PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE ECONOMÍA Y GESTIÓN EMPRESARIAL

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGÍSTER EN ADMINISTRACIÓN DE EMPRESAS CON MENCIÓN GERENCIA DE LA CALIDAD Y PRODUCTIVIDAD

PROYECTO DE DESARROLLO

MODELO DE GESTIÓN DE RIESGOS DE PROVEEDORES CRÍTICOS DE CONTINUIDAD DEL NEGOCIO DE UNA INSTITUCIÓN FINANCIERA DEL ECUADOR

PAULINA ELIZABETH PINO BOADA

DIRECTOR: MBA. JUAN CARLOS PIÑUELA

LÍNEA DE INVESTIGACIÓN: GESTIÓN ESTRATÉGICA DE LAS ORGANIZACIONES

QUITO, AGOSTO - 2025

DIRECTOR

MBA. Juan Carlos Piñuela

LECTORES

Mgtr. Elisa Bravo

DEDICATORIA

A Dios, por ser mi fortaleza en los momentos más difíciles. Junto con el inicio de esta maestría enfrenté una de las pruebas más difíciles de mi vida, y fue su voluntad, su amor y las fuerzas que puse en mi corazón lo que me permitió continuar, mantenerme de pie y seguir avanzando. Gracias a Él hoy puedo seguir adelante con mi vida y culminar este importante camino.

A mi esposo, quien ha sido mi compañero incondicional en cada uno de mis desafíos, brindándome su apoyo, comprensión y el impulso necesario en los momentos en que más lo he necesitado.

A mis hijos, que a su corta edad supieron entender mis ausencias durante el desarrollo de esta maestría, y por permitirme ser para ellos un ejemplo de dedicación, esfuerzo y resiliencia.

A mi mami, quien con su ejemplo de vida nos ha enseñado que los límites solo existen si nosotros los ponemos, y que con perseverancia y determinación siempre es posible alcanzar aquello que nos proponemos, e ir más allá.

A mi hermana, por acompañarme siempre, tanto en los momentos buenos como en los menos buenos. Gracias por tu apoyo constante a lo largo de mi vida y por estar presente para mis hijos cuando debí ausentarme por mis obligaciones.

AGRADECIMIENTO

A mi familia, por su amor, comprensión y apoyo incondicional en cada uno de mis proyectos, y por haber sacrificado tiempo en familia para permitirme dedicarlo a mis estudios y responsabilidades académicas.

A Giovanni quien, cuando las circunstancias personales y de salud me hicieron dudar de continuar, supo motivarme a no rendirme, animándome a seguir.

A Carla, quien me impulso a dar el paso que faltaba y me brindó el apoyo y la confianza necesaria para retomar este camino académico.

A Elisa, por el esfuerzo y ayuda que contribuyo para que esto sea posible.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN EJECUTIVO

La creciente dependencia de proveedores externos en el sector financiero incrementa la exposición a riesgos operativos que pueden afectar la continuidad del negocio ante eventos disruptivos. En este contexto, surge la necesidad de contar con mecanismos estructurados que permitan evaluar la resiliencia de los proveedores críticos y su impacto en los procesos institucionales.

La metodología desarrollada de gestión de riesgos para la evaluación de proveedores críticos en la Gestión de Continuidad del Negocio (BCM), propósito del presente trabajo, está alineada con las mejores prácticas internacionales establecidas en la norma IS0 22301:2019 y los lineamientos regulatorios del Digital Operational Resillience Act.

La investigación adopta un enfoque empírico-aplicado de carácter cualitativo, basado en la revisión de literatura normativa regulatoria y el análisis de impacto al negocio (BIA), para identificar procesos críticos y su dependencia de proveedores externos. A partir de este análisis se diseñó un modelo metodológico estructurado en siete dominios.

Como resultado, se desarrolló una matriz de evaluación ponderada que permite analizar el nivel de madurez de los proveedores críticos en cada dominio y clasificarlo según su grado de cumplimiento. Esta herramienta facilita la identificación de brechas y la priorización de acciones de mejora orientadas a fortalecer la resiliencia operativa.

Se concluye que la aplicación de una metodología estructurada contribuye a mejorar la gestión de riesgos de continuidad en IFI´s, al proporcionar criterios homogéneos para la identificación de vulnerabilidades y la toma de decisiones informadas.

Palabras Clave: Continuidad del negocio, Gestión de riesgos, Institución financiera, Metodología, Proveedores críticos.

ABSTRACT

The increasing dependence on external providers in the financial sector increases exposure to operational risks that may affect business continuity during disruptive events. In this context, there is a need for structured mechanisms that allow organizations to assess the resilience of critical providers and their impact on institutional processes.

The risk management methodology developed for the evaluation of critical suppliers in Business Continuity Management (BCM), which constitutes the purpose of this study, is aligned with international best practice established in ISO 22301:2019 and the regulatory guidelines of the Digital Operational Resilience Act.

The research adopts an empirical-applied qualitative approach based on the review of regulatory and normative literature and on Business Impact Analysis (BIA) to identify critical processes and their dependency on external suppliers. Based on this analysis, a methodological model was designed, structured into seven evaluation domains.

As a result, a weighted evaluation matrix was developed to analyze the maturity level of critical suppliers in each domain and classify them according to their level of compliance. This tool facilitates the identification of gaps and the prioritization of improvement actions aimed at strengthening operational resilience.

It is concluded that the application of a structured methodology contributes to improving business continuity risk management in financial institutions by providing consistent criteria for identifying vulnerabilities and supporting informed decision-making.

Keywords: *Business Continuity, Risk Management, Financial Institution, Methodology, Critical Suppliers.*

INTRODUCCIÓN

El sector financiero desempeña un papel fundamental en la estabilidad económica de cualquier país, gracias al rol en la intermediación financiera, la gestión de recursos y el soporte a las actividades productivas. En particular, las instituciones financieras, al manejar grandes volúmenes de datos y montos económicos como parte de su ejercicio de intermediación, deben garantizar la continuidad de sus operaciones en todo momento, lo cual siempre está en la palestra pública por los hechos vividos como país años atrás. La alta dependencia de tecnología y proveedores externos hace que la gestión de riesgos en estos procesos sea un reto constante. En este contexto, el análisis de la gestión de continuidad del negocio se presenta como una herramienta esencial para minimizar los riesgos que podrían interrumpir los servicios ofrecidos a los clientes.

En los últimos años, la gestión de continuidad del negocio ha adquirido mayor relevancia dentro de las organizaciones financieras, debido al incremento de materialización de riesgos asociados a eventos tecnológicos, fallas en la infraestructura, incidentes cibernéticos y dependencia de terceros. En este sentido, los proveedores externos que brindan servicios tecnológicos, telecomunicaciones, infraestructura en la nube o plataformas bancarias críticas se han convertido en actores claves para la operación diaria de las instituciones financieras, lo que hace necesario evaluar su capacidad para mantener la continuidad de los servicios antes escenarios de interrupción.

La institución financiera en cuestión se enfrenta a una creciente necesidad de fortalecer sus mecanismos de gestión de continuidad, especialmente en lo que respecta a la relación con proveedores estratégicos. Entre los principales problemas identificados se encuentra la desalineación entre los tiempos de recuperación definidos por la organización y los niveles incluidos en el servicio, así como la ausencia de criterios estandarizados para evaluar su capacidad de respuesta ante eventos disruptivos y la ausencia de cláusulas claras en los contratos que aseguren la recuperación en tiempos adecuados. Estas limitaciones pueden generar incertidumbre en situaciones de contingencia y afectar la capacidad de la institución para mantener la continuidad de los servicios críticos.

Ante esta problemática, el objetivo del presente trabajo es desarrollar una metodología de gestión de riesgos para la evaluación de proveedores críticos en el marco de la Gestión de Continuidad del Negocio, alineada con las mejores prácticas internacionales establecidas en

la norma ISO 22301:2019 y con los lineamientos regulatorios del Digital Operational Resilience Act. (DORA). Esta propuesta busca proporcionar una herramienta estructura que permite identificar brechas en la gestión de continuidad de los proveedores y fortalecer la resiliencia operativa de la organización.

El desarrollo de este proyecto se basa en un enfoque empírico-aplicado de carácter cualitativo, basado tanto en la normativa regulatoria y el análisis del contexto organizacional así como en la aplicación de un análisis de impacto al negocio (BIA) que permita identificar proveedores críticos y su dependencia con proveedores externos. A partir de este análisis surge el diseño de un modelo metodológico estructurado en dominios de evaluación que permiten medir el nivel de madurez de los proveedores en materia de continuidad del negocio.

Los principales hallazgos del estudio dejan en claro las brechas en la evaluación sistemática de proveedores críticos, así como la necesidad de disponer de criterios homogéneos que permitan analizar la capacidad de recuperación frente a interrupciones. En respuesta a esta situación, se propone una metodología de evaluación basada en dominios de continuidad y una matriz de valoración ponderada que facilita la clasificación de proveedores según su nivel de cumplimiento.

Finalmente, se recomienda la adopción progresiva de la metodología propuesta como parte de los procesos institucionales de gestión de riesgos y continuidad del negocio, con el fin de fortalecer la resiliencia organizacional y mejorar la capacidad de respuesta frente a eventos que puedan afectar la disponibilidad de los servicios críticos.

CAPÍTULO 1

ANÁLISIS INSTITUCIONAL Y CARACTERIZACIÓN DEL PROBLEMA

1.1. Descripción del sector financiero de la unidad de análisis

El sector financiero en el Ecuador constituye una pieza clave en el desarrollo de la economía y el del país, los desafíos que enfrenta en la actualidad no han dejado de ser retadores como en años anteriores lo fue, principalmente en términos de inclusión, canales de atención, uso de servicios y disponibilidad de canales, este sector representa el 3,6% del PIB nacional (Banco Central, 2025) considerando actividades de intermediación de bancos, cooperativas y mutualistas, así como los relacionados con servicios auxiliares de seguros, fondos de inversión y fintechs.

El impacto del que hacer del sector financiero para el Ecuador, dada la transversalidad de su gestión está estrechamente relacionado con el flujo y desempeño de todos los sectores productivos, así lo reflejan la evolución de las variables de agregados monetarios tales como reservas internacionales, captaciones del sistema financiero nacional y crédito al sector privado, y lo hacen a través de las estadísticas presentadas por el Banco Central del Ecuador, resultante de la agregación y consolidación de la información financiera y monetaria a través de la siguiente representación:

Figura 1. Cobertura de las Estadísticas Monetarias y Financiera

Fuente: Banco Central del Ecuador

La estructura del sector financiero está conformada por bancos privados, cooperativas de ahorro y crédito, mutualistas y otras entidades que ofrecen productos orientados tanto al financiamiento como al ahorro e inversión. Dentro de este marco, los bancos privados cuentan con una regulación estricta, pues se encuentran bajo la supervisión directa de la Superintendencia de Bancos, entidad que emite lineamientos para la gestión, entre los cuales podemos mencionar los relacionados con riesgo operativo, específicamente el LIBRO I.- Normas de Control para las Entidades de los Sectores Financieros Público y Privado, Capítulo V, Sección VII: Servicios Provistos por Terceros.

En los últimos años, el comportamiento del sector y sus indicadores han mostrado mejoras, es así como para el año 2024 según información del Banco Central del Ecuador, las captaciones de ahorro tuvieron un crecimiento anual del 15,8%, lo cual se traduce en confianza del público en las instituciones financieras. Dentro de este mismo informe, se indica que el patrimonio neto del sistema superó los USD 2.128 millones, lo cual representa el 33,2% de crecimiento, y la liquidez alcanzó niveles históricos con más de USD 4.000 millones, impulsada principalmente por las remesas y depósitos. Por otro lado, respecto del crédito este se expandió impulsado por tasas de interés más competitivas, donde el interés activo referencial bajo del 11% a menos del 8%, lo que dinamiza el consumo y la inversión (Ordóñez-Granda et al., 2020).

Basados en indicadores y resultados, podemos decir que el impacto de la industria financiera en la economía del Ecuador se manifiesta en los niveles macroeconómico y microeconómico. En el primer caso es determinante para la estabilidad monetaria, pues canaliza el ahorro hacia la inversión como parte de la intermediación financiera y facilita la circulación de dinero. Por otro lado, y a nivel microeconómico, hace posible que tanto empresas como personas puedan acceder a financiamiento, realizar transacciones y dinamizar la economía, siendo participes activos del sistema económico (Zsidisin y Ritchie, 2008). Esto además contribuye a los esfuerzos que por varios años las instituciones de gobiernos han estado realizando para consolidar la inclusión financiera, especialmente el zonas rurales y sectores tradicionalmente excluidos.

La unidad de análisis corresponde a un banco privado de amplia trayectoria en el país, que se distingue por su cobertura nacional y por la diversidad de servicios que ofrece a personas naturales y empresas (Quituisaca-León et al., 2021). Entre sus productos destacan principalmente las tarjetas de crédito, y se suman las inversiones y

financiamiento empresarial, así como en el tiempo se ha agregado créditos de consumo relacionados a las mismas tarjetas de crédito, y como cuentas de ahorro y corriente, los canales de atención habilitados son físicos y digitales, destacando este último dada la visión estratégica que está en marcha para los siguientes años, la cual busca disponibilidad en el mercado un modelo de banco digital nativo y estructurado en torno a procesos tecnológicos esenciales, para lo cual ha realizado fuertes inversiones que le permitan lograr sus objetivos estratégicos. Este nivel de digitalización ha fortalecido la relación con sus clientes, pero al mismo tiempo ha generado una fuerte dependencia de la tecnología y de ciertos proveedores externos que sostienen su operación diaria.

Como parte de este contexto, la transformación digital ha sido un factor diferenciador entre las instituciones financiera, la adopción de la tecnología en los servicios prestados, como lo son aplicaciones móviles, plataformas web, analítica de datos, cajeros automáticos y medios de contacto automatizados (Yánez & Palabras, 2012), han mejorado la eficiencia operativa, pero también han generado una alta dependencia tecnológica, lo que expone al sistema a una serie de riesgos como indisponibilidad de sus canales de atención o de sus plataformas, ciberataques, entre otros.

Dado el alto grado de digitalización que dispone la unidad de análisis, la mayor parte de sus procesos críticos están sustentados en sistemas tecnológicos propios o los de sus proveedores, todo incidente que produzca una indisponibilidad ya sea de sus canales de atención o de los servicios mismos, puede afectar la continuidad del negocio con incidencia negativa sobre la experiencia al cliente y su reputación institucional, además de generar pérdidas económicas propias o de socios de negocio como lo son sus establecimientos afiliados.

Cabe señalar que la dinámica del sector obliga a las instituciones financieras a mantener estándares altos de disponibilidad, seguridad y continuidad del negocio. El ente de control y su normativa vigente emitida, determina las acciones que los bancos están obligados a seguir ante todo incidente que implique interrupción de servicios con afectación a los clientes por 30 minutos o más, entre las cuales podemos mencionar la comunicación inmediata a la Superintendencia de Bancos por los canales determinados, así como la actualización del estado de los servicios cada 5 minutos luego de la comunicación inicial e informes posteriores al suceso, esto conforme lo dispuesto en el Código Orgánico Monetario y Financiero y las resoluciones complementarias emitidas por dicho

organismo. Esta exigencia refleja la importancia de asegurar la continuidad del negocio, ya que una falla prolongada puede generar impactos no solo operativos, sino también reputacionales, legales y financieros con proyección al sector mismo, en función del tamaño y número de clientes de la institución afectada.

En este contexto la gestión de riesgos asociados a los proveedores críticos se convierte en un aspecto estratégico. La operación misma de una institución financiera está levantada sobre una red compleja de servicios que incluyen a terceros, tales como core financiero, bases de datos, enlaces de comunicación e internet, cajeros automáticos, infraestructura tecnológica en los centros de datos y en nube, infraestructura de seguridad, software de aplicaciones, comunicaciones, entre los relevantes. Estos componentes pueden estar provistos, operados o soportados en un proveedor, el cual debe garantizar su disponibilidad acorde a los requerimientos del negocio los cuales se trasladan en contratos a niveles de servicio y niveles de respuesta ante incidentes. Sin embargo, de acuerdo al relevamiento de información realizado con el experto de la unidad de análisis, los contratos no incluyen de manera explícita los tiempos de recuperación requeridos para el servicio contratado (RTO-Recovery Time Objective, RPO-Recovery Point Recovery) ni mecanismos efectivos de verificación y auditoría. Esto genera incertidumbre sobre la capacidad de respuesta frente a incidentes y la gestión de los mismos hasta la restauración completa del servicio, lo cual se hace aún más crítico cuando en determinados servicios se cuenta con un solo proveedor al no existir más alternativas en el mercado local.

Las buenas prácticas y marcos de referencia internacionales tal como:

- Norma internacional ISO 22301:2019
- Reglamento europeo DORA (Digital Operational Resilience Act)
- BCI Good Practice Guidelines 2018, Capítulo 3 (Analysis)
- ISO 31000:2018, Principio de “Contexto Organizacional
- ISO 27036-1:2014 (Information security for supplier relationships – Overview and concepts)

Definen acciones específicas que deben ser incorporadas en la gestión de terceros de instituciones financiera, con el objetivo de garantizar la continuidad del negocio y la resiliencia operativa.

Por su lado la ISO 22301:2019 incluye requisitos específicos para la evaluación de proveedores externos. Esta norma recomienda identificar los procesos críticos, establecer planes de recuperación, definir métricas de desempeño como RTO y RPO, y realizar pruebas periódicas para validar la resiliencia operativa propia y de terceros. De igual manera, enfatiza la necesidad de contar con acuerdos contractuales que incluyan cláusulas de salida, mecanismos de supervisión y planes de comunicación ante incidentes/contingencias.

Mientras que DORA que entra en vigor en enero 2025, introduce obligaciones específicas para las entidades financieras en relación con la gestión de proveedores tecnológicos críticos. DORA exige que los contratos incluyan disposiciones claras sobre niveles de servicio, derechos de acceso, auditoría, notificación de incidentes graves y supervisión de terceros. Además, extiende la responsabilidad hacia las llamadas cuartas partes, es decir, los proveedores de los proveedores, reconociendo el efecto dominó que puede comprometer la continuidad operativa de todo el ecosistema financiero, cuartas partes que hasta hace poco no contaban con un marco de evaluación al no incluirlas como parte de este entorno.

BCI Good Practice Guidelines 2018, establece la necesidad de identificar interdependencias externas (proveedores y servicios clave) como insumo fundamental del BIA. La norma ISO 31000:2018 por su lado plantea que la identificación de riesgos debe considerar el entorno externo, como la cadena de suministro, relaciones de terceros y contratistas clave. La norma ISO 27036-1:2014 introduce el concepto de identificación y gestión de relaciones con proveedores críticos desde la perspectiva de impacto y dependencia.

Dentro de este orden de ideas, la institución objeto de análisis enfrenta retos comunes al sector: la necesidad de evaluar no solo a sus proveedores directos, sino también toda la cadena de suministro, es decir, los proveedores de sus proveedores. Este efecto hace que la continuidad del negocio dependa de múltiples actores, lo cual incrementa el nivel de exposición a fallas. A esto se suma la existencia de contratos antiguos que han sido renovados de manera automática sin ajustes a las condiciones actuales, la falta de cláusulas de salida y la ausencia de una cultura consolidada de continuidad que incluya planes de comunicación claros ante los clientes cuando se presenta una contingencia,

temas que los marcos de referencia a usar marcan claramente la gestión requerida y que ahora no se está cumpliendo.

En resumen, el sector financiero ecuatoriano exige a sus actores mantener altos niveles de resiliencia y cumplir con normativas estrictas de gestión de riesgos. No obstante, los desafíos asociados a la tercerización de servicios críticos, la dependencia tecnológica y las brechas contractuales marcan la pauta para que las instituciones refuercen sus mecanismos de control, supervisión y gobernanza sobre los proveedores estratégicos, alineándose con estándares internacionales y regulaciones emergentes.

Es así que la unidad de análisis es adecuada para analizar el impacto económico de la indisponibilidad de uno o más de sus servicios críticos, su perfil institucional, alcance operativo y nivel de digitalización permiten observar con claridad como el fallo dentro de la cadena de valor puede afectar la economía, los negocios y la confianza misma en el sector financiero.

1.2. Dependencia de proveedores críticos y procesos tercerizados

Las entidades financieras para la ejecución de sus actividades, dependiendo de su naturaleza y tamaño, generalmente recurren a proveedores de productos o servicios, especialmente cuando dichos productos o servicios no corresponden al giro de su negocio (Avilés et al, 2025). Dichos proveedores contribuyen a que las organizaciones cumplan sus objetivos según sus estrategias comerciales. No obstante, existe un riesgo implícito en las actividades de las entidades financieras, e incluso de sus proveedores, asociadas a disrupciones tecnológicas y/o operativas que pueden afectar significativamente a los productos y servicios financieros ofertados a los clientes, ocasionando pérdidas financieras, reputacionales y/o regulatorias.

En la administración integral de riesgos es esencial la incorporación de herramientas que permitan mejorar la gestión de los procesos organizacionales a partir de la gestión de proveedores críticos en Continuidad del Negocio que desempeñan un rol clave en el funcionamiento de las actividades de la organización (Loján et al, 2017). En ese sentido, es fundamental que la unidad de análisis cuente con una metodología para la identificación, evaluación y gestión de proveedores que soportan la operación de los subprocesos críticos de la organización.

Según la norma ISO para Sistemas de Gestión de Calidad (SGD) 9001 “La organización debe determinar y aplicar criterios para la evaluación, supervisión del rendimiento y la reevaluación de proveedores externos, en función de su capacidad para proporcionar procesos o productos y servicios de acuerdo a las necesidades”. Asimismo, el estándar ISO para Sistemas de Continuidad del Negocio 22301 señala que, “La organización debe establecer, implementar y mantener un proceso de evaluación formal y documentado para determinar las prioridades, objetivos y metas de continuidad y recuperación. Este proceso debe incluir la evaluación de impactos de actividades disruptivas que apoyan los productos y servicios críticos de la organización, (…) incluyendo los proveedores, socios y otras partes interesadas relevantes.”

Con lo expuesto, para el banco es de vital importancia identificar los proveedores que brindan servicios o productos que sirven de insumo para los subprocesos críticos de la organización, a fin de evaluar su nivel de riesgo en Continuidad del Negocio y supervisar que cuenten con los requerimientos regulatorios mínimos, así como también de buenas prácticas, con la finalidad de garantizar la permanencia de sus servicios en caso de un evento disruptivo, además de cumplir con estándares internacionales de calidad en la gestión de Continuidad.

Figura 2. Esquema de dependencia de proveedores críticos y procesos tercerizados
Fuente: Elaboración propia.

En los últimos años las tendencias internacionales han registrado un importante cambio de visión en el enfoque de la administración en una Organización, incrementando la importancia de los procesos como medio para conseguir los objetivos y estrategias institucionales, por lo cual el banco ha definido su organización por procesos, orientando

los mismos al cliente (estrategia multicanal) (Olarte, 2016) . La implementación de un sistema de riesgo operativo efectivo conduce a una mejor toma de decisiones y permite que las empresas optimicen la relación entre ganancias y riesgos de todo tipo; en este esquema es importante establecer un modelo para administrar y controlar el riesgo a través de todas las líneas de negocio que permitan soportar el desarrollo de un programa de riesgo exitoso, alineado con la estrategia del Banco y considerando a todos los segmentos a los cuales la organización enfoca sus productos y servicios.

La estructura por procesos que dispone el banco está diseñada para sostener su normal operación como entidad financiera especializada en medios de pago, servicios de crédito e inversiones y seguros. Siguiendo las disposiciones de la Superintendencia de Bancos (SB), la unidad de análisis define para la asignación de procesos y actividades a las Líneas de Negocios. Esta estructura cuenta en su inventario con 17 macroprocesos, 50 procesos, 1200 subprocesos de los cuales mediante la ejecución del BIA se ha definido 48 subprocesos como críticos que están soportados en 80 recursos críticos.

Todos los procesos y subprocesos deberán clasificarse en las Líneas de Negocio establecidas para la Organización, focalizados en la atención multicanal al cliente y Banca digital integral, los subprocesos productivos y gobernantes deberán clasificarse en las líneas de negocio de acuerdo con los productos y servicios que generan para los segmentos definidos, a cada subproceso le deberá corresponder una sola línea de negocio y ningún subproceso puede permanecer sin clasificación, si algún subproceso gobernante o subproceso habilitante interviene en más de una línea de negocio, éste será clasificado en la línea de negocio según la metodología definida, la clasificación de los subprocesos en las Líneas de Negocio a efectos de determinación del capital por riesgo operativo deberá ser coherente con las definiciones de las Líneas de Negocio utilizadas, los riesgos identificados y sus respectivos controles serán definidos y monitoreados por líneas de negocios y serán revisados por Auditoría Interna según su planificación anual.

Para la clasificación de subprocesos por líneas de negocio, los procesos gobernantes y habilitantes que intervienen en más de una línea de negocio deberán ser asignados a aquellas que represente su mayor grado de contribución. Esta asignación se tomará considerando los siguientes criterios:

- Generación de ingresos, costos, activos y/o utilidades

- Nivel de impacto operativo o financiero sobre una línea específica, o
- El volumen de actividades o subprocesos que se ejecuten para dicha línea

En todos los casos, se buscará reflejar con precisión el vínculo funcional y estratégico del proceso con la línea de negocio correspondiente.

En lo que respecta a los procesos de soporte que prestan servicios transversales a múltiples líneas, serán clasificados en función de su alineación con la línea de negocio principal de la organización, entendida como aquella que concentra la mayor relevancia estratégica o volumen operativo.

La identificación de la información financiera de cada línea de negocio permite evaluar la naturaleza y efectos financieros de las actividades de negocio (ingresos, gastos, rentabilidad, activos e indicadores financieros) que genera cada línea y como aporta en la estrategia y en los resultados globales de la Organización (Liliana Rodríguez-Rojas, 2021a). Esta información financiera deberá ser validada por los niveles de aprobación correspondiente.

Es así que las líneas de negocio establecidas bajo las cuales se agruparán los subprocesos para el respectivo análisis de impacto de negocio son:

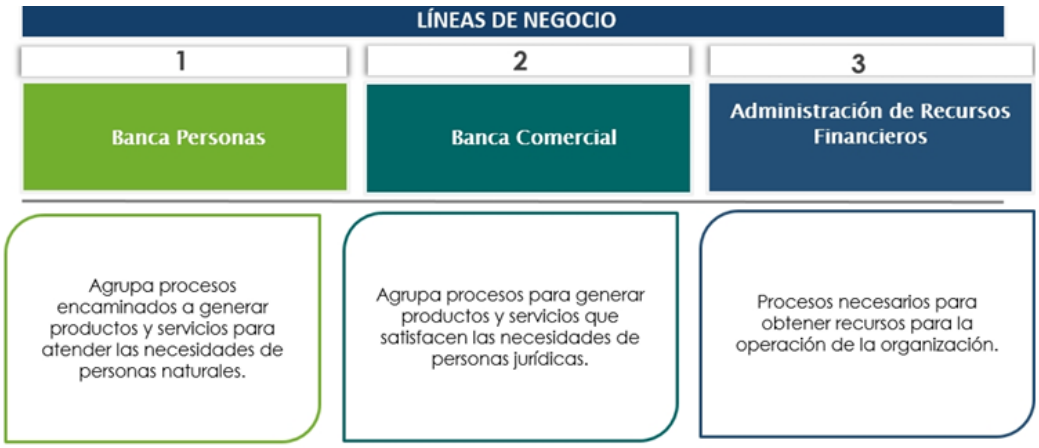

Figura 3. Líneas de Negocio bajo las cuales se agrupan los subprocesos
Fuente: Elaboración propia.

El literal d, de la Sección III Factores de Riesgo Operativo del Capítulo V, de la Norma de control para la gestión del Riesgo Operativo, Libro I.- Normas de control para las entidades de los sectores financieros público y privado, determina que, para la

administración de Continuidad del Negocio las entidades controladas deben aplicar los parámetros para la identificación de los procesos críticos, su punto y tiempos de recuperación definidos por el negocio; una vez identificados los procesos críticos, deben determinar las dependencias internas y externas; y, recursos de soporte para estos procesos, incluyendo tecnología, personal, proveedores, y otras partes interesadas.

Asimismo, en la evaluación y selección de estrategias de continuidad por cada proceso crítico que permitan mantener su operatividad, dentro del tiempo objetivo de recuperación definido para cada proceso, se debe tener en cuenta lo siguiente: la seguridad del personal, instalaciones alternas de trabajo, infraestructura alterna de procesamiento, información necesaria para el proceso; proveedores y aplicativos relacionados.

Adicional, conforme el art. 24 de la Sección VII de Servicios Provistos por Terceros, para mantener el control de los servicios provistos por terceros, incluidas las empresas de servicios auxiliares del sistema financiero, las entidades controladas deben implementar un proceso integral para la administración de proveedores de servicios que incluya las actividades previas a la contratación, suscripción, cumplimiento y renovación del contrato; para lo cual, deben cumplir, con lo siguiente:

- Definir mecanismos de gestión de riesgos asociados a los servicios provistos por terceros y que garanticen la gestión de la continuidad del negocio.
- Establecer políticas, procesos y procedimientos que aseguren el control y monitoreo de los servicios contratados, mediante la evaluación, gestión y vigilancia de estos, a fin de garantizar que se cumplan con aspectos de continuidad del negocio.
- Contar con proveedores alternos de los servicios que soportan a los procesos críticos, que tengan la capacidad de prestar el servicio para mitigar el riesgo de dependencia en un solo proveedor; en los casos de proveedor único, se debe solicitar al proveedor planes de continuidad probados actualizados, al menos, anualmente.

Por lo cual el Banco requiere implementar un modelo de gestión de riesgos de proveedores críticos de continuidad del negocio que permita categorizar y evaluar los proveedores de la organización considerando los criterios normativos y de buenas prácticas en Continuidad del Negocio. Esto deberá además facilitar el proceso de los usuarios de asociación de los proveedores a los subprocesos críticos que permita identificar los proveedores críticos, posterior a lo cual las áreas implementarán estrategias

de continuidad del negocio para los proveedores críticos, así como evaluarán la pertinencia de contar con proveedores alternos y planes de continuidad para proveedores únicos.

En la perspectiva que aquí se plantea, también se debe considerar la complejidad de trabajar con proveedores multinacionales. Estas empresas suelen regirse por decisiones de casas matrices en el extranjero, lo que dificulta ajustes específicos a la normativa local. A su vez, existen servicios provistos por un único actor en el mercado, lo que impide contar con alternativas inmediatas. En ambos casos, la capacidad de negociación se reduce y la continuidad queda condicionada a factores externos.

Otro punto relevante es la falta de cláusulas de salida claras en algunos contratos. Si un proveedor deja de operar o se niega a colaborar en cualquier actividad vital para la institución financiera, esta podría enfrentar serias dificultades para garantizar el servicio. A esto se suma que no siempre existe una cultura sólida de continuidad: en ciertas situaciones los proveedores no comunican los incidentes que acontecen ni hacen un análisis causa raíz que garantice que este tipo de eventos no se repitan, lo que limita la activación de planes de contingencia internos.

En función de lo planteado, el caso sujeto a estudio evidencia que la fuerte dependencia de procesos tercerizados convierte a los proveedores críticos en un punto vulnerable y determinante en la gestión de continuidad del negocio. Las limitaciones contractuales, la ausencia de evaluaciones integrales y la débil cultura de continuidad confirman la necesidad de establecer mecanismos más rigurosos de control y supervisión que fortalezcan la resiliencia institucional frente a posibles interrupciones.

1.3. Síntomas observables del problema

En el caso sujeto a estudio se han identificado diversos síntomas que evidencian limitaciones en la gestión de proveedores críticos y en la forma en que se administran los procesos tercerizados. Estos aspectos reflejan tanto debilidades contractuales como vacíos en la supervisión y en la cultura de continuidad. Para sintetizar los principales hallazgos, en la siguiente tabla se resumen los síntomas más representativos que afectan la capacidad de la institución para responder frente a eventos de interrupción.

Tabla 1. Síntomas observables en la gestión de proveedores críticos y continuidad del negocio

Síntoma identificado	Descripción
Desalineación de tiempos de recuperación	Los RTO y RPO definidos por la institución no están acordados contractualmente por los diferentes actores (contratante-proveedor).
Contratos antiguos y poco específicos	Existen acuerdos escuetos que no incluyen cláusulas de continuidad, salida ni atención de incidentes. Los contratos no se han adecuado a la realidad y exigencias presentes.
Dificultad con proveedores internacionales	Las decisiones dependen de casas matrices en el extranjero, lo que retrasa o impide ajustes locales.
Ausencia de control sobre cuartas partes	Los proveedores directos no evalúan a sus propios proveedores, generando un efecto dominó de fallas.
Escasa comunicación en incidentes	Falta de notificación cuando un incidente produce la indisponibilidad de servicios, lo que limita la activación oportuna de planes de contingencia.
Inexistencia de una cultura de continuidad consolidada	Se evidencia en la ausencia de pruebas periódicas y en la limitada preparación del personal para responder a crisis.
Evaluaciones de riesgos previo a la contratación insuficientes	La evaluación inicial de proveedor no contempla todos los parámetros que el proveedor está obligado a cumplir, se evalúa cumplimiento legal y financiero únicamente
Dependencia de proveedores únicos	Para servicios especializados existen proveedores únicos, así como también por directrices corporativas se impide la contratación de proveedores que son competencia

Fuente: Elaboración propia.

Como puede observarse en la tabla anteriormente expuesta se identifican distintos síntomas que reflejan fragilidades en la gestión de los proveedores críticos y en los procesos tercerizados. Uno de los más notorios es la ausencia de alineación entre los

tiempos de recuperación definidos por la institución y los que realmente ofrecen los proveedores. Aunque el banco establece internamente sus objetivos de recuperación (RTO y RPO), estos no siempre se plasman de manera explícita en los contratos. En la práctica, esto provoca que los proveedores no estén obligados a cumplir con los plazos requeridos, lo que incrementa la incertidumbre en situaciones de interrupción.

Otro síntoma evidente es la vigencia de contratos antiguos, algunos de ellos redactados en épocas donde la continuidad del negocio no tenía el mismo nivel de exigencia que hoy. Estos documentos resultan escuetos y carecen de cláusulas que detallen compromisos de recuperación, de salida o de soporte en procesos de migración hacia otros proveedores. En la actualidad, este vacío se convierte en un riesgo porque limita la capacidad de la institución para exigir respuestas claras en escenarios críticos.

Cabe señalar que la dependencia de proveedores internacionales también genera complicaciones visibles. En varios casos, la gestión de cambios o la adaptación a la normativa local depende de decisiones tomadas por casas matrices en el extranjero. Esto provoca demoras y, en algunos casos, la imposibilidad de ajustar las condiciones del servicio a lo que realmente demanda la institución.

Por otra parte, se observa que los proveedores directos no siempre extienden sus evaluaciones hacia sus propios socios estratégicos. La falta de control sobre estas "cuartas partes" produce un efecto dominó: si un tercero externo sufre una caída, la institución recibe el impacto de manera inmediata sin tener herramientas para prevenirlo ni exigir medidas correctivas.

En la perspectiva que aquí se plantea, otro síntoma relevante es la escasa comunicación de los proveedores cuando atraviesan incidentes. En algunos casos no informan oportunamente sobre fallas o limitaciones, lo que impide al banco activar a tiempo sus planes de contingencia internos. Esta carencia de información reduce la capacidad de reacción y transmite una sensación de improvisación frente al cliente final e incrementa los tiempos de indisponibilidad.

De igual forma, la inexistencia de una cultura de continuidad consolidada se hace visible en la falta de pruebas periódicas y en la limitada preparación del personal para responder

en situaciones de crisis. Esto deja en evidencia que, más allá de las políticas escritas, la práctica no siempre garantiza la resiliencia esperada.

Evaluaciones de riesgo previas a la contratación insuficientes: cuando se evalúa un nuevo proveedor, no se considera si es crítico o no, y las evaluaciones están considerando aspectos legales y financieros, sin incorporar análisis de continuidad, seguridad de la información, cumplimiento regulatorio o capacidad de recuperación ante desastres.

La dependencia de proveedores únicos ya sea por un servicio especializado, o por directivas corporativas que impiden la contratación de proveedores que son parte de grupos competidores comerciales, lo cual incrementa el riesgo de disrupción severa ante cualquier falla.

Además de estos síntomas, debemos considerar otros que afectan a la industria financiera, como es:

- Falta de integración del riesgo de terceros en el marco de gobernanza, en muchos casos, el riesgo asociado a proveedores críticos no está suficientemente incorporado en los órganos de gobierno corporativo ni en la agenda estratégica de la alta dirección, lo que limita el seguimiento estructurado y las decisiones oportunas.
- Exposición ante ciberataques de terceros: muchos proveedores tienen conexión lógica o física a los sistemas de la organización sin un adecuado control de accesos, lo que convierte a estos terceros en posibles vectores de ataque que comprometen la integridad y disponibilidad de los servicios.
- Débil transferencia de conocimiento: esto puede darse tanto en implementaciones realizadas por terceros, así como en procesos de cambio de proveedor. El cumplimiento de cronograma en nuevas implementaciones lleva a omitir procesos definidos y no transferir el conocimiento al personal interno generando una nueva dependencia. Por otro lado, los procesos de off boarding o migración suelen estar poco documentados, lo cual genera pérdidas de información crítica y retrasa la estabilización del nuevo servicio.

En resumen, los síntomas observables en el caso sujeto a estudio giran alrededor de vacíos contractuales, deficiencias en la supervisión de proveedores y carencias en la

comunicación y cultura de continuidad. Todos estos factores, al combinarse, incrementan el riesgo de interrupciones prolongadas, afectan la confianza de los clientes y exponen a la institución a impactos reputacionales y operativos significativos.

El modelo propuesto dentro del presente trabajo de investigación abordará principalmente los síntomas relacionados con:

- La falta de alineación contractual de los tiempos de recuperación (RTO y RPO)
- La ausencia de cláusulas específicas de continuidad del negocio en contratos vigentes
- Las limitaciones en la supervisión de terceros y cuartas partes
- Las deficiencias en la comunicación temprana de incidentes
- Evaluaciones incompletas para los nuevos proveedores
- Dependencia excesiva de proveedores nuevos o únicos

La priorización de estos síntomas se establecerá en función de dos criterios fundamentales; el nivel de impacto operativo que generan y la frecuencia con la que se presentan en los procesos críticos de la institución. De este modo, el modelo buscará reducir de manera efectiva los riesgos asociados a proveedores críticos, fortaleciendo tanto la capacidad de respuesta ante interrupciones, así como la resiliencia operativa de la institución financiera y la reducción a la exposición a eventos disruptivos, garantizando la continuidad y seguridad de los servicios ofrecidos al cliente final.

1.4. Importancia de la continuidad del negocio en entornos regulados

De acuerdo a Liliana Rodríguez-Rojas (2021b) en el sistema financiero, la continuidad del negocio no es solo una buena práctica, sino una exigencia regulatoria. La supervisión que ejerce la Superintendencia de Bancos establece que cualquier servicio de atención al cliente que permanezca inactivo más de treinta minutos debe ser reportado. Esta obligación refleja la sensibilidad del sector frente a interrupciones, ya que incluso una falla breve puede comprometer la confianza de los usuarios y afectar la estabilidad de la institución e incluso traspalarse al sector mismo.

Estas exigencias han ido evolucionando en el tiempo, pues a medida que las instituciones financieras iban cambiando sus modelos de atención el ente regulador establecía controles

sobre los mismos (Sitio web de la Superintendencia de Bancos), podemos mencionar las siguientes políticas y resoluciones que dan muestra de ellos:

- Resolución No. JB-2008-1202 (2008): las instituciones controladas debían implementar planes de contingencia y de continuidad, con el objetivo de garantizar su capacidad para operar de manera continua y así minimizar las pérdidas ante una interrupción mayor.
- Resolución JB2009-1405 (2009): La Superintendencia de Bancos emitió esta resolución en la cual obligaba a las nuevas instituciones financieras a implementar un sistema de control interno que les permitiera mitigar riesgos operacionales, incluyendo continuidad del servicio, lo cual debía ser cumplido dentro de los primeros noventa días de operación.
- Disposiciones sobre continuidad del negocio (2015-2016): El límite para la implementación de continuidad del negocio era octubre de 2016, los requisitos relacionados con tecnología debían cumplirse hasta diciembre 2015. Podemos considerar que esto marco el inicio de las exigencias formales en esta área.
- Resolución SB-CGPMC-2018-005 (2018): en línea con las exigencias a las entidades reguladas, la Superintendencia emitió su propia Política General de Continuidad del Negocio, consolidando de esta manera una orientación institucional hacia esta temática.
- Resolución SB-2020-496 (2020): Dado el momento que el mundo vivía en medio de la pandemia el ente de control exigió el Plan de Manejo de Emergencias, dada la necesidad de garantizar la continuidad del servicio en contextos críticos, donde no solo la tecnología debía ser vista con un recurso crítico sino también las personas y la gestión que están desarrollan dentro de los procesos/servicios críticos.
- Resolución SB-2021-2126 (2021): la Norma de Control para la Gestión de Riesgo Operativo fue reformada incorporando de manera explícita elementos como el responsable de continuidad de negocio, políticas y comité que revisará el sistema, entre otros requisitos operativos.
- Resolución SB-2023-01901 (2023): esta resolución reemplazó la norma anterior y elevó los requisitos de implementación pues, las disposiciones sobre continuidad del negocio, seguridad de la información, canales electrónicos y

servicios prestados por terceros, deben aplicar en un plazo de 90 días y su cumplimiento debía ser revisado por auditoría interna.

Esta línea de tiempo muestra la evolución del enfoque normativo, ha ido de requerimientos básicos de control interno desde 2008, hacia una regulación más estructurada y específica sobre continuidad del negocio y gestión de terceros en el año 2023.

La aplicación de estas normativas y su evolución, han mostrado resultados alentadores, como lo muestra el estudio realizado por la Asobanca basado en datos de la Superintendencia de Bancos, donde podemos resaltar los siguientes resultados:

Tabla 2 Resultados de los cambios normativos y su evolución

Beneficio	Datos
Cumplimiento Normativo	Continuidad: 85 – 94% Control de Terceros: 99%
Resilencia operativa en crisis	Mejora de planes de continuidad y liquidez
Eficiencia y reducción de costos	Costos Operativos: -20% Satisfacción: +65%
Solvencia Sólida	12 – 14% (por encima de lo requerido por Basilea)
Gestión institucional más robusta	Múltiples certificaciones implementadas

Fuente: Informe Asobanca

En el caso sujeto a estudio, garantizar la continuidad es todavía más relevante por la amplitud de servicios que ofrece y por el alto grado de digitalización en sus procesos. Transacciones en línea, uso de cajeros automáticos, consultas por aplicaciones móviles o transferencias inmediatas dependen de plataformas tecnológicas que, a su vez, requieren el respaldo de proveedores externos. Si uno de estos eslabones se interrumpe, el efecto se percibe de forma inmediata en la experiencia del cliente y puede escalar hasta convertirse en un problema reputacional.

Dentro de este orden de ideas, la normativa busca proteger no solo la operación interna del banco, sino la confianza en el sistema financiero en su conjunto. La pérdida de credibilidad ocasionada por una caída prolongada de servicios puede desencadenar retiros masivos de depósitos o la migración de clientes hacia otras instituciones. En escenarios de este tipo, la liquidez no siempre es el problema central; lo que realmente se pone en riesgo es la sostenibilidad de la institución frente a sus grupos de interés.

De igual forma, los marcos internacionales como la norma ISO 22301:2019 enfatizan que la continuidad del negocio debe ser vista como una capacidad estratégica. No basta con reaccionar ante un incidente, sino que se requiere prevenir, probar y ajustar los planes de recuperación. En la perspectiva que aquí se plantea, la institución financiera bajo análisis enfrenta el reto de fortalecer esta capacidad no solo para cumplir con la regulación, sino para sostener la confianza de sus clientes y garantizar la estabilidad de sus operaciones en el largo plazo.

En resumen, la importancia de la continuidad del negocio en entornos regulados radica en que su incumplimiento genera consecuencias que trascienden lo operativo. Afecta la imagen de la entidad, compromete la relación con los clientes y puede poner en riesgo la permanencia en el mercado. Por eso, contar con un modelo sólido de gestión y control hacia los proveedores críticos se convierte en un elemento indispensable para la resiliencia organizacional.

Los síntomas observados comprometen directamente la continuidad operativa de la institución. Cada uno de estos factores representa una amenaza latente que puede traducirse en la interrupción de servicios esenciales, con consecuencias inmediatas sobre la percepción del cliente, el cumplimiento normativo y la reputación institucional.

La urgencia de intervenir radica justamente, en que la continuidad del negocio ya no puede dependeré únicamente de la infraestructura interna, sino que debe extenderse a toda la red de proveedores críticos que sostienen la operación diaria. En un contexto de creciente digitalización y presión regulatoria, postergar una intervención estructurada sobre este frente no solo amplifica los riesgos operativos, sino que limita la capacidad del banco para responder con agilidad y eficacia frente a incidentes inesperados.

1.5. Actores involucrados y limitaciones identificadas

Los síntomas observables del problema contribuyen a las limitaciones en la gestión de la continuidad del negocio, como lo muestra la siguiente figura:

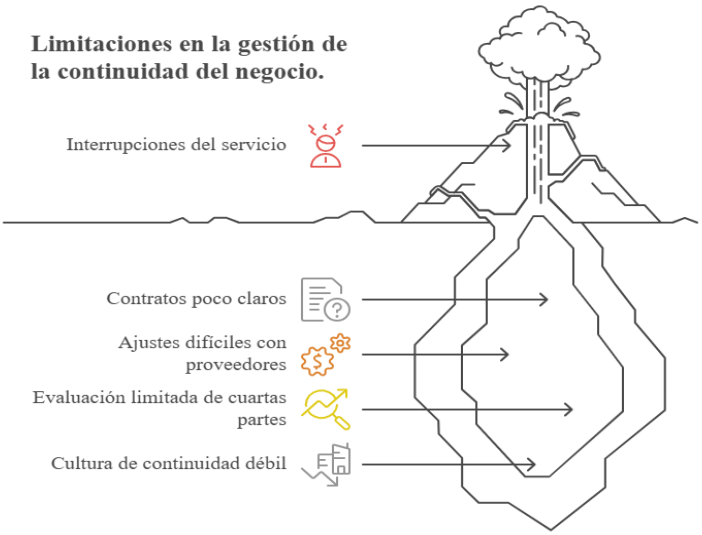

Figura 4. Actores clave y limitaciones en la gestión de continuidad del negocio
Fuente: Elaboración propia.

De acuerdo a lo manifestado por Faertes (2015) la gestión de la continuidad del negocio en una institución financiera involucra a diversos actores que cumplen funciones complementarias y, en muchos casos, interdependientes. Cada uno de estos actores aporta perspectivas, responsabilidades y expectativas distintas, lo cual exige una coordinación precisa para lograr una respuesta efectiva ante situaciones de interrupción.

En primer lugar, se encuentra la Superintendencia de Bancos**,** organismo de control responsable de establecer las normativas que rigen la continuidad operativa y supervisar su cumplimiento. Su principal interés radica en asegurar que las entidades financieras implementen planes robustos de prevención, respuesta y recuperación, con el fin de preservar la estabilidad del sistema financiero. La evaluación que realiza este actor se basa en auditorías, inspecciones periódicas y reportes regulatorios obligatorios.

Dentro de la organización, los directivos y la alta gerencia constituyen un segundo grupo clave. Son responsables de definir las políticas internas, aprobar recursos, y establecer una cultura organizacional que priorices la continuidad del negocio. Su compromiso es fundamental, ya que, sin un respaldo institucional firme, los lineamientos técnicos y

operativos pierden fuerza. La evaluación de este actor está dada por su capacidad de tomar decisiones estratégicas con la gestión del riesgo y la sostenibilidad operativa.

En un nivel operativo participan activamente las áreas de riesgos, tecnología, negocio y operaciones**,** responsables de evaluar los procesos críticos, definir los requisitos de continuidad como RTO y RPO, coordinar con proveedores y ejecutar los planes de recuperación. Estas áreas también deben documentar pruebas, monitorear indicadores clave y garantizar una comunicación continua con los terceros que soportan los procesos del banco. Su evaluación se basa en el cumplimiento del SLA, la efectividad de las pruebas de continuidad y la trazabilidad de los planes implementados.

Un actor particularmente relevante es el grupo de proveedores críticos**.** En el caso sujeto a estudio, la mayoría de los servicios esenciales dependen de terceros especializados. Su rol va más allá de la simple prestación de servicios: deben garantizar tiempos de recuperación acordes a las necesidades del banco, disponer de soluciones de respaldo y comunicar con oportunidad cualquier incidente(Gibb & Buchanan, 2006) . Los intereses de estos proveedores pueden centrarse en la rentabilidad, cumplimiento contractual y reputación comercial. La institución los evalúa a través de auditorías, revisiones contractuales, cumplimiento de SLA y procesos de homologación.

Por otra parte, aunque no intervienen directamente en la gestión de continuidad, los clientes son actores clave al ser los destinatarios finales del servicio. Su experiencia frente a interrupciones puede derivar en pérdida de confianza, reclamos formales o migración hacia otras entidades. Sus intereses se enfocan en la disponibilidad continua del servicio, seguridad y transparencia. Su impacto como actor se mide mediante indicadores de satisfacción, quejas y niveles de retención.

A continuación, se presenta un mapa de actores que sintetiza los principales grupos identificados, junto con sus respectivos requisitos, intereses y mecanismos de evaluación. De este modo se puede visualizar con mayor claridad las relaciones de poder, responsabilidad y control en torno a la continuidad del negocio, facilitando así el diseño de un modelo más efectivo y contextualizado.

Tabla 3 Mapa de actores y sus requisitos, intereses y mecanismos de evaluación

ACTOR	ROL	INTERESES	REQUISITOS	MECANISMO EVALUACIÓN

Superintendencia de Bancos	Establece normativas y supervisa cumplimiento	Estabilidad del sistema financiero Transparencia regulatoria	Planes de Continuidad documentados Reportes en caso de incidentes mayores	Inspecciones periódicas Auditorías regulatorias Revisión de reportes e indicadores
Alta Gerencia / Directivos	Define políticas Asigna recursos Aprueba estrategias	Protección institucional Reducción del riesgo reputacional	Integrar la continuidad con la estrategia institucional Aprobar recursos y planes operativos	Revisión de resultados Auditorías internas Seguimiento a indicadores de continuidad Reporte de riesgos
Área de Riesgos	Evalúa riesgos operativos y de terceros	Identificación oportuna de riesgos Mitigación efectiva	Evaluación de procesos críticos Gestión de riesgos por proveedor	Mapas de calor Controles y matrices de riesgo operativo
Área de Tecnología	Implementa soluciones tecnológicas Coordina recuperación técnica	Disponibilidad de servicios Integridad de sistemas	Definir y cumplir RTO/RPO Planes de respaldo tecnológico	Pruebas de Continuidad Indicadores de disponibilidad Auditorías de TI Resultados de pruebas
Áreas usuarias	Ejecuta procesos críticos Coordina planes de respuesta	Continuidad del servicio al cliente Eficiencia operativa	Manuales de contingencia Coordinación con TI y proveedores	Reportes de incidentes Medición de tiempos de recuperación
Proveedores críticos	Suministran servicios esenciales	Cumplimiento contractual Relación comercial estable	Cumplir SLA Comunicación de incidentes Planes de continuidad propios	Auditorías de servicio Monitoreo de SLA/KPI Evaluación periódica de desempeño
Cuartas partes	Subcontratistas de proveedores críticos	Estabilidad operativa Reducción de riesgos indirectos	Validación por parte del proveedor principal Cumplimiento de requisitos mínimos	Inclusión en auditorías Evaluación por el proveedor Certificaciones y evidencias

Clientes	Usuarios finales del servicio financiero	Acceso ininterrumpido, confianza en la institución	Disponibilidad del Servicio Información clara durante las interrupciones	Encuestas de satisfacción Indicadores de quejas Reputación canales digitales

Fuente: Elaboración propia.

En relación con las limitaciones, se identifican varias situaciones que condicionan la eficacia de este sistema. Una de ellas es la falta de cláusulas claras en los contratos, lo que impide exigir de forma contundente la recuperación en tiempos definidos. También se observa la dificultad de ajustar acuerdos con proveedores internacionales, ya que dependen de lineamientos de casas matrices fuera del país, lo que retrasa o limita la adopción de medidas locales y ajuste de los servicios a la normativa local.

De acuerdo a lo manifestado por Avila et al. (2021) otra limitación relevante es la escasa evaluación de cuartas partes. Los proveedores directos no siempre verifican a quienes les brindan soporte, generando un efecto dominó en caso de fallas. A ello se suma la ausencia de una cultura de continuidad consolidada**,** reflejada en la falta de comunicación oportuna de incidentes, la carencia de pruebas periódicas y la limitada preparación para escenarios de contingencia.

En resumen, los actores involucrados abarcan desde las autoridades regulatorias hasta los clientes finales, incluyendo tanto a las áreas estratégicas como operativas dentro de la institución, así como proveedores externos esenciales. No obstante, las limitaciones identificadas reflejan vacíos estructurales y de coordinación que afectan directamente la capacidad de respuesta ante interrupciones. Esta realidad pone de manifiesto la necesidad de contar con un modelo integral que articule los roles, responsabilidades y mecanismos de control de cada actor, bajo una visión sistemática de continuidad del negocio.

La presente tesis propone el diseño de un modelo integral para la gestión de continuidad con enfoque en proveedores críticos, que permita superar las limitaciones actuales y fortalecer la resiliencia institucional. Este modelo busca alinear las responsabilidades de todos los actores involucrados, establecer criterios claros para la evaluación y monitoreo

de terceros, y consolidar una cultura organizacional orientada a la prevención, respuesta y mejora continua. En el siguiente capítulo se presenta el objetivo general del estudio, así como la metodología que guiará el desarrollo de la propuesta.

CAPÍTULO 2

DESARROLLO DE LA PROPUESTA

En el primer capítulo se ofreció un primer vistazo sobre las debilidades en la gestión de los proveedores críticos de la institución. Estas debilidades tenían que ver con la limitada cobertura en los procesos de contratación, la necesidad de una mayor alineación entre los tiempos de recuperación y los compromisos establecidos con los terceros, así como con la necesidad de fortalecer los mecanismos de control, supervisión y reporte de incidentes.

Estas condiciones evidenciaron la necesidad de contar con un modelo metodológico para la gestión de riesgos de proveedores críticos de continuidad del negocio que contemplara los estándares internacionales y las herramientas de evaluación adecuadas para el contexto institucional. Por ello, en este capítulo se presenta la técnica de investigación aplicada y el proceso seguido para el desarrollo del modelo de gestión de riesgos de proveedores críticos (el modelo) que responda a las brechas identificadas en el diagnóstico.

2.1. Técnica de Investigación a aplicada

La técnica aplicada es de tipo empírico-aplicada, el enfoque es el diseño y desarrollo de una metodología para la gestión de riesgos de proveedores críticos de continuidad del negocio.

La construcción de la metodología sigue un enfoque paso a paso basado en orientación técnica, regulatoria y analítica. Esto es realizado en etapas para construir un modelo coherente que fuera implementable en el entorno de trabajo de una institución financiera. Inicialmente, se lleva a cabo una revisión documental y regulatoria, donde se analizan marcos de referencia internacionales, específicamente:

- ISO 22301:2019 sobre sistemas de gestión de continuidad del negocio.

- ISO 31000:2018 sobre gestión de riesgos, y
- El Reglamento DORA (UE 2022/2554) sobre resiliencia operativa digital
- Además de la legislación local relevante para el sector financiero.

El Análisis de Impacto al Negocio (BIA) es uno de los insumos de partida más relevantes para la aplicación de la metodología a desarrollar en función de la práctica, permite reconocer los procesos críticos y las dependencias importantes con los proveedores externos sobre los cuales se propone el modelo a construir.

A esto le sigue una fase de diseño estructural donde se detallan los principios, objetivos, roles y responsabilidades, y los procesos operativos y etapas que componen la metodología. Esta fase proporciona la base para la identificación, análisis y evaluación de riesgos de continuidad del negocio en servicios proporcionados por terceros, alineado esto con la Metodología de Gestión de Riesgo Operativo Institucional y lo definido dentro de la ISO31000 respecto de la evaluación de riesgos.

Figura 5 Ciclo de Evaluación de Riesgos
Fuente: Elaboración propia.

Al llevar a cabo una instancia de validación técnica enfocada en el análisis de las interrelaciones entre los elementos del sistema de continuidad del negocio y los riesgos operativos, se asegura la coherencia entre las exigencias normativas y los estándares de mejores prácticas internacionales.

De esta forma, el modelo empírico-aplicado posibilita interrelacionar la teoría, la regulación y la práctica organizacional en un modelo metodológico integral, que tiene

como propósito el fortalecimiento de la resiliencia operativa, así como el tratamiento de los riesgos de continuidad del negocio relacionados con terceros.

2.1.1. Enfoque de investigación

El enfoque de esta investigación corresponde a una orientación metodológica general que guía el estudio y determina la naturaleza del análisis realizado para responder al problema planteado. Para este caso, la investigación adopta un enfoque mixto, con predominancia cualitativa, complementando con elementos cuantitativos en las fases de evaluación y medición del riesgo.

La dimensión cualitativa resulta indispensable debido a que el estudio se fundamenta en la revisión y análisis interpretativo de normativa vigente tal como la Norma de Riesgo Operativo de la Superintendencia de Bancos, estándares internacionales como ISO 22301:2019, políticas internas, historial de incidentes que comprometieron la disponibilidad de servicios, documentación técnica generada por los proveedores mismos. Con este enfoque se comprende de mejor manera el contexto regulatorio, se identifica las brechas de cumplimiento, se evidencia patrones en la ocurrencia de incidentes y finalmente se caracteriza las prácticas actuales de continuidad del negocio y gestión de terceros.

De forma paralela, el componente cuantitativo se integra mediante la aplicación de matrices de evaluación ponderada, utilizadas para medir objetivamente el nivel de exposición al riesgo de cada proveedor crítico. Este componente permite además asginar puntajes según criterios definidos, clasificar proveedor según niveles de criticidad y establecer prioridad de tratamiento y monitoreo. Su incorporación fortalece la objetividad del modelo, al apoyar la toma de decisiones mediante resultados numéricos verificables.

La combinación de estos dos enfoques permite analizar el fenómeno desde una perspectiva integral: por un lado, interpretando la calidad, suficiencia y pertinencia de la gestión de proveedores; y por otro, midiendo su desempeño mediante indicadores, criterios y ponderaciones que permiten una clasificación clara y consistente. Esta integración es especialmente relevante en contextos regulados, donde la gestión de continuidad del negocio exige tanto la revisión documental como la evaluación medible del riesgo.

Este enfoque mixto facilita el desarrollo del modelo propuesto, ya que permite recolectar evidencia, comprender la problemática operacional, analizar los incidentes recurrentes, identificar brechas normativas y, posteriormente, construir una metodología aplicable, sistemática y replicable, que corresponde a la necesidad de la institución financiera. De igual manera garantiza que los resultados obtenidos sean robustos, coherentes con la realidad operativa y alineados con las exigencias regulatorias vigentes-

Con este enfoque se busca unir la teoría y la práctica, para obtener un resultado metodológico que sea aplicable, comprobable y coherente con los principios de resiliencia operativa y gestión integral de riesgos.

2.1.2. Diseño metodológico

El diseño metodológico corresponde a la estructura lógica que organiza el proceso de investigación y define la ruta que permite alcanzar los objetivos planteados. Por lo antes indicado se adopta un diseño de investigación aplicado, de carácter descriptivo y analítico, orientado a la construcción de un modelo de gestión de riesgos de proveedores críticos de continuidad del negocio para una institución financiera del Ecuador.

Este diseño se fundamenta en la necesidad de abordar un problema real ya que se analizó una situación institucional sin la manipulación de variables, observando los fenómenos en su contexto natural. Hernández, Fernández y Baptista (2018) señalaron que este diseño permite un examen de los hechos a medida que surgen y las relaciones entre sus componentes dentro de un intervalo especificado, en este caso, el tiempo.

Pues, dado que en la institución financiera se ha identificado una problemática recurrente relacionada con la gestión de la continuidad del negocio frente a la dependencia de proveedores externos. Existen servicios críticos cuya operación no puede ser resuelta internamente, por lo que su disponibilidad depende íntegramente de terceros. Esta situación genera vulnerabilidades operativas, especialmente cuando ocurren incidentes que afectan la prestación de servicios hacia los clientes.

Los entes de control exigen que cada incidente que impacte la disponibilidad de servicios sea reportado desde su inicio hasta el restablecimiento total, así como la elaboración de informes que detallen la causa raíz y las acciones implementadas para evitar su recurrencia. Sin embargo, los proveedores no siempre cumplen con los tiempos de

respuesta definidos por el organismo regulador y, en muchos casos, tampoco entregan los informes requeridos.

Como consecuencia, varios incidentes vuelven a presentarse de manera reiterada. La ausencia de informes que identifiquen la causa raíz impide determinar si se trata de la misma falla o de un problema distinto; no obstante, los síntomas evidencian que, en la mayoría de los casos, se trata del mismo origen no resuelto. Esta falta de control sobre las causas subyacentes interfiere directamente en la capacidad de la institución para mitigar riesgos operativos y garantizar la continuidad del servicio.

A esta situación se suma que múltiples entidades del sector financiero resultan afectadas por incidentes originados en un mismo proveedor, lo que evidencia un problema sistémico en la gestión de terceros críticos. La recurrencia, falta de trazabilidad y ausencia de soluciones definitivas ponen en riesgo la estabilidad operativa y el cumplimiento normativo, justificando la necesidad de un modelo de gestión de riesgos que permita evaluar, monitorear y controlar adecuadamente la continuidad del negocio asociada a proveedores críticos.

En función de la problemática identificada y con el propósito de contar con guías estructuradas que permitan desarrollar un modelo de gestión de riesgos de terceros eficiente, sistemático y aplicable a la realidad de una institución financiera, se plantea basar el modelo propuesto en los siete dominios de la ISO 22301:2019, estándar internacional reconocido para la gestión de la continuidad del negocio.

La selección de la ISO 22301:2019 como marco de referencia responde, en primer lugar, a que esta norma proporciona un enfoque integral, basado en riesgos y orientado a procesos, que permite evaluar de manera consistente la capacidad de una organización -en este caso, los proveedores críticos- para prevenir, responder y recuperarse ante eventos disruptivos que puedan afectar la continuidad de los servicios esenciales. A diferencia de otros marcos parciales o sectoriales, la ISO22301 aborda la continuidad del negocio desde una perspectiva holística, integrando aspectos estratégicos, operativos, tecnológicos y organizacionales, lo cual resulta fundamental en la evaluación de terceros que soportan procesos críticos de una institución financiera.

De igual manera, los siete dominios definidos por la norma (contexto de la organización, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora) permiten estructurar la evaluación de los proveedores bajo un esquema lógico y trazable,

alineado con el ciclo de mejora continua (PHVA), facilitando no solo la identificación de brechas actuales, sino también el seguimiento de su evolución en el tiempo. Esta característica resulta clave para medir el grado de madurez de la gestión de continuidad del negocio de los proveedores críticos, aspecto central del modelo propuesto.

A esto se suma que la ISO 22301:2019 mantiene una alta compatibilidad y alineación con otros marcos regulatorios y normativos relevantes, tales como las directrices del Comité de Basilea en la cual se basa la gestión de riesgos institucional y el Reglamento DORA, especialmente en lo relacionado con la gestión de riesgos operativos, la resiliencia operativa y el control de riesgos derivados de terceros. Esta alineación refuerza la pertinencia de su adopción como base metodológica, al permitir que el modelo desarrollado sea consistente con las exigencias regulatorias actuales y futuras aplicables al sector financiero.

En esto contexto, los siete dominios de la ISO 22301:2019 serán incorporados como parte de una evaluación sistemática, a través de un cuestionario según Anexo 4— que permita medir continuamente el grado de madurez en la gestión de continuidad del negocio de los proveedores críticos. Estos dominios, deberán ser el eje para interpretar la evidencia que sustente el cumplimiento o no, y definir los criterios de evaluación y las directrices técnicas del modelo. Cada dominio en función de la criticidad que tenga sobre la gestión de los riesgos de los terceros deberá tener asociado un peso dentro de la evaluación de tal manera que las brechas que existan puedan ser fácilmente identificadas para un tratamiento adecuado o el seguimiento correspondiente que permita garantizar llegar a porcentajes aceptables. A continuación, se presentan los dominios a considerar dentro de la evaluación, así como el aporte de cada uno al puntaje global:

Tabla 4 Dominios de evaluación de la gestión de continuidad del negocio de terceros

Grupos de Análisis	Ponderación 100% Meta Dominio	Aporte al Peso Global
Gobierno de Continuidad del Negocio (BCM)	100%	18%
Análisis de impacto del Negocio	100%	20%
Plan de Continuidad del Negocio	100%	18%

Anexos del Plan de Continuidad del Negocio	100%	20%
Infraestructura Tecnológica	100%	6%
Pruebas del Plan de Continuidad del Negocio	100%	10%
Mantenimiento y Capacitación del Plan de Continuidad	100%	8%

Fuente: Elaboración propia.

El peso dado a cada dominio dentro de la calificación global responde a la influencia directa en la capacidad real del proveedor para asegurar la continuidad del servicio y, por ende, en la calificación de riesgo al que se expone la **institución** financiera en caso de interrupciones. Los dominios con mayor impacto en la disponibilidad inmediata del servicio, así como aquellos que inciden en la capacidad del proveedor para ejecutar una recuperación efectiva dentro del RTO definido, reciben una ponderación más alta. Por su parte, dominios que tienen un carácter documental, complementario o de soporte mantienen pesos menores, sin restar su importancia en la evaluación integral

Cada dominio es seleccionado bajo objetivos específicos que permitan dentro de la evaluación, determinar las actividades que desde la perspectiva de terceros que soportan servicios críticos, deben cumplir. A continuación, se detalla para cada dominio el objetivo y que permitirá evaluar:

En primer lugar, el dominio de **Gobierno de Continuidad del Negocio (BCM)** establece las directrices de liderazgo, roles, responsabilidades y mecanismos de supervisión que deben existir para garantizar que el proveedor gestione adecuadamente la continuidad de los servicios que presta. Integrarlo en el modelo permite evaluar la madurez organizacional del tercero, su estructura de gobierno y su capacidad para responder a eventos disruptivos.

El **Análisis de Impacto del Negocio (BIA)** se incorpora como un requisito clave para determinar si el proveedor identifica adecuadamente sus procesos críticos, dependencias y tiempos máximos tolerables de interrupción. Al incluir este dominio en la evaluación, el modelo verifica la coherencia entre la criticidad de los servicios contratados y la capacidad del proveedor para garantizar su continuidad.

El **Plan de Continuidad del Negocio (PCN)** constituye un elemento esencial que detalla las estrategias, procedimientos y recursos definidos por el proveedor para responder ante incidentes. Su evaluación permite confirmar si el proveedor dispone de planes documentados, actualizados y efectivos para la recuperación oportuna del servicio.

De igual manera, el dominio relacionado con los **Anexos del Plan de Continuidad** asegura que los proveedores mantengan información complementaria relevante —como inventarios, contactos, acuerdos de nivel de servicio o configuraciones técnicas— indispensable para ejecutar los planes de forma exitosa.

El dominio de **Infraestructura Tecnológica** permite evaluar la robustez de la plataforma técnica del proveedor, sus mecanismos de respaldo, redundancia y disponibilidad, así como su capacidad para minimizar fallas que puedan impactar la continuidad del servicio prestado a la institución financiera.

Por su parte, el dominio de **Pruebas del Plan de Continuidad del Negocio** introduce un componente dinámico en la evaluación. Verificar la periodicidad, el alcance y los resultados de las pruebas realizadas por el proveedor permite determinar su preparación real frente a incidentes y su capacidad para validar la efectividad de los planes establecidos. Este dominio se complementa con el de Anexos del Plan de Continuidad ya que aquí se demostrará el cumplimiento de los planes documentados.

Finalmente, el dominio de **Mantenimiento y Capacitación del Plan de Continuidad** asegura que el proveedor mantenga prácticas de actualización continua, revisión periódica y formación del personal involucrado en la respuesta ante eventos disruptivos. Evaluar este dominio permite identificar si el proveedor cuenta con mecanismos de mejora continua que garanticen la actualización, pertinencia y aplicabilidad del plan a lo largo del tiempo.

La incorporación de estos siete dominios en el diseño metodológico del modelo permite realizar una evaluación exhaustiva y estandarizada de los proveedores críticos, asegurando que cada uno de los componentes fundamentales de un sistema de gestión de continuidad esté presente, sea verificable y se encuentre alineado con las mejores prácticas internacionales. De esta manera, el modelo no solo evalúa el desempeño operativo del proveedor, sino también su capacidad institucional, técnica y organizacional para garantizar la continuidad de los servicios esenciales para la institución financiera.

2.1.3. Fuentes y recolección de Información

La recopilación de información sobre el desarrollo de la metodología se basa en la documentación y técnicas operativas adecuadas a la naturaleza de la investigación. Para garantizar la validez y confiabilidad de los insumos utilizados en la construcción del modelo de gestión de riesgos de proveedores críticos, se aplica un conjunto amplio y complementario de técnicas de recolección de información. La selección de estas técnicas responde directamente a la problemática identificada en la institución financiera: incidentes recurrentes en servicios provistos por terceros, indisponibilidad prolongada, ausencia de informes de causa raíz, falta de cumplimiento de los tiempos regulatorios establecidos por la Superintendencia de Bancos y escasas prácticas formales de continuidad del negocio por parte de algunos proveedores como fue mencionado en el capítulo uno. En este contexto, la recolección de datos debe ser lo suficientemente robusta como para permitir una evaluación fiable, objetiva y alineada con estándares internacionales como ISO 22301, ISO 31000 y el marco DORA.

La primera técnica utilizada es la revisión documental exhaustiva, que incluye el análisis de:

- Normativa vigente de la Superintendencia de Bancos relacionada con riesgos operativos, incidentes de indisponibilidad, continuidad del negocio y gestión de terceros.
- Informes regulatorios que la institución debe remitir ante eventos que afectan la disponibilidad del servicio.
- Políticas internas, manuales y lineamientos de continuidad del negocio de la institución.
- Registros de incidentes históricos, tiempos de interrupción, escalamiento, comunicaciones recibidas y respuestas (o ausencia de ellas) de los proveedores.
- Contratos, acuerdos de nivel de servicio (SLA), acuerdos de nivel de operación (OLA) y anexos técnicos.

Evidencia documental enviada por proveedores, como planes de continuidad, pruebas, matrices de riesgo, arquitecturas tecnológicas o certificaciones en normas ISO. Esta

técnica permite caracterizar los patrones de incumplimiento, identificar inconsistencias entre lo declarado por los proveedores y los hechos, y detectar la falta de trazabilidad en incidentes que deberían haber sido documentados con informes de causa raíz, lo cual no tuvo lugar.

En segunda instancia, se suma la recolección de información generada por las áreas internas de la institución financiera, como lo son: Riesgo Operativo, Continuidad del Negocio, Tecnología y Administración de Contratos, esto se realiza mediante un proceso de recopilación de información a través de consultas informales, reuniones de trabajo y análisis de flujos operacionales. No se trata de entrevistas formales, sino de espacios de coordinación institucional que aportan información sobre interdependencias, incidentes, tiempos de respuesta y requerimientos operativos tanto internos como hacia los proveedores. Esta técnica aporta el complemento a la recolección de documentos a partir del conocimiento de las áreas que administran a los proveedores. Estas entrevistas no estructuradas permiten:

- Identificar la percepción institucional del desempeño de los proveedores.
- Documentar incidentes relevantes no registrados formalmente.
- Identificar vacíos operativos en los procesos de gestión de terceros.
- Conocer el impacto que los retrasos en la entrega de informes generan en el cumplimiento regulatorio.
- Recopilar experiencias relacionadas con proveedores que reinciden en fallas sin ofrecer soluciones definitivas.

La información cualitativa recopilada aporta contexto operativo y permite comprender la magnitud del problema desde la experiencia del personal involucrado al recoger prácticas reales, dificultades recurrentes y criterios técnicos aplicados en la gestión cotidiana de los proveedores críticos. Este tipo de información resulta clave para identificar debilidades no evidentes en registros documentales o en los indicadores cuantitativos, así como para entender cómo los procesos y controles definidos se ejecutan en la práctica. Adicionalmente, el análisis cualitativo facilita la interpretación de los riesgos asociados a continuidad del negocio, al incorporar el conocimiento tácito del personal responsable, contribuyendo a una evaluación más integral y realista de la situación actual.

Otra técnica fundamental es la sistematización y análisis de incidentes históricos tanto dentro de la institución como en el sistema financiero nacional, dado que múltiples entidades reportan fallas originadas en los mismos proveedores. Se recopilaron datos sobre:

- Frecuencia y severidad de los incidentes.
- Tiempo de indisponibilidad.
- Impacto en los servicios cara al cliente.
- Cumplimiento de los tiempos de notificación a entes de control.
- Existencia o ausencia de informes de causa raíz.
- Propuestas de mejora o mitigación efectiva.

Este análisis permite identificar patrones recurrentes y comportamientos que denotan la necesidad de fortalecer la madurez en continuidad del negocio por parte de varios proveedores.

Finalmente, todas las técnicas aplicadas fueron integradas mediante triangulación metodológica, la cual se utiliza de manera explícita en la fase de diagnóstico y diseño del modelo de gestión de riesgos de proveedores críticos. En esta etapa, la información cualitativa obtenida a partir de entrevistas y análisis experto, los resultados cuantitativos derivados de los cuestionarios de evaluación de madurez y el análisis documental de normativas y políticas internas son contrastados de forma sistemática para validar la consistencia de los hallazgos.

La triangulación permite, en primer lugar, confirmar o refutar las brechas identificadas en la gestión de continuidad del negocio de los proveedores críticos, asegurando que estas no respondan a percepciones aisladas o a limitaciones propias de una sola técnica de recolección. En segundo lugar, su aplicación facilita la definición de los pesos, criterios de evaluación y directrices técnicas del modelo, al respaldar cada decisión metodológica en evidencia convergente de carácter normativo, operativo y empírico. De esta manera, la triangulación metodológica fortalece la confiabilidad de los resultados y garantiza que

el diseño final del modelo sustente en una base sólida, coherente y aplicable al contexto institucional.

2.1.4. Instrumentos de investigación

Para el desarrollo del presente estudio y su enfoque, se define un conjunto de instrumentos que permiten recopilar la información necesaria para comprender la situación actual de la institución, caracterizar la problemática relacionada con los proveedores críticos y obtener las bases empíricas para construir posteriormente la metodología y el modelo de evaluación. Estos instrumentos son seleccionados de acuerdo con la naturaleza del problema, las exigencias de los estándares internacionales de gestión de continuidad del negocio y riesgos —como ISO 22301 e ISO 31000— y los marcos regulatorios aplicables al sector financiero, incluyendo la normativa de la Superintendencia de Bancos y el reglamento europeo DORA en cuanto a resiliencia operativa digital.

Se emplea una matriz destinada a organizar y clasificar todas las disposiciones relevantes emitidas tanto por estándares internacionales como por los entes reguladores nacionales. Este instrumento permite sistematizar los requisitos que posteriormente serán considerados para el diseño del modelo, tales como gobernanza, análisis de impacto, planes de continuidad, infraestructura tecnológica, pruebas y monitoreo continuo. La matriz permite identificar las obligaciones mínimas y las mejores prácticas que la metodología debía incorporar.

Tabla 5 Matriz de organización y clasificación

Dominio	Término	Definición	Fuente
Gobierno Continuidad del Negocio	Continuidad del Negocio (CN)	Capacidad de la organización de continuar la entrega de productos o servicios a niveles predefinidos aceptables luego de un incidente disruptivo.	ISO 22301
	Gestión de la Continuidad del Negocio (GCN)	Proceso de gestión holístico que identifica las amenazas potenciales de una organización y los impactos que estas pueden causar en sus operaciones de negocio si se concretaran, y que provee de un marco de trabajo para la construcción de resiliencia organizacional con la capacidad de una respuesta efectiva que proteja los intereses de las principales partes interesadas, la reputación, la marca y las actividades que generan valor.	ISO 22301
	Requisitos de Continuidad del Negocio	Periodo de tiempo, recursos y capacidades necesarias para continuar entregando los productos, servicios, procesos y actividades priorizadas luego de una disrupción.	ISO 22300

Análisis de Impacto de Negocio	Política de Continuidad del Negocio	La Política de Continuidad del Negocio provee el propósito y las metas de una organización tal y como han sido formuladas por la dirección.	ISO 22301
	Parte Interesada	Una persona y organización que puede afectar, verse afectada o percibir que se verá afectada por una decisión o actividad.	ISO 22301
	Comité de Continuidad del Negocio	El Comité es una unidad de asesoría, monitoreo y consulta creada por el Directorio y por disposición de la Superintendencia de Bancos (SB) para gestionar y controlar la continuidad del negocio. Dicho comité está encargado de planificar, coordinar, monitorear y difundir el sistema de gestión de continuidad del negocio. Adicionalmente, representa el compromiso de la Alta Gerencia de la Organización en las decisiones y estrategias relacionadas con la gestión de la Continuidad del Negocio.	Concepto IFI
	Análisis de Impacto en el Negocio (BIA)	Proceso de análisis de actividades y el efecto que una disrupción en el negocio pudiera tener sobre ellas.	ISO 22317
	Tiempo Máximo Tolerable de Disrupción (MTPD)	El tiempo que tomaría que impactos adversos, que podrían surgir como resultado de no proporcionar un producto o servicio o realizar una actividad, se torne inaceptable.	ISO 22301
	Tiempo de Recuperación Objetivo (RTO)	Tiempo objetivo en que los productos, servicios, procesos, subprocesos y los recursos humanos, físicos y tecnológicos deben ser restaurados a su actividad.	ISO 22301
	Punto de Recuperación Objetivo (RPO)	El punto en el que la información utilizada por una actividad debe ser restaurada para permitir que la actividad pueda ser reanudada.	ISO 22301
	Prueba	Ejercicio cuyo objetivo es obtener un resultado (ya sea aprobado o fallido) cuantificable dentro de los objetivos planeados del mismo.	ISO 22301
	Productos/Servicios Críticos	Oferta de valor de alta prioridad de una organización identificada en el análisis de impacto del negocio (BIA) porque su interrupción puede generar una alta afectación financiera, reputacional o regulatoria a la organización.	ISO 22300:2021
	Proveedor Crítico	Proveedor de productos o servicios críticos. Esto incluye un "proveedor interno", que es parte de la misma organización que su cliente.	ISO 22301
	Recursos	Todos los activos, personas, habilidades, información, tecnología (incluyendo instalaciones y equipos), inmuebles y suministros e información (ya sea electrónica o no) que una organización debe tener disponible, cuando sea necesario para operar y alcanzar su objetivo.	ISO 22301
	Amenaza	Causa potencial de un incidente no deseado, que puedo ocasionar daños a individuos, al ambiente o a la comunidad.	ISO 22301
	Riesgo	Efecto de la incertidumbre sobre los objetivos.	ISO/IEC Guide 73

Plan de Continuidad del Negocio	Evaluación de Riesgos	El proceso general de identificación, análisis y evaluación de riesgos.	ISO/IEC Guide 73
	Gestión de Riesgos	Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.	ISO/IEC Guide 73
	Alcance	Documento que contiene los procedimientos que orientan a las organizaciones para saber cómo proceder y reanudar su actividad habitual en caso de que ocurra una interrupción.	ISO 22301
	Propósito	Controlar/Mitigar los riesgos mediante un conjunto articulado de acciones y controles que garantizan la pronta recuperación de la operación de los sistemas y de la información sensible del negocio cada vez que se presenten eventos que afecten el normal flujo de los procesos funcionales.	ISO 22301
	Objetivos	Minimizar el impacto cuantitativo y cualitativo de una eventual interrupción de los procesos operativos, de atención, facturación y tecnológicos ejecutados por la Organización. Identificar las potenciales contingencias que afectan a los procesos críticos, mediante la evaluación de riesgos. Desarrollar una respuesta organizada ante un evento que afecte a la vitalidad de la organización y de sus colaboradores. Asegurar el funcionamiento de los procesos críticos del negocio durante los eventos contingentes, minimizando el tiempo requerido para volver a los niveles de operación normal y para atender razonablemente a los clientes del Grupo. Documentar los esquemas de contingencia que aseguren el normal desenvolvimiento de las operaciones crediticias y minimicen el riesgo inherente a la ocurrencia de acontecimientos externos imprevistos o emergencias. Implementar planes y controles de reanudación y recuperación que operen durante y después de una contingencia.	ISO 22301
	Roles y Responsabilidades	Se deben definir los roles y responsabilidades para las personas y equipos que tienen autoridad durante y después de un incidente, así como aquellos de apoyo.	
	Sitio Alterno	Locación, otra locación desde la cual opera la organización si el sitio Principal no está operativo.	ISO 22300:2021
Infraestructura Tecnológica	Componentes Redundantes	Consiste en la duplicación del hardware, de esta forma, en caso de que un sistema falle se cuente con otro servidor idéntico que lo sustituirá automáticamente, garantizando así la continuidad del servicio.	Norma Riesgo Operativo
		HA Activo-Activo: Consta de un servidor en el cual está todo duplicado. Este servidor es capaz de ejecutar los procesos con dos procesadores, Ram y controladoras de disco funcionando de forma simultánea y aprovechando su potencia. En caso de rotura de uno de los sistemas internos, pasaría toda la carga a uno de los procesadores.	Norma Riesgo Operativo

		HA Activo-Pasivo: Consta de dos servidores idénticos, uno de ellos activo ofreciendo los servicios y un segundo servidor, el pasivo que está en continua sincronización a la espera de una conmutación por error o programada.	Norma Riesgo Operativo
	Alta Disponibilidad (HA) Activo-Activo, Activo-Pasivo	Los sistemas redundantes, son aquellos en los que se repiten aquellos componentes de carácter crítico que se quiere asegurar ante los posibles fallos que puedan surgir por su uso continuo.	Concepto IFI

Fuente: Elaboración propia.

Por otro lado, el diseño de una ficha para registrar la disponibilidad, calidad y tipo de documentación existente dentro de la institución financiera relacionada con incidentes, contratos, acuerdos de nivel de servicio y lineamientos internos de gestión de continuidad permite conocer el punto de partida documental del estudio. Este levantamiento tiene como finalidad identificar el grado de formalización de la información disponible y detectar vacíos o debilidades documentales que deben ser considerados antes del diseño de la metodología. En esta fase no se evalúa el desempeño de los proveedores, sino que se determina qué información existe, en qué condiciones se encuentra y qué información no está documentada, delimitando así el alcance y las limitaciones del análisis posterior.

Sobre esta base documental, y sin reiterar la solicitud de información ya identificada, se desarrollan entrevistas no estructuradas como insumo inicial para profundizar la dimensión operativa y experiencial de la problemática. Estas entrevistas se orientan en recoger percepciones generales y lecciones aprendidas de incidentes o dificultades de la comunicación, ausencia de reportes oportunos o limitaciones en la coordinación con proveedores críticos. Su objetivo es comprender cómo estos eventos y procesos se gestionan en la práctica e identificar restricciones no evidentes en la documentación y validación de la metodología propuesta.

Con el fin de caracterizar la naturaleza de los incidentes —sin evaluarlos todavía— se diseña una plantilla para registrar elementos esenciales tales como disponibilidad de informes, tiempos de respuesta, existencia de documentación formal y mecanismos institucionales de seguimiento. Este instrumento proporciona una visión inicial de los factores que la metodología debía incorporar, considerando la problemática de reincidencias y falta de trazabilidad documental.

Finalmente, se diseña un esquema comparativo que relaciona los principios de resiliencia operativa de DORA con las exigencias regulatorias nacionales sobre interrupción de servicios, reporte de incidentes y gestión de terceros.

Tabla 6 Esquema comparativo DORA versus exigencias regulatorias

EJE DE ANÁLISIS	PRINCIPIOS DORA	EXIGENCIA SB	A INCORPORAR AL MODELO
Gestión de interrupciones del servicio	Exige que las entidades identifiquen, clasifiquen y gestionen interrupciones de servicios TIC críticos, asegurando la continuidad de las funciones esenciales y la capacidad de recuperación.	Obligación de garantizar la continuidad de los servicios financieros y minimizar el impacto de interrupciones operativas que afecten a clientes y al sistema financiero.	Continuidad de servicios críticos y capacidad de recuperación operativa.
Reporte y notificación de incidentes	Define procesos formales para la detección, clasificación, escalamiento y reporte oportuno de incidentes significativos relacionados con TIC, tanto internos como de terceros.	Exige reporte de incidentes relevantes a los entes de control dentro de plazos definidos, así como la documentación de causas, impactos y acciones correctivas.	Comunicación oportuna y estructurada de incidentes; trazabilidad y transparencia.
Gestión de riesgos de terceros	Incorpora un marco específico para la gestión de riesgos derivados de terceros proveedores de servicios TIC, enfatizando la evaluación continua, la criticidad y la dependencia operativa.	Demanda controles sobre proveedores críticos, evaluación de su impacto en la operación y mecanismos de supervisión y seguimiento.	Gestión sistemática de riesgos de terceros y evaluación de criticidad.
Responsabilidades contractuales	Establece requisitos mínimos que deben incluir los contratos con terceros, como derechos de auditoría, obligaciones de	Los contratos deben definir responsabilidades, niveles de servicio, cláusulas de contingencia y	Formalización contractual de responsabilidades y compromisos de continuidad.

	continuidad, notificación de incidentes y planes de salida.	obligaciones frente a eventos disruptivos.	
Documentación y evidencia	Exige documentación verificable sobre procesos, controles, incidentes, pruebas de resiliencia y gestión de proveedores, disponible para supervisión.	Las entidades deben mantener registros actualizados que evidencien el cumplimiento normativo y la gestión de eventos operativos relevantes.	Documentación verificable como base de control y supervisión.

Fuente: Elaboración propia.

Este instrumento permite identificar temas transversales que serán fundamentales en el modelo propuesto, como comunicación oportuna, documentación verificable, gestión de riesgos de terceros y responsabilidades contractuales.

La función de estos instrumentos será preparatoria y diagnóstica, ya que permiten:

- Organizar la información normativa y documental disponible.
- Comprender la problemática y su impacto operacional.
- Identificar los elementos técnicos y regulatorios esenciales para estructurar una metodología sólida.
- Definir los criterios y dimensiones que posteriormente se integrarían al modelo de evaluación.

En este contexto los instrumentos desarrollados suministran la evidencia normativa, los criterios de análisis y los requisitos mínimos de cumplimiento que sirven como base para estructurar y validar el modelo propuesto. Dichos instrumentos permiten identificar puntos de convergencia regulatoria y temas transversales que deben ser incorporados de manera explícita en la metodología, tales como la gestión de interrupciones de servicios, el reporte oportuno de incidentes, la gestión de riesgos de terceros, la formalización de responsabilidades contractuales y la necesidad de documentación verificable. De esta forma, el modelo no se construye únicamente sobre buenas prácticas teóricas, sino que se sustenta en obligaciones regulatorias concretas y en expectativas de supervisión

aplicables al contexto nacional, fortaleciendo su coherencia, trazabilidad y aplicabilidad práctica.

2.1.5. Resultados que dieron origen al modelo propuesto

El análisis de la información y recolección de los datos soporta la construcción del modelo de la metodología planteada en el presente estudio. Gracias al análisis de la documentación recopilada, la consideración de los aspectos normativos, y la observación directa del funcionamiento operativo de la organización, se logró vislumbrar un conjunto de impactos, patrones y necesidades que proporcionan el sentido de relevancia al implementar un sistema estructurado para la gestión de riesgos de proveedores críticos para la continuidad del negocio.

Con el conjunto de datos obtenidos en la recolección de información, se evidencia que la institución presenta un nivel de dependencia operativa de terceros que se considera muy alto para la continuidad de sus procesos críticos, además de que no cuenta con procesos estandarizados que permitan la evaluación, la priorización y el seguimiento de los riesgos que dichos proveedores generan. Por otro lado, se evidencia que la información de relevancia se encuentra distribuida en distintas áreas como se señala en el numeral 2.1.4. Fuentes y recolección de Información, lo que dificulta la trazabilidad, el control y la disponibilidad de información para la toma de decisiones.

Tabla 7 Principales resultados que dieron origen al modelo metodológico propuesto

Área de análisis	Hallazgo identificado	Implicación para la continuidad del negocio
Dependencias críticas identificadas en el BIA	Se evidenció una alta dependencia de procesos críticos respecto a proveedores externos, con relaciones directas e indirectas.	Justificó la necesidad de un modelo formal para clasificar y gestionar riesgos derivados de terceros.
Inventario de proveedores	No existía un inventario unificado ni actualizado de proveedores críticos con integración de datos operativos, logísticos y contractuales.	Motivó la elaboración de un inventario maestro como insumo estructural del modelo.
Clasificación y priorización	Se observaron diferencias significativas en dependencia operativa, alternativas disponibles,	Demostró la necesidad de criterios estandarizados y ponderados para definir prioridades de evaluación.

	riesgos financieros y nivel de integración tecnológica.	
Evaluación documental	Existían brechas en la disponibilidad, vigencia y calidad de PCN, pruebas, evidencias y certificaciones entregadas por los proveedores.	Impulsó la creación de una matriz de evaluación documental con ponderaciones y escalas uniformes.
Madurez en continuidad	Se evidenció heterogeneidad en los niveles de madurez en continuidad entre proveedores críticos.	Reforzó la necesidad de un sistema que permitiera comparar objetivamente el nivel de preparación.
Monitoreo y seguimiento	No existía un mecanismo sistemático para supervisar planes de mejora, cumplimiento de pruebas o actualización de documentación crítica.	Justificó la inclusión de KPI, KRI, alertas y un panel de seguimiento integral.
Cumplimiento normativo	Se identificaron brechas respecto a los requisitos de ISO 22301, ISO 31000, ISO 27036 y DORA sobre gestión de terceros críticos.	Respaldó la necesidad de desarrollar una metodología alineada con marcos internacionales.
Trazabilidad institucional	La información sobre incidentes, evaluaciones previas y monitoreo estaba dispersa entre áreas.	Motivó la necesidad de unificar criterios y responsabilidades para garantizar la trazabilidad del proceso.

Fuente: Elaboración propia.

Es así que, en primer lugar, el análisis preliminar de la documentación interna y de los registros institucionales como es indicado en el numeral de fuentes de información, evidencia una falta de trazabilidad completa de los incidentes relacionados con la indisponibilidad de servicios provistos por terceros, como lo muestra la tabla 8. Los instrumentos aplicados permiten identificar que, en varios casos, la información disponible es parcial, incompleta o dispersa, lo que dificulta entender las causas de origen, las acciones tomadas y las responsabilidades asociadas. Esta situación refleja la necesidad de incorporar, en el futuro modelo, mecanismos que permitan estandarizar la recopilación, clasificación y seguimiento de incidentes vinculados a proveedores críticos.

Por otro lado, la revisión inicial de las obligaciones regulatorias y de estándares internacionales reveló una desalineación entre los requisitos de ISO 22301, DORA y la normativa de la Superintendencia de Bancos, frente a la manera en que la institución recibe información de los proveedores, pues se identifica que varios de los elementos exigidos por estos marcos no están presentes o no son consistentes, lo cual deja de manifiesto la necesidad de diseñar un modelo que incorporara dichos requisitos como criterios estandarizados de evaluación. Esto se refleja en la tabla 8.

Tabla 8 Trazabilidad de información

Proveedor Crítico	Nivel de Riesgo de Continuidad	Plan de Continuidad Vigente	Pruebas de Continuidad Realizadas	Fecha Última Evaluación	Reporte Incidentes	Seguimiento Incidentes	Responsable Interno
Proveedor A	Muy Alto	S/I	S/I	S/I	No	No	J. Pérez
Proveedor B	Alto	S/I	S/I	S/I	S/I	No	L. Martínez
Proveedor C	Muy Alto	S/I	S/I	S/I	Regular	No	A. Gómez
Proveedor D	Bajo	Sí	S/I	S/I	No	No	C. Rivera
Proveedor E	Muy Bajo	S/I	S/I	S/I	No	No	F. Torres

Fuente: Elaboración propia.

Las entrevistas preliminares señaladas en el numeral 2.1.4. Fuentes y recolección de Información con actores internos permiten identificar problemas reiterativos en la comunicación y gestión con proveedores, especialmente en relación con la notificación de incidentes y la entrega de informes de causa raíz. El personal reporta casos donde los proveedores no cumplen con los plazos regulatorios, no entregan informes completos o no presentan medidas correctivas definitivas, lo cual ocasiona la reincidencia de fallas. Estos hallazgos demuestran la necesidad de que el modelo incluya criterios para evaluar la capacidad del proveedor de gestionar incidentes, comunicar oportunamente y presentar evidencia que permita mitigar la recurrencia.

Con relación a la sistematización preliminar de incidentes, muestra que varias entidades del sector financiero habían experimentado fallas similares con los mismos proveedores, lo que permite inferir que la problemática no es aislada, sino que corresponde a brechas estructurales en la gestión de continuidad por parte de ciertos terceros, considerando

además que existen varios casos que son proveedores únicos en el mercado o existe un monopolio del servicio prestado. Este resultado refuerza la importancia de integrar en el modelo un enfoque basado en riesgos, que considere la criticidad del servicio y el impacto transversal en el sistema financiero.

Finalmente, los instrumentos normativos y técnicos utilizados permiten confirmar que el conjunto de dimensiones clave consideradas incluir en el modelo son las requeridas, ratificando así que los dominios a evaluar serán: gobernanza de continuidad, análisis de impacto, estrategia de recuperación, infraestructura tecnológica, pruebas, mantenimiento del sistema y comunicación. La identificación temprana de estas dimensiones constituye uno de los resultados más relevantes, ya que se convierten en la columna vertebral del modelo que se desarrolla en secciones posteriores.

Los principales hallazgos que sustentan la base para el diseño de la metodología del modelo se resumen en la siguiente tabla:

Tabla 9 Principales resultados que dieron origen al modelo metodológico propuesto

Área de análisis	Hallazgo identificado	Implicación para la continuidad del negocio
Dependencias críticas	Alta dependencia de proveedores sobre procesos críticos.	Disponibilidad de servicios y recuperación ante incidentes, dependen directamente de los terceros.
Inventario de proveedores	Ausencia de un inventario unificado y actualizado de proveedores críticos asociados a información operativa y contractual.	La exigencia de tiempos de recuperación y cumplimiento de niveles de servicio no se basan en datos.
Clasificación y priorización	Una sola categoría para todos los proveedores críticos no existe relación con los tiempos de recuperación.	Mismas exigencias para diferentes niveles de criticidad, no permiten garantizar la recuperación en los tiempos determinados.
Madurez en continuidad	Heterogeneidad en los niveles de madurez en continuidad entre proveedores críticos.	Resultados ambiguos, ya que las métricas aplicadas tienen un solo criterio.
Cumplimiento normativo	Brechas en el cumplimiento de requisitos de ISO 22301, ISO	Auditorías arrojarán incumplimientos de la IFI causados por el tercero.

Área de análisis	Hallazgo identificado	Implicación para la continuidad del negocio
	31000, ISO 27036 y DORA sobre gestión de terceros críticos.	
Trazabilidad institucional	Información de incidentes, evaluaciones previas y monitoreo dispersa en las áreas.	Los incidentes y debilidades identificadas no tienen trazabilidad y por tanto carecen de tratamiento adecuado.

Fuente: Elaboración propia.

Esta tabla y los hallazgos en ella incluidos, constituyen el insumo fundamental para el diseño de la metodología y definición de las diferentes fases, pues permite sistematizar las debilidades actuales y establecer la causal entre la situación identificada y los elementos que deben ser incorporados en el modelo de evaluación. El análisis proporciona un diagnóstico estructurado que orienta la construcción de las fases metodológicas, los criterios de evaluación y los instrumentos necesarios para superar las brechas detectadas.

Respecto de las dependencias críticas, se justifica la necesidad de contar con una fase de identificación y mapeo basado en el BIA institucional, que asegure que la clasificación está hecha de manera técnica y tiene como soporte información verificable. Esto lleva a la **Fase 1: Identificación de proveedores críticos.**

En cuanto al hallazgo de ausencia de un inventario unificado, evidencia la escasa visibilidad institucional sobre terceros que soportan procesos críticos, lo cual lleva a la necesidad de contar con un inventario maestro de proveedores críticos clasificados y categorizados, lo cual permitirá establecer exigencias alineadas a los tiempos de recuperación de cada servicio que está soportando determinado proveedor, lo cual nos lleva a la **Fase 2: Análisis y Priorización de Proveedores Críticos.**

De igual manera, la heterogeneidad en la madurez de continuidad y brechas de cumplimiento normativo de proveedores justifica la inclusión de la **Fase 3: Evaluación de los Proveedores Críticos**, pues así se medirá el nivel real de preparación de cada proveedor bajo un marco estándar y comparativo, evitando que las deficiencias del proveedor se traduzcan en incumplimientos institucionales.

Las brechas de cumplimiento destacan la necesidad de establecer planes de acción hasta el cumplimiento normativo, esto da origen a la **Fase 4: Definición de planes de acción y mitigación**. El desconocimiento de las obligaciones contractuales o incluso contratos que no incluyen las condiciones mínimas de servicio crean la necesidad de esta fase porque convierte diagnósticos en acciones efectivas, reduce exposición operativa y regulatoria, establece responsabilidades claras, prioriza recursos y provee evidencia verificable.

Finalmente, la falta de trazabilidad institucional de incidentes, evaluaciones y monitoreo da lugar a la **Fase 5: Monitoreo y Control de Proveedores Críticos de Continuidad de Negocio**, orientada a mantener registros, verificar avances, documentar incidentes y garantizar la mejora continua del proveedor. Este componente asegura que las observaciones repetitivas no se acumulen sin tratamiento, y que la institución mantenga una visión integral del riesgo asociado a cada tercero.

En conjunto, los resultados de la Tabla 6, funcionan como un diagnóstico base para la construcción del modelo, permitiendo que la metodología se fundamente en necesidades reales y responda directamente a las debilidades operativas, contractuales, normativas y de continuidad identificadas. Esto se traduce en un modelo que sirva como herramienta práctica diseñado para cerrar las brechas detectadas y garantizar los niveles de disponibilidad de los servicios ofertados por la institución financiera.

2.2. Presentación detallada de la propuesta elaborada para el Modelo de Gestión de Riesgos de Proveedores Críticos de Continuidad del Negocio.

El modelo tiene como objetivo que la administración de proveedores críticos no se restrinja a un mero cumplimiento documental, sino que sea un elemento activo en la estrategia de resiliencia del banco. La propuesta está estructurada en fases que posibilitan la identificación, análisis y priorización, evaluación, definición de planes de acción y mitigación, y monitoreo y control de los terceros que respaldan procesos fundamentales Con el propósito de que el seguimiento no sea un evento aislado, sino que esté presente en toda la relación contractual desde su inicio hasta su renovación o terminación, cada etapa se incorpora al ciclo de vida del proveedor.

Dado esto, el diseño metodológico está estructurado en cinco fases consecutivas, cada una establece objetivos definidos, actividades, herramientas y resultados. A continuación, se detallan las mismas:

Fase I. Identificación de proveedores críticos

La Fase 1 constituye el punto de partida metodológico para la gestión de riesgos asociados a terceros que inciden en la continuidad operativa de la organización. Su propósito es reconocer, clasificar y documentar a los proveedores cuya interrupción pueda comprometer la operatividad de los procesos críticos, garantizando así que la evaluación posterior se realice sobre una base completa, trazable y alineada con el Análisis de Impacto al Negocio (BIA).

La metodología establece que la identificación de proveedores críticos debe derivarse directamente del Análisis de Impacto al Negocio (BIA), el cual determina los procesos y subprocesos críticos de la organización, junto con sus dependencias internas y externas. De acuerdo con este análisis, cada subproceso crítico debe documentar explícitamente:

- Los recursos externos necesarios para asegurar su operación ininterrumpida.
- La dependencia directa o indirecta respecto de proveedores.
- La estrategia operativa de continuidad definida en el BIA para dicho proveedor o recurso externo.

Esta información constituye el insumo principal para elaborar un primer inventario de proveedores cuya continua operación resulta indispensable para garantizar la resiliencia operativa de la organización.

Se considera proveedor crítico a todo tercero que reúna uno o más de los siguientes criterios:

- Ejecuta total o parcialmente un subproceso crítico identificado en el BIA.
- Provee un servicio, infraestructura, sistema, plataforma, información o recurso humano sin los cuales el proceso no podría mantenerse operativo dentro del RTO definido.

- Interviene de forma directa en el cumplimiento de SLA u obligaciones regulatorias asociadas al servicio final ofrecido por la organización.

Bajo esta definición, la criticidad del proveedor se fundamenta en su impacto operativo, regulatorio y de continuidad, en coherencia con los principios establecidos por ISO 22301.

El producto final de esta fase es el Inventario Maestro de Proveedores Críticos, documento fundamental para el desarrollo de las fases siguientes. Este inventario deberá contener, como mínimo, la siguiente información para cada proveedor identificado:

Tabla 10 Estructura del Inventario Maestro de Proveedores Críticos

Nombre comercial	Razón social (según SRI)	RUC	Servicio, recurso o infraestructura provista	Proceso o Subproceso crítico que soporta	Dirección o ubicación del proveedor	Área responsable del contrato / relación	Estrategia operativa - BIA	RTO Subproceso	MTPD Subproceso

Fuente: Elaboración propia.

Este inventario constituye la base estructural de la metodología, ya que establece el universo de proveedores que serán sometidos a evaluación, priorización y control en las fases posteriores.

En cuanto a la normativa se determinó que la base para el desarrollo de la fase, se encuentra en el marco normativo internacional como la ISO 22301:2019, cláusula 8.2.1. Esta última menciona la identificación de recursos internos y externos de los cuales se harán disponibles para la continuación de actividades prioritarias. También se tiene en cuenta las BCI Good Practice Guidelines (2018) y la ISO 31000:2018. Asimismo se menciona la ISO 27036-1:2014, que menciona la seguridad en las relaciones con los proveedores críticos. También el Reglamento DORA (EU 2022/2554) en los artículos 28 y 29, menciona el cumplimiento de la identificación de los terceros críticos, en especial los tecnológicos.

Fase II: Análisis y Priorización de Proveedores Críticos

La Fase 2 tiene como propósito cuantificar el nivel de exposición al riesgo de continuidad asociado a cada proveedor crítico identificado en la Fase 1, utilizando criterios objetivos y ponderados. Esta fase constituye el punto de partida para determinar cuáles proveedores

requieren una evaluación más profunda y qué nivel de recursos debe asignarse a su revisión y tratamiento, esto en función del nivel de criticidad que implica el tercero.

Tomando como base el *Inventario Maestro de Proveedores Críticos* obtenido del BIA, esta fase aplica una matriz de criterios evaluativos estandarizados, alineados con ISO 22301, DORA y la normativa de la Superintendencia de Bancos. El resultado es una puntuación consolidada que permite priorizar a los proveedores según su impacto potencial ante una interrupción.

Cada proveedor será evaluado mediante siete criterios ponderados, utilizando una escala de puntuación de 1 a 5 basada en condiciones reales, donde 5 representa el nivel más alto de exposición al riesgo. La siguiente tabla presenta los criterios con los cuales se determinará la criticidad del tercero. La suma ponderada de las puntuaciones asignadas a cada criterio otorgará una valoración global de riesgo, cuya escala situará al proveedor en una categoría específica de criticidad, de acuerdo el nivel de riesgo que representa para la organización:

Tabla 11 Criterios de criticidad de riesgo de proveedores críticos

Criterio	Condiciones observables (1 a 5 puntos)
1. RTO del Servicio	1 =Mayor a 3 horas 3 = Entre 1 y 3 horas 5 = Menor a 1 hora
2. Exclusividad / Alternativas	1= Existen múltiples proveedores alternativos 3= Entre 2 y 4 alternativas iguales 5= No existe alternativa viable (proveedor único).
3. Puede ser reemplazado el proveedor dentro del tiempo del RTO	1= SI puede ser reemplazado 5= No puede ser reemplazado
4. Nivel de intervención en el subproceso crítico	5= Total 3= Parcial 1= Marginal
5. Número de incidentes reportados en el mes	1 = Menos de 2 3 = 2 5 = Más de 2
6. Incidentes que cumplen el RTO	1 = Todos 3 = Entre el 99% y 80% 5 = Menos del 80%

Criterio	Condiciones observables (1 a 5 puntos)
7. Impacto de los incidentes	1 = Alto 3 = Medio 5 = Bajo

Fuente: Elaboración propia.

La calificación final se obtiene mediante el cálculo ponderado de los criterios.

Con base en el puntaje total, se asigna un nivel de riesgo:

Tabla 12 Niveles de riesgo de acuerdo al puntaje

Nivel de riesgo	Rango de puntaje
Extremo	35 – 24
Alto	23 – 19
Moderado	18 – 15
Bajo	14 – 0

Fuente: Elaboración propia.

Esta matriz consolida para cada proveedor el nivel de riesgo asignado en función del puntaje obtenido, lo cual determina en adelante del tipo de evaluación que debe cumplir.

Esta fase del proceso se basó en la ISO 22301, Cláusula 8.2.3, que requiere la definición de riesgos que pueden interrumpir funciones críticas y las Directrices de Buenas Prácticas del BCI (2018), Capítulos 4 y 5, que dirigen la evaluación de impactos y riesgos planteados por terceros. También se consideró la ISO 27036-3:2013, que describe los riesgos asociados con proveedores críticos y DORA (UE 2022/2554), Artículos 28 y 30, que obliga a la identificación de proveedores críticos en función del impacto operativo y la dependencia tecnológica.

Fase III: Evaluación de los Proveedores Críticos

Esta fase se ejecuta una vez que el proveedor ha sido clasificado y priorizado en la Fase II. Su propósito es realizar la evaluación formal, documental y técnica, para determinar si el proveedor cuenta con capacidades suficientes para garantizar la continuidad del servicio, conforme a estándares internacionales y exigencias regulatorias.

Mientras la Fase 2 responde a “qué tan crítico y riesgoso es el proveedor”, la Fase 3 responde a “qué tan preparado está para dar continuidad y cómo debe gestionarse”.

A partir de la categorización obtenida por el proveedor en función del nivel de criticidad de riesgo, cada uno debe someterse al tipo de evaluación que corresponde a su clasificación. Esta diferenciación permite atender uno de los hallazgos iniciales: la existencia de una única categoría para todos los proveedores críticos, lo cual generaba resultados distorsionados.

La metodología propuesta corrige esta distorsión al establecer evaluaciones diferenciales según el nivel de criticidad asignado. A continuación, se detalla el tipo de evaluación que debe aplicarse a cada proveedor en función del nivel de riesgo en el que se encuentra ubicado:

Tabla 13 Tipo de evaluación de acuerdo al nivel de riesgo

Nivel de riesgo	Tipo de Evaluación
Extremo	• Revisión y constatación. • Certificación o informe de auditoría externa o revisión por parte de una empresa certificada y con experiencia en el ramo. • Revisión documental y verificación que esta cumpla con los criterios de los dominios de evaluación.
Alto	• Certificación o informe de auditoría externa o revisión por parte de una empresa certificada y con experiencia en el ramo. • Revisión documental y verificación que esta cumpla con los criterios de los dominios de evaluación.
Moderado	• Informe de auditoría externa o revisión por parte de una empresa certificada y con experiencia en el ramo. • Autoevaluación. • Revisión documental y verificación que esta cumpla con los criterios de los dominios de evaluación.
Bajo	• Revisión documental y verificación que esta cumpla con los criterios de los dominios de evaluación.

Fuente: Elaboración propia.

Este criterio de selección se basa en la proporcionalidad del esfuerzo de gestión, según lo articulado en la ISO 27036-3:2013 y el Artículo 30 del Reglamento DORA, que establecen que la intensidad de la evaluación debe alinearse con el nivel de riesgo y dependencia.

Cada proveedor evaluado tendrá un informe formal que incluye:

- Nivel de riesgo asignado (de la Fase 2)
- Evidencia recopilada
- Brechas identificadas
- Nivel de madurez en continuidad del negocio
- Requerimientos o acciones de remediación de brechas

Lo cual exige que de acuerdo al ciclo de gestión del riesgo las brechas identificadas sean tratadas, ya sea mediante acciones que las eliminen por completo o incluir acciones que permitan mitigarlas hasta una resolución definitiva.

Figura 6 Ciclo de Gestión de Riesgos del Proveedor

Fuente: Lledó y Rivarola (2007)

La elaboración de esta fase se amplió en los intereses de las normas y marcos internacionales pertinentes, entre los cuales se encuentran:

- La norma ISO 22301:2019 en sus cláusulas 8.4.3 y 8.4.4, la cual exige la validación de las medidas que han sido adoptadas por terceros proveedores y la validación de la continuidad de los servicios.
- La norma ISO 27036-3:2013, en su cláusula 6.2, que se apersona la gestión documental y de continuidad de las relaciones con los proveedores críticos.
- Las BCI Good Practice Guidelines 2018, en sus capítulos 5 y 6, que refiere la evaluación y monitoreo de los terceros claves con una validez y preparación verificable.
- El DORA Regulation 2022/2554, en los artículos 28, 30 y 31, que establece que las entidades financieras deben asegurarse de que sus proveedores de IT críticos tengan capacidades probadas. Continuidad.

Fase IV: Definición de planes de acción y mitigación

La Fase 4 tiene como propósito establecer las acciones necesarias para corregir, reducir o controlar las brechas identificadas en la evaluación documental y técnica realizada durante la Fase 3. Esta fase permite transformar los hallazgos en medidas concretas que fortalezcan la resiliencia del proveedor y reduzcan la exposición al riesgo de continuidad del negocio para la organización.

Su objetivo es garantizar que cada proveedor crítico cuente con un plan de mitigación proporcional a su nivel de riesgo y alineado con los estándares ISO 22301:2019, DORA, las guías de la Superintendencia de Bancos y el marco interno de gestión de riesgos operacionales.

Para esto serán necesarias las siguientes acciones:

- Traducir las brechas detectadas en la Fase 3 en acciones específicas, medibles y verificables.
- Definir controles y compromisos que deben ser implementados tanto por el proveedor como por la institución.
- Asegurar que los requisitos regulatorios y las mejores prácticas de continuidad del negocio estén incorporados en la operación diaria del proveedor.
- Garantizar que los riesgos residuales queden dentro de los niveles de apetito y tolerancia definidos por la organización.

Cada acción definida debe cumplir los principios SMART (Specific Measurable Achievable Relevant Time-bound).

El resultado de esta fase es un Plan de Acción y Mitigación, formalmente documentado, que consolida todas las medidas que el proveedor debe implementar para alcanzar el nivel de continuidad requerido por la institución.

Este plan constituye la base para la Fase 5, enfocada en el monitoreo continuo, validación de avances, verificación de evidencias y cierre de acciones.

Esta fase se sustenta en la norma ISO 22301:2019, cláusula 8.4.3 y 8.4.4: Requiere asegurar la continuidad de servicios proporcionados externamente y la validación de medidas adoptadas por terceros, así como en DORA (Art. 28, 30 y 31): Obliga a garantizar que los proveedores TIC críticos dispongan de capacidades probadas de continuidad, con procesos de pruebas y auditoría.

Fase V: Monitoreo y Control de Proveedores Críticos de Continuidad de Negocio

El diseño de esta fase se basó en los estándares internacionales y marcos de referencia más importantes en relación con la continuidad y la gestión de terceros. Estos incluyen la ISO 22301:2019, cláusulas 8.4.2 y 9.1, que establecen requisitos para el seguimiento, medición y abordaje de brechas; la ISO 27036-3:2013, cláusula 6.3, respecto a los mecanismos de mejora y auditoría de las relaciones con proveedores; las Guías de Buenas Prácticas del BCI (2018), capítulo 6, que subraya la mejora continua y la validación de los controles de terceros; el Reglamento DORA (UE 2022/2554), artículos 30 y 32, que requieren que las instituciones financieras realicen revisiones periódicas sobre ICT críticas de terceros; y el NIST SP 800-161 Rev. 1, que orienta sobre la gestión continua del riesgo de la cadena de suministro.

La Fase 5 constituye la etapa continua del modelo de gestión y tiene como propósito supervisar, validar y controlar el desempeño de los proveedores críticos en materia de continuidad del negocio, asegurando que los riesgos identificados se mantengan dentro del nivel de tolerancia definido por la organización. Esta fase garantiza que los resultados obtenidos en la evaluación (Fase 3) y los compromisos establecidos en los planes de acción (Fase 4) evolucionen adecuadamente hacia un estado de madurez sostenible en el tiempo.

El monitoreo permanente se convierte en un componente esencial del ciclo de gestión, dado que los proveedores, los servicios, la tecnología y los requisitos regulatorios pueden cambiar, generando nuevas condiciones de riesgo que deben ser identificadas oportunamente.

Una vez concluida la evaluación, los proveedores son clasificados según su porcentaje de cumplimiento dentro de la evaluación formal. Esta clasificación determina la intensidad del monitoreo y las acciones que deben implementarse en cada caso.

Tabla 14 Calificación de madurez del proveedor

Calificación	Rango	Descripción general
Insuficiente	0% – 40%	Deficiencias críticas que comprometen la continuidad del negocio.
Gestionado	>40% – 60%	Brechas significativas que requieren mejoras de corto plazo.
Desarrollado	>60% – 80%	Proveedores con madurez intermedia y necesidad de ajustes.
Satisfactorio	>80% – 100%	Cumplimiento aceptable; proveedor maduro en continuidad.

Fuente: Elaboración propia.

Con base en ello, se define el plan de acción para cada calificación, así como los períodos de revisión. De esta manera se puede realizar una gestión diferenciada a los proveedores según su nivel de exposición al riesgo y priorizar los recursos de seguimiento y control sobre aquellos casos que verdaderamente puedan poner en riesgo la operación de la organización, así como tomar medidas compensatorias.

La propuesta, en su totalidad, no solo posibilita la valoración de cuán preparados están los proveedores para interrupciones, sino que también fomenta un ciclo de constante mejora. La organización tiene la posibilidad de priorizar inversiones, renegociar las condiciones de los contratos o, si lo requiere la situación, explorar otras opciones para disminuir el peligro de depender en gran medida de un único proveedor. De esta manera, el modelo se transforma en un instrumento útil para robustecer la resiliencia de la empresa y satisfacer de forma eficaz las demandas regulatorias.

2.3. Gobernanza, Responsabilidades y Roles del Modelo de Gestión

La correcta ejecución de la metodología de gestión de riesgos de proveedores críticos de continuidad del negocio requiere una estructura de responsabilidades claramente definida. Dado que el proceso involucra actividades transversales —desde la identificación de proveedores y la evaluación de su criticidad, hasta la definición de planes de acción y el monitoreo permanente— es indispensable establecer los roles, autoridades y obligaciones de cada área participante.

Este marco se fundamenta en los principios de gobernanza y gestión del riesgo operativo establecidos por Basilea, particularmente en lo relacionado al modelo de líneas de defensa para la gestión del riesgo operacional. Este enfoque establece que la efectividad del control depende de la clara segregación entre quienes ejecutan, supervisan y auditan, garantizando independencia, trazabilidad y transparencia en la gestión del riesgo derivado de terceros. Basilea destaca además que la gestión de terceros constituye un componente esencial del riesgo operacional, y que las instituciones financieras deben asegurar que los riesgos derivados de terceros sean identificados, mitigados, monitoreados y reportados de manera equivalente a los riesgos internos.

En coherencia con estos principios, la gobernanza del modelo articula las responsabilidades de las distintas áreas involucradas —riesgo operativo, continuidad del negocio, tecnología, administradores de contratos, proveedores, auditoría interna y comités especializados — de modo que la gestión de proveedores críticos se ejecute bajo criterios comunes, transparencia organizacional y control efectivo. Este enfoque permite garantizar que las decisiones se adopten con fundamento técnico, que exista trazabilidad de las actividades realizadas y que los proveedores cumplan con los estándares regulatorios, contractuales y operativos exigidos por la institución.

Esta sección describe la gobernanza operativa del modelo, precisando las funciones que deben desempeñar los distintos actores institucionales para garantizar que la metodología se aplique de manera consistente, oportuna y alineada con los estándares de continuidad del negocio (ISO 22301:2019), los requisitos regulatorios vigentes y las políticas internas de gestión de riesgos.

Asimismo, la definición clara de roles facilita la rendición de cuentas, evita duplicidad de funciones, fortalece la trazabilidad del proceso y asegura que las decisiones críticas relacionadas con terceros se basen en criterios objetivos y verificables. Con ello, la organización mantiene un control efectivo sobre la gestión de sus proveedores críticos y mitiga los riesgos asociados a la dependencia operativa de servicios externos.

A continuación, se lista cada actor con su rol:

- **Gerencia de Riesgo Operativo:** Es la instancia responsable de coordinar y organizar la ejecución integral de las evaluaciones a los proveedores críticos. Consolida los resultados obtenidos en cada fase de la metodología, realiza el análisis transversal de riesgos asociados y presenta los hallazgos y recomendaciones ante los comités correspondientes para la toma de decisiones.
- **Oficial de Continuidad del Negocio:** Se encarga de verificar la calidad, consistencia y suficiencia de la información presentada por los proveedores, asegurando que cumpla con los requisitos técnicos establecidos en materia de continuidad del negocio. Evalúa el alineamiento del proveedor con los parámetros definidos en ISO 22301, el BIA institucional y los criterios regulatorios aplicables.
- **Administradores de Contratos y Áreas Usuarias:** Son responsables de gestionar la relación operativa con los proveedores, solicitando la documentación requerida, facilitando los canales de comunicación y verificando que se cumplan las obligaciones contractuales relacionadas con continuidad del negocio. Adicionalmente, apoyan en la supervisión del avance de los planes de acción definidos.
- **Proveedor Crítico de Continuidad del Negocio:** Debe proporcionar de manera oportuna y veraz toda la documentación, evidencias y resultados de pruebas necesarias para la evaluación. Asimismo, completa los cuestionarios de autoevaluación, colabora en la validación de información técnica y ejecuta los planes de acción acordados para cerrar brechas o fortalecer su nivel de madurez.
- **CAIR (Comité de Administración Integral de Riesgos) y Comité de Continuidad:** Tienen la responsabilidad de revisar los resultados consolidados de la evaluación, analizar los riesgos identificados y tomar decisiones estratégicas en

los casos que presenten impactos significativos, incumplimientos de alto nivel o brechas críticas. Su rol es asegurar que los riesgos derivados de proveedores críticos se gestionen dentro de los niveles de apetito y tolerancia definidos por la organización.

- **Auditoría Interna:** Tiene la función de evaluar de manera independiente la efectividad de la metodología**,** verificando que su aplicación sea consistente, completa y alineada con las políticas internas, las regulaciones vigentes y las mejores prácticas internacionales. Auditoría Interna revisa la calidad de los registros, el cumplimiento de las fases metodológicas y la eficacia de los planes de acción implementados. Sus recomendaciones permiten fortalecer la gobernanza del modelo y asegurar su mejora continua.

- **Empresas Evaluadoras Externas (cuando aplique):** Podrán ser contratadas para realizar evaluaciones especializadas o independientes**,** especialmente en casos de proveedores altamente críticos, servicios tecnológicos complejos o requerimientos regulatorios específicos. Estas empresas aportan objetividad técnica**,** validez independiente y profundidad en el análisis de capacidades de continuidad, ciberseguridad, infraestructura o resiliencia operativa. Sus informes complementan y robustecen la evaluación interna del proveedor.

Tabla 15 Matriz RACI roles en cada fase

ROL	FASE I	FASE II	FASE III	FASE IV	FASE V
Gerencia de Riesgo Operativo	A	A	A	A	A / R
Oficial de Continuidad del Negocio	R	R	R	R	R
Administrador Contrato o Área Usuaria	R	C	C	R	R
Proveedor Crítico de Continuidad del Negocio	I	I	R (entrega inform.)	R	R
CAIR	I	I	I	C / A (si supera	I

				el apetito de riesgo)	
Auditoría Interna	I	I	I	I	C / R (evaluación independiente)
Empresas Evaluadoras Externas	I	I	C / R (cuando aplique)	R	C

Fuente: Elaboración propia.

Una parte elemental de la evaluación son las herramientas de apoyo**,** las cuales permiten simplificar el seguimiento y la implementación, para esto se considera como mínimo el uso de:

- Herramienta de Gestión de Riesgos: permite el registro de riesgos, planes de acción y califica el riesgo inherente y residual.
- Herramienta de Evaluación: aquí los proveedores cargan evidencias y completan autoevaluaciones, emite calificación del grado de madurez.
- Plantillas estandarizadas: listas de verificación, cuestionarios, plantillas para informes de resultados y planes de acción.

El presente capítulo ha desarrollado de manera progresiva y estructurada la metodología para la gestión de riesgos de proveedores críticos de continuidad del negocio, partiendo del análisis del contexto institucional y normativo, la descripción de las fases que conforman el modelo propuesto y la definición de roles y responsabilidades. A lo largo del capítulo se han establecido los criterios de evaluación, los instrumentos metodológicos y los mecanismos de control necesarios para asegurar una gestión sistemática, trazable y alineada con las mejores prácticas y exigencias regulatorias aplicables al sector financiero.

Con el propósito de garantizar la aplicabilidad práctica del modelo y facilitar su adopción por parte de la institución financiera objeto de estudio, el detalle completo del modelo desarrollado, incluyendo sus fases, criterios de evaluación, instrumentos, responsabilidades y lineamiento operativos se presentan en el Anexo 2. Dicho Anexo

consolida la propuesta final en una estructura de manual de aplicación, diseñada específicamente en función de las necesidades, nivel de madurez y particularidades operativas de una institución financiera regulada por la Superintendencia de Bancos, respetando la estructura documental, el lenguaje técnico y los formatos definidos.

En este manual se integran y articulan de forma coherente las herramientas expuestas en el presente capítulo tales como: fichas de evaluación de proveedores, esquemas de ponderación, planes de acción y mecanismos de monitoreo y seguimiento, dentro de un marco de aplicación práctico, secuencial y reproducible. Esta aproximación permite que el modelo no solo sea comprendido desde una perspectiva metodológica, sino que pueda ser utilizado de manera efectiva en los procesos reales de gestión de proveedores críticos de continuidad del negocio.

En consecuencia, el Anexo 2 transciende el rol de complemento teórico, constituyéndose en el producto principal de la presente tesis, al ofrecer una guía operativa integral, lista para su implementación, adaptación y mejora continua dentro de la institución financiera. De esta forma, el modelo propuesto contribuye de manera concreta al fortalecimiento de la resilencia operativa institucional, a la adecuada gestión de los riesgos derivados de terceros y al cumplimiento de las exigencias regulatorias vigentes, aportando valor tanto a nivel académico como práctico.

CAPÍTULO 3
PLAN DE IMPLEMENTACIÓN DE LA PROPUESTA

El presente capítulo tiene como propósito definir el plan de implementación del modelo de gestión de riesgos de proveedores críticos de continuidad del negocio propuesto en los capítulos anteriores, estableciendo el marco mediante el cual la institución financiera podrá adoptar la metodología e iniciar su aplicación dentro de sus procesos internos.

Este capítulo se orienta a describir las condiciones, lineamientos y actividades necesarias para la puesta en marcha del modelo, considerando la estructura organizacional, los roles definidos, los recursos requeridos y la secuencia lógica de implementación. En este sentido, el enfoque se centra en el cómo la institución incorporará el modelo a su esquema de gestión, asegurando su alineación con la normativa vigente, las políticas internas y el nivel de madurez actual en materia de continuidad del negocio y gestión de terceros.

Es importante precisar que el alcance de este capítulo no contempla la ejecución del modelo, ni la aplicación práctica de las evaluaciones a proveedores críticos. La implementación se aborda desde una perspectiva planificada y preparatoria, orientado a sentar las bases organizativas, metodológicas y operativas que permitan, en una etapa posterior no incluida dentro de esta tesis, su ejecución efectiva y sostenida en el tiempo.

De esta manera, el capítulo constituye un puente entre el diseño metodológico del modelo y su futura aplicación, proporcionando a la institución financiera una hoja de ruta clara para su adopción, minimizando riesgos de implementación y facilitando la integración del modelo en los procesos existentes de gestión de riesgos y continuidad del negocio.

3.1 Objetivo general y objetivos específicos del plan de implementación

Esta sección describe el objetivo general y los objetivos específicos del plan de implementación para la metodología en torno a los riesgos de proveedores críticos para la continuidad del negocio. Estos objetivos proporcionan una hoja de ruta para la implementación dentro de la institución financiera objeto de estudio. Esto permite el establecimiento de un enfoque estructurado que incorpora todo el ciclo de gestión de riesgos de proveedores externos: identificación, evaluación, monitoreo y control. Este enfoque también considera el cumplimiento de las regulaciones locales, la integración con las mejores prácticas internacionales y la alineación con el marco de resiliencia operativa de la institución.

3.1.1. Objetivo general

Definir un plan de implementación para la adopción institucional del modelo de gestión de riesgos de proveedores críticos de continuidad del negocio de manera ordenada y estructurada estableciendo los lineamientos, responsabilidades, actividades y condiciones necesarias para su incorporación formal en la institución financiera.

3.1.2. Objetivos específicos

- Delimitar el alcance del plan de implementación, estableciendo los supuestos, restricciones y exclusiones.
- Establecer las actividades necesarias para la adopción del modelo, asegurando una implementación ordenada y coherente con la estructura organizacional de la institución financiera.
- Definir los roles y responsabilidades institucionales involucrados en la implementación del modelo, conforme los principios de gobernanza, segregación de funciones y control interno.
- Determinar los recursos organizacionales, técnicos y documentales requeridos para la implementación del modelo, considerando el nivel de madurez institucional en gestión de continuidad del negocio y riesgo de terceros.

- Alinear el modelo propuesto con las políticas internas, la normativa vigente y los procesos existentes de gestión de riesgos, continuidad del negocio y administración de proveedores.
- Establecer mecanismos de control y seguimiento de la implementación, que permitan evaluar el nivel de preparación institucional previo al inicio de la aplicación del modelo.

3.2. Alcance del Plan de Implementación

El presente plan de implementación tiene como alcance definir las condiciones, lineamientos y actividades necesarias para la adopción institucional del modelo de gestión de riesgos de proveedores críticos de continuidad del negocio de la institución financiera objeto del estudio.

El plan contempla la integración del modelo dentro del marco de gobernanza existente, la definición de roles y responsabilidades, la articulación con las políticas internas y la normativa vigente, así como la identificación de los recursos organizacionales, técnicos y documentales requeridos para su puesta en marcha. Asimismo, establece la secuencia de actividades preparatorias que permitan a la institución financiera iniciar la aplicación del modelo de manera ordenada, consistente y alineada con su nivel de madurez en gestión de riesgos y continuidad del negocio.

El alcance del plan se limita a la fase de implementación conceptual y organizativa del modelo, por lo que no incluye la ejecución operativa de las evaluaciones a proveedores críticos, la aplicación de cuestionarios, la validación de evidencias, la definición o ejecución de planes de acción, ni el monitoreo de resultados derivados de la aplicación del modelo.

Finalmente, el Plan de Implementación no contempla la adquisición de herramientas tecnológicas, la contratación de proveedores externos, la realización de auditorías o evaluaciones independientes, salvo en lo que respecta a su identificación conceptual como requerimientos futuros. En consecuencia, el presente plan constituye una hoja de ruta institucional para la adopción del modelo, orientada a reducir riesgos de implementación y facilitar su posterior aplicación efectiva.

3.3. Actividades del Plan de Implementación del Modelo

En coherencia con el alcance del Plan de Implementación y con el objetivo de asegurar una adopción ordenada del modelo de tratamiento de riesgos de proveedores críticos de continuidad de negocio, se definen a continuación las actividades necesarias para su implementación y adopción institucional. Estas actividades constituyen la base para la elaboración de la Estructura de Desglose de Trabajo (EDT) y para la posterior construcción del cronograma de implementación.

Como actividad inicial, se establece la aprobación formal del Plan de Implementación por parte de las instancias de gobierno correspondiente a la institución financiera que opera bajo lineamientos de la Superintendencia de Bancos. Esta actividad busca otorgar la validez institucional al proceso de adopción del modelo y garantizar su alineación con las prioridades estratégicas y de gestión de riesgos de la organización.

De manera complementaria, se incluye la designación formal de los responsables de la implementación, así como la definición del patrocinio institucional del modelo. Esta actividad permite asegurar liderazgo, asignación de responsabilidades y respaldo ejecutivo para le ejecución de las actividades previstas en el plan.

La siguiente actividad definida es la configuración del esquema de gobernanza del proceso de implementación, que incluye la definición de los niveles de decisión, los mecanismos de coordinación entre las áreas participantes y los procedimientos de escalamiento. Esta actividad busca asegurar la correcta segregación de funciones y la integración del modelo dentro del sistema de control interno de la institución-

El plan además incorpora la comunicación interna del inicio de la implementación, mediante la difusión de la entrada en vigencia de la metodología, sus objetivos y principales lineamientos del modelo y su alcance con las áreas involucradas. Esta actividad es clave para generar entendimiento común, reducir resistencias organizacionales y facilitar la coordinación durante el proceso de adopción.

Una parte fundamental en la fase preparatoria es la capacitación conceptual de los actores clave, orientada a socializar la metodología de tratamiento de riesgos de proveedores críticos, sus componentes, criterios de evaluación y responsabilidades asociadas. Esta capacitación se limita a nivel conceptual y metodológico, sin incluir ejercicios prácticos ni evaluaciones operativas.

Otra de las actividades relevantes es la revisión y alineación de la documentación interna existente, incluyendo políticas, procedimientos y lineamientos relacionados con la gestión de riesgos, continuidad del negocio y gestión de proveedores. Esta actividad busca asegurar la coherencia conceptual del marco documental con el modelo propuesto, sin implicar la ejecución de cambios operativos o rediseños profundos de procesos.

Esta planificación de ejecución del modelo incluye la definición de la secuencia lógica de actividades, la identificación de dependencias, la validación de condiciones mínimas para el inicio de la fase operativa y la preparación de los insumos necesarios para su aplicación futura. Esta actividad permite cerrar la fase de implementación y habilitar el paso controlado hacia la aplicación del modelo.

En conjunto, todas estas actividades conforman una estructura lógica y progresiva que puede ser desagregada en una EDT, facilitando la asignación de responsables, la estimación de tiempos y la construcción del cronograma de implementación del modelo.

3.4. Roles y Responsabilidades Institucionales

La implementación del modelo requiere la definición clara de roles y responsabilidades institucionales involucrados, con el fin de asegurar una ejecución ordenada, coherente y alineada con los principios de gobernanza segregación de funciones y control interno, por esto, el plan de implementación establece un esquema de responsabilidades que van de la mano con la gestión de riesgos basada en Basilea, donde veremos los roles y responsabilidades por línea de defensa:

Órganos de Gobierno y Comités:

Comité de Administración Integral de Riesgos (CAIR):

En el marco del plan de implementación, el CAIR cumple un rol de supervisión y validación estratégica, siendo responsable de:

- Conocer el cronograma, fases y enfoque metodológico definidos para la implementación del modelo.
- Conocer los avances y principales hitos de implementación.
- Validar las decisiones adoptadas por el Comité de Continuidad del Negocio respecto a la preparación institucional para la evaluación del proveedores

críticos con niveles de riesgo alto o extremo, y , de ser necesario, disponer lineamientos adicionales en el marco de la gestión integral de riesgos.

Comité de Continuidad del Negocio:

Durante la fase de implementación, este Comité asume responsabilidades de dirección y coordinación metodológica, orientadas a:

- Aprobar el cronograma y fases previstas para la implementación del modelo.
- Conocer y analizar los lineamientos metodológicos definidos para la evaluación de proveedores críticos.
- Definir criterios y directrices generales que orienten la posterior ejecución del modelo.
- Informar al CAIR sobre el avance de la implementación y las decisiones adoptadas, conforme al marco de gobernanza institucional.

Primera Línea de Defensa

Proveedores Críticos de Continuidad del Negocio:

En el contexto del Plan de Implementación, la participación de los proveedores críticos se limita a actividades de preparación y coordinación, tales como:

o Conocer los lineamientos generales del modelo y de los requerimientos asociados a su futura aplicación.

o Participar cuando corresponda en actividades de socialización, talleres o capacitaciones conceptuales relacionadas con la metodología.

o Prepara las condiciones necesarias para la entrega de información y documentación durante la fase de aplicación del modelo.

Áreas de División Dueñas del Servicio:

Las áreas responsables de los servicios críticos participan en la implementación mediante:

- La identificación y validación de los proveedores críticos bajo su responsabilidad.

- Apoyo en la coordinación institucional con los proveedores durante la fase preparatoria.
- Provisión de información relevante sobre los servicios de terceros y sus dependencias, como insumo para la correcta adopción del modelo.

Segunda Línea de Defensa

Gerencia de Riesgo Operativo:

La Gerencia de Riesgo Operativo desempeña un rol central en la implementación del modelo siendo responsable de:

- Definir y documentar el cronograma, las fases y la metodología de implementación del modelo.
- Liderar la coordinación institucional del proceso de adopción del modelo.
- Validar la coherencia metodológica del modelo con las políticas internas y el marco de gestión de riesgos.
- Prepara los lineamientos, herramientas conceptuales y criterios que serán utilizados en la fase de aplicación.
- Informar a los Comités correspondientes sobre los avances, riesgos de implementación y condiciones de preparación institucional.
- Coordinar actividades de capacitación conceptual dirigidas a las áreas internas y actores relevantes.

Tercera Línea de Defensa

Auditoría Interna:

- En el marco del Plan de Implementación, Auditoría Interna cumple un rol de aseguramiento independiente orientado a**:**
- Verificar que la implementación del modelo se realice conforme a la metodología aprobada y a los principios de control interno.
- Evaluar la consistencia del esquema de gobernanza y segregación de funciones definido para la adopción del modelo.

Cuarta Línea de Defensa

Empresa Evaluadora/Auditoría Externa:

Durante la fase de implementación, la participación de evaluadores externos se limita a su identificación conceptual como un requerimiento futuro del modelo, pudiendo:

- Conocer y comprender la metodología y los lineamientos definidos.
- Preparar las condiciones necesarias para su eventual participación en la fase de aplicación operativa del modelo, sin ejecutar evaluaciones ni emitir informes durante esta etapa.

Tabla 16 Roles y Responsabilidades Plan de Implementación

Línea de defensa / Nivel	Rol / Instancia	Responsabilidades en el Plan de Implementación
Gobernanza	Comité de Administración Integral de Riesgos (CAIR)	Conocer y validar el cronograma, fases y enfoque metodológico del plan de implementación.
		Conocer los avances y principales hitos del proceso de implementación.
		Validar decisiones estratégicas adoptadas por el Comité de Continuidad del Negocio relacionadas con la preparación institucional
		Disponer lineamientos adicionales en el marco de la gestión integral de riesgos, de ser necesario.
Gobernanza	Comité de Continuidad del Negocio	Aprobar el cronograma y las fases del plan de implementación.
		Conocer y analizar los lineamientos metodológicos definidos para la adopción del modelo
		Emitir directrices generales que orienten la posterior aplicación del modelo
		Informar al CAIR sobre avances, decisiones y condiciones de preparación institucional.
Primera línea de defensa	Proveedores Críticos de Continuidad del Negocio	Conocer los lineamientos generales del modelo y sus requerimientos.
		Participar en actividades de socialización, talleres o capacitaciones conceptuales.
		Preparar condiciones para la entrega de información y documentación en la fase de aplicación del modelo.
Primera línea de defensa	Áreas Dueñas del Servicio	Identificar y validar los proveedores críticos bajo su responsabilidad.

		Coordinar institucionalmente con los proveedores durante la fase preparatoria
		Proporcionar información relevante sobre los servicios tercerizados y sus dependencias como insumo para la implementación.
Segunda línea de defensa	Gerencia de Riesgo Operativo	Definir y documentar el cronograma, fases y metodología de implementación del modelo.
		Liderar y coordinar institucionalmente el proceso de adopción del modelo.
		Alinear el modelo con políticas internas y el marco de gestión de riesgos.
		Preparar lineamientos, criterios y herramientas conceptuales.
		Coordinar actividades de capacitación conceptual
		Informar a los comités sobre avances, riesgos de implementación y nivel de preparación institucional.
Tercera línea de defensa	Auditoría Interna	Verificar que la implementación del modelo se ejecute conforme a la metodología aprobada.
		Evaluar la consistencia del esquema de gobernanza y segregación de funciones definido para la adopción del modelo.
Cuarta línea de defensa	Empresa Evaluadora / Auditoría Externa	Conocer la metodología y los lineamientos definidos para el modelo.
		Preparar condiciones para su eventual participación en la fase de aplicación operativa
		No ejecutar evaluaciones ni emitir informes durante la fase de implementación.

Fuente: Elaboración propia.

3.5. Recursos, alineación institucional y mecanismos de control del Plan de Implementación

La implementación del modelo requiere la disponibilidad y articulación de recursos organizaciones, técnicos y documentales, así como su alineación con el marco normativo interno, la normativa y los procesos vigentes de la institución financiera.

En este contexto, se integrará los elementos asociados a los recursos requeridos, la alineación institucional y los mecanismos de control, entendidos como componentes habilitantes para una implementación ordenada, coherente y sostenible del modelo.

Desde una perspectiva organizacional, la implementación se apoya en la estructura organizacional existente mediante la asignación de roles y responsabilidades de acuerdo a la intervención de las áreas. Respecto de los recursos técnicos, el plan de

implementación no requiere de herramientas específicas, sino únicamente las básicas de gestión documental, seguimiento de actividades y registro de información, las cuales pueden apoyarse en las plataformas institucionales disponibles.

En lo relacionado con recursos documentales, la implementación del modelo requiere la disponibilidad de políticas, procedimientos, metodologías y lineamientos internos relacionados con gestión de riesgos, continuidad del negocio y gestión del proveedores, los cuales sirven como base para integración conceptual del modelo del marco institucional vigentes.

Tabla 17 Recursos requeridos para la Implementación

Tipo de recurso	Descripción	Consideraciones en el Plan de Implementación
Organizacionales	Áreas de riesgos, continuidad del negocio, tecnología, compras y áreas dueñas del servicio	Uso de estructura existente, sin creación de nuevas unidades
Humanos	Roles definidos por línea de defensa	Asignación de responsabilidades y dedicación parcial
Técnicos	Herramientas institucionales existentes	No se contempla adquisición de nuevas soluciones
Documentales	Políticas, procedimientos y metodologías internas	Revisión y alineación conceptual

Un requisito indispensable es la alineación del modelo con las políticas internas de la institución financiera, así como la normativa aplicable en lo relacionado a gestión de riesgos, continuidad del negocio y administración de terceros. Esto es necesario tanto a nivel conceptual como metodológico, garantizando coherencia del modelo con los marcos regualtorios y de buenas prácticas adoptadas por la institución, como son principios Basilea, ISO 22031 y reglamento DORA.

De igual manera se considera la articulación del modelo con los procesos de gestión de riesgos, continuidad del negocio y gestión de proveedores vigentes, evitando duplicidad y promoviendo la integración dentro del sistema de gestión institucional. Esta actividad no implica modificación operativa de los procesos vigentes, sino la validación de su compatibilidad con el modelo propuesto.

Tabla 18 Alineación del modelo al Marco Institucional

Elemento institucional	Enfoque de alineación
Políticas de gestión de riesgos	Coherencia con apetito de riesgo y gobierno corporativo
Gestión de continuidad del negocio	Integración metodológica con BCM
Gestión de proveedores	Articulación con procesos de administración de terceros
Normativa externa	Alineación con Basilea, ISO 22301 y DORA

Evaluar el nivel de preparación institucional previo al inicio de la aplicación del modelo es necesario, por lo cual es Plan de Implementación establece mecanismos de control y seguimiento orientados a verificar el cumplimiento de las actividades definidas, la correcta asignación de responsabilidades y la coherencia del modelo del marco institucional.

Estos mecanismos incluyen el seguimiento periódico del avance del plan, la validación de entregables asociados a la implementación, la identificación temprana de desviaciones o riesgos de adopción y el reporte a los comités correspondientes. De esta manera, se asegura que la institución financiera cuente con las condiciones mínimas necesarias para avanzar hacia la fase de aplicación del modelo de forma controlada.

Tabla 19 Mecanismos de Control y Seguimiento

Mecanismo	Objetivo	Responsable
Seguimiento del cronograma	Verificar cumplimiento de actividades	Gerencia de Riesgo Operativo
Reportes a comités	Informar avances y riesgos de implementación	Gerencia de Riesgo Operativo
Validación de entregables	Confirmar preparación institucional	Comités de Gobernanza
Revisión independiente	Asegurar cumplimiento metodológico	Auditoría Interna

Fuente: Elaboración propia.

3.6. Estructura de desglose de trabajo (EDT)

La Estructura del Desglose de Trabajo (EDT) del Plan de Implementación tiene como objetivo descomponer el trabajo requerido en componentes jerárquicos y gestionables, que faciliten la planificación, asignación de responsabilidades, seguimiento y elaboración del cronograma de implementación.

El EDT se construye a partir de las actividades definidas en los numerales anteriores, integrando los roles y responsabilidades institucionales, los recursos requeridos y los mecanismos de control establecidos. Su alcance se limita a la fase de implementación conceptual y organizativa del modelo, excluyendo expresamente la ejecución operativa de evaluaciones, la aplicación de cuestionarios, la validación de evidencia y el seguimiento de planes de acción a proveedores críticos.

Tabla 20 Estructura de Desglose de Trabajo (EDT)

Nivel 1	Nivel 2	Nivel 3	Actividad	Responsable
1	Inicio del Plan de Implementación	1.1	Aprobación formal del Plan de Implementación	CAIR Comité de Continuidad del Negocio
		1.2	Designación de responsables y patrocinio institucional	Alta Dirección
		1.3	Comunicación interna de inicio del plan	Gerencia de Riesgo Operativo
2	Gobernanza y Coordinación	2.1	Definición del esquema de gobernanza y escalamiento	Gerencia de Riesgo Operativo
		2.2	Alineación con el modelo de líneas de defensa	Gerencia de Riesgo Operativo
		2.3	Coordinación interáreas para la implementación	Gerencia de Riesgo Operativo
3	Preparación Metodológica	3.1	Definición del enfoque metodológico y fases	Gerencia de Riesgo Operativo
		3.2	Revisión y alineación de políticas y procedimientos	Gerencia de Riesgo Operativo Continuidad del Negocio
		3.3	Definición de lineamientos y criterios metodológicos	Gerencia de Riesgo Operativo
4	Capacitación y Socialización	4.1	Identificación de actores clave involucrados	Gerencia de Riesgo Operativo
		4.2	Capacitación conceptual a áreas internas	Gerencia de Riesgo Operativo
		4.3	Socialización del modelo con proveedores críticos	Áreas Dueñas del Servicio

5	Recursos y Soporte a la Implementación	5.1	Identificación y asignación de recursos organizacionales	Gerencia de Riesgo Operativo
		5.2	Identificación de herramientas técnicas de soporte	Tecnología de la Información
		5.3	Identificación y alineación de recursos documentales	Gerencia de Riesgo Operativo
6	Control y Seguimiento del Plan	6.1	Seguimiento del cronograma de implementación	Gerencia de Riesgo Operativo
		6.2	Validación de entregables de implementación	Comité de Continuidad del Negocio
		6.3	Reporte de avances a instancias de gobierno	Gerencia de Riesgo Operativo
7	Cierre de la Implementación	7.1	Evaluación del nivel de preparación institucional	Gerencia de Riesgo Operativo
		7.2	Aprobación para inicio de la fase de aplicación	CAIR Comité de Continuidad del Negocio
		7.3	Cierre formal del Plan de Implementación	Alta Dirección

Fuente: Elaboración propia.

La asignación de responsable en la EDT se realiza a nivel de coordinación y gobierno, considerando que las actividades corresponden a la fase de implementación del moldeo y no a su aplicación operativa.

3.7. Análisis de Riesgos para la Implementación

La aplicación de la EDT puede verse afectada por factores internos y externos propios de la dinámica institucional, por ello es necesario identificar y analizar los principales riesgos asociados con el propósito de anticipar desviaciones en plazos, responsabilidades, calidad de los entregables o nivel de preparación institucional. Este análisis permite anticipar posibles obstáculos, fortalecer los controles preventivos y establecer acciones orientadas a reducir la probabilidad de materialización de los riesgos identificados.

El análisis de riesgos se desarrolla con base con los principios y lineamientos de la norma ISO 31000:2018, garantizando un enfoque sistemático, estructurado y basado en evidencia para la toma de decisiones. En particular, se adopta el principio de pensamiento basado en riesgos, que permite evaluar de manera integral los factores organizacionales, técnicos y normativos que influyen en el proceso de implementación, priorizando

acciones preventivas frente a escenarios que podrían impactar negativamente el cumplimiento de los objetivos del plan.

A continuación, se listan los riesgos identificados por cada nivel del EDT, su causa y el impacto en la implementación:

Tabla 21 Análisis de Riesgos

Bloque EDT (Nivel 1)	Riesgo identificado	Causa principal	Impacto en la implementación
1. Inicio del Plan de Implementación	Falta de aprobación o retraso en la aprobación del plan	Prioridades institucionales divergentes o falta de patrocinio	Retraso en el inicio del plan y pérdida de respaldo institucional
	Designación ambigua de responsables	Definición incompleta de roles y patrocinio	Confusión en la ejecución y debilidad en la gobernanza del proceso
2. Gobernanza y Coordinación	Esquema de gobernanza insuficientemente definido	Falta de claridad en niveles de decisión y escalamiento	Conflictos de responsabilidad y retrasos en la toma de decisiones
	Baja coordinación interáreas	Silos organizacionales o falta de comunicación	Duplicidad de esfuerzos y retrasos en actividades críticas
3. Preparación Metodológica	Definición incompleta del enfoque metodológico	Falta de alineación técnica o normativa	Inconsistencias en la adopción del modelo
	Alineación documental insuficiente	Documentación desactualizada o dispersa	Dificultades para integrar el modelo al marco institucional
4. Capacitación y Socialización	Capacitación insuficiente de actores clave	Limitaciones de tiempo o baja priorización	Aplicación incorrecta o resistencia al modelo
	Baja participación de proveedores críticos	Falta de comunicación o entendimiento del alcance	Riesgo de retrasos en la fase de aplicación
5. Recursos y Soporte	Disponibilidad limitada de recursos organizacionales	Sobrecarga operativa de áreas clave	Retrasos en la ejecución del plan

	Dependencia de herramientas no adecuadas	Limitaciones de plataformas existentes	Ineficiencias en el seguimiento y control
6. Control y Seguimiento	Seguimiento insuficiente del cronograma	Falta de mecanismos formales de control	Desviaciones no detectadas oportunamente
	Reportes tardíos a instancias de gobierno	Falta de disciplina de reporte	Decisiones correctivas tardías
7. Cierre de la Implementación	Evaluación incompleta de la preparación institucional	Falta de criterios claros de cierre	Inicio prematuro de la fase de aplicación
	Aprobación formal sin evidencia suficiente	Presión por cumplimiento de plazos	Incremento del riesgo operativo en la fase posterior

Fuente: Elaboración propia.

3.8. Cronograma

El cronograma permite visualizar la secuencia lógica de actividades, la interdependencia entre los paquetes de trabajo y el horizonte temporal requerido para la implementación institucional del modelo.

La duración y secuencia de las actividades se han definido tomando en cuenta la disponibilidad razonable de recursos, la necesidad de coordinación interdepartamental y las prácticas habituales de gestión en instituciones financieras. El cronograma propuesto puede ser ajustado por la organización en función de su contexto operativo, sin afectar la estructura ni los objetivos del plan de implementación, además es necesario considerar los tiempos que la normativa exige para la aplicación de este modelo.

La planificación se estructura en un horizonte de corto plazo, considerando dependencias entre actividades y la necesidad de validaciones institucionales progresivas. A continuación del cronograma propuesto:

Tabla 22 Cronograma del Plan de Implementación

Secuencia	Bloque EDT	Actividad	Responsable	Duración estimada (días)	Dependencia	Hito / Entregable
1		Aprobación formal del Plan de Implementación	CAIR / Comité de Continuidad del Negocio	5	-	Acta de aprobación del Plan de Implementación
2	Inicio del Plan de Implementación	Designación de responsables y patrocinio institucional	Alta Dirección	3	1	Resolución o comunicación formal de designación de responsables
3		Comunicación interna de inicio del plan	Gerencia de Riesgo Operativo	2	2	Comunicado institucional de inicio del Plan
4		Definición del esquema de gobernanza y escalamiento	Gerencia de Riesgo Operativo	4	3	Documento de gobernanza y esquema de escalamiento aprobado
5	Gobernanza y Coordinación	Alineación del modelo con líneas de defensa	Gerencia de Riesgo Operativo	3	4	Mapa de roles por línea de defensa
6		Coordinación interáreas para la implementación	Gerencia de Riesgo Operativo	5	4	Actas de reuniones de coordinación interáreas
7		Definición del enfoque metodológico y fases	Gerencia de Riesgo Operativo	6	5	Documento metodológico del modelo
8	Preparación Metodológica	Revisión y alineación de políticas y procedimientos	Gerencia de Riesgo Operativo / Continuidad del Negocio	8	7	Matriz de alineación documental

9		Definición de lineamientos y criterios metodológicos	Gerencia de Riesgo Operativo	5	8	Lineamientos metodológicos aprobados
10		Identificación de actores clave involucrados	Gerencia de Riesgo Operativo	3	6	Listado de actores clave por área
11	Capacitación y Socialización	Capacitación conceptual a áreas internas	Gerencia de Riesgo Operativo	5	10	Material de capacitación y registros de asistencia
12		Socialización del modelo con proveedores críticos	Áreas Dueñas del Servicio	7	11	Presentaciones y actas de socialización con proveedores
13		Identificación y asignación de recursos organizacionales	Gerencia de Riesgo Operativo	4	6	Matriz de recursos y responsables
14	Recursos y Soporte	Identificación de herramientas técnicas de soporte	Tecnología de la Información	5	13	Informe de herramientas y capacidades disponibles
15		Identificación y alineación de recursos documentales	Gerencia de Riesgo Operativo	4	8	Inventario documental del modelo
16		Seguimiento del cronograma de implementación	Gerencia de Riesgo Operativo	Transversal	Inicio del plan	Reportes periódicos de avance
17	Control y Seguimiento	Validación de entregables de implementación	Comité de Continuidad del Negocio	5	9, 11, 15	Acta de validación de entregables
18		Reporte de avances a instancias de gobierno	Gerencia de Riesgo Operativo	3	17	Informe ejecutivo de avances

19		Evaluación del nivel de preparación institucional	Gerencia de Riesgo Operativo	5	18	Informe de preparación institucional
20	Cierre de la Implementación	Aprobación para inicio de la fase de aplicación	CAIR / Comité de Continuidad del Negocio	3	19	Acta de autorización para fase de aplicación
21		Cierre formal del Plan de Implementación	Alta Dirección	2	20	Acta de cierre del Plan de Implementación

Fuente: Elaboración propia.

Adicionalmente, con el objetivo de detectar de manera oportuna posibles desviaciones respecto al cronograma establecido, se han definido hitos o entregables por nivel, los cuales permiten monitorear el avance, evaluar el cumplimiento de los entregables esperados y activar mecanismos de alerta y escalamiento cuando sea necesario. Estos hitos se vinculan directamente con la identificación de los riesgos asociados a cada nivel, facilitando su análisis preventivo y tratamiento oportuno de aquellos eventos que puedan afectar el cumplimiento de los objetivos del Plan de Implementación:

3.9. Presupuesto estimado

El presupuesto estimado del Plan de Implementación se construye a partir de la identificación de las actividades definidas en el EDT, los responsables institucionales involucrados y la estimación del tiempo de dedicación requerido para cada actividad, en concordancia con el cronograma propuesto.

En este sentido, los valores asignados no representan costos directos de ejecución operativa, sino una estimación del esfuerzo organizacional requerido para la adopción institucional del modelo, considerando principalmente horas de trabajo de comités, gerencias y áreas técnicas, así como apoyos especializados puntuales cuando el nivel de madurez o complejidad así lo requiera.

El presupuesto incorpora tanto recursos internos como costos mixtos o externos de carácter referencial, permitiendo visualizar de forma anticipada los requerimientos económicos del plan y facilita la toma de decisiones por parte de la alta dirección, en línea con los principios de eficiencia, control y gestión prudencial de recursos promovidos por Basilea y el enfoque de gestión de riesgos de ISO31000.

Tabla 23 Presupuesto Estimado

Nivel	Actividad	Tipo de Costo	Descripción del Recurso	Presupuesto Estimado (USD)
1	Gestión y Gobierno del plan	Interno	Tiempo de Comités, gerencia y coordinación del plan	2.000

	2	Alineación normativa y documental	Interno	Revisión y ajuste de políticas, procedimientos y lineamientos	1.500
	3	Adecuación organización y de roles	Interno	Definición de roles, validación RACI, coordinación interáreas	2.000
	4	Preparación de recursos y capacidades	Mixto	Diagnóstico de capacidades y diseño del plan de capacitación	2.000
	5	Gestión de riesgos del plan de implementación	Interno	Identificación, análisis y tratamiento de riesgos	1.500
	6	Definición del esquema de control y seguimiento	Interno	Definición de indicadores, reportes y puntos de control	1.000
	7	Formalización del modelo para su adopción	Mixto	Consolidación documental, validación y aprobación institucional	2.000
		Subtotal Plan de Implementación			12.000
-		Apoyo especializado (opcional)	Externo	Asesoría técnica puntual	3.000
		TOTAL ESTIMADO CON APOYO ESPECIALIZADO			**15.000**

Fuente: Elaboración propia.

El presupuesto estimado del Plan de Implementación proporciona una visión integral y realista de los recursos económicos requeridos para la adopción del modelo propuesto, sin comprometer a la institución financiera con costos asociados a su ejecución operativa. Este enfoque permite a la alta dirección evaluar de forma anticipada la factibilidad del plan, priorizar recursos y garantizar que la implementación se realice bajo criterios de eficiencia, control y alineación con el apetito de riesgo institucional.

3.10. Análisis costo - beneficio

El análisis costo–beneficio del Plan de Implementación tiene como finalidad evaluar la razonabilidad económica y el valor agregado institucional derivado de la adopción del modelo propuesto, en relación con el presupuesto estimado para su implementación.

Dado que el alcance del plan se limita a la adopción organizacional y formalización del modelo, los beneficios analizados se enfocan principalmente en beneficios cualitativos y preventivos, asociados a la mejora de la gobernanza, la reducción de riesgos futuros y el fortalecimiento del cumplimiento normativo, más que en retornos financieros directos de cortos plazo.

Los costos identificados se basan en los valores de salarios del personal, así como las dietas de directores miembros de los diferentes Comités y el tiempo requerido para las actividades previstas para el desarrollo del modelo y corresponden principalmente a:

- Uso de recursos humanos internos, destinado a actividades de coordinación, análisis normativo, adecuación organizacional y consolidación documental.
- Costos asociados a la formalización del modelo en formato de manual operativo alienado con políticas internas y marcos normativos aplicables.
- Inversión en la identificación y planificación de capacidades, incluyendo el diseño de esquemas de capacitación y la evaluación de brechas institucionales.
- Costos potenciales de apoyo externo especializado, considerados de manera opcional y preventiva.

Estos costos, estimados de forma referencial, representan una inversión acotada y controlada, especialmente si se compara con los impactos financieros, operativos y reputacionales que podrían derivarse de una gestión inadecuada de proveedores críticos.

Los beneficios derivados del Plan del Implementación se clasifican en cuatro dimensiones principales:

a) Beneficios estratégicos y de gobernanza
    - Fortalecimiento del marco de gobernanza y riesgos de terceros.
    - Claridad en roles, responsabilidades y mecanismos de escalamiento.
    - Mayor alineación entre áreas de riesgos, continuidad, administrativa y negocio.
b) Beneficios regulatorios y de cumplimiento
    - Reducción del riesgo de incumplimiento normativo frente a la Superintendencia de Bancos.

- Disponibilidad de documentación estructurada y verificable para auditorías internas y externas.
- Preparación institucional para escenarios de mayor exigencia regulatoria.

c) Beneficios operativos y de continuidad
   - Mejora en la capacidad de identificar y priorizar proveedores críticos.
   - Base metodológica sólida para evaluar la madurez de continuidad del negocio de terceros.
   - Reducción del riesgo de interrupciones prolongadas por dependencia no gestionada de proveedores.

d) Beneficios económicos indirectos
   - Prevención de pérdidas financieras asociadas a interrupciones de servicios críticos.
   - Reducción de costos futuros por reacciones correctivas, sanciones o reprocesos.
   - Optimización del uso de recursos en fases posteriores de ejecución del modelo.

Desde una perspectiva costo-beneficio, el presupuesto estimado del Plan de Implementación resulta proporcional y justificado, considerando que:

- Los costos se concentran en una fase única de adopción, mientras que los beneficios se extienden a lo largo del tiempo.
- La inversión realizada habilita una gestión preventiva del riesgo, cuyo costo es significativamente menor que el impacto de eventos de continuidad no gestionados.
- El plan genera una base reutilizable y escalable, aplica a distintos proveedores y servicios críticos.

En este sentido, aun cuando muchos de los beneficios no son directamente cuantificables en términos monetarios inmediatos, su impacto sobre la resiliencia operativa, la estabilidad institucional y la sostenibilidad del negocio justifica ampliamente la inversión requerida, sin embargo, de esto y con el objetivo de tener claridad sobre pérdidas evitadas se realiza un análisis cuantitativo de cada nivel:

Tabla 24 Análisis Cuantitativo

Nivel	Actividad	Presupuesto Estimado (USD)	Concepto	Monto Estimado de Pérdida (USD)	Relación B/C
1	Gestión y Gobierno del plan de implementación	2.000	Retrasos por falta de patrocinio institucional	6.000	5
			Reuniones adicionales y redefiniciones de alcance	4.000	
2	Alineación normativa y documental	1.500	Retrabajo documental por observaciones regulatorias internas	2.000	3
			Ajustes tardíos a políticas y procedimientos	2.500	
3	Adecuación organización y de roles	2.000	Duplicidad de funciones y conflictos interáreas	5.000	4
			Reprocesos por roles no definidos	3.000	
4	Preparación de recursos y capacidades	2.000	Capacitación reactiva no planificada	2.500	3
			Contratación urgente de soporte externo	3.500	
5	Gestión de riesgos del plan de implementación	1.500	Incidentes de implementación no anticipados	4.000	4,33
			Interrupciones del cronograma por eventos no gestionados	2.500	
6	Definición del esquema de control y seguimiento	1.000	Falta de detección temprana de desviaciones	4.000	6
			Escalamientos tardíos a comités	2.000	
7	Formalización del modelo para su adopción	2.000	Retrabajo por documentación incompleta o no estandarizada	5.000	4,5
			Atrasos en aprobación institucional	4.000	

-	Apoyo especializado (opcional)	3.000	Falta de alineación a la normativa	6.000	2
	Relación Beneficio / Costo Global				**3,98**

Fuente: Elaboración propia.

El análisis costo-beneficio evidencia que el Plan de Implementación del modelo de gestión de riesgos de proveedores críticos de continuidad del negocio representa una inversión estratégica de alto valor para la institución financiera. Los costos asociados son controlados y previsibles, mientras que los beneficios -especialmente en términos de prevención de riesgos, cumplimiento normativo y fortalecimiento de la gobernanza- superan ampliamente la inversión realizada. En consecuencia, el Plan de Implementación se presenta como económicamente viable, eficiente y justificable. Estos resultados refuerzan la pertinencia del plan como un paso previo indispensable para una futura aplicación efectiva y sostenible del modelo de gestión de riesgos de proveedores críticos de continuidad del negocio.

CONCLUSIONES

1. La investigación parte de la identificación de una problemática recurrente en las instituciones financieras: la gestión de proveedores críticos desde una perspectiva contractual, con una limitada integración de criterios de continuidad del negocio, gobernanza y tratamiento estructurado del riesgo. Esta situación expone a las organizaciones a riesgos significativos de interrupción operativa, incumplimiento normativo y afectación a la resiliencia institucional, especialmente en un entorno regulatorio cada vez más exigente.
2. A lo largo del estudio se evidencia que, si bien existen lineamientos normativos, buenas prácticas internacionales aplicables a la continuidad del negocio y a la gestión de terceros, estos no siempre se encuentran articulados de forma coherente dentro de un modelo operativo que facilita su adopción institucional. El análisis normativo comparativo permite identificar brechas relevantes entre los requerimientos establecidos por marcos como ISO22301 y DORA, y las prácticas observadas en la gestión de proveedores críticos, particularmente en lo relacionado con evaluación de capacidades, seguimiento y gobernanza, lo cual justifica la necesidad de diseñar una metodología que recoja los requerimientos

en un esquema práctico, alineado con la realidad organizacional del sector financiero.

3. A partir del diagnóstico institucional y análisis de brechas, sustentado en la revisión documental, las entrevistas y triangulación metodológica se evidencia la fragmentación de la gestión de proveedores críticos, con un enfoque predominante contractual y operativo que influye en la gestión del riesgo de terceros. Esta aproximación cualitativa evidencia que la ausencia de una metodología formalizada no responde únicamente a falta de normativa institucional, sino a debilidades en la definición de responsabilidades, en los mecanismos de control y en la preparación institucional para su implementación.
4. Como resultado de este análisis, se desarrolla un modelo de gestión de riesgos de proveedores críticos de continuidad del negocio estructurado en las fases secuenciales, alineado con los dominios de ISO22301 e integrado a los principios de gestión de riesgos y control interno promovidos por Basilea. El modelo no se limita a evaluar el cumplimiento de requisitos, sino que permite identificar brechas, priorizar riesgos y orientar la toma de decisiones desde un enfoque preventivo y de mejora continua, fortaleciendo la resiliencia operativa de la institución financiera.
5. Un aspecto clave evidenciado en la investigación es la importancia de la gobernanza como habilitador del modelo. La definición clara de roles, responsabilidades, esquemas RACI y líneas de defensa contribuye a reducir ambigüedades, mejorar la coordinación interáreas y asegurar que las decisiones relacionadas con proveedores críticos se adopten dentro de un marco de control y supervisión adecuado. Esta estructura de gobernanza resulta fundamental para la sostenibilidad del modelo y para mitigar riesgos de implementación futura.
6. En relación con el Plan de Implementación, se concluye que la delimitación de un alcance centrado exclusivamente en la adopción organizacional del modelo es una decisión estratégica adecuada. Esta aproximación permite preparar a la institución financiera antes de la ejecución operativa, reduciendo el riesgo de implementaciones apresuradas, desalineadas o carentes de respaldo institucional, y facilitando una transición controlada hacia la aplicación del modelo.
7. El análisis de riesgos del Plan de Implementación evidencia que incluso las fases preparatorias conllevan riesgos relevantes de carácter operativo, tecnológico, contractual y de cumplimiento. La incorporación de este análisis fortalece el plan

al anticipar posibles desviaciones, establecer responsabilidades claras para su tratamiento y reforzar la coherencia con los principios de gestión de riesgos establecidos en ISO 31000 y Basiela.

8. Desde una perspectiva económica, el análisis costo-beneficio permite confirmar que la inversión requerida para la implementación del modelo es significativamente menor en comparación con los costos potenciales asociados a fallas de gobernanza, reprocesos, sanciones regulatorias o interrupciones operativas derivadas de una gestión deficiente de proveedores críticos. En este sentido, el Plan de Implementación se presenta como una alternativa económicamente viable y estratégicamente justificada.
9. Finalmente, en relación con el objetivo general de la investigación, orientado al diseño de una metodología estructurada para la gestión de riesgos de proveedores críticos de continuidad del negocio en una institución financiera, se concluye que el proyecto permite establecer un modelo integral y sistemático que responde a una problemática real de tercerización y dependencia operativa.

   De este modo, se establece que el objetivo general no solo fue alcanzado, sino que dio lugar a una propuesta aplicable que fortalece la gestión del riesgo operativo y aporta una herramienta concreta para la toma de decisiones en materia de continuidad del negocio.

Las conclusiones presentadas evidencia coherencia entre el problema planteado, los objetivos definidos, la metodología aplicada y los resultados obtenidos, lo que fortalece la consistencia interna de la investigación, los conocimientos adquiridos durante toda la maestría lo cual demuestra la pertinencia académica y práctica del trabajo desarrollado.

RECOMENDACIONES

A partir de los resultados obtenidos y del análisis realizado a lo largo de la investigación, se formulan las siguientes recomendaciones orientadas a fortalecer la gestión de riesgos de proveedores críticos de continuidad del negocio en instituciones financieras:

1. Adoptar la metodología desarrollada como parte estable y obligatoria del Sistema de Gestión de Continuidad del Negocio. Es importante que su aplicación no se limite a un proyecto puntual, sino que forme parte del trabajo cotidiano de la institución. Además, debería revisarse y actualizarse periódicamente, considerando los cambios tecnológicos, las nuevas regulaciones y la evolución de los riesgos asociados a los proveedores. Integrarla en las auditorías internas y en los procesos de planificación fortalecerá su permanencia y garantizará que los resultados sigan siendo útiles con el tiempo.
2. Con el fin de garantizar el cumplimiento de la normativa vigente, se recomienda mantener un monitoreo continuo de las disposiciones de la Superintendencia de Bancos y de los estándares internacionales relacionados con la continuidad del negocio. Cada actualización regulatoria debe reflejarse en los procedimientos internos. También se aconseja mantener evidencia documental clara y trazable de cada evaluación, de modo que la institución esté siempre preparada ante auditorías o revisiones externas.
3. Considerar el Plan de Implementación propuesto como una fase previa a la ejecución del modelo, respetando el alcance definido y los hitos de control establecidos. Esta secuencia permitirá reducir riesgos organizacionales, asegurar la disponibilidad de capacidades internas y generar las condiciones necesarias para una ampliación efectiva y sostenible del modelo.
4. Fortalecer las capacidades del personal involucrado mediante programas de capacitación específicos, orientados a continuidad del negocio, gestión de terceros y evaluación de proveedores críticos. El desarrollo de estas capacidades es clave para asegurar una aplicación homogénea del modelo y evitar desviaciones en los criterios de evaluación.
5. Se recomienda establecer mecanismos formales de coordinación interdepartamental, particularmente entre las áreas de riesgos, tecnología, continuidad del negocio, administrativo y jurídico. Esta coordinación permitirá una gestión integral de los proveedores críticos y reducirá riesgo derivados de enfoques fragmentados o responsabilidades poco claras.
6. Se recomienda incorporar indicadores de desempeño y mecanismos de seguimiento periódico del modelo, incluso antes de su ejecución operativa. El seguimiento temprano permitirá identificar oportunidades de mejora, ajustar criterios y fortalecer el modelo antes de su aplicación plena.

7. Se recomienda que el departamento de auditoría de la entidad financiera, incluya en sus evaluaciones el modelo, de manera tal que se cuente con una evaluación independiente que valide la efectividad, asegure esté alineado con la normativa y así fortalecer la mejora continua.
8. Se recomienda incluir el modelo en la base de documentación institucional, y que cumpla con los requisitos de actualización y mantenimiento periódicos, considerando cambios regulatorios, tecnológicos y del entorno de riesgos, lo cual permitirá garantizar la vigencia del modelo y su capacidad de respuesta frente a nuevos escenarios de continuidad del negocio.
9. Para futuras investigaciones, se recomienda ampliar el alcance del estudio hacia la ejecución y medición del desempeño del modelo, incorporando métricas de madurez y análisis comparativos entre proveedores. Esto permitirá evaluar el impacto del modelo en la resiliencia operativa institucional.
10. Finalmente se recomienda considerar la replicabilidad del modelo en otras instituciones financiera ampliando la cobertura a la regida por la Superintendencia de Economía Popular y Solidario, ajustándolo a sus particularidades operativas y regulatorias. La estructura metodológica desarrollada constituye una base adaptable que puede contribuir al fortalecimiento del sistema financiero en su conjunto.

BIBLIOGRAFÍA

Avila et al. (2021). *Dialnet-EvaluacionDeLaGestionDeProveedoresEnLaUniversidadD-8273825 (1)*.

Avilés et al. (2025). *Auditoría Interna de la gestión operativa del Cloud*. www.auditoresinternos.es

Banco Central. (2025). *BCE - Banco Central del Ecuador*. https://www.bce.fin.ec/

Becerra Acevedo, R., Benavides Muñoz, J. R., Camacho Camacho, H., & Obando, C. J. (2021). *Evolución y modelos de implementación de sistemas de gestión de continuidad del negocio * [Artículos de revisión]*. https://doi.org/10.15332/24631140

Casas en ruinas son hogar de vagabundos - El Comercio. (n.d.). Retrieved August 4, 2025, from https://www.elcomercio.com/actualidad/quito/casas-ruinas-personas-hogar-delincuencia/

Faertes, D. (2015). Reliability of supply chains and business continuity management. *Procedia Computer Science*, *55*, 1400–1409. https://doi.org/10.1016/j.procs.2015.07.130

Gibb, F., & Buchanan, S. (2006). A framework for business continuity management. *International Journal of Information Management*, *26*(2), 128–141. https://doi.org/10.1016/J.IJINFOMGT.2005.11.008

Herbane, B. (2010). Small business research: Time for a crisis-based view. *International Small Business Journal*, *28*(1), 43–64. https://doi.org/10.1177/0266242609350804

ISO 22301. (2019). *ISO 22301:2019 - Business continuity management systems*. https://www.iso.org/standard/75106.html

Liliana Rodríguez-Rojas, Y. (2021a). *Continuidad del negocio: conceptualización y metodologías de evaluación*. *13*. https://doi.org/10.15332/24631140

Liliana Rodríguez-Rojas, Y. (2021b). *Continuidad del negocio: conceptualización y metodologías de evaluación*. *13*. https://doi.org/10.15332/24631140

Loján et al. (2017). *Assessment model business continuity management based on ISO 22301: 2012*.

Ocampo-Murillo, H. F., & Quintero-Garzón, M. L. (2020). Selección de proveedores de insumos críticos en términos de sostenibilidad, a través de la metodología multicriterio,

en una empresa del sector azucarero. *Entramado*, *16*(2), 24–44. https://doi.org/10.18041/1900-3803/entramado.2.6436

Olarte. (2016). *Propuesta metodológica para la evaluación de la madurez del sistema de gestión de continuidad del negocio en el sector financiero bancario colombiano bajo el enfoque de la norma ISO 22301:2012**.

Ordóñez-Granda, E. M., Narváez-Zurita, C. I., & Erazo-Álvarez, J. C. (2020). El sistema financiero en Ecuador: Herramientas innovadoras y nuevos modelos de negocio. *Revista Arbitrada Interdisciplinaria Koinonía*, *5*(10), 195. https://doi.org/10.35381/r.k.v5i10.693

Quituisaca-León, A. K., Ruilova-Morocho, A., & Araujo-Ochoa, G. I. (2021). Continuidad de las MiPymes bajo la norma ISO 22301. Caso Cuenca – Azuay. *593 Digital Publisher CEIT, ISSN-e 2588-0705, Vol. 6, No. 2, 2021, Págs. 30-42*, *6*(2), 30–42. https://doi.org/10.33386/593dp.2021.2.441

Supriadi, L. S. R., & Pheng, L. S. (2017). Business Continuity Management (BCM). *Business Continuity Management in Construction*, 41. https://doi.org/10.1007/978-981-10-5487-7_3

Yánez, J., & Palabras, R. Y. (2012). *Auditorías, Mejora Continua y Normas ISO: factores clave para la evolución de las organizaciones Audits, Continuous Improvement and ISO Standards: key factors in the evolution of organizations*.

Zsidisin y Ritchie. (2008). *Supply Chain Risk: A Handbook of Assessment, Management, and Performance - Google Libros*. https://books.google.com.ec/books?id=nrThOSr_XWoC&printsec=copyright#v=onepage&q&f=false

International Organization for Standardization. (2019). ISO 22301:2019: Societal security — Business continuity management systems — Requirements. https://www.iso.org/standard/75106.html

International Organization for Standardization. (2018). ISO 31000:2018: Risk management — Guidelines. https://www.iso.org/standard/65694.html

International Organization for Standardization. (2014). ISO 27036-1:2014: Information security — Information security for supplier relationships — Part 1: Overview and concepts. https://www.iso.org/standard/44383.html

International Organization for Standardization. (2013). ISO 27001:2013: Information technology — Security techniques — Information security management systems — Requirements. https://www.iso.org/standard/54534.html

International Organization for Standardization. (2013). ISO 27036-3:2013: Information security — Information security for supplier relationships — Part 3: Risk management for supplier relationships. https://www.iso.org/standard/44384.html

European Union. (2022). Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital de las entidades financieras (DORA). Diario Oficial de la Unión Europea. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32022R2554

Business Continuity Institute. (2018). BCI Good Practice Guidelines (2018). Business Continuity Institute.

Basel Committee on Banking Supervision. (2011). Principles for the Sound Management of Operational Risk. Bank for International Settlements.

Basel Committee on Banking Supervision. (2005). Outsourcing in Financial Services. Bank for International Settlements.

ANEXOS

Anexo 1 Marco Conceptual

- **Productos y Servicios Críticos:** Son aquellos productos o servicios que no pueden suspender la operación sin que se afecte de manera sustancial la sobrevivencia del negocio. Se clasifican como productos y servicios críticos en Continuidad del Negocio todos aquellos que posterior a la ejecución del Análisis de Impacto del Negocio obtienen una calificación de 3 (consecuencia moderada) o superior en cualquiera de las dimensiones establecidas, en un horizonte temporal menor a 24 horas de no entregar dicho producto y servicio.

- **BIA:** Análisis de Impacto de Negocio, es una herramienta que permite a las organizaciones entender como un incidente inesperado pude afectar sus operaciones y procesos.

- **Herramienta de Evaluación:** Herramienta usada para la gestión de la evaluación, aquí se carga los cuestionarios de autoevaluación y es el repositorio de los sustentos de las respuestas. De igual manera el equipo evaluador o empresas evaluadoras registrarán las mejoras que surjan de la revisión. El entregable de esta herramienta una vez cumplido el proceso es una calificación de madurez del proveedor en la Gestión de Continuidad del Negocio.

- **Módulo de Continuidad del Negocio (MCN):** Incluido en la herramienta de Gestión de Riesgos, tiene funcionalidades para gestionar de manera eficiente y efectiva la continuidad del negocio de la organización.

- **MTPD:** Es Tiempo Máximo Tolerable de Disrupción. Es definido en el análisis de Impacto del Negocio (BIA).

- **RPO:** El punto en el que la información utilizada por una actividad debe ser restaurada para permitir que la actividad pueda ser reanudada.

- **RTO:** Tiempo objetivo en que los productos, servicios, procesos, subprocesos y los recursos humanos, físicos y tecnológicos deben ser restaurados a su actividad.

- **Subproceso crítico:** Son aquellos subprocesos que soportan de manera directa a los productos y servicios críticos de la Organización, resultantes de la evaluación del BIA. Se clasifican como subprocesos críticos todos aquellos que posterior a la ejecución del

Análisis de Impacto del Negocio obtienen una calificación de 3 (consecuencia moderada) o superior en cualquiera de las dimensiones establecidas, en un horizonte temporal menor a 24 horas de no operar.

- **Proveedor crítico:** Un proveedor crítico es aquel que brinda servicios o productos que sirven de insumo para los subprocesos críticos de la organización. En la fase de asociación de la *Metodología del Análisis de Impacto del Negocio (BIA)* se vinculan los proveedores a los subprocesos críticos y como resultado, se obtienen el listado de proveedores críticos.

- **Proveedor crítico de Continuidad del Negocio:** proveedor cuya falla o ausencia puede interrumpir significativamente las operaciones esenciales de la organización y comprometer seriamente a la empresa.

- **Productos y Servicios de Contingencia:** Corresponden a productos y servicios que pueden funcionar en un esquema operativo/tecnológico cuando el servicio principal está afectada su disponibilidad, evitando la afectación de la sobrevivencia del negocio.

- **Equipo Evaluador:** el equipo evaluador está conformado por personal experto, el cual puede ser interno o externo. Interno, cuando el proveedor evaluado cuenta con la certificación ISO22301 y será necesario verificar la documentación entregada. Externo o empresa evaluadora de continuidad del negocio.

- **Empresas evaluadoras de Continuidad del Negocio (cuarta línea de defensa):** Empresas autorizadas por la Organización que cuentan con un equipo evaluador experto y serán las encargadas de Ejecutar el proceso de evaluación de proveedores bajo los lineamientos establecidos en la presente metodología, así como dar seguimiento al cumplimiento de planes de acción producto de la evaluación de proveedores críticos.

Anexo 2 Metodología para la gestión de riesgos de proveedores críticos

METODOLOGÍA PARA LA GESTIÓN DE RIESGOS DE PROVEEDORES CRÍTICOS DE CONTINUIDAD DEL NEGOCIO

I. INTRODUCCIÓN

La presente Metodología establece los lineamientos para la evaluación, monitoreo y control de riesgos de continuidad del negocio asociados a proveedores críticos de EL BANCO. Su aplicación garantiza la resiliencia operativa de los servicios críticos que dependen de un tercero para su disponibilidad.

II. OBJETIVOS

- Identificar y clasificar los proveedores críticos, basados en los resultados del BIA de los proveedores que son esenciales para el normal desarrollo de las operaciones del Banco, considerando factores como la criticidad de servicios o productos que entregan, el nivel de integración en los subprocesos internos, y finalmente el análisis de las áreas de dueñas de los subprocesos en conjunto con la Gerencia de Riesgo Operativo, así como la dificultad de reemplazo en caso de indisponibilidad de los bienes y servicios prestados.

- Establecer un proceso de análisis de riesgos que cada tercero crítico representa para la continuidad del negocio y cuya gestión estará alineada e integrada con sistema de gestión de continuidad del negocio institucional.

- Establecimiento de estrategias de continuidad del negocio, conforme al nivel de riesgo de los productos y servicios críticos recibidos por los terceros de la organización, alineando los RTO y RPO requeridos en los subprocesos que soportan los terceros con los entregados por estos.

- Determinar los mecanismos para la supervisión constante del desempeño y la situación de los terceros críticos, así como la revisión periódica de los riesgos asociados y la efectividad de los planes de contingencia establecidos. Esto permite adaptar las estrategias a cambios del entorno en la relación con los terceros.

III. BASE NORMATIVA

- **Norma de control para la gestión del Riesgo Operativo**: El literal d, de la Sección III Factores de Riesgo Operativo del Capítulo V, Libro I.- Normas de control para las entidades de los sectores financieros público y privado, determina que, para la administración de Continuidad

del Negocio las entidades controladas deben aplicar los parámetros para la identificación de los procesos críticos, su punto y tiempos de recuperación definidos por el negocio; una vez identificados los procesos críticos, deben determinar las dependencias internas y externas; y, recursos de soporte para estos procesos, incluyendo tecnología, personal, proveedores, y otras partes interesadas.

Asimismo, en la evaluación y selección de estrategias de continuidad por cada proceso crítico que permitan mantener su operatividad, dentro del tiempo objetivo de recuperación definido para cada proceso, se debe tener en cuenta lo siguiente: la seguridad del personal, instalaciones alternas de trabajo, infraestructura alterna de procesamiento, información necesaria para el proceso; proveedores y aplicativos relacionados.

Adicional, conforme el art. 24 de la Sección VII de Servicios Provistos por Terceros, para mantener el control de los servicios provistos por terceros, incluidas las empresas de servicios auxiliares del sistema financiero, las entidades controladas deben implementar un proceso integral para la administración de proveedores de servicios que incluya las actividades previas a la contratación, suscripción, cumplimiento y renovación del contrato; para lo cual, deben cumplir, con lo siguiente:

- Definir mecanismos de gestión de riesgos asociados a los servicios provistos por terceros y que garanticen la gestión de la continuidad del negocio.
- Establecer políticas, procesos y procedimientos que aseguren el control y monitoreo de los servicios contratados, mediante la evaluación, gestión y vigilancia de estos, a fin de garantizar que se cumplan con aspectos de continuidad del negocio.
- Contar con proveedores alternos de los servicios que soportan a los procesos críticos, que tengan la capacidad de prestar el servicio para mitigar el riesgo de dependencia en un solo proveedor; en los casos de proveedor único, se debe solicitar al proveedor planes de continuidad probados actualizados, al menos, anualmente.

- **ISO 22301:2019** – "Seguridad y resiliencia – Sistemas de gestión de continuidad del negocio"
- **ISO 22317:2021** – "Directrices para el análisis de impacto en el negocio (BIA)"
- **DORA (EU 2022/2554)** – "Reglamento sobre resiliencia operativa digital para el sector financiero"
- Normas internas del Banco para gestión de riesgos, continuidad operativa y tercerización.

IV. CONCEPTOS Y DEFINICIONES

- **Productos y Servicios Críticos:** Son aquellos productos o servicios que no pueden suspender la operación sin que se afecte de manera sustancial la sobrevivencia del negocio. Se clasifican como productos y servicios críticos en Continuidad del Negocio todos aquellos que posterior a la ejecución del Análisis de Impacto del Negocio obtienen una calificación de 3 (consecuencia moderada) o superior en cualquiera de las dimensiones establecidas, en un horizonte temporal menor a 24 horas de no entregar dicho producto y servicio.

- **BIA:** Análisis de Impacto de Negocio, es una herramienta que permite a las organizaciones entender como un incidente inesperado pude afectar sus operaciones y procesos.

- **Productos y Servicios de Contingencia:** Corresponden a productos y servicios que pueden funcionar en un esquema operativo/tecnológico cuando el servicio principal está afectada su disponibilidad, evitando la afectación de la sobrevivencia del negocio.

- **Risk Discovery Solution (RDS):** Es una herramienta de gestión de riesgos y de continuidad del negocio.

- **Riskallay:** Es una herramienta de evaluación usada para la autoevaluación, por otro lado, también es el repositorio de los sustentos de las respuestas. El entregable de esta herramienta una vez cumplido el proceso es una calificación de madurez del proveedor en la Gestión de Continuidad del Negocio.

- **Módulo de Continuidad del Negocio (MCN):** Módulo de RDS que tiene funcionalidades para gestionar de manera eficiente y efectiva la continuidad del negocio de la organización.

- **MTPD:** Es Tiempo Máximo Tolerable de Disrupción. Es definido en el análisis de Impacto del Negocio (BIA).

- **RPO:** El punto en el que la información utilizada por una actividad debe ser restaurada para permitir que la actividad pueda ser reanudada.

- **RTO:** Tiempo objetivo en que los productos, servicios, procesos, subprocesos y los recursos humanos, físicos y tecnológicos deben ser restaurados a su actividad.

- **Subproceso crítico:** Son aquellos subprocesos que soportan de manera directa a los productos y servicios críticos de la Organización, resultantes de la evaluación del BIA. Se clasifican como subprocesos críticos todos aquellos que posterior a la ejecución del Análisis de Impacto del Negocio obtienen una calificación de 3 (consecuencia moderada)

o superior en cualquiera de las dimensiones establecidas, en un horizonte temporal menor a 24 horas de no operar.

- **Proveedor crítico:** Un proveedor crítico es aquel que brinda servicios o productos que sirven de insumo para los subprocesos críticos de la organización. En la fase de asociación de la *Metodología del Análisis de Impacto del Negocio (BIA)* se vinculan los proveedores a los subprocesos críticos y como resultado, se obtienen el listado de proveedores críticos.
- **Proveedor crítico de Continuidad del Negocio:** proveedor que:
    - Ejecuta total o parcialmente un subproceso crítico
    - Provee un servicio, infraestructura, sistema o personal sin los cuales el subproceso no podría mantenerse operativo dentro del RTO definido.
    - Tiene una participación directa en el cumplimiento de los SLA´s regulatorios o contractuales del servicio ofertado por la organización.
- **Equipo Evaluador:** el equipo evaluador está conformado por personal experto, el cual puede ser interno o externo. Interno, cuando el proveedor evaluado cuenta con la certificación ISO22301 y será necesario verificar la documentación entregada. Externo o empresa evaluadora de continuidad del negocio.
- **Empresas Evaluadoras de Continuidad del Negocio (cuarta línea de defensa):** Empresas autorizadas por la Organización que cuentan con un equipo evaluador experto y serán las encargadas de Ejecutar el proceso de evaluación de proveedores bajo los lineamientos establecidos en la presente metodología, así como dar seguimiento al cumplimiento de planes de acción producto de la evaluación de proveedores críticos.

V. PRINCIPIOS GENERALES

- **Continuidad del Servicio**: Garantizar la disponibilidad de los productos y servicios críticos ante disrupciones.
- **Gestión del Riesgo**: Evaluar los riesgos inherentes y residuales asociados a proveedores críticos.
- **Cumplimiento Normativo**: Asegurar la conformidad con la Normativa de los Entes de Control, ISO 22301:2019, y DORA.

- **Ciclo de Vida del Proveedor**: Aplicación durante la selección, contratación, monitoreo y renovación de proveedores.
- **Enfoque Basado en Riesgos**: Proporcionalidad en la profundidad de evaluación según criticidad y nivel de exposición.
- **Actualización del Documento**: las siguientes condiciones requieren actualización del documento:
    - Cambios regulatorios
    - Resultados de auditorías
    - Retroalimentación del ciclo de vida de proveedores.

VI. ALCANCE

Desde la contratación de proveedores críticos, el diseño, implementación y mantenimiento del Plan de continuidad del Negocio, hasta el monitoreo a lo largo de la relación contractual con el Banco.

VII. ROLES Y RESPONSABILIDADES

- **GOBIERNO DE GESTIÓN DE TERCEROS CRÍTICOS**

Comité de Administración Integral de Riesgos (CAIR):

o Conocer el cronograma, fases y enfoque metodológico definidos para la evaluación de proveedores críticos.

o Conocer los avances, hallazgos y resultados de la evaluación de continuidad del negocio realizada a proveedores críticos de continuidad del negocio.

o Conocer y validar las decisiones adoptadas por el Comité de Continuidad del Negocio respecto a proveedores críticos de continuidad del negocio con calificación de riesgo alto y extremo, y, de ser necesario, definir acciones adicionales en el marco de la gestión integral de riesgos.

Comité de Continuidad del Negocio:

o Aprobar el cronograma y fases para la evaluación de proveedores críticos de continuidad del negocio.

o Analizar los resultados de las evaluaciones, emitir recomendaciones y definir las acciones correctivas o de mitigación para los proveedores evaluados cuyo resultado implique un riesgo alto o extremo.

o Informar al Comité de Administración Integral de Riesgos sobre las decisiones adoptadas y los planes de acción definidos, para su conocimiento y validación conforme al marco regulatorio.

- **PRIMERA LÍNEA DE DEFENSA:**

Proveedores Críticos de Continuidad del Negocio:

o Cumplir con la evaluación de proveedor crítico de continuidad de negocio, si fue catalogado como tal por el Banco.

o Asistir a las reuniones, talleres y capacitaciones que se programen de manera coordinada entre las partes, dentro de la ejecución de la evaluación de proveedores críticos de continuidad del negocio.

o Entregar la documentación requerida en el proceso de evaluación de terceros críticos y/o contratar la empresa evaluadora en caso de no presentar una certificación o informe de auditoría.

o Implementar las oportunidades de mejora fruto de la evaluación.

Áreas de División Dueñas del Servicio:

o Participar en las reuniones de los talleres de evaluación a las que fuere invitado.

o Proporcionar información referente al tercero/servicio y gestionar el contacto con el mismo.

o Gestionar que los terceros faciliten toda la evidencia documental que demuestre el cumplimiento de los lineamientos y estándares de Continuidad del Negocio en los tiempos establecidos.

- **SEGUNDA LÍNEA DE DEFENSA:**

Gerencia de Riesgo Operativo:

- Definir el cronograma, fases y metodología de evaluación de proveedores críticos de continuidad del negocio, incluyendo su ajuste o aprobación, según corresponda.

- Liderar reuniones de inicio y coordinar el proceso con proveedores, administradores de contrato y empresas evaluadoras**.**

- Validar los resultados de las evaluaciones en la herramienta de gestión, incluyendo documentos de respaldo como certificaciones o auditorías externas.

- Aprobar informes de evaluación.

- Informar al CAIR y al Comité de Continuidad del Negocio sobre el cronograma, avances, resultados y niveles de riesgo identificados.

- Comunicar a las Vicepresidencias dueñas de los subprocesos relacionados con los proveedores críticos los resultados de los proveedores bajo su gestión y asesorar en la toma de decisiones frente a incumplimientos.

- Reportar al Comité de Continuidad del Negocio las desviaciones, riesgos relevantes y planes de mitigación acordados.

- De ser requerido, asesorar a terceros en gestión de continuidad del negocio y absolver consultas técnicas relacionadas con lineamientos aplicables.

- Capacitar a proveedores y evaluadores externos en la metodología y uso de herramientas.

- En coordinación con dichas Vicepresidencias, definir y recomendar planes de acción para proveedores cuyo nivel de riesgo sea alto o extremo.

- Comunicar al Equipo Evaluador Externo cuando el proveedor haya cumplido con los requisitos que le permitan dar inicio a la revisión de cuestionarios y evidencia.

- Realizar reuniones con los proveedores y administradores de contrato para notificar aspectos relevantes de la evaluación y las observaciones generadas.

- **TERCERA LÍNEA DE DEFENSA:**

Auditoría Interna

- Control al cumplimiento de la presente metodología.

- **CUARTA LÍNEA DE DEFENSA:**

Empresa Evaluadora/Auditoría Externa:

- Garantizar la confidencialidad durante todo el proceso.

- Capacitarse en la metodología y uso de la herramienta para gestionar la evaluación.

- Una vez recibida la comunicación que el proveedor ha cumplido los requisitos, analizar y evaluar las respuestas de cuestionarios y documentación soporte, así como establecer plan de remediación, verificar el cumplimiento del plan y emitir observaciones cuando sea necesario, elaborar el informe final donde se muestre el Nivel de Madurez en Gestión de Continuidad de Negocio (BCM) del proveedor crítico.

- Comunicar a la Gerencia de Riesgos los resultados de la evaluación de los terceros, sus planes de mitigación, fechas, responsables con el correspondiente nivel de riesgo obtenido por la evaluación de Continuidad del Negocio.

- Dar seguimiento a las observaciones o planes de acción que se identifique ante los riesgos detectados en la evaluación y respaldar la información de soporte del cumplimiento de los planes de acción.

- Entregar el informe de evaluación de acuerdo, a la Metodología establecida para el efecto.

VIII. METODOLOGIA

8.1. Identificación de proveedores críticos de continuidad del negocio:

Los subprocesos críticos, identificados a partir del Análisis de Impacto al Negocio (BIA), corresponden a aquellos directamente relacionados con los productos y servicios esenciales de la institución, así como a los subprocesos que resultan indispensables para su funcionamiento. Una vez definidos estos subprocesos, las Gerencias de División de la organización deberán llevar a cabo sesiones de trabajo orientadas a vincular los recursos necesarios para su operación, incluyendo dentro de estos a los proveedores externos.

Para ello, y con base en el inventario actualizado de proveedores —cuyo custodio es la Gerencia Administrativa— se deberá realizar un proceso de depuración y clasificación. Esta actividad permitirá establecer una asociación formal entre subprocesos críticos y recursos externos, identificando aquellos proveedores que resultan fundamentales para la continuidad operativa de dichos subprocesos.

Como resultado del BIA, se obtendrá un **listado de proveedores críticos**, el cual deberá ser entregado oficialmente para su incorporación en los procesos de gestión de riesgos y monitoreo continuo de proveedores con al menos la siguiente información:

a. Nombre del Proveedor
b. Servicio Entregado
c. Área de Ejecución
d. RTO del servicio
e. RPO del servicio
f. Subproceso asociado
g. Estrategia operativa
h. Nivel de Criticidad de Riesgo

8.2. Análisis y Priorización:

Con el objetivo de determinar el tipo de evaluación a ejecutar con cada proveedor, entre el área de ejecución o usuaria del servicio y la Gerencia de Riesgo Operativo asignarán en función de los siguientes aspectos, una calificación objetiva de criticidad y riesgo relativo del proveedor:

- RTO requerido del servicio
- Número de Proveedores iguales en el mercado
- Factibilidad de reemplazar el proveedor dentro del RTO
- Nivel de intervención del proveedor en el subproceso crítico
- Número de incidentes reportados
- Cumplimiento del RTO en estos incidentes
- Impacto de los incidentes reportados

Cada aspecto y el rango de este otorgarán una calificación, cuyo resultado final ubicará al proveedor en un nivel de criticidad como lo detalla el Anexo 3, el cual determinará el nivel de evaluación y los requisitos de la misma.

Los niveles de criticidad de riesgo establecidos de acuerdo a esta calificación son:

- Extremo
- Alto
- Moderado
- Bajo

8.3. Evaluación de los Proveedores Críticos

8.3.1. Dominios de Evaluación

Para evaluar el **Nivel de Madurez en Gestión de Continuidad de Negocio** (BCM) del proveedor crítico, se ha determinado siete dominios, veinte y cinco subdominios, cuya evaluación (Anexo 4) se ha plasmado en cuestionarios con ponderación determinada en función del grado de relevancia de cada uno y su contenido.

Los siguientes son los dominios y subdominios considerados en la evaluación:

- Gobierno de Continuidad del Negocio (BCM)
  - Política de Continuidad del Negocio: Alcance y objetivos; Alcance del modelo de gestión de Continuidad (productos y servicios); Roles y responsabilidades; Control y Seguimiento, Directrices, Periodicidad y criterios de actualización
  - Comité de Continuidad del Negocio
  - Presupuesto para la administración de Continuidad del Negocio
- Análisis de impacto del Negocio
  - Identificación de los productos y servicios críticos
  - Identificación de los procesos que soportan los productos y servicios críticos
  - Tiempos de recuperación objetivo y máximo tiempo tolerable de disrupción para cada producto/servicio o proceso crítico
  - Identificación de recursos: Al menos recurso humanos y recursos tecnológicos.
- Plan de Continuidad del Negocio
  - Alcance
  - Objetivos
  - Roles y responsabilidades definidos para las personas y equipos que tienen autoridad durante y después de un incidente
  - Criterios de activación del Plan de Continuidad del Negocio
  - Identificación de principales escenarios de riesgos
  - Estrategias de continuidad que permitan mantener la operación del Negocio antes durante y después de una contingencia.
- Anexos Plan de Continuidad del Negocio
  - Plan de respuesta ante incidentes
  - Plan de recuperación ante desastres
  - Plan de comunicación
  - Personal contingente

- Infraestructura Tecnológica
    - Soluciones Tecnológicas alternas a las principales
    - Certificaciones existentes en los Data Center
- Pruebas del Plan de Continuidad del Negocio
    - Plan de Pruebas del Plan de Continuidad del Negocio, que incluya periodicidad, alcance, detalle de aspectos a probar.
    - Informe de resultados de pruebas con conclusiones y recomendaciones, los cuales deberían ser parte del soporte de información entregada. RTO y RPO alcanzados, así como oportunidades de mejoras identificadas.
- Mantenimiento y Capacitación del Plan de Continuidad
    - Actualización del Modelo de Gestión de Continuidad del Negocio (Planes y procedimientos)
    - Capacitación al personal contingente y no contingente

8.3.2. Evaluación de los proveedores críticos de Continuidad del Negocio

Los proveedores que sean categorizados como críticos desde la perspectiva de Continuidad del Negocio deberán demostrar el cumplimiento de la normativa regulatoria vigente, la normativa interna de la organización y las buenas prácticas aplicables en función del servicio que prestan. Para ello, el área de Riesgo Operativo será responsable de definir los requerimientos específicos que dichos proveedores deben cumplir. Esta área incluirá en su planificación anual los mecanismos y el cronograma destinados a validar el grado de cumplimiento en materia de gestión de continuidad del negocio por parte de los proveedores críticos. La evaluación se desarrollará conforme los criterios dispuestos por la Superintendencia de Bancos en la normativa de control para la gestión del riesgo operativo, específicamente en el apartado de Administración de Continuidad del Negocio del Capítulo V del Libro I, aplicable a entidades de los sectores financieros público y privado, así como a los lineamientos establecidos en el estándar ISO 22301:2019 sobre Sistemas de Gestión de Continuidad del Negocio.

Los requisitos que debe cumplir cada proveedor estarán en relación directa con el nivel de criticidad de riesgo asignado dentro de la fase de análisis y priorización, la siguiente tabla resume:

Criticidad de Riesgo Proveedor	Certificación ISO22301	Informe Auditoria Externa/ Empresa Evaluadora	Autoevaluación	Plan de Continuidad	Cronograma de Pruebas	Informe de pruebas	Revisión y Constatación
Extremo	X	X		X	X	X	X
Alto	X	X		X	X	X	
Moderado		X	X	X	X	X	
Bajo				X	X	X	

Tabla 1: Requisitos por nivel de criticidad de riesgo del proveedor

Los tipos de evaluación son:

1. Evaluación Documental
2. Revisión y Constatación por parte de la organización
3. Autoevaluación
4. Validación e implementación de mejoras
5. Informe final de resultados

1. **Evaluación Documental:** Aplicable a todos los proveedores categorizados como críticos de continuidad del negocio y a todos los niveles de criticidad de riesgo.
   Deberán entregar los siguientes documentos en función del nivel de criticidad de riesgo determinado:
   a. Certificaciones
      Certificaciones de Continuidad del Negocio ISO 22301:2019 (solo para proveedores de Criticidad Extremo y Alto)
      Informe de auditoría externa sobre el cumplimiento de los aspectos relacionados al contenido de los estándares Continuidad del Negocio practicados por personal o empresas independientes con experiencia acreditada en el ramo emitidos en el último año, o contratación de una de las empresas calificadas para realizar la Evaluación de proveedor crítico de Continuidad del Negocio (solo para proveedores de Criticidad Moderado y Bajo)
   b. Plan de Continuidad del Negocio vigente
   c. Cronograma de Pruebas de Continuidad del Negocio para el año en curso
   d. Informe de Pruebas de Continuidad del Negocio del último año, que incluya los resultados obtenidos y los tiempos RTO y RPO alcanzados, los cuales deben estar alienados a los tiempos requeridos por la organización

2. **Revisión y Constatación por parte de la Organización:** Aplicable a los proveedores críticos de continuidad del negocio de criticidad extremo.
   Con el objetivo de verificar que los compromisos contractuales, normativos y operativos asumidos por el proveedor se estén cumpliendo de manera efectiva, donde se hará la revisión documental, inspección técnica, entrevistas y validación con personal clave, revisión de mecanismos de monitoreo y alertas, revisión de incidentes previos.
3. **Autoevaluación:** Aplicable a los proveedores críticos de continuidad del negocio de criticidad moderado.

En función de los dominios y subdominios, se construirán cuestionarios que cada proveedor debe responder, así como agregar la evidencia que sustente sus respuestas. Esta fase se encuentra automatizada con una herramienta, en la cual se podrá programar las fechas de inicio y fin de cada evaluación, agregar los proveedores que forman parte de esta con sus respectivos correos y números de contacto; esta herramienta centralizará la evaluación y la documentación de soporte.

El cuestionario se encuentra en el Anexo 4 y forma parte de esta fase, tiene una ponderación definida para cada pregunta que los conforma, la cual al final del ejercicio determinará una calificación de cumplimiento.

4. **Informe final de resultados:** Aplicable a todos los proveedores.

   Como resultado de la evaluación aplicada se emite un informe el cual contendrá los hallazgos y brechas identificadas, así como las mejoras que deban implementar y emitir el informe final de resultados y el cronograma establecido en acuerdo con el proveedor para el cierre de brechas o la mitigación de las mismas.

   El informe de resultados de la evaluación de los proveedores críticos y su documentación serán custodiados por la Gerencia de Riesgo Operativo.

8.4. Definición de planes de acción y mitigación

Dentro de la evaluación y como resultado de la misma se evidencias brechas de cumplimiento o deficiencias en la gestión de continuidad del negocio por parte de los proveedores, lo cual implica obligatoriamente la necesidad de establecer un plan de remediación, que pude involucrar tareas mínimas o complejas implementaciones, es por esto que en acuerdo entre la institución financiera y el tercero crítico de continuidad del negocio se deberá establecer el plan de acción, definiendo entregables y tiempos de cumplimiento.

Estas revisiones serán parte de la siguiente fase, donde de igual manera deberá reportar el avance a los actores en función de su campo de responsabilidad.

8.5. Monitoreo y Control de Proveedores Críticos de Continuidad del Negocio

El BANCO a través del área de Riesgo Operativo establece, implementa, mantiene y mejora continuamente su Plan de Continuidad del Negocio con el objetivo de mantener un estándar de calidad alto en la dotación de productos y servicios, así como asegurar la permanencia de operaciones en caso de eventos de disrupción tecnológica y operativa en base a Normas Internacionales alineadas al marco regulatorio para entidades financieras en el ámbito nacional.

En lo que respecta a las Estrategias de Continuidad de Negocio conforme el Estándar Internacional para los Sistemas de Continuidad del Negocio ISO 22301:2012, "La organización debe realizar evaluaciones de las capacidades de continuidad del negocio de los proveedores." Adicionalmente, la alta dirección debe revisar el Plan de Continuidad de la organización, a intervalos planificados sobre los resultados de las auditorías y revisiones de este, incluidos los de proveedores y socios clave cuando corresponda, es así que en este sentido y alineado a la gestión de continuidad de negocio organizacional los proveedores críticos de negocio deben ser monitoreados a lo largo de la relación contractual, si bien la principal evaluación constituye la referenciada en el numeral anterior, los períodos inter evaluación requieren de un monitoreo, el cual es posible ejecutarlos a través de indicadores clave de riesgo y/o indicadores clave de desempeño.

Cada año la Gerencia de Riesgo Operativo revisará los indicadores que permitan monitorear al proveedor crítico.

A partir de estos indicadores, sin perjuicio de un nivel de madurez aceptable como resultado de la evaluación de proveedor crítico de continuidad del negocio, si el proveedor durante el monitoreo presenta indicadores que dan muestra de una deficiencia que pueda afectar a la Continuidad de las operaciones de EL BANCO, la Gerencia de Riesgo Operativo comunicará el riesgo de afectación en Continuidad a la Gerencia Administrativa, al área usuaria del servicio contratado y al proveedor. En ese sentido, el área de Riesgo Operativo en ejercicio de sus atribuciones como segunda línea de defensa a partir de estos resultados, recomendará a la Gerencia Administrativa, para que ésta a su vez comunique a las áreas responsables la renovación o no del contrato, en línea con el cumplimiento de los estándares regulatorios y de buenas prácticas para la Continuidad de las Operaciones de EL BANCO.

Los indicadores para esta fase se resumen en la siguiente tabla, su aplicación irá estrechamente relacionado con el nivel de criticidad de riesgo:

TIPO DE INDICADOR	NOMBRE	DESCRIPCIÓN	FORMULA/FUENTE	FRECUENCIA
KPI	Disponibilidad del servicio	Mide el tiempo que el servicio está disponible según lo pactado.	% de disponibilidad mensual = (Tiempo operativo / Tiempo total) × 100	Mensual
	Cumplimiento del SLA	Evalúa si el proveedor cumple los tiempos de respuesta y recuperación.	% de SLA cumplidos / Total SLA definidos	Trimestral
	Resultados de pruebas de continuidad	Tiempos alcanzados de RTO y RPO en pruebas	# de pruebas con tiempos dentro de los límites establecidos/#de pruebas total	Según cronograma

	Tasa de incidentes críticos reportados	Mide la frecuencia de eventos que afectan servicios críticos.	N.º de incidentes críticos / período	Mensual
KRI	Falta de pruebas documentadas	Riesgo por ausencia de evidencia de pruebas BCP/DRP.	No realizar pruebas ≥ 1 vez al año = riesgo crítico	Anual
	Frecuencia de incidentes no reportados a tiempo	Riesgo de opacidad o falta de transparencia operativa.	% de incidentes reportados fuera de plazo	Mensual

8.6. Cumplimiento

Para monitorizar el cumplimiento de los requerimientos aplicables a los proveedores críticos, la Gerencia de Riesgo Operativo de acuerdo a su planificación anual:

- Mantendrá actualizado el listado de proveedores críticos en Continuidad de Negocio de la Organización.
- Aplicará la metodología para la identificación de proveedores críticos en conjunto con las Gerencias de División.
- Consolidará los informes y documentación entregada por las empresas evaluadoras de proveedores críticos de continuidad del negocio.
- Analizará el resultado del informe entregado por la empresa evaluadora, correspondiente a la evaluación de cada proveedor crítico.
- Realizará el seguimiento de la implementación de las oportunidades de mejora a los proveedores críticos de las brechas identificadas en el cumplimiento de los Requerimientos definidos en la metodología en conjunto con las empresas evaluadoras, determinando niveles de severidad y plazos específicos de cumplimiento.
- Se presentará el resumen del informe en el Comité de Administración Integral de Riesgos (CAIR) y en el Comité de Continuidad del Negocio (COCONT).

IX. TRATAMIENTO DEL PROVEEDOR CRÍTICO DE ACUERDO A LOS RESULTADOS DE LA EVALUACIÓN

Una vez finalizado el proceso de evaluación de proveedores críticos de Continuidad del Negocio y habiendo obtenido los resultados del nivel de madurez de cada proveedor en la gestión misma, se procederá a clasificar los resultados y establecer planes de acción y seguimiento con el propósito de mitigar el nivel de riesgo identificado, así como el grado de exposición y el impacto potencial que una interrupción del servicio podría generar sobre la organización.

La clasificación de riesgo y las acciones correspondientes se establecerán según el siguiente esquema en función de la calificación alcanzada dentro de la evaluación sobre el total de puntos:

Calificación	Rango
Insuficiente	**(0%-40%)**
Gestionado	**(>40%-60%)**
Desarrollado	**(>60%-80%)**
Satisfactorio	**(>80%-100%)**

Tabla 2: Calificación del proveedor en función del rango alcanzado en la evaluación

9.1. Calificación Insuficiente: Cumplimiento entre el 0% y 40%

Se refiere a aquellos proveedores en los que se han identificado deficiencias críticas que comprometen de forma directa e inmediata la continuidad del negocio. Este nivel requiere una atención prioritaria y correctiva en el menor tiempo posible.

Acciones:

- Requiere un plan de acción correctivo obligatorio con plazos no mayores a 3 meses.
- Evaluar la posibilidad de implementar controles compensatorios internos mientras el proveedor fortalece su gestión.
- Reconsiderar la criticidad o reemplazo del proveedor si no mejora.
- El avance será objeto de seguimiento intensivo y deberá ser reportado a la alta dirección o comité de riesgos.

9.2. Calificación Gestionado: Cumplimiento mayor a 40% o hasta el 60%

Corresponde a proveedores que presentan brechas significativas en su gestión de continuidad del negocio, pero cuyo nivel de exposición no compromete de forma inmediata la operación, aunque sí requiere atención y mejora en un horizonte de corto plazo.

Acciones:

- Exigir un **plan de mejora estructurado** con seguimiento hasta en 6 meses.

- La organización deberá realizar un seguimiento trimestral, con validación de evidencias de avance y cumplimiento.
- Priorizar la alineación con los RTO/RPO definidos en el BIA.
- Mantener controles compensatorios si aplica.
- Se podrán establecer medidas adicionales o cláusulas contractuales de refuerzo si así lo amerita la criticidad del servicio.

9.3. Calificación Desarrollado: Cumplimiento mayor al 60% y hasta el 80%

En este rango se encuentran los proveedores que requieren de mayor madurez en sus procesos o ajustes de acuerdo a las mejores prácticas.

Acciones:

- Recomendaciones de mejora continua con revisión anual, a menos que se presenten incidentes en cuyo caso la revisión será semestral.
- Reevaluación anual o según criticidad, considerando el número de incidentes que se presenten.
- Solicitar evidencias de pruebas y revisión de lecciones aprendidas.

9.4. Calificación Satisfactoria: Cumplimiento mayor al 80%

Cuando el proveedor cumple plenamente con los requisitos de continuidad del negocio establecidos por la organización y no se han identificado observaciones relevantes.

Acciones:

- No se requieren acciones correctivas.
- El proveedor será reevaluado en el siguiente ciclo definido, o si se producen cambios en su operación, contrato o criticidad.

De esta manera se puede realizar una gestión diferenciada a los proveedores según su nivel de exposición al riesgo y priorizar los recursos de seguimiento y control sobre aquellos casos que verdaderamente puedan poner en riesgo la operación de la organización, así como tomar medidas compensatorias.

Anexo 3 Calificación de criticidad de riesgo de proveedores críticos de continuidad del negocio

CALIFICACÓN DEL RIESGO DE PROVEEDORES CRITICOS DE CONTINUIDAD DEL NEGOCIO

$$Criticidad\ Total = i=1 \sum n (Puntaje i \times Ponderacion i)$$

CRITERIO	RANGO	CALIFICACIÓN
RTO del Servicio	Menor a 1 horas	5
	Entre 1 y 3 horas	3
	Mayor a 3 horas	1
Número de proveedores iguales en el mercado	Único	5
	2 a 4	3
	Más de 5	1
Puede ser reemplazado el proveedor dentro del RTO	No	5
	Si	1
Nivel de intervención del proveedor en el subproceso crítico	Total	5
	Parcial	3
	Marginal	1
Número de incidentes reportados en el mes	Más de 2	5
	2	3
	Menos de 2	1
Incidentes cumplen RTO	Menos del 80%	5
	99% - 80%	3
	Todos	1
Impacto de los incidentes	Alto	5
	Medio	3
	Bajo	1

Criticidad	Puntaje
Extremo	35-24
Alto	23-19
Moderado	18-15
Bajo	14 o menos

Anexo 3 Cuestionario de evaluación de proveedores críticos de continuidad del negocio

Dominio	Meta	Resultados	Subdominio	Meta	Resultados	Preguntas	Respuestas y Evidencias	Meta Pregunta	Resultados Pregunta	Tipo de Respuesta	Documentacion	Comentarios
Gobierno de Continuidad del Negocio (BCM)	**12%**	**12%**	**Política de Continuidad del Negocio**	**8,5%**	**8,5%**	El Proveedor debe tener una Política de Continuidad del Negocio documentada y aprobada.	**SI**	**1%**	**1,00%**	SI o NO	Si (Obligatoria)	Opcional
						El Proveedor debe tener en su Política la definición de Continuidad de Negocio alineada con la definición de la IFI.	**SI**	**1%**	**1,00%**	SI o NO	No	Opcional
						Los objetivos definidos en la Política de Continuidad del Proveedor deben estar alineados al objetivo de la IFI.	**SI**	**1%**	**1,00%**	SI o NO	No	Opcional
						En el alcance de la Política debe existir un apartado donde se evidencia el compromiso de la Alta Dirección para crear, mantener y monitorear un efectivo Sistema de Gestión de Continuidad del Negocio y a dotar de recursos humanos, tecnológicos, de infraestructura y recursos financieros para asegurar el correcto desempeño del Sistema de Gestión de Continuidad del Negocio.	**SI**	**1%**	**1,00%**	SI o NO	No	Opcional

						La Política debe contar con un apartado en el cual se describa la relación con las partes interesadas (Stakeholders), en la IFI esté identificada como cliente. (Ejm: Mapa de Actores)	**SI**	**1%**	**1,00%**	SI o NO	No	Opcional
						La Política debe determinar lineamientos de Medición del Sistema de Gestión de Continuidad del Negocio (SGCN) que permita monitorear el desempeño del SGCN y tomar acciones reactivas y preventivas frente a variaciones relevantes en el mismo. (Ejm: Indicadores de Desempeño, Cumplimiento, Disponibilidad, Riesgos)	**SI**	**1%**	**1,00%**	SI o NO	No	Opcional
						La Política debe contar con un apartado en el cual se expongan los lineamientos de capacitación a los gestores de Continuidad del Negocio y campañas de sensibilización del Sistema de Continuidad del Negocio a toda la Organización.	**SI**	**0,5%**	**0,50%**	SI o NO	No	Opcional
						La Política debe incluir las directrices de un Sistema de comunicación sobre las actividades a realizarse en la gestión de continuidad del negocio en caso de la existencia de eventos de Continuidad del Negocio.	**SI**	**1%**	**1,00%**	SI o NO	No	Opcional
						La política debe definir la periodicidad y los criterios de actualización de los documentos (Política El BIA, Pruebas, Capacitaciones) para la Gestión de Continuidad del Negocio. Debe evidenciarse una frecuencia de actualización, así como también	**SI**	**1%**	**1,00%**	SI o NO	No	Opcional

						puede estar sujeta a modificaciones según las siguientes causas: materialización de nuevos riesgos, cambios de condiciones de mercado, nuevos productos y servicios, cambios en productos y servicios críticos y/o cambios en requerimientos regulatorios, etc.						
			Comité de Continuidad del Negocio	**2,5%**	**2,5%**	La empresa evaluada debe tener un encargado de la Gestión del Sistema de Continuidad del Negocio y/o un equipo de aplicación en función del tamaño o naturaleza del negocio de la empresa evaluada. (Ejm: Líder o Responsable de Continuidad del Negocio)	**SI**	**0,5%**	**0,50%**	SI o NO	No	Opcional
						El proveedor evaluado debe contar con un Comité o Colectivo de Continuidad del Negocio en el que participen miembros de la Alta Gerencia en sus decisiones	**SI**	**1%**	**1,00%**	SI o NO	No	Opcional
						El Comité o Colectivo de Continuidad debe disponer de un reglamento, metodología o ficha que determine los miembros, roles y responsabilidades, frecuencia y criterios de sesión (Propósito y Mandato, Funciones y Responsabilidades del Comité, Conformación, Periodicidad de Reuniones, Actas de Sesión, Acceso a la información a miembros de Comité, Gestión de contratación de servicios, Gestión de conflicto de intereses, Transferencia de Conocimiento, Obligatoriedad de Revisión y Aprobación.)	**SI**	**1%**	**1,00%**	SI o NO	Si (Obligatoria)	Opcional

			Presupuesto	**1%**	**1%**	El Sistema de Continuidad del Negocio debe contar con un Presupuesto Anual para su Gestión.	**SI**	**1%**	**1,00%**	SI o NO	No	Opcional
Análisis de impacto del Negocio	**20%**	**20%**	**Identificación de los P/S**	**5%**	**5%**	El proveedor evaluado debe contar con una metodología actualizada y aprobada para identificar productos y servicios críticos, basado en las recomendaciones ISO 22301:2019, ISO 22317 u otro marco de referencia aplicable para el Análisis de Impacto del Negocio (BIA).	**SI**	**2,50%**	**2,50%**	SI o NO	Si (Opcional)	Opcional
						La entidad evaluada debe identificar los Productos y Servicios críticos de la empresa evaluada y dentro de estos, deben estar los productos y servicios críticos que prestan a la IFI.	**SI**	**2,50%**	**2,50%**	SI o NO	Si (Opcional)	No
			Procesos que soportan los P/S	**5%**	**5%**	El proveedor evaluado debe contar con una metodología actualizada y aprobada para identificar los procesos o subprocesos que soportan los productos y servicios críticos, basado en las recomendaciones ISO 22301, ISO 22317 u otro marco de referencia aplicable para el Análisis de Impacto del Negocio (BIA).	**SI**	**2,50%**	**2,50%**	SI o NO	Si (Opcional)	Opcional
						El Análisis de Impacto del Negocio debe contar con un inventario de procesos o subprocesos críticos que soporten a los Productos y Servicios Críticos otorgados a la IFI.	**SI**	**2,50%**	**2,50%**	SI o NO	Si (Opcional)	Opcional

							SI	**2,00%**	**2,00%**	SI o NO	Si (Opcional)	No
			RTO, RPO, MTPD	**5%**	**5%**	La empresa evaluada debe contar con métricas RTO y RPO por cada producto y servicio crítico otorgado a LA IFI, cuyos resultados deben constar en la pestaña Productos y Servicios.	**SI**	**1,00%**	**1,00%**	SI o NO	Si (Opcional)	No
						¿Se ha mantenido una reunión entre los responsables de Continuidad del Negocio de la IFI y el proveedor crítico con el objetivo de integrar el RTO y RPO de los servicios críticos otorgados a la IFI?	**SI**	**1,00%**	**1,00%**	SI o NO	Si (Opcional)	No
						¿La empresa evaluada cuenta con una aprobación formal por correo electrónico, contrato, acuerdo de nivel de servicio (ANS), u otro medio documental respecto a la aceptación de las métricas de Continuidad del Negocio por parte de la IFI?	**SI**	**1,00%**	**1,00%**	SI o NO	Si (Obligatoria)	Obligatorios
			Identificación de Recursos Críticos	**5%**	**5%**	La empresa evaluada debe contar con el inventario de los cargos críticos que soportan a cada producto y servicio crítico otorgado a la IFI.	**SI**	**1,00%**	**1,00%**	SI o NO	Si (Opcional)	Opcional
						La empresa evaluada debe contar con el inventario de las aplicaciones tecnológicas críticas que soporta a los productos y servicios críticos otorgados a la IFI.	**SI**	**1,00%**	**1,00%**	SI o NO	Si (Opcional)	Opcional

						La empresa evaluada debe contar con el inventario de activos de información físico y digital que soporta a los productos y servicios críticos otorgados a la IFI.	**SI**	**1,00%**	**1,00%**	SI o NO	Si (Opcional)	Opcional
						La empresa evaluada debe contar con el inventario de proveedores críticos que brinda servicios de manera directa a los productos y servicios críticos otorgados a la IFI.	**SI**	**1,00%**	**1,00%**	SI o NO	Si (Opcional)	Opcional
						La empresa evaluada debe contar con planes de continuidad de negocio para los servicios críticos provistos por proveedores alternos	**SI**	**1,00%**	**1,00%**	SI o NO	Si (Obligatoria)	Opcional
Plan de Continuidad del Negocio	**18%**	**18%**	**Propósito y alcance**	**1%**	**1%**	El Plan de Continuidad del Negocio debe incluir el detalle del propósito y alcance alineados a la IFI.	**SI**	**1%**	**1,00%**	SI o NO	No	Opcional
			Objetivos	**1%**	**1%**	El Plan de Continuidad del Negocio debe contener objetivos alineados a lo documento en el Plan de Continuidad de Negocio de la IFI.	**SI**	**1%**	**1,00%**	SI o NO	No	Opcional
			Roles y responsabilidades	**1%**	**1%**	El Plan de Continuidad del Negocio debe detallar los roles y responsabilidades previo, durante y posterior a un evento de	**SI**	**1%**	**1,00%**	SI o NO	No	Opcional

						contingencia/continuidad alineados a la IFI.						
			Criterios de activación del Plan	**5%**	**5%**	Se deben evidenciar criterios de activación del Plan de Continuidad del Negocio conforme al tiempo de no disponibilidad y/o impacto financiero y/o reputacional, como mínimo en el que se encuentren mapeados los productos y servicios que se otorga a la IFI. (Ejm: No operación de Producto crítico que afecte a más de 3000 usuarios por 6 horas.)	**SI**	**5%**	**5,00%**	SI o NO	No	Opcional
			Identificación escenarios	**5%**	**5%**	Debe existir la identificación de amenazas, riesgos o escenarios asociados a los recursos críticos identificados en el Análisis de impacto en el negocio (BIA), como mínimo en el que se encuentren los productos y servicios que se otorga a la IFI.	**SI**	**5%**	**5,00%**	SI o NO	No	Opcional
			Estrategias de Continuidad	**5%**	**5%**	Se debe disponer de un documento que evidencie las estrategias de continuidad según las amenazas y riesgos identificados, como mínimo de aquellos productos y servicios entregados a la IFI (Ejm: Estrategias de Diversificación, Replicación, Recursos en Espera o Adquisición posterior a un incidente.)	**SI**	**5%**	**5,00%**	SI o NO	Si (Obligatoria)	Opcional
Anexos del Plan de Continuidad del Negocio	**20%**	**20%**	**Plan de respuesta Incidentes**	**5%**	**5%**	El proveedor debe contar con un procedimiento que describa las actividades para recuperar los recursos críticos que soporten como mínimo a los productos y servicios de la IFI.	**SI**	**5%**	**5,00%**	SI o NO	Si (Obligatoria)	Opcional

			Plan de recuperación desastres (DRP) Operativo y Tecnológico del Core Bancario	**5%**	**5%**	El proveedor debe contar con un plan de recuperación de desastres, en los que como mínimo deben constar los productos y servicios críticos otorgados a la IFI.	**SI**	**5%**	**5,00%**	SI o NO	Si (Opcional)	Opcional
			Plan de comunicación	**5%**	**5%**	El proveedor debe contar con un Plan de Comunicación interna en caso de la materialización de un evento que afecte la Continuidad del Negocio de la Organización.	**SI**	**2,5%**	**2,50%**	SI o NO	Si (Opcional)	Opcional
						El Plan de Comunicación mencionado en el apartado anterior debe incluir la estructura y los canales de comunicación principales y alternos a llevarse a cabo con la IFI.	**SI**	**2,5%**	**2,50%**	Con Opciones	No	Opcional
			Personal contingente	**5%**	**5%**	El proveedor debe contar con la identificación del personal primario, así como la información de contacto y los medios que faciliten la comunicación en caso de un evento o incidente disruptivo con la IFI.	**SI**	**1,7%**	**1,67%**	SI o NO	No	Opcional
						El proveedor debe identificar el personal secundario o backups que suplan al personal primario en caso de incidente disruptivo, así como la información de contacto y los medios que faciliten la comunicación en caso de un evento disruptivo con la IFI.	**SI**	**1,7%**	**1,67%**	SI o NO	No	Opcional
						El proveedor debe comunicar al equipo de Continuidad del Negocio y Operativo de la IFI el personal primario y secundario a actuar en caso de evento contingente.	**SI**	**1,7%**	**1,66%**	SI o NO	No	Opcional

Infraestructura Tecnológica	**10%**	**10%**	**Soluciones de infraestructura instalados de los Data Center Alterno**	**8%**	**8%**	El proveedor debe contar con soluciones de estrategias de continuidad alternas en la infraestructura tecnológica crítica para los Productos o Servicios Otorgados a la IFI en caso de que aplique en su infraestructura. (Ejm: Esquemas De Infraestructura como Alta Disponibilidad (Activo-Activo o Activo Pasivo), Componentes Redundantes, Replicación en Línea y/o Sitio Alterno).	**SI**	**4,0%**	**4,00%**	SI o NO	No	Opcional
						Detallar las soluciones de infraestructura implementadas para cada Producto o Servicio Crítico Otorgado a la IFI (En caso de aplicar).	**SI**	**4,0%**	**4,00%**	Con Opciones	Si (Opcional)	Obligatorios
			Certificaciones existen en los Data Center	**2%**	**2%**	La empresa debe contar con algún tipo de certificación (Ejm: TIER III) o homologables en el Data Center que garanticen criterios de calidad en el funcionamiento del Data Center Principal y Alterno.	**SI**	**2%**	**2,00%**	SI o NO	Si (Obligatoria)	Opcional
Pruebas del Plan de Continuidad del Negocio	**12%**	**12%**	**Plan de pruebas del Plan de Continuidad**	**4%**	**4%**	El proveedor debe contar con un Plan de Pruebas Anual en el cual se calendarice las pruebas operativas y tecnológicas de la Continuidad del Negocio de la Organización, en el que se consideren los recursos de las productos y servicios críticos otorgados a la IFI.	**SI**	**4%**	**4,00%**	SI o NO	Si (Opcional)	Opcional
			Resultados de las Pruebas	**4%**	**4%**	El proveedor debe contar con un documento o informe en el que se recopilen los resultados de las Pruebas del Plan de Continuidad del Negocio, incidentes y oportunidades de mejora, que incluyan los recursos de los	**SI**	**4%**	**4,00%**	SI o NO	Si (Opcional)	Opcional

						productos y servicios críticos otorgados a la IFI.						
			Cumplimiento de Métricas	**4%**	**4%**	¿El proveedor posterior a la ejecución de las pruebas valida que el tiempo de recuperación documentado en el informe es menor o igual a lo acordado con la IFI?	**SI**	**4%**	**4,00%**	SI o NO	Si (Obligatoria)	Obligatorios
Mantenimiento y Capacitación del Plan de Continuidad	**8%**	**8%**	**Actualización del Plan de Continuidad**	**4%**	**4%**	La empresa evaluada debe evidenciar la actualización de los documentos de la Gestión de Continuidad del Negocio conforme la frecuencia establecida en la Política. (BIA, Evaluación de Riesgos, BCP, Anexos, etc)	**SI**	**4%**	**4,00%**	SI o NO	Si (Opcional)	Opcional
			Capacitación al personal	**4%**	**4%**	El proveedor debe presentar un esquema de capacitación en Continuidad del Negocio.	**SI**	**4%**	**4,00%**	SI o NO	Si (Obligatoria)	Opcional