Estructuras organizacionales: son las entidades claves en la toma de decisiones de la empresa.
- Cultura, ética y comportamiento: la cultura, ética y comportamiento de los individuos y de la empresa muchas veces son sobrestimados como un factor de éxito en las actividades de gobierno y gestión.
- Información: requerida para mantener la empresa en ejecución y bien gobernada. En el nivel operacional, la información es un producto clave de la empresa.
- Servicios, infraestructura y aplicaciones: incluye la infraestructura, la tecnología y las aplicaciones para proveer a la empresa los servicios y procesamiento de Tecnología de la Información.
- Gente, habilidades y competencias: requeridas para completar con éxito las actividades y para tomar las decisiones correctas y acciones correctivas (Muñoz, 2012).

2.4.5.1. Catalizadores de COBIT 5

Los catalizadores de COBIT 5 cuentan con un conjunto de dimensiones comunes que facilitan una manera simple y estructurada de tratar con ellos. Además permiten a la organización manejar las interacciones complejas facilitando resultados exitosos.

Entre las dimensiones de estos catalizadores pueden encontrarse los grupos de interés, las metas, el ciclo de vida y las buenas prácticas. Cada una de estas dimensiones será explicada a continuación.

Grupos de interés: cada catalizador tiene su propio grupo de interés, los mismos que pueden ser internos o externos. Cada uno presenta sus propias necesidades e intereses y en muchas ocasiones son contrarios entre sí.

Metas: cada catalizador cuenta con varias metas, las mismas que pueden ser definidas en resultados esperados, aplicación y operación.

Ciclo de Vida: cada catalizador cuenta con su propio ciclo de vida. Comienza pasando por su vida útil operativa hasta su eliminación, lo cual se aplica a las estructuras, procesos y políticas. Este ciclo se centra en la planificación, diseño, construcción, utilización y evaluación de la organización.

Buenas prácticas: estas son las encargadas del soporte para la consecución de los objetivo de la organización. Proporcionan ejemplos y sugerencias sobre la implementación y los productos, así como las entradas o las salidas que son necesarios.

La siguiente figura muestra los catalizadores de COBIT 5 de manera más comprensible:

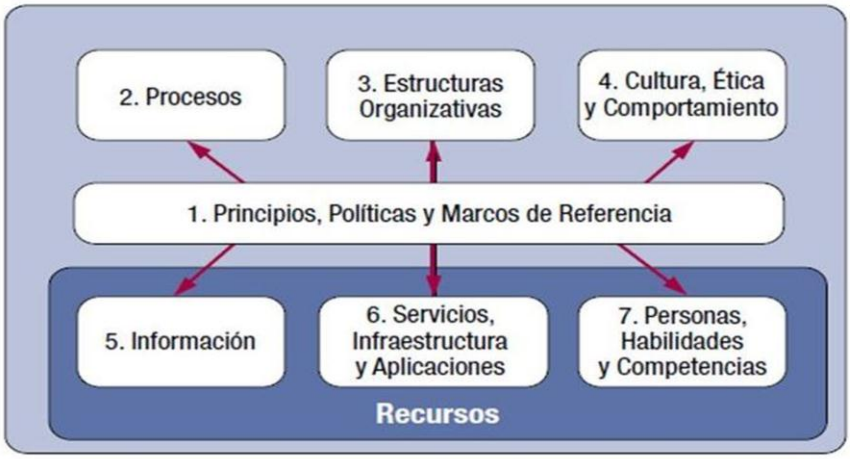


Figura 5. Catalizadores de COBIT 5.
Tomado de (Alcarraz, 2014)

2.4.5.2. Modelo de referencia de Procesos de COBIT 5

Los procesos habilitadores complementan el marco COBIT 5 y contienen una guía de referencia detallada sobre los procesos que están definidos en el Modelo de referencia de Procesos de COBIT 5.

El Modelo de Referencia de Procesos de COBIT 5 subdivide las actividades y prácticas de la Organización relacionadas con la TI en dos áreas principales: el área de gobierno y la de administración, siendo esta última dividida en dominios de procesos.

Para COBIT 5, el Dominio de GOBIERNO se asocia con cinco procesos enfocados hacia las prácticas de Evaluar, Dirigir y Monitorear.

Por su parte los dominios de la ADMINISTRACIÓN contemplan planificación, construcción, operación y monitoreo. A continuación se presenta de manera gráfica.

Figura 6. Modelo de Referencia de Procesos de COBIT 5.
Tomado de (ISACA, 2012)

Las guías COBIT 5 cuentan con 5 dominios y 37 procesos que contribuyen a la creación de un plan de continuidad factible del negocio.

A pesar de que COBIT 5 establece una alineación de los procesos en cada uno de los niveles organizacionales, en el caso particular de este estudio de acuerdo a la temática de interés, se selecciona específicamente el proceso DSS04 enfocado en la gestión de la continuidad. Este fundamenta algunas prácticas claves que son específicas para la continuidad del negocio, las cuales facilitan comprender y aplicar mucho mejor los principios de dicho proceso.

A continuación se hace una valoración de aquellos aspectos involucrados en cada una de las prácticas planteadas por DSS04:

- DSS04.01 Definir la política de continuidad del negocio, objetivos y alcance: definir la política y alcance de continuidad del negocio alineada con los objetivos de negocio y de las partes interesadas, identificando los procesos y actividades críticas, así como los roles y responsabilidades para definir y acordar la política de continuidad y su alcance. Identificar procesos esenciales de soporte al negocio y servicios TI relacionados (Palacios, 2016).
- DSS04.02 Mantener una estrategia de continuidad: evaluar las opciones de gestión de la continuidad del negocio y escoger una estrategia de continuidad viable y efectiva en coste, que pueda asegurar la continuidad y recuperación de la empresa frente a un desastre u otro incidente mayor o disrupción. Identificar escenarios potenciales probables que puedan estimular eventos que puedan causar incidentes disruptivos importantes y que permitan realizar un análisis de impacto y efecto en el negocio. Establecer el tiempo mínimo necesario para recuperar un proceso de negocio y su soporte de TI, y analizar la probabilidad de amenazas que puedan causar pérdidas de continuidad del negocio e identificar medidas que puedan reducir la probabilidad y el impacto (Palacios, 2016).
- DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio: desarrollar un plan de continuidad del negocio (BCP) basado en la estrategia que documente los procedimientos y la información lista para el uso en un incidente para facilitar que la empresa continúe con

sus actividades críticas. Desarrollar y mantener planes del continuidad del negocio operativos que contengan los procedimientos que deben ser seguidos para permitir continuar operando los procesos críticos de negocio y/o planes temporales de procesos, definiendo las acciones y comunicaciones de respuesta a incidentes que deben ser realizadas. Definir las condiciones y procedimientos de recuperación. Definir y documentar los recursos necesarios para soportar los procedimientos de continuidad y recuperación, los requerimientos de información de respaldo para soportar los planes, y determinar las habilidades necesarias para los individuos implicados en la ejecución de los planes y procedimientos (Palacios, 2016).

- DSS04.04 Ejercitar, probar y revisar el plan de continuidad: probar los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará, en el tiempo, como se espera. Definir los objetivos para ejercitar y probar los sistemas del plan y acordar ejercicios que sean razonables con las partes interesadas (Palacios, 2016).
- DSS04.05 Revisar, mantener y mejorar el plan de continuidad: realizar una revisión, por la dirección, de la capacidad de continuidad a intervalos regulares para asegurar su continua idoneidad, adecuación y efectividad. Gestionar los cambios en el plan de acuerdo al proceso de control de cambios para asegurar que el plan de continuidad se mantiene actualizado y refleja continuamente los requerimientos actuales del negocio. Revisar el plan y la capacidad de continuidad de forma regular frente a las asunciones hechas y los objetivos de negocio actuales, recomendando y comunicando los cambios en la política, planes, procedimientos, infraestructura, roles y responsabilidades (Palacios, 2016).
- DSS04.06 Proporcionar formación en el plan de continuidad: proporcionar a todas las partes implicadas, internas y externas, de

sesiones formativas regulares que contemplen los procedimientos y sus roles y responsabilidades en caso de disrupción. Definir y mantener los planes y requerimientos de formación para quienes realicen de manera continuada la planificación de la continuidad, el análisis de impacto, las evaluaciones de riesgos, la comunicación con los medios y la respuesta a incidentes. Supervisar habilidades y competencias (Palacios, 2016).

- DSS04.07 Gestionar acuerdos de respaldo: mantener la disponibilidad de la información crítica del negocio. Hacer copias de seguridad de sistemas, aplicaciones, datos y documentación de acuerdo a una planificación definida, considerando: frecuencia, modo de copias de seguridad, tipo de copias de seguridad, tipo de soporte, copias de seguridad automatizadas en línea, tipos de datos, creación de registros, datos de cálculos críticos de usuario final, localización física y lógica de las fuentes de los datos, seguridad y derechos de acceso, cifrado. Considerar la accesibilidad requerida a las copias de seguridad (Palacios, 2016).
- DSS04.08 Ejecutar revisiones post reanudación: evaluar la adecuación del Plan de Continuidad del Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios ante una disrupción. Determinar la efectividad del plan, capacidades de continuidad, roles y responsabilidades, habilidades y competencias, incidentes, infraestructura técnica y estructuras organizativas y relaciones. Identificar debilidades u omisiones en el plan, sus capacidades y hacer recomendaciones para la mejora (Palacios, 2016).

Es importante resaltar que estas prácticas se orientan en la definición, estrategia, implantación, pruebas y mejoras de un plan de continuidad.

Este estándar fue creado para ayudar a las empresas a obtener el mejor valor de las tecnologías de la información, lo cual permite obtener un balance entre la realización de beneficios, los niveles de riesgo asumidos y la utilización de los recursos. Puede ser aplicado en organizaciones de todo tipo, ya sea en el sector público, privado o bien en organizaciones sin fines de lucro. La

utilización de este estándar es muy efectiva para todo tipo de organización, pues permite realizar mejores inversiones y tomar las decisiones adecuadas en relación con las tecnologías de la información y de este modo agregar valor a los activos tecnológicos y a la información en sí, estableciendo además, las pautas para garantizar la consecución de las operaciones, al proponer estrategias de continuidad del negocio.

2.4.6. Good Practice Guidelines (GPG)

La guía elaborada por el Business Continuity Institute (BCI), denominada Good Practice Guidelines (GPG), que en español se traduce: Buenas prácticas para la continuidad del negocio, explica el cómo y el porqué de los principios de la disciplina de continuidad del negocio, incluyendo la terminología de la norma ISO 22301, y fundamentos de la norma BS 25999, para asegurar los más altos estándares en su ejecución (BCI, 2013).

El sistema de Good Practice Guidelines contiene el Ciclo de Vida de la Gestión de Continuidad del negocio (BCM) y además cuenta con una detallada descripción de las seis prácticas profesionales, que son utilizadas por los especialistas de Business Continuity (BC) (Sáez V., 2015).

- Política de BCM y programa de administración.
- Entendimiento de la organización.
- Determinando la estrategia de continuidad del negocio.
- Desarrollo e implementación de responsabilidades.
- Probar, dar mantenimiento y revisión del programa de continuidad del negocio.
- Desarrollando una cultura de continuidad del negocio en la organización.

2.4.6.1. Prácticas Profesionales que establece Good Practice Guidelines

Entre estas prácticas profesionales se encuentran:

Administración de Políticas y programas: la presente práctica profesional hace énfasis en la necesidad de que la directiva de la organización demuestre

el compromiso con el programa de continuidad del negocio y sus políticas para poder prevenir y estar preparados para responder idóneamente ante cualquier incidente que pueda presentarse. Por este motivo la empresa debe adherirse a las políticas, seguir los procedimientos establecidos y del mismo modo ejecutar los planes para dar soporte al programa.

Análisis de la organización: esta práctica parte del punto de conocer las funciones de la institución y la actividad que responde al objetivo principal, para de este modo conocer el efecto que la interrupción puede provocar sobre ella.

Diseño de la estrategia de continuidad del negocio: la organización debe implementar estrategias de continuidad del negocio que le permitan evitar la presencia de incidentes que amenacen de algún modo tanto a los recursos humanos como a la propiedad y del mismo modo al medio ambiente. Esta estrategia debe estar fundamentada en la identificación de peligros y en la evaluación de los riesgos, así como en el análisis del impacto, del costo-beneficio y de las restricciones del programa. La entidad debe poseer un proceso de monitoreo de dichos peligros y ajustar las medidas preventivas en relación al riesgo (Blanco E., 2008).

Desarrollo e implementación de responsabilidades: la empresa debe evaluar las necesidades de la administración basándose en los posibles peligros, por lo cual debe estar preparado para el establecimiento de procedimientos de ubicación, adquisición, almacenamiento y mantenimiento de los servicios, materiales, equipos y recursos humanos para dar una respuesta certera a la recuperación ante el impacto de los peligros identificados.

Prueba, mantenimiento y revisión del programa de continuidad del negocio: en la organización deben realizarse evaluaciones sobre los planes del programa y sus procedimientos para conocer las capacidades de respuesta. Dichas pruebas y ejercicios deben ser realizados periódicamente para fomentar y mantener las capacidades requeridas y de este modo

incrementar el entendimiento de los riesgos y el impacto que provocan en la entidad.

Desarrollo de una cultura de continuidad del negocio en la organización: es importante destacar en esta etapa la participación de los miembros de la organización en todos sus niveles, puesto que debe crearse un alto grado de concientización imprescindible para que el personal pueda identificar las funciones y responsabilidades que la entidad le ha entregado. Se busca que la alineación del personal y los recursos, tanto tecnológicos como físicos, faciliten el cumplimiento dinámico de los objetivos trazados (BCI, 2013).

El valor de estas guías radica fundamentalmente en el hecho de que toma en consideración no solo el “qué” sino también el porqué, cómo y cuándo de los principios de la disciplina de continuidad del negocio. Además, facilita las técnicas y competencias profesionales.

2.4.6.2. Procedimiento que establece Good Practice Guidelines

En el caso específico de la GBP 2013, cabe señalar que ofrece una exhaustiva revisión de la anterior versión vigente en 2010, en la cual se incluyen tanto las novedades en relación a las buenas prácticas, como en una adaptación a las directrices marcadas por la norma ISO22301:2012 (Business Continuity Institute, 2013).

En cuanto a los procedimientos establecidos para las Guías de Buenas Prácticas es importante señalar que el BCI, en su código de buenas prácticas para la gestión de continuidad del negocio, especifica algunas herramientas que se ajustan a cada etapa del ciclo de vida de la gestión de continuidad del negocio, las cuales son:

- El business impact analisys (BIA); continuity requirement analisys (CRA) y el risk assesment (RA), para la fase de “entendimiento de la organización”,

- El establecimiento de parámetros como el recovery time objective (RTO), recovery point objective (RPO) así como el maximum tolerable period of disruption (MTPD) y el maximum tolerable data lost (MTDL) para la “determinación de las estrategias”.

Sin dejar de mencionar la selección e identificación de respuestas tácticas y la consolidación de niveles de recursos, presenta una serie de pasos detallados para las demás fases del ciclo. Ofrece un enfoque estructurado y claro para el desarrollo de un programa de gestión de la continuidad del negocio, que fue tratado previamente en el análisis de la norma ISO22301:2012.

2.5. Normativa legal de continuidad del negocio en el Ecuador

En este contexto, es importante mencionar el acuerdo de Basilea II, emitido a finales del 2005 por el Comité de Supervisión Bancaria de Basilea. A través de la colaboración de varios representantes de diferentes bancos centrales de todo el mundo, se elaboró “un compendio que define los requerimientos necesarios del capital que deben presentar las instituciones financieras para el programa de administración de los riesgos que podrían afectar la estabilidad de operación de las mismas” (Motta, 2006, p. 81).

Este nuevo acuerdo se basa fundamentalmente en el análisis de los riesgos operacionales (Basel Committee on Banking Supervision, 2005), donde a su vez se exige a las instituciones financieras el cumplimiento de ciertas normas o características esenciales. Entre esas regulaciones se incluye la elaboración de planes de continuidad del negocio para garantizar de manera óptima el restablecimiento de las operaciones en caso de incidentes y desastres con las mínimas afectaciones y el empleo de recursos para ello.

Respetando los parámetros internacionales dispuestos por Basilea, el Ecuador, por medio de la Junta Bancaria y la Superintendencia de Bancos, ha dictado un compendio de resoluciones bancarias, dentro de las cuales resalta la JB-2004-631 del 22 de enero de 2004, en la cual se exige a las instituciones financieras la administración de riesgos. Específicamente el Artículo 1 plantea:

> “Las instituciones del sistema financiero controladas por la Superintendencia de Bancos y Seguros, deberán establecer esquemas eficientes y efectivos de administración y control de todos los riesgos a los que se encuentran expuestas en el desarrollo del negocio, conforme su objeto social, sin perjuicio del cumplimiento de las obligaciones que sobre la materia establezcan otras normas especiales y/o particulares. La administración integral de riesgos es parte de la estrategia institucional y del proceso de toma de decisiones” (Superintendencia de Bancos y Seguros, 2004, p. 560).

Por otra parte, el Artículo 8 de la normativa anteriormente nombrada, hace referencia a las características que debe presentar una institución financiera respecto a la gestión del riesgo. Para ello se tiene en cuenta lo siguiente (Superintendencia de Bancos y Seguros, 2004):

- Adecuada definición de la estrategia de negocio de la entidad, que incluya los riesgos asociados al mercado objetivo.
- Contar con políticas de gestión de riesgo y sus respectivos límites de exposición.
- Contar con la metodología adecuada para la gestión de riesgos.
- Contar con la estructura organizativa necesaria y eficiente donde se tenga en cuenta la unidad encargada de la gestión del riesgo.
- Contar con los sistemas de información óptimos y eficientes para garantizar el flujo de información interna y externa con la calidad necesaria y de manera oportuna.
- Considerar los recursos económicos, materiales y humanos necesarios para enfrentar las amenazas que se pudiesen suscitar y que afectarían la continuidad del negocio.

Por otro lado, la Resolución JB-2005-834 (2005), contiene especificaciones sobre la gestión del riesgo, haciendo énfasis en la administración de riesgo operativo que se suscita en las entidades financieras. También se definen los elementos esenciales donde tienen lugar dichos riesgos y las acciones de

identificación, valoración, evaluación, planeación y mitigación que deben emprenderse. Los elementos anteriormente mencionados se definen en el Artículo 4 de la nombrada resolución como: procesos, personas y tecnologías de la información (Superintendencia de Bancos y Seguros, 2005).

2.6. Análisis de requerimientos en las instituciones financieras del sector privado bancario del Ecuador

La seguridad es un aspecto esencial en la actividad bancaria, independientemente de que sean públicas o privadas. En este sentido, la Superintendencia de Bancos, ha dictado un compendio de resoluciones a modo de organizar y guiar a dichas instituciones en función de la minimización de los riesgos y la planificación necesaria para enfrentar las amenazas que puedan tener lugar en el medio y que afectarían la funcionabilidad de las entidades. El propósito de la legislación es garantizar, por responsabilidad normativa, que las instituciones protejan sus procesos críticos a fines de mantener la funcionabilidad del sector.

Teniendo en cuenta lo anterior y respecto a los riesgos informáticos, las instituciones financieras ecuatorianas son administradas a través de departamentos y directivos de TI, los cuales tienen la responsabilidad de brindar soporte a todas las sucursales de la entidad bancaria. Las organizaciones deben someterse a auditorías regulares llevadas a cabo por organismos internacionales pertinentes de acuerdo con las normativas legales sobre las TI en el Ecuador.

Dentro del área de administración de servicios informáticos de la institución financiera analizada, se atienden cuatro funciones fundamentales, las cuales se describen a continuación:

- Desarrollo: dentro de esta función el objetivo fundamental se basa en la creación, búsqueda e implementación de las aplicaciones informáticas más eficientes en función de las necesidades tanto de empleados como

de clientes, de manera que se facilite y mejore el funcionamiento de las operaciones.

- Seguridad Informática: es la encargada de elaborar los procedimientos generales, tanto para clientes internos como externos, en base a la prevención y mitigación de las amenazas que atentan contra la seguridad operativa de las instituciones financieras.
- Help Desk: se trata de la función encargada de administrar y dirigir los medios digitales en función de las necesidades de los usuarios de los sistemas internos utilizados en las instituciones financieras; cuyo personal responsable debe tener un amplio conocimiento y especialización tanto en los medios tecnológicos como en el objeto social del negocio al que responde, de manera que le permita dar un soporte técnico eficiente.
- Infraestructura: esta área se enfoca fundamentalmente a la gestión administrativa, dígase: adquisición, ubicación, instalación y mantenimiento de los medios o recursos físicos que intervienen en los procesos operacionales generales, y soportes tanto de información, como de comunicación y seguridad.

A modo de conclusión sobre lo antes expuesto, debe entenderse que para cada uno de los servicios informáticos anteriormente mencionados es necesario aplicar procedimientos de continuidad y contingencia.

Por otra parte, se deben tener en cuenta los requisitos que establece la normativa de la Superintendencia de Bancos (Superintendencia de Bancos y Seguros, 2005). En la Sección IV “Continuidad del Negocio”, Artículo 15, plantea la forma en que se debe orientar esta función en las instituciones financieras ecuatorianas, para lo cual se debe establecer un proceso de administración de la continuidad del negocio tomando como referencia los preceptos de la ISO 22301 o su forma más actualizada.

Esta norma señala los siguientes aspectos como elementos que se deben considerar para la administración de la función antes mencionada:

- “Definir objetivos, políticas, estrategias, procedimientos, metodología, planes y presupuesto para la administración de la continuidad
- Conformar el comité de continuidad del negocio
- Analizar el impacto, producto de la detención de los procesos por interrupciones
- Analizar los diferentes escenarios de riesgo
- Selección de la estrategia de continuidad por proceso
- Realización de pruebas del plan de continuidad
- Aplicar procedimientos para la concientización del plan y su cumplimiento
- Inclusión de la función de administración de continuidad al proceso de administración integral de riesgos” (Superintendencia de Bancos y Seguros, 2005).

El Artículo 16 de dicha norma, plantea otras consideraciones importantes que deben tenerse en cuenta durante el desarrollo de la continuidad del negocio, dentro de las cuales resaltan aspectos como:

- “Considerar escenarios de riesgo y procesos críticos
- Determinar roles y responsabilidades en cada caso
- Definir los criterios de activación del plan
- Dejar en claro las acciones y procedimientos a seguir al momento de activación del plan
- Establecer los tiempos máximos de interrupción y de recuperación de cada proceso
- Manejo de la comunicación e información
- Establecer el centro de mando
- Definir los parámetros de recuperación a través de procedimientos” (Superintendencia de Bancos y Seguros, 2005).

En resumen, la norma establece los requisitos básicos que deben considerarse en la administración de la continuidad del negocio, teniendo en cuenta los criterios esenciales para el desarrollo de la misma.

3. ANÁLISIS DE REFERENTES PARA GENERACIÓN DEL BCP

En el siglo XXI los modelos organizacionales y sistemas empresariales han evolucionado considerablemente desde sus perspectivas de gestión y estrategia. Han surgido nuevos enfoques y teorías sobre el modo de gestionar los recursos y perfeccionar los modos de actuación administrativos. Dicho accionar ha estado siempre direccionado a la constitución de una empresa eficiente, capaz de satisfacer las necesidades del cliente, optimizando siempre los recursos que dispone para garantizar una mayor utilidad y beneficio.

Para lograr entonces la misión que se plantea ha necesitado alinear muy cautelosamente sus procesos y los procedimientos de trabajo. Sin embargo, no es suficiente alinear los procesos con los objetivos y con la misión que se definen cuando el entorno y el medio en el que se desarrollan las organizaciones es constantemente cambiante y fuente inevitable de amenazas que pueden afectar su estabilidad, lo cual hace a las organizaciones de hoy día, vulnerables a la ocurrencia de eventos negativos.

Por este motivo, las empresas deben estar preparadas para reaccionar ante posibles incidentes de seguridad que provoquen la minimización de su capacidad operativa o pongan en peligro la continuidad del negocio, y consecuentemente la insatisfacción del cliente. Es necesario que la organización esté en su entera capacidad para responder rápida y oportunamente ante cualquier contingencia grave, de modo que la reanudación de las actividades sea garantizada en un plazo de tiempo óptimo, para que no se comprometa su eficiencia.

3.1. Comparación de referentes para la determinación de una metodología de generación de BCP

A partir de dicha necesidad es que surgen los llamados Planes de Continuidad del Negocio y la necesaria gestión de los mismos.

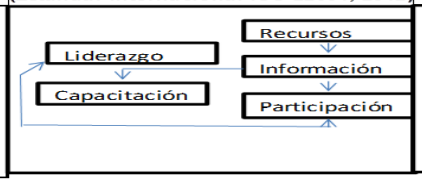
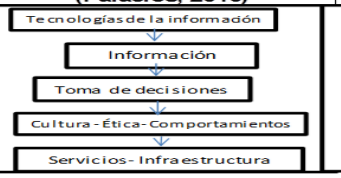
En el capítulo anterior fueron analizados algunos de los referentes más significativos que a lo largo de los años han tratado profundamente la temática

desde sus diferentes enfoques y perspectivas y que en el presente acápite se analizarán de manera intencionada, para establecer una comparación entre los mismos. Los referentes en cada momento aluden a la gestión, y no es posible hacer un estudio de este tipo sin establecer una alineación con los procesos que plantea la gestión de mejora continua en las organizaciones como parte fundamental de la gestión de la calidad.

Es por ello que a continuación se presenta un cuadro comparativo entre los modelos referentes estudiados y la manera en que cada uno de ellos, explícita o implícitamente, aluden a los procesos de Planificar, Hacer, Verificar y Actuar que plantea Deming en su ciclo.

Tabla 1.

Comparación de referentes enfoques de BCP

REFERENTES INTERNACIONALES PARA LA CONTINUIDAD DEL NEGOCIO				
MEJORA CONTINUA	ISO/IEC 27005: 2011 (A)	22301:2012 (B)	COBIT 5 ©	BUENAS PRÁCTICAS (D)
PLANIFICAR	**Establecimiento del contexto** Conocer la organización Determinar alcances y limitaciones **Identificación y estimación de riesgos** Identificar activos de soporte/ Procesos/ Datos Determinar amenazas * Estrategias * Materiales * Técnicas * Accidentales ^Intencionales Establecer prioridades Evaluación de riesgos **Plan de Comunicación** * Aspectos generales sobre los riesgos * Comunicación sobre la marcha * Comunicación de resultados **Establecer acciones para enfretar los riesgos definidos** **(ISO, 2011) (SGSI, 2015)**	**Contexto de la organización** Actividades/ Priorizadas Vinculación de objetivos y políticas Necesidades de partes interesadas Legislaciones Estrategia organizacional * Integración de los requisitos del sistema con los proceso Determinación de riesgos Evaluación de los riesgos definidos Determinacion de : **Políticas de CN** **Requisitos del BCP** **Principios del BCP** **Objetivos del BCP** **Determinar procedimientos de actuación** Protocolos de comunicación Impactos de eventos no deseados Presuposiciones y análisis de interdependencia **(Estándar Internacional ISO 22301, 2012)**	**Definir objetivos organizacionales** **Definir objetivos de TI** **Definir principios, políticas y modelos** Guías prácticas **Actividades para el logro de los objetivos** **Definir requerimiento de CN, objetivos y alcance** **Definir escenarios de incidencia** **Definir estrategias de CN** Socialización y capacitación **Definir acciones de capacitación** **Procedimientos de actuacion** **(Palacios, 2016)**	**Entendimiento de la organización** **Identificar necesidades** **Identificar peligros y evaluación de riesgos** Matriz de riesgos Probabilidad de ocurrencua Vulnerabilidades Impacto **Estrategias de mitigación** **(Blanco, 2008)**
HACER	**Implementación del tratamiento de riesgos** **(SGSI, 2015)**	Implantar Operación Análisis del impacto del SGCN Implementar estrategias de CN Aplicación de los procedimientos **(Estándar Internacional ISO 22301, 2012)**	**Operar** **Desarrollo e implementacion** **Ejecutar** **(Palacios, 2016)**	**Implementación** **Operaciones y procedimientos** **Ejecutar planes de soporte al programa** **(Blanco, 2008)**
VERIFICAR	**Monitoreo y revisión** Control de cambios Evaluar cumplimiento de los planes Análisis costo-beneficio **(ISO, 2011)**	**Revisar y Monitorear** Supervisión de la dirección Pruebas de seguimiento Evaluación del desempeño ^ Revisar periodicamente Metas * Auditorías internas **(Estándar Internacional ISO 22301, 2012)**	**Monitorear** **Pruebas y revision** **Revisiones post-reanudacion** **Evaluación de CN** **Acuerdos de respaldo** **(Palacios, 2016)**	**Dirección, control y coordinación** **Evaluaciones** **Monitoreo** **(Blanco, 2008)**
ACTUAR	**Mantener la gestión continuamente actualizada** **(ISO, 2011)**	**Mejora continua** **Mantenimiento del plan** **Sistematización** **Informes de resultados** **(Estándar Internacional ISO 22301, 2012)**	**Construir e implementar mejoras** **Mantenimiento** **(Palacios, 2016)**	**Recuperación** **Acciones correctivas y preventivas** **(Blanco, 2008)**
PILARES	**INFORMACIÓN**			

Todas estas normas en sí engloban el ciclo de vida de la continuidad del negocio y esto puede afirmarse teniendo en cuenta que cada una parte de comprender la organización, trazar las estrategias de continuidad, desarrollar e implementar el plan y probar y revisar continuamente el mismo.

A pesar de que cada norma presenta un enfoque diferente, todas se basan en identificar las actividades críticas que pueden tener gran impacto en cortos períodos de tiempo por la necesidad que posea la organización y que deben ser rápidamente recuperadas en caso de existir interrupciones. Además, todas incitan a analizar el posible impacto que podría causar en el negocio un desastre de cualquier índole y proponen tener diseñadas las medidas necesarias para reducir los impactos potenciales.

Proponen que la institución identifique las apropiadas estrategias que faciliten el mantenimiento de las habilidades y el conocimiento clave, así como la capacitación del personal para enfrentar dichas situaciones.

A pesar de que todas engloban este ciclo, cada una hace énfasis en aspectos que consideran primordiales. Por ejemplo, en el caso de ISO 22301:2012 Sistema de Gestión de Continuidad del Negocio, se enfoca principalmente en que la organización tome la determinación de qué aspectos serán cubiertos por la continuidad del negocio y del mismo modo decida qué será excluido y posteriormente comunicar a todas las partes, tanto externas como internas, cuál será el alcance que tendrá el mismo (Cañas, 2009).

Las normas analizadas también hacen hincapié en garantizar que la información vitalicia de la empresa se encuentre completamente protegida y que su recuperación sea efectiva, garantizando con ello la confidencialidad, integridad y disponibilidad de dichos datos, a través de las copias de seguridad ya sean digitales o físicas. En este sentido enfatiza la norma ISO/IEC 27005:2011 que se enfoca directamente en la gestión de la seguridad de la información, y plantea que es responsabilidad de la organización definir su propio enfoque de la gestión de riesgos, por lo que en relación con las otras 3

objeto de estudio es la más relevante para los gerentes y el personal que se encuentra directamente relacionado con la seguridad de la información.

En este caso es imprescindible resaltar que cada norma va enfocada a directrices que, a pesar de ser diferentes entre sí, poseen elementos esenciales que facilitan a la organización la realización de un óptimo y ajustable plan de continuidad del negocio.

Por su parte COBIT 5, al ser un marco comprensivo de herramientas, prácticas y modelos, se enfoca en ayudar a la organización a obtener la eficiencia mediante la gobernanza, la gestión de la información y la tecnología. Por lo que a diferencia de las otras normas objeto de estudio, COBIT 5 incita a los profesionales a nivel mundial a que comprendan el potencial positivo que ofrece el uso de la tecnología en el mundo digital en evolución, fomentando de este modo el negocio electrónico.

De una forma u otra, cada referente presenta su modo de implementación de respuestas, con el desarrollo de planes para garantizar la continuidad de las actividades en caso de la ocurrencia de riesgos, por lo que enfatizan en la importancia de que la empresa tenga definidas las estructuras de respuesta ante incidentes, para tomar el control de la situación.

Good Practice Guidelines (GPG) marca una pauta al proponer la creación de una cultura de continuidad del negocio, lo cual es destacable teniendo en cuenta que mientras mayor preparación posean los individuos respecto a los riesgos, más rápida será su respuesta ante incidentes repentinos, pues ya estarían listadas las tareas y acciones, así como el mecanismo de activación, los recursos requeridos para enfrentar la crisis en dependencia de la que fuere y las responsabilidades.

Cada uno de los referentes estudiados muestra un enfoque específico hacia varios elementos organizacionales, considerados para el análisis como pilares de soporte para garantizar la continuidad. Por citar un ejemplo, el caso de la ISO/IEC 27005:2011 hace especial énfasis en la información. Por otra parte, la

ISO 22301:2012 alude a la incidencia que tienen los recursos, ya sean informacionales, materiales o humanos, siendo estos últimos un importante eslabón en la consecución de las actividades y la eficiente gestión de los planes de continuidad, garantizando como premisa la participación colectiva, en lo cual tiene notable incidencia el tipo de liderazgo que se fomenta en la organización. Hace referencia también a la necesidad de capacitación oportuna, para lo cual debe ser usada toda la información respectiva a las acciones propias de los planes. COBIT 5 en cambio se centra en las TI en toda su magnitud, soportadas obviamente en la información y en aquellos elementos que la posicionan adecuadamente en la organización, dígase servicios, infraestructura, aplicaciones, cultura, ética y comportamientos. Alude también a la importancia que cobra la toma de decisiones. Por su parte GPG da mayor importancia a los recursos, considerando siempre la necesidad de fomentar las habilidades de estos a partir del entrenamiento y sustentados por las facilidades y la logística respectiva para la eficiente consecución de las actividades que plantea.

A modo general puede decirse que estas normas son aplicables a todas las instituciones, aunque cada una tenga un enfoque diferente, todas tienen la finalidad de construir el plan de continuidad del negocio más idóneo para cada empresa y de esa manera fomentar el eficiente desempeño de los procesos en las mismas.

3.2. Diseño de una metodología para la generación de un BCP

Una vez analizados los estándares internacionales anteriores, y basados en sus principios y bases teóricas, se procede al diseño de una metodología integrada que contemple las visiones básicas del diseño de BCP, con un sencillo nivel de comprensión, de manera que pueda ser implementada por las organizaciones con básicos conocimientos respectivos a la CN.

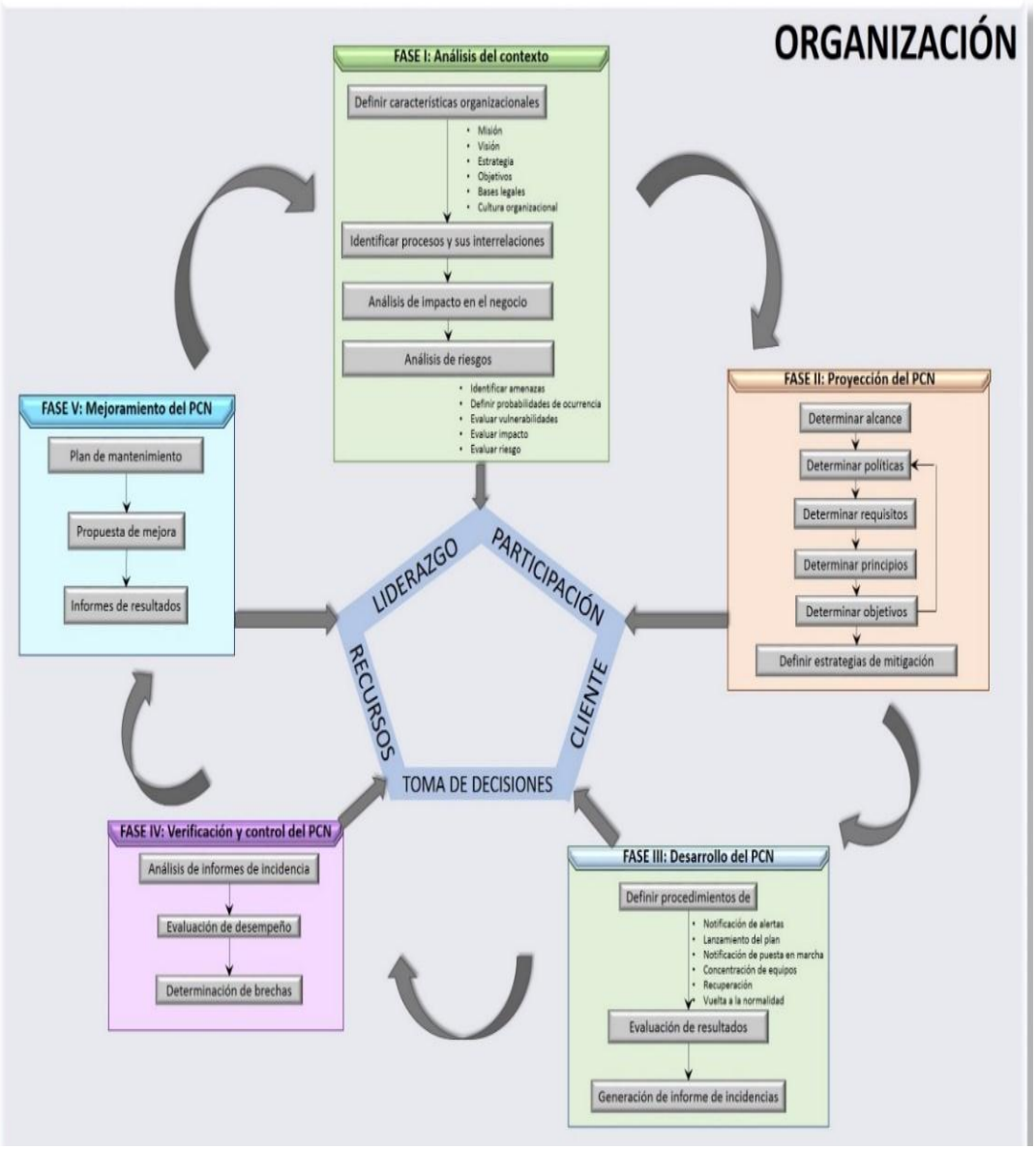


Figura 7. Organización por fases

En la siguiente tabla se especifican los referentes que sirvieron como base para el establecimiento de las actividades planteadas en cada fase propuesta, según la nomenclatura de la Tabla 1, donde: A: ISO/IEC 27005: 2011, B: 22301:2012, C: COBIT 5 y D: BUENAS PRÁCTICAS.

Tabla 2.

Soporte de referentes para la elaboración de la MEBCP

Actividades	Referente que sustenta la actividad
FASE I: Análisis del contexto	
Definir características organizacionales	A-B-C
Identificar procesos y sus interrelaciones	A-B-C
Determinar procesos críticos y sus RMP	A-B
Análisis de riesgos	A-B-C-D
FASE II: Proyección del PCN	
Determinar alcance	C
Determinar políticas	B
Determinar requisitos	B-C
Determinar principios	B
Determinar objetivos	B-C
Definir estrategias de mitigación	A-B-C-D
FASE III: Desarrollo del PCN	
Definir procedimientos	A-B-D
Análisis de impacto	A-B
Generación de informe de incidencias	Autor
FASE IV: Verificación y control del PCN	
Análisis de informes de incidencia	Autor
Evaluación de desempeño	A-B-C-D
Determinación de brechas	Autor
FASE V: Mejoramiento del PCN	
Plan de mantenimiento	A-B-C
Propuesta de mejora	A-B-C-D
Informes de resultados	B
Pilares	
Recursos	A-B-C-D
Liderazgo	B-C
Participación	B-C-D
Cliente	A-B-C-D
Toma de decisiones	B-C

En la figura 7 se puede apreciar la metodología para el diseño de un plan de continuidad del negocio, denominada por sus siglas MEBCP. La misma cuenta con 5 fases que van desde el análisis y caracterización del contexto de desarrollo, hasta el mejoramiento del BCP resultante.

En la primera fase esta metodología plantea que deben ser definidas las características organizacionales, con el propósito de saber inicialmente a qué tipo de organización se enfrenta el análisis. No es posible mejorar aquello que no se conoce. Esta caracterización debe ser lo más detallada y abarcadora posible ya que a partir de esta etapa estarán fundamentadas las demás.

La identificación de los procesos y la determinación de las interrelaciones entre ellos es otra de las actividades indicadas. Este punto pretende determinar las prácticas de la organización y la dependencia que tienen unas de otras. Es recomendado contemplar los recursos asociados a los mismos (materiales, financieros, humanos, tecnológicos, etc.) y el papel que cada uno de ellos juega en el desempeño de cada proceso. Para la ejecución de esta tarea se recomienda el uso del mapa de procesos.

Una vez identificados los procesos organizacionales se está en la capacidad de identificar cuáles de ellos figuran como críticos, o cuáles de las actividades que en ellos se desarrollan pueden ser consideradas críticas para el eficiente desempeño de la organización y la continuidad del negocio, analizando el impacto que puede provocar la interrupción de alguno de ellos en la eficiencia del mismo.

La siguiente y última etapa de la primera fase es el análisis de riesgos (Humanos-Tecnológicos-Naturales), en la cual deben ser muy bien definidas todas las amenazas internas y externas que pueden provocar de algún modo el paro de alguna de las actividades de la organización. Deben ser definidas las probabilidades de ocurrencia de éstas. Se establece también la evaluación de las vulnerabilidades, los impactos y los riesgos. Se recomienda para esta etapa el uso de matrices de riesgos.

Una vez que se tenga una idea concreta de lo que ocurre en la organización, así como la influencia que el entorno ejerce, negativa o positivamente sobre ella, es momento de iniciar la proyección del BCP por el cual se va a orientar la gestión de ésta. Es entonces donde inicia la Fase II de Proyección. En esta fase se fundamentan las políticas, el alcance, requisitos, principios y objetivos

del BCP. Estos últimos deben ser concretos, medibles y responder a las políticas determinadas. En este momento deben ser definidas las estrategias de mitigación, teniendo en cuenta los riesgos y fundamentos propios del plan. En las estrategias debe ser explícita la forma en que se desarrollarán las acciones que garanticen la mitigación de los efectos negativos. Deben dejar claramente dicho, qué hacer en cada caso, dónde hacerlo y con el empleo de qué medios y recursos. Deben quedar determinadas las acciones a tomar para cada evento inesperado, para lo cual resultaría de gran utilidad el apoyo en la matriz de riesgos.

Hasta el momento se ha trazado el camino hacia la implementación del BCP, el cual, hasta acá, contiene las acciones que deben ser tomadas, sin embargo, no es hasta la Fase III que se implementan dichas acciones y aparece la necesidad de definir cómo realizarlas y aquellos elementos que sustentan su correcta ejecución. En la Fase III de Desarrollo del BCP se establece la definición de los procedimientos de notificación de alerta, lanzamiento del plan, notificación de puesta en marcha, concentraciones de equipos, recuperación y vuelta a la normalidad. Se alude a la evaluación de los resultados obtenidos tras la implementación del BCP y de igual manera a la generación de informes como estrategia de documentación de incidentes. En esta fase se deben dejar bien establecidos los procedimientos de comunicaciones y transmisión de información hacia todas las partes implicadas en la implementación del BCP.

Una vez desarrollado e implementado el BCP, la metodología establece, en la Fase IV, que se realice la pertinente verificación y control sobre los resultados obtenidos tras la implementación. A partir del análisis de los informes de incidencia pueden ser evaluados los resultados, y alineándolos con los objetivos del plan, determinar las brechas y deficiencias existentes.

Al ser determinadas las vulnerabilidades del BCP, solo queda indicar las propuestas de mejora, las cuales pueden contemplar las acciones correctivas o preventivas necesarias. Puede establecerse entonces un plan de

mantenimiento y documentar los resultados alcanzados. Ello está establecido en la fase V.

La MEBCP planteada, puede ser empleada para lograr la sistematización del plan, pues a pesar de que en la fase V queden propuestas las mejoras pertinentes, hay que tener presente que la misma está basada sobre los fundamentos de mejora continua de Deming. Ello significa que esas mejoras pueden conllevar a cambios de la organización y por consiguiente los elementos definidos en la Fase I pueden ser modificados. Por otra parte, las influencias del constante cambio que se manifiesta en el entorno, también son elementos que definen nuevos puntos de partida que pueden o no modificar el resto del plan.

Al desarrollar la MEBCP, es fundamental contemplar los pilares que en cada una de sus etapas sustentan la correcta implementación de la misma. Se habla precisamente del liderazgo, participación, recursos, toma de decisiones y satisfacción del cliente, siendo este último el objetivo fundamental del desarrollo de cualquier BCP. Es a éste a quien se necesita satisfacer a partir de la ininterrumpida consecución de los negocios. Son definidos estos pilares como elementos primordiales a considerar para el correcto desarrollo de la MEBCP y por consiguiente para la adecuada gestión del BCP resultante tras su implementación, puesto que son los elementos centrales que en cualquier organización sustentan la consecución de las actividades y el eficiente desempeño de las mismas.

Queda de este modo determinada una metodología para la confección de un BCP, con un enfoque sistémico y de mejora continua, que además puede ser empleada por las organizaciones para establecer su BCP de acuerdo a la norma 22301:2012. A partir de su implementación se obtienen los documentos de tipo obligatorio que la empresa debe desarrollar, según establece la normativa, para obtener la certificación.

4. IMPLEMENTACIÓN DE UNA METODOLOGÍA DE GENERACIÓN DE BCP ENFOCADO A LOS RIESGOS TECNOLÓGICOS

4.1. Análisis del contexto

El análisis del contexto empresarial, es uno de los factores más importantes al establecer una determinada metodología, en cualquiera de las organizaciones económicas que conforman un sistema, es por ello que en esta primera fase de implementación para la generación de BCP enfocado a los riesgos tecnológicos, se realiza en primer lugar una caracterización del entorno, teniendo en cuenta los elementos que intervienen en el comportamiento empresarial y que son la base para las demás etapas propuestas en esta investigación.

4.1.1. Definir las características organizacionales

Las características adoptadas por las organizaciones dependen en gran medida del desarrollo alcanzado por el entorno que la rodea. El progreso económico y tecnológico es sin lugar a dudas uno de los principales elementos que lo condicionan (López, 2012). El Banco ABC no está exento de todo esto y es por ello que busca formas alternativas y novedosas con las cuales logre cubrir las necesidades financieras de sus clientes, personalizando cada caso, para poder lograr la productividad y la eficiencia de la organización.

Su modelo de negocio está centrado en elevar la calidad de los procesos que en ella se desarrollan y en su expansión hacia las principales ciudades del país, perfeccionando su imagen permanentemente. Sus políticas con respecto al manejo de los riesgos, hacen posible que la institución sea muy confiable y que mediante ella se impulsen los proyectos tanto personales, como empresariales de los usuarios. La utilización de la tecnología de punta, su solvencia, su solidez financiera y su prudente política de riesgos, son aspectos que la caracterizan y que hacen posible lograr la confianza de sus clientes.

Es una organización que ha acumulado una vasta experiencia en su rama que hace posible que pueda adaptarse a los cambios del mercado con facilidad y al

mismo tiempo continuar creciendo paulatinamente. Cuenta con un capital humano que tiene pasión por prestar un servicio de excelencia, con valores que constituyen al mismo tiempo la principal fortaleza de la institución. Cuenta con estándares de calidad altos, los ejecutivos realizan su trabajo con excelencia, tiene iniciativas que aportan al trabajo, su colectivo es entusiasta, son leales a la organización y a sus clientes (Banco Capital , 2015).

En todos los años de labor, se han obtenido logros que los motiva a seguir ofreciendo servicios con todos los requisitos y profesionalidad que el sistema requiere, se encuentran comprometidos con los nuevos retos que tienen que enfrentar en correspondencia con el desarrollo económico y social del país, para lo cual se esfuerzan en brindar un mejor servicio en la protección del patrimonio de los clientes y el futuro financiero de cada uno de ellos.

En el año 1993, se conforma la Sociedad Financiera CBA, ubicada en la parte norte de Ecuador, la que, por su trabajo constante y destacado, logra posicionarse en el año 1997 en todo el país, hasta llegar a convertirse en la segunda sociedad financiera más grande del país, obteniendo éxitos en sus operaciones y ganando prestigio entre sus clientes. Esto hace posible que en el año 2007 por su crecimiento se convierta de CBA en Banco ABC, es en este período donde se abren nuevas sucursales, ubicadas en las principales ciudades del país. Su desarrollo durante 22 años de operaciones financieras, ha direccionado sus esfuerzos al cumplimiento de sus metas y de sus objetivos, buscando optimizar sus recursos y perfeccionando la gestión empresarial (Banco Capital, 2016) .

Actualmente, el Banco ABC, cuenta con una probada solidez y al mismo tiempo con una de las mejores clasificaciones del sistema financiero AA-, que otorga el SCR. La institución cuenta con todos los recursos que necesita para que sus operaciones sean confiables, y que además tengan la calidad necesaria y percibida por el usuario, tiene servicio de banca en línea, lo que agiliza las transacciones e incrementa la fluidez de las gestiones y al mismo tiempo ahorra tiempo tanto a usuarios como al personal del banco.

Los servicios que ofrece de banca personal son:

- Cuentas de ahorros
- Cuenta corriente
- Crédito de consumo
- Inversiones
- Crédito automotriz

Servicios

Se enfoca al servicio corporativo, en dependencia de las necesidades de las organizaciones mediante su asistencia de Banca Empresas, a este sector le brinda los siguientes servicios:

- Cuenta corriente
- Cuenta de ahorros
- Inversiones
- Cash management
- Factoring

Misión

Proveer una gama de servicios de calidad orientados a satisfacer las necesidades financieras de nuestros clientes, basados en un proceso de constante innovación, con un servicio personalizado, eficiente y transparente. Nuestra gestión está centrada en el cliente y orientada hacia la productividad y la creación de valor (Banco Capital, 2016).

Visión

Ser el mejor banco, basado en altos índices de calidad, solvencia, eficiencia, rentabilidad y servicio (Banco Capital, 2016).

Estrategia

Posicionar al Banco ABC como una institución de preferencia a partir del asentamiento de las bases para el desarrollo de la máxima cobertura nacional en áreas de mejorar los resultados económico financieros de la institución, y en concordancia con ello, la equidad y desarrollo del país, garantizando la constante mejora e innovación de productos y servicios, procedimientos y estrategias de trabajo que garanticen la satisfacción de las necesidades de cada segmento de cliente, con el soporte del crecimiento de las capacidades del talento humano y el uso de la tecnología (Banco Capital, 2016).

Objetivos Estratégicos

1- Trabajar en el perfeccionamiento y mejora continua de los procesos y procedimientos internos, garantizando el incremento de la calidad de los servicios.
2- Ampliar la cobertura geográfica y soporte de los productos y servicios, en función de las necesidades del cliente.
3- Establecer mecanismos de respuesta rápida que garanticen la continuidad de los procesos y los servicios, así como la satisfacción de las reclamaciones del cliente.
4- Garantizar la constante oferta de servicios y productos novedosos para los diferentes segmentos de mercado, que garanticen el posicionamiento y reconocimiento nacional.
5- Fomentar la inteligencia de negocios a partir del empleo de herramientas de intercambio con el cliente.
6- Fomentar la diferenciación institucional basada en la calidad del servicio, el desarrollo profesional y ético de las personas y las condiciones óptimas del ambiente laboral (Banco Capital, 2016).

Bases Legales

La base legal del Banco ABC, está encaminada a desarrollar sus servicios y cumplir sus funciones eficientemente, además de estar acorde con las normas

establecidas a nivel nacional al respecto ya que es por ellas, por donde se le hacen los controles, a continuación, se muestran algunos ejemplos:

Código Orgánico Monetario y Financiero

Este código tiene como objetivo, potenciar la regulación de trabajo, la producción de riquezas, así como su distribución y redistribución, por otro lado asegura que el ejercicio de las actividades monetarias y financieras de valores y seguros sea consistente e integrado. O de los objetivos más importantes de este documento es asegurar los niveles de liquidez de la economía, mitigar los riesgos sistémicos y reducir las fluctuaciones de la economía (Código Orgánico Monetario y Financiero, 2014).

Instrumentos de normalización nacional

- Código Orgánico Monetario y Financiero
- Ley de Burós de Información
- Ley de Creación de la Red de Seguridad Financiera
- Ley Orgánica de Servicio Público
- Normas Generales del Cheque

Alineamiento con el Plan Nacional para el Buen Vivir 2013-2017.

Otra de las características con las que cuenta el Banco ABC, es que, sus estrategias están en correspondencia con el Plan Nacional del Buen Vivir, aprobado para los años 2007-2017, en específico a los siguientes objetivos del mismo:

- Consolidar el sistema económico social y solidario, de forma sostenible
- Garantizar la soberanía y la paz, profundizar la inserción estratégica en el mundo y la integración latinoamericana (Plan Nacional del Buen Vivir, 2013).

Cultura Organizacional

La cultura organizacional del Banco ABC, está caracterizada por mantener los negocios comerciales bajo los principios de recíproca fiabilidad y confianza, constituyendo no solo una función contractual con sus clientes, sino que al mismo tiempo se reconoce como aseguradora de los intereses patrimoniales de éstos y es responsable de su capital e interés individual.

En la organización se percibe un clima de confianza y honestidad adecuado en el ambiente de trabajo interno, lo que al mismo tiempo permite la demanda entre sus miembros de un correcto desempeño de las actividades a desarrollar en el trabajo, el cual está lleno de iniciativas, lealtad, respeto y confianza mutua. Otro de los aspectos fundamentales que caracteriza a la institución es su preocupación por la capacitación constante de sus empleados, elevando el nivel intelectual del capital humano (Banco Capital , 2015).

Por otro lado, realiza acciones mediante las cuales se logren fortalecer los valores, tanto los éticos como los profesionales de su comunidad, mayormente encaminados a la integridad, productividad, lealtad, honestidad y compromiso, teniendo en cuenta los principios y normas conductuales que deben direccionar la actitud y comportamiento de los empleados, directivos, colaboradores y funcionarios. De esta manera se garantiza el fortalecimiento de las relaciones sociales y la existencia de un entorno laboral acogedor.

4.1.2. Identificación de procesos organizacionales y sus interrelaciones.

En este epígrafe y para enriquecer la caracterización del Banco ABC, se hace un análisis un poco más interno, donde se identifican los procesos que sirven de base al buen funcionamiento y desarrollo de los servicios que se prestan. Utilizando las técnicas de la observación directa y las entrevistas realizadas se detallan los procesos y macroprocesos en el siguiente mapa:

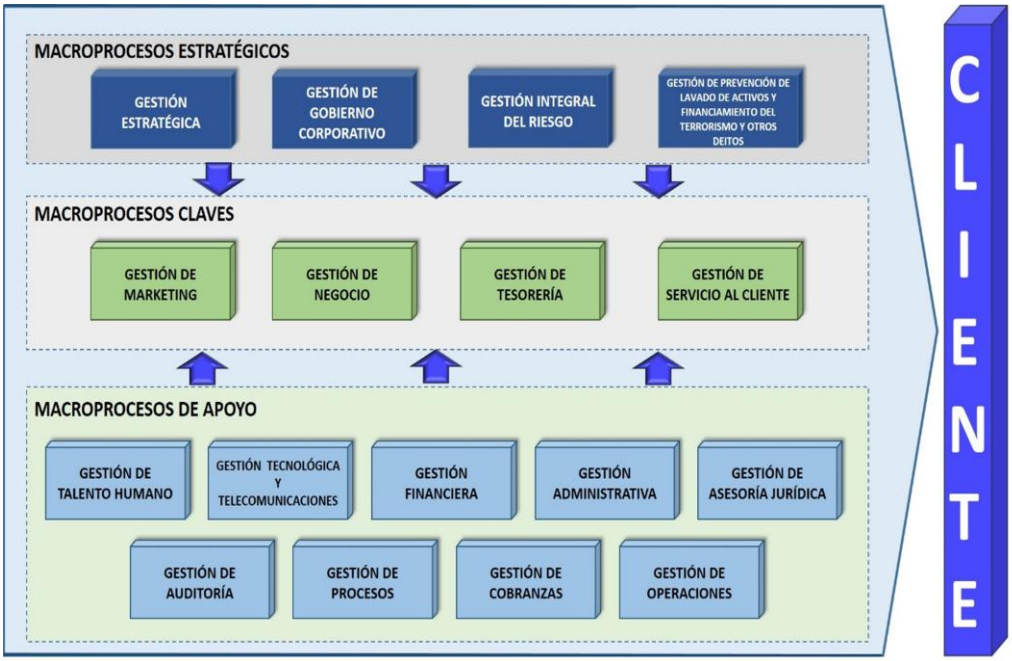


Figura 8. Alineación de estándares ISO 31000 e ISO 27005 con modelo PHVA

Son 17 macroprocesos definidos en el mapa anterior, y se clasifican en 4, que son los estratégicos, 4 son claves y 9 son de apoyo. Al mismo tiempo se definen los procesos y los subprocesos que lo sustenta y que se definen en la siguiente tabla:

Tabla 3.

Macroprocesos, procesos y subprocesos del Banco ABC

Macroproceso	Proceso	Subproceso
GESTIÓN ESTRATÉGICA	Planificación estratégica	• Actualización del plan estratégico • Elaboración y actualización del plan operativo anual • Ejecución y evaluación de planes operativos • Difusión de resultados de planificación institucional • Seguimiento y evaluación del plan estratégico
	Planificación financiera	• Elaboración de presupuesto general • Seguimiento y evaluación del presupuesto general • Cálculo y análisis de indicadores financieros
	Planificación comercial	• Elaboración del plan de negocios • Seguimiento y evaluación del plan de negocios

GESTIÓN DE GOBIERNO CORPORATIVO	Transparencia de la información	• Emisión de resoluciones del directorio
	Gestión de la administración institucional	• Nombramiento de presidente, dignidades y secesión de ejecutivos • Creación y actualización de reglamentos internos • Elaboración y actualización de manuales requeridos por organismos externos • Actualización de organigramas y orgánico funcional
GESTIÓN INTEGRAL DEL RIESGO	Administración del riesgo	• Administración de riesgo de crédito (Considerar seguimiento y control de garantías) • Administración de riesgo de mercado y liquidez • Administración de riesgo operativo
	Calificación de riesgos	• Calificación de activos de riesgos • Administración de seguridad de la información (Cash management)
	Administración de planes de contingencia y continuidad	• Administración e la continuidad del negocio
	Seguridad y control de información	• Administración de seguridad de la información
GESTIÓN DE PREVENCIÓN DE LAVADO DE ACTIVOS Y FINANCIAMIENTO DEL TERRORISMO Y OTROS DELITOS	Gestión del programa de prevención y control de lavado de activos y financiamiento del terrorismo y otros delitos	• Elaboración, actualización y difusión del manual de control interno para la prevención de lavado de activos y financiamiento del terrorismo y otros delito • Debida diligencia • Inducción y capacitación en temas de prevención de lavado de activos, financiamiento del terrorismo y otros delitos
	Gestión de reportes	• Elaboración y envío de informes a organismos de control • Elaboración del plan anual de trabajo, plan anual de capacitación
	Gestión de monitoreo	• Protocolo de lista de observados • Actualización de las bases de datos de listas reservadas
GESTIÓN DE MARKETING	Administración de productos	• Desarrollo de investigaciones de mercado y difusión de resultados • Definición, diseño e implementación de nuevos productos y servicios • Mantenimiento, modificación, eliminación de productos y servicios • Implementación de tarifas diferenciadas • Desarrollo, seguimiento y evaluación de campañas
	Calidad de servicio e información	• Administración de canales virtuales y telefónicos • Mantenimiento y actualización de bases de datos • Anclaje de asesores a cliente
	Imagen	• Modelamiento de la imagen corporativa

	institucional	• Desarrollo de campañas de comunicación institucional interna y externa
GESTIÓN DE NEGOCIOS	Gestión de Captaciones	• Apertura de cuentas corrientes • Cierre de cuentas corrientes • Sobregiros • Apertura de cuentas de ahorro • Apertura de cuentas de ahorro crédito automotriz • Cierre de cuentas de ahorro • Apertura de inversiones a plazo • Renovación de inversiones a plazo • Cancelación-Pre cancelación inversiones a plazo • Endoso de certificados de deposito • Negociación Cash Management
	Gestión de Colocaciones	• Concesión crédito canal Automotriz • Concesión crédito canal Banca • Factoring • Compra de cartera • Análisis de créditos • Aprobación de créditos
GESTIÓN DE TESORERÍA	Administración de portafolio	• Administración de fideicomisos • Inversiones de portafolio propio en el mercado primario extrabursátil • Inversiones portafolio propio en mercado secundario • Inversiones portafolio propio en mercado secundario bursátil • Renovación de la inversión • Cancelación de la inversión • Inversiones de portafolio en mercado primario extrabursátil • Cancelación de la inversión a través de mercado de valores • Cesión de instrumentos financieros • Venta de instrumentos financieros • Colocación de inversiones sobre el exterior • Cancelación de inversiones sobre el exterior
	Manejo de liquidez	• Elaboración de flujos de liquidez • Proyección de liquidez diaria • Compra/Venta de moneda extranjera • Contratación de financiamiento • Cancelación de capital e interés de financiamiento
GESTIÓN DE SERVICIO AL CLIENTE	Estándares de atención	• Manejo de sugerencias de clientes • Evaluación del nivel de satisfacción del cliente • Tarifario de productos y servicios
	Atención de reclamos y quejas	• Recepción, análisis y atención de reclamos y quejas de clientes • Elaboración de informe anual sobre atención al cliente
GESTIÓN DE TALENTO HUMANO	Gestión de incorporación	• Reclutamiento • Selección • Contratación • Inducción integral del personal

	Gestión de permanencia	• Levantamiento y actualización de perfiles • Evaluación del desempeño • Capacitación • Desarrollo y plan de carrera • Clima laboral
	Planificación y administración del personal	• Registro de entrada y salida en el IESS • Actualización de información y documentación del personal • Valoración de cargos • Administración salarial • Beneficios e incentivos • Administración de nómina • Control de póliza de seguro de vida y asistencia médica del personal • Definición y control de vinculados
GESTIÓN TECNOLÓGICA Y TELECOMUNICA_ CIONES	Administración, mantenimiento y control del desarrollo de aplicaciones	• Desarrollo de sistemas • Diseño de páginas web • Compra de herramientas de desarrollo • Administración de calidad de los proyectos • Control de versionamiento de desarrollo • Seguimiento del desarrollo del ciclo de vida de las aplicaciones
	Organización de TI	• Seguimiento de proyectos de sistemas • Monitoreo de servicios • Monitoreo del seguimiento del presupuesto asignado
	Administración, mantenimiento y control de TI	• Compra de Software de terceros • Transferencia tecnológica de Software de terceros • Generación de respaldos • Creación y mantenimiento de ambientes T24 • Mantenimiento de las Bases de Datos SQL • Paso de programas a producción • Paso a producción emergentes • Creación, mantenimiento y eliminación de usuarios • Mantenimiento de claves de acceso a servidores • Control de inventario de Hardware • Control de inventario de Software • Protección a equipos de virus informáticos • Control de difusión de software pirata • Actualizaciones (Parches) de software en producción • Revisión periódica de los derechos de usuario • Revisión periódica de virus • Aplicación de seguridad • Reporte de problemas al departamento de soporte del departamento de sistemas • Reporte de errores en T24 con soporte externo del proveedor • Selección y adquisición de hardware y software • Administración y monitoreo de red • Revisión de Desempeño-Capacidad y

		disponibilidad de recursos informáticos • Evaluación del desempeño del sistema • Administración de configuraciones de la infraestructura tecnológica • Administración del proceso de externalización o de consultoría • Validación de respaldos del CORE del banco • Respaldo de información de usuarios • Mantenimiento de hardware (equipos finales de usuario) • Destrucción de respaldos CORE bancario y bases de Datos • Redimensión de tablas (Resize) • Definición de acuerdo de niveles de servicio • Validación de respaldos antiguos • Ejecución del cierre del sistema • Validación del proceso de redimensionamiento de tablas en el sistema CORE T24
GESTIÓN FINANCIERA	Fijación de tasas y precios	• Costeo de productos y servicios
	Control presupuestario	• Administración y definición de estrategias de captación institucional • Administración y definición de estrategias de colocación institucional • Elaboración de informes al directorio • Elaboración de control presupuestario • Informe de transparencia de la información • Elaboración de indicadores financieros • Actualización de base de dato de depósitos, ahorros a plazo, monetarios, en base al DWH • Elaborar reportes de información gerencial internos • Elaborar reportes entidades de control • Modelo de pago comisiones • Elaboración de reporte de créditos castigados • Elaboración de patrimonio técnico • Elaboración de reporte de sectorización semanal • Administración y definición de estrategias de reserva de liquidez • Análisis, aprobación y seguimiento de mercado y entidades financieras y comerciales autorizadas
	Gestión contable	• Elaboración de estados financieros periódicos y por requerimiento • Envío de balance general a SBS • Revisión de pago COSEDE • Administración del plan de cuentas • Contabilización de ajuste de fin de mes (provisiones, garantías, demandas, vinculados) • Contabilización de ajuste (Depreciaciones, amortizaciones) • Revisión y conciliación de cuentas • Conciliación de cuentas bancarias

		• Elaboración de estados financieros periódicos y por requerimientos • Declaración de IVA e Impuesto a la Renta • Declaración de activos en el exterior • Declaración de Impuesto a la Renta en RDEP • Declaración a la salida de divisas • Revisión de archivos de movimientos con y sin maduración • Transferencias recibidas SPI, SPL •
GESTIÓN ADMINISTRATIVA	Administración de activos fijos	• Inventario y codificación de activos fijos • Mantenimiento de activos • Cambios de dependencia de activos • Bajas de activos
	Gestión de adquisiciones y manejo de proveedores	• Calificación de proveedores • Selección de proveedores • Adquisición de bienes y contratación de servicios • Pagos de proveedores • Evaluación de proveedores • Administración fondo de caja chica
	Administración de seguridades físicas	• Administración y control de llaves • Administración y control de seguros institucionales • Administración y control de dispositivos de protección contra incendios
	Gestión de monitoreo y vigilancia	• Monitoreo y vigilancia de oficinas, agencias y sucursales • Control de ingreso y salida de visitantes
	Gestión de servicios generales	• Mantenimiento de oficinas • Administración de servicios básicos • Envío de correspondencia • Administración de proveeduría • Recepción y distribución de correspondencia
GESTIÓN DE ASESORÍA JURÍDICA	Gestión contractual	• Constitución de garantías prendarias de propiedad del cliente o de terceros • Constitución de garantías prendarias a adquirir • Constitución de garantías hipotecarias de propiedad del cliente o de terceros • Constitución de garantías hipotecarias a adquirir • Asesoría legal y defensa de tramites del banco • Atención al cliente interno y externo • Titularización de cartera • Asesoría jurídica de todas las áreas del banco a nivel nacional • Elaboración y actualización de contratos • Revisión de contratos con proveedores del banco • Revisión de documentación legal • Elaboración de minutas y escrituras de poderes especiales, declaraciones, compraventa, constitución de hipotecas y cancelaciones de las mismas • Elaboración de informes legales de personas

		jurídicas • Legalización de contratos de prenda y reserva de dominio, ante autoridades competentes • Tramite y legalización de cambios de garantías • Revisión de operaciones para su procesamiento • Obtención de documentos en los diferentes organismos estatales • Elaboración de documentación crediticia y contratos para operaciones Factoring • Revisión y elaboración de informes acerca de la cartera adquirida por el banco • Elaboración de informes legales para apertura de cuentas • Revisión de documentación crediticia para desembolso • Revisión de facturas y documentos comerciales para inicio de relación crediticia
	Gestión judicial	• Atención de reclamos presentados ante la unidad de reclamos • Representación en trámites judiciales • Registro de marcas y patentes
GESTIÓN DE AUDITORÍA	Auditoría interna	• Elaboración de plan anual de auditoria interna • Planificación de auditorías internas (financiera, operativa, administrativa, informática, etc.) • Ejecución de auditorías internas y emisión de resultados • Seguimiento al cumplimiento de observaciones de auditorías internas, externas y organismos de control • Realización de exámenes especiales de auditoria • Elaboración de informes para organismos de control externo e interno • Coordinación y revisión de resultados de auditorías externas
	Gestión de control interno	• Elaboración y ejecución del programa de control interno • Asesoría en temas relacionados con el control interno
GESTIÓN DE PROCESOS	Gestión documental	• Manejo de documentación administrativa • Control de documentación administrativa
	Mejora continua de procesos	• Actualización del inventario de procesos • Definición y mejoramiento de procesos • Creación y actualización de instructivos, formatos, documentos externos y de referencia • Difusión y comunicación de procesos • Control generación de resultados de indicadores de gestión de procesos • Implementación de mejoras a procesos
GESTIÓN DE COBRANZAS	Gestión preventiva	• Elaboración, seguimiento control de campaña de cobranza vía call center

		• Elaboración, seguimiento y control de campaña de cobranza vía sms • Avisos de vencimiento y seguimiento de créditos • Novación de crédito
GESTIÓN DE OPERACIONES	Operaciones integrales del Back Office	• Cámara preliminar, enviada, recibida • Cámara definitiva, enviada, recibida • Afectación cuentas y entrega de cheques devueltos • Cheques protestados • Legalización de documentos • Levantamiento de garantías • Entrega de documentos legales por demanda • Ingreso, cuadre y mantenimiento de garantías • Control y custodia de documentos de productos del activo • Control y custodia de documentos de productos del pasivo • Endoso de seguro • Pre cancelación de crédito • Liquidación Factoring • Liquidación de compra/venta de cartera • Captura de firmas • Administración y conciliación seguros y dispositivos • Cambio de garantías • Levantamiento de garantías • Emisión y entrega de estados de cuenta • Transportación de valores • Seguimiento y control de cuentas inhabilitadas • Cuentas inmovilizadas • Elaboración y envío de las estructuras entes de control • Seguimiento y control de cajas servipagos • Cuentas inactivas
	Operaciones Front Office	• Activación de cuentas inactivas • Apertura, cuadre y cierre de bóveda • Incremento de efectivo en bóveda • Apertura, cuadre y cierre de caja • Transferencias enviadas SPI, SPL • Arqueo de cajas • Emisión y entrega de tarjetas de debito • Emisión, reposición y entrega de libretas de ahorro • Actualización de libretas de ahorro • Actualización y captura de firmas • Arqueo de bóveda • Certificación de cheques • Depósitos en cuentas corrientes y cuentas de ahorro • Detección de billetes falsos e informe ente de control • Control de formas numeradas • Control límite de efectivo en caja • Control límite de efectivo en bóveda/oficina

		• Pago de cheques y efectivo en caja • Pagos varios en caja • Recaudos en caja/punto matico • Facturación electrónica • Cancelación de tarjeta de débito • Revocatoria, suspensión y anulación de cheques • Bloqueo de tarjeta de debito • Renovación de tarjeta de debito • Emisión y entrega de chequera • Emisión de certificado bancario • Emisión y entrega de cheques de gerencia • Anulación de cheques de gerencia • Providencia judicial • Afiliación de cash Management

Adaptado de investigación de campo

Una vez determinados los procesos de la institución, así como los subprocesos que los soportan se procede a la determinación de los procesos críticos. Para determinar la criticidad de los procesos primeramente se determinan 5 aspectos fundamentales que pueden influir en el nivel de criticidad de un proceso. En este caso se toman como elementos determinantes los siguientes (Banco Capital , 2015):

- Proceso de cara al cliente: el proceso cumple actividades que atienden directamente a los clientes que se encuentran en las oficinas de la institución.

- Proceso de producto específico: el proceso atiende actividades propias de productos específicos de la institución que se entregan a los clientes y que forman parte del portafolio de productos y servicios.

- Proceso con volumen monetario significativo: el proceso mueve volúmenes monetarios significativos, sean de los clientes o fondos propios de la institución. Se considera significativo cuando los montos son superiores a 50000 USD diarios en el acumulado transaccional.

- Proceso para cumplimiento regulatorio: el proceso elabora el reporte que se remite a los organismos de control para atender requerimientos

puntuales cuyo incumplimiento provocaría la violación de regulaciones, estatutos y leyes dando lugar a una sanción o amonestación.

- Proceso con alta transaccionalidad: El proceso atiende un alto volumen de transacciones del negocio de la institución, procesadas por o para el cliente. Las transacciones ejecutan acciones puntuales inmediatas y son repetitivas, su interrupción provoca pérdida de clientes, pérdida de competitividad, pérdida de confianza y exposición indeseada a medios. Se considera alta transaccionalidad cuando supera las 50 transacciones diarias.

Una vez establecidos los criterios de criticidad se procede al diseño de una herramienta que brinda la capacidad de tabular cuantitativamente la opinión de todos los jefes de área y responsables de procesos, quienes han brindado la colaboración necesaria para realizar la actividad. A cada jefe de área y responsable se le ha entregado una tabla que detalla cada subproceso y los aspectos de criticidad a evaluar, para que sea colocada una calificación que puede estar entre el 1 y el 5, donde 1 significa que el subproceso no está altamente identificado con ese elemento de criticidad y donde 5 significa que existe una alta concordancia entre el subproceso y el elemento determinado. Los criterios que se utilizarán para la calificación de los procesos serán considerados como: Muy Alta (5), Alta (4), Media (3), Baja (2) y Muy Baja (1). A continuación, se muestra el formato de tabla diseñado.

Tabla 4.

Modelo para la determinación de los procesos críticos

Macroproceso	Proceso	Subproceso	Responsable	Tipo de cliente	Proceso de cara al Cliente	Proceso de producto especifico	Proceso con volumen monetario significativo	Proceso para cumplimiento regulatorio	Proceso con alta transaccionalidad
					Calificación	Calificación	Calificación	Calificación	Calificación

Adaptado de (Banco Capital , 2015)

Una vez diseñada la herramienta fue entregada a cada jefe de área y responsable de proceso, conteniendo en cada caso los procesos respectivos a cada área, de manera que las observaciones de cada elemento y las opiniones obtenidas sean dadas por los expertos del área en cada caso.

Una vez que se aplica el cuestionario a cada individuo participante, se realiza entonces una tabla resumen con la tabulación general de los resultados, determinando la calificación promedio entre todos los participantes. Así entonces se realiza la sumatoria de las calificaciones otorgadas a cada subproceso y se determina la criticidad de los mismos a partir de la siguiente escala:

Tabla 5.

Escala de clasificación de procesos críticos

Calificación	Clasificación	Significado
Entre 20 y 25	**Crítico**	• Sus funciones no pueden ser ejecutadas a menos que sean reemplazadas por recursos idénticos. • No pueden reemplazarse por métodos manuales. • El costo de interrupción es muy alto. • Muy baja tolerancia a interrupciones.
Entre 16 y 19	**Vital**	• Sus funciones pueden ser ejecutadas manualmente durante un período corto de tiempo. • Costo de interrupción un poco más bajos, solo si son restaurados dentro de un tiempo determinado (5 o menos días). • Mayor tolerancia a las interrupciones.
Entre 5 y 15	**Deseable**	• Sus funciones pueden ser ejecutadas manualmente durante un período relativamente largo. • El proceso manual no requiere de personal adicional, los costos de interrupción son bajos.

Adaptado de (Banco Capital , 2015)

De esta manera se tabulan las calificaciones otorgadas por los participantes, obteniéndose los resultados para determinar una calificación.

Posteriormente se procede con el análisis de los 45 procesos del Banco ABC, los cuales se encuentran distribuidos en 295 subprocesos, determinándose como procesos críticos los detallados a continuación:

Gestión de Negocio

✓ Gestión de Captaciones

- Apertura de inversiones a plazo
- Renovación de inversiones a plazo
- Cancelación Pre cancelación de inversiones a plazo

✓ Gestión de Colocaciones

- Concesión crédito canal automotriz
- Concesión crédito canal banca
- Aprobación de créditos

Gestión de Operaciones

✓ Operaciones integrales Back Office

- Cámara preliminar, enviada, recibida
- Cámara definitiva, enviada, recibida
- Seguimiento y control cajas servipagos

✓ Operaciones Front Office

- Apertura, cuadre y cierre de bóveda
- Incremento de efectivo en bóveda
- Apertura, cuadre y cierre de caja
- Transferencias enviadas SPI, SPL
- Emisión y entrega de tarjetas de débito
- Depósitos en cuentas corrientes y cuentas de ahorro
- Pago de cheques y efectivo en caja
- Pagos varios en caja

Al determinarse los procesos críticos, se definen también los recursos que son necesarios para su ejecución. Para ello se identifican los elementos para el análisis.

Tabla 6.

Recursos de soporte a los procesos críticos

Recurso	Descripción
Recursos de Tecnologías de la Información	
Aplicaciones	Son todos aquellos módulos o funciones específicas de las aplicaciones propias o adquiridas que son utilizadas para la ejecución del proceso.
Herramientas de oficina	Conjunto de programas de software que sirven para realizar tareas específicas ya sea de redacción de documentos, análisis y cálculos de datos contables (Word, Excel, etc.).
Servicios de telefonía	Uso de teléfonos en actividades del proceso, ya sean llamadas a proveedores u otra gestión correspondiente.
Correo electrónico	Medio de comunicación requerido por los intervinientes en el proceso.
Internet	Actividades realizadas a través de la web como parte de la ejecución del proceso.
Otros equipos de oficina	Son aquellos dispositivos tecnológicos que se emplean en la ejecución del proceso.
Otros recursos	
Recursos Humanos	Es el personal crítico sin el cual no podría operar el proceso y su correspondiente respaldo.
Relación con proveedores	Es cualquier acuerdo legal u obligaciones que se tengan establecidas con terceros relacionados con el proceso.
Recursos de soporte	Son todos aquellos manuales y procedimientos de usuario que se emplean para la capacitación del personal involucrado en la ejecución de los procesos.
Recursos de papelería y material de oficina	Es toda aquella documentación como papelería pre-impresa, documentos numerados, documentos valorados, sellos especiales que se utilizan en el proceso.

Adaptado de (Banco Capital , 2015)

A partir de los elementos anteriores se realiza la determinación de los recursos necesarios en cada proceso.

Una vez identificados los procesos críticos de la institución, así como los recursos que soportan los mismos, se procede con la determinación del Tiempo de Recuperación Objetivo (RTO) y Punto de Recuperación Objetivo (RPO) para cada uno de ellos.

El Tiempo de Recuperación Objetivo (RTO) establece la urgencia que las diferentes unidades de negocio precisan para volver a su funcionamiento habitual. Por tanto, determina los plazos en los que deben volver a funcionar con normalidad. Estos pueden establecerse en períodos de tiempo en función de la criticidad de los procesos y pueden ser cuestión de horas o semanas en aquellos procesos prescindibles. Por tanto, se trata de identificar el orden en que hay que tratar de reconstruir la actividad, recuperando antes, aquellos procesos cuya paralización suponen un mayor impacto para la organización. En una situación de crisis siempre hay recursos limitados y es necesario elegir qué hacer primero atendiendo a un criterio de negocio.

El Punto de Recuperación de la Información (RPO) se refiere al punto más reciente en el tiempo en el que los sistemas pueden ser recuperados, reflejando por tanto la cantidad de información que una organización puede permitirse perder sin que le afecte negativamente. Por tanto, el RPO determina la periodicidad con la que deben salvaguardar los datos para los procesos de negocio.

Es importante definir el RPO anticipadamente y asegurarse que los procesos de recuperación consideran estos tiempos requeridos. Una mala definición de RPO producirá impactos operacionales, económicos y financieros.

A través de reuniones con los responsables de los procesos y Gerentes de las áreas, se determinan los tiempos máximos que los procesos críticos podrían permanecer interrumpidos por la pérdida del servicio informático u otros motivos sin afectar significativamente al negocio, así como el tiempo máximo en que debe haberse obtenido el último respaldo para cada proceso crítico obteniéndose los siguientes resultados, los cuales se determinaron a partir de la evaluación que se muestra en las tablas:

Tabla 7.

Matriz de RTO y RPO del proceso crítico Gestión de Captaciones

Proceso	Subproceso	Responsable/ Dueño del Proceso	Tiempo Máximo de Recuperación (RTO)	Tiempo Máximo de Obtención de Respaldos (RPO)
GESTIÓN DE CAPTACIONES	APERTURA DE INVERSIONES A PLAZO	GERENTE BANCA PRIVADA	4 horas	4 horas
	RENOVACION DE INVERSIONES A PLAZO	GERENTE BANCA PRIVADA	4 horas	4 horas
	CANCELACION - PRECANCELACION INVERSIONES A PLAZO	GERENTE BANCA PRIVADA	4 horas	4 horas

Adaptado de (Banco Capital , 2015)

Tabla 8.

Matriz de RTO y RPO del proceso crítico Gestión de Colocaciones

Proceso	Subproceso	Responsable/ Dueño del Proceso	Tiempo Máximo de Recuperación (RTO)	Tiempo Máximo de Obtención de Respaldos (RPO)
GESTIÓN DE COLOCACIONES	CONCESION CRÉDITO CANAL AUTIOMOTRIZ	SUBGERENTE DE NEGOCIOS	48 horas	24 horas
	CONCESION CRÉDITO CANAL BANCA	SUBGERENTE DE NEGOCIOS	48 horas	24 horas
	APROBACIÓN DE CRÉDITOS	JEFE DE RIESGOS	24 horas	24 horas

Adaptado de (Banco Capital , 2015)

Tabla 9.

Matriz de RTO y RPO del proceso crítico Operaciones Integrales del Back Office

Proceso	Subproceso	Responsable/ Dueño del Proceso	Tiempo Máximo de Recuperación (RTO)	Tiempo Máximo de Obtención de Respaldos (RPO)
OPERACIONES INTEGRALES DEL BACK OFFICE	CAMARA PRELIMINAR, ENVIADA, RECIBIDA	GERENTE DE OPERACIONES	4 horas	8 horas
	CAMARA DEFINITIVA, ENVIADA, RECIBIDA	GERENTE DE OPERACIONES	1 hora	1 hora
	SEGUMIENTO Y CONTROL CAJAS SERVIPAGOS	GERENTE DE OPERACIONES	8 horas	8 horas

Adaptado de (Banco Capital , 2015)

Tabla 10.

Matriz de RTO y RPO del proceso crítico Operaciones Integrales del Front Office

Proceso	Subproceso	Responsable/ Dueño del Proceso	Tiempo Máximo de Recuperación (RTO)	Tiempo Máximo de Obtención de Respaldos (RPO)
OPERACIONES FRONT OFFICE	APERTURA, CUADRE Y CIERRE DE BOVEDA	GERENTE DE OPERACIONES	4 horas	4 horas
	INCREMENTO DE EFECTIVO EN BOVEDA	GERENTE DE OPERACIONES	24 horas	24 horas
	APERTURA, CUADRE Y CIERRE DE CAJAS	GERENTE DE OPERACIONES	1 hora	4 horas
	TRANSFERENCIAS ENVIADAS SPI, SPL	GERENTE DE OPERACIONES	24 horas	24 horas
	EMSION Y ENTREGA DE TARJETAS DE DEBITO	GERENTE DE OPERACIONES	24 horas	24 horas
	DEPOSITOS CTAS CTES Y CUENTAS DE AHORRO	GERENTE DE OPERACIONES	4 horas	4 horas
	PAGO DE CHEQUES Y EFECTIVO EN CAJA	GERENTE DE OPERACIONES	4 horas	4 horas
	PAGOS VARIOS EN CAJA	GERENTE DE OPERACIONES	24 horas	24 horas

Adaptado de (Banco Capital , 2015)

4.1.3. Análisis de impacto en el negocio

En el presente epígrafe se procede a analizar el impacto que los procesos identificados pueden provocar en el negocio. El Análisis de Impacto en el Negocio (BIA) permite identificar, cuantificar y cualificar los impactos en el negocio a causa de una pérdida, interrupción o ruptura de los procesos críticos del negocio y proveer la información necesaria para determinar las estrategias apropiadas para la continuidad.

El alcance determinado para el Análisis de Impacto en el Negocio (BIA) se concentra en los procesos que soportan los productos y servicios claves identificando aquellos cuya interrupción puede amenazar más rápidamente la entrega a los clientes. Estos procesos involucran actividades operacionales, las cuales interactúan directamente con clientes u otros fuera de la organización. Sin embargo, estas actividades pueden depender del soporte de otros procesos internos y externos, productivos, gobernantes o de apoyo, que también son considerados (Banco Capital, 2015).

Para la determinación del impacto, en cada una de las actividades, se califican los impactos de interrupción de una manera objetiva y acorde a la realidad institucional, del entorno social y financiero.

El BIA provee datos confiables sobre los potenciales impactos y costos de los desastres, y establecer las bases para determinar las prioridades de recuperación y la selección de apropiadas estrategias de recuperación.

El impacto operacional involucra el impacto no monetario, incluyendo cómo sería impactada la organización por la interrupción de la imagen, el servicio al cliente, la gente, los procesos, la tecnología de información.

El impacto económico / financiero involucra el impacto monetario, es decir cómo afectaría la interrupción del negocio a los ingresos de la institución.

Para el análisis del impacto se enfoca la influencia hacia las áreas que mayor repercusión van a tener en la consecución de las actividades. En este caso se definen:

- Necesidades de clientes/Servicio al cliente
- Requerimientos legales/Incremento en las responsabilidades legales
- Imagen en el medio-Reputación
- Relación con los proveedores
- Clientes internos
- Financiera

Del análisis de la información contenida en las tablas de definición del impacto operacional y financiero de la Tabla 9, se puede decir que operacionalmente el proceso operativo de Back Office refleja un elevado impacto negativo en el negocio a partir de las 8 horas de inoperatividad, incidiendo en todas las áreas definidas, excepto clientes internos.

En el caso del proceso de Front Office existen algunos de los subprocesos que comienzan a influir negativamente en el negocio a partir de las 4 horas de inoperatividad, fundamentalmente en las áreas de necesidades de clientes/Servicio al cliente, imagen en el medio-Reputación y clientes internos.

El proceso de captaciones tiene un impacto operacional elevado generalmente a partir de las 8 horas de inoperatividad, excepto en el área de Relaciones con los proveedores. Sin embargo, su subproceso de cancelación y pre cancelación de inversiones a plazo, desde apenas menos de las 4 horas de inoperatividad ya comienza a influir negativamente en la mayoría de las áreas señaladas.

El proceso de colocaciones a partir de las 48 horas de no operar es que comienza a tener un elevado impacto en la mayoría de las áreas, exceptuando los Requerimientos legales/Incremento en las responsabilidades legales y la relación con los proveedores.

4.1.4. Análisis de riesgo

En el presente epígrafe se procede a la identificación de los riesgos tecnológicos que pueden amenazar la correcta ejecución de los procesos del negocio y que pueden provocar grandes daños en el mantenimiento del servicio. A continuación, se listan las amenazas tecnológicas que ponen en riesgo la eficiente operatividad y que fueron obtenidas por los criterios emitidos por los especialistas del Banco ABC y por los detalles que se observan en sus procedimientos de evaluación de riesgos para la continuidad del negocio, también se seleccionaron mediante la observación de los procesos tecnológicos que allí se desarrollan, detectando todo lo que pudiese afectar a la red, a los software y a los sistemas eléctricos de forma general, el listado que se muestra a continuación se realizó de conjunto con los especialistas del centro, tomando como referencia a:.

- Instalación de dispositivos USB no autorizados en la red interna
- Robo de identidad utilizando simuladores de sitios Web, mensaje de correo o actos de ingeniería social
- Acceso no autorizado a la red del banco para obtener y/alterar información sensible
- Utilización de herramientas o Software no licenciado o no autorizado (Software pirata)

- Interrupción o fluctuaciones del suministro eléctrico
- Daños en los ascensores
- Daños o fallas en el sistema de climatización
- Daño o falla en central telefónica
- Daño o falla en componentes de telecomunicaciones (switch o routers)
- Daño o falla en el banco de transformadores del edificio matriz
- Daño o falla en los discos donde reside la base de datos de producción
- Daño o falla en los generadores y sus componentes, del edificio matriz
- Daño o falla en UPS
- Daños severos en los servidores críticos
- Errores en la configuración de hardware de misión critica
- Fallas o daños en los equipos del sistema de distribución eléctrica interna
- Caída del sistema por agotamiento de recursos (memoria, capacidad de almacenamiento, canales de comunicación, etc.)
- Pérdida o falla en el almacenamiento de datos (Ramirez & Ortiz, 2011)

Para cada una de las amenazas se ha identificado los controles y seguridades implementadas en la institución para disminuir la probabilidad de que se materialicen las amenazas o reducir el impacto en caso de presentarse ver Anexo 11.

Una vez que se ha efectuado la evaluación de los controles implementados por la institución se ha determinado las vulnerabilidades que tiene el Banco ABC, frente a las amenazas identificadas. Para el análisis se procede con la definición de escenarios de indisponibilidad e interrupción de operaciones. Para lo cual, se realizó la determinación de daños que podrían ocasionar las amenazas aprovechando las vulnerabilidades desde el punto de vista de la disponibilidad y efecto que provocaría en la atención a los clientes del Banco. Así mismo se define el nivel de riesgo para cada amenaza.

Para la definición del nivel de riesgo se ha considerado la siguiente matriz de calificación de riesgos:

Tabla 11.

Matriz de calificación del nivel de riesgo

		IMPACTO				
		1 Bajo	2 Medio Bajo	3 Medio	4 Medio Alto	5 Alto
PROBABILIDAD	5 Alta	Alto	Alto	Muy Alto	Muy Alto	Muy Alto
	4 Media Alta	Medio	Alto	Alto	Muy Alto	Muy Alto
	3 Media	Bajo	Medio	Alto	Muy Alto	Muy Alto
	2 Media Baja	Bajo	Bajo	Medio	Alto	Muy Alto
	1 Baja	Bajo	Bajo	Medio	Alto	Alto

Adaptado de (Ramirez & Ortiz, 2011)

La probabilidad de ocurrencia de la amenaza y el nivel de impacto en la organización, se califica teniendo en cuenta la Tabla 12 y Tabla 13 respectivamente.

Tabla 12.

Guía de calificación para la probabilidad de ocurrencia de las amenazas

Probabilidad de Ocurrencia	Calificación	Criterio	Especificación
Baja	1	Improbable	La situación se presenta 1 vez en 30 años
Media Baja	2	Raramente	La situación se presenta 1 vez en 10 años
Media	3	Moderada	La situación se presenta 1 vez en 5 años
Media Alta	4	Frecuente	La situación se presenta 1 vez en 3 años
Alta	5	Siempre	La situación se presenta 1 vez o más en el año.

Tabla 13.

Guía de calificación para determinar el nivel del impacto

Impacto	Calificación	Criterio
Baja	1	Molesta
Media Baja	2	Controlable
Media	3	Moderado
Media Alta	4	Crítico/Desastroso
Alta	5	Terminal

A partir de las tablas anteriores se procede a realizar la calificación de cada una de las amenazas y finalmente definir el nivel de riesgo que representa cada una de ellas para la institución. La información detallada se muestra en la tabla titulada: Matriz de calificación de riesgo.

Con la evaluación de los riesgos se puede calificar las amenazas determinadas, según las vulnerabilidades, el nivel de impacto ver Anexo 6 y la probabilidad de ocurrencia de las mismas, cuentan con un nivel de riesgo Alta, Media Alta, Media, Media Baja, Baja como se puede apreciar en el Anexo 2. Por este motivo se puede decir, de manera general, que el nivel de riesgo en la institución se puede calificar acorde a está guía.

4.2. Proyección del BCP

Una vez que se conocen las características y comportamientos de la organización, se puede emprender el direccionamiento del plan, teniendo en cuenta las amenazas que afectan a la misma y los objetivos fundamentales que se buscan con la creación del mismo. Es por ello que en este cápitulo se procede a la declaración del plan con los fundamentos básicos que lo sustentan.

La ocurrencia de algún incidente en la institución trae como consecuencia problemas financieros, además de daños intangibles como disminución de la productividad, estrés, recursos desviados, y todo ello genera una mala imagen de la empresa. Además conlleva una mala reputación de la institución, el nombre de los ejecutivos responsables es lo que se pone en juego. No hay que

olvidar que las instituciones que sufren este tipo de incidentes son la noticia al día siguiente, la prensa es la responsable de señalar con nombres y apellidos a los responsables. Además, por si fuera poco, los directores corporativos pueden ser demandados por las consecuencias de interrupción del negocio.

El Banco ABC con una posición importante y creciente en el sistema financiero ecuatoriano, requiere dentro del alcance de sus proyectos de mejoramiento continuo, implementar las mejores prácticas que le permitan mantener el mejor posicionamiento en su sector de negocios, implementando nuevos controles y mecanismos para su administración centralizada, además convirtiendo a la Institución en una empresa más segura.

De acuerdo a estos antecedentes, es objetivo del Banco ABC, establecer el Plan de Continuidad del Negocio (BCP), de modo que la Institución pueda, gradualmente hacia el futuro, mejorar las condiciones y la capacidad de recuperación de la operatividad de los procesos del negocio ante un eventual desastre que afecte a la continuidad del mismo.

El Plan de Continuidad del Negocio (BCP) es un proceso de dirección que identifica los impactos potenciales que amenazan a la organización y proporciona el marco adecuado para desarrollar la capacidad de dar una respuesta efectiva, que permita proteger los intereses, imagen y valor de las actividades realizadas por la misma (Sáez, 2011).

4.2.1. Alcance

El alcance del BCP del Banco ABC está orientado al uso práctico de todos los colaboradores directos, temporales, pasantes, proveedores de servicios, etc.; así como cualquier tercero que tuviere acceso directa o indirectamente a información de Banco ABC en cualquiera de sus oficinas, en caso de ocurrencia de un evento de desastre u otro que conllevara a la paralización del servicio.

4.2.2. Política

Establecer las capacidades de actuación y de respuesta rápida que sean necesarias para garantiza la seguridad de los intereses de los clientes y colaboradores de la institución, durante la ocurrencia de una situación de emergencia que provoque la inoperatividad de los procesos críticos y el colapso del servicio, minimizando los tiempos de afectación y los daños colaterales, de modo que no se vea deteriorado el prestigio de la organización ante el mercado, ni su imagen corporativa.

4.2.3. Requisitos

- Concienciación de todo el personal involucrado en los procesos y servicios, de las posibles amenazas que pueden afectar a la institución.
- Conocimiento de las bases y fundamentos de los procedimientos de actuación ante posibles casos de emergencia, a través de la capacitación periódica.
- Disponibilidad de los recursos que sean necesarios para llevar a cabo los procedimientos de respuesta rápida ante la ocurrencia de posibles incidentes desfavorables.
- Alineación entre los intereses de los colaboradores, que soportan los procesos y consecuentemente la organización, con los intereses propios de ésta, de modo que cada uno se sienta identificado con el deseo de sobreponerse a las dificultades, haciendo un basamento práctico en su sentido de pertenencia.

4.2.4. Principios

Proteger los procesos críticos del negocio, contra desastres o fallas mayores, junto con las posibles consecuencias que se puedan tener, como pérdidas de tipo financiero, credibilidad, productividad, etc. debido a la no disponibilidad de los recursos de la organización.

Mitigar el riesgo a las fallas o desastres inminentes, mediante un plan que permita la pronta recuperación de la operación, en caso de presentarse algún evento que afecte el flujo normal de las actividades de la institución.

Satisfacción permanente del cliente, mediante la actuación preventiva y la determinación oportuna de los canales de operación alternativa ante vulnerabilidades existentes y la ocurrencia de eventos desfavorables.

4.2.5. Objetivos

- Garantizar una respuesta rápida ante incidentes que pueden poner en riesgo la operación de la organización.
- Brindar seguridad a los empleados, proteger tanto los activos de la organización como sus procesos y la tecnología que los soporta.
- Minimizar el tiempo de interrupción provocado y asegurar una prestigiosa imagen de la organización ante el mercado.

4.2.6. Estrategias de mitigación

Basado en los datos obtenidos en los acápites anteriores, se procede a la determinación de las estrategias de recuperación tecnológica que de manera general satisfacen las necesidades de mitigación de los riesgos.

Tabla 14.

Estrategias de recuperación tecnológica

Estrategia de Recuperación Tecnológica	Descripción
Sitio Alterno Espejo o Duplicado (Mirrored Site)	Centro de Datos Alterno que está equipado y operando exactamente igual al principal. Todos los servidores y dispositivos de comunicación están funcionando. Los datos se replican en tiempo real. Dispone de personal de operación propio.
Sitio Alterno Equipado (Hot Site)	Centro de datos alterno que cuenta con todos los equipos de computación y de comunicación necesarios para operar en contingencia. No dispone de personal de operación como en el sitio principal. Puede requerir la instalación de algún componente menor de hardware o software previo a su funcionamiento. Generalmente no está prendido ni funcionando, o mantener las aplicaciones en modo "*stand by*. En algunos casos se lo utiliza para replicar datos, obtener respaldos o para ciertos procesos menores de la operación normal del negocio.
Sitio Alterno Semi- Equipado (Warm Site)	Sitio que cuenta con algunos servidores y equipos de computación así como algunos dispositivos de comunicaciones. Con lo que tiene no podría entrar en funcionamiento. Cuenta con instalaciones eléctricas y telefónicas. Generalmente no dispone de los servidores principales ni todos los dispositivos de comunicación necesarios para la operación.
Sitio Alterno sin Equipamiento (Cold Site)	Espacio físico vacío que sólo tienen instalaciones básicas eléctricas, telefónicas, ambientales y en algunos casos de comunicaciones. No dispone de ningún equipamiento de IT.
Sitio Alterno Contratado con Proveedor	Puede ir desde un sitio completamente equipado hasta un sitio sin equipos con sólo las facilidades eléctricas, telefónicas y de comunicación. Se acuerda con el proveedor las características del sitio alterno.

Adaptado de (Banco Capital , 2015)

Los tiempos de recuperación estimados para cada una de las estrategias, definidas por las mejores prácticas, son los siguientes:

Tabla 15.

Tiempos de recuperación estimado de las estrategias de recuperación tecnológica

Estrategia de Recuperación Tecnológica	Tiempo de Recuperación Estimada
Sitio Alterno Espejo o Duplicado (Mirrored Site)	5 minutos en condiciones favorables. Hasta 1 hora máximo.
Sitio Alterno Equipado (Hot Site)	16 horas en condiciones favorables. Hasta 48 horas máximo
Sitio Alterno Semi- Equipado (Warm Site)	1 semana en condiciones favorables. Hasta 4 semanas máximo
Sitio Alterno sin Equipamiento (Cold Site)	1 mes en condiciones favorables. Hasta 3 meses máximo.
Sitio Alterno Contratado con Proveedor	De pocos minutos a varios días. Depende de los términos contratados con el proveedor.

Adaptado de (Banco Capital , 2015)

Los procesos críticos de Banco ABC y los tiempos máximos de interrupción que pueden soportar estos procesos sin afectar seriamente la operación, rentabilidad e imagen de la institución, definidos anteriormente, se presentan a continuación junto con la estrategia de recuperación que mejor responde a las exigencias de disponibilidad del servicio informático de cada proceso. Se debe tomar muy en cuenta que los procesos críticos con menor tiempo de interrupción (RTO) son los que definen la estrategia de recuperación que debe ser seleccionada en cada caso, cuando están involucrados los mismos servidores o aplicaciones, como es el caso de Banco ABC con la aplicación Core Globus T24.

Tabla 16.

Propuesta de estrategias al proceso crítico de Gestión de Captaciones

Proceso	Subproceso	Responsable/ Dueño del Proceso	Tiempo Máximo de Recuperación (RTO)	Estrategia Requerida
GESTIÓN DE CAPTACIONES	APERTURA DE INVERSIONES A PLAZO	GERENTE BANCA PRIVADA	4 horas	Sitio Alterno Espejo o Duplicado (Mirrored Site)
	RENOVACION DE INVERSIONES A PLAZO	GERENTE BANCA PRIVADA	4 horas	Sitio Alterno Espejo o Duplicado (Mirrored Site)
	CANCELACION - PRECANCELACION INVERSIONES A PLAZO	GERENTE BANCA PRIVADA	4 horas	Sitio Alterno Espejo o Duplicado (Mirrored Site)

Adaptado de (Banco Capital , 2015)

Tabla 17.

Propuesta de estrategias al proceso crítico de Gestión de Colocaciones

Proceso	Subproceso	Responsable/ Dueño del Proceso	Tiempo Máximo de Recuperación (RTO)	Estrategia Requerida
GESTIÓN DE COLOCACIONES	CONCESION CRÉDITO CANAL AUTIOMOTRIZ	JEFE DE RIESGOS	48 horas	Sitio Alterno Equipado (Hot Site)
	CONCESION CRÉDITO CANAL BANCA	JEFE DE RIESGOS	48 horas	Sitio Alterno Equipado (Hot Site)
	APROBACIÓN DE CRÉDITOS	JEFE DE RIESGOS	24 horas	Sitio Alterno Equipado (Hot Site)

Adaptado de (Banco Capital , 2015)

Tabla 18.

Propuesta de estrategias al proceso crítico de Operaciones Integrales del Back Office

Proceso	Subproceso	Responsable/ Dueño del Proceso	Tiempo Máximo de Recuperación (RTO)	Estrategia Requerida
OPERACIONES INTEGRALES DEL BACK OFFICE	CAMARA PRELIMINAR, ENVIADA, RECIBIDA	GERENTE DE OPERACIONES	4 horas	Sitio Alterno Espejo o Duplicado (Mirrored Site)
	CAMARA DEFINITIVA, ENVIADA, RECIBIDA	GERENTE DE OPERACIONES	1 hora	Sitio Alterno Espejo o Duplicado (Mirrored Site)
	SEGUMIENTO Y CONTROL CAJAS SERVIPAGOS	GERENTE DE OPERACIONES	8 horas	Sitio Alterno Espejo o Duplicado (Mirrored Site)

Adaptado de (Banco Capital , 2015)

Tabla 19.

Propuesta de estrategias al proceso crítico de Operaciones Integrales del Front Office

Proceso	Subproceso	Responsable/ Dueño del Proceso	Tiempo Máximo de Recuperación (RTO)	Estrategia Requerida
OPERACIONES FRONT OFFICE	APERTURA, CUADRE Y CIERRE DE BOVEDA	GERENTE DE OPERACIONES	4 horas	Sitio Alterno Espejo o Duplicado (Mirrored Site)
	INCREMENTO DE EFECTIVO EN BOVEDA	GERENTE DE OPERACIONES	24 horas	Sitio Alterno Equipado (Hot Site)
	APERTURA, CUADRE Y CIERRE DE CAJAS	GERENTE DE OPERACIONES	1 hora	Sitio Alterno Espejo o Duplicado (Mirrored Site)
	TRANSFERENCIAS ENVIADAS SPI, SPL	GERENTE DE OPERACIONES	24 horas	Sitio Alterno Equipado (Hot Site)
	EMSION Y ENTREGA DE TARJETAS DE DEBITO	GERENTE DE OPERACIONES	24 horas	Sitio Alterno Equipado (Hot Site)
	DEPOSITOS CTAS CTES Y CUENTAS DE AHORRO	GERENTE DE OPERACIONES	4 horas	Sitio Alterno Espejo o Duplicado (Mirrored Site)
	PAGO DE CHEQUES Y EFECTIVO EN CAJA	GERENTE DE OPERACIONES	4 horas	Sitio Alterno Espejo o Duplicado (Mirrored Site)
	PAGOS VARIOS EN CAJA	GERENTE DE OPERACIONES	24 horas	Sitio Alterno Equipado (Hot Site)

Adaptado de (Banco Capital , 2015)

Con base en los requerimientos de los tiempos máximos de recuperación (RTO) de los procesos críticos del Banco ABC, se recomienda seleccionar la estrategia de “Sitio Alterno Espejo o Duplicado (Mirrored Site)”, que permita recuperar el sitio alterno y estar listos para operar en un tiempo máximo de 4 horas.

El Banco ABC cuenta con un sitio alterno ubicado en la ciudad de Ibarra. El área de Sistemas se encuentra realizando el análisis para desarrollar las adecuaciones necesarias para que el sitio alterno cuente con los recursos tecnológicos que permitan mantener la operatividad de los procesos críticos del negocio, durante un evento que afecte la continuidad.

El RTO global definido para Banco ABC es de 4 horas, por lo que el data center alterno ubicado en la ciudad de Ibarra debe estar listo para la operación de las oficinas en un tiempo máximo de 4 horas, incluyendo los procesos de apertura y cierre de operaciones en oficinas, en los casos que aplique.

Los principales eventos que podrían afectar la continuidad del negocio y las acciones que deben desarrollarse para la recuperación son:

Tabla 20.

Acciones de recuperación ante eventos de interrupción

Definiciones para la recuperación		
Escenario	**Evento**	**Acción de Recuperación**
Interrupción de la continuidad del negocio a nivel nacional		
Pérdida del servicio informático a nivel nacional	Evento que afecte al edificio matriz del Banco ABC y que ocasione daños en el centro de datos principal.	Levantar el Data Center del sitio alterno ubicado en la ciudad de Ibarra
	Evento que ocasione daños severos en los servidores del sistema Core Bancario T24, de la base de datos o en los nodos principales y secundarios de comunicaciones.	
Interrupción de la continuidad del negocio en forma parcial		
Pérdida de operatividad de una oficina	Evento que ocasione la pérdida de operatividad en alguna de las oficinas del Banco ABC	El personal de los procesos críticos de la oficina afectada debe trasladarse a la oficina más cercana y operar con normalidad.

Así mismo, del análisis de los recursos críticos requeridos por los procesos también críticos, se definen las siguientes acciones para la recuperación operativa:

Tabla 21.

Recursos críticos requeridos

Recursos críticos	Riesgo	Acción para la Recuperación
Personal de Respaldo (backup)	Interrupción de los procedimientos de contingencia operativa por falta de personal crítico del proceso	Designar, entrenar y probar el personal de respaldo
Documentación física de las Carpetas de Crédito, Respaldo del área de Cajas y expedientes de Colocaciones.	Pérdida o deterioro de los expedientes de crédito, colocaciones y respaldos de las transacciones de cajas.	Almacenamiento en un sitio seguro contratado o propio. Digitalización de las carpetas.

4.3. Desarrollo del PCN

Hasta este momento se tienen definidas las características propias de la organización y el contexto en el cual se desarrollan los procesos organizacionales, ambientado también por las amenazas que el propio medio impone. Además se ha definido el propósito y definiciones centrales del plan de continuidad así como el que hacer para mitigar los efectos desencadenantes, sin embargo es hasta ésta fase en la que será definido el cómo deben llevarse a cabo las acciones de restauración y de continuidad de los procesos críticos. Es por ello que en este acápite se definen los procedimientos de trabajo para desarrollar las acciones respectivas a garantizar la continuidad de los procesos y la estabilidad de los servicios ante un evento no deseado.

4.3.1. Definición de procedimientos e impactos

En este acápite se declaran los procedimientos de trabajo para enfrentar la ocurrencia de eventos inesperado y que traen consigo la paralización de los procesos críticos, como herramientas que soportan el plan de continuidad diseñado para direccionar el modo de actuación en cada caso.

Se diseñan los procedimientos de:

- Procedimiento para la declaración de emergencia
- Procedimiento para la difusión y concienciación
- Procedimiento para capacitaciones
- Procedimiento de Recuperación de Desastres
- Procedimientos de Operación de Contingencia Captaciones
- Procedimientos de Operación de Contingencia Colocaciones
- Procedimientos de Operación de Contingencia Back Office
- Procedimientos de Operación de Contingencia Front Office
- Procedimiento de realización de pruebas y evaluación de resultados

A continuación, se realiza un resumen del contenido dispuesto en cada uno de los procedimientos ya que cada uno de ellos constituye un documento anexo al plan de continuidad.

Tabla 22.

Procedimiento de declaración de emergencias

Procedimiento de Declaración de Emergencia	
Objetivo	Comunicar al personal de Banco ABC en general y a los involucrados en los comités relacionados con la continuidad del negocio, los pasos que deben seguir cuando se presenta un incidente en la organización que puede afectar el servicio informático o las operaciones en las oficinas e impactar en la continuidad de los procesos críticos y servicios de la institución.
Alcance	Este procedimiento cubre las actividades que se deben desarrollar desde el momento que se identifica un incidente que puede paralizar las operaciones de la organización hasta el momento en que el Presidente Ejecutivo o el Comité de Administración de la Crisis declaran la emergencia y disponen activar los “Planes de continuidad del negocio y recuperación de desastres”.
Responsable operativo	Responsable del área de Riesgos /Jefe de Riesgo operativo
Lineamientos	Involucrados: Todo el personal de Banco ABC además de directores, proveedores y guardias de seguridad que se encuentren en las instalaciones de la institución o presten servicio para la misma. Eventos de Riesgo: Los eventos de riesgo que pueden ocasionar la interrupción del servicio informático o la operación de las oficinas del Banco ABC.
Responsable	**Actividades**
TODO EL PERSONAL DEL BANCO	Comunicar de inmediato a los organismos de auxilio o socorro, como bomberos, Cruz Roja, Hospitales, etc., en la respectiva ciudad, al identificar la presencia de un incidente que se está presentando o se ha presentado, y que sea de tipo incendio, inundación o similar, etc.
	Notificar de inmediato a uno de los miembros del Equipo de Evaluación del Incidente, en el siguiente orden: 1. Vicepresidenta del Banco ABC 2. Gerente de Tecnología de la Información y Jefe de Producción 3. Jefe de Riesgos Integrales
	Notificar telefónicamente y luego por correo electrónico la presencia de un incidente que tiene riesgo de interrupción del servicio informático o de la oficina.
	La notificación por correo electrónico será siempre al correo personal con copia al correo institucional de las personas notificadas. Bajo ninguna circunstancia, la notificación vía correo electrónico remplazará la llamada telefónica a los miembros del Equipo de Evaluación del Incidente.

EQUIPO DE EVALUACIÓN DEL INCIDENTE	La persona del Equipo de Evaluación del Incidente que recibió la notificación por teléfono y/o correo electrónico, debe cumplir: 1. Se presentará en el sitio del incidente o se comunicará a través de Internet o vía telefónica con el Gerente de Tecnología de la Información en el plazo máximo de 1 hora de recibida la notificación. 2. Comunicará del incidente a los demás miembros del Equipo de Evaluación del Incidente, por teléfono o correo electrónico, para que se trasladen al lugar del incidente o se conecten vía Internet o telefónicamente. 3. Evaluarán el incidente o analizarán el incidente cuando el impacto del mismo no sea totalmente evidente. 4. Determinarán si el incidente ha ocasionado u ocasionará la suspensión del servicio informático o la operación de alguna oficina, para lo cual se utilizará los siguientes niveles de alerta: **Nivel de Alerta 1 (Baja)** Cuando la situación de riesgo está controlada, no se afectan las operaciones del negocio ni el servicio tecnológico. **Nivel de Alerta 2 (Media)** El evento de riesgo impide las operaciones en oficinas puntuales pero no existe una afectación en la continuidad del negocio a nivel nacional. Este evento se comunica a los Gerentes de Negocios y al Gerente de Tecnología de la Información. **Nivel de Alerta 3 (Alta)** El evento de riesgo afecta o afectará el servicio informático o la operación de la oficina impactando en la continuidad del negocio. Si es del caso, se notificará a los organismos de auxilio o socorro. Este evento se comunica a los Gerentes de Negocios y al Gerente de Tecnología de la Información.
EQUIPO DE EVALUACIÓN DEL INCIDENTE	El evento de riesgo afecta o afectará el servicio informático o la operación de la oficina impactando en la continuidad del negocio. Si es del caso, se notificará a los organismos de auxilio o socorro. Este evento se comunica a los Gerentes de Negocios y al Gerente de Tecnología de la Información.
GERENTE DE TECNOLOGÍA DE LA INFORMACIÓN	Por instrucción del Gerente de Tecnología de la Información en los casos de alerta roja y amarilla (niveles 2 y 3), a los 15 minutos de presentado el evento, se activarán los procedimientos de contingencia y se informará al Gerente General y Gerentes de Negocios.
GERENTE GENERAL Y GERENTES DE NEGOCIOS	Determinarán el tiempo estimado que demandará solucionar el problema o daño presentado en un plazo máximo de 2 horas desde que recibieron la primera notificación.
	Si la solución va a tomar más de 3 horas, comunicarán el incidente a uno de los miembros del Comité de Administración de la Crisis sobre la gravedad del incidente, en el orden que se indica más adelante, primero telefónicamente y luego por correo electrónico, a la dirección de correo personal con copia al correo institucional. Posteriormente, esta notificación deberá regularizarse a través de informe escrito.

GERENTE GENERAL Y GERENTES DE NEGOCIOS	Notificará al Comité de Administración de la Crisis en el siguiente orden: 1. Presidente Ejecutivo Banco ABC 2. VP de Banco ABC. 3. Gerente de Banca Privada 4. Subgerente de Negocios 5. Gerente de Tecnología de la Información 6. Jefe de Producción 7. Auditor Interno
COMITÉ DE ADMINISTRACIÓN DE LA CRISIS	El Presidente Ejecutivo del Banco ABC o su delegado, u otro miembro del Comité, en el orden indicado, analizarán la notificación del incidente remitido por el Equipo de Evaluación del Incidente, con especial énfasis en el tiempo que tomará solucionar el problema presentado.
PRESIDENTE EJECUTIVO	Consultará, si considera necesario, con los miembros del Comité de Administración de la Crisis u otros directivos que estime pertinente, antes de declarar o no la emergencia.
EL PRESIDENTE EJECUTIVO O COMITÉ DE ADMINSITRACIÓN DE LA CRISIS	Decidirá la declaración de la emergencia y la activación del sitio alterno ubicado en la ciudad de Ibarra.
	Notificará la decisión de declarar la emergencia y activar el BCP y PRD al equipo gerencial de Banco ABC. A través del medio más efectivo y oportuno.

Adaptado de (Banco Capital , 2015)

Tabla 23.

Procedimiento para la difusión y concienciación

Procedimiento para la difusión y concienciación	
Objetivo	Establecer los lineamientos de difusión, comunicación, entrenamiento y concienciación del Plan de Continuidad del negocio con el propósito de capacitar al personal del Banco ABC para que gestionen de manera adecuada los procesos de la institución en situaciones de crisis o desastres.
Alcance	El alcance del manual es para todo el personal del Banco ABC en todos los niveles.
Responsable operativo	Responsable de Riesgos Integrales/ Jefe de Riesgo Operativo y Oficial de Seguridad de la Información.

Lineamientos	El área de Riesgo Operativo será responsable de promover la concientización de la disciplina de la continuidad del negocio, mediante herramientas de comunicación internas. La concientización debe estar orientada a todo el personal del Banco, a los proveedores de los servicios claves de la Institución y, al personal que ingresa a la Institución. La Difusión de los temas de Continuidad del Negocio al personal del Banco ABC deberá ser coordinada con el área de Talento Humano especialmente los que se realizarán mediante charlas y correos electrónicos. El personal será convocado por el Área de Talento Humano, el mismo que tendrá la obligación de asistir a las charlas y talleres en donde se impartan temas sobre Continuidad del Negocio.
Responsable	**Actividades**
JEFE DE RIESGO OPERATIVO /RESPONSABLE DE RIESGOS INTEGRALES	Identifican la necesidad de difundir y concienciar al personal del Banco ABC. en temas de Continuidad del Negocio.
	Evalúa y selecciona los temas que serán importantes para la Continuidad del Negocio.
	Definen el contenido del tema para efectuar las charlas informativas de la Continuidad del Negocio.
	Escoge el tipo de alternativas para comunicar los temas de la Continuidad del Negocio, entre las cuales pueden ser charlas al personal del Banco, difusión mediante correo electrónico, publicación en intranet en los procedimientos del área de Riesgos Integrales u otras alternativas que se definan entre el Jefe de Riesgo Operativo y Responsable de Riesgos Integrales.
	Elabora las pruebas para la evaluación al personal del Banco mediante las cuales se determinará el entendimiento y asimilación del personal del Banco en temas de Continuidad del Negocio.
	Planifica y coordina con el personal de Talento Humano la exposición de los temas de continuidad y la disposición de los recursos.
JEFE DE TALENTO HUMANO	Realiza la convocatoria de los participantes conforme al programa de Talento Humano.
JEFE DE RIESGO OPERATIVO	En caso de considerar la realización de charlas sobre Continuidad del Negocio, en las fechas establecidas se expondrá sobre: el sistema de Continuidad del Negocio, la importancia de cumplir con las políticas, procedimientos y programas de Continuidad del Negocios, las potenciales consecuencias de no cumplir con los procedimientos operativos de los Planes de Continuidad del Negocio, roles y responsabilidades para cumplir con el sistema de Continuidad, la preparación de respuestas y emergencias y aspectos significativos asociados con las actividades de trabajo, los objetivos y metas del personal clave o alterno.
	Evaluará los conocimientos adquiridos que son de interés del personal, una vez que se ha finalizado la charla.
	Comunica al Responsable de Riesgos Integrales, Comité de Continuidad del Negocio, Comité de Administración Integral de Riesgos y Directorio los resultados de la capacitación y evaluación realizada al personal mediante los Informes mensuales.
	En coordinación con el Responsable de Riesgos publica en intranet la información que consideren necesaria.

ORGANIZACIÓN Y PROCESOS	Comunica vía mail la publicación de información de Continuidad del Negocio al personal del Banco ABC.

Adaptado de (Banco Capital , 2015)

Tabla 24.

Procedimiento para la capacitación

Procedimiento para la capacitación	
Objetivo	Establecer los lineamientos de difusión, comunicación, entrenamiento y concienciación del Plan de Continuidad del negocio con el propósito de capacitar al personal del Banco ABC para que gestionen de manera adecuada los procesos de la institución en situaciones de crisis o desastres.
Alcance	El alcance del manual es para todo el personal del Banco ABC.
Responsable operativo	Responsable de Riesgos Integrales/ Jefe de Riesgo Operativo y Oficial de Seguridad de la Información.
Lineamientos	El área de Riesgo Operativo capacitará al personal responsable de realizar las tareas de recuperación y reanudación, con la finalidad del asegurar al Banco la continuidad de las operaciones. La capacitación al personal del Banco deberá ser orientada a roles y responsabilidades individuales y basadas en pruebas y ejercicios para fortalecer el entrenamiento. La capacitación deberá incluir lineamientos y procedimientos de notificación, evacuación, movilización, puntos de reunión y respuesta a la crisis. Anualmente se realizará la difusión y capacitación para la Continuidad del Negocio y deberá efectuarse un proceso de evaluación, a través de pruebas y su asistencia las mismas que serán obligatorias. Los programas de difusión y capacitación para la Continuidad del Negocio deberán ser aprobados por el Comité de Continuidad del Negocio. Los programas de difusión y comunicación para la Continuidad que se realicen serán conocidos por el Comité de Continuidad del Negocio, Comité de Administración Integral de Riesgos y Directorio del Banco, a través de informes realizados por parte del área de Riesgo Operativo.
Responsable	**Actividades**
JEFE DE RIESGO OPERATIVO OFICIAL DE SEGURIDAD DE LA INFORMACIÓN	Planifica la capacitación de los planes de continuidad al personal clave de los procesos críticos.
	Comunica al área de Talento Humano mediante correo electrónico el programa de capacitación de los planes de Continuidad del Negocio.

JEFE DE TALENTO HUMANO	Recibe por parte del Jefe de Riesgo Operativo el programa de capacitación de los Planes de Continuidad.
	Organiza el día y hora de la capacitación del personal clave previa coordinación con el Jefe inmediato.
JEFE DE RIESGO OPERATIVO	Expone sobre la estructura de la continuidad del negocio, las responsabilidades del personal clave, las actividades críticas y vitales del negocio, los servicios a restablecer, políticas internas y de seguridad, etc.
	Realiza la capacitación al personal clave y al personal alterno de la institución.
	Elabora un informe sobre el cumplimiento de los objetivos de la capacitación de los Planes de Continuidad del Negocio indicando si los conocimientos impartidos a los participantes fueron asimilados
	La evaluación de los conocimientos impartidos debe contemplar el conocimiento y destrezas del personal clave y cumplimiento de las labores encomendadas en los procedimientos de los planes de Continuidad del Negocio.
	Envía al Responsable de Riesgos Integrales el Informe con el resultado de la capacitación.
RESPONSABLE DE RIESGO INTEGRALES	Analiza los resultados de la capacitación de los Planes de Continuidad del Negocio y el cumplimiento de los objetivos planteados.
JEFE DE RIESGO OPERATIVO / OFICIAL DE SEGURIDAD DE LA INFORMACIÓN	En caso de no cumplir con los objetivos planteados en la capacitación de los Planes de Continuidad del Negocio planifica con Jefe de Talento Humano una nueva capacitación con el personal clave o alterno previa coordinación con el Jefe Inmediato.
JEFE DE RIESGO OPERATIVO	Emite un Informe Final del cumplimiento de los objetivos de la capacitación de los Planes de Continuidad del Negocio y envía al Responsable de Riesgos para su análisis.
RESPONSABLE RIESGOS INTEGRALES	Analiza los resultados de la capacitación de los Planes de Continuidad del Negocio y el cumplimiento de los objetivos planteados.
JEFE DE RIESGO OPEATIVO	Pone en conocimiento del Presidente Ejecutivo, Miembros del Comité de Continuidad del Negocio, Comité de Administración Integral de Riesgos y Directorio el resultado de la capacitación de los Planes de Continuidad del Negocio al personal clave y alterno a través de los informes mensuales.

Adaptado de (Banco Capital , 2015)

Tabla 25.

Procedimiento para la recuperación de desastres

Procedimiento para la Recuperación de Desastres	
Objetivo	Detallar las diferentes etapas que componen el Plan de Recuperación de Desastres, así como también los procedimientos necesarios para su aplicación, con la finalidad de disponer de un esquema tecnológico que brinde soporte continuo a las operaciones del negocio ante eventos imprevistos que demanden la aplicación de procesos de contingencia.

Alcance	Este procedimiento cubre las actividades que se deben desarrollar en un Plan de Recuperación de Desastres, que consiste en identificar aquellas áreas que tienen prioridad y que por su naturaleza pueden afectar el funcionamiento del Banco ABC. Si no se cuenta con el servicio que las mismas ofrecen. Este plan identifica como prioridad el área de Sistemas y la plataforma tecnológica de la institución.
Responsable operativo	Equipo de recuperación de desastres • Gerente de Tecnología/Subgerente de Tecnología • Vicepresidente/Jefe de operaciones • Jefe de Riesgos Integrales/Jefe de Riesgo Operativo
Emergencia	**Análisis Previa Activación** Los eventos o indicios del día a día deberán ser atendidos o resueltos por el personal de Tecnología; el PRD se activará únicamente cuando los eventos o incidentes por su naturaleza interrumpan las operaciones del Data Center principal en la ciudad de Quito. Todo el personal del Banco ABC notificará de forma inmediata un evento que podría afectar la continuidad del negocio a los miembros del *Equipo de Evaluación del Incidente*, quienes deberán efectuar un análisis del evento reportado siguiendo lo indicado en documento "*Procedimiento para la Declaración de la Emergencia*". Dentro del proceso de evaluación de un incidente se podrían presentar los siguientes tipos de eventos: 1. El ingreso al data center principal o al Edificio Matriz se encuentra físicamente interrumpido de forma temporal o permanente. Eventos que pueden catalogarse dentro de este grupo de incidentes son: • Desastres naturales (Sismos, erupciones volcánicas) • Ataques intencionados (Disturbios y manifestaciones, asaltos, ataques terroristas) • Eventos Accidentales (Incendios, daños en los ascensores) • Perdida de Servicios Públicos (pérdida de energía eléctrica) 2. Los recursos o elementos que componen el data center principal presentan algún problema de forma temporal o permanente. Eventos que pueden catalogarse dentro de este grupo de incidentes son: • Eventos Accidentales (Incendio en Data Center Principal, Inundación en el Data Center Principal) • Daño de Tecnología (Daños Severos en Servidores críticos, Daños Severos en Nodo Central de Comunicaciones, Daños en los UPS, Fallas Severas en Aire Acondicionado, Problemas serios en sistema operativo y bases de datos) • Ataques intencionados (Hackers, Virus y Malware) 3. Los servicios requeridos para el funcionamiento del data center principal o Edificio Matriz presentan un problema de forma temporal o permanente. Eventos que pueden catalogarse dentro de este grupo de incidentes son: • Interrupción de fluido eléctrico

	• Interrupción de comunicaciones • Interrupción de sistema de aire acondicionado • Factor Humano (Errores, rotación del personal) El funcionario del Área de Sistemas encargado, adicionalmente a la estimación del tiempo de solución del incidente, debe identificar si el proceso de activación del PRD demanda la utilización de soporte de sistemas interno o externo.
	Reubicación de Personal y Recursos de TI Cuando el incidente presentado obedece específicamente a una pérdida de acceso al data center principal o edificio matriz, puede ser necesario, en función de la magnitud del evento, efectuar una reubicación tanto del personal como de los recursos tecnológicos mínimos necesarios para restablecer la operación del negocio. Para este caso es necesario considerar y aplicar los siguientes lineamientos: <u>Plan de Evacuación</u> En caso de que el evento se produzca durante la jornada normal o extendida de trabajo, el personal del Área de Sistemas y del Edificio Matriz presente debe seguir el plan establecido para la evacuación del edificio. En caso de que el evento se produzca en un momento que no existe personal en las oficinas no es necesario aplicar el plan de evacuación. <u>Reubicación de Personal de la Área de Sistemas</u> En caso de que el evento ocasione la pérdida total del espacio físico en el cual opera el data center principal, el personal del Área de Sistemas requerido y disponible debe trasladarse a la ciudad de Ibarra donde se encuentra operando el sitio alterno de Banco ABC. El Área de Sistemas definirá que el personal que no sea requerido para la activación y operación del sitio alterno pueda ser ubicado en la oficina más cercana que se encuentre disponible. El traslado del personal disponible del Área de Sistemas se realizará por vía terrestre inmediatamente después de la declaración de la emergencia. El sitio alterno deberá contar con los recursos mínimos necesarios para reanudar las operaciones como: puestos y estaciones de trabajo, teléfonos, impresoras, puntos de red, entre los principales recursos. <u>Reubicación del Personal Crítico del Edificio Matriz</u> El personal crítico de las gerencias funcionales puede ser ubicado en la oficina más cercana disponible. En caso de que no se requiera del sistema Globus T24 y se tiene las condiciones para trabajar desde su casa podrá hacerlo previa autorización del Comité de Administración de Crisis.
	Declaración Una vez declarada formalmente la emergencia conforme al procedimiento respectivo, el funcionario encargado del Área de Sistemas inicia el proceso de recuperación del sitio alterno.

Actividades
Ubicación Para la implementación del PRD se dispone de un sitio alterno de procesamiento de información, ubicado físicamente en la oficina de Ibarra, a 120 Km de la ciudad de Quito. Este sitio alterno se encuentra implementado con los servicios y recursos necesarios para soportar las operaciones de la entidad financiera bajo un esquema de contingencia. **Recursos** Servidores Alternos El sitio alterno dispone de los siguientes servidores: Las características de los equipos como: marca, modelo y capacidad. Aplicativos Los servidores del sitio alterno están en capacidad de soportar las operaciones del negocio con los siguientes sistemas: Indicar que aplicativos se tendrá, habrá correo, servidor de comunicaciones Comunicaciones El sitio alterno dispone de dispositivos de comunicaciones que son: Firewall, Router y Switch de marca CISCO, los cuales serán indispensables para la comunicación con las oficinas. **Recuperación** Respaldos de información en medio magnético El Banco ABC debe asegurar la integridad y disponibilidad de la información de la que depende su funcionamiento. Para ello establece la necesidad de contar con procedimientos adecuados de respaldo, almacenamiento y restauración de la información de sus sistemas. Respaldos de Información vía Replicación al Sitio Alterno Se ha establecido un proceso para que la información de la Base de Datos SQL del aplicativo T24 que se encuentra alojada en un servidor del Data Center Principal sea replicada de forma transaccional a la Base de Datos SQL en el servidor ubicado en el Data Center Alterno ubicado en la ciudad de Ibarra. *Respaldo de Programas* El esquema implementado para disponer en todo momento de una copia de la versión actual del sistema es mantener una copia en carpetas compartidas tanto en el servidor de producción como en el servidor de respaldo; además siempre que se realicen cambios a los programas se respalda una copia en cinta. El control de versiones se mantiene bajo resguardo del Área de Tecnología. Equipos de Recuperación *Soporte Técnico Interno* El soporte técnico interno encargado de ejecutar el proceso de recuperación del sitio alterno está definido de acuerdo a los siguientes niveles de atención: • Equipo para la valoración del daño.- La valoración del daño será liderada por el Gerente de Tecnología, quien definirá si se requiere del soporte de la Unidad Administrativa o de otras áreas. • Equipo de logística.- El equipo de logística será conducido por el Jefe de Talento Humano, quien será responsable de seleccionar los otros miembros del equipo, para dar atención a las solicitudes requeridas para la preparación del sitio de recuperación y garantizar la logística y recursos requeridos por el personal técnico que participará en la recuperación. Este equipo será también responsable por la reparación y/o

reconstrucción del data center principal.

- Equipo para la recuperación en casos de daños en los componentes de la infraestructura tecnológica.- Este equipo será dirigido por el Gerente de Tecnología y/o el personal designado por este, será responsable de realizar la recuperación del componente afectado, que puede ser: redes, servidores, aplicaciones, bases de datos, otros.

Soporte Técnico Externo

Cuando por efecto de las circunstancias propias del evento que origina la activación del PDR, se defina la necesidad de solicitar soporte técnico externo o de los proveedores de servidores críticos o de los enlaces de comunicaciones.

El Gerente de Tecnología gestionará el tipo de soporte técnico externo que se requiera y contratará los servicios de los proveedores que considere pertinentes, previa aprobación del Comité de Administración de Crisis

Procesos de Recuperación

Secuencia de Recuperación para el Data Center Alterno

La secuencia de recuperación de los servicios informáticos requeridos por Banco ABC para su operación seguirá el orden establecido en el Plan de Contingencias Departamento de Sistemas, una vez efectuado el análisis del incidente y declarada formalmente la emergencia, el funcionario encargado de la recuperación del sitio alterno, selecciona el proceso adecuado de recuperación considerando las siguientes alternativas:

Servidor Principal y Comunicaciones Disponibles

Para aquellos incidentes en los cuales existe pérdida de servicios en el data center principal sin que hayan comprometido el funcionamiento de los servidores, el proceso de recuperación, en dependencia de la causa, podrá estar conformado por las siguientes actividades:

- Detener Sistema Sitio Principal
- Activar las conexiones de comunicación alternas
- Configurar Base de Datos Alterna
- Configurar la aplicaciones de las Oficinas
- Activar Sistema Sitio Alterno
- Notificar Recuperación

La activación del Sitio Alterno se lo realizaría desde el Edificio Matriz

Servidor Principal No Disponible y Comunicaciones Disponibles

Para aquellos incidentes en los cuales existe “Pérdida de Acceso” o “Pérdida de Recursos” en el data center principal los cuales hayan comprometido el funcionamiento del servidor principal, el proceso de recuperación está conformado por las siguientes actividades:

- Configurar la aplicaciones de las Oficinas
- Configurar Base de Datos Alterna
- Activar Sistema Sitio Alterno
- Notificar Recuperación

La activación del Sitio Alterno se lo realizaría desde el Edificio Matriz ya que se cuenta con las comunicaciones activas

Servidor Principal y Comunicaciones No Disponibles

Para aquellos incidentes en los cuales existe pérdida completa del data center principal, el proceso de recuperación, debe estar conformado por las siguientes actividades:

- Movilizar al equipo de Área de al Sitio Alterno en Ibarra
- Activar las conexiones de comunicación alternas
- Configurar Base de Datos Alterna
- Configurar la aplicaciones de las Oficinas
- Activar Sistema Sitio Alterno
- Notificar Recuperación

El personal del Área de Sistemas tendrá que trasladarse a la ciudad de Ibarra que sería de 3 horas aproximadamente y activar el Sitio Alterno.

Procesos de Restauración del Sitio Principal

El retorno al Sitio Principal se lo llevará a cabo de acuerdo a lo indicado en el documento "*Políticas para la Administración de la Crisis*", el equipo encargado de habilitar el sitio principal realizará el proceso de recuperación de la siguiente manera:

- Esperar al Cierre de Operaciones del Día
- Respaldar la Base de Datos del Sitio Alterno
- Detener Sistema Sitio Alterno
- Habilitar Enlaces de Comunicación
- Configurar y Cargar Respaldo en Base de Datos en el Sitio Principal
- Configurar las aplicaciones de las Oficinas
- Activar Sistema Sitio Principal
- Notificar el restablecimiento

Pruebas

Pruebas de Activación de PRD

La Área de Sistemas realizará pruebas del PRD de forma periódica, al menos una vez al año.

El alcance de las pruebas deberá cubrir al menos uno de los siguientes escenarios:

Escenario 1

Serán pruebas básicamente de control de conexión en las cuales no se requiere efectuar transacciones financieras sobre los productos del Banco ABC. Consisten en aplicar el PRD considerando:

- Activación del Sitio Alterno
- Conexión de las oficinas
- Recuperación sitio principal

Escenario 2

Son pruebas de aplicación de transacciones financieras de manera controlada durante un día de trabajo específico siempre llegando al cierre del sistema en el Sitio Alterno y se aplica considerando:

- Activación del sitio alterno
- Conexión de las oficinas
- Transacciones a las oficinas
- Cierre de operaciones

- Cierre de sistema
- Restauración del sitio principal

Dada la naturaleza de las pruebas se deberá analizar los riesgos que conlleva y solicitar la aprobación de la Presidencia Ejecutiva, éstas deben efectuarse seleccionado un día bajo en volumen de transacciones y con la participación de todos los involucrados en el BCP, se deberá dejar evidencias de las pruebas efectuadas

Mantenimiento

Actualizaciones al Plan

Como resultado de la aplicación de las pruebas del PRD, el Gerente de Tecnología con su equipo identificará los inconvenientes presentados y determina si su solución demanda ajustes de configuración o ajustes de procedimientos. Procediendo luego de ello a plantear las acciones correctivas necesarias las cuales se complementan con actualización de la documentación correspondiente al plan y/o a los procedimientos definidos.

Cuando la solución a los inconvenientes presentados deriva en ajustes, correcciones u optimizaciones al esquema tecnológico que soporta el PRD, el Gerente de Tecnología propondrá alternativas para la modificación del mencionado esquema.

Adaptado de (Banco Capital , 2015)

Tabla 26.

Procedimiento de Operación de Contingencia Captaciones

Procedimiento de Operación de Contingencia Captaciones	
Objetivo	Establecer los lineamientos y acciones a tomar en caso de evidenciarse alguno de los incidentes de riesgo, para minimizar el impacto provocado.
Alcance	El alcance del procedimiento es para todo el personal del Banco ABC, en todos los niveles.
Responsable operativo	Responsable de Riesgos Integrales/ Jefe de Riesgo Operativo /Responsable de proceso
Actividades	

APERTURA, RENOVACIÓN Y CANCELACIÓN

El "*Procedimiento de Operación en Contingencia – Apertura, Renovación y Cancelación*" deberá ser puesto en funcionamiento en caso de presentarse los siguientes eventos:

- Indisponibilidad del sistema Core Globus T24

Actividades del proceso

- Solicitud inicio de relación comercial – Actualización de Datos
- Ingreso de información en Comprobante de Negociación
- Emisión del Certificado de Depósito a Plazo
- Solicitud de Apertura de Cuentas y Servicios
- Solicitud de renovación del Certificado de Depósito a Plazo por parte del cliente
- Carta de instrucción del cliente de Cancelación del Certificado de Depósito a Plazo

- Entrega del Certificado de Depósito a Plazo por parte del cliente
- Pago del capital más los intereses generados por la inversión

Recursos críticos

Recursos Humanos:

- Oficial de Captaciones (Backup: Oficial de Captaciones Ibarra)
- Asistente de Operaciones Quito (Backup: Supervisor Operativo Ibarra)
- Gerente de Captaciones (Backup: Gerente Sucursal Ibarra)

Aplicaciones:

- Core Globus T24
- Listas

Servicios:

- Teléfono
- Correo Electrónico

Recursos Informáticos:

- 5 computadores (3 Quito – 2 Ibarra)
- 5 puntos de red
- 2 impresoras
- 2 escáner

Plan de contingencia

- En el caso de apertura y renovación de inversiones se procede a llenar el Comprobante de Negociación con la información que será ingresada cuando se mantenga el sistema T24.
- En el caso de cancelaciones se debe elaborar una herramienta (Excel) que permita al Oficial de Captaciones calcular el valor a pagar y la retención que debe descontar al cliente.
- El área de Sistemas en el proceso batch generará un reporte con la información base de los clientes y de los certificados de depósito con los vencimientos mensuales, con al menos la siguiente información:
  - Nombre del cliente
  - Número de teléfono del cliente
  - Fecha de apertura del certificado de depósito
  - Monto del certificado de depósito
  - Fecha de vencimiento
  - Valor total a pagar
  - Valor de la retención por servicios financieros

El reporte deberá ser obtenido posterior al cierre diario luego de los cálculos de interés, este proceso batch se ejecutará de forma quincenal y enviará automáticamente el archivo a las cuentas de correo electrónico institucional al Gerente de Captaciones.

- El Gerente de Captaciones debe entregar el reporte generado a los Oficiales de Captaciones, quiénes se comunicarán

telefónicamente con los clientes para confirmar la cancelación o renovación de los certificados de depósitos a plazo.

- El Oficial de Captaciones llenará un comprobante de negociación con las instrucciones del cliente, indicando la cancelación o renovación de la inversión, y llevar un registro de las transacciones realizadas en una hoja en EXCEL.
- El Oficial de Captaciones deberá revisar en el reporte las características del Certificado de Depósito para proceder con las instrucciones del cliente.
- El cliente deberá entregar el documento original del Certificado de Depósito.
- En caso de disponibilidad del sistema se cancelarán los valores pertinentes por medio de transferencia, caso contrario se debe realizar el pago con cheque.
- Para realizar el pago con cheque, el Oficial de Captaciones debe solicitar autorización al área de Finanzas. Con esta autorización, procede a emitir el cheque al cliente con los valores correspondiente
- El Oficial de Captaciones debe imprimir los documentos de liquidación, retención y hacer firmar al cliente.
- El Oficial de Captaciones debe entregar al cliente un respaldo de la transferencia realizada o el cheque.
- Una vez que se tenga disponible el sistema T24, el Oficial de Captaciones ingresará en el aplicativo las transacciones

Adaptado de (Banco Capital , 2015)

Tabla 27.

Procedimiento de Operación de Contingencia Colocaciones

Procedimiento de Operación de Contingencia Colocaciones	
Objetivo	Establecer los lineamientos y acciones a tomar en caso de evidenciarse alguno de los incidentes de riesgo, para minimizar el impacto provocado.
Alcance	El alcance del procedimiento es para todo el personal del Banco ABC, en todos los niveles.
Responsable operativo	Responsable de Riesgos Integrales/ Jefe de Riesgo Operativo / Responsable de proceso
Actividades	
INSPECCIÓN Y EVALUACIÓN DE CRÉDITOS	
El "*Procedimiento de Operación en Contingencia – Inspeccionar y Evaluar Créditos*" deberá ser puesto en funcionamiento en caso de presentarse indisponibilidad del sistema Core Globus T24 y el sistema Originador de Crédito SOC. **Actividades del proceso** • Verificación de clientes en el buró de crédito • Verificación de clientes en Listas • Análisis del crédito del cliente • Revisión de la carpeta del cliente	

- Elaboración del Medio de Aprobación

Recursos críticos

Recursos Humanos:

- Asesor de Crédito (Backup: Subgerente de Negocios)

Aplicaciones:

- Core Globus T24
- Buro de Crédito – Equifax
- Listas
- Web Cobrador

Servicios:

- Teléfono
- Correo Electrónico
- Internet

Recursos Informáticos:

- 1 computador
- 1 impresora
- 1 puntos de red

Plan de contingencia

- En los casos que se deba realizar la consulta del buró y exista indisponibilidad del sistema Core Globus T24 se debe consultar el buró de crédito del cliente. De no poder realizar la consulta del buro se pondrá en el frente de las carpetas una hoja grapada indicando "Expediente por Regularizar".
- El Asesor de Crédito debe llevar un registro en una hoja en EXCEL de las carpetas de los créditos que se encuentran por regularizar la consulta del buró de crédito.
- Cuando las carpetas de los clientes se encuentren completas, el Analista de Crédito verificará que se encuentra toda la documentación del crédito, para lo cual deberá contar con el "Check List de Crédito" actualizado de los documentos. Luego de verificada la información, la carpeta del cliente se entrega al Comité de Crédito
- En base a la información de la carpeta del cliente, el Comité de Crédito analizará la aprobación o negación del mismo, la decisión deberá constar en el Informe de Análisis Crediticio.
- El Asesor de Crédito deberá notificar al cliente el dictamen tomado por el Comité de Crédito (Aprobado o Rechazado), en caso de que el crédito fue aprobado deberá acordar con los clientes la fecha y hora para que se acerquen a las oficinas para la firma de documentos y entrega de dinero.
- Una vez que el sistema Core Globus T24 se encuentre disponible se deberá ingresar la información de los créditos, la fecha de ingreso deberá ser la misma en la cual se procedió con el desembolso.

APROBACIÓN DE CRÉDITOS

El "*Procedimiento de Operación en Contingencia – Aprobar Créditos*" deberá ser puesto en funcionamiento en caso de presentarse indisponibilidad del sistema Core Globus T24.

Actividades del proceso

- Verificación del Informe de Análisis
- Revisión del Medio de Aprobación
- Aprobación de créditos en el sistema

Recursos críticos

Recursos Humanos:

- Ingreso de la información del crédito.- Asistente Operativo (Backup: Asistente Operativo)
- Aprobación.- Analista de Riesgos (Backup: Jefe de Riesgos)

Aplicaciones:

- Core Globus T24
- Buro de Crédito – Equifax
- Listas

Servicios:

- Servicio de Telefonía
- Correo electrónico

Recursos Informáticos:

- 1 computador
- 1 punto de red

Plan de contingencia

- El Asistente Operativo deberá verificar que se encuentra toda la documentación del crédito en la carpeta del cliente, para lo cual deberá contar con el "Check List de Crédito" actualizado.
- En caso de que el Comité de Crédito de la aprobación para el desembolso, las carpetas de los clientes deberán ser entregados al Gerente de Operaciones para que se efectué el proceso para la entrega del dinero al Cliente.
- Una vez que el sistema Core Globus T24 se encuentre disponible se deberá ingresar la información de los créditos, la fecha de ingreso deberá ser la misma en la cual se procederá con el desembolso.

DESEMBOLSO DE CRÉDITOS

El "*Procedimiento de Operación en Contingencia – Desembolsar Créditos*" deberá ser puesto en funcionamiento en caso de presentarse los siguientes eventos:

- Indisponibilidad del sistema Core Globus T24

Actividades del proceso

- Registro de firmas de los clientes en la documentación del desembolso
- Entrega del dinero de crédito al cliente

Recursos críticos

Recursos Humanos:

- Asistente Operativo (Backup: Asistente Operativo)

Aplicaciones:

- Core Globus T24

Servicios:

- Teléfono
- Internet
- Correo electrónico

Recursos Informáticos:

- 1 computador
- 1 impresora y copiadora
- 2 puntos de red

Plan de contingencia

- El Asistente de Operaciones debe contar con los documentos que deben firmar los clientes para el desembolso, se debe actualizar la información en caso de que los formatos cambien.
- El Asistente de Operaciones procederá a imprimir los documentos requeridos para el desembolso y hará firmar los documentos al cliente.
- El Asistente de Operaciones debe enviar un mail al /Asesor de Crédito confirmando que se va a realizar el desembolso.
- En caso de que no se pueda realizar el desembolso por medio del sistema, el Asistente de Operaciones debe solicitar al área de Finanzas por medio de mail, la autorización para realizar el desembolso mediante cheque.
- El Asistente de Operaciones debe sacar una copia del cheque emitido y en el talonario del cheque se debe registrar los datos del cliente indicando “Desembolso en Contingencia”.
- El Asistente de Operaciones debe enviar un registro en EXCEL al Jefe Operativo, con todos los desembolsos realizados durante la contingencia y adjuntar las copias de los cheques.
- Una vez que el sistema Core Globus T24 se encuentre disponible se deberá ingresar la información del desembolso de créditos, la fecha de ingreso deberá ser la misma en la cual se procedió con el desembolso.

Adaptado de (Banco Capital , 2015)

Tabla 28.

Procedimiento de Operación de Contingencia Back Office

Procedimiento de Operación de Contingencia Back Office	
Objetivo	Establecer los lineamientos y acciones a tomar en caso de evidenciarse alguno de los incidentes de riesgo, para minimizar el impacto provocado.
Alcance	El alcance del procedimiento es para todo el personal del Banco ABC, en todos los niveles.
Responsable operativo	Responsable de Riesgos Integrales/ Jefe de Riesgo Operativo / Responsable de proceso
Actividades	
GENERACIÓN DE INFORMACIÓN Y CARGA DE ARCHIVO	

El "*Procedimiento de Operación en Contingencia – Generación de Información y Carga de Archivo*" deberá ser puesto en funcionamiento en caso de presentarse los siguientes eventos:

- Indisponibilidad del sistema Core Globus T24
- Indisponibilidad del servicio de internet

Actividades del proceso

- Carga del archivo en el SCCC (Sistema de Cámara de Compensación de Cheques)
- Confirmación al BCE (Banco Central del Ecuador) de la carga exitosa
- Confirmación a los Bancos por cheques cargados fuera de cámara

Recursos críticos

Recursos Humanos:

- Asistente Operativo (Backup: Asistente Operativo Ibarra)

Aplicaciones:

- Core Globus T24
- DCNET
- SFTP

Servicios:

- Teléfono
- Correo Electrónico
- Internet

Recursos Informáticos:

- 1 computador
- 1 lectora
- 1 punto de red
- 1 impresora

- Certificado digital SFTP

Plan de contingencia

- En caso de indisponibilidad del sistema Core Globus T24, el proceso “Generación de información y carga de archivos” no podrá ser efectuado hasta la activación del aplicativo
- En el caso de no tener disponible el servicio de internet para la carga de información no podrá ser efectuado el proceso hasta la activación del internet.

GENERACIÓN DE INFORMACIÓN DE TRANSACCIONES EN SERVIPAGOS

El “*Procedimiento de Operación en Contingencia – Generación de Información y Transacciones en Servipagos* ” deberá ser puesto en funcionamiento en caso de presentarse los siguientes eventos:

- Indisponibilidad del sistema Core Globus T24
- Indisponibilidad del servicio de internet

Actividades del proceso

- Cuadre de saldos Banco ABC Vs Servipagos
- Notificación al área de Contabilidad, Operaciones y Oficial de cuentas en caso de descuadres

Recursos críticos

Recursos Humanos:

- Asistente Operativo (Backup: Asistente Operativo Ibarra)

Aplicaciones:

- Core Globus T24
- SFTP

Servicios:

- Teléfono
- Correo Electrónico
- Internet

Recursos Informáticos:

- 1 computador
- 1 punto de red
- 1 impresora

Plan de contingencia

- En caso de indisponibilidad del sistema Core Globus, el proceso “Generación de información de Transacciones de Servipagos” no podrá ser efectuado hasta la activación del aplicativo

• En el caso de no tener disponible el servicio de internet para la revisión de la información de las transacciones procesadas en Servipagos, no podrá ser efectuado el proceso hasta la activación del internet.

Tabla 29.

Procedimiento de Operación de Contingencia Front Office.

Procedimiento de Operación de Contingencia Front Office	
Objetivo	Establecer los lineamientos y acciones a tomar en caso de evidenciarse alguno de los incidentes de riesgo, para minimizar el impacto provocado.
Alcance	El alcance del procedimiento es para todo el personal del Banco ABC, en todos los niveles.
Responsable operativo	Responsable de Riesgos Integrales/ Jefe de Riesgo Operativo / Responsable de proceso
Actividades	
APERTURA Y CIERRE DE BÓVEDA Y CAJAS	
El "*Procedimiento de Operación en Contingencia – Apertura y Cierre de Bóveda y Cajas"* deberá ser puesto en funcionamiento en caso de presentarse los siguientes eventos: • Indisponibilidad del sistema Core Globus T24 • Indisponibilidad del servicio de internet **Actividades del proceso** • Apertura de Bóveda y Cajas • Cuadre y Cierre de Bóveda y Cajas • Incremento de efectivo en Bóveda • Entrega y Recepción de Efectivo **Recursos críticos** *Recursos Humanos:* • Supervisor Operativo (Backup: Asistente Operativo) • Cajero (Backup: Asistente Operativo) *Aplicaciones:* • Core Globus T24 • Puntomático *Servicios:* • Teléfono • Correo Electrónico *Recursos Informáticos:*	

- 1 computador
- 1 impresora
- 1 scanner

Plan de contingencia

- En caso de indisponibilidad del sistema Core Globus T24, el proceso “Apertura y Cierre de Bóveda y Cajas” no podrá ser efectuado hasta la activación del aplicativo

PROCESO DE TRANSACCIONES

El “*Procedimiento de Operación en Contingencia – Proceso de Transacciones*” deberá ser puesto en funcionamiento en caso de presentarse los siguientes eventos:

- Indisponibilidad del sistema Core Globus T24
- Indisponibilidad del servicio de internet

Actividades del proceso

- Confirmación del pago con el cliente
- Consulta de saldos del cliente
- Consulta de pagos
- Carga y autorización de transferencias

Recursos críticos

Recursos Humanos:

- Supervisor Operativo (Backup: Asistente Operativo)
- Cajero (Backup: Asistente Operativo)

Aplicaciones:

- Core Globus T24
- Puntomático

Servicios:

- Teléfono
- Correo Electrónico
- Internet

Recursos Informáticos:

- 1 computador
- 1 punto de red
- 1 impresora
- 1 sumadora
- 1 scanner para microfilm

Plan de contingencia

- En caso de indisponibilidad del sistema Core Globus T24 , el “Proceso de Transacciones” no podrá ser efectuado hasta la activación del aplicativo
- El área de Sistemas en el proceso batch generará un archivo con al menos los siguientes datos: nombres completos del cliente, cédula, dirección de domicilio, teléfono, producto de crédito, código de préstamo, datos de mora (Monto de mora, tiempo en días y meses), número de la cuota, valor del pago, fecha de pago, valor total para la cancelación del crédito, entre otros, el reporte deberá ser obtenido posterior al cierre diario luego de los cálculos de interés, este proceso batch se ejecutará de forma quincenal y enviará automáticamente el archivo a las cuentas de correo electrónico institucional del Gerente de Operaciones.
- El Supervisor Operativo deberá enviar mediante mail a todos los Asesores de Crédito, el archivo con los vencimientos, para que éstos se comuniquen con los clientes.
- En caso de indisponibilidad del sistema Core Globus T24, no se realizará la carga de información y se le comunicará al cliente que debe acercarse a la IFI y realizar el depósito del pago de la cuota en la cuenta de Banco ABC.

EMISIÓN Y ENTREGA DE TARJETAS DE DÉBITO

El “*Procedimiento de Operación en Contingencia – Emisión y Entrega de Tarjetas de débito*” deberá ser puesto en funcionamiento en caso de presentarse los siguientes eventos:

- Indisponibilidad del sistema Core Globus T24
- Indisponibilidad del servicio de internet

Actividades del proceso

- Solicitud de emisión de tarjeta de débito
- Entrega de la tarjeta
- Solicitud al proveedor de la emisión de la tarjeta

Recursos críticos

Recursos Humanos:

- Asistente Operativo (Backup: Asistente Operativo)
- Supervisor Operativo (Backup: Asistente de Custodia)

Aplicaciones:

- Core Globus T24
- Extreme Web

Servicios:

- Teléfono
- Correo Electrónico
- Internet

Recursos Informáticos:

- 1 computador
- 1 punto de red
- 1 impresora

Plan de contingencia

- En caso de indisponibilidad del sistema Extreme Web, el proceso “Emisión y Entrega de Tarjetas de Débito” no podrá ser efectuado hasta la activación del aplicativo.
- El Asistente Operativo deberá receptar la solicitud de emisión de tarjeta de débito suscrita por el cliente.
- El Asistente Operativo una vez que se encuentre activado el sistema se ingresará los datos de la tarjeta solicitada.

Adaptado de (Banco Capital , 2015)

Tabla 30.

Procedimiento de realización de pruebas y evaluación de resultados

Procedimiento de realización de pruebas y evaluación de resultados	
Objetivo	Realizar pruebas que aseguren la efectividad de los Planes de Continuidad del Negocio desarrollados para el Banco ABC
Alcance	E El contenido de este manual tiene alcance a todo el personal del Banco ABC
Responsable operativo	Responsable del área de Riesgos /Jefe de riesgo operativo
Lineamientos	Banco asegurará la continuidad de sus operaciones a través, de un sistema de gestión para la continuidad del negocio (Programa ACN) debidamente actualizado y probado periódicamente. El área de Riesgos, debe asegurarse que queda minimizado el riesgo de impacto del trastorno, que la realización de las pruebas podría producir a la Institución. El negocio deberá entender y aceptar el riesgo de la realización de la prueba. El área de Riesgos, deberá implementar un esquema para el desarrollo de las Pruebas que incluya la definición de escenarios, alcances, objetivos, factores críticos de éxito, controles, responsabilidades y un reporte escrito de la evaluación de los resultados y lecciones aprendidas. El área de Riesgos deberá diseñar el Plan de Pruebas para la Continuidad del Negocio, a través de reuniones en los que participarán los grupos responsables de preparar y ejecutar las pruebas. El Banco diseñará y ejecutará pruebas, que cumplirán con criterios de rigurosidad, realismo y exposición mínima, que sean coherentes con los alcances del Programa ACN. El área de riesgos podrá solicitar pruebas parciales de Continuidad a los responsables de área, cuando las necesidades del Banco lo requieran. Sin embargo, si la prueba tiene cierto grado de complejidad y exposición. La ejecución de la prueba deberá ser aprobada por el Comité de Continuidad del Negocio y si se dan las siguientes condiciones: a.) La prueba afecta a los procesos calificados como esenciales por el BIA y aquellos procesos que originan

	dependencias en los calificados como críticos. b.) El ámbito de afectación de la prueba es Nacional, Regional, Oficinas Principales. c.) La prueba contempla la activación, parcial o total, de los Sitios Alternos simulando el traslado de uno o más procesos con sus respectivas funciones. d.) La prueba constituye ejercicios elementales para la ejecución de respuestas a la emergencia o para la administración de una crisis. e.) La prueba constituye ejercicios elementales para la ejecución de respuestas a desastres tecnológicos. El área responsable de ejecutar las pruebas debe asegurarse de que existen puntos acordados previamente para continuar o detener la prueba a lo largo de etapas claves, además de planes adecuados de respaldo en caso de que se requiere interrumpir la prueba y regresar al ambiente normal. Es responsabilidad del Jefe de Riesgos revisar el cumplimiento de las pruebas periódicas del plan para cada uno de los escenarios priorizados y los procesos implantados que permitan comprobar su éxito. El Jefe de Riesgos deberá realizar un seguimiento a las pruebas realizadas en el Sitio Alterno u Oficinas, examinando la efectividad de los Planes de Continuidad para restablecer las operaciones del negocio. Es responsabilidad de los dueños del proceso evaluar el desarrollo de las pruebas con la finalidad de asegurarse que el personal clave y alterno estén listos para una pronta y efectiva respuesta ante un incidente que interrumpa las operaciones de negocio del Banco. El personal de auditoría debe participar como observador tanto en las actividades de preparación como durante la ejecución de las pruebas. Deberá emitir un informe con las observaciones in-situ y posteriores a la ejecución de las pruebas. Los planes de continuidad del negocio deben ser probados mediante pruebas parciales en el año y considerar al menos una prueba global cada 12 meses o cuando ocurran cambios significativos en los procesos. Los resultados de la prueba deben ser claramente documentados, y los cambios o mejoras al plan de pruebas.
Responsable	**Actividades de elaboración del plan de pruebas para la continuidad del negocio**
RESPONSABLE DE RIESGO OPERATIVO	Determina las pruebas que se tienen que desarrollar de acuerdo a las instrucciones impartidas por el Jefe de Riesgos.
	Coordina con los responsables del proceso, la participación de los Líderes de Áreas o Usuarios, sobre las actividades de preparación para las pruebas.
	Prepara, un esquema preliminar de los puntos que se deben cubrir en el Plan de Pruebas.
	Convoca a los Líderes de Áreas o Usuarios para desarrollar el Plan de Pruebas de Continuidad.
	Durante las reuniones, expone de manera general a los Líderes de Áreas o Usuarios, las actividades que se deben cubrir en el Plan de Pruebas.
RESPONSABLES DE ÁREA Y JEFE DE RIESGOS/ JEFE DE RIESGO OPERATIVO	Analizan y establecen cada una de las actividades que se deben ejecutar antes y durante las pruebas, incluyendo las responsabilidades y los factores críticos de éxito.
	Definen los puntos de control para continuar o detener la prueba y la ejecución de los respaldos que permitan interrumpir las pruebas y regresar al ambiente normal.
JEFE DE RIESGO	Registra en formato en Excel lo expuesto por los Líderes de Áreas o Usuarios.

OPERATIVO	Al finalizar la reunión organiza la información registrada, diseña el Plan de Pruebas y lo remite a los Líderes de Áreas o Usuarios para su confirmación, incluyendo: Escenarios Objetivos Alcance de la prueba Factores críticos de éxito Controles Responsables Personal de soporte Cronograma de tareas asignadas a Líderes de Áreas o Usuarios con sus respectivos plazos de ejecución
	Una vez confirmado el Plan de Pruebas por parte de Líderes de Áreas / Usuarios, remite el Plan al Jefe de Riesgos para su revisión.
	Prepara o actualiza la lista de chequeo (checklist) de los puntos que se deben cubrir durante las pruebas.
JEFE DE RIESGOS	En caso en que las pruebas tengan cierto grado de complejidad y exposición: Se asegura de minimizar el riesgo y lo expone a los miembros del Comité de Continuidad del Negocios y Manejo de Crisis.
	Revisa el contenido del Plan de Prueba.
COMITÉ DE CONTINUIDAD DEL NEGOCIO	Conforme lo expuesto por parte del Jefe de Riesgos, aprueban o niegan la ejecución de la prueba.
JEFE DE RIESGOS	Si el Plan de Pruebas no es aprobado, convoca a los responsables para reestructurar el escenario y alcance de las pruebas.
	Remite a los Coordinadores de las pruebas el Plan de Pruebas para su respectiva ejecución.
Responsable	**Actividades de preparación previa y aseguramiento de la prueba de continuidad del negocio**
RESPONSABLE DE RIESGO OPERATIVO	Revisa periódicamente el cronograma de Pruebas de la Continuidad del Negocio, a fin de cumplir con las fechas establecidas.
	Antes de la fecha prevista para realizar la prueba, verifica el cumplimiento de las tareas asignadas a los Líderes de Áreas o usuarios para la ejecución del Plan de Pruebas de Continuidad.
	Confirma en la medida de lo posible, que los recursos necesarios para la ejecución de las pruebas estén disponibles y cumplan con los requisitos de continuidad establecidos.
	En caso que no se cumpla los requisitos de continuidad: Registra en la lista de chequeo, los recursos que no se encuentran disponibles o requisitos que no se cumplen.
	Solicita al responsable del proceso tomar las accione correctivas necesarias para continuar o reprogramar la fecha de ejecución de las Pruebas de Continuidad.

RESPONSABLE DEL PROCESO	Gestiona en conjunto con los Líderes de Áreas la ejecución de las tareas asignadas para la realización de las pruebas; caso contrario solicita al Jefe de Riesgos la reprogramación de la fecha para la realización de las pruebas y finaliza el proceso.
RESPONSABLE DE RIESGO OPERATIVO	Confirma al Jefe de Riesgos, que todas las condiciones necesarias para la ejecución de la prueba han sido validadas.
Responsable	**Actividades de ejecución de pruebas de continuidad**
RESPONABLE DE RIESGO OPERATIVO	Notifican al responsable del proceso, Líderes de Áreas, Usuarios, y Auditoría la ejecución de la prueba.
RESPONSABLE DEL PROCESO	Recibe por parte del responsable de riesgo operativo la notificación de ejecutar la prueba o medir el desarrollo del simulacro.
	Instruye a los Líderes de Áreas sobre las actividades que se deben ejecutar durante la prueba o medición del desarrollo del simulacro.
RESPONSABLES DE ÁREA /USUARIOS	Proceden a ejecutar la Prueba.
RESPONSABLES DE ÁREA	Observan las tareas realizadas por parte del personal a su cargo.
RESPONSABLES DE ÁREA /USUARIOS	En la lista de Chequeo registran: Las observaciones o novedades de las tareas ejecutadas durante la prueba Comentarios adicionales y nivel de cumplimiento.
	Entregan a los Responsables de los Procesos, la lista de chequeo (checklist) de las tareas de continuidad del negocio con su respectiva firma.
RESPONSABLES DEL PROCESO	De acuerdo a los parámetros normales del proceso, evalúan el desempeño de las operaciones de continuidad del negocio y la respuesta a la emergencia o desastre.
	Retroalimentan de esta información al Jefe de Riesgos
RESPONSABLE DE RIESGO OPERATIVO	Identifican posibles anomalías en el funcionamiento de los activos críticos o deficiencias en el desempeño de las pruebas de continuidad del negocio, conforme lo previsto en el Plan de Prueba o medición de Simulacros.
	Informan al Jefe de Riesgos: Tiempo de respuesta a la emergencia, Tiempo de recuperación de las actividades críticas del negocio y tiempo de respuesta de los servicios provistos por terceros, Tiempo del trabajo, Posibles anomalías en el funcionamiento de los activos críticos o deficiencias en el desempeño de las tareas de continuidad del negocio establecidas en los Planes.
Responsable	**Actividades de revisión de los resultados y corrección**
JEFE DE RIESGOS	Recibe de responsable de riesgo operativo:

	- Tiempo de respuesta a la emergencia - Tiempo de recuperación de las actividades críticas del negocio - Posibles anomalías en el funcionamiento de los activos críticos o deficiencias en el desempeño de las tareas de continuidad del negocio establecidas en los Planes.
JEFE DE RIESGOS / RESPONSABLE DE RIESGOS	Evalúan la eficacia y eficiencia de la ejecución de las tareas de continuidad del negocio establecidas en el Plan de Pruebas.
	Analizan los resultados de las pruebas
	Elaboran un informe a los Miembros del Comité de Continuidad del Negocio sobre el resultado de las Pruebas de Continuidad, incluyendo: Cumplimiento de los objetivos, Tiempo de realización de las tareas de continuidad del negocio Colaboradores que participaron Tareas realizadas Capacidad del personal para ejecutar las tareas de continuidad del Negocio Funcionamiento de los equipos y sistemas para realizar la prueba o desarrollo del simulacro Desempeño de las operaciones de continuidad del negocio en los sitios alternos
JEFE DE RIESGOS	Expone a los miembros del Comité de Continuidad del Negocio el informe de resultados de las pruebas.
	Recibe de Auditoría el informe de las observaciones in-situ y posteriores a la ejecución de las pruebas.
JEFE DE RIESGOS / RESPONSABLE DE RIESGO OPERATIVO	Analizan el contenido del informe de Auditoría y establecen acciones correctivas, preventivas o de mejoras para el Plan de Pruebas de la Continuidad del Negocio.

Adaptado de (Banco Capital , 2015)

4.3.2. Generación de informe de incidencia

Una vez definidos los diferentes procedimientos por los cuales se van a regir las acciones del plan de continuidad, se alude a la elaboración de un informe de incidencias luego de la ejecución de una prueba/simulacro o de la ocurrencia de un evento inesperado, según contiene el propio procedimiento anterior de revisión de los resultados y corrección.

Como bien se define anteriormente cuando los Miembros del Comité de Continuidad del Negocio elaboran el informe sobre el resultado de las Pruebas de Continuidad este debe contener:

- Cumplimiento de los objetivos.
- Tiempo de realización de las tareas de continuidad del negocio.
- Colaboradores que participaron.
- Tareas realizadas.
- Capacidad del personal para ejecutar las tareas de continuidad del Negocio.
- Funcionamiento de los equipos y sistemas para realizar la prueba o desarrollo del simulacro.
- Desempeño de las operaciones de continuidad del negocio en los sitios alternos.

De forma general se propone a continuación un modelo para el registro y descripción, ya sea de los resultados de la prueba provocada o de la respuesta ante un evento no deseado ocurrido.

Tabla 31.

Plantilla de Informe de incidencias y resultados

Nombre del Informe	Nombre del Informe de prueba o evento inesperado
Fecha de elaboración	Fecha en la que se realiza la prueba
Destinatario/Cargo	Personas a las cuales va dirigido el informe, que está en función de los objetivos específicos de la prueba
Objetivo	Objetivos que se persiguen al realizar el simulacro o al desarrollar las acciones de continuidad ante un evento inesperado, según sea el caso.
Alcance	A qué área, equipo o proceso de trabajo está orientada la prueba. En caso de ocurrencia de evento inesperado el área afectada.
Participantes	Todos los participantes en la actividad, ya sean del equipo coordinador o del equipo de evaluación, detallando en cada caso nombre, cargo, área que atiende y la responsabilidad que ocupa en ella.
Proveedor	En caso de afectación de equipos, los proveedores deben participar en el diagnóstico de los mismos, ya que ellos son quienes conocen las propiedades de fabricación y demás características.
Pruebas ejecutadas	En este apartado deben detallarse todas las actividades que se ejecutan durante el simulacro (o acciones durante el paro) determinando puntualmente la hora de inicio y fin de cada una, tiempo de duración estimado, tiempo de duración real, el cumplimiento o no de la actividad y las observaciones necesarias.
Conclusiones	En este caso deben figurar claramente los resultados de la actividad y el impacto provocado tras el incidente, en caso de paro.
Recomendaciones	Recomendar las acciones necesarias, para minimizar el impacto ocasionado o para eliminar las vulnerabilidades detectadas durante la ejecución de la prueba, de modo que pueda fundamentar la mejora continua del plan.
Anexos	Todos los argumentos que pueden constituir elementos esenciales en la interpretación y comprensión de las actividades realizadas, así como demostraciones de los comportamientos generados.

4.4. Verificación y control del BCP

4.4.1. Análisis de informes de incidencia

Para verificar y controlar el funcionamiento del BPC es preciso conocer como se está aplicando el mismo en la organización, observando la reducción de las interrupciones, que los tiempos de esas interrupciones eventuales hayan disminuido paulatinamente, determinar el límite de que una paralización de actividades críticas pueda ser representativa para la organización, además de verificar que el negocio se está fortaleciendo y al mismo tiempo se eliminen los puntos de fallos.

Los aspectos verificados se exponen en el informe de incidencias y se muestran a continuación:

Tabla 32.

Informe de incidencia

Nombre del Informe	Informe de incidencias
Fecha de elaboración	10/2/2017
Destinatario/Cargo	Administración del Banco ABC
Objetivo	Describir las acciones realizadas por los trabajadores del Banco ABC ante la presencia de riesgos o eventos inesperados.
Alcance	Gerencia del Banco ABC
Participantes	Gerente del Banco Trabajadores de la Gerencia Trabajadores del Banco
Proveedor	En caso de afectación de equipos, los proveedores deben participar en el diagnóstico de los mismos, ya que ellos son quienes conocen las propiedades de fabricación y demás características.
Pruebas ejecutadas	1- Se chequeó el compromiso formal del Consejo de la administración y la alta gerencia con el cumplimiento del BPC. 2- Se observó la funcionabilidad de las tecnologías de la información y su alineación con el plan estratégico de la organización. 3- Se verificó que existe un responsable de la información que se encargue de definir y autorizar formalmente los accesos y cambios funcionales, así como monitorear las necesidades de crecimiento de la organización. 4- Se comprobó que existe un responsable de la información y que al mismo tiempo se encarga de definir y autorizar de manera formal los cambios funcionales, así como monitorear el cumplimiento de

	los controles establecidos. 5- Las políticas, los procesos y los procedimientos de la tecnología de la información, deben perfeccionarse ya que estén definidos bajo estándares de general aceptación y deben garantizar la eficacia de los controles internos. 6- Se verificó que son poco difundidas dentro del personal involucrado las políticas que se requieren y los procedimientos que aseguren su implementación. 7- Se pudo observar que se realiza capacitación y entrenamiento al personal del área de tecnología de la información y a los usuarios de la misma, pero que no son suficientes. 8- Los manuales y reglamentos internos deben estar aprobados por el consejo de la administración, donde se establezcan los niveles de responsabilidad y proceder para cada operación. 9- Existe clasificación y control de los activos de la tecnología de la información, e incluye los registros e identificación, así como los responsables de su uso. 10- Existen requerimientos contractuales o convenidos que establecen la propiedad de la información y la responsabilidad de la empresa proveedora de la tecnología, en el caso de que sus sistemas sean vulnerables. 11- Deben perfeccionarse las políticas y procedimientos de seguridad de la información y que sus objetivos estén bien definidos, las normas, los principios, los requisitos y las responsabilidades ante la ocurrencia de incidentes y su comunicación. 12- Debe perfeccionarse el funcionamiento de los requerimientos de seguridad que están vinculados con la tecnología de la información, requisitos legales y contractuales. 13- Existen los controles necesarios que aseguran la integridad, la disponibilidad y la confidencialidad de la información, sin embargo, es necesario actualizaros y perfeccionarlos. 14- No existe un sistema de seguridad de acceso a la información donde se definan las facultades y atributos de los usuarios, desde el registro, eliminación y modificación de los controles necesarios que permitan verificar su cumplimiento en todos los ambientes de procesamiento. 15- Están establecidos los niveles de autorización de acceso y ejecución de las funciones del procesamiento de las aplicaciones, mediante el cual se garantice la desagregación de funciones. 16- Se comprobaron los accesos que permiten evitar los no autorizados. 17- Deben establecerse controles adecuados que permitan la identificación de software no autorizados o sin la respectiva licencia. 18- Se observó la existencia de controles para la documentación, medios de almacenamiento y otros dispositivos externos, posibles robos y daños. 19- La infraestructura es buena infraestructura, con áreas protegidas, donde se evita la entrada de personal no

	autorizado. 20- No existen planes elaborados para que el desempeño del sistema de administración de la seguridad de la información sea el correcto y en correspondencia a los objetivos de la entidad. 21- Se verificó que existen políticas y procedimientos que garantizan que solo las personas designadas tengan acceso a ellas.
Conclusiones	Como se pudo observar en el simulacro de ocurrencia de eventos se detectaron una serie de dificultades que deben ser manejadas con cuidado en la organización para que el trabajo fluya correctamente y que, al mismo tiempo, se logre que el Plan de continuidad del negocios se realice con el éxito que se quiere alcanzar, deben establecerse controles adecuados a la documentación y a los sistemas informáticos. Los planes deben ser elaborados en correspondencia con los problemas detectados en el desempeño del trabajo por parte de los implicados en el desarrollo de los procesos de la gerencia.
Recomendaciones	1- Perfeccionar los controles necesarios que aseguran la integridad, la disponibilidad y la confidencialidad de la información 2- Establecer un sistema de seguridad de acceso a la información donde se definan las facultades y atributos de los usuarios. 3- Incrementar las capacitaciones al personal de la entidad. 4- Los manuales y reglamentos internos deben estar aprobados por el consejo de la administración.
Anexos	(Se adjunta en los anexos del trabajo los documentos y procedimientos verificados)

Como se puede observar se han propuesto una serie de aspectos que pueden ser utilizados en la etapa de verificación del BCP, una de las más importantes, pues en ella se van a esclarecer las pautas a seguir, para poder tener criterios sobre cómo se está cumpliendo con los objetivos trazados en el plan. La organización es la encargada de seleccionar al personal que debe llevarlo a cabo y al mismo tiempo tener en cuenta que deben ser profesionales de experiencia y que hayan participado de alguna manera en la elaboración del BCP.

4.5. Mejoramiento del BCP

4.5.1. Plan de mantenimiento

En la revisión periódica de los lineamientos, estrategias, técnicas y planes, es necesario mantener actualizados y capacitados al personal. De esta forma, las

actividades de misión crítica serán perfeccionadas y se logran los resultados esperados en el Plan de continuidad del Negocios.

Objetivos del plan de mantenimiento:

1- Validar las estrategias y planes del BCP.
2- Detallar todos los cambios y estrategias del plan.

A continuación, se realiza el plan de mantenimiento.

Tabla 33.

Plan de mantenimiento

Nro	Actividades	Responsable	Fecha
1	Perfeccionar las políticas, los procesos y los procedimientos de la tecnología de la información.	Gerencia	22/03/2017
2	Difundir dentro del personal involucrado, las políticas que se requieren y los procedimientos que aseguren su implementación.	Gerencia	22/03/2017
3	Incrementar la capacitación del área de tecnología de la información y a los usuarios de la misma.	Gerencia	12/04/2017
4	Aprobar los manuales y reglamentos internos por parte del consejo de la administración.	Gerencia	15/04/2017
5	Perfeccionar las políticas y procedimientos de seguridad de la información y que sus objetivos estén bien definidos, así como las normas, los principios, los requisitos y las responsabilidades ante la ocurrencia de incidentes y su comunicación.	Gerencia	25/04/2017
6	Establecer mecanismos para elevar la seguridad en el acceso de la información.	Gerencia	07/05/2017
7	Actualizar los accesos a los locales.	Gerencia	22/05/2017
8	Realizar controles que permitan la identificación de software no autorizados o sin licencia.	Gerencia	05/06/2017
9	Elaborar planes elaborados para que el desempeño del sistema de administración de la seguridad de la información sea el correcto y en correspondencia a los objetivos de la entidad.	Gerencia	15/06/2017

Este plan de mantenimiento no es estático y puede ser modificado cuando lo estipule conveniente la gerencia y en correspondencia con la solución de los problemas detectados o la existencia de otros nuevos, que no estén comprendidos en este trabajo.

4.5.2. Propuesta de mejora

Para lograr un correcto funcionamiento del plan es importante realizar las siguientes mejoras continuas del sistema, tomando como referencia lo expuesto por Peña (2013) y los criterios del autor de esta investigación, acorde a los resultados obtenidos en la implementación de la propuesta:

1- Actualización de los requerimientos legales.
2- Actualización de nuevos productos.
3- Introducir nuevos hardware, plataformas, aplicativos u otros cambios de tecnología.
4- Adoptar los cambios en las comunicaciones en correspondencia con las nuevas tecnologías de la información.
5- Cambiar los proveedores que se consideren en estado crítico.
6- Transferir funciones en los sitios existentes.
7- Tercerización de funciones.
8- Tener presente los resultados de las pruebas del Plan de Continuidad del Negocios.
9- Realizar todos los cambios necesarios en el sistema en correspondencia con el Plan implementado.

4.6. Certificación de la institución financiera ABC según la ISO 22301:2012

Para lograr la certificación de la entidad objeto de estudio, es necesario contar con una serie de documentos y registros mínimos que conforman la información documentada, la cual se puede apreciar a continuación con el punto de la norma al que corresponde:

Tabla 34.

Documentos y registros necesarios para certificar la organización según la ISO 22301:2012

Documentos y registros	Punto en ISO 22301:2012
Determinación del contexto de la organización	4.1
Procedimiento para identificación de requerimientos legales y normativos aplicables	4.2.2
Lista de requisitos legales, normativos y de otra índole	4.2.2
Alcance del SGCN (Sistema de gestión de la continuidad del negocio) y explicación de las exclusiones	4.3
Política de la continuidad del negocio	5.3
Objetivos de la continuidad del negocio	6.2
Competencias del personal	7.2
Comunicación con las partes interesadas	7.4
Proceso para análisis de impactos en el negocio y evaluación de riesgos	8.2.1
Resultados del análisis del impacto en el negocio	8.2.2
Resultados de la evaluación de riesgos	8.2.3
Procedimientos de la continuidad del negocio	8.4.1
Procedimientos de respuesta a incidentes	8.4.2
Decisión sobre si los riesgos e impactos se deben comunicar externamente	8.4.2
Comunicación con las partes interesadas, incluido el sistema nacional o regional de asesoramiento de riesgos	8.4.3
Registros de información importante sobre el incidente, medidas adoptadas y decisiones tomadas	8.4.3
Procedimientos para respuesta ante incidentes disruptivos	8.4.4
Procedimientos para restaurar y reiniciar actividades a partir de las medidas temporales	8.4.5
Resultados de las acciones que abordan tendencias o resultados adversos	9.1.1
Datos y resultados de seguimiento y medición	9.1.1
Resultados de la revisión posterior al incidente	9.1.2
Resultados de la auditoría interna	9.2
Resultados de la revisión por parte de la dirección	9.3
Naturaleza de las no conformidades y acciones tomadas	10.1
Resultados de acciones correctivas	10.1

Adaptado de (27001 Academy, 2014)

A pesar de que se deben tener estos registros y documentos presentados en la tabla anterior, hay que destacar que no significa que sean documentos rígidos o estáticos, por lo que esto no es una lista definitiva y pueden incorporarse (porque así lo permite la norma) cualquier otro documento que pueda mejorar el nivel de resistencia.

Tabla 35.

Otros documentos de uso no obligatorio para implementar la ISO 22301:2012

Documentos	Punto en ISO 22301:2012
Plan de implementación para alcanzar los objetivos de continuidad del negocio	6.2
Plan de capacitación y concienciación	7.2,7.3
Procedimiento para control de información documentada	7.5
Contratos y acuerdos de niveles de servicio (SLA) con proveedores y socios externos	8.1
Estrategia de la continuidad del negocio	8.3
Mitigación de riesgos	8.3.3
Escenarios de incidentes	8.5
Planes de prueba y verificación	8.5
Informes posteriores a las pruebas	8.5
Programa de mantenimiento del SGCN	9.1.1
Métodos para supervisión, medición, análisis y evaluación	9.1.1
Procedimiento para auditoría interna	9.2
Programa de auditoría interna	9.2
Procedimiento para medidas correctivas	10.1

Adaptado de (27001 Academy, 2014)

Estos son otros documentos de uso frecuente, aunque no son obligatorios para que pueda certificarse la organización. Se han de considerar diversas cuestiones como se indica en la ISO 22301:2012 (27001 Academy, 2014):

1- Determinación del contexto de la organización.
2- Procedimiento para identificación de documentos legales y normativos aplicables y lista de requisitos legales, normativos y de otra índole.
3- Alcance del SNG y explicación de las exclusiones.
4- Política y objetivos de la continuidad del negocio.
5- Plan d capacitación y concienciación, competencias del personal.
6- Comunicación de las partes interesadas.
7- Procedimiento para control de información documentada.
8- Contratos y acuerdos de niveles de servicio.
9- Proceso para análisis de impactos en el negocio y sus resultados.
10- Estrategia de la continuidad del negocio.
11- Mitigación de riesgo y plan de implementación para el logro de los objetivos.
12- Procedimientos para la continuidad del negocio.

13- Procedimientos de respuestas ante incidentes y registros sobre un incidente.
14- Procedimientos de comunicación.
15- Procedimientos para respuestas ante incidentes disruptivos.
16- Procedimientos para restaurar y reiniciar a partir de las medidas temporales.
17- Escenarios de incidentes.
18- Planes de prueba y verificación e informes posteriores.
19- Resultados de las acciones que abordan tendencias o resultados adversos.
20- Programa de mantenimiento de SGCN.
21- Métodos de supervisión, análisis, medición y evaluación.
22- Datos y resultados de seguimiento y evaluación.
23- Resultados de la revisión posterior al incidente.
24- Procedimientos programas y resultados de auditoría interna.
25- Resultados de la revisión por parte de dirección.
26- No conformidades y medidas correctivas (27001 Academy, 2014).

Como se ha visto anteriormente, son muchos los elementos que deben tenerse en cuenta para que la institución quede debidamente certificada acorde a la ISO 22301:2012. Estos requisitos deben ser establecidos antes de la implementación, para que los trabajadores y las partes interesadas se familiaricen en el contexto a desarrollar, tomando en consideración todos y cada uno de los aspectos, documentos y registros que se necesitan para la certificación.

4.7. Análisis de resultados

Como se ha podido observar en la investigación realizada se deja establecido el Plan de Continuidad del Negocio para el Banco ABC, para poder aminorar los daños que pueden traer consigo determinados eventos y que pueden afectar el bienestar de la organización.

La información confiable se ha convertido en uno de los recursos más importantes con los que cuenta cualquier organización, es por ello que trabajar para su resguardo y cuidado es imprescindible y trae consigo la perfección de los procesos.

En este trabajo, se lograron identificar los incidentes que pueden atentar contra los procesos, posibilitando identificar los tiempos críticos de recuperación y volver a la posición anterior a la catástrofe sin comprometer el negocio. La implementación del Plan representa una ventaja competitiva para la organización.

Se definieron y perfeccionaron aspectos, mediante un análisis del contexto, que permitieron definir las características de la organización, donde los principales servicios que ofrece como banca personal son, las cuentas de ahorro, la cuenta corriente, el crédito de consumo, las inversiones, el crédito automotriz y los servicios. En el caso de los servicios corporativos, se le incrementa el cash management y el factoring.

Se identificaron los procesos y subprocesos del Banco ABC. Sus macroprocesos, son la gestión estratégica, la gestión de gobierno corporativo, la gestión integral del riesgo, la gestión de prevención de lavado de activos y financiamiento del terrorismo y otros delitos, la gestión de marketing, la gestión de negocios, la gestión de tesorería, la gestión de servicio al cliente, la gestión del talento humano, la gestión tecnológica y telecomunicaciones, la gestión financiera, la gestión administrativa, la gestión de asesoría jurídica, la gestión de auditoría, la gestión de procesos, la gestión de cobranzas y la gestión de operaciones, cada uno de los cuales tiene un procesos y un subproceso.

Se determinaron los recursos de soporte de los procesos críticos, el tiempo de recuperación objetivo y punto de recuperación objetivo. Donde el TRO es el que establece la urgencia de las diferentes unidades del negocio y el RPO determina el punto más reciente en el tiempo en que los sistemas puedan ser recuperados.

Se identificaron los riesgos más relevantes con respecto al funcionamiento de la organización como lo son la instalación de dispositivos no autorizados en la red interna, el robo de identidad utilizando simuladores de sitios web, mensajes de correo u otros actos de ingeniería social. Otros de los riesgos pueden ser interrupciones o fluctuaciones del servicio eléctrico, daños de los componentes de las telecomunicaciones, daño o fallo en el banco de transformadores del edifico matriz y fallos en el disco donde está ubicada la base de datos de la entidad.

Se identificaron los controles para cada una de las amenazas mediante la matriz de calificación de riesgos, donde la gerencia de la organización puede apoyarse para saber en qué sentido darles prioridad a dichos riesgos detectados, mediante la guía de calificación para la probabilidad de ocurrencia de los mismos.

Posteriormente se realizó la proyección del BCP, determinando su alcance, las políticas en las que se basa y se determinaron sus objetivos y los requisitos para su puesta en marcha. Se presenta además una estrategia de mitigación y los procedimientos de declaración de emergencias.

En este trabajo también se establecieron los informes que resultan de los análisis y verificaciones realizadas. Queda establecido un plan de mantenimiento para la organización y una propuesta de mejoras que hacen posible la perfección del sistema propuesto e implementado.

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

Con el detalle de las características fundamentales de las instituciones financieras del sector privado en Ecuador, se establecieron los principales flagelos y riesgos del tipo tecnológico a los que están sometidas estas empresas y maneras de no verse afectadas por los mismos.

Las amenazas y los riesgos, fueron identificados satisfactoriamente, lo cual asegura la prevención de los daños, así como las posibles pérdidas que pueden traer consigo la ocurrencia de desastres en el Banco ABC, lo cual hace posible un manejo más eficiente de los recursos, tanto materiales como humanos y por ende continuar trabajando para ser más competitivos frente a otras organizaciones que tiene actividades y procesos semejantes a los suyos.

Para establecer la metodología propuesta se tuvieron en cuenta los estándares internacionales que se consideran a la hora de implementar un Plan de Continuidad del Negocio, como por ejemplo lo estipulado en las normas ISO.

Con el diseño del plan de continuidad del negocio adaptado al Banco ABC, que es el caso de estudio correspondiente a este trabajo, se demuestran las imperfecciones de los procesos actuales y la forma en que pueden ser rediseñados o reelaborados, para disminuir las consecuencias que la ocurrencia de eventos inesperados pueda traer consigo.

Se establecieron acciones para la perfección constante del plan de continuidad de negocios, como lo son, su verificación y control, así como un plan de mantenimiento que ajusta cada una de las problemáticas detectadas a soluciones precisas, y el responsable para que se cumpla en cada una de ellas, a partir de lo cual también se establecen propuestas de mejora continua, todo ello en correspondencia con las normas de calidad.

5.2. Recomendaciones

Mantener un monitoreo constante en la entidad, de la ocurrencia de los principales riesgos que se han detectado en la presente investigación.

Prevenir con anterioridad las pérdidas que pueden ocasionarse por la incidencia de fenómenos que agraven los procesos, para ello se recomienda el uso de la matriz de calificación del nivel de riesgo, que se propone en el trabajo y que ella se convierta en una herramienta de uso permanente en el Banco ABC.

Desarrollar las acciones de verificación y control establecidas en el modelo para el Banco ABC, y su plan de mantenimiento, vertiendo cada uno de los resultados en el informe de las incidencias donde se muestren las pruebas ejecutadas y lo que se recomienda para cada uno de los problemas que se detecten.

Utilizar el modelo de Plan de Continuidad del Negocio basado en las normas ISO 22301:2012, que ha sido diseñado para el caso de estudio, de modo que se perfeccione el trabajo de las entidades financieras de Ecuador y su implementación en tantas como sea posible.

REFERENCIAS

SGSI. (2015). Gestión de la Información. Recuperado el 19 de octubre de 2016, de Blog de Sistema de Gestión de la Información: http://www.pmg-ssi.com/2015/10/iso-22301-2012-sistema-gestion-continuidad-negocio/.

27001 Academy. (2014). *Informe: Lista de documentación obligatoria para ISO 22301.* Bogotá: Academy.

Alcarraz, G. (2014). Como lograr Aseguramiento de TI utilizando COBIT 5. *CLAIN 2014. XVIII Congreso latinoamericano de auditoria interna y evaluacion de riesgos.* Bueos Aires: Independiente.

Alexander, A. (2007). *Diseño y Gestión de un Sistema de Seguridad de la Información.* Colombia: Alfa.

Alexander, A. (2012). *Nuevo Estándar Internacional en Continuidad del Negocio.* Recuperado el 19 de noviembre de 2016, de Herramientas Gerenciales: http://gestion.com.do/pdf/018/018-nuevo-estandar-internacional.pdf.

Banco Capital . (2015). *Metodología para la implementación de los procesos críticos .* Quito: El Banco Impulso.

Banco Capital . (2015). *Plan de Continuidad del Negocio BCP .* Quito: Banco Capital.

Banco Capital. (2015). *Matriz de Riesgos.* Quito: Banco Capital.

Banco Capital. (2016). *Banca en línea*. Recuperado de Banca en línea: https://www.bancocapital.com/conocenos/historia.html.

Basel Committee on Banking Supervision. (2005). *Bank For International Settlements.* s.c.: International Convergence of Capital Measurement and Capital Standars.

BCI. (2013). *The Good Practice Guidelines*. Recuperado de BCI: http://www.thebci.org/index.php/resources/the-good-practice-guidelines.

Béjar R. (2013). *La importancia de implementar un Plan de Continuidad de Negocios .* México.

Bello, J. (2008). BS 25999, la nueva norma para Sistemas de Gestión de la Continuidad del Negocio. *Calidad Q*, 16-19.

Blanco E. (2008). *Plan de continuidad para lograr la eficacia Escolar en México.* México.

Blanco, S. (2008). *BS25999-1: Gestión de la Continuidad del Negocio.* Recuperado el 18 de noviembre de 2016, de Marble Station: https://www.marblestation.com/?p=650.

BSI GROUP. (2007). *Business Continuity Management. Specification (BS 25999-2: 2007).* Londres: BSI.

Business Continuity Institute. (2013). *ISO 22301: Guía de Buenas Prácticas 2013*. Recuperado el 22 de noviembre de 2016, de ISO 22301 Sistemas de Gestión & Continuidad del Negocio: http://normaiso22301.com/bci-business-continuity-institute-ha-publicado-la-ultima-edicion-de-la-guia-de-buenas-practicas-gpg/.

Cañas, L. E. (2009). Gestión de riesgos de negocios. desarrollo e implementación de Sistemas de gestión de riesgos. *Documentos Ocacionales* .

Castro, A. R. (2011). Gestion de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *Artículos de Investigación*, 56-66.

Código Orgánico Monetario y Financiero. (2014). *Segundo suplemento .* Quito : Asamblea Nacional República de Ecuador .

Cubadebate. (2016). *Terremoto en Ecuador provoca pérdidas por tres mil millones de dólares (Fotos)*. Recuperado de Cuba debate: http://www.cubadebate.cu/noticias/2016/04/19/terremoto-en-ecuador-provoca-perdidas-por-tres-mil-millones-de-dolares-fotos/.

Echemendía, B. (2010). *Definiciones acerca del riesgo y sus implicaciones*. Recuperado de Scielo: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1561-30032011000300014.

El Comercio. (2016). Ecuador recibió USD 12,9 millones en donaciones de países tras sismo. *El Comercio*.

Espasa Calpe. (1995). Diccionario de la Lengua Española [CD-ROM]. Versión 21.1.0. Riesgo. Madrid, Madrid, España.

Estándar Internacional ISO 22301. (2012). *Seguridad de la Sociedad: Sistemas de continuidad del Negocio-Requisitos.*

Estupiñan, R. (2006). *Administración de riesgos ERM y la auditoria interna.* Bogotá: Ecoe Ediciones.

Estupiñan, R. (2007). *Administración o Gestión de Riesgos E.R.M. y la Auditoria Interna.* Colombia: Ecoe ediciones Ltda.

FNPA. (2016). *NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity/Continuity of Operations Programs*. Recuperado de FNPA: http://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards?mode=code&code=1600.

Gonzalez L. (2012). *Factores que inciden en el riesgo operacional de fraude de la banca universal del municipio maracaibo.* Maracaibo.

Gualim, N. (2014). *Plan de acción para minimizar la exposición al riesgo tecnológico de una pyme basada en el marco de referencia risk it.*

Recuperado de USAC: http://biblioteca.usac.edu.gt/tesis/08/08_0788_CS.pdf.

Hamidovic, H. (2011). An Introduction to ICT Continuity Based on BS 25777. *ISACA Journal, 2*, 1-5.

Hidalgo, A. (2004). *Una introducción a la gestión de riesgos tecnológicos*. Recuperado de Madrimasd: http://www.madrimasd.org/revista/revista23/tribuna/tribuna1.asp.

Hogart, R. (s.f.). Recuperado el 8 de agosto de 2016, de http://www.cholonautas.edu.pe/modulo/upload/Segur.pdf.

Hogarth, R. (2006). *Los seguros y la seguridad después del 11 de Septiembre: ¿Acaso el mundo se ha vuelto un lugar más "riesgoso"?* Recuperado de Cholonautas: http://www.cholonautas.edu.pe/modulo/upload/Segur.pdf.

ISACA. (2012). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Recuperado el 21 de noviembre de 2016, de ISACA: http://www.isaca.org/COBIT/Pages/default.aspx.

ISACA. (2012). *COBIT 5*. Recuperado de ISACA: http://www.isaca.org/COBIT/Pages/default.aspx

ISO. (2011). *ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management*. Recuperado de ISO: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56742.

ISO. (2012). *ISO 22301:2012 Societal security -- Business continuity management systems --- Requirements*. Recuperado de ISO: http://www.iso.org/iso/catalogue_detail?csnumber=50038.

ITEAM. (2014). *Plan de Continuidad de Negocio*. Recuperado de ITEAM: http://iteamgroupcorp.com/index.php/es/.

Junta Bancaria del Ecuador. (2014). *Resolución JB-2014-3066.* Quito: s.e.

Junta de Andalucía. Consejería de salud. (2010). *Diccionario de divulgación, Riesgo*. Recuperado de Observatorio de Salud y Medio Ambiente de Andalucía: http://www.osman.es/ficha/13931.

López, R. (2012). *Innovación del Modelo de Negocios .* Madrid: Universidad Autónoma de Madrid.

Mendoza, M. (2014). *Business Impact Analysis (BIA) y la importancia de priorizar procesos*. Recuperado de Welivesecurity: http://www.welivesecurity.com/la-es/2014/11/06/business-impact-analysis-bia/.

Meza, N. (2009). *¿Qué es un plan de continuidad de negocio?* Recuperado de Entrepreneur: https://www.entrepreneur.com/article/262893.

Montenegro, G. (2013). *Riesgos Tecnologicos para Banca*. Recuperado de Prezi: https://prezi.com/qnb6avdkxoos/riesgos-tecnologicos-para-banca/

Motta, G. (2006). *Importancia de la planeacióm de la continuidad de negocio.* Bogotá: s.e.

Muñoz, R. (2012). *Caracterización de Procesos de Gestión de TI basados en COBIT 5 y mapeo con ISO27002, ITIL, CMMI DEV, PMBOK, para la implementación en la industria Editorial Colombiana, apoyando el proceso de transformación digital.* Santiago de Cali: ICESI.

Narvaez, H. (2016). *Modelo de Gobierno de TI para la gestión de la empresa SAITEL Matriz Ibarra.* Ibarra.

OSIATIS. (2013). *Fundamentos de la Gestión TI*. Recuperado de Econocom: http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php.

Osores, M. (2014). *Principios de COBIT 5 para el gobierno efectivo de TI*. Recuperado el 20 de noviembre de 2016, de TechTarget: http://searchdatacenter.techtarget.com/es/cronica/Principios-de-COBIT-5-para-el-gobierno-efectivo-de-TI.

Palacios, J. (2016). *Primer dominio Entrega,Servicio y Soporte DSS.*

Peña, L. (2013). *Guía metodológica para la elaboración de un Plan de Continuidad de Negocios en entidades estatales.* Bogotá: Escuela Colombiana de Ingeniería Julio Garavito.

Plan Nacional del Buen Vivir. (2013). *Buen vivir.* Quito : Gobierno Nacional de la República de Ecuador .

Ramirez, A., & Ortiz, Z. (2011). Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *Ingeniería, 6*(2), 56-66.

Sáez V. (2015). *“Modelo integral para la implementacion de un Plan de Continuidad de Negocio en Chile".* Chile.

Sáez, V. (2011). *Modelo Integral para la implementación de un Plan de Continuidad de Negocio en Chile .* Puerto Montt: universidad Austral de Chile .

Sanchéz, M. (2013). *Peores escenarios de riesgo tecnológico en el e-commerce: guía para el comité de dirección*. Recuperado de Security Advisors: https://ssa-asesores.es/wordpress/blog/2013/09/16/peores-escenarios-de-riesgo-tecnologico-en-el-e-commerce-guia-para-el-comite-de-direccion/.

Serrano, R. (2013). *La importancia de implementar un Plan de Continuidad de Negocios (1ra parte)*. Recuperado de Dinero en imagen: http://www.dineroenimagen.com/2013-07-01/22403

Shahrawat, D. (2004). *Perceptions On BCP in The Securities Industries.* New York: SIA BC Conference Exhibit.

Sun Gard Availability Services (SGAS). (2005). *Business Impact Analysis (BIA).* Connecticut: Connecticut Community Colleges.

Superintendencia de Bancos y Seguros. (2004). *Resolución JB-2004-631.* Quito: s.e.

Superintendencia de Bancos y Seguros. (2005). *Resolución JB-2005-834 de la gestión y administración de riesgos operativos.* Quito: s.e.

Woodman, P. (2007). *Business Continuity Management.* Reino Unido: Chartered Management .

ANEXOS

Anexo 1- Lista de aspectos verificados

Nro	Aspectos verificados.
1	Compromiso formal del Consejo de la administración y la alta gerencia con el cumplimiento del BPC.
2	Observar la funcionabilidad de las tecnologías de la información y su alineación con el plan estratégico de la organización.
3	Verificar que exista un responsable de la información que se encargue de definir y autorizar formalmente los accesos y cambios funcionales, así como monitorear las necesidades de crecimiento de la organización.
4	Comprobar que existe un responsable de la información y que al mismo tiempo se encargue de definir y autorizar de manera formal los cambios funcionales, así como monitorear el cumplimiento de los controles establecidos.
5	Comprobar que las políticas, los procesos y los procedimientos de la tecnología de la información estén definidos bajo estándares de general aceptación y que garanticen la eficacia de los controles internos.
6	Verificar que se difunden dentro del personal involucrado todas las políticas que se requieren y los procedimientos que aseguren su implementación.
7	Observar si se realiza capacitación y entrenamiento al personal del área de tecnología de la información y a los usuarios de la misma.
8	Deben existir manuales y reglamentos internos que estén aprobados por el consejo de la administración, donde se establezcan los niveles de responsabilidad y proceder para cada operación.
9	Comprobar la existencia de la clasificación y control de los activos de la

	tecnología de la información, que incluya los registros e identificación, así como los responsables de su uso.
10	Verificar la existencia de requerimientos contractuales convenidos que establezcan la propiedad de la información y la responsabilidad de la empresa proveedora de la tecnología, en el caso de que sus sistemas sean vulnerables.
11	Observar las políticas y procedimientos de seguridad de la información y que sus objetivos están bien definidos, las normas, los principios, los requisitos y las responsabilidades ante la ocurrencia de incidentes y su comunicación.
12	Observar el funcionamiento de los requerimientos de seguridad que están vinculados con la tecnología de la información, requisitos legales y contractuales.
13	Comprobar que existen los controles necesarios que aseguran la integridad, la disponibilidad y la confidencialidad de la información.
14	Debe existir un sistema de seguridad de acceso a la información donde se definan las facultades y atributos de los usuarios, desde el registro, eliminación y modificación de los controles necesarios que permitan verificar su cumplimiento en todos los ambientes de procesamiento.
15	Deben estar establecidos los niveles de autorización de acceso y ejecución de las funciones del procesamiento de las aplicaciones, mediante el cual se garantice la desagregación de funciones.
16	Se deben comprobar los accesos para evitar los no autorizados.
17	Determinar la existencia de controles adecuados que permitan la identificación de software no autorizados o sin la respectiva licencia.
18	Verificar la existencia de controles para la documentación, medios de

	almacenamiento y otros dispositivos externos, posibles robos y daños.
19	Observar que se mantiene una buena infraestructura, con áreas protegidas, donde se evite la entrada de personal no autorizado.
20	Deben existir planes elaborados para que el desempeño del sistema de administración de la seguridad de la información sea el correcto y en correspondencia a los objetivos de la entidad.
21	Verificar la existencia de políticas y procedimientos que garanticen que solo las personas designadas tengan acceso a ellas.

Anexo 2- Matriz de calificación de procesos críticos

Macroproceso	Proceso	Subproceso	Responsable	Proceso de Cara al Cliente	Proceso de Producto Específico	Proceso con volumen monetario significativo	Proceso para cumplimiento regulatorio	Proceso con alta transaccionalidad	Total	Criticidad
				Calificación	Calificación	Calificación	Calificación	Calificación		
GESTIÓN DE NEGOCIO	GESTIÓN DE CAPTACIONES	APERTURA DE CUENTAS CORRIENTES	NEGOCIOS	5	5	3	2	4	19	Vital
		CIERRE DE CUENTAS CORRIENTES	NEGOCIOS	5	5	3	2	3	18	Vital
		SOBREGIROS	NEGOCIOS	5	4	3	2	3	17	Vital
		APERTURA DE CUENTAS DE AHORRO	NEGOCIOS	5	5	3	2	4	19	Vital
		APERTURA DE CUENTAS DE AHORRO CREDITO AUTOMOTRIZ	NEGOCIOS	5	5	3	2	4	19	Vital
		CIERRE DE CUENTAS DE AHORRO	NEGOCIOS	5	3	4	2	3	17	Vital
		APERTURA DE INVERSIONES A PLAZO	NEGOCIOS	5	5	5	5	5	25	Crítico
		RENOVACION DE INVERSIONES A PLAZO	NEGOCIOS	5	5	5	5	5	25	Crítico
		CANCELACION - PRECANCELACION INVERSIONES A PLAZO	NEGOCIOS	5	5	5	5	5	25	Crítico
		ENDOSO DE CERTIFICADOS DE DEPÓSITO	NEGOCIOS	5	4	4	3	3	19	Vital
		NEGOCIACIÓN CASH MANAGEMENT	NEGOCIOS	3	4	4	3	4	18	Vital

Macroproceso	Proceso	Subproceso	Responsable	Proceso de Cara al Cliente	Proceso de Producto Específico	Proceso con volumen monetario significativo	Proceso para cumplimiento regulatorio	Proceso con alta transaccionalidad	Total	Criticidad
				Calificación	Calificación	Calificación	Calificación	Calificación		
GESTIÓN DE NEGOCIO	GESTIÓN DE COLOCACIONES	CONCESION CRÉDITO CANAL AUTIOMOTRIZ	CRÉDITO	5	5	5	3	5	23	Crítico
		CONCESION CRÉDITO CANAL BANCA	CRÉDITO	5	5	4	3	5	22	Crítico
GESTIÓN TECNOLÓGICA Y TELECOMUNICACIONES	ADMINISTRACION, MANTENIMIENTO Y CONTROL DEL DESARROLLO DE APLICACIONES	DESARROLLOS DE SISTEMAS	TECNOLOGÍA	1	1	2	4	4	12	Sensitivo
		DISEÑO DE PÁGINAS WEB	TECNOLOGÍA	1	1	3	4	4	13	Sensitivo
		COMPRA DE HERRAMIENTAS DE DESARROLLO	TECNOLOGÍA	1	1	3	3	3	11	Sensitivo
		ADMINISTRACIÓN DE LA CALIDAD DE LOS PROYECTOS	TECNOLOGÍA	1	1	4	5	4	15	Sensitivo
		CONTROL DE VERSIONAMIENTO DE DESAROLLO	TECNOLOGÍA	1	1	4	4	4	14	Sensitivo
		SEGUIMIENTO DEL DESARROLLO DEL CICLO DE VIDA DE LAS APLICACIONES	TECNOLOGÍA	1	1	2	4	4	12	Sensitivo
	ORGANIZACIÓN DE TI	SEGUIMIENTO DE PROYECTOS DE SISTEMAS	TECNOLOGÍA	1	1	3	4	1	10	Sensitivo
		MONITOREO DE SERVICIOS (*)	TECNOLOGÍA	2	3	3	4	5	17	Vital
		MONITOREO DEL CUMPLIMIENTO DEL PRESUPUESTO ASIGNADO	TECNOLOGÍA	1	2	5	2	2	12	Sensitivo
	ADMINISTRACIÓN, MANTENIMIENTO CONTROL DE TI	COMPRA DE SOFTWARE DE TERCEROS	TECNOLOGÍA	1	1	4	3	3	12	Sensitivo
		TRANSFERENCIA TECNOLOGICA DE SOFTWARE DE TERCEROS	TECNOLOGÍA	1	1	3	1	4	10	Sensitivo
		GENERACIÓN DE RESPALDOS (*)	TECNOLOGÍA	1	2	3	5	3	14	Sensitivo
		CREACIÓN Y MANTENIMIENTO DE AMBIENTES T24	TECNOLOGÍA	1	1	3	2	1	8	Deseable

Macroproceso	Proceso	Subproceso	Responsable	Proceso de Cara al Cliente	Proceso de Producto Específico	Proceso con volumen monetario significativo	Proceso para cumplimiento regulatorio	Proceso con alta transaccionalidad	Total	Criticidad
				Calificación	Calificación	Calificación	Calificación	Calificación		
GESTIÓN TECNOLÓGICA Y TELECOMUNICACIONES	ADMINISTRACIÓN, MANTENIMIENTO CONTROL DE TI	MANTENIMIENTO DE LAS BASES DE DATOS SQL (*)	TECNOLOGÍA	1	1	5	3	4	14	Sensitivo
		PASO DE PROGRAMAS A PRODUCCIÓN	TECNOLOGÍA	1	1	2	3	2	9	Deseable
		PASOS A PRODUCCION EMERGENTES	TECNOLOGÍA	1	1	2	3	2	9	Deseable
		CREACIÓN, MANTENIMIENTO Y ELIMINACIÓN DE USUARIOS (*)	TECNOLOGÍA	1	1	2	5	2	11	Sensitivo
		MANTENIMIENTO DE CLAVES DE ACCESO A SERVIDORES (*)	TECNOLOGÍA	1	1	2	4	2	10	Sensitivo
		CONTROL DE INVENTARIO DE HARDWARE	TECNOLOGÍA	1	1	3	5	2	12	Sensitivo
		CONTROL DE INVENTARIO DE SOFTWARE	TECNOLOGÍA	1	1	3	5	2	12	Sensitivo
		PROTECCIÓN A EQUIPOS DE VIRUS INFORMÁTICOS (*)	TECNOLOGÍA	1	1	4	5	4	15	Sensitivo
		CONTROL DE DIFUSIÓN DE SOFTWARE PIRATA	TECNOLOGÍA	1	1	4	5	2	13	Sensitivo
		ACTUALIZACIONES (PARCHES) DE SOFTWARE EN PRODUCCIÓN	TECNOLOGÍA	1	1	3	3	3	11	Sensitivo
		REVISIÓN PERIÓDICA DE LOS DERECHOS DE USUARIO	TECNOLOGÍA	1	1	1	4	2	9	Deseable
		REVISIÓN PERIÓDICA DE VIRUS	TECNOLOGÍA	1	1	4	5	4	15	Sensitivo
		APLICACIÓN DE SEGURIDAD	TECNOLOGÍA	1	1	4	3	4	13	Sensitivo
		REPORTE DE PROBLEMAS AL DEPARTAMENTO DE SOPORTE DEL DEPARTAMENTO DE SISTEMAS	TECNOLOGÍA	1	1	4	5	5	16	Vital
		REPORTE DE ERRORES EN T24 CON SOPORTE EXTERNO DEL PROVEEDOR (*)	TECNOLOGÍA	1	1	5	4	4	15	Sensitivo

Macroproceso	Proceso	Subproceso	Responsable	Proceso de Cara al Cliente	Proceso de Producto Específico	Proceso con volumen monetario significativo	Proceso para cumplimiento regulatorio	Proceso con alta transaccionalidad	Total	Criticidad
				Calificación	Calificación	Calificación	Calificación	Calificación		
GESTIÓN TECNOLÓGICA Y TELECOMUNICACIONES	ADMINISTRACIÓN, MANTENIMIENTO CONTROL DE TI	SELECCIÓN Y ADQUISICIÓN DE HARDWARE Y SOFTWARE	TECNOLOGÍA	1	1	5	3	3	13	Sensitivo
		ADMINISTRACIÓN Y MONITOREO DE RED (*)	TECNOLOGÍA	1	1	4	4	4	14	Sensitivo
		REVISION DE DESEMPEÑO - CAPACIDAD Y DISPONIBILIDAD DE RECURSOS INFORMÁTICOS	TECNOLOGÍA	1	1	4	4	4	14	Sensitivo
		EVALUACIÓN DEL DESEMPEÑO DEL SISTEMA	TECNOLOGÍA	1	1	4	4	4	14	Sensitivo
		ADMINISTRACIÓN DE CONFIGURACIONES DE LA INFRAESTRUCTURA TECNOLOGICA.	TECNOLOGÍA	1	1	4	4	4	14	Sensitivo
		ADMINISTRACION DEL PROCESO DE EXTERNALIZACION O DE CONSULTORIA	TECNOLOGÍA	1	1	5	3	2	12	Sensitivo
		VALIDACION DE RESPALDOS DEL CORE DEL BANCO (*)	TECNOLOGÍA	1	1	2	4	3	11	Sensitivo
		RESPALDOS DE INFORMACION DE USUARIOS	TECNOLOGÍA	1	1	4	3	3	12	Sensitivo
		MANTENIMIENTO DE HARDWARE (EQUIPOS FINALES DE USUARIO)	TECNOLOGÍA	1	1	3	4	4	13	Sensitivo
		DESTRUCCION DE RESPALDOS CORE BANCARIO Y BASES DE DATOS	TECNOLOGÍA	1	1	2	4	1	9	Deseable
		REDIMENSION DE TABLAS (RESIZE)	TECNOLOGÍA	1	1	3	2	3	10	Sensitivo
		DEFINICIÓN DE ACUERDO DE NIVELES DE SERVICIO	TECNOLOGÍA	1	1	4	4	4	14	Sensitivo
		VALIDACIÓN DE RESPALDOS ANTIGUOS	TECNOLOGÍA	1	1	4	4	3	13	Sensitivo
		EJECUCIÓN DEL CIERRE DEL SISTEMA (*)	TECNOLOGÍA	1	1	4	5	5	16	Vital
		VALIDACIÓN DEL PROCESO DE REDIMENSIONAMIENTO DE TABLAS EN EL SISTEMA CORE T24	TECNOLOGÍA	1	1	3	2	3	10	Sensitivo
GESTIÓN ESTRATÉGICA	PLANIFICACIÓN ESTRATÉGICA	ACTUALIZACIÓN DEL PLAN ESTRATÉGICO	PRESIDENCIA EJECUTIVA	1	1	1	5	1	9	Deseable

Macroproceso	Proceso	Subproceso	Responsable	Proceso de Cara al Cliente	Proceso de Producto Específico	Proceso con volumen monetario significativo	Proceso para cumplimiento regulatorio	Proceso con alta transaccionalidad	Total	Criticidad
				Calificación	Calificación	Calificación	Calificación	Calificación		
GESTIÓN ESTRATÉGICA	PLANIFICACIÓN ESTRATÉGICA	ELABORACIÓN Y ACTUALIZACIÓN DEL PLAN OPERATIVO ANUAL	PRESIDENCIA EJECUTIVA	1	1	1	4	1	8	Deseable
		EJECUCIÓN Y EVALUACIÓN DE PLANES OPERATIVOS	PRESIDENCIA EJECUTIVA	1	1	1	4	1	8	Deseable
		DIFUSIÓN DE RESULTADOS DE PLANIFICACIÓN INSTITUCIONAL	PRESIDENCIA EJECUTIVA	1	1	1	4	1	8	Deseable
		SEGUIMIENTO Y EVALUACIÓN DE PLAN ESTRATÉGICO	PRESIDENCIA EJECUTIVA	1	1	1	4	1	8	Deseable
	PLANIFICACIÓN FINANCIERA	ELABORACIÓN DE PRESUPUESTO GENERAL	PRESIDENCIA EJECUTIVA	1	1	1	3	1	7	Deseable
		SEGUIMIENTO Y EVALUACIÓN DEL PRESUPUESTO GENERAL	PRESIDENCIA EJECUTIVA	1	1	1	3	1	7	Deseable
		CÁLCULO Y ANÁLISIS DE INDICADORES FINANCIEROS	PRESIDENCIA EJECUTIVA	1	1	1	3	1	7	Deseable
	PLANIFICACIÓN COMERCIAL	ELABORACIÓN DEL PLAN DE NEGOCIOS	PRESIDENCIA EJECUTIVA	1	5	1	4	1	12	Sensitivo
		SEGUIMIENTO Y EVALUACIÓN DEL PLAN DE NEGOCIOS	PRESIDENCIA EJECUTIVA	1	5	1	2	1	10	Sensitivo
GESTIÓN DE GOBIERNO CORPORATIVO	TRANSPARENCIA DE LA INFORMACIÓN	EMISIÓN DE RESOLUCIONES DEL DIRECTORIO	DIRECTORIO	1	1	1	5	1	9	Deseable
	GESTIÓN DE LA ADMINISTRACIÓN INSTITUCIONAL	NOMBRAMIENTO DE PRESIDENTE DIGNIDADES Y SUCESIÓN DE EJECUTIVOS	DIRECTORIO	1	1	1	2	1	6	Deseable
		CREACIÓN Y ACTUALIZACIÓN DE REGLAMENTOS INTERNOS	PRESIDENCIA EJECUTIVA	1	1	1	2	1	6	Deseable
		ELABORACIÓN Y ACTUALIZACIÓN DE MANUALES REQUERIDOS POR ORGANISMOS EXTERNOS	PRESIDENCIA EJECUTIVA	1	1	1	3	1	7	Deseable
		ACTUALIZACIÓN ORGANIGRAMAS Y ORGÁNICO FUNCIONAL	PRESIDENCIA EJECUTIVA	1	1	1	3	1	7	Deseable

Macroproceso	Proceso	Subproceso	Responsable	Proceso de Cara al Cliente	Proceso de Producto Específico	Proceso con volumen monetario significativo	Proceso para cumplimiento regulatorio	Proceso con alta transaccionalidad	Total	Criticidad
				Calificación	Calificación	Calificación	Calificación	Calificación		
GESTIÓN INTEGRAL DE RIESGO	ADMINISTRACIÓN DE RIESGOS	ADMINISTRACIÓN DE RIESGO DE CRÉDITO (CONSIDERAR SEGUIMIENTO Y CONTROL DE GARANTIAS)	RIESGOS	1	3	1	5	1	11	Sensitivo
		ADMINISTRACIÓN DE RIESGO DE MERCADO Y LIQUIDEZ	RIESGOS	1	1	1	5	1	9	Deseable
		ADMINISTRACIÓN DE RIESGO OPERATIVO	RIESGOS	1	1	1	5	1	9	Deseable
	CALIFICACIÓN DE RIESGOS	CALIFICACIÓN DE ACTIVOS DE RIESGOS	RIESGOS	1	1	1	5	1	9	Deseable
		ADMINSTRACION DE SEGURIDAD DE LA INFORMACION (CASH MANAGEMENT)	RIESGOS	1	1	1	3	1	7	Deseable
	ADMINISTRACIÓN DE PLANES DE CONTINGENCIAS Y CONTINUIDAD	ADMINISTRACIÓN DE LA CONTINUIDAD DEL NEGOCIO	RIESGOS	1	1	1	5	1	9	Deseable
	SEGURIDAD Y CONTROL DE INFORMACIÓN.	ADMINSTRACION DE SEGURIDAD DE LA INFORMACION	RIESGOS	1	1	1	5	1	9	Deseable
GESTIÓN DE PREVENCIÓN DE LAVADO DE ACTIVOS Y FINANCIAMIENTO DEL TERRORISMO Y OTROS DELITOS	GESTIÓN DEL PROGRAMA DE PREVENCIÓN Y CONTROL DE LAVADO DE ACTIVOS Y FINANCIAMIENTO DEL TERRORISMO Y OTROS DÉLITOS	ELABORACIÓN, ACTUALIZACIÓN Y DIFUSIÓN DEL MANUAL DE CONTROL INTERNO PARA PREVENCIÓN DE LAVADO DE ACTIVOS, FINANCIAMIENTO DEL TERRORISMO Y OTROS DELITOS	CUMPLIMIENTO	1	1	3	5	5	15	Sensitivo
		DEBIDA DILIGENCIA	CUMPLIMIENTO	1	1	5	5	5	17	Vital
		INDUCCIÓN Y CAPACITACIÓN EN TEMAS DE PREVENCIÓN DE LAVADO DE ACTIVOS FINANCIAMIENTO DEL TERRORISMO Y OTROS DELITOS	CUMPLIMIENTO	1	1	5	4	5	16	Vital
	GESTION DE REPORTES	ELABORACIÓN Y ENVIO DE INFORMES A ORGANISMOS DE CONTROL	CUMPLIMIENTO	1	1	5	5	5	17	Vital
		ELABORACIÓN DEL PLAN ANUAL DE TRABAJO, PLAN ANUAL DE CAPACITACIÓN PARA EL NUEVO AÑO; (INFORME DEL CUMPLIMIENTO DE OBJETIVOS, E INFORME DE CAPACITACIÓN DEL AÑO INMEDIATO ANTERIOR E PARA ENVIO A ORGANISMOS DE CONTROL)	CUMPLIMIENTO	1	1	5	5	5	17	Vital

Macroproceso	Proceso	Subproceso	Responsable	Proceso de Cara al Cliente	Proceso de Producto Específico	Proceso con volumen monetario significativo	Proceso para cumplimiento regulatorio	Proceso con alta transaccionalidad	Total	Criticidad
				Calificación	Calificación	Calificación	Calificación	Calificación		
GESTIÓN DE PREVENCIÓN DE LAVADO DE ACTIVOS Y FINANCIAMIENTO DEL TERRORISMO Y OTROS DELITOS	GESTIÓN DE MONITOREO	PROTOCOLO DE LISTAS DE OBSERVADOS	CUMPLIMIENTO	1	1	5	5	5	17	Vital
		ACTUALIZACIÓN DE LA BASES DE DATOS DE LISTAS RESERVADAS	CUMPLIMIENTO	1	1	5	5	5	17	Vital
GESTIÓN DE MARKETING	ADMINISTRACIÓN DE PRODUCTOS	DESARROLLO DE INVESTIGACIONES DE MERCADO Y DIFUSIÓN DE RESULTADOS.	MARKETING	1	3	1	3	4	12	Sensitivo
		DEFINICIÓN, DISEÑO E IMPLEMENTACIÓN DE NUEVOS PRODUCTOS Y SERVICIOS	MARKETING	1	3	4	2	5	15	Sensitivo
		MANTENIMIENTO, MODIFICACION , ELIMINACION DE PRODUCTOS Y SERVICIOS.	MARKETING	1	2	4	2	5	14	Sensitivo
		IMPLEMENTACIÓN DE TARIFAS DIFERENCIADAS	MARKETING	2	2	5	5	5	19	Vital
		DESARROLLO, SEGUIMIENTO Y EVALUACIÓN DE CAMPAÑAS	MARKETING	1	2	3	1	2	9	Deseable
	CALIDAD DE SERVICIO E INFORMACIÓN	ADMINMISTRACION DE CANALES VIRTUALES Y TELEFONICOS	MARKETING	1	2	3	5	5	16	Vital
		MANTEMINIENTO Y ACTUALIZACION BASE DE DATOS	MARKETING	2	1	3	5	3	14	Sensitivo
		ANCLAJE DE ASESORES A CLIENTES	MARKETING	2	2	3	2	3	12	Sensitivo
	IMAGEN INSTITUCIONAL	MODELAMIENTO DE LA IMAGEN CORPORATIVA	MARKETING	1	1	2	1	5	10	Sensitivo
		DESARROLLO DE CAMPAÑAS DE COMUNICACIÓN INSTITUCIONAL INTERNA Y EXTERNA	MARKETING	2	1	1	2	2	8	Deseable
GESTIÓN DE NEGOCIO	GESTIÓN DE COLOCACIONES	DESPIGNORACION	CRÉDITO	3	3	3	3	3	15	Sensitivo
		FACTORING	CRÉDITO	3	3	3	3	2	14	Sensitivo

Macroproceso	Proceso	Subproceso	Responsable	Proceso de Cara al Cliente	Proceso de Producto Específico	Proceso con volumen monetario significativo	Proceso para cumplimiento regulatorio	Proceso con alta transaccionalidad	Total	Criticidad
				Calificación	Calificación	Calificación	Calificación	Calificación		
GESTIÓN DE NEGOCIO	GESTIÓN DE COLOCACIONES	COMPRA DE CARTERA	CRÉDITO	2	3	3	3	2	13	Sensitivo
		ANÁLISIS DE CRÉDITOS	CRÉDITO	2	5	2	2	2	13	Sensitivo
		APROBACIÓN DE CRÉDITOS	CRÉDITO	4	5	5	3	3	20	Crítico
GESTIÓN DE TESORERÍA	ADMINISTRACION DE PORTAFOLIO	ADMINISTRACION DE FIDEICOMISOS (APORTE DE CARTERA EN GARANTIA)	TESORERÍA	1	3	3	3	2	12	Sensitivo
		INVERSIONES PORTAFOLIO PROPIO EN MERCADO PRIMARIO EXTRABURSATIL	TESORERÍA	1	2	5	2	2	12	Sensitivo
		INVERSIONES PORTAFOLIO PROPIO EN MERCADO SECUNDARIO	TESORERÍA	1	2	5	2	2	12	Sensitivo
		INVERSIONES PORTAFOLIO PROPIO EN MERCADO SECUNDARIO BURSATIL	TESORERÍA	1	2	5	2	2	12	Sensitivo
		RENOVACIÓN DE LA INVERSIÓN	TESORERÍA	5	5	5	2	2	19	Vital
		CANCELACIÓN DE LA INVERSION	TESORERÍA	5	5	5	2	2	19	Vital
		INVERSIONES DE PORTAFOLIO EN MERCADO PRIMARIO EXTRABURSATIL	TESORERÍA	1	1	5	2	2	11	Sensitivo
		CANCELACIÓN DE LA INVERSION A TRAVEZ DE MERCADO DE VALORES	TESORERÍA	1	3	5	2	2	13	Sensitivo
		CESIÓN DE INSTRUMENTOS FINANCIEROS	TESORERÍA	1	1	3	2	2	9	Deseable
		VENTA DE INSTRUMENTOS FINANCIEROS	TESORERÍA	1	3	5	4	4	17	Vital
		COLOCACIÓN DE INVERSIONES SOBRE EL EXTERIOR	TESORERÍA	1	2	5	2	2	12	Sensitivo
		CANCELACIÓN DE INVERSIONES SOBRE EL EXTERIOR	TESORERÍA	1	2	5	2	2	12	Sensitivo

Macroproceso	Proceso	Subproceso	Responsable	Proceso de Cara al Cliente	Proceso de Producto Específico	Proceso con volumen monetario significativo	Proceso para cumplimiento regulatorio	Proceso con alta transaccionalidad	Total	Criticidad
				Calificación	Calificación	Calificación	Calificación	Calificación		
GESTIÓN DE TESORERÍA	MANEJO DE LIQUIDEZ	ELABORACIÓN DE FLUJOS DE LIQUIDEZ	TESORERÍA	1	1	1	3	2	8	Deseable
		PROYECCIÓN DE LIQUIDEZ DIARIA	TESORERÍA	1	1	1	3	2	8	Deseable
		COMPRA / VENTA DE MONEDA EXTRANJERA	TESORERÍA	1		1	3	2	7	Deseable
		CONTRATACIÓN DE FINANCIAMIENTO	TESORERÍA	2	2	2	3	2	11	Sensitivo
		CANCELACIÓN DE CAPITAL E INTERES DE FINANCIAMIENTO	TESORERÍA	2	2	2	3	2	11	Sensitivo
GESTIÓN DE SERVICIO AL CLIENTE	ESTÁNDARES DE ATENCIÓN	MANEJO DE SUGERENCIAS DE CLIENTES	ATENCIÓN AL CLIENTE	2	2	1	3	2	10	Sensitivo
		EVALUACIÓN DEL NIVEL DE SATISFACCIÓN DE CLIENTES	ATENCIÓN AL CLIENTE	2	2	1	3	2	10	Sensitivo
		TARIFARIO DE PRODUCTOS Y SERVICIOS	ATENCIÓN AL CLIENTE	5	2	1	5	3	16	Vital
	ATENCIÓN DE RECLAMOS Y QUEJAS	RECEPCIÓN, ANÁLISIS Y ATENCIÓN DE RECLAMOS Y QUEJAS DE Y CLIENTES	ATENCIÓN AL CLIENTE	5	2	1	5	2	15	Sensitivo
		ELABORACIÓN INFORME ANUAL SOBRE ATENCIÓN AL CLIENTE	ATENCIÓN AL CLIENTE	1	2	1	3	1	8	Deseable
GESTIÓN DE TALENTO HUMANO	GESTIÓN DE INCORPORACIÓN	RECLUTAMIENTO	TALENTO HUMANO	1	1	1	4	1	8	Deseable
		SELECCIÓN	TALENTO HUMANO	1	1	1	4	1	8	Deseable
		CONTRATACIÓN	TALENTO HUMANO	1	1	2	5	1	10	Sensitivo
		INDUCCIÓN INTEGRAL DEL PERSONAL	TALENTO HUMANO	1	1	2	4	1	9	Deseable
	GESTIÓN DE PERMANENCIA	LEVANTAMIENTO Y ACTUALIZACIÓN DE PERFILES	TALENTO HUMANO	1	1	1	4	2	9	Deseable

Macroproceso	Proceso	Subproceso	Responsable	Proceso de Cara al Cliente	Proceso de Producto Específico	Proceso con volumen monetario significativo	Proceso para cumplimiento regulatorio	Proceso con alta transaccionalidad	Total	Criticidad
				Calificación	Calificación	Calificación	Calificación	Calificación		
GESTIÓN DE TALENTO HUMANO	GESTIÓN DE PERMANENCIA	EVALUACION DEL DESEMPEÑO	TALENTO HUMANO	1	1	1	5	1	9	Deseable
		CAPACITACIÓN	TALENTO HUMANO	1	1	2	5	1	10	Sensitivo
		DESARROLLO Y PLAN DE CARRERA	TALENTO HUMANO	1	1	1	3	1	7	Deseable
		CLIMA LABORAL	TALENTO HUMANO	1	1	1	4	1	8	Deseable
	PLANIFICACIÓN Y ADMINISTRACIÓN DEL PERSONAL	REGISTRO DE AVISOS DE ENTRADA Y SALIDA EN EL IESS	TALENTO HUMANO	1	1	1	5	2	10	Sensitivo
		ACTUALIZACIÓN DE INFORMACIÓN Y DOCUMENTACIÓN DEL PERSONAL	TALENTO HUMANO	1	1	1	5	1	9	Deseable
		VALORACIÓN DE CARGOS	TALENTO HUMANO	1	1	1	5	2	10	Sensitivo
		ADMINISTRACION SALARIAL	TALENTO HUMANO	1	1	5	5	4	16	Vital
		BENEFICIOS E INCENTIVOS	TALENTO HUMANO	1	1	1	3	2	8	Deseable
		ADMINISTRACIÓN DE NÓMINA	TALENTO HUMANO	1	1	2	5	1	10	Sensitivo
		CONTROL DE POLIZAS DE SEGURO DE VIDA Y ASISTENCIA MÉDICA DEL PERSONAL	TALENTO HUMANO	1	1	2	4	2	10	Sensitivo
		DEFINICION Y CONTROL DE VINCULADOS	TALENTO HUMANO	1	1	2	4	3	11	Sensitivo
GESTIÓN FINANCIERA	FIJACIÓN DE TASAS Y PRECIOS	COSTEO DE PRODUCTOS Y SERVICIOS	FINANZAS	1	4	3	3	1	12	Sensitivo
	CONTROL PRESUPUESTARIO	ADMINISTRACION Y DEFINICION DE ESTRATEGIAS DE CAPTACION INSTITUCIONAL	FINANZAS	1	2	2	3	1	9	Deseable
		ADMINISTRACION Y DEFINICION DE ESTRATEGIAS DE COLOCACION INSTITUCIONAL	FINANZAS	1	2	2	3	1	9	Deseable
		ELABORACION DE INFORMES AL DIRECTORIO (MENSUAL, TRIMESTRAL)	FINANZAS	1	1	1	3	1	7	Deseable

Macroproceso	Proceso	Subproceso	Responsable	Proceso de Cara al Cliente	Proceso de Producto Específico	Proceso con volumen monetario significativo	Proceso para cumplimiento regulatorio	Proceso con alta transaccionalidad	Total	Criticidad
				Calificación	Calificación	Calificación	Calificación	Calificación		
GESTIÓN FINANCIERA	CONTROL PRESUPUESTARIO	ELABORACION DE CONTROL PRESUPUESTARIO (MENSUAL, TRIMESTRAL)	FINANZAS	1	2	2	3	1	9	Deseable
		INFORME DE TRANSPARENCIA DE LA INFORMACION (TRIMESTRAL)	FINANZAS	2	1	1	4	1	9	Deseable
		ELABORACION DE INDICADORES FINANCIEROS	FINANZAS	1	1	1	3	1	7	Deseable
		ACTUALIZACION DE BASE DATOS DE DEPOSITOS, AHORROS A PLAZO, MONETARIOS, EN BASE AL DWH (DATA WARE HOUSE)	FINANZAS	1	1	1	2	1	6	Deseable
		ELABORAR REPORTE DE INFORMACION GERENCIAL INTERNO	FINANZAS	1	1	1	2	1	6	Deseable
		ELABORAR REPORTE ENTIDADES DE CONTROL	FINANZAS	1	1	1	5	1	9	Deseable
		MODELO DE PAGO COMISIONES (NEGOCIO, INVERSIONES, AUTOMOTRIZ, COBRANZAS)	FINANZAS	1	1	1	1	1	5	No Crítico
		ELABORACION DE REPORTE DE CRÉDITOS CASTIGADOS	FINANZAS	1	1	1	1	1	5	No Crítico
		ELABORACION DE PATRIMONIO TÉCNICO	FINANZAS	1	1	1	5	1	9	Deseable
		ELABORACIÓN DE REPORTE DE SECTORIZACIÓN SEMANAL	FINANZAS	1	1	1	2	1	6	Deseable
		ADMINISTRACION Y DEFINICION DE ESTRATEGIAS DE RESERVAS DE LIQUIDEZ	FINANZAS	1	1	1	2	1	6	Deseable
		ANALISIS, APROBACION Y SEGUIMIIENTO DE MERCADO Y ENTIDADES FINANCIERAS Y COMERCIALES AUTORIZADAS	FINANZAS	1	1	1	2	1	6	Deseable
	GESTIÓN CONTABLE	ELABORACIÓN DE ESTADOS FINANCIEROS PERIODICOS Y POR REQUERIMIENTO	FINANZAS	1	1	5	5	3	15	Sensitivo
		ENVIO DE BALANCE GENERAL A SBS	FINANZAS	1	1	5	5	3	15	Sensitivo
		REVISION PAGO COSEDE (MENSUAL), ENVIO COMPROBANTE DE PAGO	FINANZAS	1	1	5	5	3	15	Sensitivo
		ADMINISTRACIÓN DEL PLAN DE CUENTAS	FINANZAS	1	1	5	5	3	15	Sensitivo

Macroproceso	Proceso	Subproceso	Responsable	Proceso de Cara al Cliente	Proceso de Producto Específico	Proceso con volumen monetario significativo	Proceso para cumplimiento regulatorio	Proceso con alta transaccionalidad	Total	Criticidad
				Calificación	Calificación	Calificación	Calificación	Calificación		
GESTIÓN FINANCIERA	GESTIÓN CONTABLE	CONTABILIZACIÓN DE AJUSTES DE FIN DE MES (PROVISIONES, GARANTIAS, DEMANDAS, VINCULADOS)	FINANZAS	1	1	5	5	2	14	Sensitivo
		CONTABILIZACIÓN DE AJUSTES (DEPRECIACIONES, AMORTIZACIONES)	FINANZAS	1	1	2	2	2	8	Deseable
		REVISIÓN Y CONCILIACIÓN DE CUENTAS.	FINANZAS	1	1	3	3	2	10	Sensitivo
		CONCILIACIÓN DE CUENTAS BANCARIAS	FINANZAS	1	1	3	3	2	10	Sensitivo
		ELABORACIÓN DE ESTADOS FINANCIEROS PERIÓDICOS Y POR REQUERIMIENTO (INICIA POR LA MAYORIZACIÓN)	FINANZAS	1	1	5	5	3	15	Sensitivo
		DECLARACIÓN DE IVA E IMPUESTO A LA RENTA	FINANZAS	1	1	5	5	2	14	Sensitivo
		DECLARACIÓN DE ACTIVOS EN EL EXTERIOR	FINANZAS	1	1	5	5	2	14	Sensitivo
		DECLARACIÓN DE IMPUESTO A LA RENTA EN RDEP	FINANZAS	1	1	5	5	2	14	Sensitivo
		DECLARACIÓN A LA SALIDA DE DIVISAS	FINANZAS	1	1	5	5	2	14	Sensitivo
		REVISIÓN DE ARCHIVOS DE MOVIMIENTOS CON Y SIN MADURACION	FINANZAS	1	1	3	5	2	12	Sensitivo
		TRANSFERENCIAS RECIBIDAS, SPI, SPL	FINANZAS	2	1	5	5	5	18	Vital
GESTIÓN ADMINISTRATIVA	ADMINISTRACIÓN ACTIVOS FIJOS	INVENTARIO Y CODIFICACIÓN DE ACTIVOS FIJOS (PROPIEDAD, PLANTA Y EQUIPO)	FINANZAS	2	1	1	4	1	9	Deseable
		MANTENIMIENTO DE ACTIVOS	FINANZAS	2	1	2	4	4	13	Sensitivo
		CAMBIOS DE DEPENDENCIA DE ACTIVOS	FINANZAS	1	1	3	1	1	7	Deseable

Macroproceso	Proceso	Subproceso	Responsable	Proceso de Cara al Cliente	Proceso de Producto Específico	Proceso con volumen monetario significativo	Proceso para cumplimiento regulatorio	Proceso con alta transaccionalidad	Total	Criticidad
				Calificación	Calificación	Calificación	Calificación	Calificación		
GESTIÓN ADMINISTRATIVA	ADMINISTRACIÓN ACTIVOS FIJOS	BAJAS DE ACTIVOS	FINANZAS	1	1	2	2	2	8	Deseable
	GESTIÓN DE ADQUICISIONES Y MANEJO DE PROVEEDORES	CALIFICACIÓN DE PROVEEDORES	FINANZAS	1	3	3	5	2	14	Sensitivo
		SELECCIÓN DE PROVEEDORES	FINANZAS	1	3	2	5	2	13	Sensitivo
		ADQUISICIÓN DE BIENES Y CONTRATACIÓN DE SERVICIOS	FINANZAS	1	1	2	5	4	13	Sensitivo
		PAGOS DE PROVEEDORES	FINANZAS	1	1	3	5	5	15	Sensitivo
		EVALUACION PROVEEDORES	FINANZAS	1	1	3	5	2	12	Sensitivo
		ADMINISTRACIÓN FONDO CAJA CHICA	FINANZAS	1	2	2	3	3	11	Sensitivo
	ADMINISTRACIÓN DE SEGURIDADES FÍSICAS	ADMINISTRACIÓN Y CONTROL DE LLAVES	FINANZAS	1	1	1	2	1	6	Deseable
		ADMINISTRACIÓN Y CONTROL DE SEGUROS INSTITUCIONALES	FINANZAS	1	2	2	5	1	11	Sensitivo
		ADMINISTRACIÓN Y CONTROL DE DISPOSITIVOS DE PROTECCIÓN CONTRA INCENDIOS	FINANZAS	1	2	4	5	5	17	Vital
	GESTIÓN DE MONITOREO Y VIGILANCIA	MONITOREO Y VIGILANCIA DE OFICINAS, AGENCIAS Y SUCURSALES	SEGURIDAD FÍSICA	3	2	3	3	5	16	Vital
		CONTROL DE INGRESO Y SALIDA DE VISITANTES	SEGURIDAD FÍSICA	2	1	3	2	1	9	Deseable
	GESTION DE SERVICIOS GENERALES	MANTENIMIENTO DE OFICINAS (LIMPIEZA, ARREGLOS, ADECUACIONES MENORES, INSTALACIONES ELÉCTICAS, EQUIPOS, ETC.)	FINANZAS	2	2	2	4	4	14	Sensitivo
		ADMINISTRACIÓN DE SERVICIOS BÁSICOS	FINANZAS	1	1	5	4	4	15	Sensitivo
		ENVÍO DE CORRESPONDENCIA	FINANZAS	2	1	3	4	3	13	Sensitivo

Macroproceso	Proceso	Subproceso	Responsable	Proceso de Cara al Cliente	Proceso de Producto Específico	Proceso con volumen monetario significativo	Proceso para cumplimiento regulatorio	Proceso con alta transaccionalidad	Total	Criticidad
				Calificación	Calificación	Calificación	Calificación	Calificación		
GESTIÓN ADMINISTRATIVA	GESTION DE SERVICIOS GENERALES	ADMINISTRACIÓN DE PROVEEDURÍA	FINANZAS	1	1	3	3	3	11	Sensitivo
		RECEPCIÓN Y DISTRIBUCIÓN DE CORRESPONDENCIA (VALIJA INTERNA)	FINANZAS	1	2	3	4	1	11	Sensitivo
GESTIÓN DE ASESORIA JURIDICA	GESTIÓN CONTRACTUAL	CONSTITUCIÓN DE GARANTÍAS PRENDARIAS DE PROPIEDAD DEL CLIENTE O DE TERCEROS	LEGAL	4	3	4	2	3	16	Vital
		CONSTITUCIÓN DE GARANTÍAS PRENDARIAS A ADQUIRIR	LEGAL	4	4	4	2	3	17	Vital
		CONSTITUCIÓN DE GARANTÍAS HIPOTECARIAS DE PROPIEDAD DEL CLIENTE O DE TERCEROS	LEGAL	4	3	4	2	3	16	Vital
		CONSTITUCIÓN DE GARANTÍAS HIPOTECARIAS A ADQUIRIR	LEGAL	4	4	4	2	3	17	Vital
		ASESORIA LEGAL Y DEFENSA DE TRAMITES DEL BANCO	LEGAL	2	3	2	3	2	12	Sensitivo
		ATENCION CLIENTE INTERNO Y EXTERNO	LEGAL	5	4	2	4	3	18	Vital
		TITULARIZACIÓN DE CARTERA	LEGAL	3	3	3	3	3	15	Sensitivo
		ASESORIA JURÍDICA DE TODAS LAS ÁREAS DEL BANCO A NIVEL NACIONAL	LEGAL	1	2	1	2	2	8	Deseable
		ELABORACIÓN Y ACTUALIZACIÓN DE CONTRATOS	LEGAL	5	4	2	3	3	17	Vital
		REVISIÓN DE CONTRATOS CON PROVEEDORES DEL BANCO	LEGAL	4	3	2	3	3	15	Sensitivo
		REVISIÓN DE DOCUMENTACIÓN LEGAL. (EXTRANJEROS, PODERES, POSESIONES EFECTIVAS, DISOLUCIONES DE SOCIEDAD CONYUGAL, ETC.)	LEGAL	2	2	1	2	2	9	Deseable
		ELABORACIÓN DE MINUTAS Y ESCRITURAS DE PODERES ESPECIALES, DECLARACIONES, COMPRAVENTAS, CONSTITUCIÓN DE HIPOTECAS Y CANCELACIONES DE LAS MISMAS	LEGAL	3	3	3	2	2	13	Sensitivo
		ELABORACIÓN DE INFORMES LEGALES PERSONAS JURÍDICAS	LEGAL	3	3	2	2	2	12	Sensitivo

Macroproceso	Proceso	Subproceso	Responsable	Proceso de Cara al Cliente	Proceso de Producto Específico	Proceso con volumen monetario significativo	Proceso para cumplimiento regulatorio	Proceso con alta transaccionalidad	Total	Criticidad
				Calificación	Calificación	Calificación	Calificación	Calificación		
GESTIÓN DE ASESORÍA JURÍDICA	GESTIÓN CONTRACTUAL	LEGALIZACIÓN DE CONTRATOS DE PRENDA Y RESERVA DE DOMINIO, ANTE AUTORIDDES COMPETENTES	LEGAL	4	2	4	2	2	14	Sensitivo
		TRÁMITE Y LEGALIZACIÓN DE CAMBIOS DE GARANTÍAS	LEGAL	4	3	3	3	2	15	Sensitivo
		REVISIÓN DE OPERACIONES PARA SU PROCESAMIENTO	LEGAL	2	3	2	3	2	12	Sensitivo
		OBTENCIÓN DE DOCUMENTOS EN LOS DIFERENTES ORGANISMOS ESTATALES	LEGAL	3	2	1	2	1	9	Deseable
		ELABORACIÓN DE DOCUMENTACIÓN CREDITICIA Y CONTRATOS PARA OPERACIONES DE FACTORING	LEGAL	3	2	2	2	1	10	Sensitivo
		REVISIÓN Y ELABORACIÓN DE INFORMES ACERCA DE LA CARTERA ADQUIRIDA POR EL BANCO	LEGAL	2	2	2	2	1	9	Deseable
		ELABORACIÓN DE FORMATOS PARA LAS NEGOCIACIONES CREDITICIAS DEL BANCO	LEGAL	3	2	1	1	2	9	Deseable
		ELABORACION DE INFORMES LEGALES PARA APERTURA DE CUENTAS	LEGAL	2	2	1	1	1	7	Deseable
		REVISIÓN DE DOCUMENTACION CREDITICIA PARA DESEMBOLSO	LEGAL	4	4	2	3	3	16	Vital
		REVISIÓN DE FACTURAS Y DOCUMENTOS COMERCIALES PARA INICIO DE RELACIÓN CREIDITICIA CON BANCO CAPITAL	LEGAL	3	3	2	2	3	13	Sensitivo
	GESTIÓN JUDICIAL	ATENCIÓN DE RECLAMOS PRESENTADOS ANTE LA UNIDAD DE RECLAMOS	PROCURADOR LEGAL	5	3	3	3	3	17	Vital
		REPRESENTACIÓN EN TRÁMITES JUDICIALES (CIVILES, LABORALES, PENALES, ETC.)	PROCURADOR LEGAL	3	2	3	3	3	14	Sensitivo
		REGISTRO DE MARCAS Y PATENTES	PROCURADOR LEGAL	2	2	2	3	3	12	Sensitivo
GESTIÓN DE AUDITORÍA	AUDITORÍA INTERNA	ELABORACIÓN DEL PLAN ANUAL DE AUDITORÍA INTERNA	AUDITORÍA	1	1	3	5	3	13	Sensitivo
		PLANIFICACIÓN DE AUDITORÍAS INTERNAS (FINANCIERA, OPERATIVA, ADMINISTRATIVA, INFORMÁTICA, ETC.)	AUDITORÍA	1	1	2	5	1	10	Sensitivo
		EJECUCIÓN DE AUDITORÍAS INTERNAS Y EMISIÓN DE RESULTADOS (INCLUYE EVALUACIÓN A CUMPLIMIENTO Y RIESGOS)	AUDITORÍA	1	1	2	5	2	11	Sensitivo

Macroproceso	Proceso	Subproceso	Responsable	Proceso de Cara al Cliente	Proceso de Producto Específico	Proceso con volumen monetario significativo	Proceso para cumplimiento regulatorio	Proceso con alta transaccionalidad	Total	Criticidad
				Calificación	Calificación	Calificación	Calificación	Calificación		
GESTIÓN DE AUDITORÍA	AUDITORÍA INTERNA	SEGUIMIENTO AL CUMPLIMIENTO DE OBSERVACIONES DE AUDITORÍAS INTERNAS, EXTERNAS Y ORGANISMOS DE CONTROL	AUDITORÍA	1	1	2	5	1	10	Sensitivo
		REALIZACIÓN DE EXÁMENES ESPECIALES DE AUDITORÍA	AUDITORÍA	1	1	2	5	1	10	Sensitivo
		ELABORACIÓN DE INFORMES PARA ORGANISMOS DE CONTROL EXTERNOS E INTERNOS	AUDITORÍA	2	1	2	5	3	13	Sensitivo
		COORDINACIÓN Y REVISIÓN DE RESULTADOS DE AUDITORÍA EXTERNA	AUDITORÍA	1	1	1	5	1	9	Deseable
	GESTIÓN DE CONTROL INTERNO	ELABORACIÓN Y EJECUCIÓN DEL PROGRAMA DE CONTROL INTERNO	AUDITORÍA	1	1	1	3	1	7	Deseable
		ASESORÍA EN TEMAS RELACIONADOS CON CONTROL INTERNO	AUDITORÍA	2	1	1	5	1	10	Sensitivo
GESTIÓN DE PROCESOS	GESTIÓN DOCUMENTAL	MANEJO DE DOCUMENTACIÓN ADMINISTRATIVA	TECNOLOGÍA	1	1	3	3	2	10	Sensitivo
		CONTROL DE DOCUMENTACIÓN ADMINISTRATIVA	TECNOLOGÍA	1	1	3	3	2	10	Sensitivo
	MEJORA CONTINUA DE PROCESOS	ACTUALIZACIÓN DEL INVENTARIO DE PROCESOS	TECNOLOGÍA	1	1	2	2	2	8	Deseable
		DEFINICIÓN Y MEJORAMIENTO DE PROCESOS (EMISIÓN DE PROCEDIMIENTOS)	TECNOLOGÍA	1	1	3	3	3	11	Sensitivo
		CREACIÓN Y ACTUALIZACIÓN DE INSTRUCTIVOS, FORMATOS, DOCUMENTOS EXTERNOS Y DE REFERENCIA	TECNOLOGÍA	1	1	3	3	4	12	Sensitivo
		DIFUSIÓN Y COMUNICACIÓN DE PROCESOS	TECNOLOGÍA	1	1	3	4	3	12	Sensitivo
		CONTROL Y GENERACIÓN DE RESULTADOS DE INDICADORES DE GESTIÓN DE PROCESOS	TECNOLOGÍA	1	1	2	2	2	8	Deseable
		IMPLEMENTACIÓN DE MEJORAS A PROCESOS	TECNOLOGÍA	1	1	3	3	3	11	Sensitivo
GESTIÓN DE COBRANZAS	GESTIÓN DE COBRANZA PREVENTIVA	ELABORACIÓN, SEGUIMIENTO Y CONTROL DE CAMPAÑA DE COBRANZA VÍA CALL CENTER	COBRANZAS	2	5	3	2	2	14	Sensitivo

Macroproceso	Proceso	Subproceso	Responsable	Proceso de Cara al Cliente	Proceso de Producto Específico	Proceso con volumen monetario significativo	Proceso para cumplimiento regulatorio	Proceso con alta transaccionalidad	Total	Criticidad
				Calificación	Calificación	Calificación	Calificación	Calificación		
GESTIÓN DE COBRANZAS	GESTIÓN DE COBRANZA PREVENTIVA	ELABORACIÓN, SEGUIMIENTO Y CONTROL DE CAMPAÑA DE COBRANZA VÍA SMS	COBRANZAS	2	5	3	2	2	14	Sensitivo
		AVISOS DE VENCIMIENTO Y SEGUIMIENTO DE CRÉDITOS	COBRANZAS	2	5	3	2	2	14	Sensitivo
		NOVACIÓN DE CRÉDITO	COBRANZAS	1	4	2	2	2	11	Sensitivo
GESTIÓN DE OPERACIONES	OPERACIONES INTEGRALES DEL BACK OFFICE	CAMARA PRELIMINAR, ENVIADA, RECIBIDA	TECNOLOGÍA	5	4	5	5	5	24	Crítico
		CAMARA DEFINITIVA, ENVIADA, RECIBIDA	TECNOLOGÍA	5	4	5	5	5	24	Crítico
		AFECTACION CUENTAS Y ENTREGA CHEQUES DEVUELTOS	TECNOLOGÍA	2	1	3	3	3	12	Sensitivo
		CHEQUES PROTESTADOS	TECNOLOGÍA	3	2	2	5	4	16	Vital
		LEGALIZACION DE DOCUMENTOS (GARANTIAS, FIDEICOMISO, PRENDA INDUSTRIAL, RESERVA DE DOMINIO, NOTARIA, REGISTRO MERCANTIL, ETC.)	TECNOLOGÍA	3	3	3	4	4	17	Vital
		LEVANTAMIENTO DE GARANTÍAS	TECNOLOGÍA	5	5	3	2	3	18	Vital
		ENTREGA DE DOCUMENTOS LEGALES POR DEMANDA	TECNOLOGÍA	3	2	2	3	2	12	Sensitivo
		INGRESO, CUADRE Y MANTENIMIENTO DE GARANTIAS	TECNOLOGÍA	3	2	2	3	2	12	Sensitivo
		CONTROL Y CUSTODIA DE DOCUMENTOS DE PRODUCTOS DEL ACTIVO	TECNOLOGÍA	2	2	3	4	3	14	Sensitivo
		CONTROL Y CUSTODIA DE DOCUMENTOS DE PRODUCTOS DEL PASIVOS	TECNOLOGÍA	2	2	3	4	2	13	Sensitivo
		ENDOSO DE SEGURO	TECNOLOGÍA	2	2	2	3	3	12	Sensitivo
		PRECANCELACION CRÉDITO	TECNOLOGÍA	5	4	4	2	3	18	Vital

Macroproceso	Proceso	Subproceso	Responsable	Proceso de Cara al Cliente	Proceso de Producto Específico	Proceso con volumen monetario significativo	Proceso para cumplimiento regulatorio	Proceso con alta transaccionalidad	Total	Criticidad
				Calificación	Calificación	Calificación	Calificación	Calificación		
GESTIÓN DE OPERACIONES	OPERACIONES INTEGRALES DEL BACK OFFICE	LIQUIDACION FACTORING	TECNOLOGÍA	3	3	3	3	3	15	Sensitivo
		LIQUIDACION DE COMPRA / VENTA DE CARTERA	TECNOLOGÍA	3	2	3	3	3	14	Sensitivo
		CAPTURA DE FIRMAS	TECNOLOGÍA	4	3	3	4	5	19	Vital
		ADMINISTRACION Y CONCILIACION SEGUROS Y DISPOSITIVOS	TECNOLOGÍA	3	3	3	2	3	14	Sensitivo
		CAMBIO DE GARANTIAS	TECNOLOGÍA	3	3	3	2	3	14	Sensitivo
		LEVANTAMIENTO DE GARANTÍAS	TECNOLOGÍA	5	4	3	3	3	18	Vital
		EMISION Y ENTREGA DE ESTADOS DE CUENTA	TECNOLOGÍA	2	2	2	3	5	14	Sensitivo
		TRASPORTACION DE VALORES (BLINDADO)	TECNOLOGÍA	5	5	4	2	2	18	Vital
		ENDOSOS DE SEGUROS	TECNOLOGÍA	2	3	2	3	3	13	Sensitivo
		SEGUIMIENTO Y CONTROL DE CUENTAS INHABILITADAS	TECNOLOGÍA	3	3	2	4	5	17	Vital
		CUENTAS INMOVILIZADAS	TECNOLOGÍA	2	3	3	4	2	14	Sensitivo
		ELABORACIÓN Y ENVÍO DE LAS ESTRUCTURAS ENTES DE CONTROL (T21, T22,T23, TIN,C31,C32, C41, C70, E02, C02, C11, C21, C23, R)	TECNOLOGÍA	2	2	2	5	2	13	Sensitivo
		SEGUIMIENTO Y CONTROL CAJAS SERVIPAGOS	TECNOLOGÍA	5	5	5	2	5	22	Crítico
		CUENTAS INACTIVAS	TECNOLOGÍA	2	3	2	3	2	12	Sensitivo

Macroproceso	Proceso	Subproceso	Responsable	Proceso de Cara al Cliente	Proceso de Producto Específico	Proceso con volumen monetario significativo	Proceso para cumplimiento regulatorio	Proceso con alta transaccionalidad	Total	Criticidad
				Calificación	Calificación	Calificación	Calificación	Calificación		
GESTIÓN DE OPERACIONES	OPERACIONES FRONT OFFICE	ACTIVACIÓN DE CUENTAS INACTIVAS	TECNOLOGÍA	5	4	2	2	3	16	Vital
		APERTURA, CUADRE Y CIERRE DE BOVEDA	TECNOLOGÍA	5	4	5	4	5	23	Crítico
		INCREMENTO DE EFECTIVO EN BOVEDA	TECNOLOGÍA	5	4	5	2	5	21	Crítico
		APERTURA, CUADRE Y CIERRE DE CAJAS	TECNOLOGÍA	5	4	5	4	5	23	Crítico
		TRANSFERENCIAS ENVIADAS SPI, SPL	TECNOLOGÍA	5	5	5	4	5	24	Crítico
		ARQUEO DE CAJAS	TECNOLOGÍA	3	3	3	3	2	14	Sensitivo
		EMSION Y ENTREGA DE TARJETAS DE DEBITO	TECNOLOGÍA	5	5	4	3	4	21	Crítico
		EMSION, REPOSICION Y ENTREGA DE LIBRETAS DE AHORRO	TECNOLOGÍA	5	5	4	2	2	18	Vital
		ACTUALIZACION LIBRETAS DE AHORRO	TECNOLOGÍA	3	3	2	3	3	14	Sensitivo
		ACTUALIZACION Y CAPTURA DE FIRMAS	TECNOLOGÍA	4	3	3	3	3	16	Vital
		ARQUEO DE BOVEDA	TECNOLOGÍA	3	3	2	3	2	13	Sensitivo
		CERTIFICACION DE CHEQUES	TECNOLOGÍA	5	3	2	4	5	19	Vital
		DEPOSITOS CTAS CTES Y CUENTAS DE AHORRO	TECNOLOGÍA	5	5	5	2	5	22	Crítico
		DETECCION DE BILLETES FALSOS E INFORME ENTE DE CONTROL	TECNOLOGÍA	2	3	2	2	5	14	Sensitivo
		CONTROL DE FORMAS NUMERADAS	TECNOLOGÍA	2	3	2	2	2	11	Sensitivo
		CONTROL LIMITE DE EFECTIVO EN CAJA	TECNOLOGÍA	5	4	3	3	2	17	Vital

Macroproceso	Proceso	Subproceso	Responsable	Proceso de Cara al Cliente	Proceso de Producto Específico	Proceso con volumen monetario significativo	Proceso para cumplimiento regulatorio	Proceso con alta transaccionalidad	Total	Criticidad
				Calificación	Calificación	Calificación	Calificación	Calificación		
GESTIÓN DE OPERACIONES	OPERACIONES FRONT OFFICE	CONTROL LIMITE DE EFECTIVO EN BOVEDA/ OFICINA	TECNOLOGÍA	5	4	3	3	2	17	Vital
		PAGO DE CHEQUES Y EFECTIVO EN CAJA	TECNOLOGÍA	5	5	5	3	5	23	Crítico
		PAGOS VARIOS EN CAJA	TECNOLOGÍA	5	5	5	3	3	21	Crítico
		RECAUDOS EN CAJA/ PUNTO MATICO	TECNOLOGÍA	5	3	4	3	4	19	Vital
		FACTURACION ELECTRONICA	TECNOLOGÍA	3	3	3	5	4	18	Vital
		CANCELACIÓN DE TARJETA DE DÉBITO	TECNOLOGÍA	5	5	3	2	3	18	Vital
		REVOCATORIA, SUSPENSION Y ANULACION DE CHEQUES	TECNOLOGÍA	5	3	3	3	4	18	Vital
		BLOQUEO DE TARJETA DE DÉBITO	TECNOLOGÍA	5	5	3	2	4	19	Vital
		RENOVACIÓN DE TARJETAS DE DEBITO	TECNOLOGÍA	5	5	3	2	4	19	Vital
		EMISION Y ENTREGA DE CHEQUERAS	TECNOLOGÍA	5	4	3	3	3	18	Vital
		EMISION DE CERTIFICADOS BANCARIOS	TECNOLOGÍA	3	3	2	2	3	13	Sensitivo
		EMISION Y ENTREGA DE CHEQUES DE GERENCIA	TECNOLOGÍA	3	3	2	3	3	14	Sensitivo
		ANULACIÓN DE CHEQUES DE GERENCIA	TECNOLOGÍA	3	3	2	3	3	14	Sensitivo
		PROVIDENCIA JUDICIALES	TECNOLOGÍA	3	3	2	5	5	18	Vital
		AFILIACIÓN, DE CASH MANAGEMENT	TECNOLOGÍA	3	2	2	2	4	13	Sensitivo
		SOPORTE CASH MANAGEMENT	TECNOLOGÍA	3	3	2	2	4	14	Sensitivo

Anexo 3- Necesidad de recursos de procesos críticos

Proceso	Responsable	Área Responsable	Recursos Críticos que necesita el Proceso											
			Recursos de Tecnología de Información					Recursos Humanos - Personal Crítico y back up	Relación con proveedores	Recursos de Soporte (Manuales y procedimientos de usuario)	Recursos de papelería y Material de Oficina	Cantidad de Recursos Informáticos utilizados actualmente	Cantidad de recursos informáticos mínimos requeridos en caso de desastre	Documentación relacionada con el proceso que puede hacer falta después de la interrupción
			Aplicaciones	Herramientas de oficina	Servicios de Telefonía	Correo Electrónico	Internet							
CAMARA PRELIMINAR, ENVIADA, RECIBIDA	GERENTE DE OPERACIONES	OPERACIONES	DCNET Core Globus T24 SFTP	- Word elaboraciòn de carta solicitando al Banco emisor del cheque el pago del mismo debido a que no se generò en el archivo zip MTP escaneado por parte de las agencias. - Excel cuadre de càmara por agencia de la localidad Quito y sucursales a nivel nacional.	Si en caso de confirmaciòn a BCE de la carga exitosa de los SCCC (Sistema de Càmara de Compensaciòn de Cheques). Confirmaci[on a los Bancos por cheques cargaddos fuera de camara.	SI confirmacion camara preliminar cargas inconsistencias, notificar cuadres errores	Pagina del BCE para carga y descarga de planillas y confirmacion de archivos SCCC	Normal 1 persona en matriz en cada una de las agencias de Quito el cajero microfilma los depositos en cheques Agencias 1 persona en camara ibarra 1 otavalo 1 guayaquil 1 cuenca 1 y ambato Critico 1 persona con los accesos de camara, BCE, Certificado digital SFTP se puede asignar a cualquier persona de camara de las sucursales	No	En proceso de aprobacion	Sello para garantizar el endoso Sello de endoso en caso de que la lectora no funcione	1 computadora 1 lectora 1 impresora 1 punto de red	1 computadora 1 lectora 1 impresora 1 punto de red	cheques de otros bancos cheques propios papeletas de deposito
CAMARA DEFINITIVA, ENVIADA, RECIBIDA	GERENTE DE OPERACIONES	OPERACIONES	DCNET Core Globus T24 SFTP	- Excel cuadre de cheques devueltos y protestados, pago manual de cheques con sobregiro.	Si en caso de confirmaciòn a BCE de la carga exitosa de los SCCC (Sistema de Càmara de Compensaciòn de Cheques). Confirmaci[on a los Bancos por cheques cargaddos fuera de camara.	SI confirmacion camara definitiva cargas inconsistencias, notificar cuadres errores	Pagina del BCE para carga y descarga de planillas y confirmacion de archivos SCCC	Normal Quito 2 personas 1 de camara y 1 persona de operaciones 1 ibarra, 1 cuenca, 1 ambato y 1 guayaquil Critico 1 persona con accesos al BCE y Certificado digital SFTP se puede asignar a cualquier persona de camara de las sucursales	No	En proceso de aprobacion	Sellos por devolucion por foma y protesto de cheques por fondo de acuerdo a la causal 8 sellos	1 computadora 1 lectora 1 impresora 1 punto de red	1 computadora 1 lectora 1 impresora 1 punto de red	cheques de otros bancos cheques propios
SEGUMIENTO Y CONTROL CAJAS SERVIPAGOS	GERENTE DE OPERACIONES	OPERACIONES	Core Globus T24 SFTP	- Excel cuadre de las transacciones procesadas en servipagos y los sistemas del Banco en caso de diferencias.	Si seguimiento depositos mal efectuados Cuadre de saldos Banco Capital vs Servipagos	si notificar diariamente los cuadres, en caso de descuadre se notifica a contabilidad, operaciones y oficial de cuenta	Consulta de correo electrnico de la agencia de servipagos en caso de reclamos por transacciones no porcesadas o mal procesadas	Normal 1 persona de camara Critico 1 persona de cualquier localidad	Servipagos	No	No	1 computadora 1 punto de red	1 computadora 1 punto de red	cheques de otros bancos cheques propios papeletas de deposito

Proceso	Responsable	Área Responsable	Recursos Críticos que necesita el Proceso											
			Recursos de Tecnología de Información					Recursos Humanos - Personal Crítico y back up	Relación con proveedores	Recursos de Soporte (Manuales y procedimientos de usuario)	Recursos de papelería y Material de Oficina	Cantidad de Recursos Informáticos utilizados actualmente	Cantidad de recursos informáticos mínimos requeridos en caso de desastre	Documentación relacionada con el proceso que puede hacer falta después de la interrupción
			Aplicaciones	Herramientas de oficina	Servicios de Telefonía	Correo Electrónico	Internet							
CONCESION CRÉDITO CANAL AUTIOMOTRIZ	SUBGERENTE DE NEGOCIOS	NEGOCIOS	Core Globus T24 Buro de crédito - Equifax Listas Web cobrador Sistema Originador de Crédito	Excel Simulación de crédito Word Entrega de documentos a la parte operativa Carta de Compromiso del cliente	Si Confirmación de datos Aprobación vía telefónica Coordinación con otras áreas el estado del proceso	Si coordinar excepciones Autorizaciones Solicitar documentación al cliente o a la concesionaria	Si página intranet T24 página de CNT para teléfono del domicilio Link del Sri creación de la empresa, dirección y datos de los accionistas Páginas Judiciales (si se encuentran en demanda) Páginas del Banco Central (tasas efectivas y nominales)	Normal 3 Asesores del Banco Capital 1 Gerente de Negocios 1 Asesor Legal Crítico 3 Asesores del Banco Capital 1 Gerente de Negocios 1 Asesor Legal	No	Políticas de Crédito	- Solicitud de Crédito - Autorización de Buró - Actualización de Datos - Conozca a su cliente	Normal 3 Computadoras 1 Impresora 1 Copiadora 1 punto de red	Crítico 3 Computadoras 1 Impresora 1 Copiadora 1 punto de red	Expediente del cliente
CONCESION CRÉDITO CANAL BANCA	SUBGERENTE DE NEGOCIOS	NEGOCIOS	Core Globus T24 Buro de crédito - Equifax Listas Web cobrador	Excel Simulación de crédito Word Entrega de documentos a la parte operativa Carta de Compromiso del cliente	Si Confirmación de datos Aprobación vía telefónica Coordinación con otras áreas el estado del proceso	Si coordinar excepciones Autorizaciones Solicitar documentación al cliente	Si página intranet T24 página de CNT para teléfono del domicilio Link del Sri creación de la empresa, dirección y datos de los accionistas Páginas Judiciales (si se encuentran en demanda) Páginas del Banco Central (tasas efectivas y nominales)	Normal 3 Asesores del Banco Capital 1 Gerente de Negocios 1 Asesor Legal Crítico 3 Asesores del Banco Capital 1 Gerente de Negocios 1 Asesor Legal	No	Políticas de Crédito	- Solicitud de Crédito - Autorización de Buró - Actualización de Datos - Conozca a su cliente	Normal 3 Computadoras 1 Impresora 1 Copiadora 1 punto de red	Crítico 3 Computadoras 1 Impresora 1 Copiadora 1 punto de red	Expediente del cliente
APROBACIÓN DE CRÉDITOS	JEFE DE RIESGOS	RIESGOS	Core Globus T24 Buro de crédito - Equifax Listas Web cobrador	Excel Medio de Aprobación de Crédito	si para comunicir al cliente la aprobación del préstamo	Si comunicación de aprobación o negación del crédito al asesor.	No	Normal 1 Jefe de Riesgos Integrales Crítico 1 Jefe de Riesgos Integrales	No	Políticas de Crédito	- Plantilla de Medio de Aprobación	Normal '- 1 Computadora - 1 Copiadora - 1 Impresoara - 1 Punto de red	Crítico '- 1 Computadora - 1 Copiadora - 1 Impresoara - 1 Punto de red	Expediente del cliente

Proceso	Responsable	Área Responsable	Recursos Críticos que necesita el Proceso											
			Recursos de Tecnología de Información					Recursos Humanos - Personal Crítico y back up	Relación con proveedores	Recursos de Soporte (Manuales y procedimientos de usuario)	Recursos de papelería y Material de Oficina	Cantidad de Recursos Informáticos utilizados actualmente	Cantidad de recursos informáticos mínimos requeridos en caso de desastre	Documentación relacionada con el proceso que puede hacer falta después de la interrupción
			Aplicaciones	Herramientas de oficina	Servicios de Telefonía	Correo Electrónico	Internet							
Apertura de Bóveda Cuadre y Cierre de Bóveda	Vicepresidenta	Operaciones	- Core Globus T24 Repemerge	Excel para el cuadre de bóveda	Si para comunicarse con las agencias si alguna no se encuentra aperturada, cerrada o presenta diferencias.	Si enviar reportes a Gerencia de Operaciones y Auditoría	No	Normal 1 Supervisor Operativo 1 Asistente de Custodia (apertura, cuadre y cierre de bóveda) Crítico 1 Supervisor Operativo Agencias Normal 1 Asistente Operativo - Balcón de Servicios 1 Cajero Crítico 1 Asistente Operativo	No	Instructivo	- Formulario de Transferencia de Efectivo - Sello de cajero - Formulario de Cuadre (excel)	Normal Apertura, Cuadre y Cierre - 1 Computador - 1 Impresora - 1 Scaner	Crítico - 1 Computador - 1 Impresora - 1 Scaner	- Formularios de Transferencia - Formulario del cuadre del día anterior
Incremento de Efectivo en Bóveda	Vicepresidenta	Operaciones	- Core Globus T24 - Repemerge	Excel llenar el formulario de transferencia Word para realizar la solicitud de fondeo	Si para realizar confirmaciones de recepción del efectivo	Si para requerimiento del fondeo al Jefe Operativo	No	Normal 1 Supervisor Operativo 1 Jefe de Operaciones Crítico 1 Supervisor Operativo Agencias Normal 1 Asistente Operativo - Balcón de Servicios 1 Supervisor Operativo Crítico 1 Supervisor Operativo	No	Instructivo apertura y cierre de bóveda	No	Normal - Computadora - 1 impresora	Crítico - 1 Computadora - 1 Impresora	- Formulario de Transferencia
Apertura de Cajas Cuadre y Cierre de Cajas	Vicepresidenta	Operaciones	- Core Globus T24 - Repemerge	Excel para el cuadre de caja Word en caso de faltantes la carta de aceptación	Si para comunicarse con las agencias si alguna no se encuentra aperturada, cerrada o presenta diferencias.	Si enviar reportes a Gerencia de Operaciones y Auditoría	No	Normal 1 Supervisor Operativo 1 Cajero Crítico 1 Supervisor Operativo 1 Cajero Agencias Normal 1 Asistente Operativo - Balcón de Servicios 1 Cajero Crítico 1 Asistente Operativo - Balcón de Servicios 1 Cajero	No	Instructivo	- Formulario de Transferencia de Efectivo - Sello de cajero - Formulario de cuadre (excel)	Normal - 1 computadora - 1 impresora - 1 sumadora - 1 recontadora - 1 scaner para microfilm	Crítico - 1 computadora - 1 impresora - 1 sumadora - 1 scaner para microfilm	- Formularios de Transferencia - Formulario del cuadre del área de Cajas del día anterior - Respaldos físicos de las transacciones (papeletas de depósito, retiro de ahorros, cheques, comprobante de ingreso y egreso, comprobantes de puntomático)
Transferencias enviadas SPI, SPL	Vicepresidenta	Operaciones	- Core Globus T24 - Repemerge	Excel llenar el formulario de transferencia	Si para confirmar con el que procesa la trasferencia si esta fue realizada o rechazada	Si para envio del formulario al asistente operativo o Supervisor Operativo para que procese la transferencia.	Si para la carga y autorización de transferencias por medio de la plataforma del Banco Central	Normal 1 Asistente Operativo - Balcón de Servicios 1 Supervisor Operativo o Asistente Operativo - Operaciones Crítico 1 Asistente Operativo - Balcón de Servicios 1 Supervisor Operativo o Asistente Operativo - Operaciones	No	Instructtivo	- Formulario de Transferencia (excel) - Sellos de firma verificada	Normal Transferencias enviada SPI , SPL - 1 Computador - 1 Impresora - 1 Scaner	Crítico - 1 Computadora - 1 Impresora - 1 Scaner	- Formulario de transferencia
Emisión y Entrega de Tarjetas de Débito	Vicepresidenta	Operaciones	- Core Globus T24 - Extreme Web	Excel para reporte de tarjetas solicitadas y entregadas	Si para confirmar la emisión o entrega de la tarjeta con el proveedor o adminsitrador, respectivamente	Si para poner en conocimiento el envio de las tarjetas emitidas por parte del asistente operativo al Supervisor y este comunica al Balcón.	Si para el uso de la plataforma del extremeweb	Normal 1 Asistente Operativo - Balcón de Servicios 1 Supervisor Operativo - Adminsitrador 1 Supervisor Operativo Crítico 1 Asistente Operativo - Balcón de Servicios 1 Supervisor Operativo - Adminsitrador	No	Manual operativo	- Formulario solicitud de tarjeta de débito - Contrato de uso de tarjeta de débito	Normal - 1 Computadora - 1 Impresora	Crítico - 1 Computadora - 1 Impresora	- Solicitud de emisión de tarjeta de débito

Proceso	Responsable	Área Responsable	Recursos Críticos que necesita el Proceso											
			Recursos de Tecnología de Información					Recursos Humanos - Personal Crítico y back up	Relación con proveedores	Recursos de Soporte (Manuales y procedimientos de usuario)	Recursos de papelería y Material de Oficina	Cantidad de Recursos Informáticos utilizados actualmente	Cantidad de recursos informáticos mínimos requeridos en caso de desastre	Documentación relacionada con el proceso que puede hacer falta después de la interrupción
			Aplicaciones	Herramientas de oficina	Servicios de Telefonía	Correo Electrónico	Internet							
Depósitos Ctas Ctes y Cuentas de Ahorros	Vicepresidenta	Operaciones	- Core Globus T24 - Repemerge	Excel para llenar el reporte de cheques pagados durante el día.	Si para autorización de reversos por Supervisor Operativo.	Si para autorización de reversos por Supervisor Operativo.	No	Normal 1 Cajero 1 Supervisor Operativo o Asistente de Balcón de Servicios Crítico 1 Cajero	No		- Papeletas de depósito - Comprobante de transacción - Tirilla de la sumadora	Normal '- 1 computadora - 1 impresora - 1 sumadora - 1 recontadora - 1 scaner para microfilm Crítico '- 1 computadora - 1 impresora - 1 sumadora - 1 scaner para microfilm		'- Respaldos físicos de las transacciones (papeletas de depósito, y cheques, comprobante de ingreso)
Pago de Cheques y Retiro de Efectivo en Caja	Vicepresidenta	Operaciones	- Core Globus T24 - Repemerge	No se utiliza excel ni word	Si para confirmación por montos con el cliente por el pago del cheque o retiro de ahorros	No se utiliza	No	Normal 1 Cajero 1 Supervisor Operativo o Asistente de Balcón de Servicios Crítico 1 Cajero 1 Supervisor Operativo	No		- Papeletas de Retiro de Ahorros - Libretas de Ahorros - Tirilla de la sumadora	Normal '- 1 computadora - 1 impresora - 1 sumadora - 1 recontadora - 1 scaner para microfilm Crítico '- 1 computadora - 1 impresora - 1 sumadora - 1 scaner para microfilm		'- Respaldos físicos de las transacciones (cheques, papeletas de retiro de ahorros y comprobantes de egreso)
Pagos Varios en Caja	Vicepresidenta	Operaciones	Puntomatico	Excel reporte de puntomático del día	Si de no haber sistema las agencias se comunican al Supervisor Operativo quien se comuncia con el adminsitrador (asistente operativo) y el comunica al proveedor.	Si de no haber sistema las agencias se comunican al Supervisor Operativo quien se comuncia con el adminsitrador (asistente operativo) y el comuncia al proveedor.	Si para el uso de la plataforma del extremeweb	Normal 1 Cajero 1 Supervisor Operativo o Asistente de Balcón de Servicios Crítico 1 Cajero	Si Puntomático		- Comprobante de Transacción - Rollo de la impresora - Tirilla de la sumadora	Normal '- 1 computadora - 1 impresora - 1 sumadora - 1 recontadora Crítico '- 1 computadora - 1 impresora - 1 sumadora		'- Respaldos físicos de las transacciones (comprobantes de puntomático)

Proceso	Responsable	Área Responsable	Recursos Críticos que necesita el Proceso											
			Recursos de Tecnología de Información					Recursos Humanos - Personal Crítico y back up	Relación con proveedores	Recursos de Soporte (Manuales y procedimientos de usuario)	Recursos de papelería y Material de Oficina	Cantidad de Recursos Informáticos utilizados actualmente	Cantidad de recursos informáticos mínimos requeridos en caso de desastre	Documentación relacionada con el proceso que puede hacer falta después de la interrupción
			Aplicaciones	Herramientas de oficina	Servicios de Telefonía	Correo Electrónico	Internet							
APERTURA DE INVERSIONES A PLAZO	GERENTE BANCA PRIVADA	NEGOCIOS	Core Globus T24 Listas	excel reporte semanal de las inversiones aperturadas por monto y nùmero de inversiòn	si negociar la inversiòn, para concretar la visita, negociar tasa	Para mandar la carta de presentaciòn al cliente informandole tasas, plazos, Aprobaciones internas de niveles a tesorerìa, presidencia, informaciòn a las àreas internas para parametrizaciòn de tasas.	No	Normal 6 Oficiales de Negociación 1 Oficial que procesa 1 Asistente de operaciones 1 Gerente de inversiones 1 Gerente de finanzas 1 Tesorería 1 Presidente Crítico 1 Oficial de Inversión 1 Asistente de operaciones 1 Jefe de Aprobación	no	Manual de Apertura de Certificados de Depòsito a Plazo (pendiente de aprobaciòn)	Solicitud de apertura de cuentas y servicios Solicitud inicio relaciòn comercial - actualizaciòn de datos Comprobante de negociaciòn Formulario de Certificado de depòsito a plazo	Normal 12 Computadoras 1 Impresora 12 puntos de red	Normal 3 Computadoras 3 Impresoras 3 puntos de red	Expediente del Cliente La informaciòn física podrìa recuperarse con el cliente y el certificado de depòsito original y la informaciòn del certificado se mantiene en el sistema.
RENOVACION DE INVERSIONES A PLAZO	GERENTE BANCA PRIVADA	NEGOCIOS	Core Globus T24 Listas	excel reporte de renovaciones con montos fechas (inicio vencimiento),cliente y plazo	si para renovar	para paremetrizar correos internos negociar tasa ajuste especial, aprobaciòn de tasas, plazos parametirzaciòn operativa.	No	Normal 6 Oficiales de Negociación 1 Oficial que procesa 1 Asistente de operaciones 1 Gerente de inversiones 1 Gerente de finanzas 1 Tesorería 1 Presidente Crítico 1 Oficial de Inversión 1 Asistente de operaciones 1 Jefe de Aprobación	no	Manual de Apertura de Certificados de Depòsito a Plazo (pendiente de aprobaciòn)	Comprobante de negociaciòn Certificado de depòsito a plazo (al momento de emitirle en nuevo certificado, la renovaciòn puede ser por telèfono)	Normal 12 Computadoras 1 Impresora 12 puntos de red	Normal 3 Computadoras 3 Impresoras 3 puntos de red	Expediente del Cliente La informaciòn física podrìa recuperarse con el cliente y el certificado de depòsito original y la informaciòn del certificado se mantiene en el sistema.
CANCELACION - PRECANCELACION INVERSIONES A PLAZO	GERENTE BANCA PRIVADA	NEGOCIOS	Core Globus T24 Listas	excel reportes de cancelaciones word carta solicitada por el cliente cuando se requiere que los intereses sean acreditados en otro banco o el capital, intruccion de credito de capital o intereses en cancelaciòn o renovaciòn.	si se comunica al cliente antes del vencimiento para decidir si va a renovar la inversiòn, el funcionario tiene que estar pendiente del vencimiento para la cancelaciòn o negociar una renovaciòn	correo interno autorizaciòn via correo electrònico a tesorerìa para procesar la transferencia emitir el cheque o pagar en cajas una vez aprobado por parte de tesorerìa y opepraciones procesa la cancelaciòn.	No	Normal 6 Oficiales de Negociación 1 Oficial que procesa 1 Asistente de operaciones 1 Gerente de inversiones 1 Gerente de finanzas 1 Tesorería 1 Presidente Crítico 1 Oficial de Inversión 1 Asistente de operaciones 1 Jefe de Aprobación	no	Manual de Apertura de Certificados de Depòsito a Plazo (pendiente de aprobaciòn)	Carta de instrucciòn del cliente de cancelaciòn Certificado de Depòsito a Plazo original sello de cancelado	Normal 12 Computadoras 1 Impresora 12 puntos de red	Normal 3 Computadoras 3 Impresoras 3 puntos de red	Expediente del Cliente La informaciòn física podrìa recuperarse con el cliente y el certificado de depòsito original y la informaciòn del certificado se mantiene en el sistema.

Anexo 4- BIA Matriz de impacto operacional y financiero

Proceso	Área Impactada	Impacto del proceso (si el proceso no funciona)							
		Menos de 4 horas		4-8 horas		8-24 horas		Más de 48 horas	
CAMARA PRELIMINAR, ENVIADA, RECIBIDA	Necesidades de clientes / Servicio al cliente	2	Medio	3	Alto	3	Alto	4	Muy Alto
	Requerimientos Legales / Incremento en las responsabilidades legales	2	Medio	3	Alto	3	Alto	4	Muy Alto
	Imagen en el medio - Reputación	2	Medio	3	Alto	3	Alto	4	Muy Alto
	Relación con proveedores	0	N/A	0	N/A	0	N/A	0	N/A
	Clientes Internos	1	Bajo	2	Medio	2	Medio	2	Medio
	Financiera	1	Bajo	2	Medio	3	Alto	3	Alto
CAMARA DEFINITIVA, ENVIADA, RECIBIDA	Necesidades de clientes / Servicio al cliente	2	Medio	3	Alto	3	Alto	4	Muy Alto
	Requerimientos Legales / Incremento en las responsabilidades legales	2	Medio	3	Alto	3	Alto	4	Muy Alto
	Imagen en el medio - Reputación	2	Medio	3	Alto	3	Alto	4	Muy Alto
	Relación con proveedores	0	N/A	0	N/A	0	N/A	0	N/A
	Clientes Internos	1	Bajo	2	Medio	2	Medio	2	Medio
	Financiera	1	Bajo	2	Medio	3	Alto	3	Alto
SEGUMIENTO Y CONTROL CAJAS SERVIPAGOS	Necesidades de clientes / Servicio al cliente	1	Bajo	1	Bajo	2	Medio	2	Medio
	Requerimientos Legales / Incremento en las responsabilidades legales	0	N/A	0	N/A	0	N/A	0	N/A
	Imagen en el medio - Reputación	1	Bajo	2	Medio	2	Medio	3	Alto
	Relación con proveedores	1	Bajo	2	Medio	3	Alto	4	Muy Alto
	Clientes Internos	0	N/A	1	Bajo	1	Bajo	1	Bajo
	Financiera	1	Bajo	2	Medio	2	Medio	2	Medio

Anexo 5- Matriz de impacto financiero Back Office

Proceso	Rango	Transaccional
		No. de transacciones
CAMARA PRELIMINAR, ENVIADA, RECIBIDA	Menos de 4 horas	10
	4-8 horas	20
	8-24 horas	60
	Más de 48 horas	120
CAMARA DEFINITIVA, ENVIADA, RECIBIDA	Menos de 4 horas	1
	4-8 horas	2
	8-24 horas	6
	Más de 48 horas	12
SEGUMIENTO Y CONTROL CAJAS SERVIPAGOS	Menos de 4 horas	26
	4-8 horas	51
	8-24 horas	153
	Más de 48 horas	306

Anexo 6- Matriz de impacto operacional Front Office

Proceso	Área Impactada	Impacto del proceso (si el proceso no funciona)							
		Menos de 4 horas		4-8 horas		8-24 horas		Más de 48 horas	
APERTURA, CUADRE Y CIERRE DE BOVEDA	Necesidades de clientes / Servicio al cliente	2	Medio	3	Alto	4	Muy Alto	4	Muy Alto
	Requerimientos Legales / Incremento en las responsabilidades legales	0	N/A	1	Bajo	2	Medio	4	Muy Alto
	Imagen en el medio - Reputación	2	Medio	3	Alto	4	Muy Alto	4	Muy Alto
	Relación con proveedores	0	N/A	0	N/A	0	N/A	0	N/A
	Clientes Internos	2	Medio	3	Alto	4	Muy Alto	4	Muy Alto
	Financiera	1	Bajo	2	Medio	3	Alto	4	Muy Alto
INCREMENTO DE EFECTIVO EN BOVEDA	Necesidades de clientes / Servicio al cliente	1	Bajo	2	Medio	3	Alto	4	Muy Alto
	Requerimientos Legales / Incremento en las responsabilidades legales	0	N/A	0	N/A	1	Bajo	2	Medio
	Imagen en el medio - Reputación	1	Bajo	2	Medio	3	Alto	4	Muy Alto
	Relación con proveedores	0	N/A	0	N/A	0	N/A	0	N/A
	Clientes Internos	1	Bajo	2	Medio	3	Alto	4	Muy Alto
	Financiera	1	Bajo	2	Medio	3	Alto	4	Muy Alto
APERTURA, CUADRE Y CIERRE DE CAJAS	Necesidades de clientes / Servicio al cliente	1	Bajo	3	Alto	4	Muy Alto	4	Muy Alto
	Requerimientos Legales / Incremento en las responsabilidades legales	1	Bajo	2	Medio	3	Alto	4	Muy Alto
	Imagen en el medio - Reputación	1	Bajo	2	Medio	3	Alto	4	Muy Alto
	Relación con proveedores	0	N/A	0	N/A	0	N/A	0	N/A
	Clientes Internos	1	Bajo	2	Medio	3	Alto	4	Muy Alto
	Financiera	1	Bajo	2	Medio	3	Alto	4	Muy Alto
TRANSFERENCIAS ENVIADAS SPI, SPL	Necesidades de clientes / Servicio al cliente	1	Bajo	1	Bajo	2	Medio	4	Muy Alto
	Requerimientos Legales / Incremento en las responsabilidades legales	1	Bajo	1	Bajo	1	Bajo	2	Medio
	Imagen en el medio - Reputación	1	Bajo	1	Bajo	1	Bajo	3	Alto
	Relación con proveedores	0	N/A	0	N/A	0	N/A	0	N/A
	Clientes Internos	1	Bajo	1	Bajo	1	Bajo	3	Alto
	Financiera	1	Bajo	1	Bajo	2	Medio	3	Alto
EMSION Y ENTREGA DE TARJETAS DE DEBITO	Necesidades de clientes / Servicio al cliente	1	Bajo	1	Bajo	2	Medio	3	Alto
	Requerimientos Legales / Incremento en las responsabilidades legales	0	N/A	0	N/A	0	N/A	1	Bajo
	Imagen en el medio - Reputación	0	N/A	0	N/A	1	Bajo	2	Medio
	Relación con proveedores	0	N/A	0	N/A	0	N/A	0	N/A
	Clientes Internos	0	N/A	0	N/A	1	Bajo	2	Medio
	Financiera	0	N/A	0	N/A	1	Bajo	2	Medio

Proceso	Área Impactada	Impacto del proceso (si el proceso no funciona)							
		Menos de 4 horas		4-8 horas		8-24 horas		Más de 48 horas	
DEPOSITOS CTAS CTES Y CUENTAS DE AHORRO	Necesidades de clientes / Servicio al cliente	1	Bajo	3	Alto	4	Muy Alto	4	Muy Alto
	Requerimientos Legales / Incremento en las responsabilidades legales	0	N/A	1	Bajo	1	Bajo	1	Bajo
	Imagen en el medio - Reputación	1	Bajo	2	Medio	4	Muy Alto	4	Muy Alto
	Relación con proveedores	0	N/A	0	N/A	0	N/A	0	N/A
	Clientes Internos	1	Bajo	1	Bajo	1	Bajo	1	Bajo
	Financiera	1	Bajo	1	Bajo	2	Medio	3	Alto
PAGO DE CHEQUES Y EFECTIVO EN CAJA	Necesidades de clientes / Servicio al cliente	1	Bajo	2	Medio	4	Muy Alto	4	Muy Alto
	Requerimientos Legales / Incremento en las responsabilidades legales	1	Bajo	1	Bajo	2	Medio	2	Medio
	Imagen en el medio - Reputación	1	Bajo	2	Medio	3	Alto	4	Muy Alto
	Relación con proveedores	0	N/A	0	N/A	0	N/A	0	N/A
	Clientes Internos	1	Bajo	1	Bajo	2	Medio	3	Alto
	Financiera	1	Bajo	1	Bajo	2	Medio	3	Alto
PAGOS VARIOS EN CAJA	Necesidades de clientes / Servicio al cliente	1	Bajo	2	Medio	3	Alto	4	Muy Alto
	Requerimientos Legales / Incremento en las responsabilidades legales	0	N/A	0	N/A	0	N/A	0	N/A
	Imagen en el medio - Reputación	1	Bajo	1	Bajo	2	Medio	2	Medio
	Relación con proveedores	0	N/A	0	N/A	0	N/A	0	N/A
	Clientes Internos	1	Bajo	1	Bajo	1	Bajo	1	Bajo
	Financiera	1	Bajo	1	Bajo	1	Bajo	1	Bajo

Anexo 7- Matriz de Impacto financiero Front Office

Proceso	Rango	Transaccional
		No. de transacciones
APERTURA, CUADRE Y CIERRE DE BOVEDA	Menos de 4 horas	- Apertura de Bóveda es diaria
	4-8 horas	- Cuadre y cierre de bóveda es diario
	8-24 horas	- Apertura de Bóveda es diaria - Cuadre y cierre de bóveda es diario
	Más de 48 horas	- Apertura de Bóveda es diaria - Cuadre y cierre de bóveda es diario
INCREMENTO DE EFECTIVO EN BOVEDA	Menos de 4 horas	N/A
	4-8 horas	- Incremento de efectivo se realiza a diario considerando la necesidad de la agencia
	8-24 horas	- Incremento de efectivo se realiza a diario considerando la necesidad de la agencia
	Más de 48 horas	- Incremento de efectivo se realiza a diario considerando la necesidad de la agencia
APERTURA, CUADRE Y CIERRE DE CAJAS	Menos de 4 horas	- Apertura de cajas es diario
	4-8 horas	- Cuadre y cierre de cajas es a diario
	8-24 horas	- Apertura de cajas es diario - Cuadre y cierre de cajas es a diario
	Más de 48 horas	- Apertura de cajas es diario - Cuadre y cierre de cajas es a diario

Proceso	Rango	Transaccional
		No. de transacciones
EMSION Y ENTREGA DE TARJETAS DE DEBITO	Menos de 4 horas	- Emisión y entrega de tarjetas de débito se encuentra en un plan piloto.
	4-8 horas	- Emisión y entrega de tarjetas de débito se encuentra en un plan piloto.
	8-24 horas	- Emisión y entrega de tarjetas de débito se encuentra en un plan piloto.
	Más de 48 horas	- Emisión y entrega de tarjetas de débito se encuentra en un plan piloto.
DEPOSITOS CTAS CTES Y CUENTAS DE AHORRO	Menos de 4 horas	56
	4-8 horas	448
	8-24 horas	1344
	Más de 48 horas	2688
PAGO DE CHEQUES Y EFECTIVO EN CAJA	Menos de 4 horas	148
	4-8 horas	296
	8-24 horas	888
	Más de 48 horas	1776
PAGOS VARIOS EN CAJA	Menos de 4 horas	26
	4-8 horas	51
	8-24 horas	153
	Más de 48 horas	306

Anexo 8- Matriz de impacto operacional Captaciones

Proceso	Área Impactada	Impacto del proceso (si el proceso no funciona)							
		Menos de 4 horas		4-8 horas		8-24 horas		Más de 48 horas	
APERTURA DE INVERSIONES A PLAZO	Necesidades de clientes / Servicio al cliente	2	Medio	3	Alto	4	Muy Alto	4	Muy Alto
	Requerimientos Legales / Incremento en las responsabilidades legales	1	Bajo	2	Medio	4	Muy Alto	4	Muy Alto
	Imagen en el medio - Reputación	1	Bajo	2	Medio	4	Muy Alto	4	Muy Alto
	Relación con proveedores	0	N/A	0	N/A	0	N/A	0	N/A
	Clientes Internos	1	Bajo	1	Bajo	2	Medio	3	Alto
	Financiera	1	Bajo	2	Medio	3	Alto	4	Muy Alto
RENOVACIÓN DE INVERSIONES A PLAZO	Necesidades de clientes / Servicio al cliente	1	Bajo	2	Medio	3	Alto	4	Muy Alto
	Requerimientos Legales / Incremento en las responsabilidades legales	1	Bajo	2	Medio	3	Alto	4	Muy Alto
	Imagen en el medio - Reputación	1	Bajo	2	Medio	3	Alto	4	Muy Alto
	Relación con proveedores	0	N/A	0	N/A	0	N/A	0	N/A
	Clientes Internos	1	Bajo	2	Medio	3	Alto	4	Muy Alto
	Financiera	1	Bajo	2	Medio	3	Alto	4	Muy Alto
CANCELACIÓN - PRECANCELACIÓN INVERSIONES A PLAZO	Necesidades de clientes / Servicio al cliente	3	Alto	3	Alto	4	Muy Alto	4	Muy Alto
	Requerimientos Legales / Incremento en las responsabilidades legales	3	Alto	3	Alto	4	Muy Alto	4	Muy Alto
	Imagen en el medio - Reputación	3	Alto	3	Alto	4	Muy Alto	4	Muy Alto
	Relación con proveedores	0	N/A	0	N/A	0	N/A	0	N/A
	Clientes Internos	3	Alto	3	Alto	4	Muy Alto	4	Muy Alto
	Financiera	2	Medio	2	Medio	2	Medio	2	Medio

Anexo 9- Matriz de impacto financiero Captaciones

Proceso	Rango	Transaccional
		No. de transacciones
APERTURA DE INVERSIONES A PLAZO	Menos de 4 horas	1
	4-8 horas	2
	8-24 horas	6
	Más de 48 horas	12
RENOVACIÓN DE INVERSIONES A PLAZO	Menos de 4 horas	6
	4-8 horas	11
	8-24 horas	33
	Más de 48 horas	66
CANCELACIÓN - PRECANCELACIÓN INVERSIONES A PLAZO	Menos de 4 horas	2
	4-8 horas	4
	8-24 horas	12
	Más de 48 horas	24

Anexo 10- Matriz de impacto operacional Colocaciones

Proceso	Área Impactada	Impacto del proceso (si el proceso no funciona)							
		Menos de 4 horas		4-8 horas		8-24 horas		Más de 48 horas	
CONCESIÓN CRÉDITO CANAL AUTOMOTRIZ	Necesidades de clientes / Servicio al cliente	0	N/A	0	N/A	2	Medio	3	Alto
	Requerimientos Legales / Incremento en las responsabilidades legales	0	N/A	0	N/A	0	N/A	0	N/A
	Imagen en el medio - Reputación	0	N/A	1	Bajo	2	Medio	3	Alto
	Relación con proveedores	0	N/A	0	N/A	0	N/A	0	N/A
	Clientes Internos	0	N/A	0	N/A	0	N/A	2	Medio
	Financiera	0	N/A	0	N/A	2	Medio	3	Alto
CONCESIÓN CRÉDITO CANAL BANCA	Necesidades de clientes / Servicio al cliente	0	N/A	0	N/A	2	Medio	3	Alto
	Requerimientos Legales / Incremento en las responsabilidades legales	0	N/A	0	N/A	0	N/A	0	N/A
	Imagen en el medio - Reputación	0	N/A	1	Bajo	2	Medio	3	Alto
	Relación con proveedores	0	N/A	0	N/A	0	N/A	0	N/A
	Clientes Internos	0	N/A	0	N/A	0	N/A	2	Medio
	Financiera	0	N/A	0	N/A	2	Medio	3	Alto
ANÁLISIS DE CRÉDITOS	Necesidades de clientes / Servicio al cliente	0	N/A	0	N/A	1	Bajo	3	Alto
	Requerimientos Legales / Incremento en las responsabilidades legales	0	N/A	0	N/A	0	N/A	0	N/A
	Imagen en el medio - Reputación	0	N/A	0	N/A	1	Bajo	3	Alto
	Relación con proveedores	0	N/A	0	N/A	0	N/A	0	N/A
	Clientes Internos	0	N/A	0	N/A	1	Bajo	3	Alto
	Financiera	0	N/A	0	N/A	0	N/A	0	N/A
APROBACIÓN DE CRÉDITOS	Necesidades de clientes / Servicio al cliente	0	N/A	0	N/A	1	Bajo	3	Alto
	Requerimientos Legales / Incremento en las responsabilidades legales	0	N/A	0	N/A	0	N/A	0	N/A
	Imagen en el medio - Reputación	0	N/A	0	N/A	1	Bajo	3	Alto
	Relación con proveedores	0	N/A	0	N/A	0	N/A	0	N/A
	Clientes Internos	0	N/A	0	N/A	1	Bajo	3	Alto
	Financiera	0	N/A	0	N/A	0	N/A	0	N/A

Anexo 11- Evaluación de amenazas, vulnerabilidades y determinación del nivel de riesgo

Amenaza	Control	Vulnerabilidad	Indisponibilidades (Daños)	Interrupciones	Probabilidad	Impacto	Nivel de Riesgo
Instalación de dispositivos USB no autorizados en la red interna	Política de seguridad de la información Bloqueo de los puertos para el uso de dispositivos USB a través de la herramienta de Antivirus Charlas de concientización al momento que ingresa nuevo personal Controles de permiso de acceso realizados por Seguridad de la Información	No se ha realizado una depuración de los usuarios que mantiene acceso a los dispositivos USB	Pérdida parcial o total del servicio informático	Interrupción total o parcial de atención a clientes a nivel nacional (Procesos que requieren infraestructura tecnológica)	Media Alta	Baja	Media
Robo de identidad utilizando simuladores de sitios Web, mensaje de correo o actos de ingeniería social	Concienciación al personal del banco y a los clientes de esta modalidad de estafa. Instalación de certificados digitales de seguridad Sistemas de monitoreo y antiphishing Soporte a clientes ante eventos de violación	No identificada	Pérdida parcial o total del servicio informático	Interrupción total o parcial de atención a clientes a nivel nacional (Procesos que requieren infraestructura tecnológica)	Media	Media	Alta
Acceso no autorizado a la red del banco para obtener y/alterar información sensible	Políticas que definen controles para conexiones hacia la red del banco Firewall de seguridad perimetral e interna Sistemas de autenticación a la red y aplicaciones Procedimientos y políticas internas que establece la responsabilidad de mantener las claves de acceso de manera confidencial Ethical Hacking programados Control de virus	No identificada	Pérdida parcial del servicio informático	Interrupción parcial de atención a clientes a nivel nacional (Procesos que requieren infraestructura tecnológica)	Media	Media	Alta

	Bloqueo de contenido sospechoso en el correo Instalación de antivirus Actualización de parches y definiciones Bloqueo de dispositivos USB Bloqueo de instalación del software no permitido Controles de permisos de acceso realizados por seguridad de la información						
Utilización de herramientas o Software no licenciado o no autorizado (Software pirata)	Permisos a nivel de usuario para no poder instalar programas no licenciados Filtrado de la navegación por funciones Bloqueo de puertos USB Políticas y procedimientos de seguridad Controles de permisos de acceso realizados por seguridad de la información	No identificada	Pérdida parcial o total del servicio informático	Interrupción total o parcial de atención a clientes a nivel nacional (Procesos que requieren infraestructura tecnológica)	Media Alta	Media	Alta
Interrupción o fluctuaciones del suministro eléctrico	Contar con un generador de energía para el edificio matriz del banco Contrato de mantenimiento del generador de energía Contar con UPS para precautelar la continuidad de	No existe un inventario de repuestos de equipos críticos No hay plantas de energía eléctrica en	Pérdida total del servicio informático	Interrupción de atención a clientes a nivel nacional (Procesos que requieren infraestructura tecnológica)	Media Alta	Media Baja	Alta

	energía eléctrica Contar con un contrato de mantenimiento de UPS en la matriz Monitoreo en sitio con personal 24x7	las agencias Contrato de mantenimiento de UPS en agencias					
Daños en los ascensores	Escaleras de emergencia Salidas de emergencia Señalización de las salidas de emergencia Mantenimiento mensual de los ascensores	En el proceso de inducción del personal nuevo no se considera el plan de emergencia para cada agencia	Dificultad parcial de acceso al edificio del Banco ABC	Interrupción parcial de atención a clientes	Media	Baja	Baja
Daños o fallas en el sistema de climatización del Data Center	Aire acondicionado de acuerdo a las características del Data Center Monitoreo en sitio con personal 24x7	Falta de un equipo de climatización backup Implementar software de monitoreo	Pérdida parcial o total del servicio informático	Interrupción total o parcial de atención a clientes a nivel nacional (Procesos que requieren infraestructura tecnológica)	Media Alta	Media	Alta
Daño o falla en central telefónica del Data Center	Mantener contrato del servicio de soporte Monitoreo de Log Monitoreo en sitio con personal 24x7	El sitio alterno de procesamiento ubicado en la localidad Ibarra permite levantar únicamente el CORE T24 y SFC Reporting, debe s	Perdida de comunicación con las oficinas	Interrupción de atención al cliente en oficinas afectadas	Media	Media Baja	Media

Daño o falla en componentes de telecomunicaciones (Switch o Routers)	Contrato de servicios con proveedor Level 3 Mantener un anillo de datos redundante Se mantiene un router principal y uno secundario Monitorean sitio con personal 24x7	Mantener Switch de Backup	Perdida de comunicación con las oficinas Pérdida del servicio informático en oficinas afectadas	Interrupción de atención al cliente en oficinas afectadas (Procesos que requieren infraestructura tecnológica)	Media Alta	Media	Alta
Daño o falla en el banco de transformadores del edificio matriz	Mantener un generador UPS redundantes de 60 KVA UPS de 20 KVA dedicado al Data Center Tableros de transferencia Contrato de mantenimiento de UPS Contrato de mantenimiento generador Monitoreo en sitio con personal 24x7	No hay mantenimientos, revisiones periódicas de instalaciones eléctricas	Pérdida total del servicio informático	Interrupción de atención a clientes a nivel nacional (Procesos que requieren infraestructura tecnológica)	Media Alta	Media	Alta
Daño o falla en los discos donde reside la base de datos de producción	Respaldo diario de la base de datos Respaldo de la información en cinta Respaldo de la información se custodia en la	Equipo de base de datos de Backup no respalda en línea El sitio al término de procesamiento	Pérdida total o parcial del servicio informático	Interrupción de atención a clientes a nivel nacional (Procesos que requieren infraestructura	Media Baja	Media	Media

	localidad de Ibarra	ubicado en la localidad de Ibarra permite levantar únicamente el CORE y SFC Reporting, debe ser activado manualmente, no hay personal capacitado de la localidad de Ibarra que lo active		tecnológica)			
Daño o falla en los generadores y sus componentes, del edificio matriz	Generador de energía para el edificio matriz del banco Contrato de mantenimiento del generador de energía UPS para precautelar la continuidad de energía eléctrica Monitoreo en sitio con personal 24x7	No se realizan pruebas periódicas del funcionamiento de la planta de energía eléctrica No existe un inventario de repuestos de equipos críticos No hay plantas de energía eléctrica en las agencias	Pérdida total del servicio informático	Interrupción de atención a clientes a nivel nacional (Procesos que requiere infraestructura tecnológica)	Media Alta	Media	Alta
Daño o falla en UPS	Los UPS se encuentran instalados a distintas tomas de luz, su capacidad es de 60 KVA	No se mantiene visible los números de contacto del	Equipos susceptibles a daños por falas	Interrupción de atención a clientes a nivel nacional	Baja	Media Baja	Baja

	Planta de energía eléctrica para el edificio Alertas de daños o mal funcionamiento del UPS Conexión a tierra Contratos de mantenimientos preventivos de los UPS vigentes Monitoreo en sitio con personal 24x7	proveedor en caso de daños en el UPS No todo el personal conoce el procedimiento a seguir en caso de daños del UPS	de energía	(Procesos que requieren infraestructura tecnológica)			
Daños severos en los servidores críticos	Mantener contratos de mantenimiento de Hardware Mantener contratos de mantenimiento de software Mantener la temperatura y humedad adecuada para los servidores Mantener respaldos de información Mantener equipos de protección para la alimentación eléctrica como UPS Revisión de Logs y su monitoreo Monitoreo en sitio con personal 24x7	Contar con el presupuesto para mantener los contratos	Pérdida total del servicio informático	Interrupción de atención a clientes a nivel nacional (Procesos que requieren infraestructura tecnológica)	Media Baja	Media Alta	Alta
Errores en la configuración de hardware de misión critica	Mantener respaldos de la información Llevar un registro de los cambios pasos a producción Monitoreo en sitio con personal 24x7	No identificada	Demoras en la ejecución de tares Problemas en aplicaciones que no permitan	Interrupción de atención a clientes a nivel nacional (Procesos que requieren infraestructura	Media Alta	Media	Alta

			brindar los servicios a los clientes	tecnológica)			
Fallas o daños en los equipos del sistema de distribución eléctrica interna	Mantener contrato de mantenimiento de UPS en la matriz Contar con un generador de energía eléctrica Monitoreo en sitio con personal 24x7	No identificada	Pérdida total del servicio informático	Interrupción de atención a clientes a nivel nacional (Procesos que requieren infraestructura tecnológica)	Media Alta	Media	Alta
Caída del sistema por agotamiento de recursos (memoria, capacidad de almacenamiento, canales de comunicación, etc.)	Manejar turnos para el procesamiento del COB Manejar un Flujo secuencial de pasos para el procesamiento de COB Manejar los respaldos antes y después del COB Manejar respaldos previos a los cambios o afectación en producción Manejar documentos de pasos a producción Llevar registros de pasos a producción Monitoreo en sitio con personal 24x7	No contar con el personal necesario para cubrir las necesidades	Pérdida total del servicio informático	Interrupción de atención a clientes a nivel nacional (Procesos que requieren infraestructura tecnológica)	Media Alta	Media Baja	Alta
Pérdida o falla en el almacenamient	Administración de cambios de configuración Controles y periodicidad sobre la verificación del	Mantener los medios magnéticos para obtener los	Pérdida total del servicio	Interrupción de atención a clientes a nivel nacional	Media Baja	Media	Media

o de datos	estado de la base de datos Mantener respaldos de información contratos de mantenimiento de Hardware	respaldos	informático	(Procesos que requieren infraestructura tecnológica)			