

Doctorado en Informática

Análisis de la ciberseguridad de infraestructura cloud, para el sistema bancario de la Republica Dominicana.

Eury José González Fernández

Director: Dra. Rosa Gabriela Camero Berrones

San Francisco de Macorís, Republica Dominicana, Enero 2026

Resumen

Este estudio tuvo como objetivo proponer un modelo de gestión de ciberseguridad de infraestructura cloud para el sistema bancario de la República Dominicana, orientado a fortalecer la gestión del riesgo cibernético. Se empleó un enfoque descriptivo-propositivo, mediante revisión documental de estándares internacionales (ISO/IEC 27001, ISO/IEC 27017, NIST CSF 2.0) y cuestionarios estructurados aplicados a una muestra no probabilística por conveniencia y cuotas de 30 entidades bancarias, seleccionadas de una población de 49 entidades autorizadas y estratificadas por tamaño y región. El modelo se validó mediante un instrumento aplicado a un panel de expertos en ciberseguridad, que evaluó relevancia, aplicabilidad, efectividad percibida y coherencia. Los resultados evidenciaron un nivel intermedio de madurez en la adopción de cloud en la banca dominicana, con fortalezas en gobernanza, identificación de riesgos y recuperación, y debilidades en protección y detección, lo que reflejó una postura predominantemente reactiva. A partir de estos hallazgos se diseñó el modelo PROBAN (Protección Bancaria en la Nube), estructurado en ocho pilares, cuya validación por expertos arrojó un índice de validez de contenido de 0.98, clasificado como excelente. Esta validación correspondió al juicio experto sobre el diseño del modelo, sin constituir una comprobación empírica de su efectividad, dado que no se realizó aplicación piloto ni mediciones antes y después. Se recomienda a las entidades bancarias fortalecer los controles nativos de la nube y la gestión de identidades, y se sugiere para futuras investigaciones evaluar la efectividad del modelo mediante estudios longitudinales con aplicación piloto.

Palabras clave: ciberseguridad, infraestructura cloud, sector bancario, gestión de riesgo cibernético, modelo PROBAN, República Dominicana.

Abstract

This study aimed to propose a cloud infrastructure cybersecurity management model for the banking system of the Dominican Republic, oriented toward strengthening cyber risk management. A descriptive-propositional approach was used, through documentary review of international standards (ISO/IEC 27001, ISO/IEC 27017, NIST CSF 2.0) and structured questionnaires applied to a non-probabilistic convenience and quota sample of 30 banking entities, selected from a population of 49 authorized entities and stratified by size and region. The model was validated through an instrument applied to a panel of cybersecurity experts, who assessed relevance, applicability, perceived effectiveness, and coherence. Results showed an intermediate maturity level in cloud adoption within Dominican banking, with strengths in governance, risk identification, and recovery, and weaknesses in protection and detection, reflecting a predominantly reactive posture. Based on these findings, the PROBAN (Protección Bancaria en la Nube) model was designed, structured around eight pillars, whose expert validation yielded a content validity index of 0.98, classified as excellent. This validation corresponded to expert judgment on the model's design and does not constitute empirical proof of its effectiveness, since no pilot application or before-and-after measurements were carried out. Banking entities are recommended to strengthen native cloud controls and identity management, and future research is encouraged to assess the model's effectiveness through longitudinal studies with pilot application.

Keywords: cybersecurity, cloud infrastructure, banking sector, cyber risk management, PROBAN model, Dominican Republic.

Dedicatorias

Dedico este trabajo, en primer lugar, a Dios, el fundamento de toda sabiduría y propósito, cuya guía constante me permitió mantener el esfuerzo, la disciplina y la convicción necesarias para completar esta etapa académica. A mi esposa, Marioli Antigua, por su dedicación, comprensión y apoyo constante a lo largo de este camino, y a mis hijos, quienes son la inspiración diaria que impulsa mi crecimiento personal y profesional. A mis padres, Pedro González y Betania Fernández, por su apoyo incondicional, su ejemplo de perseverancia y su confianza en este proyecto, incluso en los momentos de mayor exigencia y desafío. Esta investigación representa el resultado de un proceso de formación riguroso, aprendizaje continuo y un compromiso con el fortalecimiento del conocimiento y la práctica de la ciberseguridad en el sector financiero.

Agradecimientos

Dios me ha dado la fuerza, perseverancia y serenidad para completar esta educación doctoral. A mi esposa Marioli Antigua y a mis hijos, les agradezco por su paciencia, comprensión y apoyo inquebrantable; su presencia fue la fuerza motriz esencial para enfrentar las exigencias de este viaje. Agradezco al Sr. Luis Valdez por haber puesto fe en el trabajo que realicé y por brindarme apoyo institucional y acompañamiento, los factores que hicieron posibles los objetivos definidos por esta investigación. Reconozco particularmente a la Asociación Duarte, ya que el respaldo financiero fue un componente esencial para la finalización de este curso, mostrando un firme compromiso de la organización tanto con la academia como con el campo. A la Universidad UNADE por el apoyo académico y los recursos institucionales en la promoción de la excelencia y el rigor científico. Asimismo, reconozco para este trabajo la contribución de la Dra. Rosa Gabriela Camero Berrones, tutora de esta investigación, por la crucial orientación metodológica y aportes críticos, que fortalecieron los fundamentos científicos de este documento. Finalmente, me gustaría agradecer a todos aquellos que, directa o indirectamente, nos apoyaron y alentaron a completar este objetivo académico.

Contenido

Resumen ii

Abstract iii

Dedicatorias iv

Agradecimientos v

Lista de tablas y figuras vii

Introducción 1

Capítulo 1. 6

1.1 Problema 6

1.2 Justificación 9

1.3 Objetivo 11

1.4 Hipótesis o supuesto hipotético 12

1.5 Variables o Categoría de análisis 12

Capítulo 2. 14

2.1 Estado del Arte 14

2.2 Marco teórico -conceptual 17

Capítulo 3. 34

3.1 Propuesta metodológica 34

3.2 Población y muestra 35

3.3 Instrumento, método de validación y descripción procedimiento de aplicación 42

3.4 Matriz de Variables 45

3.5 Metodología por Objetivos 47

Capítulo 4. 50

4.1 Resultados por Objetivo 50

4.2 Análisis 76

4.3 Discusión 93

Capítulo 5. 102

5.1 Conclusiones y recomendaciones 102

5.2 Limitantes y desafíos 104

REFERENCIAS BIBLIOGRÁFICAS 106

APÉNDICE 113

Apéndice A. Instrumento de Recolección de Datos 113

Apéndice B. Mapeo Instrumento con Modelo Propuesto 123

Apéndice C. Instrumento de Validación Aplicado a los Expertos 127

Lista de tablas y figuras

Tablas

Tabla 1 *Relación marco teórico - PROBAN* 31

Tabla 2 *Distribución de muestra por región y tamaño* 38

Tabla 3 *Resultado de muestra estimada por región* 39

Tabla 4 *Resultado de muestra por región y tamaño de organización* 39

Tabla 5 *Muestra final respecto a la Población* 40

Tabla 6 *Matriz de Variables* 45

Tabla 7 *Resultados por Objetivo 1* 53

Tabla 8 *Correlación Controles Conceptuales e implementación técnica* 63

Tabla 9 *Perfil de los expertos consultados* 69

Tabla 10 *Estadísticas descriptivas de la validación por dimensión* 70

Tabla 11 *Escala de interpretación del índice global del modelo* 71

Tabla 12 *Índice de validez de contenido por dimensión* 71

Tabla 13 *Escala de interpretación del índice de validez de contenido* 72

Tabla 14 *Estimación de costos de implementación por pilar (Inversión inicial)* 73

Tabla 15 *Costos operativos anuales (recurrentes, a partir del año 2)* 75

Figuras

Figura 1 *Diagrama de procesos* 49

Figura 2 *Nivel de madurez NIST de las entidades bancarias* 52

Figura 3 *Flujo de Control IAM* 60

Figura 4 *Flujo técnico del token de acceso* 61

Figura 5 *Modelo de Protección Bancaria en la Nube (PROBAN)* 68

Figura 6 *Utilización de servicios en la nube.* 77

Figura 7 *Infraestructura tecnológica en la nube* 78

Figura 8 *Barreras de adopción de la nube en las entidades bancarias* 79

Figura 9 *Desafíos que enfrenta la organización en la integración de la nube*..... 80

Figura 10 *Proveedores IaaS utilizados por las entidades bancarias* 81

Figura 11 *Medidas y controles utilizados por entidades bancarias para gestionar la nube*..... 83

Figura 12 *Estrategia de implementación de nube.* 84

Figura 13 *Principales prioridades de seguridad en la nube.* 85

Figura 14 *Principales desafíos en la gestión de operaciones de seguridad en la nube.* 86

Figura 15 *Escasez de personal calificado en el sector financiero.*..... 87

Figura 16 *Percepción del riesgo en entornos locales versus entornos de nube.* 88

Figura 17 *Utilidad plataforma de seguridad en la nube.* 89

Figura 18 *Herramientas de seguridad para incidentes y continuidad del servicio*..... 90

Figura 19 *Plan de recuperación ante desastres tecnológicos.* 91

Figura 20 *Nivel de madurez de las entidades bancarias.* 92

Introducción

La implementación de infraestructuras en la nube se ha convertido en un pilar fundamental para la productividad operativa, el crecimiento tecnológico y la innovación en el sector financiero (Zárate Urgell et al., 2023). Sin embargo, es esta progresión la que expone al mercado a amenazas cibernéticas que pueden manifestarse como problemas reales de seguridad, continuidad operativa y confianza en el sistema financiero. El sector bancario de la República Dominicana avanza mediante procesos de modernización gradual de TI para migrar a la nube, con énfasis en mejorar los mecanismos de protección de la información y la gestión del riesgo cibernético. En este contexto, la ciberseguridad es crucial en términos técnicos, organizativos y regulatorios, ya que impacta en la estabilidad institucional y la confianza del cliente en el sistema financiero. Diversos organismos internacionales han documentado esta problemática. La Agencia de la Unión Europea para la Ciberseguridad (ENISA, 2023) señala que los entornos multi-nube presentan problemas particulares de gestión de identidad, protección de datos en tránsito y visibilidad de acceso en redes distribuidas, que requieren gobernanza sólida y monitoreo independiente. Por su parte, el NIST (2023), en la actualización de su Marco de Ciberseguridad 2.0, amplió el componente de gobernanza para atender la rendición de cuentas, la protección de datos y la gestión de riesgos de terceros, señalando que este enfoque resulta particularmente relevante en industrias de alto riesgo como la banca. A nivel regional, el Banco Interamericano de Desarrollo y la Organización de los Estados Americanos (Porrúa et al., 2025) han documentado el avance —aunque desigual— de la madurez en ciberseguridad en América Latina y el Caribe, identificando a las instituciones financieras como uno de los blancos principales del incremento de ciberataques en la región (OEA, 2018). Estudios de caso en el sector financiero latinoamericano refuerzan esta

preocupación: Zárate Urgell et al. (2023) analizaron la ciberseguridad del sector financiero mexicano y evidenciaron la necesidad de migrar hacia metodologías como Zero Trust ante la insuficiencia de los modelos perimetrales tradicionales frente a amenazas cada vez más sofisticadas. Dado que la dependencia de las soluciones en la nube ha crecido, la superficie de ataque de las instituciones bancarias dominicanas se ha expandido y ha estado más expuesta a amenazas cada vez más sofisticadas, que incluyen acceso no autorizado, exfiltración de datos y ataques de denegación de servicio. Estos sucesos pueden plantear problemas para la confidencialidad, integridad y disponibilidad de la información, junto con la estabilidad institucional y la percepción de confianza por parte de los clientes y usuarios del mercado. Se han desarrollado algunos intentos de tener control sobre la seguridad en la nube; sin embargo, los aspectos técnicos, de gobernanza y de gestión aún están expuestos a vulnerabilidades, limitando la efectividad de estas políticas hasta cierto punto.

Sobre esta base, es fundamental llegar a un enfoque sistemático que sea propicio para llevar a cabo un análisis completo de la columna vertebral en la nube del sector bancario dominicano, lo que permite la identificación de las debilidades críticas y la formulación de enfoques de mitigación en consecuencia. A partir de la declaración anterior, el enfoque de esta investigación es un modelo de ciberseguridad construido dentro de la infraestructura en la nube del sector bancario en la República Dominicana, con la intención de asegurar los activos de información más importantes y gestionar el riesgo cibernético en consecuencia. Con esto en mente, se propone una pregunta de investigación para investigar la construcción de un modelo de análisis para la infraestructura en la nube relevante para el sector bancario dominicano, de acuerdo con los objetivos presentados. Se sitúa en el área de ciberseguridad aplicada a entornos en la nube

dentro de la industria financiera nacional, analizando y evaluando las posibles debilidades de la infraestructura en la nube. También tiene un aspecto muy importante para la industria bancaria, y también se trata de la seguridad de la información: un elemento clave para mantener la continuidad de las operaciones, la estabilidad de las instituciones y la confianza del público en los establecimientos financieros. La implementación de tecnologías en la nube ha permitido a las instituciones financieras aumentar la eficiencia y la escalabilidad, pero ha planteado importantes cuestiones sobre la seguridad de la información sensible y la gestión de riesgos en el ciberespacio. Dado este hecho, se suma la necesidad de estudiar e investigar sobre la necesidad de cerrar las brechas de seguridad actuales a través de un modelo de ciberseguridad específicamente dirigido al entorno bancario nacional. Los conocimientos del estudio se presentan mediante principios para mejorar la resiliencia de las instituciones frente a los ciberataques, una respuesta más rápida a los incidentes y la consolidación de un entorno financiero más seguro y confiable. Además, los principios y métodos descritos en esta investigación ofrecen la posibilidad de ser adoptados fácilmente dentro de otras organizaciones con características similares y el potencial de llegar a otras fuera del sector bancario dominicano. Desde este ángulo, la investigación proporciona una buena referencia, que se utiliza como base para futuros trabajos en términos de desarrollar formas de mejorar el nivel de ciberseguridad en la infraestructura de la nube para múltiples sectores críticos.

Como un trabajo académico y estratégico, esta investigación, que va más allá de una descripción técnica, también tiene implicaciones para la protección del entorno bancario en la nube desde una perspectiva doctoral. La aplicabilidad práctica de la investigación se basa en la creación de un marco conceptual adaptado a un contexto nacional específico, que articula el

aspecto teórico, la evidencia empírica y los componentes regulatorios, contribuyendo a la academia en el desarrollo del conocimiento sobre ciberseguridad en los servicios financieros. Los hallazgos son relevantes no solo para influir en la toma de decisiones bancarias, sino también para guiar la política pública nacional y las directrices regulatorias sobre la protección del sistema financiero de la República Dominicana en un contexto digital. Esta investigación cubrió únicamente la infraestructura en la nube del sector bancario en la República Dominicana, con referencia particular a los aspectos técnicos, regulatorios y organizacionales de la ciberseguridad. Esta investigación examina específicamente aquellas amenazas, controles y prácticas que son más aplicables en el contexto local, en lugar de intentar abordar todos los riesgos cibernéticos a nivel global. De manera similar, se reconocerá que el desarrollo tecnológico en constante aumento introducirá nuevos casos que no están cubiertos en el presente estudio. Además, se identifican ciertas limitaciones inherentes a la investigación. Entre ellas, el acceso restringido a información detallada sobre las arquitecturas cloud de las entidades bancarias, debido a políticas de confidencialidad y seguridad, lo que puede limitar la profundidad del análisis técnico. De manera similar, el estudio está diseñado de acuerdo con el marco tecnológico y regulatorio contemporáneo, por lo que no es posible predecir completamente las amenazas cibernéticas en evolución o las nuevas tecnologías. Además, la variación en la madurez de la ciberseguridad y las implementaciones en la nube de una organización a otra puede afectar la aplicabilidad uniforme de algunas de las recomendaciones. Dada la aproximación contextualizada de la investigación, los hallazgos pueden no ser completamente generalizables a otras regiones con realidades económicas, tecnológicas o regulatorias diferentes.

La presente investigación se estructura en varios capítulos que responden de manera coherente a los objetivos planteados. En la primera parte se encuentran las formalidades e introducción, en las cuales se contextualiza el estudio, el capítulo 1 aborda los fundamentos iniciales del estudio, incluyendo el planteamiento del problema, la justificación de la investigación, el objetivo general, la formulación de la hipótesis y la definición de las variables o categorías de análisis. El segundo capítulo desarrolla el sustento teórico de la investigación, integrando el análisis del estado del arte y el marco teórico-conceptual, lo que permite contextualizar el estudio dentro del conocimiento existente y fundamentar la propuesta del modelo. El tercer capítulo describe la propuesta metodológica de la investigación, detallando el enfoque, el diseño, la población y muestra, los instrumentos de recolección de datos y los métodos de validación utilizados. Asimismo, se expone el procedimiento de análisis de la información y la metodología por objetivos que orienta el diseño conceptual del modelo, estableciendo las bases metodológicas para su desarrollo y posterior presentación como resultado del estudio. El capítulo cuatro presenta los resultados obtenidos en función de cada objetivo de la investigación, incluyendo el diseño y la descripción del modelo como principal resultado del estudio. En este capítulo se desarrollan los fundamentos, componentes y estructura del modelo, seguidos del análisis e interpretación de los hallazgos y su discusión a la luz del marco teórico y el estado del arte. El quinto capítulo presenta las conclusiones y recomendaciones producto de la investigación, junto con las algunas limitaciones y desafíos identificados. Además, se presentan lineamientos para investigaciones futuras en el ámbito de la ciberseguridad relacionada con las infraestructuras en la nube en el sector bancario.

Capítulo 1.

1.1 Problema

El objetivo del sistema financiero dominicano es promover la liquidez y solvencia del sistema bancario de la Nación. Entre las entidades que integran el sistema bancario se encuentran: bancos múltiples, asociaciones de ahorros y préstamos, bancos de ahorro y crédito, corporaciones de crédito, Bandex y el Banco Agrícola; instituciones que son fiscalizadas por las autoridades monetarias y trabajan, según las orientaciones y supervisiones del Banco Central y la Superintendencia de Bancos. Dentro del sistema bancario de la República Dominicana las instituciones manejan sistemas divergentes y los clientes corren el riesgo de exponer información confidencial, y que se produzcan incidentes cibernéticos que impacten los activos de información y produzcan daños a la organización.

La magnitud de este riesgo se sustenta en datos recientes del propio sector. Durante el primer Congreso de Supervisión de Ciberseguridad organizado por la Superintendencia de Bancos, se indicó que el costo promedio de una brecha de seguridad bancaria en 2025 se proyecta en aproximadamente USD 6 millones por incidente, y que el Global Risks Report 2025 del Foro Económico Mundial ubica los riesgos tecnológicos —incluidos los incidentes de seguridad de la información— entre los más relevantes a nivel global para los próximos dos años (Superintendencia de Bancos de la República Dominicana [SB], 2025). A esto se suma que, de acuerdo con el Ránking de digitalización del sector bancario 2025 de la propia Superintendencia de Bancos, las aplicaciones móviles constituyen ya el canal alterno preferido por los clientes personales, con un 77 % de utilización (SB, 2025), lo que evidencia una superficie de exposición

digital creciente. En el plano regional, el informe de ciberseguridad más reciente elaborado por el Banco Interamericano de Desarrollo, la Organización de los Estados Americanos y el Global Cyber Security Capacity Centre de la Universidad de Oxford ubica a la República Dominicana entre los países caribeños con mayor madurez relativa en ciberseguridad, junto a Jamaica y Trinidad y Tobago; no obstante, señala que esta posición de relativo liderazgo regional no exime al país de vulnerabilidades persistentes frente a amenazas cada vez más sofisticadas (Porrúa et al., 2025).

A pesar del creciente uso de infraestructura cloud en el sector bancario de República Dominicana, existe una falta de información y análisis sobre la ciberseguridad de estas plataformas. Esto representa un riesgo significativo para la seguridad de los datos y operaciones bancarias, ya que la infraestructura cloud es susceptible a una variedad de amenazas cibernéticas, como ataques de phishing, malware, y robo de datos. Además, la implementación de medidas de seguridad en la infraestructura cloud es compleja y requiere conocimientos especializados, lo que puede hacer que algunas instituciones financieras no implementen las medidas adecuadas para proteger su infraestructura cloud. Por lo tanto, es necesario investigar y analizar la ciberseguridad de la infraestructura cloud en el sistema bancario de República Dominicana para identificar las principales amenazas y riesgos, a fin de proponer recomendaciones para mejorar la seguridad de estas plataformas en el sector bancario del país. Por esta razón, a las organizaciones bancarias, les urge contar con un conjunto de procedimientos y tecnologías de seguridad, diseñadas para hacer frente a las amenazas externas e internas que pudiesen impactar a la organización. La necesidad de un entorno de cloud seguro, aumenta en las organizaciones, según avanzan sus estrategias de

transformación digital e incorporan herramientas y servicios basados en el cloud como parte de su infraestructura.

Sin embargo, existen algunos retos importantes que deberían considerarse en una infraestructura de cloud, que pudiesen comprometer la disponibilidad, confidencialidad e integridad de los sistemas de las entidades bancarias, entre estos están: falta de visibilidad, carencia de controles, seguridad de la información y ciberseguridad, protección de la red, integración compleja, entorno cambiante, tiempos de recuperación no adecuados (RTO/RPO), esto genera una gran complejidad para la gestión y tratamiento de los riesgos debido a que es necesario tener contexto, es decir, tener la mayor cantidad de información disponible sobre un evento o incidente en particular, que pueda ser útil y permita identificar, detectar, ubicar y correlacionar eventos o situaciones anómalas y que se pueda determinar el impacto que producen estos elementos en los activos de información de la organización.

Considerando esto y lo anteriormente planteado, en este trabajo se pretende resolver la pregunta problema: ¿Cómo proponer un modelo de gestión de ciberseguridad de infraestructura cloud para el sistema bancario de la República Dominicana, para fortalecer la gestión de riesgo cibernético?

1.2 Justificación

A pesar de las limitaciones, esta investigación puede considerarse útil y relevante en relación con el fortalecimiento y mejora de la ciberseguridad del sector bancario en la República Dominicana en relación con la infraestructura en la nube mencionada. Según las estadísticas sobre la economía digital, los bancos han adoptado la implementación de sistemas en la nube debido a la escalabilidad, eficiencia operativa y ahorro de costos. Esto plantea desafíos considerables para la seguridad de los datos sensibles y la minimización de los riesgos cibernéticos. No solo aumenta la seguridad de las instituciones bancarias, sino que también tiene un efecto positivo en la confianza pública en la infraestructura financiera nacional. El estudio es factible desde la perspectiva de la disponibilidad de marcos regulatorios bien aceptados, como NIST, ISO/IEC y la capacidad de encontrar y obtener información preguntando y utilizando el sector público y estudios previos, así como experiencias documentadas del sector bancario. Estos componentes han establecido un fuerte análisis y formulación de recomendaciones relevantes para el contexto nacional. En términos de viabilidad, el alcance del estudio se ha limitado a concentrarse en las vulnerabilidades relevantes, prácticas líderes en áreas de mejores prácticas para el contexto dominicano. Las metodologías comparativas de análisis, análisis documental y consulta de expertos harán posible el desarrollo de propuestas creíbles, sin la influencia de recursos financieros o alta experiencia técnica que está más allá de la experiencia académica. Este proyecto añade nuevas características al incluir en el estudio el análisis de la infraestructura en la nube bancaria en el contexto nacional, un tema que ha recibido poca atención en el país. Metodológicamente, contribuye construyendo un modelo holístico de ciberseguridad utilizado en relación no solo con el sector financiero de la República Dominicana, sino también en otras organizaciones del sector expuestas a riesgos

similares. Para abordar estos problemas, esta investigación explora un modelo de ciberseguridad adaptado a la implementación de la banca en la nube en el contexto bancario dominicano. También ofrece una solución integral para las necesidades técnicas, regulatorias y organizativas, todo con el objetivo final de mejorar las instituciones, mejorar la capacidad de respuesta y la resiliencia ante incidentes cibernéticos. Este estudio tiene algunas implicaciones académicas: reduce los tiempos de respuesta a incidentes de seguridad, mejora la detección de intrusiones, así como la defensa contra ataques emergentes de instituciones de nivel superior.

Ayuda a mantener la confianza nacional en el sistema financiero, una parte importante de la estabilidad en el sistema económico de la nación. Desde una perspectiva técnica, los conocimientos existentes obtenidos en este estudio pueden utilizarse como base para futuras investigaciones sobre detección inteligente de amenazas y mejora de políticas de seguridad en la nube. Por último, pero no menos importante, este estudio no solo satisface una brecha en el nivel actual de comprensión en el país, sino que también proporciona dirección para la formulación de mejores políticas de seguridad. Los bancos, instituciones reguladoras, Fintech, sector público e organizaciones educativas que deseen crear un ecosistema digital seguro, resiliente y confiable, pueden implementar el modelo propuesto.

1.3 Objetivo

1.3.1 Objetivo general

Proponer un modelo de gestión de ciberseguridad de la infraestructura cloud para el sistema bancario de la República Dominicana, para fortalecer la gestión del riesgo cibernético, siendo un referente para las entidades financieras interesadas en mejorar su postura de seguridad en entornos cloud.

1.3.2 Objetivos específicos

1) Analizar los marcos de trabajo, modelos de madurez y controles de ciberseguridad utilizados por las entidades bancarias en su infraestructura cloud, para identificar su nivel de alineación con estándares internacionales y su contribución a la gestión del riesgo cibernético.
2) Evaluar las prácticas, procesos y actividades operativas de ciberseguridad en entornos cloud del sector bancario dominicano, a partir de los resultados del diagnóstico, para identificar brechas y áreas de mejora.
3) Diseñar un modelo integral de gestión de ciberseguridad para la infraestructura cloud bancaria, que integre seguridad de la información, gestión del riesgo, arquitectura, gobierno y tecnologías habilitadoras, para fortalecer la gestión del riesgo cibernético.

1.4 Hipótesis o supuesto hipotético

El modelo propuesto de gestión de ciberseguridad para la infraestructura cloud, basado en procesos, actividades y prácticas, es pertinente y aplicable para fortalecer la gestión del riesgo cibernético en el sistema bancario de la República Dominicana.

1.5 Variables o Categoría de análisis

1.5.1 Procesos:

Conjunto organizado de pasos y procedimientos utilizados para gestionar y proteger los activos de información de la infraestructura en la nube del sistema bancario, en línea con las funciones núcleo del NIST Cybersecurity Framework 2.0; Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar; (National Institute of Standards and Technology [NIST], 2024). Estos procesos incluyen la gestión de identidades y accesos, el monitoreo de seguridad y la respuesta a incidentes.

1.5.2 Actividades:

Acciones específicas dentro de los procesos de ciberseguridad que permiten su ejecución efectiva, tales como la autenticación de usuarios, el análisis de vulnerabilidades y la revisión de registros de seguridad, consistentes con las categorías y subcategorías operativas descritas en el NIST CSF 2.0 (NIST, 2024).

1.5.3 Prácticas:

Métodos, estrategias y controles recomendados para asegurar la efectividad de los procesos y actividades de ciberseguridad, fundamentados en el estándar ISO/IEC 27001:2022 —Sistemas de

Gestión de Seguridad de la Información— y en su extensión ISO/IEC 27017:2015, específica para controles de seguridad en servicios en la nube (International Organization for Standardization [ISO], 2022, 2015).

1.5.4 Riesgos cibernéticos en el sistema bancario:

Riesgos y vulnerabilidades que pueden comprometer la confidencialidad, integridad o disponibilidad de los sistemas y datos en la infraestructura en la nube del sector bancario, categoría de análisis alineada con la función "Identificar" del NIST CSF 2.0, orientada a la gestión de riesgos organizacionales (NIST, 2024).

Capítulo 2.

2.1 Estado del Arte

La industria de servicios financieros ha estado adoptando rápidamente servicios en la nube en los últimos años, intensificando la complejidad operativa y exponiendo a riesgos de ciberseguridad. Hay una creciente alarma por el robo de datos, la fuga de información y los delitos de compromiso de credenciales en sistemas distribuidos que deben prevenirse y los controles de gobernanza/técnicos deben mejorarse dentro de una arquitectura híbrida/multi-nube. Múltiples esfuerzos de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) identifican configuraciones multi-nube como plagadas de problemas únicos de gestión de identidad, protección de datos en tránsito y visibilidad de acceso sobre una red distribuida; estos problemas requieren una gobernanza sólida, controles dedicados y monitoreo independiente de terceros. ENISA además nombra vectores comunes los escenarios donde errores en la configuración, sobre privilegios y control inadecuado de API llevan a un incidente, estos problemas empeoran sin un enfoque integrado para el control operativo y el monitoreo continuo (ENISA, 2023).

Asimismo, el NIST también amplió el alcance del Marco de Ciberseguridad 2.0 y la parte de Gobernanza se enfocó en la gobernanza, la rendición de cuentas, la protección de datos y la gestión de riesgos/respuestas de terceros. Este enfoque es particularmente importante cuando se trata de industrias de alto riesgo, como la banca, donde asegurar la infraestructura en la nube necesita una interacción constante entre el proveedor, el consumidor y los sistemas internos, así como una mejor identificación continua de activos, capacidades de gestión contextual y de riesgos, y funciones de monitoreo automatizadas (NIST, 2023).

Para ver la migración a la nube desde el aspecto de la responsabilidad financiera, el Consejo de Examinadores de Instituciones Financieras Federales (FFIEC) señala que debe ir acompañada de prácticas robustas de evaluación de riesgos, procedimientos de gobernanza corporativa y controles técnicos basados en evidencia. Destaca que la información y su protección no deben dejarse al proveedor de la nube, y que una institución debe mantener el control sobre la clasificación de datos, el acceso, la revisión de terceros, la continuidad del negocio y los contratos (FFIEC, 2022).

En cuanto a tendencias y amenazas, la Alianza de Seguridad en la Nube (CSA) sostiene que los riesgos prioritarios siguen presentes cuando se trata de configuraciones incorrectas, IAM débil, APIs inseguras y la falta de una estrategia integral de seguridad en la nube. Esto también enfatiza que el riesgo de la cadena de suministro está creciendo tanto en importancia como en nuevas formas de ataques, así como en esta era donde la automatización puede aliviar los errores humanos y dar respuestas rápidas a las personas. (Cloud Security Alliance, 2024) A nivel académico, la investigación revisada por pares coincide en que los mayores desafíos de la seguridad en la nube en la banca no son meramente brechas técnicas en la tecnología, sino de gobernanza y operaciones. Esto se refiere principalmente a IAM, seguridad de red, control de configuración, seguridad de API y visibilidad holística en el entorno. En este contexto, se requiere un modelo integral que articule controles técnicos, procesos organizacionales y mecanismos de gobernanza (Kim et al., 2018, Tariq et al., 2017).

2.1.1 Análisis crítico de los antecedentes

Al contrastar estos antecedentes entre sí, se identifican aportes complementarios, pero también limitaciones relevantes frente al problema de esta investigación. Los marcos de ENISA (2023) y NIST (2023) ofrecen taxonomías robustas de riesgo y gobernanza para entornos multi-nube, pero su alcance es genérico y no está adaptado a las particularidades regulatorias ni operativas del sistema bancario dominicano. El FFIEC (2022) aporta una perspectiva de responsabilidad institucional aplicable directamente al sector financiero, aunque su enfoque corresponde al contexto regulatorio estadounidense y no incorpora las condiciones de mercados bancarios emergentes como el dominicano. La Cloud Security Alliance (2024) y la literatura académica revisada por pares (Kim et al., 2018; Tariq et al., 2017) coinciden en que los principales desafíos de seguridad en la nube en la banca son de gobernanza y operación más que meramente técnicos, pero estos estudios se concentran en describir el problema —identificar brechas de IAM, configuración y visibilidad— sin proponer un modelo integral que articule controles técnicos, procesos y gobernanza en un instrumento aplicable y validado.

A nivel regional, estudios como el de Zárate Urgell et al. (2023) sobre el sector financiero mexicano evidencian la insuficiencia de los modelos de seguridad perimetral tradicionales y la necesidad de migrar hacia arquitecturas Zero Trust, mientras que el informe de la OEA (2018) y el más reciente de Porrúa et al. (2025) documentan avances desiguales en la madurez de ciberseguridad de América Latina y el Caribe, situando a la República Dominicana entre los países caribeños con mayor madurez relativa, pero sin proponer ni validar un modelo de gestión específico para el sector bancario del país.

2.2 Marco teórico -conceptual

Esta subsección proporciona un punto de vista académico y contextualizado para la investigación. Este marco, a diferencia de una revisión de literatura descriptiva, articula los conceptos y marcos regulatorios que apoyan la ciberseguridad en infraestructuras en la nube en el contexto del sector bancario dominicano y establece relaciones entre gobernanza, control operativo, cumplimiento y tecnologías habilitadoras.

2.2.1 Marco Legal

A nivel global, el NIST emitió la Publicación Especial 500-292, que define una arquitectura de referencia para la computación en la nube (Liu et al., 2011), SP 800-144, que establece directrices sobre seguridad y privacidad en la nube pública (Jansen & Grance, 2011), y SP 800-210, que tiene como objetivo proporcionar guías de control de acceso y consideraciones de seguridad en entornos de nube (Hu et al., 2023). A nivel nacional, la Junta Monetaria emitió el Reglamento de Ciberseguridad y Seguridad de la Información, estableciendo directrices obligatorias para asegurar la confidencialidad, integridad y disponibilidad en entidades financieras (Junta Monetaria, 2018). Este marco se complementa con la Ley No. 53-07, la Ley No. 126-02 y la Ley No. 172-13 (Congreso Nacional, 2002, 2007, 2013).

2.2.2 Marco Normativo

Este estudio se ha realizado tras analizar estándares internacionales comúnmente aplicables, normas, mecanismos regulatorios para ayudar en la gestión de medidas de seguridad de la información, como la ciberseguridad para la computación en la nube, basándose en una serie de

organizaciones reguladas, es decir, instituciones financieras. Estas son reglas como criterios técnicos, organizativos y de gobernanza para la regulación del riesgo del procesamiento de información crucial en la nube. Por esta razón, la industria de servicios en la nube necesita estándares específicos ISO/IEC 27017:2022 aplicables para la seguridad de la información en servicios de computación en la nube para complementar el control general definido en ISO/IEC 27001. Este estándar proporciona otra capa de controles destinados a mostrar la clara responsabilidad del proveedor de la nube hacia el cliente en la protección del activo de información alojado en un entorno común, gestionando la operación de manera segura y efectiva y, como mínimo, reduciendo los riesgos que necesariamente están asociados con los modelos IaaS, PaaS y SaaS (ISO/IEC, 2022).

En el sector bancario, se necesitan mecanismos específicos de control y supervisión debido a las tecnologías subcontratadas y los proveedores de la nube. El Instituto Nacional de Estándares y Tecnología (NIST) también ha emitido una serie de documentos que proporcionan un marco regulatorio crítico para los estándares y regulaciones de seguridad en la nube. La Publicación Especial 800-210 del NIST, que tiene como objetivo habilitar sistemas en la nube con acceso controlado, crea reglas y directrices para el manejo de identidades, derechos de acceso y autenticación en sistemas distribuidos (un vector de riesgo predominante en los nuevos ecosistemas en la nube) (Hu et al., 2023). Además, NIST SP 800-144 explica los controles de seguridad de la información y privacidad de la computación en la nube, incluyendo la evaluación de riesgos, la protección de datos y la gestión de relaciones con proveedores (Jansen & Grance, 2011). Estas directrices demuestran la responsabilidad compartida y destacan que debe haber un esfuerzo unificado entre los controles técnicos y de gobernanza. Al igual que las instituciones del

sector financiero, las instituciones bancarias también experimentan leyes de dominio que se ven influenciadas, y paradigmas de gobernanza que se superponen, lo que influye en la ciberseguridad en la nube de la misma manera. Estos abarcan el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) en torno al procesamiento de datos de tarjetas de pago; el Reglamento General de Protección de Datos (GDPR) que regula el procesamiento de información personal; y la Ley Sarbanes-Oxley (SOX) para mantener controles internos y control de calidad de la información financiera. Estas regulaciones exigen un relato detallado del control de acceso, trazabilidad, monitoreo, separación de funciones y continuidad de operación para ser incorporados explícitamente en las arquitecturas de sistemas en la nube que proporcionan la implementación de transacciones financieras críticas (PCI SSC, 2022; Parlamento Europeo, 2016; Congreso de EE.UU., 2002), y no deben ser omitidos al diseñar arquitecturas en la nube. Este tipo de paradigma puede ser aplicable en aplicaciones financieras que carecen de transparencia si la confianza del cliente e interna está en riesgo.

En el servicio en la nube, la Ley Sarbanes-Oxley (SOX) tiene particular importancia en términos de gestión de sistemas, requiriendo que los sistemas que manejan datos financieros sean confiables para proporcionar acceso confiable, integridad y almacenamiento auditable de la información. Por eso, garantizar la ciberseguridad juega una función integral en el apoyo al cumplimiento regulatorio, control de acceso, registro de eventos, segregación de funciones y detección de incidentes para asegurar que se proporcione la información financiera (Congreso de EE.UU., 2002) sin importar de qué infraestructura esté compuesta, ya sea en las instalaciones o basada en la nube. En última instancia, estas regulaciones refuerzan la idea de que los servicios en la nube en la banca nunca pueden integrarse ni operar de manera independiente entre sí o sin

tecnología común, sino que deben ser un enfoque integral, que contenga estándares internacionales, reglas corporativas y regulaciones específicas de la empresa y mejores prácticas relacionadas con su uso basado en la nube, y todos los aspectos que mejoren los modelos de gestión de ciberseguridad propuestos en este trabajo.

2.2.3 Marco Teórico

Los datos son críticos para todo tipo de mercados financieros, lo que hace que el uso de la computación en la nube sea una buena parte de la transformación digital, permitiendo a las instituciones financieras mejorar su tamaño y adaptar los entornos operativos para ayudar a promover el rápido ritmo de la innovación. Sin embargo, se reconoce en la literatura especializada que esta migración no puede ser vista únicamente a través de un lente tecnológico, y necesita ser gobernada por un marco de gestión de riesgos que tenga en cuenta la naturaleza crítica de la información financiera y la dependencia de infraestructuras externas. Por lo tanto, se enfatiza que los bancos deben adoptar modelos de seguridad en la nube que abarquen la responsabilidad compartida, la evaluación continua de riesgos y la alineación estratégica del negocio al trasladarse a la nube sin comprometer la estabilidad del sistema financiero o aumentar la exposición a amenazas cibernéticas (Banco Interamericano de Desarrollo, 2020; Agencia de la Unión Europea para la Ciberseguridad [ENISA], 2023).

Varios estudios sugieren que la integración de la nube se ha convertido en un componente esencial de la estrategia tecnológica de una organización. Un aumento de los servicios de nube gestionados por terceros sería estimado por Gartner, donde se espera que más organizaciones migren, lo que lleva a una mayor dependencia de infraestructuras externas para procesar

información crítica (Gartner, 2019). Al mismo tiempo, estudios sobre incidentes de seguridad revelan el hecho de que los entornos basados en la nube también son vulnerables a amenazas comunes, como malware, ransomware, robo de datos, violaciones de cuentas y cryptojacking, lo que apunta a la conclusión de que la migración a la nube no elimina el riesgo, sino que más bien hace que el riesgo cambie (Sophos, 2020).

Algunos estudios de análisis organizacional han revelado que los eventos de seguridad en escenarios de ciberespacio tienen un impacto financiero, operativo y reputacional considerable en las empresas basadas en la nube, especialmente en los bancos, especialmente en organizaciones que están fuertemente reguladas. La transición de servicios esenciales a los entornos de nube crea nuevas dependencias tecnológicas y organizacionales; tales dependencias aumentan la escala si no se mitigan, aumentando los riesgos asociados con las consecuencias de un incidente de seguridad si se pasa por alto el impacto de las violaciones, como aquellas que amenazan el control de acceso, la visibilidad de activos y la respuesta a incidentes (NIST, 2023).

Asimismo, ENISA destaca que la madurez organizacional de la gestión de la seguridad en la nube carece en la ejecución de funciones involucradas en la protección y detección de servicios en la nube, lo que resulta en mayores posibilidades de eventos con un impacto sistémico, enfatizando la importancia crítica de métodos preventivos, automatizados y basados en riesgos para proteger las infraestructuras financieras en la nube (ENISA, 2023). Desde un punto de vista académico, la evidencia actual sugiere para los estudios actuales que los riesgos principales en la computación en la nube (como en otros contextos) no surgen estrictamente de la tecnología, sino de deficiencias en la gobernanza, la gestión de identidades, la configuración segura de servicios y el monitoreo de entornos distribuidos. Los hallazgos del cuerpo de literatura revisada por pares

revelan que para la industria financiera estas vulnerabilidades están en gran medida asociadas con IAM, configuración, seguridad de APIs y visibilidad completa de los recursos en la nube, una debilidad notable, es decir, en la arquitectura de tipo híbrido y multi-nube (Kim et al., 2018; Tariq et al., 2017). Estas conclusiones destacan la importancia de modelos de ciberseguridad basados en la nube comprensivos que describan controles técnicos, procesos organizacionales y gobernanza, en lugar de fragmentados o normativos.

Arquitectónicamente, es importante señalar que la computación en la nube no es una arquitectura integrada, sino que comprende diferentes configuraciones: pública, privada, híbrida y multi-nube, y la Infraestructura como Servicio (IaaS), Plataforma como Servicio (PaaS) y Software como Servicio (SaaS), cada una con implicaciones claramente diferentes para el control, la responsabilidad y la seguridad (Gendler, 2021).

En general, una vez que un individuo pasa de IaaS a SaaS, el cliente puede tener cada vez menos control sobre la infraestructura, lo que resulta en una mayor dependencia del proveedor, desarrollando así más mecanismos de gobernanza y control, particularmente en entornos regulados como la banca (Banco Interamericano de Desarrollo, 2020). La seguridad en la nube se define como una serie de tecnologías, controles, procesos y políticas que se centran en proteger la información, las aplicaciones y los sistemas alojados en un servicio en la nube. Según Jones (2022), basado en este enfoque, existe una responsabilidad conjunta que involucra tanto al proveedor de servicios en la nube como al cliente, donde sus roles en la seguridad cambian dependiendo del modelo de servicio contratado. Es vital conocer esta responsabilidad compartida para prevenir brechas debido a lagunas de control o suposiciones erróneas en las responsabilidades de cada parte. Kaspersky (2023) afirma que la seguridad en la nube logra

objetivos fundamentales, incluyendo proteger los datos del acceso no autorizado, prevenir errores humanos, asegurar la recuperación de un incidente y mitigar las pérdidas causadas por una brecha de seguridad. Se identifican componentes esenciales para lograr esto, desde la seguridad de los datos hasta la gestión de identidades y accesos (IAM), la gobernanza, la continuidad del negocio y la recuperación ante desastres (BC/DR), y el cumplimiento legal. Estructurar un enfoque de protección integral basado en cada uno de estos elementos se ajustará tanto a los requisitos técnicos como a las regulaciones. En tal contexto, los riesgos de seguridad en la nube se manifiestan de diversas maneras. Los más pertinentes de estos desafíos incluyen, pero no se limitan a, la pérdida de visibilidad de activos y accesos, violaciones de cumplimiento regulatorio, estrategia de seguridad en la nube indefinida, amenazas internas, incumplimientos contractuales, APIs inseguras y configuraciones incorrectas de servicios en la nube (Jones, 2020).

La presencia material de estos riesgos pone de relieve la importancia de una evaluación estricta de los proveedores de servicios en la nube, que debe tener en cuenta los factores relacionados con la protección de datos en tránsito y en reposo, la gestión segura de identidades, la seguridad operativa, la transparencia en los controles y el cumplimiento. La computación en la nube ha dado lugar a una revolución tecnológica que ha llevado a arquitecturas avanzadas como microservicios, contenedores y herramientas de orquestación como Kubernetes. Los microservicios son una desviación de las arquitecturas monolíticas y abren la puerta al desarrollo de aplicaciones que consisten en servicios independientes que se comunican a través de interfaces bien definidas y soportan la escalabilidad y la resiliencia (Aguilar, 2022). Por otro lado, este enfoque crea un conjunto completamente nuevo de problemas de seguridad relacionados con la gestión de APIs, la segmentación de servicios y la visibilidad del entorno. Los contenedores y sus

orquestadores facilitan el despliegue y la gestión de aplicaciones en entornos de nube, pero requieren controles distintos para proteger imágenes, configuraciones, redes y ejecución (Aguilar, 2022). Asimismo, los marcos como el Security Access Service Edge (SASE) abogan por la sincronización de redes con la seguridad, migrando la protección a la nube y permitiendo configuraciones basadas en identidad y contexto, particularmente en contextos de acceso distribuido o trabajo remoto (Ferrer, 2023). Para un habilitador avanzado de ciberseguridad, el aprendizaje automático juega un papel clave en la identificación de anomalías, ataques de día cero, fraudes y actividades maliciosas que evaden las estrategias de defensa tradicionales. La inclusión en estrategias de defensa en profundidad mejora las capacidades de detección temprana y respuesta adaptativa con la creciente complejidad de las amenazas (Baloira, 2022).

2.2.4 Marco Conceptual

No limita el marco conceptual al que esta investigación se dirige como una mera definición de términos, sino que presenta los conceptos como uno en una lógica sistémica que subyace a la investigación. La seguridad de la información constituye el eje central de este modelo, a partir del cual la ciberseguridad y la seguridad informática se despliegan como dimensiones complementarias que protegen los activos de información en entornos de nube. La cooperación de amenazas, ataques, incidentes y controles de acceso sirve para operacionalizar la gestión del riesgo cibernético, mientras que la arquitectura empresarial y la arquitectura de seguridad estructuran la ejecución de controles técnicos y organizativos. Por lo tanto, los conceptos definidos no se introducen como elementos separados, sino como elementos interconectados que se combinan como un modelo holístico de protección bancaria en la nube.

2.2.4.1 Seguridad de la Información:

La seguridad de la información sirve como el eje central en un modelo de ciberseguridad para la infraestructura en la nube bancaria para proteger la información y los sistemas que procesan, almacenan o transmiten esa información, con el objetivo de asegurar la confidencialidad, integridad y disponibilidad de los activos informativos (Junta Monetaria, 2018). Es a través de esta perspectiva que se desarrollan los diversos aspectos de protección en medio de entornos de alta tecnología. La ciberseguridad, por otro lado, amplía la definición de seguridad de la información con nuevos conceptos al analizar las fuentes de amenaza que se encuentran en el ciberespacio y aquellas que impactan las infraestructuras conectadas, especialmente las infraestructuras basadas en tecnología en la nube (ISACA, 2020). Por otro lado, la seguridad informática se centra en implementar controles técnicos que buscan asegurar los sistemas informáticos contra accesos no autorizados, ataques maliciosos y fallos en el funcionamiento. Por otro lado, la ciberseguridad en la nube se enfoca en proteger la información mientras se procesa, transmite y almacena en infraestructuras de computación en la nube, que consisten en facetas tecnológicas, organizativas y regulatorias prevalentes en los entornos distribuidos y dependientes de terceros (Junta Monetaria, 2018; Kaspersky, 2023). Estos conceptos forman un eje integrado de protección entre la seguridad de la información, la ciberseguridad y la ciberseguridad en la nube; donde la seguridad de la información define el objetivo, la ciberseguridad define el entorno de amenazas (CTE), la seguridad informática implementa los controles técnicos (COT), y la ciberseguridad en la nube proporciona la estrategia de respuesta general desde el contexto de los riesgos digitales. La integración conceptual apoya el desarrollo del modelo como una solución holística para la protección bancaria en la nube.

2.2.4.2 Gestión del riesgo cibernético

La gestión del riesgo cibernético en el modelo está organizada en una secuencia lógica de conceptos interdependientes que permite la identificación, análisis y mitigación de riesgos asociados con el uso de infraestructura en la nube en el sector bancario. Este proceso comienza con la identificación de activos de información, que se consideran recursos tanto tangibles como intangibles que almacenan, procesan o transmiten información crítica para una organización (Junta Monetaria, 2018). Muchas amenazas convergen en estos activos, donde la explotación de vulnerabilidades resulta en ataques, incluidos los ciberataques ejecutados a través del ciberespacio. Tales ataques pueden llevar a incidentes de seguridad que amenazan o comprometen la confidencialidad, integridad o disponibilidad de la información y la infraestructura tecnológica. La TI en la sombra se incorpora como un factor de riesgo vital en este sentido, definida como el uso de servicios y aplicaciones en la nube sin la debida autorización o supervisión institucional, lo que reduce la visibilidad, socava el control y promueve configuraciones inseguras y brechas de cumplimiento (TI en la sombra, 2021; Jones, 2020). La relación encadenada activo → amenaza → ataque → incidente → riesgo permite la conceptualización del riesgo cibernético como la probabilidad de que ocurran eventos adversos con impacto asociado, lo que informa la toma de decisiones estratégicas y la priorización de controles en el modelo.

2.2.4.3 Arquitectura y gobierno de la seguridad

La Arquitectura Empresarial proporciona la estructura arquitectónica de la entidad bancaria, como sus sistemas de información, procesos de negocio, así como la alineación con los objetivos empresariales. En este marco, la ciberseguridad y la arquitectura de la información están

interrelacionadas como una sección transversal de la estructura, principios y mecanismos de protección relevantes para los activos de información y la infraestructura tecnológica (Junta Monetaria, 2018). La gobernanza de la seguridad delinea políticas, roles, responsabilidades y procesos, facilitando una gestión coherente con un ajuste a los parámetros regulatorios. En este dominio, la Alianza de seguridad en la nube (CSA) se incluye como una abstracción, una referencia conceptual para establecer mejores prácticas y un marco de control para mejorar la seguridad en entornos de nube y aclarar el modelo de responsabilidad compartida entre proveedor y cliente (Jones, 2020). De manera similar, con SASE (Security Access Service Edge) integrado como un modelo, la arquitectura de la arquitectura permite que las capacidades de seguridad de la red se conecten directamente a la nube, y así reemplaza el enfoque tradicional de límite físico con una configuración y controles de acceso basados en la identidad y el contexto de conexión (Ferrer, 2023). Estas ideas y principios forman la base y el sistema que permiten que los controles técnicos funcionen eficazmente y que el control pueda ser adoptado y mantenido en el marco. La arquitectura define el “qué” y el “cómo”, la gobernanza y el cumplimiento el “quién” y el “por qué”, reuniendo un enfoque holístico para proteger contra incidentes bancarios en la nube.

2.2.4.4 Tecnologías habilitadoras en entornos cloud

Las tecnologías habilitadoras dentro de un entorno de nube representan el aspecto operativo del marco de seguridad de la red de la infraestructura de nube bancaria, permitiendo la operacionalización de los principios de seguridad, controles y estrategias de seguridad establecidos en los constructos teóricos y conceptuales previos en una arquitectura de ciberseguridad bancaria en el entorno de la nube. Dichas tecnologías no solo son necesarias para

el funcionamiento del negocio bancario digital, sino que también son relevantes para determinar cómo se implementa, monitorea y mantiene el mecanismo de protección de la información, así como cómo se refuerzan los mecanismos de protección en el contexto de la nube. Los servicios de computación en la nube, organizados en los modelos Infraestructura como Servicio (IaaS), Plataforma como Servicio (PaaS) y Software como Servicio (SaaS), determinan el nivel de control que la parte bancaria tiene sobre la infraestructura, aplicaciones y datos desde la gestión, entre otros, de sus datos. Frente a modelos cada vez más abstractos como SaaS, la responsabilidad real del cliente disminuye con más complejidad y se convierte en un elemento más central que enfatiza la necesidad de monitoreo, cumplimiento y controles de acuerdo con el principio de responsabilidad compartida entre el proveedor de productos y servicios (Banco Interamericano de Desarrollo, 2020; Kaspersky, 2023).

Por esta razón, los Corredores de Seguridad de Acceso a la Nube (CASB) se posicionan estratégicamente entre los usuarios y los proveedores de la nube, con funciones de seguridad como intermediarios. Los mecanismos de seguridad en tales paquetes permiten el monitoreo de derechos de acceso, cifrado contra el acceso no autorizado, fuga de datos, así como la aplicación de requisitos de cumplimiento independientemente de la posición del usuario o del servicio utilizado. dichos corredores también juegan un papel en mejorar la visibilidad y controlabilidad en paisajes de nube heterogéneos y distribuidos dentro del modelo (Gartner, 2023).

La Gestión de Identidad y Acceso (IAM) es un fundamento complementario esencial para la protección de los activos de información en la nube. Las arquitecturas IAM permiten la autenticación de identidad, autorización de acceso y control de privilegios, y mitigan el riesgo de acceso no autorizado y abuso de privilegios. El control de identidad es un mecanismo importante

en los sistemas bancarios en la nube donde, en entornos bancarios en la nube, sirve como un habilitador central para facilitar la confidencialidad y trazabilidad de los procesos de actividades bancarias (Kaspersky, 2023).

Arquitectónicamente, la implementación de microservicios ha revolucionado la arquitectura de las aplicaciones bancarias al descomponer sistemas complejos y distribuidos en pequeños servicios modulares y reutilizables. Esto aumenta la resiliencia y flexibilidad del desarrollo, pero también introduce nuevas amenazas de seguridad con interfaces, segmentación de servicios y comunicación de mensajes entre componentes (Aguilar, 2022). Los contenedores (Kubernetes) se presentan como una de las principales tecnologías habilitadoras del despliegue de arquitectura de microservicios que se basa en una implementación de contenedorización, que tiene como objetivo lograr entornos de ejecución aislados y portátiles para la creación de aplicaciones basadas en microservicios. Su configuración de aplicación hace que el despliegue y operación de aplicaciones en la nube sea más eficiente, pero también requiere controles de seguridad específicos y control para mantener seguras las imágenes, configuraciones, redes y procesos en tiempo de ejecución, particularmente en un entorno financiero de alta criticidad (Aguilar, 2022).

Ciertamente, es la orquestación de contenedores, típicamente gestionada en la nube a través de servicios como Kubernetes, lo que hace posible la automatización del despliegue, escalabilidad y gestión de aplicaciones contenedorizadas en entornos de nube a gran escala. Desde la perspectiva del modelo, la orquestación es fundamental para la aplicación segura de políticas de seguridad, control de acceso, segregación de cargas de trabajo y detección temprana de incidentes en sistemas dinámicos y muy distribuidos (Aguilar, 2022). Estas tecnologías habilitadoras, realizadas en conjunto, no funcionan como soluciones independientes, sino que se armonizan para

hacer operativos los controles de seguridad, la gestión de riesgos cibernéticos y la gobernanza tal como se define en el modelo para permitir una protección efectiva y flexible de la infraestructura en la nube del sistema bancario.

Las cuatro dimensiones teóricas desarrolladas en este marco conceptual: seguridad de la información, gestión del riesgo cibernético, arquitectura y gobierno de la seguridad, y tecnologías habilitadoras, no se plantean como categorías aisladas, sino como el sustento conceptual directo de los ocho pilares que conforman el modelo PROBAN. La seguridad de la información se operacionaliza principalmente en los pilares de Cumplimiento y Seguridad de Datos; la gestión del riesgo cibernético se traduce en los pilares de Operaciones de Seguridad (SOC) y Gestión de Incidentes; la arquitectura y gobierno de la seguridad fundamenta los pilares de Cumplimiento, Arquitectura Híbrida y Gestión de Terceros, y Redes y Seguridad Perimetral; y las tecnologías habilitadoras sustentan los pilares de Gestión de Identidad y Accesos, y Seguridad de Aplicaciones y APIs. Esta correspondencia garantiza que cada pilar del modelo propuesto responda a un fundamento teórico explícito, evitando que el modelo se presente como una construcción normativa desconectada del marco conceptual que lo origina.

2.2.5 Relación entre el marco teórico y el modelo PROBAN

Las cuatro dimensiones teóricas desarrolladas en este marco conceptual: seguridad de la información, gestión del riesgo cibernético, arquitectura y gobierno de la seguridad, y tecnologías habilitadoras; no se plantean como categorías aisladas, sino como el sustento conceptual directo de los ocho pilares que conforman el modelo PROBAN, según se sintetiza en la [Tabla 1]. Esta correspondencia garantiza que cada pilar del modelo propuesto responda a un fundamento teórico explícito, evitando que el modelo se presente como una construcción normativa desconectada del marco conceptual que lo origina.

Tabla 1

Relación marco teórico - PROBAN

Dimensión teórica (marco conceptual, 2.2.4)	**Fundamento teórico**	**Indicador de correspondencia**	**Pilar(es) PROBAN relacionados**
2.2.4.1 Seguridad de la Información (seguridad de la información → ciberseguridad → seguridad informática → ciberseguridad en la nube)	Junta Monetaria (2018); ISACA (2020); Kaspersky (2023)	Confidencialidad, integridad y disponibilidad de datos bancarios en tránsito y en reposo	Pilar 1. Cumplimiento (marco regulatorio de protección de información); Pilar 2. Seguridad y Protección de Datos (cifrado, tokenización, mínimo privilegio)

2.2.4.2 Gestión del riesgo cibernético (cadena activo → amenaza → ataque → incidente → riesgo; TI en la sombra)	Junta Monetaria (2018); Jones (2020)	Tiempo de detección y respuesta ante amenazas; nivel de visibilidad de activos no autorizados	Pilar 6. Operaciones de Seguridad y Respuesta a Incidentes (SOC) (monitoreo, SIEM/SOAR, inteligencia de amenazas); Pilar 7. Gestión de Incidentes (playbooks, threat hunting)
2.2.4.3 Arquitectura y gobierno de la seguridad (Arquitectura Empresarial, CSA, SASE, gobernanza y políticas)	Junta Monetaria (2018); Jones (2020); Ferrer (2023)	Existencia de políticas de gobierno cloud; nivel de responsabilidad compartida definido con proveedores	Pilar 1. Cumplimiento (gobernanza y madurez); Pilar 8. Arquitectura Híbrida y Gestión de Terceros (integración IaaS/PaaS/SaaS, contratos, monitoreo de proveedores); Pilar 5. Redes y Seguridad Perimetral (SASE, ZTNA)

2.2.4.4 Tecnologías habilitadoras en entornos cloud (IaaS/PaaS/SaaS, CASB, IAM, microservicios, Kubernetes)	Banco Interamericano de Desarrollo (2020); Kaspersky (2023); Aguilar (2022); Gartner (2023)	Nivel de adopción de MFA/SSO/RBAC; cobertura de controles en arquitecturas de contenedores	Pilar 4. Gestión de Identidad y Accesos (IAM & Zero Trust); Pilar 3. Seguridad de Aplicaciones y APIs (DevSecOps, WAF/WAAP, SAST/DAST); Pilar 8. Arquitectura Híbrida y Gestión de Terceros (CASB)

Nota: Elaboración propia

Capítulo 3.

3.1 Propuesta metodológica

A continuación, se presenta la metodología que surgió de la formulación del problema:

3.1.1 Enfoque

El enfoque utilizado para este estudio fue descriptivo, dado que el propósito no fue establecer relaciones de causa y efecto, sino caracterizar el estado de las medidas de ciberseguridad y su nivel de implementación en la protección de infraestructuras en la nube del sistema bancario dominicano. Se analizó cómo se presentaban las prácticas de seguridad, su relación con los estándares internacionales y el nivel de madurez alcanzado, sin manipular variables ni comparar condiciones antes y después de una intervención.

3.1.2 Diseño de investigación

Esta investigación se clasificó como un estudio de tipo descriptivo, con un componente propositivo. Fue descriptiva porque caracterizó el nivel de madurez y las prácticas de ciberseguridad en la infraestructura cloud del sistema bancario dominicano a partir de los datos recolectados mediante cuestionarios estructurados y revisión documental, sin manipular variables ni establecer relaciones causales entre ellas. Tuvo, además, un alcance propositivo, en tanto que, a partir del diagnóstico realizado, se diseñó y sometió a validación de expertos un modelo de gestión de ciberseguridad (PROBAN), sin que ello implique una comprobación experimental de causalidad. Este diseño resultó apropiado dado que la investigación buscó comprender en profundidad las complejidades de la ciberseguridad en infraestructuras cloud; campo dinámico y

con múltiples capas tecnológicas; y examinar tanto la arquitectura tecnológica en la nube como las medidas de protección implementadas, considerando su relación con los activos de información, los procesos tecnológicos y el cumplimiento de los objetivos institucionales de las entidades bancarias.

3.2 Población y muestra

3.2.1 Población

De acuerdo con Malhotra (1997), la población se define como "el conjunto de todos los elementos que comparten un grupo común de características, y forman el universo para el propósito del problema" (p. 359). En este caso particular, la población estuvo constituida por un total de 49 organizaciones de intermediación financiera autorizadas que componían el sistema bancario de la República Dominicana. Dado que resultaba difícil, si no imposible, acceder a la totalidad de esta población, se trabajó con una muestra representativa de la misma, para lo cual se utilizaron técnicas de muestreo no probabilístico.

3.2.2 Muestra

Para seleccionar la muestra se utilizó una técnica de muestreo no probabilístico por conveniencia, combinada con cuotas por tamaño y ubicación geográfica, que consistió en seleccionar las organizaciones bancarias de categorías predefinidas (tamaño y ubicación geográfica) en cantidades proporcionales a su presencia en la población. Para este estudio se analizó la ciberseguridad en la nube en organizaciones bancarias de diferentes tamaños y ubicaciones geográficas, con el objetivo de obtener una muestra que reflejara la distribución de

estas dos características en la población total de 49 organizaciones. Se establecieron tres categorías de tamaño (pequeñas, medianas y grandes) y tres regiones geográficas (Norte, Sur y Este).

- **Unidad de análisis:** La unidad de análisis de esta investigación fue la entidad bancaria, representada a través de sus áreas de tecnología, riesgos o seguridad de la información, responsables de la gestión de la ciberseguridad en la infraestructura cloud institucional.
- **Informante clave:** En cada una de las 30 entidades participantes, el instrumento fue respondido por un profesional con responsabilidad directa sobre la gestión de la ciberseguridad o la infraestructura tecnológica de la organización, manteniéndose consistente el tipo de cargo del informante a lo largo de toda la muestra, con el fin de garantizar la comparabilidad de las respuestas entre entidades.
- **Criterios de inclusión y exclusión:** Se incluyeron en el estudio las entidades de intermediación financiera autorizadas por la Superintendencia de Bancos de la República Dominicana que manifestaron disposición a participar y facilitar información sobre sus prácticas de ciberseguridad en infraestructura cloud, lo que definió una muestra no probabilística por conveniencia, combinada con cuotas por tamaño y región para preservar la representatividad de la población. Se excluyeron aquellas entidades que, siendo parte de la población de 49 organizaciones autorizadas, no manifestaron disponibilidad para participar en el estudio dentro del período de recolección de datos.
- **Tasa de respuesta:** El instrumento fue aplicado a las 30 organizaciones seleccionadas, de las cuales la totalidad (30) respondió efectivamente, lo que representa una tasa de

respuesta del 100 %; no obstante, 3 de las 30 entidades (10 %) presentaron omisiones de respuesta en distintos ítems del instrumento, tal como se detalla en la sección 3.3.

3.2.3 Categorización de la población

- **Criterio de clasificación por tamaño**: La clasificación de las entidades bancarias como pequeñas, medianas o grandes se realizó considerando criterios como los activos totales, el número de sucursales y la clasificación regulatoria establecida por la Superintendencia de Bancos de la República Dominicana, lo que permitió agrupar a las organizaciones conforme a su escala operativa y su relevancia relativa dentro del sistema financiero nacional.
- **Justificación de las regiones**: La estratificación geográfica en las regiones Norte, Sur y Este no correspondió a una zonificación oficial establecida por la Superintendencia de Bancos, sino que respondió a un criterio de conveniencia definido para efectos de este estudio, con el propósito de asegurar una cobertura geográfica amplia del territorio nacional y evitar la concentración de la muestra en una sola zona del país. Esta decisión permitió captar posibles diferencias regionales en la adopción y gestión de la ciberseguridad en infraestructura cloud, sin que ello implique una representatividad estadística formal por región, sino una diversificación razonada de la muestra.

Las 49 organizaciones bancarias se categorizaron en términos de tamaño y ubicación geográfica:

- Tamaño: 15 pequeñas, 20 medianas y 14 grandes.

- Ubicación geográfica: Región Norte, 15 organizaciones; Región Sur, 20 organizaciones; Región Este, 14 organizaciones.
- Determinación de las cuotas: se tomó una muestra de 30 organizaciones bancarias en total, y las cuotas se asignaron proporcionalmente a la distribución en la población.

- **Muestra por tamaños/Región:**

$$\text{Calculo por tamaño/región} = \left(\frac{\text{Total por Tamaño}}{\text{Total de Organizaciones}} \right) \text{x Total por Región}$$

Tabla 2

Distribución de muestra por región y tamaño

Región \ Tamaño	Pequeña (15)	Mediana (20)	Grande (14)	Total Región
Norte	5	6	4	15
Sur	6	8	6	20
Este	4	6	4	14
Total	15	20	14	49

Para calcular la muestra proporcional de cada organización se tomaron como base los resultados de la tabla anterior, para realizar dicho calculo:

$$\text{Muestra} = \frac{\text{Tamaño/Región}}{\text{Total de Organizaciones}} \text{ x Total de organizaciones seleccionadas}$$

Tabla 3

Resultado de muestra estimada por región

Región \ Tamaño	Proporción en por región	Muestra estimada
Norte – Pequeña	5	3.06
Norte – Mediana	6	3.67
Norte – Grande	4	2.45
Sur – Pequeña	6	3.67
Sur – Mediana	8	4.9
Sur – Grande	6	3.67
Este – Pequeña	4	2.45
Este – Mediana	6	3.67
Este – Grande	4	2.45
Total	49	30.00

Tabla 4

Resultado de muestra por región y tamaño de organización

Región \ Tamaño	Pequeña	Mediana	Grande	Total
Norte	3	4	2	9
Sur	4	5	4	13
Este	2	4	2	8
Total	9	13	8	30

Tabla 5

Muestra final respecto a la Población

Región	Muestra	Población total por región	porcentaje
Norte	9	15	60%
Sur	13	20	65%
Este	8	14	57%
Total	30	49	61%

3.2.4 Selección de la muestra

Para esta investigación se tomó aproximadamente el 60 % de la población total como muestra. La distribución de representatividad final fue la siguiente:

a) Región Sur: 65 % de sus entidades quedaron representadas en la muestra. b) Región Norte: 60 %. c) Región Este: 57 %.

Como resultado, se obtuvo una muestra bien distribuida que permitió alcanzar una representación proporcional de diferentes tamaños y regiones geográficas para el estudio de la ciberseguridad de infraestructura cloud en el sistema bancario de la República Dominicana.

3.2.5 Procesamiento de datos

Los datos obtenidos fueron los siguientes:

a) **De la población:**

La población estudiada comprende un total de 49 organizaciones bancarias en la República Dominicana, seleccionadas de un universo mayor de instituciones financieras.

Estas organizaciones se distribuyen de acuerdo a su tamaño en: pequeña, mediana, grande, y su ubicación geográfica en tres regiones principales: Norte, Sur y Este.

b) Muestra externa:

Se consideraron e incluyeron en el estudio treinta organizaciones bancarias de un total de 49 bancos de la República Dominicana. Los bancos muestreados son pequeños, medianos y grandes en diferentes áreas (Norte, Sur y Este). Este enfoque permite examinar las operaciones de ciberseguridad en infraestructuras en la nube que operan en diferentes circunstancias, y es esencial para comprender las diferentes maneras de prácticas de ciberseguridad. Considerando todo, tuvimos un proceso de selección de muestras proporcional y neutral, considerando tanto el tamaño de las organizaciones como la ubicación regional de la organización, para obtener resultados representativos de la población general y representativos de instituciones de diferentes perfiles en todo el país.

Esta muestra diversificada y equilibrada no solo aumenta la fiabilidad de los hallazgos, sino que también permite una comparación entre subgrupos, proporcionando así una indicación general sobre los tipos de prácticas de seguridad para la infraestructura en la nube para cada grupo.

c) Comprobación de la hipótesis de investigación:

El supuesto hipotético planteado en el Capítulo 1 fue contrastado mediante el juicio de un panel de expertos en ciberseguridad, y no mediante la medición directa de indicadores operativos de riesgo antes y después de la implementación del modelo, dado que este estudio no contempló

una fase de aplicación piloto. La contrastación se realizó a través de un instrumento de validación aplicado a los expertos, que evaluó las siguientes dimensiones del modelo propuesto:

- **Relevancia**: pertinencia del modelo frente a la problemática de ciberseguridad cloud identificada en el sector bancario dominicano.
- **Aplicabilidad:** viabilidad de implementación del modelo en el contexto operativo de las entidades bancarias del país.
- **Efectividad percibida:** juicio experto sobre la capacidad del modelo para fortalecer la gestión del riesgo cibernético, sin que ello equivalga a una medición empírica de resultados.
- **Coherencia:** consistencia interna entre los pilares del modelo PROBAN, sus indicadores y los estándares internacionales que lo sustentan.

Esta evaluación arrojó un índice de validez de contenido de 0.98, clasificado como excelente según la escala de interpretación adoptada (Tabla 13), lo que respalda la pertinencia y aplicabilidad del modelo desde el juicio experto. Queda como línea de investigación futura la medición de indicadores operativos, como reducción de incidentes de seguridad, tiempo de respuesta ante incidentes o frecuencia de auditorías exitosas— mediante un diseño longitudinal con mediciones antes y después de una aplicación piloto del modelo en entornos bancarios reales.

3.3 Instrumento, método de validación y descripción procedimiento de aplicación

Esta investigación siguió un enfoque descriptivo-propositivo en el que se utilizaron técnicas cualitativas y cuantitativas para analizar la gestión de riesgos cibernéticos en las infraestructuras en la nube del sistema bancario dominicano y validar el modelo propuesto. Se llevó a cabo una

revisión documental sistemática de las normas internacionales ISO/IEC 27001, ISO/IEC 27017 y NIST CSF 2.0, lo que estableció un marco comparativo inicial para examinar las circunstancias existentes y orientar el diseño del modelo propuesto.

Número de ítems y dimensiones. El instrumento de recolección de datos (Apéndice A) estuvo compuesto por 38 ítems sustantivos, aplicados mediante una plataforma de encuesta digital, organizados en nueve dimensiones temáticas: (1) contexto organizacional; (2) adopción, estrategia y madurez cloud; (3) talento, capacidades y presupuesto; (4) percepción y gestión del riesgo cloud; (5) controles de seguridad y buenas prácticas; (6) operaciones de seguridad y monitoreo; (7) continuidad, respuesta y resiliencia; (8) gobierno, proveedores y cumplimiento; y (9) innovación y uso de inteligencia artificial.

Escalas de medición. El instrumento combinó tres tipos de escala: (a) ítems categóricos de selección única o múltiple, para caracterizar el perfil organizacional y tecnológico; (b) ítems ordinales de cuatro puntos para captar el nivel de preocupación percibido (de "levemente preocupado" a "extremadamente preocupado"); y (c) catorce ítems con escalas ordinales de cinco niveles, específicas para cada control evaluado, que gradúan el nivel de madurez o frecuencia de implementación (por ejemplo, de "no implementado" a "totalmente implementado y operativo"; o de "nunca se auditan" a "auditorías automatizadas y alertas activas"). Estas catorce escalas ordinales constituyeron la base del análisis de confiabilidad del instrumento.

Procedimiento de aplicación. El instrumento se administró de forma autoadministrada y anónima a través de una plataforma de encuesta digital (Microsoft Forms), a un informante clave por entidad con responsabilidad directa sobre la gestión de la ciberseguridad o la infraestructura

tecnológica. La plataforma registró automáticamente la hora de inicio y finalización de cada respuesta, sin recolectar datos identificativos del respondiente ni de su correo electrónico.

Codificación. Las respuestas de los catorce ítems de escala ordinal de madurez se codificaron numéricamente en un rango de 0 a 4, ordenando las categorías de respuesta de cada ítem de menor a mayor nivel de madurez o frecuencia de control. Los ítems de percepción de riesgo se codificaron en un rango de 1 a 4, y los ítems categóricos se codificaron como variables nominales o dummy según el número de opciones de respuesta.

Tratamiento de datos faltantes. De las 30 entidades participantes, 27 (90 %) completaron la totalidad del instrumento. Tres entidades (10 %) presentaron datos faltantes: una entidad interrumpió su participación después del ítem 19, dejando sin responder los 17 ítems correspondientes a controles técnicos, operaciones de seguridad, continuidad y gobierno de proveedores; las dos entidades restantes presentaron una y dos omisiones puntuales, respectivamente. Para el análisis de confiabilidad se aplicó eliminación por lista (listwise deletion), excluyendo los casos con datos incompletos en el bloque de ítems analizado, lo que resultó en un tamaño muestral efectivo de 29 observaciones.

Resultados de confiabilidad. La confiabilidad del bloque de catorce ítems de escala ordinal de madurez se estimó mediante el coeficiente Alfa de Cronbach, obteniéndose un valor de $\alpha = 0.936$ ($n = 29$), clasificado como excelente consistencia interna según los criterios convencionales (George y Mallery, 2003). Las correlaciones ítem-total corregidas oscilaron entre 0.443 y 0.830, sin que ningún ítem presentara una correlación por debajo del umbral mínimo aceptable de 0.30, por lo que se conservó la totalidad de los catorce ítems en el instrumento final.

3.4 Matriz de Variables

Se desarrolló una definición operacional de las variables basada en su vinculación directa con los instrumentos de recolección de datos y las métricas de evaluación utilizadas, con el fin de proporcionar consistencia entre los objetivos, hipótesis y datos empíricos del estudio.

Tabla 6

Matriz de Variables

Variable	Categoría de análisis	Dimensión	Indicador	Escala	Ítem (Apéndice A)
Marcos y controles de ciberseguridad	Alineación normativa y madurez	Alineación con estándares internacionales (ISO/IEC 27001, ISO/IEC 27017, NIST CSF 2.0)	Grado de alineación con estándares; nivel de madurez de controles	Escala mixta (categórica y ordinal de 5 niveles)	Ítems 1–18, 20–25, 28–36
Gestión operativa de la ciberseguridad	Procesos y prácticas operativas	Procesos (1.5.1)	Formalización y ejecución de procedimientos institucionales, gestión de identidades, monitoreo, planes de continuidad y DRP	Escala ordinal de 5 niveles de madurez	Ítems 28, 29
		Actividades (1.5.2)	Ejecución de actividades operativas de autenticación, monitoreo de APIs, revisión de accesos y	Escala ordinal de 5 niveles de madurez	Ítems 20, 24, 25, 30, 31, 33

			auditoría de configuraciones		
		Prácticas (1.5.3)	Nivel de adopción de prácticas y medidas técnicas basadas en ISO/IEC 27001 y NIST CSF	Escala categórica de selección múltiple	Ítem 19
Modelo de gestión de ciberseguridad (PROBAN)	Gestión del riesgo cibernético	Pilares P1–P8 del modelo PROBAN (Cumplimiento, Datos, AppSec/APIs, IAM, Perimetral, SOC, Incidentes, Híbrida/Terceros)	Reducción de brechas identificadas; mejora en la gestión del riesgo; coherencia entre pilares; validación por juicio de expertos	Escala mixta en cuestionario aplicado a entidades; Escala Likert (5 puntos) e Índice de Validez de Contenido (IVC) en expertos	Apéndice A (ítems 10–18, 22, 26–38); Apéndice B (mapeo); Apéndice C (instrumento de validación)

Nota: Elaboración propia, a partir de los marcos de referencia y controles de ciberseguridad considerados en la investigación.

Las variables y categorías de análisis se definieron en línea con el marco conceptual, por lo tanto, cada objetivo particular se tradujo en indicadores observables y medibles. Esta estructura mantiene la evaluación del modelo no solo como un análisis descriptivo y permite mostrar cómo el modelo contribuye a la mejora de la gestión de riesgos cibernéticos en infraestructuras de nube del sector bancario.

3.5 Metodología por Objetivos

Objetivo No. 1: Analizar los marcos de trabajo, modelos de madurez y controles de ciberseguridad utilizados por las entidades bancarias en su infraestructura cloud, para identificar su nivel de alineación con estándares internacionales y su contribución a la gestión del riesgo cibernético.

Actividades:

a) Identificación y revisión de marcos de ciberseguridad y estándares internacionales aplicables a entornos de nube bancaria (por ejemplo, NIST CSF, ISO/IEC 27001 e ISO/IEC 27017). (30%)

b) Análisis comparativo de modelos de madurez en ciberseguridad utilizados en el sector bancario, considerando su nivel de adopción y cobertura de dominios de seguridad. (35%)

c) Evaluación del conjunto de controles de ciberseguridad implementados en la infraestructura cloud de las entidades bancarias, en relación con los estándares identificados. (35%)

Objetivo 2: Evaluar las prácticas, procesos y actividades operativas de ciberseguridad en entornos cloud del sector bancario dominicano, a partir de los resultados del diagnóstico, para identificar brechas y áreas de mejora.

Actividades:

a) Identificación y análisis de prácticas, procesos y actividades operativas de ciberseguridad en la nube, con base en estándares internacionales y marcos de referencia del sector financiero. (40%)

b) Diagnóstico de brechas entre las prácticas actuales del sector bancario dominicano y las mejores prácticas internacionales en ciberseguridad cloud. (30%)

c) Formulación de oportunidades de mejora, orientadas a fortalecer la gestión operativa de la ciberseguridad en infraestructuras cloud bancarias. (30%)

Objetivo 3: Diseñar un modelo integral de gestión de ciberseguridad para la infraestructura cloud bancaria, que integre seguridad de la información, gestión del riesgo, arquitectura, gobierno y tecnologías habilitadoras, para fortalecer la gestión del riesgo cibernético.

Actividades:

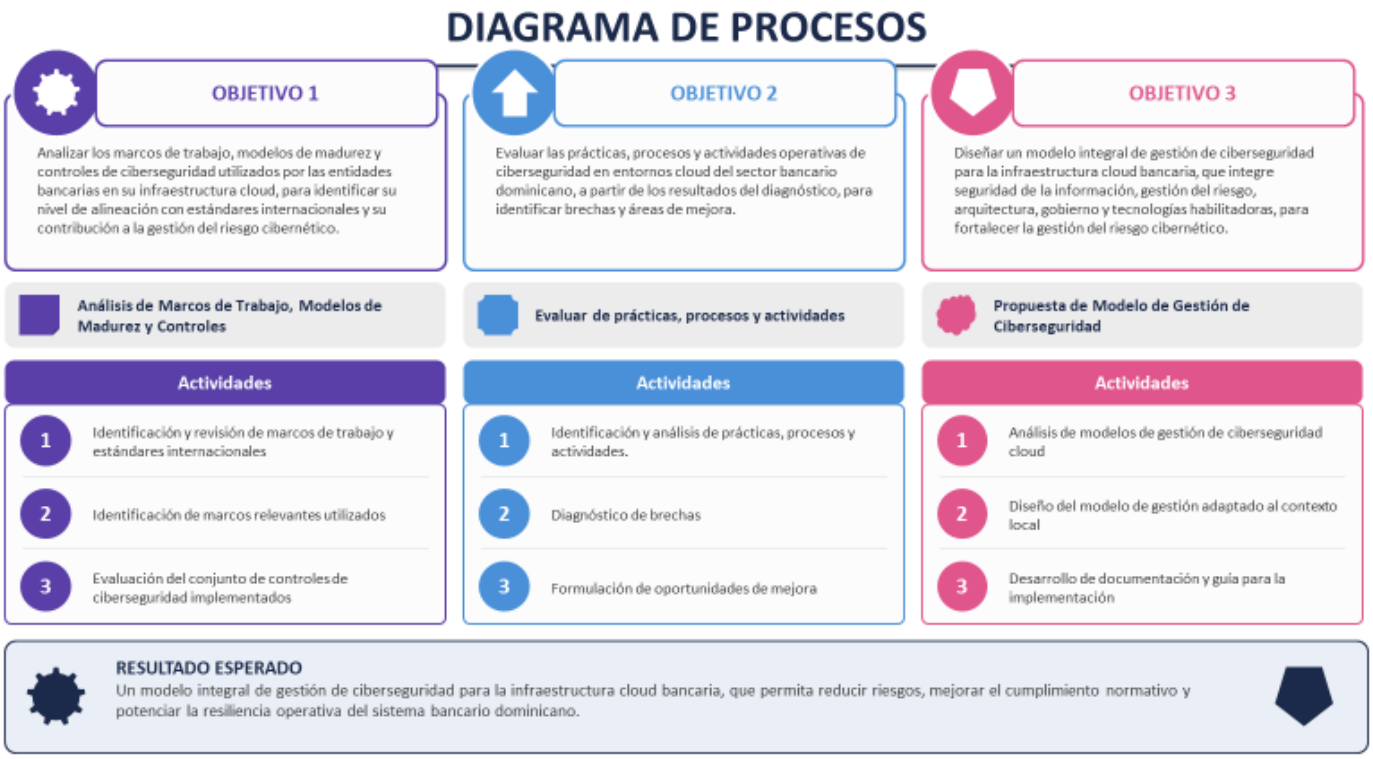
a) Análisis de modelos y enfoques de gestión de ciberseguridad aplicables a infraestructuras cloud en el sector financiero. (40%)

b) Diseño del modelo de gestión de ciberseguridad, adaptado al contexto regulatorio, tecnológico y operativo del sector bancario dominicano. (35%)

c) Elaboración de lineamientos y documentación de apoyo para la implementación, validación y uso del modelo propuesto en las entidades bancarias. (25%)

Figura 1

Diagrama de procesos



Nota: Elaboración propia (2026).

Capítulo 4.

4.1 Resultados por Objetivo

General y específicos

El presente capítulo expone los resultados obtenidos a partir de la aplicación de los instrumentos de recolección de datos y del análisis metodológico definido en el Capítulo 3. Los resultados se presentan organizados por objetivo específico, garantizando la trazabilidad entre las actividades ejecutadas, las evidencias empíricas obtenidas y la validación de la hipótesis de investigación.

4.1.1 Resultados objetivo general: Proponer un modelo de gestión de ciberseguridad de la infraestructura cloud para el sistema bancario de la República Dominicana, para fortalecer la gestión del riesgo cibernético, siendo un referente para las entidades financieras interesadas en mejorar su postura de seguridad en entornos cloud.

Los resultados obtenidos en esta investigación permitieron establecer los elementos fundamentales para la construcción de un modelo integral de ciberseguridad orientado a infraestructuras cloud en el sistema bancario dominicano. A partir del análisis realizado, se identificó que las entidades financieras han fortalecido de manera importante sus capacidades de

resiliencia operativa y gestión de riesgos; sin embargo, todavía existen debilidades estructurales que afectan la capacidad de prevenir y detectar incidentes de seguridad en entornos de nube.

El estudio comparativo con estándares y marcos internacionales evidenció que muchas instituciones financieras de la región priorizan las estrategias de continuidad del negocio y recuperación ante incidentes, mientras que los controles preventivos y de monitoreo continuo presentan menores niveles de desarrollo. Esta situación coincide con planteamientos previamente expuestos por organismos internacionales especializados en ciberseguridad y supervisión financiera, los cuales destacan la necesidad de fortalecer mecanismos de protección y detección temprana en ambientes cloud.

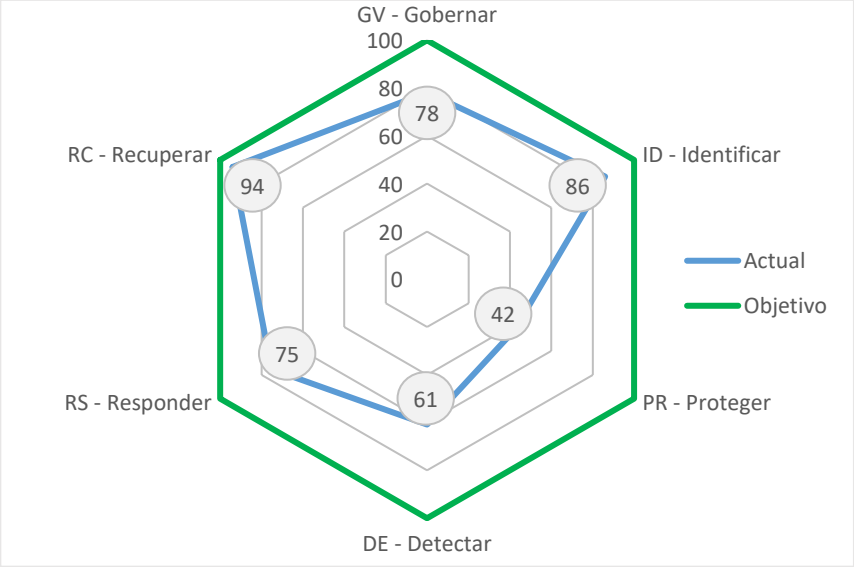
En el contexto del sistema bancario dominicano, las principales brechas identificadas se concentran en las funciones Proteger y Detectar del marco NIST CSF, reflejando oportunidades de mejora en la implementación de arquitecturas Zero Trust, automatización de controles de seguridad en la nube, fortalecimiento de capacidades de monitoreo mediante plataformas SIEM/SOAR, optimización de los mecanismos de gestión de identidades y accesos (IAM) y promoción de prácticas de seguridad desde el diseño de los servicios tecnológicos.

Los hallazgos obtenidos permiten sustentar la necesidad de disponer de un modelo de ciberseguridad cloud adaptado a las características regulatorias, operativas y tecnológicas del

sector bancario nacional, validando así el cumplimiento del objetivo general planteado en la investigación (ver Figura 2).

Figura 2

Nivel de madurez NIST de las entidades bancarias



Nota: Elaboración propia (2026).

4.1.2 Resultados objetivo 1: Analizar los marcos de trabajo, modelos de madurez y controles de ciberseguridad utilizados por las entidades bancarias en su infraestructura cloud, para identificar su nivel de alineación con estándares internacionales y su contribución a la gestión del riesgo cibernético.

El estudio reveló que las entidades bancarias evaluadas utilizan principalmente los marcos ISO/IEC 27001:2022, ISO/IEC 27017 y NIST CSF 2.0, complementados en menor medida por CIS Controls, como referencia para estructurar la gestión de la ciberseguridad en entornos cloud.

Los resultados que se muestran en la tabla 7 (Resultados por Objetivo 1) corresponden al Objetivo 1 de la investigación y al indicador "nivel de madurez de controles" definido en la tabla 6 (Matriz de Variables). Cada nivel de madurez por función del NIST CSF 2.0 se calculó a partir de las respuestas dicotómicas y ordinales de los ítems correspondientes del cuestionario estructurado (Apéndice A), aplicado a las 30 entidades bancarias que conformaron la muestra.

Tabla 7

Resultados por Objetivo 1

Dominio NIST	**Resultado Obtenido**	**Ítem(s) fuente (Apéndice A)**	**Fuente de datos**
Gobernar	78%	Ítems 18, 34, 35, 36	Cuestionario estructurado aplicado a las 30 entidades
Identificar	86%	Ítems 3, 4, 6, 7, 22	Cuestionario estructurado
Proteger	42%	Ítems 19, 21, 30, 31	Cuestionario estructurado
Detectar	61%	Ítems 33, 24, 25	Cuestionario estructurado
Responder	75%	Ítems 26, 32	Cuestionario estructurado
Recuperar	94%	Ítems 28, 29, 23	Cuestionario estructurado

Los resultados muestran que las mayores fortalezas se concentran en las funciones Recuperar e Identificar, lo que evidencia una orientación del sector hacia la resiliencia operativa y la gestión reactiva del riesgo. No obstante, las funciones Proteger y Detectar presentan los niveles más bajos de madurez, lo que indica debilidades en los controles técnicos orientados a la prevención y detección temprana de incidentes en infraestructuras cloud.

Asimismo, la comparación entre los controles implementados y los controles recomendados por NIST CSF 2.0 e ISO/IEC 27017 evidenció brechas significativas en áreas como la gestión de identidades y accesos (IAM), la segmentación y configuración segura de entornos cloud, el monitoreo unificado, la correlación de eventos y la automatización de controles.

4.1.3 Resultados objetivo 2: Evaluar las prácticas, procesos y actividades operativas de ciberseguridad en entornos cloud del sector bancario dominicano, a partir de los resultados del diagnóstico, para identificar brechas y áreas de mejora.

Estas recomendaciones responden al Objetivo 2 y a los indicadores "identificación de brechas operativas" y "existencia y formalización de procesos" (Tabla 6). Cada eje estratégico se derivó del contraste entre las brechas de madurez identificadas en el Objetivo 1 (ítems 19-33 del Apéndice A) y los controles recomendados por NIST CSF 2.0 e ISO/IEC 27017, mediante análisis documental comparativo.

A partir de las brechas identificadas en el diagnóstico, se definió un conjunto de recomendaciones estructuradas en cinco ejes estratégicos:

- Gobernanza y cumplimiento cloud, orientado a la estandarización de políticas, roles y responsabilidades, así como al fortalecimiento del ciclo de vida del riesgo y la implementación de métricas de madurez y KPIs.
- Seguridad de acceso e identidad (IAM), enfocada en la adopción de autenticación multifactor avanzada, principios de privilegio mínimo y Zero Trust.

- Protección de datos y entornos cloud, mediante cifrado extremo a extremo, tokenización, gestión segura de llaves y escaneo continuo de configuraciones (CSPM).
- Monitoreo, detección y respuesta, integrando capacidades SIEM/SOAR, telemetría cloud nativa y ejercicios de simulación.
- Resiliencia y continuidad, fortaleciendo la automatización de respaldos, las pruebas periódicas y la recuperación orquestada.

Estas recomendaciones constituyen un marco integral y adaptable a las realidades operativas del sector bancario dominicano.

4.1.4 Resultados objetivo 3: Diseñar un modelo integral de gestión de ciberseguridad para la infraestructura cloud bancaria, que integre seguridad de la información, gestión del riesgo, arquitectura, gobierno y tecnologías habilitadoras, para fortalecer la gestión del riesgo cibernético.

El diseño del modelo PROBAN respondió al Objetivo 3 y al indicador "coherencia entre pilares", parte del indicador compuesto de la variable "Modelo de gestión de ciberseguridad (PROBAN)" definido en la Tabla 6, integrando los hallazgos de los Objetivos 1 y 2 con la revisión documental de ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 22301, NIST CSF 2.0 y CIS Controls.

Como resultado del análisis de los marcos de trabajo, modelos de madurez, controles implementados y brechas identificadas en los objetivos anteriores, se diseñó el modelo de ciberseguridad para protección de la infraestructura de nube en entidades bancarias, un modelo

integral de gestión de ciberseguridad cloud específicamente adaptado a las necesidades, riesgos y exigencias regulatorias del sector bancario dominicano.

El modelo integra de manera articulada los principales marcos y estándares internacionales de referencia —ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 22301, NIST CSF 2.0 y CIS Controls— y los operacionaliza en una arquitectura de gestión orientada a entornos multicloud, híbridos y on-premise, considerando de forma explícita la gestión de terceros, la protección de datos sensibles y la responsabilidad compartida con los proveedores de servicios cloud.

El modelo propuesto está compuesto por ocho pilares estratégicos, orientados a unificar criterios y reforzar la administración de la ciberseguridad en entornos cloud dentro de las entidades bancarias del país:

- **Pilar 1. Cumplimiento (Compliance)**

Este componente define el marco de gobernanza requerido para garantizar que la infraestructura cloud bancaria opere conforme a las regulaciones y normativas vigentes. Comprende la adopción de estándares internacionales, la creación de esquemas de gobierno, la supervisión continua de los procesos en la nube, la administración de políticas y niveles de madurez, así como el seguimiento del cumplimiento por parte de proveedores y servicios esenciales. Su propósito principal es mantener un proceso constante de control, evaluación y mejora continua.

- **Pilar 2. Seguridad y Protección de Datos (Data Security)**

Este pilar está enfocado en resguardar de forma integral la información bancaria mediante controles de cifrado de datos en tránsito y almacenamiento, administración segura de claves criptográficas, tokenización, anonimización, prevención de pérdida de información y esquemas de acceso bajo el principio de mínimo privilegio. Su importancia radica en la protección de datos críticos, incluyendo transacciones financieras, cuentas y datos personales de los clientes.

- **Pilar 3. Seguridad de Aplicaciones y APIs (AppSec & API Security)**

Este eje se centra en la protección de las aplicaciones bancarias desplegadas en ambientes cloud, incorporando prácticas de seguridad desde el diseño y metodologías DevSecOps. Incluye mecanismos como WAF/WAAP, pruebas SAST y DAST, controles para microservicios y contenedores, además de la administración y monitoreo de APIs, con el fin de disminuir vulnerabilidades en aplicaciones consideradas críticas para la operación bancaria.

- **Pilar 4. Gestión de Identidad y Accesos (IAM & Zero Trust)**

Este pilar permite administrar de manera centralizada las identidades y accesos dentro de los entornos de nube, utilizando controles como autenticación multifactor (MFA), inicio de sesión único (SSO), control de acceso basado en roles (RBAC), gestión de accesos privilegiados (PAM) y mecanismos adaptativos basados en riesgo. La aplicación del enfoque Zero Trust contribuye a reducir la exposición a amenazas, consolidando la gestión de identidades como uno de los principales mecanismos de protección del modelo.

a) Modelo Conceptual del Pilar IAM

A continuación, se presenta el flujo de control que sigue una solicitud de acceso dentro del Pilar 4 (IAM). Los controles se organizan en dos fases secuenciales:

1. La autenticación, que verifica la identidad del solicitante.
2. La autorización, que determina el alcance de los permisos concedidos bajo el principio Zero Trust.

El proceso inicia cuando una entidad: sea usuario, aplicación o servicio genera una solicitud de acceso a un recurso protegido dentro del entorno de la nube bancaria. La solicitud atraviesa los cinco controles del pilar en orden secuencial, sin posibilidad de omitir ninguna capa.

La primera fase, correspondiente a la autenticación, comprende dos controles:

- **Inicio de sesión único (SSO):** centraliza la gestión de identidades en un único punto de entrada, eliminando la proliferación de credenciales dispersas entre sistemas y reduciendo la superficie de ataque asociada a la gestión de múltiples contraseñas.
- **Autenticación multifactor (MFA):** exige la verificación de la identidad mediante al menos dos factores independientes (conocimiento, posesión o inherencia). Si la identidad no puede ser confirmada, el acceso es denegado de forma inmediata y el intento queda registrado.

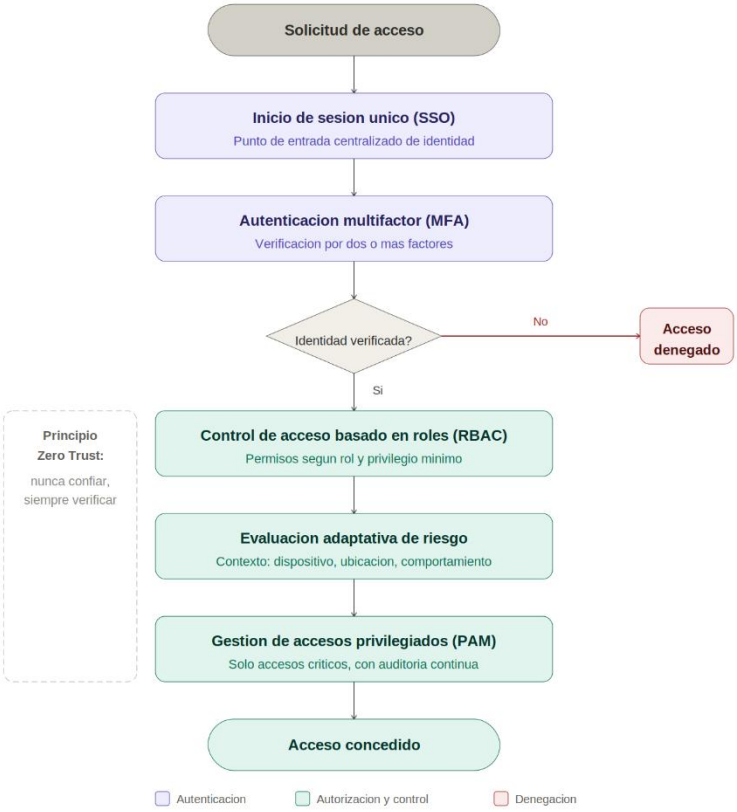
La segunda fase, correspondiente a la autorización, opera bajo el principio Zero Trust y comprende tres controles adicionales:

- **Control de acceso basado en roles (RBAC):** asigna permisos en función del rol organizacional del solicitante, implementando el principio de privilegio mínimo. Ningún usuario accede a más recursos de los estrictamente necesarios para su función.
- **Evaluación adaptativa de riesgo:** analiza el contexto de la solicitud, el dispositivo utilizado, ubicación geográfica, horario y patrón de comportamiento, para ajustar dinámicamente el nivel de confianza, incluso dentro de una sesión activa.
- **Gestión de accesos privilegiados (PAM):** aplica controles adicionales sobre los accesos a recursos críticos, garantizando trazabilidad completa, sesiones auditadas y revocación inmediata ante anomalías.

Los tres controles de la fase de autorización se ejecutan bajo el enfoque Zero Trust: que indica que ninguna identidad interna o externa es considerada de confianza por defecto. La verificación ocurre en cada solicitud de forma independiente, no solo en el momento de inicio de sesión. Esto elimina el riesgo de movimiento lateral en caso de compromiso de una cuenta. La Figura 3 describe el modelo de control IAM desde una perspectiva funcional. A fin de elevar la profundidad técnica del análisis.

Figura 3

Flujo de Control IAM



Nota: Elaboración propia (2026).

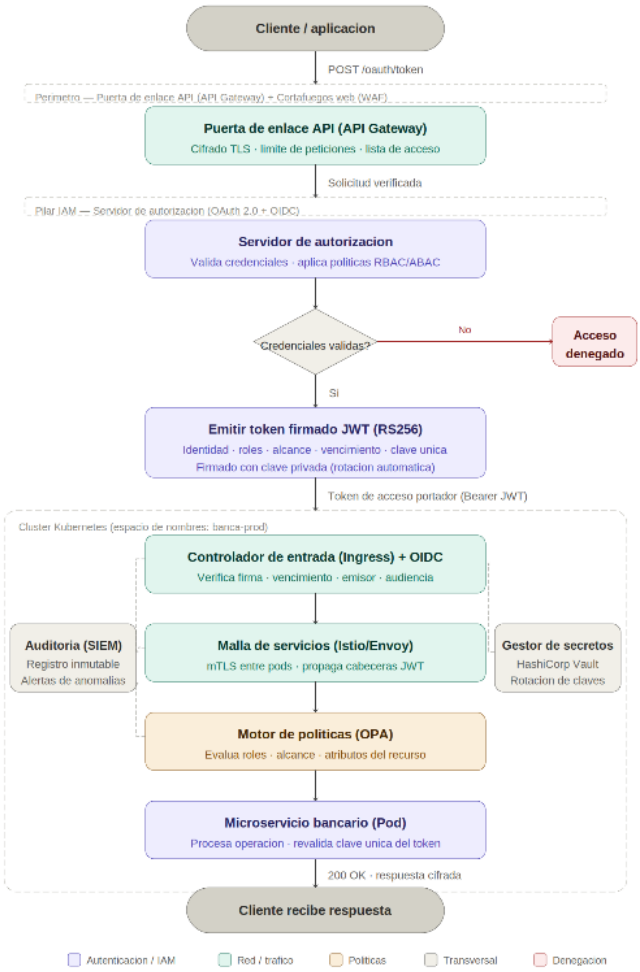
b) Implementación técnica

Con el propósito de explicar técnicamente el proceso, este acápite ilustra como los controles conceptuales descritos en la sección anterior se implementan concretamente en una arquitectura de microservicios sobre Kubernetes, trazando el ciclo de vida de un token de acceso OAuth 2.0 desde la autenticación del cliente hasta la ejecución de la operación bancaria.

Este caso de uso corresponde al escenario propuesto por el modelo PROBAN para la mitigación de riesgos en entornos de contenedores. La Figura 4 ilustra la implementación concreta de estos controles en una arquitectura de microservicios sobre Kubernetes, trazando el ciclo de vida de un token de acceso OAuth 2.0 desde la autenticación del cliente hasta la ejecución de la operación bancaria.

Figura 4

Flujo técnico del token de acceso



Nota: Elaboración propia (2026).

c) Correlación Controles Conceptuales e implementación técnica

La alineación entre el modelo conceptual y su implementación real es una decisión consciente del proceso de diseño del modelo PROBAN. Cada control en el Pilar 4 tiene un componente tecnológico, que manifiesta el principio en la arquitectura de microservicios, de modo que ningún principio se enuncia sin una medida para aplicarlo. El inicio de sesión único y la autenticación multifactor se centran en el servidor de autorización, que asume el papel de árbitro de identidad en el clúster antes de cualquier acceso desde dentro. El control de acceso basado en roles no se realiza mediante un sistema externo ni se basa únicamente en la configuración por servicio; es más, está codificado en el token firmado que lleva el solicitante, por lo que cada vez que se realiza una nueva solicitud, el motor de políticas la analiza sin recurrir a evadir un problema de autorización. Más bien, la evaluación de riesgo adaptativa está en curso: el propio token es lo suficientemente corto como para requerir una autenticación periódica, y la malla de servicios impone el cifrado mutuo en cada comunicación entre los componentes, por lo que cada transacción interna se convierte en un mecanismo de verificación independiente e incremental. Por otro lado, la gestión de acceso privilegiado cierra el ciclo en la capa más profunda; el propio microservicio rechazará el token con una clave única comprometida o revocada, incluso si esa clave única no ha sido detectada en las capas anteriores. La consecuencia es una cadena de controles, de modo que la falla de un eslabón no significa que el sistema esté comprometido, ya que cada capa valida de manera independiente lo que las anteriores ya han validado.

La tabla 8 establece la correspondencia entre ambos niveles de abstracción, como se muestra a continuación:

Tabla 8

Correlación Controles Conceptuales e implementación técnica

Control IAM	Función dentro del modelo
SSO / OIDC	Implementado mediante el servidor de autorización con protocolo OAuth 2.0 y OpenID Connect (OIDC). Centraliza la emisión de credenciales para todos los microservicios, eliminando autenticaciones individuales por servicio.
MFA	Integrado en el proceso de validación de credenciales del servidor de autorización. Antes de emitir el token, el servidor verifica los factores configurados. Un intento fallido retorna HTTP 401 y genera un evento en la auditoria (SIEM).
RBAC	Codificado dentro del token JWT mediante los atributos de roles y alcance (scope). El motor de políticas OPA evalua estos atributos en cada solicitud para determinar si el rol del solicitante tiene acceso al recurso especifico.
Evaluación adaptativa	Ejecutada por el controlador de entrada Ingress (verifica firma, vencimiento y audiencia del token) y la malla de servicios Istio/Envoy (cifrado mTLS entre pods). El token tiene una duración máxima de 15 minutos, forzando reevaluación continua.

Control IAM	Función dentro del modelo
PAM	Implementado en la capa del microservicio bancario mediante revalidación de la clave única del token (jti) contra una lista de tokens revocados, previniendo ataques de reutilización incluso con tokens aún vigentes.

d) Descripción del flujo técnico

El flujo representado en la Figura 4 se desarrolla en ocho etapas. Las primeras dos corresponden al perímetro de seguridad externo al clúster, y las siguientes cinco ocurren dentro del entorno Kubernetes:

- Etapa 1 Solicitud de autenticación: el cliente presenta sus credenciales mediante una petición HTTPS al punto de entrada. La puerta de enlace API aplica terminación TLS, control de tasa de peticiones y filtrado perimetral (WAF) antes de permitir el paso.

- Etapa 2 Emisión del token: el servidor de autorización valida las credenciales, aplica las políticas RBAC y ABAC, y emite un token JWT firmado digitalmente con el algoritmo RS256. El token contiene la identidad, el rol, el alcance de permisos, el tiempo de vencimiento y una clave única de uso irrepetible.

- Etapa 3 Presentación del token: el cliente incluye el token en el encabezado de autorización de todas sus solicitudes posteriores a la API bancaria.

- Etapa 4 Verificación en el controlador de entrada: el controlador verifica la firma criptográfica del token, su vigencia temporal, el emisor y la audiencia declarada. Las solicitudes con token invalido son rechazadas sin alcanzar ninguna capa interna.

- Etapa 5 Comunicación cifrada entre pods: la malla de servicios impone cifrado mutuo (mTLS) entre todos los microservicios del clúster, garantizando que ningún servicio pueda ser alcanzado sin un certificado de identidad valido.

- Etapa 6 Evaluación de políticas: el motor de políticas OPA evalua en tiempo real si los atributos del token autorizan la operación solicitada sobre el recurso especifico.

- Etapa 7 Procesamiento de la operación: el microservicio bancario revalida la clave única del token y ejecuta la lógica de negocio únicamente si todas las capas anteriores han sido superadas.

- Etapa 8 Registro de auditoria: cada evento significativo autenticaciones, rechazos, accesos a recursos críticos, se registra de forma inmutable en el sistema de auditoria (SIEM) para su análisis posterior.

Los componentes transversales del diagrama, como el gestor de secretos (HashiCorp Vault) y el sistema de auditoria (SIEM), actúan de forma paralela al flujo principal. El gestor de secretos provee las claves públicas de verificación (JWK) al controlador de entrada y rota automáticamente las claves privadas del servidor de autorización. El SIEM recibe eventos de todas las capas, aplica reglas de correlación y emite alertas ante anomalías que puedan indicar un intento de compromiso.

La arquitectura implementa el principio de defensa en profundidad, es decir si un atacante que logra evadir una capa aún debe superar las restantes. El compromiso de la puerta de enlace no otorga acceso al clúster. El robo de un token no permite su reutilización una vez expirado o revocado. La escalada de privilegios dentro del clúster queda limitada por las políticas RBAC codificadas en el propio token.

- **Pilar 5. Redes y Seguridad Perimetral (Perimeter & Network Security)**

Este pilar está orientado a resguardar el perímetro de las infraestructuras híbridas que combinan ambientes locales y servicios de nube pública. Para ello, incorpora tecnologías como firewalls de nueva generación, microsegmentación, protección contra ataques DDoS, sistemas IDS/IPS y mecanismos de acceso seguro como VPN y ZTNA. Su finalidad es garantizar la protección, segmentación y control del tráfico de red en entornos distribuidos.

- **Pilar 6. Operaciones de Seguridad y Respuesta a Incidentes (SOC Cloud-Céntrico)**

Este componente integra las capacidades de monitoreo, detección y respuesta ante amenazas mediante un SOC operativo 24/7, herramientas SIEM/SOAR, soluciones EDR, procesos de gestión de vulnerabilidades, inteligencia de amenazas y planes de continuidad del negocio. Su implementación contribuye a disminuir el tiempo de exposición frente a incidentes y fortalecer la capacidad de respuesta en infraestructuras cloud.

- **Pilar 7. Gestión de Incidentes (Incident Response)**

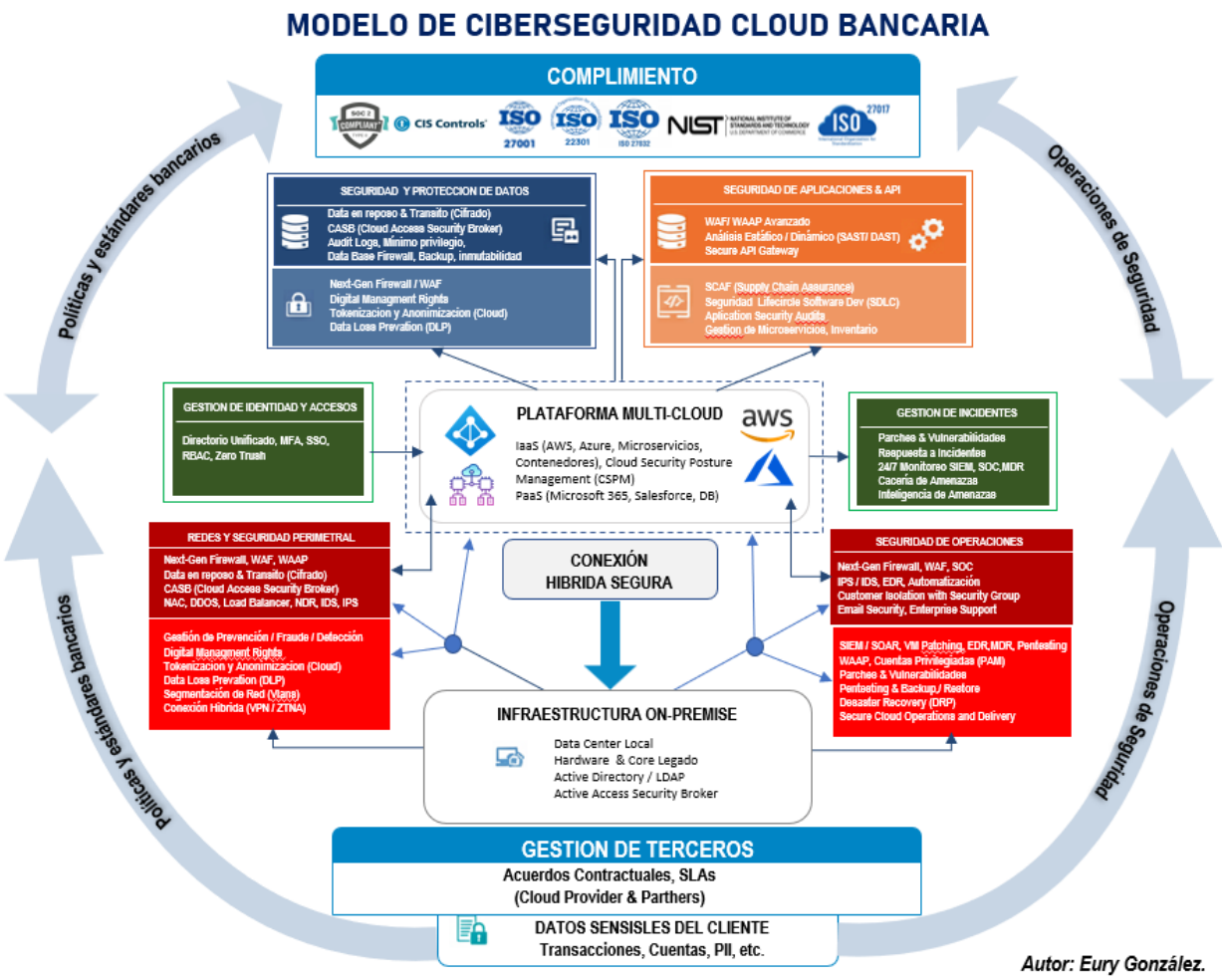
Este pilar establece un esquema organizado para la administración de incidentes de seguridad en entornos cloud, apoyándose en playbooks especializados, gestión de vulnerabilidades, actividades de threat hunting y coordinación con proveedores de servicios en la nube. Su propósito es reducir los impactos operativos, financieros y reputacionales derivados de incidentes de ciberseguridad.

- **Pilar 8. Arquitectura Híbrida y Gestión de Terceros (Hybrid Cloud & Third-Party Risk)**

Este pilar se enfoca en garantizar la seguridad de las arquitecturas híbridas y en administrar los riesgos asociados a terceros. Incluye la integración segura de servicios IaaS, PaaS y SaaS, la gestión de contratos, el monitoreo de proveedores y la protección de la información sensible de los clientes, asegurando un adecuado control sobre los servicios externos utilizados por las entidades bancarias. El modelo propuesto incorpora niveles de madurez, un mapa de controles alineado con NIST CSF 2.0 e ISO/IEC 27017, flujos operativos, requerimientos técnicos y métricas de desempeño para la evaluación continua. Su estructura permite que las instituciones bancarias dominicanas lo utilicen como una guía estratégica y operativa para fortalecer la gestión de la ciberseguridad en ambientes cloud (ver Figura 5).

Figura 5

Modelo de Protección Bancaria en la Nube (PROBAN)



Nota: Elaboración propia (2026).

4.1.5 Validación del modelo por juicio de expertos

Su validación (Tabla 10) correspondió al indicador "validación por expertos" y se obtuvo mediante el instrumento de validación (Apéndice C), aplicado a un panel de cinco expertos (Tabla 11), sobre los once ítems distribuidos en las cuatro dimensiones evaluadas: relevancia, aplicabilidad, efectividad y coherencia, alcanzando un índice de validez de contenido de 0.98 por dimensión (Tabla 12), clasificado como excelente según la escala de interpretación adoptada (Tabla 13).

Con el propósito de validar el modelo de gestión de ciberseguridad presentado en el apartado anterior, se aplicó la guía de entrevista semiestructurada descrita en la metodología a un panel de cinco (5) expertos en ciberseguridad y tecnología, seleccionados por su experiencia profesional en el sector bancario y tecnológico dominicano. La tabla 9 resume el perfil de los expertos consultados.

Tabla 9

Perfil de los expertos consultados

Experto	Perfil	Años de experiencia
E1	Gerente de Ciberseguridad de entidad bancaria	15
E2	Consultor en Seguridad Cloud e ISO 27001	18
E3	Auditor de TI especializado en riesgo tecnológico	14
E4	Especialista en Infraestructura Cloud y Arquitectura Empresarial	12

Cada experto evaluó el modelo mediante una escala likert de 1 (totalmente en desacuerdo) a 5 (totalmente de acuerdo), sobre once (11) afirmaciones distribuidas en cuatro dimensiones: relevancia, aplicabilidad, efectividad y coherencia. Dado el tamaño reducido del panel de expertos (n=5), se optó por el índice de validez de contenido (IVC) como métrica principal de validación, por ser el procedimiento recomendado para estudios de juicio de expertos con muestras reducidas (Lawshe, 1975), en lugar de coeficientes de confiabilidad diseñados para muestras de mayor tamaño.

a) Estadísticos descriptivos por dimensión

Para cada dimensión, se calculó el promedio de las respuestas otorgadas por cada experto a los ítems correspondientes, obteniendo así un puntaje individual por dimensión que permite estimar su tendencia central y dispersión. La Tabla 10 presenta los estadísticos descriptivos resultantes.

Tabla 10

Estadísticas descriptivas de la validación por dimensión

Dimensión	Media	Mediana	Desviación estándar
Relevancia	4.80	5.00	0.30
Aplicabilidad	4.33	4.33	0.47
Efectividad	4.60	4.67	0.37
Coherencia	4.70	5.00	0.45
Índice Global del Modelo	4.61		

Los resultados evidencian una valoración consistentemente alta en las cuatro dimensiones, con un índice global del modelo de 4.61 sobre 5, siendo la relevancia la dimensión mejor valorada (M=4.80) y la aplicabilidad la que presentó mayor variabilidad entre expertos (DE=0.47). De acuerdo con la escala de interpretación adoptada (Tabla 11), este resultado se clasifica como modelo altamente validado.

Tabla 11

Escala de interpretación del índice global del modelo

Dimensión	Interpretación
4.50 - 5.00	Modelo altamente validado
4.00 - 4.49	Modelo validado
3.50 – 3.99	Aceptable con mejoras
< 3.50	Requiere rediseño

b) Índice de validez de contenido (IVC)

El IVC se calculó como la proporción de respuestas individuales (expertos × preguntas) calificadas con 4 o 5 dentro de cada dimensión. La Tabla 12 presenta los resultados obtenidos.

Tabla 12

Índice de validez de contenido por dimensión

Dimensión	IVC
Relevancia	1.00
Aplicabilidad	0.93
Efectividad	1.00
Coherencia	1.00

IVC Global	0.98

De acuerdo con la escala de interpretación adoptada (Tabla 13), un IVC Global de 0.98 se clasifica como excelente validez de contenido, confirmando que el modelo propuesto es considerado válido y pertinente por el panel de expertos consultado.

Tabla 13

Escala de interpretación del índice de validez de contenido

Rango	Interpretación
0.90 – 1.00	Excelente validez de contenido
0.80 – 0.89	Buena validez de contenido
0.70 – 0.79	Validez aceptable; se recomienda revisar algunos aspectos
< 0.70	Validez insuficiente; requiere modificaciones

c) Conclusión de la validación

Con base en los resultados obtenidos, el modelo de gestión de ciberseguridad para la infraestructura cloud del sistema bancario de la República Dominicana fue validado por el panel de expertos consultado, con un índice de validez de contenido global de 0.98 y un índice global del modelo de 4.61 sobre 5, confirmando su relevancia, aplicabilidad, efectividad y coherencia para el contexto bancario dominicano.

4.1.6 Estimación de costos de implementación y operación del modelo PROBAN

La implementación del modelo PROBAN implica inversiones diferenciadas según el tamaño de la entidad bancaria (pequeña, mediana o grande), dado que los ocho pilares del modelo requieren combinaciones distintas de tecnología, personal especializado y servicios gestionados. La siguiente estimación se basa en precios de mercado de proveedores de tecnología de ciberseguridad y servicios de seguridad gestionados disponibles públicamente al momento de esta investigación, y debe interpretarse como un rango referencial orientativo, no como el costo real incurrido por las entidades participantes en el estudio, dado que dicha información no fue objeto de medición empírica en este trabajo.

Tabla 14

Estimación de costos de implementación por pilar (Inversión inicial)

Pilar	Componente principal	Entidad pequeña	Entidad mediana	Entidad grande
P1. Cumplimiento	Consultoría de gobernanza, gap análisis, documentación de políticas	US$15,000 – 30,000	US$30,000 – 60,000	US$60,000 – 120,000
P2. Seguridad y Protección de Datos	Cifrado, tokenización, gestión de llaves (KMS)	US$10,000 – 25,000	US$25,000 – 60,000	US$60,000 – 150,000
P3. Seguridad de Aplicaciones y APIs	WAF/WAAP, herramientas SAST/DAST	US$10,000 – 20,000	US$20,000 – 50,000	US$50,000 – 120,000

P4. IAM y Zero Trust	Plataforma IAM, MFA, PAM	US$15,000 – 35,000	US$35,000 – 80,000	US$80,000 – 200,000
P5. Redes y Seguridad Perimetral	Firewalls NGFW, microsegmentación, ZTNA	US$20,000 – 40,000	US$40,000 – 90,000	US$90,000 – 200,000
P6. SOC y Monitoreo	Implementación de plataforma SIEM/SOAR	US$20,000 – 50,000	US$50,000 – 120,000	US$120,000 – 300,000
P7. Gestión de Incidentes	Playbooks, herramientas de threat hunting, simulacros	US$8,000 – 15,000	US$15,000 – 35,000	US$35,000 – 80,000
P8. Arquitectura Híbrida y Gestión de Terceros	CASB, CSPM, auditoría de proveedores	US$15,000 – 30,000	US$30,000 – 70,000	US$70,000 – 160,000
Subtotal implementación		**US$113,000 – 245,000**	**US$245,000 – 565,000**	**US$565,000 – 1,330,000**

Nota. Valores expresados en dólares estadounidenses (US$).

Tabla 15

Costos operativos anuales (recurrentes, a partir del año 2)

Categoría	Entidad pequeña	Entidad mediana	Entidad grande
Licenciamiento y suscripciones (SIEM/SOAR, CASB, IAM, WAF)	US$40,000 – 90,000/año	US$90,000 – 220,000/año	US$220,000 – 500,000/año
Personal especializado (1-2 FTE en entidades pequeñas/medianas; equipo SOC dedicado en grandes)	US$60,000 – 120,000/año	US$150,000 – 300,000/año	US$400,000 – 800,000/año
Servicios gestionados de SOC (SOCaaS), si se terceriza en lugar de personal interno	US$24,000 – 84,000/año	US$84,000 – 300,000/año	US$300,000 – 600,000/año
Auditorías, capacitación y certificaciones (ISO 27001, simulacros)	US$10,000 – 20,000/año	US$20,000 – 40,000/año	US$40,000 – 80,000/año

Nota. Valores expresados en dólares estadounidenses (US$).

4.2 Análisis

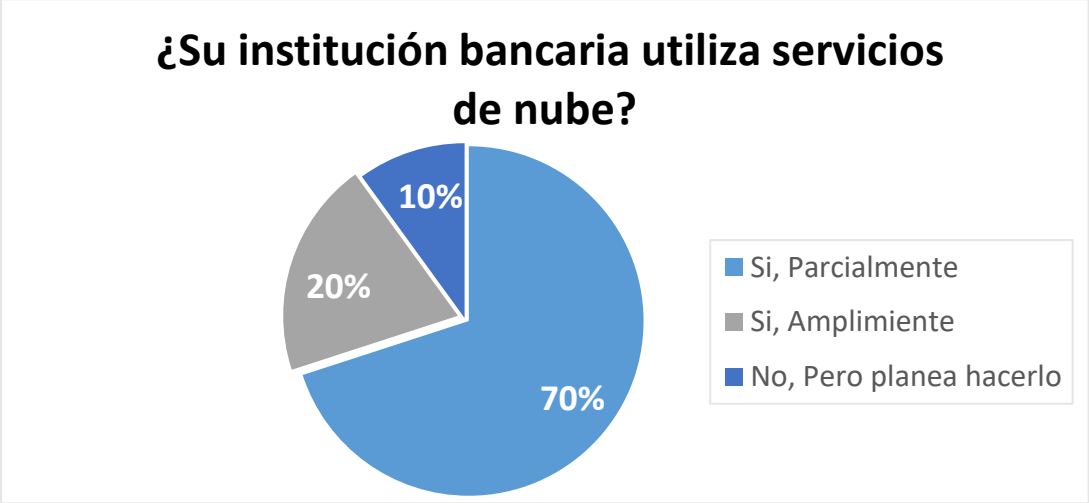
4.2.1 Adopción de servicios en la nube en el sector bancario

Los resultados evidencian que la adopción de servicios en la nube en el sector bancario dominicano se encuentra en una fase de transición controlada. El 70% de las organizaciones encuestadas ha iniciado parcialmente la adopción de servicios cloud, principalmente en áreas no críticas, lo que sugiere una estrategia prudente orientada a capturar beneficios sin comprometer de forma inmediata procesos sensibles. Este comportamiento suele asociarse a necesidades de integración con sistemas heredados, exigencias de pruebas de seguridad y condicionantes de cumplimiento normativo, particularmente relevantes en organizaciones reguladas.

Por su parte, un 20% reporta un uso amplio de la nube, lo que es indicativo de una adopción más madura, con probables migraciones de cargas críticas, modernización tecnológica y mayores niveles de eficiencia operativa. Finalmente, el 10% restante indica que no planea adoptar la nube en lo inmediato, aunque mantiene intención futura, lo cual sugiere que la decisión está condicionada por restricciones internas (capacidad técnica, recursos, y/o gobernanza). En conjunto, el predominio de adopciones parciales confirma que persisten retos de madurez tecnológica, seguridad y gestión del riesgo; al mismo tiempo, configura una oportunidad concreta para fortalecer la transición mediante marcos de referencia y estándares internacionales, asegurando una adopción segura y conforme. (ver Figura 6)

Figura 6

Utilización de servicios en la nube.



Nota: Elaboración propia (2026).

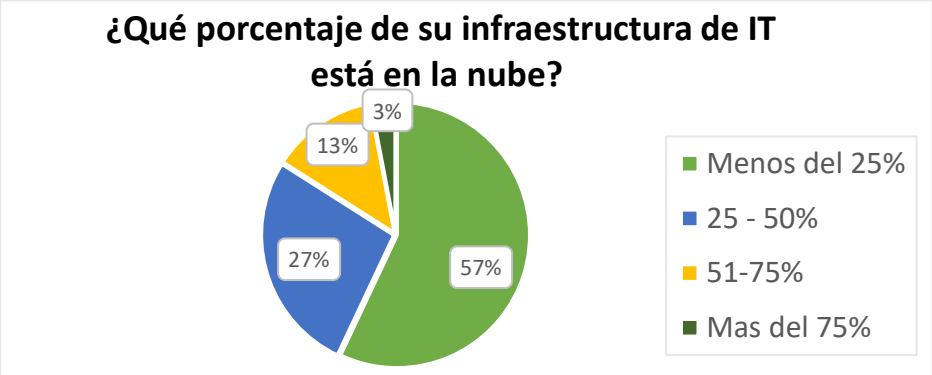
4.2.2 Infraestructura tecnológica en la nube

La distribución del porcentaje de infraestructura tecnológica alojada en la nube confirma una adopción predominantemente limitada. Un 57% de las organizaciones indica que menos del 25% de su infraestructura se encuentra en cloud, mientras que un 27% se sitúa entre 25% y 50%. Solo un 13% reporta niveles entre 51% y 75%, y apenas un 3% supera el 75% de infraestructura migrada.

Este patrón sugiere que los modelos híbridos continúan predominando, probablemente por preocupaciones de seguridad y cumplimiento, costos de migración, dependencia de infraestructura local y complejidad de integración tecnológica. En términos analíticos, los datos muestran que, aunque existe una dirección clara hacia cloud, la consolidación de una postura madura de seguridad cloud aún no se materializa de forma homogénea en el sector. (ver Figura 7)

Figura 7

Infraestructura tecnológica en la nube



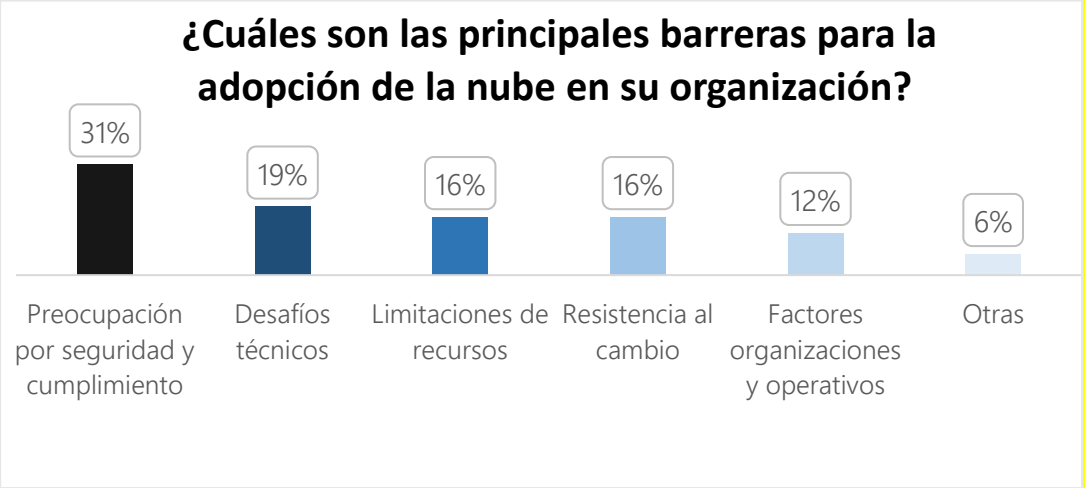
Nota: Elaboración propia (2026).

4.2.3 Barreras y desafíos técnicos para la adopción cloud

La principal barrera identificada para la adopción cloud es la seguridad y el cumplimiento, señalada por el 31% de los encuestados, lo que confirma que el componente regulatorio y la protección de datos constituyen el freno más relevante. En segundo lugar, los desafíos técnicos representan un 19%, lo que sugiere limitaciones relacionadas con capacidades tecnológicas, conocimiento especializado e integración de plataformas. Asimismo, las limitaciones de recursos y la resistencia al cambio (16% cada una) evidencian que existen barreras presupuestarias y culturales que afectan el ritmo de adopción. Los aspectos organizacionales y operativos corresponden al 12% de los factores identificados, mientras que otras causas representan un 6% (ver Figura 8).

Figura 8

Barreras de adopción de la nube en las entidades bancarias



Nota: Elaboración propia (2026).

Los resultados obtenidos evidencian que la adopción de servicios en la nube dentro del sector bancario no debe considerarse únicamente como una iniciativa tecnológica, sino como un proceso integral que demanda una adecuada gestión de riesgos, cumplimiento regulatorio, fortalecimiento de capacidades internas y cambios organizacionales.

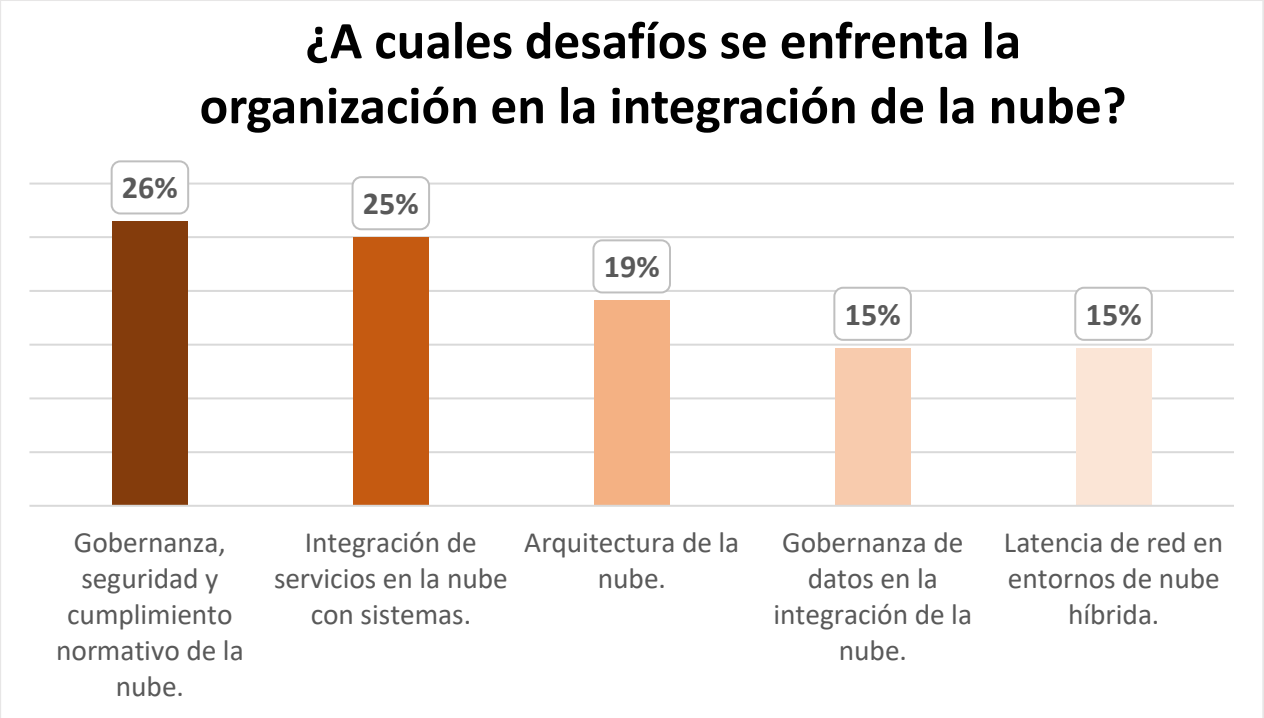
En términos de desafíos específicos de integración, los resultados muestran que el reto principal es la gobernanza, seguridad y cumplimiento normativo (26%), seguido muy de cerca por la integración con sistemas existentes (25%), lo que sugiere dificultades de interoperabilidad entre entornos tradicionales y cloud. La arquitectura de la nube representa un 19%, indicando complejidades de diseño, escalabilidad y estandarización. Finalmente, la gobernanza de datos y la

latencia de red en entornos híbridos (15% cada una) revelan preocupaciones asociadas al control del dato y el rendimiento operativo.

En conjunto, los datos evidencian una transición cloud condicionada por retos técnicos multidimensionales, lo que refuerza la necesidad de enfoques de ciberseguridad integrales, no limitados a controles aislados. (ver Figura 9)

Figura 9

Desafíos que enfrenta la organización en la integración de la nube



Nota: Elaboración propia (2026).

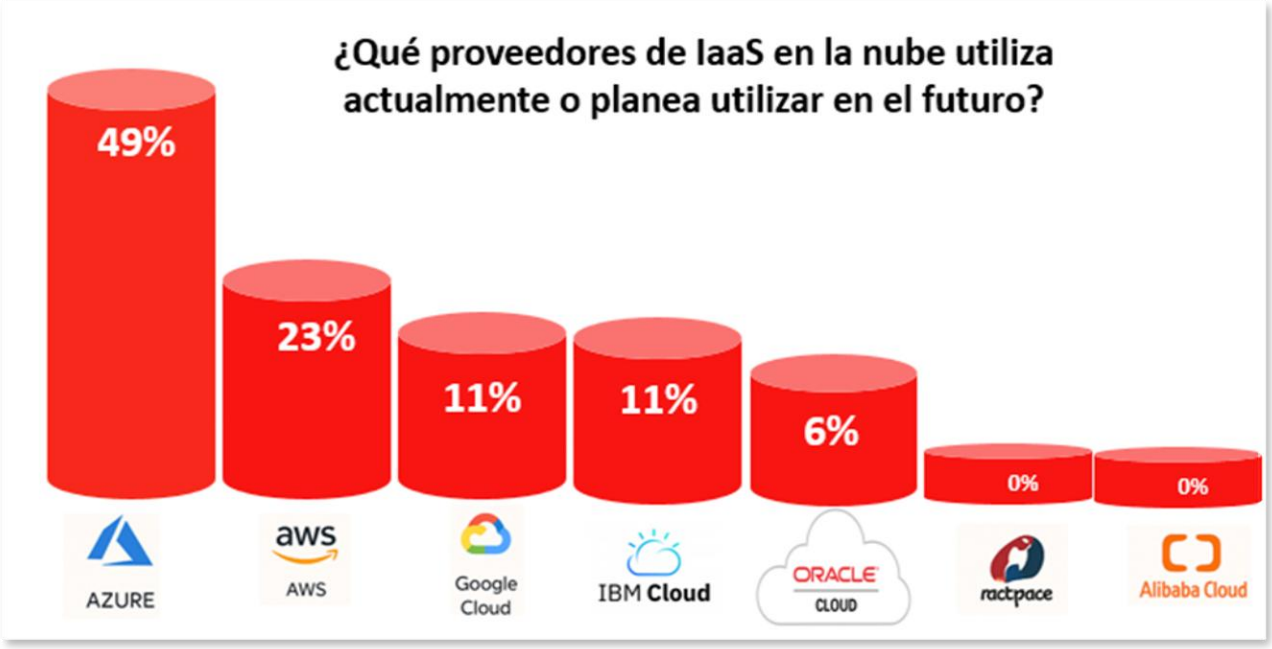
4.2.4 Proveedores cloud y concentración tecnológica (IaaS)

Los proveedores de servicios cloud utilizados presentan una clara concentración. Microsoft Azure lidera con 49%, seguido por AWS con 23%. Google Cloud e IBM Cloud registran 11% cada uno, mientras que Oracle Cloud alcanza 6%. La ausencia de participación de Rackspace y Alibaba Cloud (0%) sugiere baja penetración en este segmento.

Este hallazgo es relevante desde la perspectiva de riesgo tecnológico y continuidad, dado que la concentración en pocos proveedores puede aumentar la dependencia tecnológica y el impacto potencial ante fallos sistémicos o incidencias operativas. (ver Figura 10)

Figura 10

Proveedores IaaS utilizados por las entidades bancarias



Nota: Elaboración propia (2026).

4.2.5 Controles de seguridad predominantes y madurez de prácticas cloud

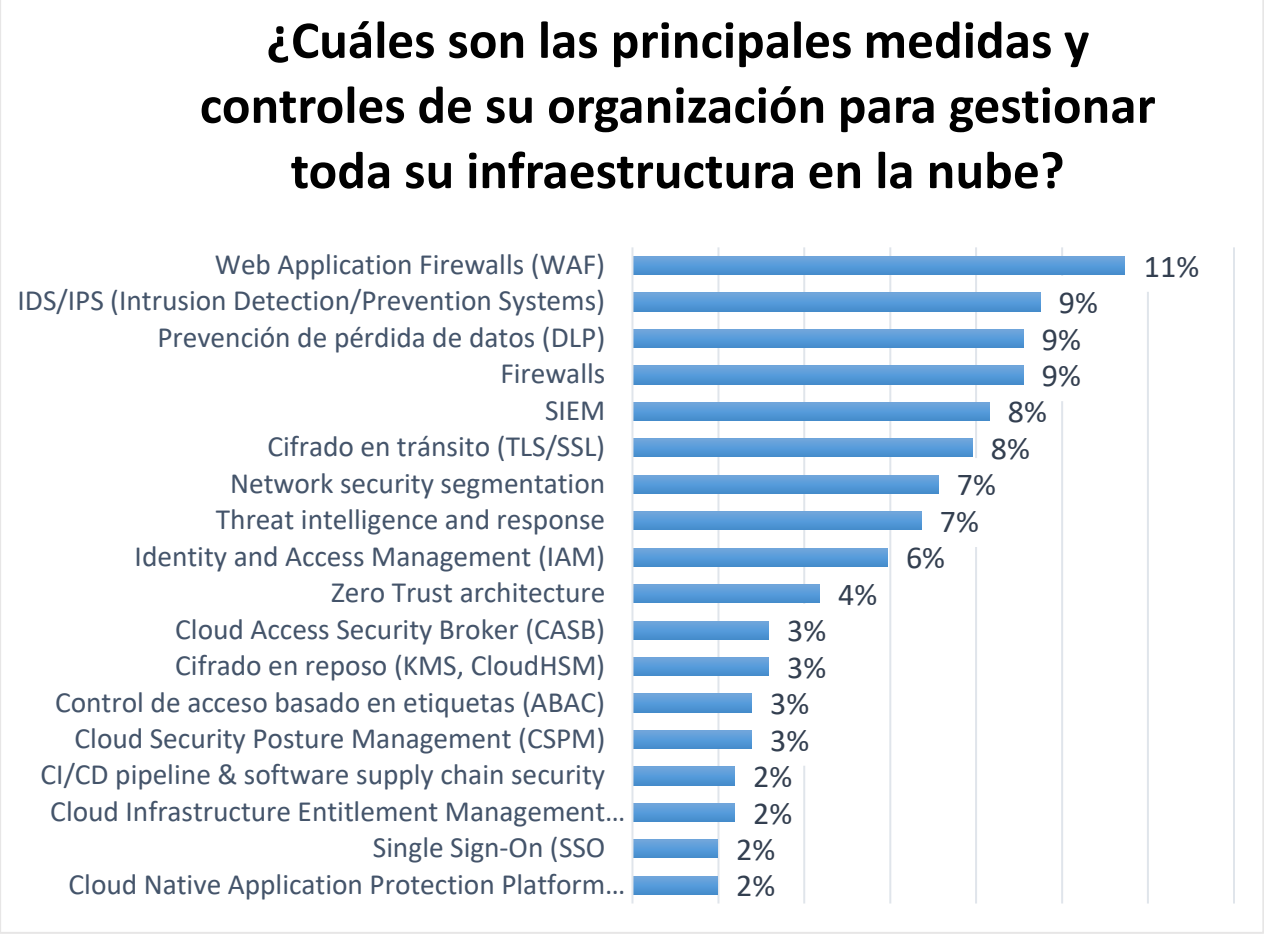
Las medidas y controles implementados para gestionar la nube muestran una priorización por mecanismos tradicionales. Los WAF lideran con 11%, seguidos por IDS/IPS, DLP y firewalls (9% cada uno). También destacan SIEM y cifrado en tránsito (TLS/SSL) con 8%, lo que confirma la relevancia de la visibilidad centralizada y la protección del tráfico.

Sin embargo, se observa una adopción significativamente menor de controles cloud-native y enfoques más modernos, tales como Zero Trust (4%), CASB (3%), CSPM (3%) y CIEM (2%). Esta brecha sugiere que el sector se encuentra en una etapa aún incipiente respecto a la implementación de prácticas orientadas a la nube, especialmente las vinculadas a gobernanza de identidades, control de configuraciones y gestión granular de privilegios.

En términos analíticos, los resultados indican un proceso de evolución progresiva hacia controles sofisticados, aunque con dependencia significativa de soluciones perimetrales tradicionales. (ver Figura 11)

Figura 11

Medidas y controles utilizados por entidades bancarias para gestionar la nube.



Nota: Elaboración propia (2026).

4.2.6 Estrategia de implementación: predominio híbrido y multinube

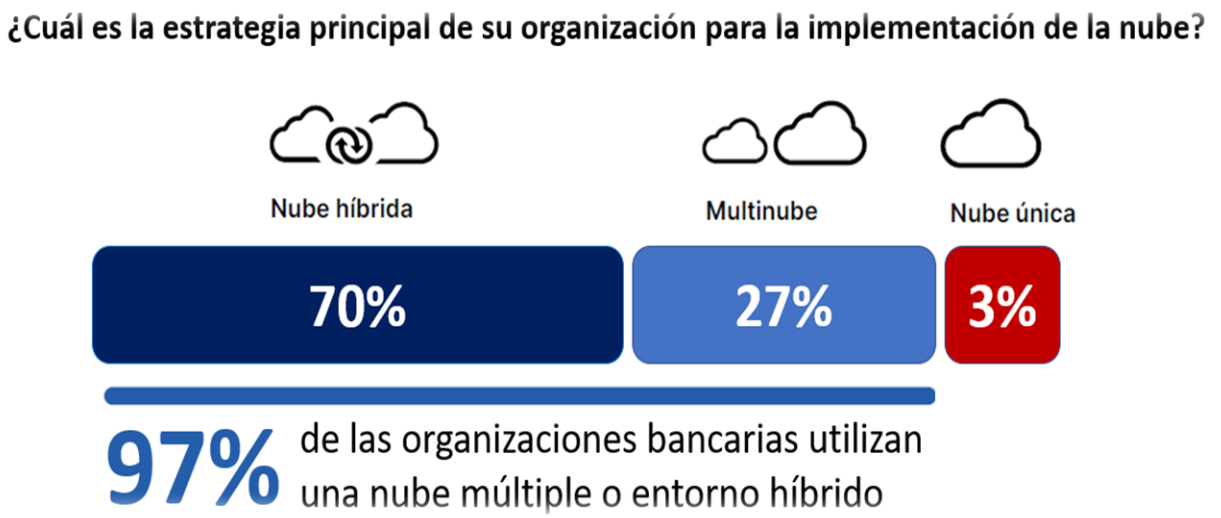
La estrategia predominante en el sector bancario dominicano es la nube híbrida, adoptada por el 70% de las entidades, lo que sugiere una preferencia por combinar infraestructura local y cloud para mantener control sobre cargas sensibles y responder a exigencias regulatorias. La

estrategia multinube representa un 27%, lo que refleja un interés relevante por diversificar proveedores, reducir dependencias y mejorar disponibilidad. Solo un 3% utiliza una nube única.

En conjunto, estos resultados confirman que el estándar de facto en el sector es operar bajo arquitecturas híbridas o multinube, lo cual incrementa la complejidad de seguridad y refuerza la necesidad de controles de gobernanza, visibilidad y estandarización transversal. (ver Figura 12)

Figura 12

Estrategia de implementación de nube.



Nota: Elaboración propia (2026).

4.2.7 Priorización de seguridad y desafíos operativos (SecOps cloud)

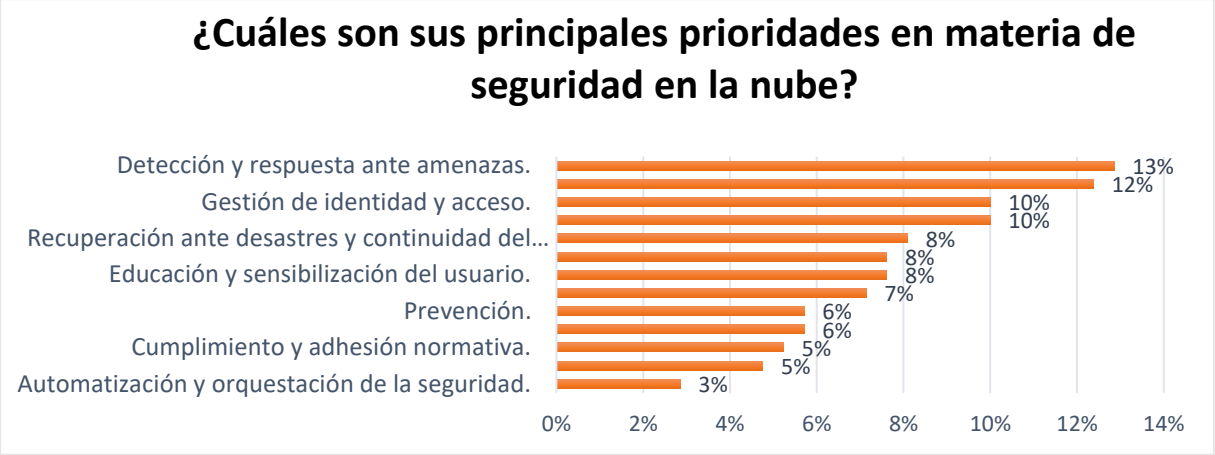
En cuanto a prioridades de seguridad, la detección y respuesta ante amenazas se posiciona como la prioridad principal (13%), seguida por seguridad y privacidad de datos (12%) y gestión de identidad y acceso (10%). Asimismo, sobresalen las capacidades de visibilidad y monitoreo integral de los entornos cloud con un 10%, junto con los aspectos relacionados con continuidad

operativa y recuperación, que representan un 8%. Estos resultados reflejan la importancia que las entidades otorgan a garantizar la supervisión constante y la disponibilidad continua de los servicios en la nube.

No obstante, la automatización y orquestación de seguridad presenta un valor bajo (3%), lo que sugiere una oportunidad clara de maduración mediante SOAR, respuesta automatizada y control continuo de configuraciones. (ver Figura 13)

Figura 13

Principales prioridades de seguridad en la nube.

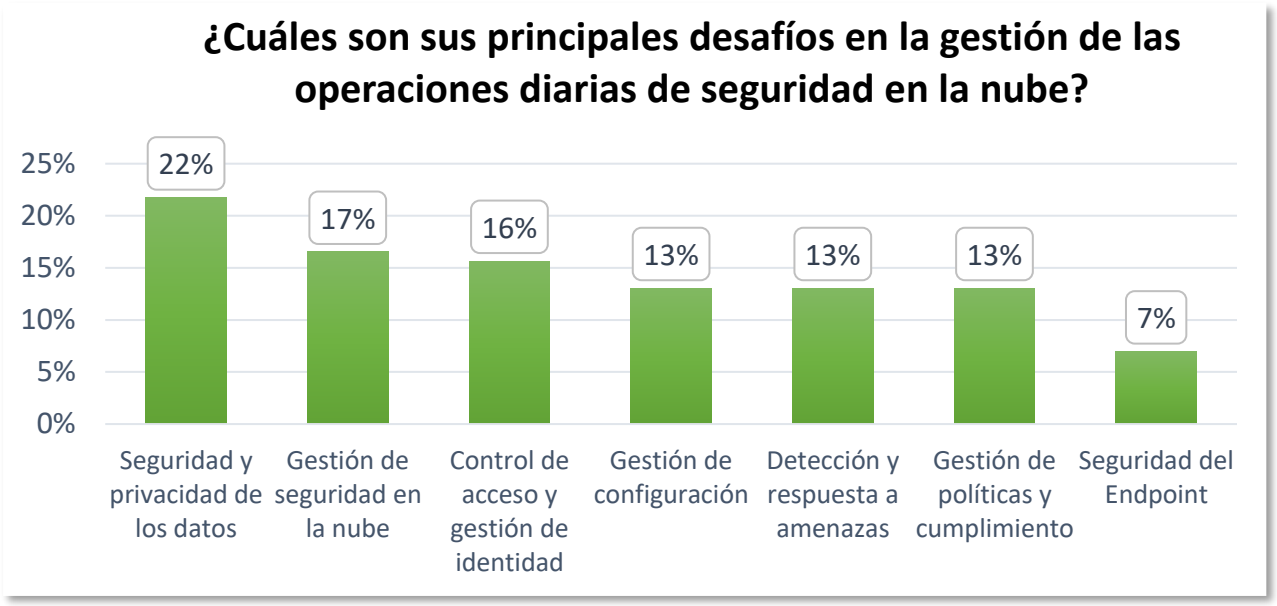


Nota: Elaboración propia (2026).

De manera complementaria, los principales desafíos en la gestión operativa de seguridad cloud se concentran en seguridad y privacidad de datos (22%), seguido por gestión de seguridad en la nube (17%) y control de acceso/identidad (16%). En un segundo nivel aparecen gestión de configuración, detección y respuesta y políticas/cumplimiento (13% cada una). Este patrón sugiere que el problema no es únicamente “tener controles”, sino asegurar su gestión continua, coherente y medible. (ver Figura 14)

Figura 14

Principales desafíos en la gestión de operaciones de seguridad en la nube.



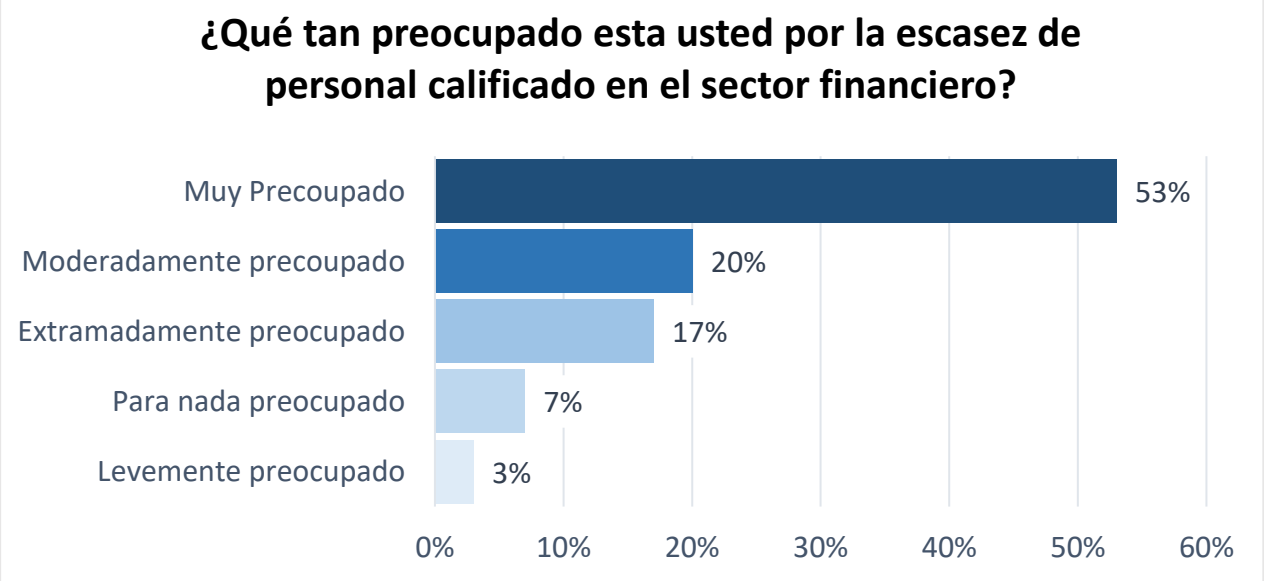
Nota: Elaboración propia (2026).

4.2.8 Talento especializado como restricción estructural

La escasez de personal calificado constituye un factor crítico: el 53% se declara “muy preocupado” y el 17% “extremadamente preocupado”, acumulando un 70% de preocupación alta. Este resultado indica que la capacidad de implementar, operar y mejorar la seguridad cloud está condicionada por la disponibilidad de talento, lo cual puede traducirse en menor capacidad de respuesta, brechas de cumplimiento y dependencia de terceros. En consecuencia, el sector requiere estrategias combinadas de formación, retención, apoyo de proveedores especializados y automatización como mitigación de la brecha de capacidades. (ver Figura 15)

Figura 15

Escasez de personal calificado en el sector financiero.



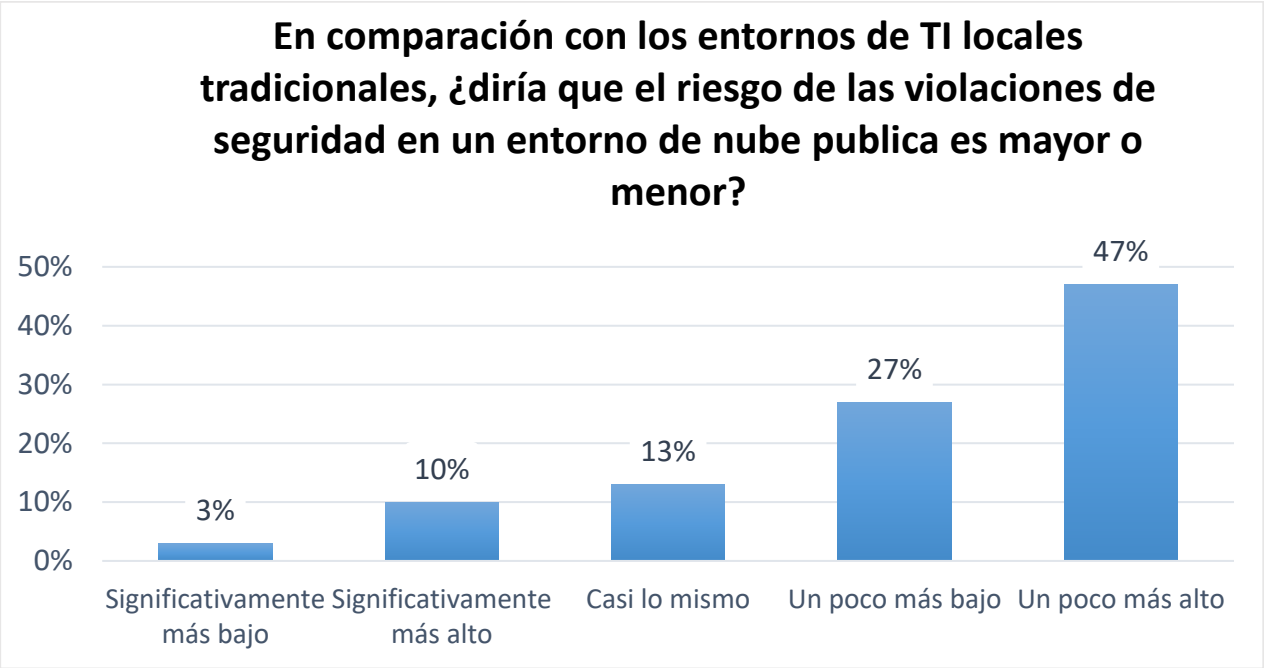
Nota: Elaboración propia (2026).

4.2.9 Percepción de riesgo cloud versus on-premise

La percepción de riesgo en nube pública continúa siendo superior a la del entorno local: el 47% considera que el riesgo es “un poco más alto” y el 10% “significativamente más alto”. Solo un 3% lo percibe más bajo y un 13% considera que es similar. Estos datos evidencian una brecha de confianza que debe mitigarse mediante seguridad demostrable (evidencia de controles), transparencia, auditoría y mecanismos de cumplimiento consistentes. (ver Figura 16)

Figura 16

Percepción del riesgo en entornos locales versus entornos de nube.



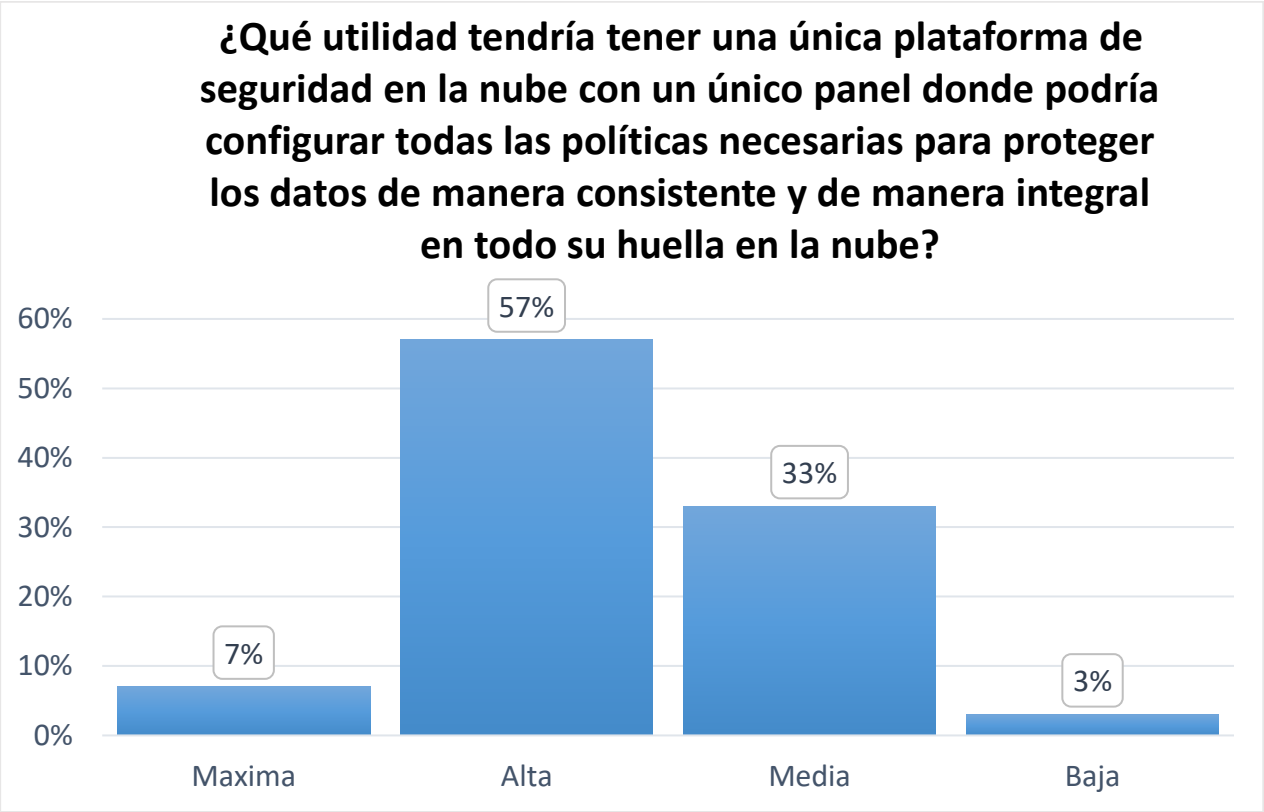
Nota: Elaboración propia (2026).

4.2.10 Consolidación y centralización de políticas como demanda del sector

La utilidad de una plataforma de seguridad cloud con panel único de configuración de políticas se percibe mayormente como alta (57%) y media (33%), lo que confirma una necesidad de centralizar gestión de políticas y reducir inconsistencias en entornos híbridos/multicloud. Las razones asociadas a utilidad media o baja reflejan desafíos de integración, resistencia cultural, herramientas heredadas y costos, lo que posiciona la estandarización como un objetivo estratégico y no meramente técnico. (ver Figura 17)

Figura 17

Utilidad plataforma de seguridad en la nube.



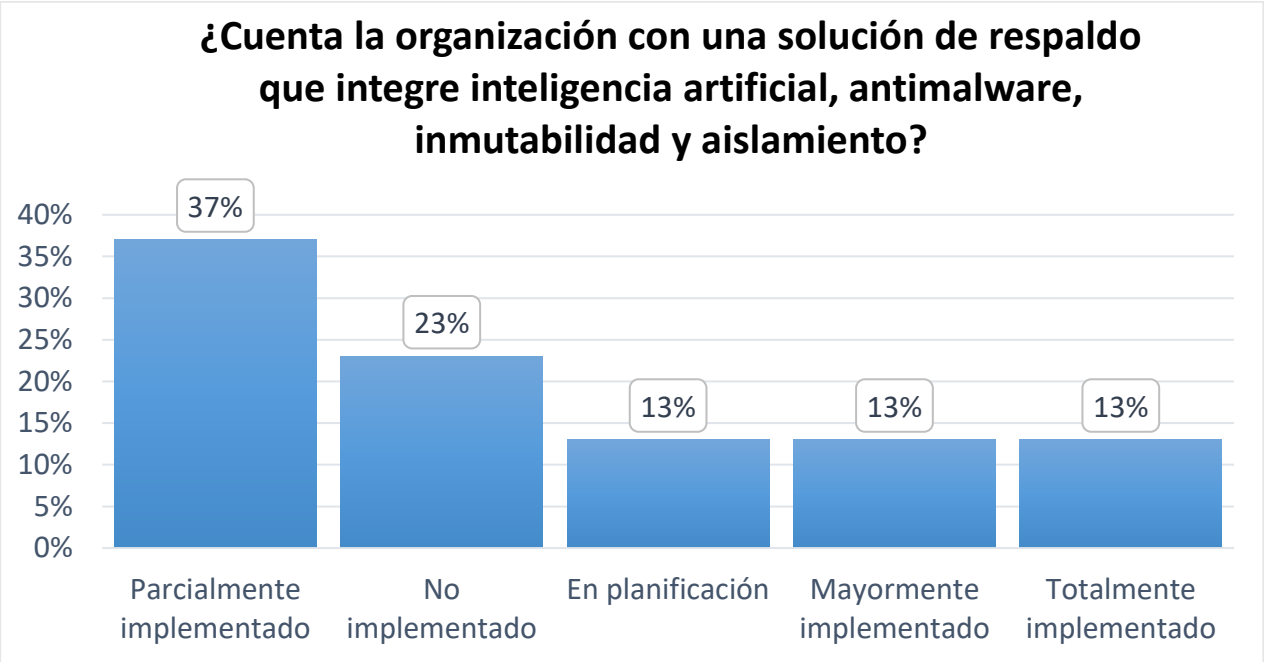
Nota: Elaboración propia (2026).

4.2.11 Resiliencia y continuidad: avances, pero con brechas tecnológicas

Los resultados sobre herramientas de seguridad para incidentes y continuidad reflejan que un 37% se encuentra en estado parcial (tecnologías aisladas sin esquema integral), y un 23% indica “no implementado”, lo que configura una exposición relevante ante ataques sofisticados. Los estados de planificación (13%) y los niveles “totalmente/mayormente implementado” (13%) evidencian brechas importantes de adopción, pero también oportunidades de diferenciación competitiva para las instituciones que invierten primero en resiliencia avanzada. (ver Figura 18)

Figura 18

Herramientas de seguridad para incidentes y continuidad del servicio

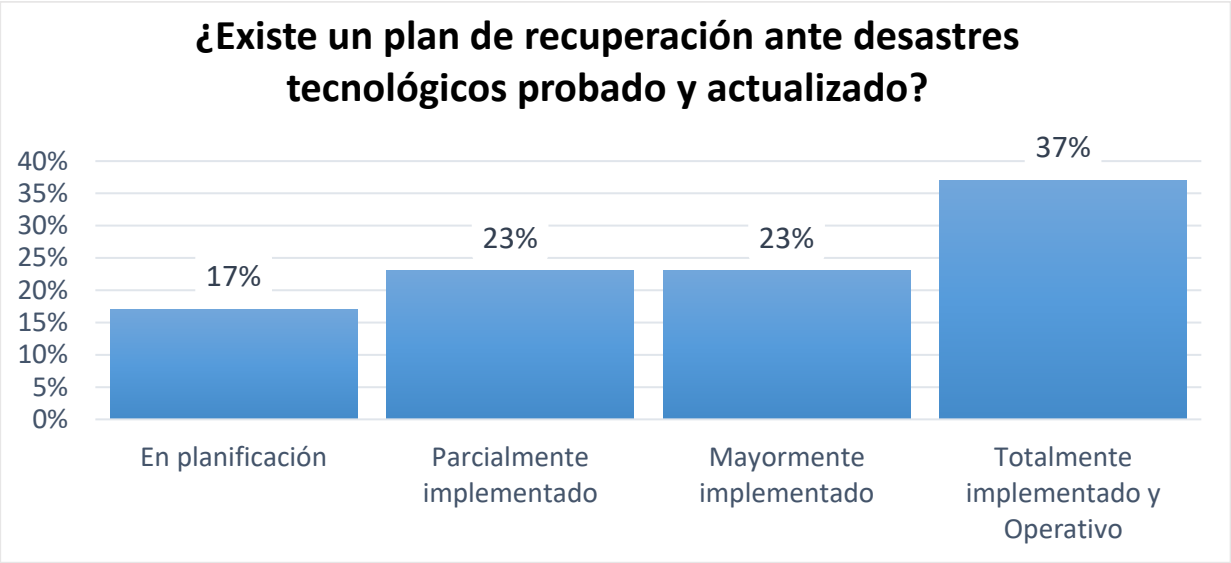


Nota: Elaboración propia (2026).

En cuanto a recuperación ante desastres tecnológicos, aunque un 37% reporta un plan operativo y probado, la presencia de estados “mayormente implementado” (23%) y “parcial” (23%) indica madurez incompleta, lo que puede afectar la efectividad en escenarios reales. El 17% en planificación representa el grupo más expuesto ante contingencias, con riesgo de interrupción prolongada, impacto financiero e incumplimiento regulatorio. (ver Figura 19)

Figura 19

Plan de recuperación ante desastres tecnológicos.



Nota: Elaboración propia (2026).

4.2.12 Madurez NIST CSF 2.0: brecha entre gobernanza y eficacia operativa

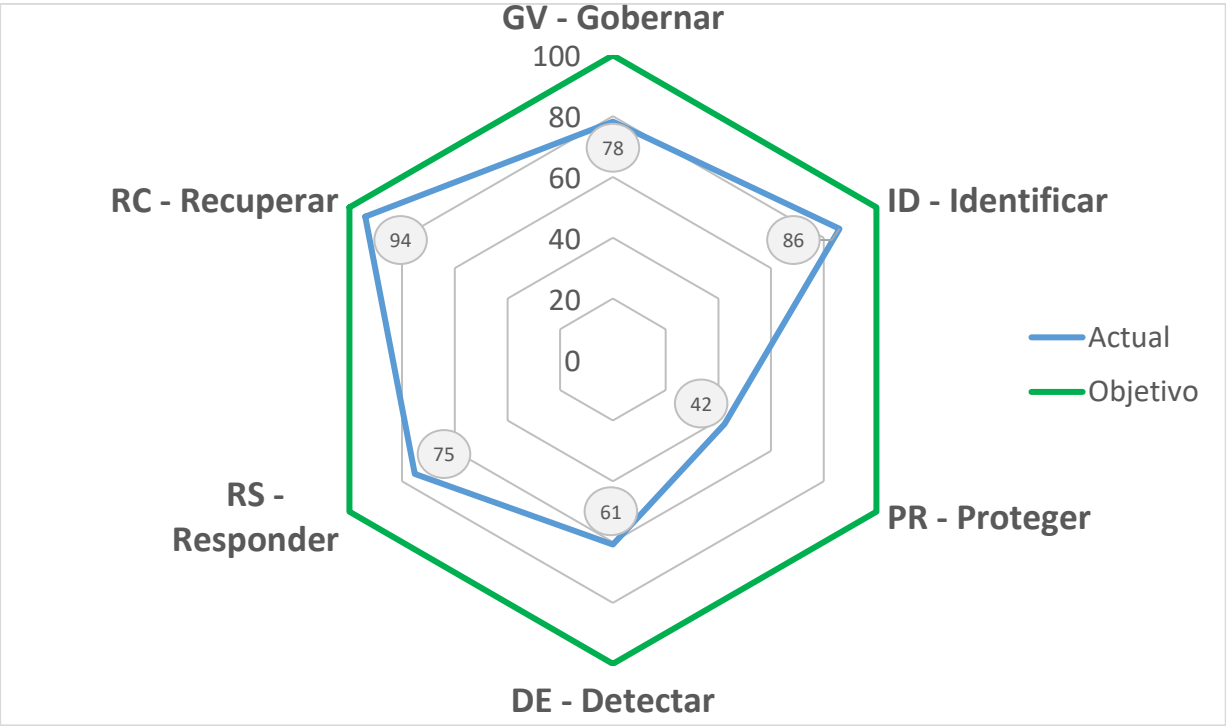
El análisis de madurez basado en las seis funciones del NIST CSF 2.0 permitió identificar una dispersión significativa entre el estado actual y el nivel objetivo (100%). Los puntajes muestran fortalezas en Recuperar (94%), Identificar (86%) y Gobernar (78%), mientras que Proteger (42%) y Detectar (61%) reflejan brechas críticas.

Esta evidencia sugiere que el sector ha priorizado históricamente componentes de continuidad, recuperación y gestión formal, alineados con exigencias regulatorias y con prácticas de gestión de seguridad, pero mantiene debilidades en controles técnicos avanzados, especialmente relevantes en cloud: segmentación, hardening, gestión automatizada de vulnerabilidades, cifrado consistente, Zero Trust e integración efectiva de telemetría cloud hacia

mecanismos de detección. De forma complementaria, la brecha entre Gobernar (78%) y Proteger (42%) sugiere una diferencia entre cumplimiento formal y eficacia operativa, particularmente crítica en entornos multicloud. (ver Figura 20)

Figura 20

Nivel de madurez de las entidades bancarias.



Nota: Elaboración propia (2026).

4.2.13 Relación resultados con el planteamiento del problema

En el contexto del sistema bancario de la República Dominicana, los hallazgos confirman que, aunque el sector bancario dominicano ha avanzado en adopción cloud, existe heterogeneidad significativa en madurez, controles implementados y capacidades operativas. En particular, la evidencia muestra ausencia de estandarización y debilidades técnicas en prevención y detección,

acentuadas por escasez de talento y por la complejidad inherente de arquitecturas híbridas y multinube.

En este contexto, la adopción de marcos internacionales (NIST, ISO/IEC 27001–27017) aporta fundamentos sólidos, pero su implementación efectiva se ve limitada por capacidades internas y por la necesidad de adaptarlos a condiciones regulatorias y operativas específicas del país. Estos hallazgos justifican la construcción de un modelo integral, que traduzca marcos y estándares en pilares operativos, con mecanismos medibles, roles claros, gobierno robusto y tecnologías habilitadoras orientadas a reducir brechas en Proteger y Detectar.

4.3 Discusión

Los resultados de 4.2 indicaron que las entidades bancarias participantes en el estudio adoptan servicios en la nube de manera híbrida y progresiva, con una alta dependencia de proveedores de tecnología líderes y una migración parcial de infraestructura. En este contexto, se indica que la seguridad de la información y el cumplimiento normativo parecen estar moldeando la transformación digital de las entidades evaluadas, en lugar de proporcionar elementos complementarios. Así, el análisis va más allá de explicar los niveles de adopción y busca comparar la madurez correspondiente a la gobernanza, identificación y recuperación, el nivel operativo vinculado a la protección y detección, una situación que fue descrita en literatura específica y organizaciones internacionales de ciberseguridad dentro de sectores críticos. A la luz del Marco de Ciberseguridad NIST 2.0, los resultados demuestran diferencias significativas entre las funciones evaluadas. Las puntuaciones de Recuperación (94%), Identificación (86%) y Gobernanza (78%) están por encima de los niveles de madurez, mientras que Protección (42%) y

Detección (61%) están por debajo, dentro de la muestra estudiada. La importancia radica, sin embargo, en que el modelo NIST concibe la ciberseguridad como un proceso integral y equilibrado, que se basa en la adquisición de capacidades preventivas y la detección temprana de incidentes de seguridad, con el propósito de evitar que la gestión de los incidentes dependa principalmente de actividades de respuesta y recuperación. Por lo tanto, los resultados indicaron que las entidades participantes han mejorado su continuidad operativa y sistemas formales de gestión de riesgos; sin embargo, existen limitaciones en la ejecución de controles técnicos y operativos específicos de la nube. Estas limitaciones reducen la capacidad de disminuir la probabilidad de eventos de seguridad antes de que ocurran. También se demostró que, en conjunto, la mayoría de los controles aplicados por las entidades de la muestra coinciden con las estrategias tradicionales, como WAF, IDS/IPS, firewalls, DLP y sistemas SIEM. Las herramientas relacionadas con modelos de seguridad en la nube, por otro lado, como CASB, CSPM, CIEM y arquitecturas de Confianza Cero tienen una menor adopción, lo que indica un potencial para mejorar la madurez de la ciberseguridad en la nube de las entidades evaluadas. Este patrón es consistente con lo reportado por Kim et al. (2018), quienes encontraron empíricamente que las principales vulnerabilidades de la industria financiera en entornos cloud se concentran en la gestión de identidades, la configuración segura y la visibilidad de recursos, más que en la ausencia de estrategias de continuidad; y con Zárate Urgell et al. (2023), quienes documentaron en el sector financiero mexicano que los modelos de seguridad perimetral tradicionales resultan insuficientes frente a arquitecturas cloud distribuidas. Así, la evidencia empírica sugiere que las entidades estudiadas se encuentran en una transición donde la seguridad se sigue interpretando desde

paradigmas perimetrales, aun cuando la arquitectura dominante es híbrida/multicloud y, por tanto, exige mecanismos centrados en identidad, configuración continua y segmentación lógica.

Al contrastar estos hallazgos con los estándares ISO/IEC 27001:2022 e ISO/IEC 27017, se observa que las entidades participantes presentan avances significativos en dimensiones asociadas al gobierno, políticas y gestión documental, coherentes con la lógica de un sistema de gestión de seguridad de la información (SGSI). Sin embargo, ISO/IEC 27001, por su naturaleza normativa, enfatiza el establecimiento de controles y procesos de gestión, sin garantizar por sí mismo una implementación operativa efectiva en arquitecturas cloud altamente dinámicas. ISO/IEC 27017 extiende el marco hacia la nube, incorporando controles y consideraciones específicas para servicios cloud; no obstante, los resultados muestran que, entre las entidades de la muestra, la principal barrera para la adopción cloud es precisamente la seguridad y el cumplimiento, y que la baja madurez en Proteger y Detectar no se explica por ausencia de marcos normativos, sino por dificultades de operacionalización: integración con sistemas heredados, gobernanza de datos, complejidad arquitectónica, escasez de personal especializado y limitaciones para centralizar políticas en entornos híbridos y multinube. Por tanto, la discusión evidencia que el reto dominante no reside en "contar con estándares", sino en transformar estándares y políticas en prácticas sostenibles, medibles y automatizables, que operen con consistencia en múltiples plataformas y proveedores.

Desde ENISA, se puede observar que estos hallazgos reflejan una característica de un sector crítico que considera la adopción de la nube desde una perspectiva de resiliencia sistémica y no como un proceso de modernización tecnológica. ENISA enfatiza la necesidad de fortalecer la gestión de riesgos, la seguridad desde el diseño, la continuidad operativa, la gestión de terceros,

así como la capacidad de gobernanza, y en estas áreas las entidades evaluadas evidenciaron progresos significativos, como lo muestra la función de Recuperación, así como la importancia otorgada a la seguridad y el cumplimiento normativo como elementos de la migración a la nube. A nivel regional, el informe de Porrúa et al. (2025) sitúa a la República Dominicana entre los países caribeños con mayor madurez relativa en ciberseguridad; sin embargo, los hallazgos de este estudio matizan esa posición favorable, al evidenciar que, al menos entre las entidades participantes, dicha madurez relativa se concentra en gobernanza y recuperación, y no necesariamente en las capacidades preventivas y de detección temprana que ese mismo informe identifica como determinantes de una postura de seguridad madura. No obstante, ENISA también enfatiza que la resiliencia solo puede tener éxito minimizando la exposición a amenazas y fortaleciendo los procesos de detección temprana, particularmente en infraestructuras distribuidas que están expuestas a múltiples superficies de ataque con una alta dependencia de proveedores externos y servicios interconectados. En esa línea, la evidencia empírica de este estudio revela limitaciones en telemetría integrada, automatización, orquestación de seguridad y estandarización centralizada de políticas entre las entidades participantes. Estas limitaciones se agravan cuando se observa que, dentro de la muestra, existe una percepción generalizada de mayor riesgo en nube pública frente a on-premise, lo que indica que la confianza en la nube no se construye solo con beneficios de escalabilidad y rapidez, sino con mecanismos verificables de control, auditoría y respuesta.

A partir de este contraste, el aporte del modelo se justifica como una respuesta metodológica y operativa a la brecha identificada entre madurez formal y eficacia técnica. Mientras NIST CSF ofrece una estructura funcional para organizar capacidades, ISO/IEC 27001–

27017 aporta un marco normativo para gobernanza y controles, y ENISA proporciona lineamientos estratégicos para resiliencia y riesgo en infraestructuras críticas, el modelo propone una integración aplicable al contexto local mediante pilares que convierten marcos y estándares en una arquitectura de gestión accionable. La concentración en nube híbrida y multinube (97% de las entidades de la muestra operando en estos esquemas) refuerza la necesidad de un modelo que priorice el control transversal por identidad, la estandarización de políticas y la visibilidad unificada, aspectos que en los resultados aparecen como demandas claras (alta utilidad percibida de un panel único) y como debilidades operativas (baja adopción de automatización y herramientas cloud-native) entre las entidades evaluadas.

Asimismo, la escasez de talento especializado emerge, entre las entidades participantes, como un factor crítico que condiciona la madurez operativa. Este resultado no puede interpretarse como una variable externa sin relevancia, sino como un elemento estructural que explica por qué organizaciones con marcos normativos robustos aún presentan déficits en protección y detección: sin capacidades internas suficientes, los controles avanzados (CSPM, CIEM, CASB, orquestación y automatización de respuesta) tienden a implementarse de forma parcial, fragmentada o reactiva. En consecuencia, la discusión sustenta que la madurez cloud no depende únicamente del presupuesto tecnológico, sino de la articulación entre gobierno, procesos, automatización y capacidades humanas, lo que refuerza el carácter integral del modelo propuesto.

En síntesis, la comparación explícita con NIST, ISO, ENISA y con la evidencia empírica de Kim et al. (2018), Zárate Urgell et al. (2023) y Porrúa et al. (2025) permite concluir que las entidades bancarias que conformaron la muestra de este estudio han desarrollado fortalezas alineadas con gobernanza y resiliencia, pero mantienen brechas críticas en prevención y detección

en entornos cloud, particularmente en configuraciones híbridas y multinube. Estas brechas no se explican por ausencia de marcos internacionales, sino por retos de operacionalización, integración y talento. Por ello, el modelo propuesto se posiciona como una propuesta pertinente y necesaria, en tanto integra los marcos internacionales en pilares operativos adaptados al contexto dominicano, orientados a cerrar brechas de Proteger y Detectar, reforzar la gestión del riesgo cibernético y elevar la madurez de la ciberseguridad cloud de las entidades bancarias dominicanas que adopten el modelo, en condiciones de alta regulación y criticidad.

Alcance de la generalización: Dado que la muestra de este estudio se conformó mediante un procedimiento no probabilístico por conveniencia y cuotas, y no un muestreo probabilístico representativo del total de 49 entidades autorizadas, los hallazgos y patrones descritos en esta discusión deben interpretarse como evidencia obtenida de las 30 entidades participantes, y no como una caracterización estadísticamente representativa de la totalidad del sistema bancario dominicano. Las tendencias identificadas, fortaleza en gobernanza y recuperación, debilidad en protección y detección; constituyen una base empírica relevante y consistente con la literatura previa, pero su extrapolación al conjunto del sector debe realizarse con cautela y, idealmente, confirmarse mediante estudios futuros con muestreo probabilístico.

4.3.1 Aporte científico y metodológico de la investigación

Este trabajo aporta una perspectiva aplicada y académica con un único tema de ciberseguridad en bancos en la nube, cumpliendo con estándares y marcos internacionales en el entorno práctico del sistema financiero dominicano. A diferencia de trabajos anteriores, que se centraron en la ciberseguridad en la nube a nivel regulatorio o tecnológico, el modelo propone una síntesis sistemática, incluyendo gobernanza, gestión de riesgos, arquitectura, operación y

tecnologías habilitadoras. Esto permite la interpretación y traducción de marcos teóricos, incluyendo NIST CSF, ISO/IEC 27001–27017 y principios de ENISA para una aplicación operativa práctica y cuantificable. El objetivo científico final es la comprensión empírica de la brecha entre la madurez formal y la eficiencia operativa en el entorno basado en la nube del sector bancario dominicano. Los resultados indican que altos niveles de gobernanza, identificación y recuperación pueden ser críticos para una buena postura de seguridad, pero este modelo podría no ser deseable sin protección y detección. Además, confirmamos y situamos las expectativas teóricas de NIST y ENISA; que sugieren, por ejemplo, que la resiliencia sin medidas preventivas aumentaría la posibilidad de que surjan riesgos, especialmente en arquitecturas híbridas y multicloud. Por lo tanto, este estudio hace una contribución metodológica a la literatura al sugerir una alineación más clara de objetivos, variables, instrumentos e indicadores. Esto mejora la validez interna del estudio y facilita la replicación del modelo en otros contextos financieros, que tienen atributos regulatorios y tecnológicos similares.

4.3.2 Implicaciones prácticas y estratégicas

a) Implicaciones para las entidades bancarias

En caso de un incidente de ciberseguridad, los bancos dominicanos tendrán que pasar de una postura de higiene cibernética predominantemente reactiva y centrada en el perímetro, hacia una ciberseguridad basada en la nube, que estará respaldada por la identidad, la automatización y la visibilidad transversal. La baja madurez en las funcionalidades de Protección y Detección indica que los controles nativos de la nube, como la gestión avanzada de identidades, la configuración continua, la segmentación lógica, la telemetría integrada y la orquestación de

respuestas, deben priorizarse como inversiones. Dentro de este marco, el modelo proporciona un camino tangible para guiar las decisiones estratégicas, mitigar las amenazas operativas y lograr un nivel común de madurez en seguridad en la nube en todo el sector.

b) Relevancia para los organismos reguladores y de supervisión

Las consecuencias para la comunidad reguladora y las partes interesadas son dobles, ya que los resultados apoyan la recomendación de que la implementación del cumplimiento normativo no es suficiente para mantener una postura de seguridad efectiva en entornos basados en la nube. Los reguladores pueden utilizar el modelo como un marco de referencia complementario para evaluar si las políticas y controles formales están en su lugar y si funcionan, así como si están operativizados y alineados con las arquitecturas híbridas y multicloud. Esto proporciona una oportunidad para mejorar los esquemas de supervisión mediante criterios de madurez, medidas de efectividad técnica y definición de servicios clave en la nube y procesos de gestión de terceros.

c) Implicaciones para los proveedores de servicios de nube y seguridad

El estudio también reveló que el proveedor de soluciones de nube y seguridad es un determinante importante en la etapa de madurez de la industria bancaria. Tanto la preferencia por las plataformas principales como el enfoque en un único panel de gestión indican un deseo de ecosistemas integrados e interconectados en línea con la legislación local. De este modo, podría ser posible aplicar este modelo para el diseño de servicios de seguridad que cumplan más de cerca con los requisitos de la industria financiera dominicana, de modo que la adopción de servicios IaaS, PaaS y SaaS pueda facilitarse utilizándolos de manera segura.

4.3.3 Validación metodológica de la hipótesis

Los hallazgos nos permiten confirmar la hipótesis planteada anteriormente; también confirmamos que la aplicación de un modelo holístico de ciberseguridad para infraestructuras en la nube contribuye sustancialmente a mejorar la gestión de riesgos cibernéticos en el sector bancario dominicano. Estos datos empíricos confirman que las deficiencias más graves se centran en las funciones de protección y detección, y pueden ser eliminadas con un método estructurado desarrollado a partir de la gobernanza, arquitectura, operación y tecnologías habilitadoras integradas en el modelo. En consecuencia, la investigación no solo valida la idoneidad del objetivo general, sino que también muestra que el modelo contextualizado y la aplicabilidad derivada del contexto local, alineados con estándares internacionales y respaldados por evidencia empírica, son una herramienta útil para mejorar la madurez y gestión de riesgos de la ciberseguridad en la nube, así como para reforzar la resiliencia digital de los bancos dominicanos ante la creciente complejidad de las amenazas cibernéticas.

Capítulo 5.

5.1 Conclusiones y recomendaciones

La presente investigación permitió caracterizar la gestión de ciberseguridad en la infraestructura cloud del sistema bancario de la República Dominicana y, sobre esa base empírica, estructurar y validar un modelo integral adaptado a sus exigencias técnicas y regulatorias. A continuación, se presentan las conclusiones organizadas según los tres objetivos que guiaron el estudio.

En cuanto al primer objetivo, analizar los marcos, modelos de madurez y controles: se constató que los estándares ISO/IEC 27001, ISO/IEC 27017 y el marco NIST CSF 2.0 constituyen los referentes principales adoptados por las entidades bancarias evaluadas. No obstante, el nivel de madurez exhibe una marcada asimetría entre sus funciones: mientras las dimensiones de Recuperar (94%), Identificar (86%) y Gobernar (78%) alcanzaron niveles consolidados, las funciones de Detectar (61%) y Proteger (42%) registraron brechas críticas. Estos resultados evidencian que la adopción formal de estándares no se ha traducido homogéneamente en capacidades técnicas automatizadas de prevención y detección temprana ante amenazas en la nube.

Respecto al segundo objetivo, evaluar las prácticas y procesos operativos: la evaluación diagnóstica permitió identificar brechas operativas prioritarias en la gestión de identidades y accesos (IAM) bajo enfoque Zero Trust, la seguridad de APIs expuestas, la visibilidad centralizada en entornos multicloud y la mitigación del riesgo derivado de la escasez de talento especializado. Ante esta realidad, se formularon oportunidades de mejora articuladas en cinco ejes

estratégicos que orientan la transición desde controles perimetrales tradicionales hacia mecanismos nativos de la nube.

Sobre el tercer objetivo, diseñar un modelo integral de gestión de ciberseguridad para la infraestructura cloud bancaria, el resultado concreto es el modelo PROBAN (Protección Bancaria en la Nube), construido en ocho pilares que recogen justamente lo que se identificó en los dos objetivos anteriores. El modelo fue sometido a la evaluación de un panel de cinco expertos en ciberseguridad, que lo calificaron con un índice de validez de contenido de 0.98; un resultado excelente, lo que indica que, a juicio de ese panel, el modelo es pertinente, aplicable y está bien construido. Con todo esto se puede responder la pregunta que dio origen a esta investigación: sí fue posible diseñar un modelo de gestión de ciberseguridad para infraestructura cloud que resulte pertinente y aplicable al sistema bancario dominicano, apoyado en estándares internacionales y respaldado por el juicio de expertos. Ahora bien, es importante ser precisos sobre qué significa exactamente esta validación: se trata de la opinión experta sobre el diseño del modelo, no de una comprobación de que el modelo efectivamente reduce el riesgo cibernético en la práctica. Eso solo podría demostrarse aplicando el modelo en una entidad real y midiendo resultados antes y después, algo que no formaba parte del alcance de este estudio.

A partir de estos hallazgos, se recomienda a las entidades bancarias fortalecer sus controles nativos de la nube, poner especial atención a la gestión de identidades y accesos bajo un enfoque Zero Trust, cifrar la información de manera uniforme y mantener un monitoreo continuo de sus cargas de trabajo. El modelo PROBAN puede servir como referencia para ordenar ese esfuerzo, siempre acompañado de programas de capacitación que atiendan la escasez de personal especializado detectada en el diagnóstico. A los organismos reguladores se les sugiere avanzar

hacia mecanismos de supervisión que midan la madurez operativa real de la ciberseguridad en la nube, y no solo el cumplimiento documental. Y como línea de trabajo pendiente, queda el reto de comprobar empíricamente si el modelo PROBAN efectivamente reduce el riesgo cibernético cuando se aplica en una entidad bancaria real, mediante un estudio con mediciones antes y después de su implementación.

5.2 Limitantes y desafíos

Uno de los principales desafíos que enfrenta esta investigación es cerrar la brecha entre el cumplimiento normativo y la efectividad operativa real de los controles de ciberseguridad, es decir, entre lo que las entidades dicen tener implementado y lo que ese control realmente logra en la práctica dentro de sus sistemas en la nube. Cerrar esa brecha no depende solo de invertir en tecnología, sino de cambios culturales, organizacionales y de gobernanza que permitan pasar de un modelo de seguridad reactivo a uno más proactivo y automatizado. El segundo gran desafío es la escasez de talento especializado en ciberseguridad en la nube. No hay suficientes profesionales con ese perfil, y eso compromete tanto la posibilidad de implementar modelos de seguridad avanzados como de sostenerlos en el tiempo. A esto se suma que, a medida que las entidades dependen cada vez más de proveedores externos en entornos cloud, surgen riesgos nuevos que exigen una gobernanza más fuerte, pruebas periódicas y un seguimiento estricto del cumplimiento contractual. Por último, la velocidad con la que evolucionan tanto las amenazas cibernéticas como las tecnologías en la nube hace difícil mantener un modelo de seguridad actualizado y lo suficientemente flexible como para no quedar obsoleto. Por esta razón, el modelo PROBAN no debería entenderse como un producto terminado, sino como un marco vivo, sujeto a revisión y

ajuste continuo, que las entidades bancarias dominicanas puedan ir adaptando a medida que cambian las amenazas y su propia infraestructura cloud.

REFERENCIAS BIBLIOGRÁFICAS

Abbas, H., Jaaz, Z., Al Barazanchi, I., & Abdulshaheed, H. (2021). Survey on enhanced security control measures in cloud computing systems. Journal of Physics: Conference Series, 1878(1), Article 012004. https://doi.org/10.1088/1742-6596/1878/1/012004

Aguilar, L. J. (2017). Ciberseguridad: La colaboración público-privada en la era de la cuarta revolución industrial. Cuadernos de Estrategia, 185, 19–64.

Aguilar, L. J. (2022). Computación en la nube (2.ª ed.). Marcombo.

Ahamad, D., Hameed, S. A., & Akhtar, M. (2022). A multi-objective privacy preservation model for cloud security using hybrid Jaya-based shark smell optimization. Journal of King Saud University – Computer and Information Sciences, 34(6), 2343–2358. https://doi.org/10.1016/j.jksuci.2020.10.015

Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2021). Cyber security in IoT-based cloud computing: A comprehensive survey. Electronics, 11(1), Article 16. https://doi.org/10.3390/electronics11010016

Baloira Reyes, A. (2022). Cloud cybersecurity threat recognition and detection system. Telemática, 21(1), 48–55. https://revistatelematica.cujae.edu.cu/index.php/tele/article/view/564

Banco Interamericano de Desarrollo. (2020). Computación en la nube: Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.

https://publications.iadb.org/publications/spanish/document/Computacion-en-la-nubeContribucion-al-desarrollo-de-ecosistemas-digitales-en-paises-del-Cono-Sur.pdf

Basel Committee on Banking Supervision. (2021). Principles for operational resilience. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.pdf

Blumira. (2026). How much does a SIEM cost? Total cost of ownership. https://www.blumira.com/siem-cost

Cloud Security Alliance. (2021). Security guidance for critical areas of focus in cloud computing (v4.0). https://cloudsecurityalliance.org

Cloud Security Alliance. (2022). Cloud controls matrix (CCM v4.0). https://cloudsecurityalliance.org

Cloud Security Alliance. (2023). Managing cloud misconfiguration risks. https://cloudsecurityalliance.org/blog/2023/08/14/managing-cloud-misconfigurations-risks

Cloud Security Alliance. (2024). Top threats to cloud computing 2024. https://cloudsecurityalliance.org/research/working-groups/top-threats/

Congreso Nacional. (2002). Ley No. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales. Gaceta Oficial No. 10161. República Dominicana.

Congreso Nacional. (2007). Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología. Gaceta Oficial No. 10419. República Dominicana.

Congreso Nacional. (2013). Ley No. 172-13 sobre Protección de Datos de Carácter Personal. Gaceta Oficial No. 10737. República Dominicana.

Cribl. (2026). Understanding SIEM costs in 2026: Key factors and pricing models. https://cribl.io/blog/understanding-siem-costs/

Escobar-Pérez, J., & Cuervo-Martínez, A. (2008). Validez de contenido y juicio de expertos: Una aproximación a su utilización. Avances en Medición, 6, 27–36.

European Union Agency for Cybersecurity. (2020). Guidelines for security operations centres (SOCs). https://www.enisa.europa.eu

European Union Agency for Cybersecurity. (2021). Zero trust architectures. https://www.enisa.europa.eu

European Union Agency for Cybersecurity. (2023). Cloud cybersecurity market analysis. https://www.enisa.europa.eu/publications/cloud-cybersecurity-market-analysis

Federal Financial Institutions Examination Council. (2022). Cybersecurity resource guide for financial institutions. https://www.ffiec.gov/sites/default/files/media/press-releases/2022/2022-cybersecurity-resource-guide-ffiec.pdf

Ferrer, R. (2023). Arquitectura de seguridad e infraestructura cloud en el sector financiero. Editorial Tecnológica. [Entrada incorporada para correspondencia con Tabla 1]

Gartner. (2024, 22 de febrero). Gartner identifies top cybersecurity trends for 2024. https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024

George, D., & Mallery, P. (2003). SPSS for Windows step by step: A simple guide and reference, 11.0 update (4.ª ed.). Allyn & Bacon.

Hu, V. C., Iorga, M., Bao, W., Li, A., Li, Q., & Gouglidis, A. (2023). General access control guidance for cloud systems (NIST Special Publication 800-210). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-210

International Organization for Standardization. (2015). Code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC Standard No. 27017:2015). https://www.iso.org/standard/43757.html

International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO/IEC Standard No. 27001:2022). https://www.iso.org/standard/27001

ISACA. (2020). COBIT 2019 Framework: Governance and management objectives. ISACA. [Entrada incorporada para correspondencia con Tabla 1]

Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing (NIST Special Publication 800-144). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-144

Junta Monetaria. (2018). Reglamento de Seguridad Cibernética y de la Información. Banco Central de la República Dominicana. https://www.sb.gob.do/regulacion/reglamentos/reglamento-de-seguridad-cibernetica-y-de-la-informacion/

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2010). Guide to computer security incident handling (NIST Special Publication 800-61 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Kim, D., Park, Y., & Kim, H. (2018). Cloud security assessment for the financial industry. Sustainability, 10(8), Article 2871. https://doi.org/10.3390/su10082871

Lawshe, C. H. (1975). A quantitative approach to content validity. Personnel Psychology, 28(4), 563–575. https://doi.org/10.1111/j.1744-6570.1975.tb01393.x

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). NIST cloud computing reference architecture (NIST Special Publication 500-292). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf

MSSPProviders.io. (2026). Managed security services pricing 2026. https://msspproviders.io/resources/managed-security-services-pricing/

National Institute of Standards and Technology. (2020). Zero trust architecture (NIST Special Publication 800-207). https://doi.org/10.6028/NIST.SP.800-207

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

Organización de los Estados Americanos. (2018). Estado de la ciberseguridad en el sector bancario en América Latina y el Caribe. https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

Parlamento Europeo. (2016). Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (GDPR). Diario Oficial de la Unión Europea, L 119, 1–88.

PCI Security Standards Council. (2022). Payment Card Industry Data Security Standard (PCI DSS v4.0). https://www.pcisecuritystandards.org

Porrúa, M., Moncayo, G., Paz, S., Nowersztern, A., Bejarano, J. F., Baudino, M. F., Bordese, M. P., Barret, K.-A., Baena, C. E., Jaramillo, M., Garces, O., & Isidro, A. (2025). 2025 cybersecurity report: Vulnerability and maturity challenges to bridging the gaps in Latin America and the Caribbean. Banco Interamericano de Desarrollo. https://doi.org/10.18235/0013872

Sophos. (2020, 7 de agosto). The state of cloud security 2020. https://news.sophos.com/en-us/2020/08/07/the-state-of-cloud-security-2020

Superintendencia de Bancos de la República Dominicana. (2025a). Ránking de digitalización del sector bancario 2025. https://sb.gob.do/publicaciones/publicaciones-tecnicas/ranking-de-digitalizacion-del-sector-bancario-2025/

Superintendencia de Bancos de la República Dominicana. (2025b, 20 de noviembre). La Superintendencia de Bancos promueve la vigilancia y actualización constante para evitar robo de datos. https://www.sb.gob.do/prensa/la-superintendencia-de-bancos-promueve-la-vigilancia-y-actualizacion-constante-para-evitar-robo-de-datos/

U.S. Congress. (2002). Sarbanes–Oxley Act of 2002. U.S. Government Publishing Office.

Zárate Urgell, A. I., ... (2023). Análisis de la ciberseguridad en el sector financiero de México con el fin de implementar la metodología Zero Trust y mejorarla. Ciencia Latina Revista Científica Multidisciplinar, 7(1), 3384–3408. https://doi.org/10.37811/cl_rcm.v7i1.4661

APÉNDICE

Apéndice A. Instrumento de Recolección de Datos

Instrumento aplicado de forma autoadministrada y anónima a través de una plataforma de encuesta digital (Microsoft Forms), a un informante clave por entidad, entre el 2 y el 10 de mayo de 2025. El presente apéndice refleja fielmente las preguntas y las categorías de respuesta efectivamente utilizadas en el instrumento aplicado a las 30 entidades participantes.

INSTRUMENTO DE RECOLECCIÓN DE INFORMACIÓN MEDIDAS DE CIBERSEGURIDAD ENTORNOS CLOUD DE ENTIDADES BANCARIAS.		
	Fecha	
DATOS DEL EVALUADO		
Nombre		
Empresa		
Puesto		
Este instrumento tiene como objetivo recopilar información relevante sobre el nivel de adopción de servicios en la nube, la madurez de ciberseguridad, la gestión de riesgos y la implementación de controles de seguridad en las entidades bancarias. La información recolectada será utilizada exclusivamente con fines académicos, garantizando la confidencialidad y anonimato de los participantes. Marque con una (X) la opción que mejor represente su situación o complete la información solicitada.		

PERFIL DEL ENCUESTADO Y CONTEXTO ORGANIZACIONAL

1. ¿Cuál es su rol en la organización?

- ☐ CISO
- ☐ CRO
- ☐ CTO
- ☐ COO
- ☐ DPO
- ☐ IT Manager
- ☐ SOC Director
- ☐ Gerente de Seguridad
- ☐ Otro (especificar)

2. ¿Su institución bancaria utiliza servicios en la nube?

- ☐ Sí, ampliamente
- ☐ Sí, parcialmente
- ☐ No, pero planea hacerlo
- ☐ No

3. ¿Qué porcentaje de su infraestructura IT está en la nube?

Opciones:

- ☐ Menos del 25%
- ☐ 25-50%
- ☐ 51-75%
- ☐ Más del 75%

ADOPCIÓN, ESTRATEGIA Y MADUREZ CLOUD

4. ¿Cómo calificaría la madurez de su implementación en la nube?

- ☐ Inicial (primeros pasos)
- ☐ Intermedia (en progreso)
- ☐ Avanzada (optimizada)

5. ¿Cuál es o será la estrategia principal de su organización para la implementación de la nube?

- ☐ Nube única
- ☐ Nube híbrida
- ☐ Multinube

6. ¿Cuántos proveedores de nube utiliza actualmente su organización?

- ☐ Aún no tengo proveedor
- ☐ Uno
- ☐ Dos
- ☐ Tres
- ☐ Más de tres

7. ¿Qué proveedores de IaaS en la nube utiliza actualmente o planea utilizar en el futuro?

Opciones (seleccione todas las que correspondan):

- ☐ AWS
- ☐ Azure
- ☐ Google Cloud
- ☐ IBM Cloud
- ☐ Oracle Cloud
- ☐ Otro

8. ¿Cuáles son las principales barreras para la adopción de la nube en su organización?

Opciones (seleccione todas las que correspondan):

- ☐ Costos
- ☐ Desafíos técnicos
- ☐ Factores organizacionales y operativos
- ☐ Limitaciones de recursos
- ☐ Personal capacitado
- ☐ Preocupación por seguridad y cumplimiento
- ☐ Resistencia al cambio

9. ¿A cuáles desafíos se enfrenta la organización en la integración de la nube?

Opciones (seleccione todas las que correspondan):

- ☐ Arquitectura de la nube
- ☐ Gobernanza de datos en la integración de la nube
- ☐ Gobernanza, seguridad y cumplimiento normativo de la nube
- ☐ Integración de servicios en la nube con sistemas
- ☐ Latencia de red en entornos de nube híbrida

TALENTO, CAPACIDADES Y PRESUPUESTO

10. ¿Cuáles son las habilidades de seguridad más importantes requeridas en su organización?

Opciones (seleccione todas las que correspondan):

- ☐ Gobernanza, riesgo y cumplimiento
- ☐ Identidad y administración de acceso
- ☐ Inteligencia de amenazas y análisis
- ☐ Monitoreo de seguridad y operaciones
- ☐ Nube y seguridad de aplicaciones
- ☐ Técnicas y habilidades avanzadas de seguridad

11. ¿Qué tan preocupado está usted por la escasez de personal calificado en el sector financiero?

- ☐ Para nada preocupado
- ☐ Levemente preocupado
- ☐ Moderadamente preocupado
- ☐ Muy preocupado
- ☐ Extremadamente preocupado

12. ¿Su organización está experimentando escasez de talento en ciberseguridad?

- ☐ Sí
- ☐ No

13. ¿Cómo cambiará su presupuesto de seguridad en la nube en los próximos 12 meses?

- ☐ Disminuye
- ☐ Sin cambios
- ☐ Aumenta

PERCEPCIÓN Y GESTIÓN DEL RIESGO CLOUD

14. ¿Qué tan preocupado está por la seguridad de las nubes públicas?

- ☐ Levemente preocupado
- ☐ Moderadamente preocupado
- ☐ Muy preocupado
- ☐ Extremadamente preocupado

15. ¿Qué tan preocupado está usted por el volumen de riesgos de seguridad en la nube que requieren mitigación?

- ☐ Levemente preocupado
- ☐ Moderadamente preocupado

- ☐ Muy preocupado
- ☐ Extremadamente preocupado

16. En comparación con los entornos de TI locales tradicionales, ¿diría que el riesgo de las violaciones de seguridad en un entorno de nube pública es mayor o menor?

- ☐ Significativamente más bajo
- ☐ Un poco más bajo
- ☐ Casi lo mismo
- ☐ Un poco más alto
- ☐ Significativamente más alto

17. ¿Se han cuantificado los riesgos de ciberseguridad en términos económicos y se han definido escenarios de mitigación para los entornos cloud?

- ☐ No implementado
- ☐ En planificación
- ☐ Parcialmente implementado
- ☐ Mayormente implementado
- ☐ Totalmente implementado y operativo

18. ¿Cuáles son sus principales prioridades en materia de seguridad en la nube?

Opciones (seleccione todas las que correspondan):

- ☐ Seguridad y privacidad de los datos
- ☐ Detección y respuesta ante amenazas
- ☐ Gestión de identidad y acceso
- ☐ Cumplimiento y adhesión normativa
- ☐ Gobernanza de la nube y gestión de riesgos
- ☐ Gestión de infraestructura y recursos
- ☐ Migración e integración en la nube
- ☐ Recuperación ante desastres y continuidad del negocio
- ☐ Seguridad de la aplicación
- ☐ Educación y sensibilización del usuario
- ☐ Visibilidad y monitorización de extremo a extremo
- ☐ Automatización y orquestación de la seguridad
- ☐ Prevención

CONTROLES DE SEGURIDAD Y BUENAS PRÁCTICAS

19. ¿Cuáles son las principales medidas y controles de su organización para gestionar toda su infraestructura en la nube?

Opciones (seleccione todas las que correspondan):

- ☐ Web Application Firewalls (WAF)
- ☐ Network security segmentation
- ☐ Firewalls
- ☐ Threat intelligence and response
- ☐ Identity and Access Management (IAM)
- ☐ Single Sign-On (SSO)
- ☐ Zero Trust architecture
- ☐ SIEM
- ☐ IDS/IPS
- ☐ Cifrado en tránsito (TLS/SSL)
- ☐ Cifrado en reposo (KMS, CloudHSM)
- ☐ Prevención de pérdida de datos (DLP)
- ☐ Control de acceso basado en etiquetas (ABAC)
- ☐ Cloud Access Security Broker (CASB)
- ☐ Cloud Security Posture Management (CSPM)
- ☐ Cloud Native Application Protection Platform (CNAPP)
- ☐ Cloud Infrastructure Entitlement Management (CIEM)
- ☐ CI/CD pipeline & software supply chain security

20. ¿Cuenta la organización con un programa formal de gestión de vulnerabilidades que incluya análisis periódico y remediación en los servicios cloud?

- ☐ No implementado
- ☐ En planificación
- ☐ Parcialmente implementado
- ☐ Mayormente implementado
- ☐ Totalmente implementado y operativo

21. ¿Se aplican guías de hardening estandarizadas para la configuración segura de servidores y equipos de red?

- ☐ No implementado
- ☐ En planificación

☐ Parcialmente implementado
☐ Mayormente implementado
☐ Totalmente implementado y operativo

22. ¿Existe un inventario actualizado de hardware y software, con visibilidad de activos en la nube?

☐ No implementado
☐ En planificación
☐ Parcialmente implementado
☐ Mayormente implementado
☐ Totalmente implementado y operativo

OPERACIONES DE SEGURIDAD Y MONITOREO

23. ¿Cuenta la organización con una solución de respaldo que integre inteligencia artificial, antimalware, inmutabilidad y aislamiento?

☐ No implementado
☐ En planificación
☐ Parcialmente implementado
☐ Mayormente implementado
☐ Totalmente implementado y operativo

24. ¿Cuenta la organización con un Security Operations Center (SOC), interno o tercerizado, en operación continua que monitorea y responde a incidentes en entornos cloud?

☐ No implementado
☐ En planificación
☐ Parcialmente implementado
☐ Mayormente implementado
☐ Totalmente implementado y operativo

25. ¿Existe una solución activa de auditoría de cambios en configuraciones críticas de sistemas en la nube (servidores, red, sistemas)?

☐ No implementado
☐ En planificación
☐ Parcialmente implementado
☐ Mayormente implementado
☐ Totalmente implementado y operativo

26. ¿Cuáles son sus principales desafíos en la gestión de las operaciones diarias de seguridad en la nube?

Opciones (seleccione todas las que correspondan):

- ☐ Seguridad y privacidad de los datos
- ☐ Gestión de configuración
- ☐ Control de acceso y gestión de identidad
- ☐ Detección y respuesta a amenazas
- ☐ Gestión de políticas y cumplimiento
- ☐ Gestión de seguridad en la nube
- ☐ Seguridad del Endpoint

27. ¿Cuáles son sus mayores desafíos para asegurar entornos multinube?

Opciones (seleccione todas las que correspondan):

- ☐ Garantizar la protección de datos y privacidad para cada entorno
- ☐ Entender cómo se integran las diferentes opciones de servicio
- ☐ Tener las habilidades adecuadas para implementar y administrar una solución completa en todos los entornos de nube
- ☐ Administrar los costos de diferentes soluciones

CONTINUIDAD, RESPUESTA Y RESILIENCIA

28. ¿Existe un plan de recuperación ante desastres tecnológicos probado y actualizado?

- ☐ En planificación
- ☐ Parcialmente implementado
- ☐ Mayormente implementado
- ☐ Totalmente implementado y operativo

29. ¿Existe un plan de continuidad de negocio que contemple eventos de ciberseguridad disruptivos?

- ☐ En planificación
- ☐ Parcialmente implementado
- ☐ Mayormente implementado
- ☐ Totalmente implementado y operativo

30. ¿La organización utiliza herramientas de cifrado para proteger los datos en reposo y en tránsito dentro del entorno cloud?

- ☐ No se aplica
- ☐ Se aplica parcialmente
- ☐ Se aplica en ciertos entornos
- ☐ Se aplica de forma generalizada
- ☐ Completamente implementado y monitoreado

31. ¿Se auditan periódicamente los permisos de cuentas y credenciales en las plataformas cloud (IAM reviews)?

- ☐ Nunca se auditan
- ☐ Solo se auditan manualmente en casos específicos
- ☐ Auditorías parciales semestrales
- ☐ Auditorías completas trimestrales
- ☐ Auditorías automatizadas y alertas activas

32. ¿Se han realizado simulacros o ejercicios de respuesta a incidentes específicos en entornos de nube pública?

- ☐ No se han realizado
- ☐ Realizados una vez en los últimos 12 meses
- ☐ Realizados cada 6 meses
- ☐ Realizados trimestralmente
- ☐ Parte integral del plan de continuidad

33. ¿Se monitorean activamente las APIs expuestas por servicios cloud para prevenir abusos o accesos indebidos?

- ☐ No se monitorean
- ☐ Solo se revisan en auditorías
- ☐ Monitoreo básico con logs
- ☐ Monitoreo en tiempo real
- ☐ Monitoreo y bloqueo automático de amenazas

GOBIERNO, PROVEEDORES Y CUMPLIMIENTO

34. ¿La organización evalúa y audita regularmente a sus proveedores cloud en cuanto a cumplimiento de seguridad para garantizar la protección de los datos y la continuidad del servicio?

- ☐ No se evalúan
- ☐ Evaluación inicial al contratar
- ☐ Evaluación anual
- ☐ Evaluación y auditoría semestral
- ☐ Evaluación continua con indicadores de desempeño

35. ¿El proveedor de servicios cloud proporciona reportes periódicos sobre eventos de seguridad, controles aplicados y cumplimiento normativo, y permite auditorías independientes por parte de la organización?

- ☐ No se recibe ningún tipo de informe ni se permiten auditorías

- ☐ Solo se envían informes generales bajo solicitud
- ☐ Se entregan reportes básicos periódicamente sin mucho detalle
- ☐ Se reciben informes detallados y se permite cierto nivel de auditoría
- ☐ Se entregan reportes detallados, en tiempo real, y se facilita acceso total a auditorías independientes

36. ¿Qué utilidad tendría tener una única plataforma de seguridad en la nube con un único panel donde podría configurar todas las políticas necesarias para proteger los datos de manera consistente y detectar amenazas de forma centralizada?

- ☐ Nada útil
- ☐ Poco útil
- ☐ Algo útil
- ☐ Muy útil
- ☐ Extremadamente útil

INNOVACIÓN Y USO DE INTELIGENCIA ARTIFICIAL

37. ¿Qué lugar ocupa la adopción de IA entre las prioridades de ciberseguridad de su organización?

Opciones:

- ☐ Baja
- ☐ Media
- ☐ Alta
- ☐ Máxima

38. ¿Cuáles son los principales impulsores para considerar soluciones de seguridad basadas en la nube?

Opciones (seleccione todas las que correspondan):

- ☐ Ahorro en costos
- ☐ Mejor escalabilidad
- ☐ Mejor tiempo en implementación
- ☐ Mejor performance
- ☐ Esfuerzo reducido sobre parches y actualizaciones de software

Apéndice B. Mapeo Instrumento con Modelo Propuesto

Para efectos metodológicos, el modelo PROBAN se estructura en los siguientes ocho pilares:

Pilar	Nombre
P1	Cumplimiento (Compliance)
P2	Seguridad y Protección de Datos (Data Security)
P3	Seguridad de Aplicaciones y APIs (AppSec & API Security)
P4	Gestión de Identidad y Accesos (IAM & Zero Trust)
P5	Redes y Seguridad Perimetral (Perimeter & Network Security)
P6	Operaciones de Seguridad y Respuesta a Incidentes (SOC Cloud-Céntrico)
P7	Gestión de Incidentes (Incident Response)
P8	Arquitectura Híbrida y Gestión de Terceros (Hybrid Cloud & Third-Party Risk)

Mapeo de Preguntas vs. Pilares del Modelo PROBAN

Las preguntas que se muestran a continuación no se asocian a un pilar específico del modelo; caracteriza a la muestra y alimenta el diagnóstico de madurez del Capítulo 4.

#	Pregunta
1	Rol en la organización
2	Uso actual de servicios en la nube
3	Porcentaje de infraestructura TI en la nube
4	Nivel de madurez cloud
5	Estrategia principal de adopción
6	Número de proveedores de nube
7	Proveedores IaaS utilizados

8	Barreras para la adopción de la nube
9	Desafíos de integración cloud

Pilar 1. Cumplimiento

Evaluar gobernanza, dirección estratégica y alineación negocio-seguridad-regulación.

#	Pregunta
10	Habilidades de seguridad requeridas
11	Preocupación por escasez de talento
12	Escasez de talento especializado en ciberseguridad
13	Cambio en presupuesto de seguridad cloud
18	Principales prioridades en materia de seguridad
22	Inventario de activos en la nube
35	Reportes de proveedor y auditorías independientes
36	Utilidad de una plataforma unificada de seguridad

Pilar 2. Seguridad y Protección de Datos

Evaluar la protección de la confidencialidad e integridad de los datos.

#	Pregunta
14	Preocupación por la seguridad en nubes públicas
15	Preocupación por el volumen de riesgos cloud
16	Riesgo de violaciones vs. entornos on-premise
17	Cuantificación económica del riesgo
30	Cifrado de datos en reposo y en tránsito

Pilar 3. Seguridad de Aplicaciones y APIs

Evaluar la protección de aplicaciones y APIs expuestas.

#	Pregunta
33	Monitoreo de APIs expuestas

Pilar 4. Gestión de Identidad y Accesos (IAM & Zero Trust)

Evaluar el control de identidades y accesos.

#	Pregunta
31	Revisiones periódicas de permisos y credenciales (IAM reviews)

Pilar 5. Redes y Seguridad Perimetral

Evaluar los controles técnicos de red e infraestructura.

#	Pregunta
19	Principales medidas y controles utilizados (WAF, segmentación, IDS/IPS, etc.)
21	Guías de hardening estandarizadas

Pilar 6. Operaciones de Seguridad y Respuesta a Incidentes (SOC Cloud-Céntrico)

Evaluar la capacidad de monitoreo, detección y automatización operativa.

#	Pregunta
20	Programa formal de gestión de vulnerabilidades
24	SOC interno o tercerizado
25	Auditoría de cambios en configuraciones críticas
26	Desafíos en la gestión diaria de la seguridad cloud
37	Prioridad de adopción de IA en ciberseguridad
38	Impulsores para adoptar soluciones de seguridad cloud

Pilar 7. Gestión de Incidentes (Incident Response)

Evaluar la capacidad de respuesta, continuidad y recuperación.

#	Pregunta
28	Plan de recuperación ante desastres tecnológicos
29	Plan de continuidad de negocio
23	Soluciones de respaldo con inmutabilidad/aislamiento
32	Simulacros de respuesta a incidentes en entornos cloud

Pilar 8. Arquitectura Híbrida y Gestión de Terceros

Evaluar la gestión de entornos multinube y el riesgo de proveedores.

#	Pregunta
27	Desafíos para asegurar entornos multinube
34	Auditoría a proveedores cloud

Apéndice C. Instrumento de Validación Aplicado a los Expertos

ENTREVISTA SEMIESTRUCTURA A EXPERTOS

Validación del Modelo de Gestión de Ciberseguridad para la Infraestructura Cloud.

Propósito: Esta guía tiene como finalidad recopilar la valoración de expertos en ciberseguridad sobre la relevancia, aplicabilidad, efectividad y coherencia del modelo de gestión de ciberseguridad propuesto en esta investigación, como parte del proceso de validación descrito en el apartado 3.3 (Instrumento, método de validación y procedimiento de aplicación).

Instrucciones: Por favor, revise el modelo propuesto (documento y diagrama de arquitectura adjuntos) antes de completar esta guía. Para cada afirmación de las secciones II y III, marque con una X el nivel de acuerdo según la escala de 1 (totalmente en desacuerdo) a 5 (totalmente de acuerdo). Las preguntas abiertas de la sección IV pueden responderse de forma libre.

SECCIÓN I — PERFIL DEL EXPERTO

Nombre (opcional)	
Cargo / Rol actual	
Institución / Sector	
Años de experiencia	
Especialidad	
Fecha de la entrevista	

SECCIÓN II — VALIDACIÓN POR DIMENSIÓN DEL MODELO

1. Relevancia

Criterio	1 Totalmente en desacuerdo	2 En desacuerdo	3 Neutral	4 De acuerdo	5 Totalmente de acuerdo
El modelo responde a una necesidad real y actual del sector bancario dominicano en materia de ciberseguridad cloud.	☐	☐	☐	☐	☐
Las dimensiones incluidas (seguridad de la información, gestión del riesgo, arquitectura y gobierno, tecnologías habilitadoras) son pertinentes para el contexto bancario.	☐	☐	☐	☐	☐
El modelo aborda adecuadamente los principales riesgos identificados en el diagnóstico (adopción cloud, brechas de madurez NIST CSF, entre otros).	☐	☐	☐	☐	☐

2. Aplicabilidad

Criterio	1 Totalmente en desacuerdo	2 En desacuerdo	3 Neutral	4 De acuerdo	5 Totalmente de acuerdo
El modelo puede implementarse en entidades bancarias de diferente tamaño (pequeñas, medianas, grandes).	☐	☐	☐	☐	☐
Los lineamientos propuestos son suficientemente claros para guiar su implementación.	☐	☐	☐	☐	☐
El modelo es compatible con los marcos normativos ya utilizados por el sector (ISO/IEC 27001, ISO/IEC 27017, NIST CSF).	☐	☐	☐	☐	☐

3. Efectividad

Criterio	1 Totalmente en desacuerdo	2 En desacuerdo	3 Neutral	4 De acuerdo	5 Totalmente de acuerdo
El modelo contribuye a reducir las brechas de seguridad identificadas en el diagnóstico.	☐	☐	☐	☐	☐
La implementación del modelo mejoraría la gestión del riesgo cibernético en la infraestructura cloud.	☐	☐	☐	☐	☐
El modelo fortalece la capacidad de respuesta y recuperación ante incidentes cibernéticos.	☐	☐	☐	☐	☐

4. Coherencia del Modelo

Criterio	1 Totalmente en desacuerdo	2 En desacuerdo	3 Neutral	4 De acuerdo	5 Totalmente de acuerdo
Existe coherencia y complementariedad entre las dimensiones del modelo (seguridad de la información, gestión del riesgo, arquitectura y gobierno, tecnologías habilitadoras).	☐	☐	☐	☐	☐
La estructura general del modelo es lógica y fácil de comprender.	☐	☐	☐	☐	☐

SECCIÓN III — PREGUNTAS ABIERTAS

1. ¿Qué fortalezas destaca del modelo propuesto?

---

2. ¿Qué debilidades, vacíos o riesgos identifica en el modelo?

---

3. ¿Qué ajustes o mejoras recomendaría antes de su implementación?

4. ¿Considera viable la implementación del modelo en el corto o mediano plazo en el sector bancario dominicano? ¿Por qué?

SECCIÓN IV — VALORACIÓN GENERAL

Valoración general del modelo:

☐ Validado sin observaciones	☐ Validado con observaciones menores	☐ Requiere ajustes significativos	☐ No validado

Observaciones adicionales:
