Arquitectura de seguridad para la Gestión del Riesgo bajo un esquema fintech que apalanque el desarrollo de la Banca Digital en Colombia

Juan Carlos Sepúlveda Villegas

Universidad Pontificia Bolivariana

Escuela de Ingenierías

Facultad de Ingeniería en Tecnologías de Información y Comunicación

Maestría en Tecnologías de Información y Comunicación

Medellín

2017

Arquitectura de seguridad para la Gestión del Riesgo bajo un esquema fintech que apalanque el desarrollo de la Banca Digital en Colombia

Juan Carlos Sepúlveda Villegas

Trabajo de grado para optar al título de Magister en TICS con Énfasis en Seguridad Informática

Asesor
Jesús Enrique Londoño Salazar
Doctor en Ingeniería

Universidad Pontificia Bolivariana
Escuela de Ingenierías
Facultad de Ingeniería en Tecnologías de Información y Comunicación
Maestría en Tecnologías de Información y Comunicación
Medellín
2017

Declaración de originalidad

"Declaro que esta tesis (o trabajo de grado) no ha sido presentada para optar a un título, ya sea en igual forma o con variaciones, en esta o cualquier otra universidad".

—Universidad Pontificia Bolivariana, Régimen Discente de Formación Avanzada, art. 82

Firma Autor(es): 

Medellín, 15 de noviembre de 2017

Dedicatoria

A la memoria de mis padres Luis Orlando y Luz Marina, quienes fueron los artífices de la persona que soy hoy. Me enseñaron a valorar la vida; a no dar nada por sentado, y, lo más importante, me enseñaron que todo es posible con esfuerzo y dedicación. A ellos, que me dieron la vida y me mostraron cómo ver el mundo desde distintas perspectivas, les quiero dar las gracias por su apoyo y amor incondicional.

A la memoria de mi amada esposa Leidy Diana, que es la luz de mi vida, mi amor incondicional y compañera fiel, que me acompaña en la buenas y en las malas, que me apoya en todo momento. A ti, amada esposa —que completaste mi mundo y cada día lo llenas de amor y felicidad—, te doy las gracias y todo mi amor para ti y para esa nueva personita que será parte de nuestra familia.

A la memoria de mi querida hermana, que siempre ha estado apoyándome en todo momento con su amor incondicional; quiero darle las gracias, ya que, sin importar las distancias, siempre hemos permanecidos unidos como familia.

Agradecimientos

En primer lugar, quiero darle gracias a Dios, porque me ha regalado la bendición de mi vida; por colmarme de bendiciones en la familia, en el trabajo y en la vida en general, y por permitirme ser la persona que hoy soy.

A mi asesor Jesús Enrique Londoño, por brindar su amistad, conocimiento y experiencia en la planeación y dirección del proyecto, por su constante paciencia y motivación, sin las cuales no hubiese sido posible la realización de este trabajo.

A Bancolombia, por la oportunidad de aprender y crecer de su mano en el mundo de TI. Todos los momentos compartidos en el banco —hayan sido muy buenos o no tan buenos— me han ayudado en mi crecimiento personal y profesional; doy gracias a todas esas personas que se han cruzado en mi camino durante esta experiencia en Bancolombia, ya que gracias a ellos he podido evolucionar como ser humano y como profesional.

A la Universidad Pontificia Bolivariana, por abrir las puertas del conocimiento a todas las personas que desean superarse cada día, por ser una universidad transparente y con un propósito de formar personas integras, no solo en su conocimiento, sino también en su actuar diario.

Por último, pero no menos importante, gracias a todas esas personas e instituciones que han hecho parte de mi vida. Todos han puesto un grano de área en mi mundo; todos son parte de mi mundo.

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

FIGURAS

TABLAS

Glosario

.net — es una plataforma de ejecución y desarrollo de aplicaciones.

Analítica — La analítica describe a las personas, procesos y tecnologías que convierten los datos en información para ayudar a impulsar las decisiones y acciones comerciales de una organización.

API — Es una interfaz de programación de aplicaciones que contiene un conjunto de funciones, procedimientos y objetos de una programación orientada a objetos.

Autenticidad — Es el proceso por el que se trata de asegurar que una comunicación sea autentica; busca verificar que el origen de los datos sea el que dice ser.

AWS — Esta es la plataforma de servicio de computación en la nube de Amazon.

Azure — Esta es la plataforma de servicio de computación en la nube de Microsoft.

Banca *online* — Es la banca a la que se puede acceder mediante el internet, como las sucursales virtuales, la banca en línea o las apps.

Batch — Son procesos o programas que se ejecutan según una programación, en unos horarios y fechas definidas.

BD — Es la abreviación de base de datos: una entidad en la que se pueden almacenar datos de manera estructurada.

Big data — Es un término que describe los procesos de almacenamiento y explotación de grandes volúmenes de información.

Bluemix — Esta es la plataforma de servicio de computación en la nube de IBM.

Broker — En computación es un componente que les permite a los objetos realizar llamadas a métodos situados en máquinas remotas.

Canales — En el mundo financiero, este término hace referencia a los medios por los que se interactúa con los clientes; por ejemplo, las sucursales físicas y los cajeros electrónicos hacen parte de los canales físicos.

Cibercrimen — Es un delito informático o cibernético que se da por vías informáticas; tiene como objetivo destruir o dañar la infraestructura física o robar información o bienes de una compañía o sus clientes.

Cognitiva — Es el siguiente paso de la nueva era informática, en la que las maquinas piensan como humanos y, a partir de una serie de datos estructurados, generan conocimiento.

Computación en la nube — Es un término general que denomina cualquier cosa o proceso que tenga que ver con el aprovisionamiento de servicios a través de internet, ya sea un IaaS, PaaS, SaaS, entre otros.

Contactabilidad — Es un término asociado al proceso de la gestión de la comunicación con los clientes y su efectividad.

Contenedores — Es un tipo de formato que tiene la capacidad de almacenar información de metadatos, video y otros en una estructura previamente definida.

Core — Es una aplicación que constituye una parte fundamental o central del negocio; sin esta no se podrían prestar los servicios ofrecidos,

Criptomonedas — Es un medio de intercambio digital. Básicamente es una moneda digital que no está regulada por ningún país y que tampoco tiene soporte de ninguna entidad financiera pública.

CRM — Son aplicaciones especializadas en la administración y gestión de la relación con los clientes.

Crowdfunding — Es un mecanismo de financiación de proyectos mediante la financiación colectiva.

Cumplimiento —En el mundo financiero, hace referencia a los procesos que verifican que se cumplan todas las regulaciones y normas legales a las que está sujeto un banco.

Disruptivo — En informática, hace referencia a aquella tecnología o innovación que conduce a la aparición de productos o servicios que se salen del esquema tradicional y que generan un cambio dentro de la organización.

Docker — Es un proyecto que automatiza el despliegue de aplicaciones dentro de contenedores de software; como resultado, proporciona una capa adicional de abstracción y automatización de virtualización a nivel del sistema operativo.

ERP — Son un conjunto de sistemas que permiten la integración de ciertas operaciones del negocio. En consecuencia, ayudan a la planificación de los recursos empresariales.

Fintech — Estas son un dominio de actividad en el cual las empresas tecnológicas utilizan las tecnologías de la información y la comunicación para crear y/u ofrecer servicios financieros de forma más eficaz y menos costosa.

Gateway — Es un dispositivo, con frecuencia un ordenador, que permite interconectar redes con protocolos y arquitecturas diferentes.

Hardware — En informática se refiere a las partes físicas tangibles de un sistema informático: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos.

HCM — Es una aplicación especializada en el desarrollo de talento humano para la empresa, con una gestión optimizada de recursos en la nube.

Hibridad — En los modelos de nube, hace referencia a una forma de despliegue de soluciones tanto en nube como *on-premise*, por eso se conoce como modelos de nube híbridos.

IA — Es la abreviación de inteligencia artificial, también conocida como inteligencia computacional: la inteligencia exhibida por las maquinas.

IAAS — En informática, es la capacidad de ofrecer infraestructura como un servicio a las organizaciones que lo requieran. Algunas de las compañías especializadas en IaaS son AWS, Azure, entre otras.

Integridad — En informática, hace referencia a la propiedad que busca mantener los datos libres de modificaciones no autorizadas.

IOT — El internet de las cosas es un concepto que se refiere la interconexión digital de objetos cotidianos al internet.

ISO — Es un conjunto de normas establecidas por la Organización Internacional de Normalización. Se pueden aplicar en cualquier tipo de organización o actividad orientada a la producción de bienes o servicios.

Java — Es un lenguaje de programación de propósito general orientado a objetos y que está construido para tener pocas dependencias de implementación.

Kernel — En informática, es un software que constituye una parte fundamental del sistema operativo.

Microservicios — Es un enfoque para desarrollar una aplicación de software como una serie de pequeños servicios, en la que cada uno se puede ejecutar de forma autónoma y comunicándose entre sí.

Monitoreo — Es un proceso que las empresas realizan examinando los registros electrónicos de auditoria, en busca de indicaciones de actividades no autorizadas en relación con la seguridad; estas actividades se intentaron o realizaron en un sistema o aplicación.

Movilidad — En las entidades financieras, el término de movilidad hace referencia al uso de las tecnologías móviles para virtualizar las capacidades.

Nequi — Es una app desarrollada como una aplicación financiera de cuentas de bajo monto establecidas por el gobierno o cuentas CAD. Esta app fue desarrollada bajo un esquema de fintech, usando la nube de AWS.

NIST — Es el Instituto Nacional de Normas y Tecnología; es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos.

No repudio — En seguridad informática, hace referencia a la capacidad que les permite a los emisores o receptores probar que el mensaje fue enviado por el supuesto emisor.

On premise — Son aquellas capacidades que tienen las organizaciones de alojar, soportar y mantener sus aplicaciones en sus instalaciones o data center de la organización.

PAAS — Es un entorno de desarrollo e implementación bajo un esquema 100 % en la nube.

PHP — Es un lenguaje de programación de propósito general, de código del lado del servidor; fue diseñado originalmente para el desarrollo web de contenido dinámico

Push — Las Notificaciones Push son mensajes que se envían de forma directa a dispositivos móviles (Smartphone y/o Tablet) con sistema operativo iOS, Android, BlackBerry y/o Windows Phone. Las notificaciones Push ayudan a los desarrolladores independientes y dueños de aplicaciones a mantener informados a sus usuarios.

Python — Se trata de un lenguaje de programación multiparadigma, ya que soporta orientación a objetos, programación imperativa y, en menor medida, programación funcional.

SAAS — Es un modelo de distribución de software, donde el soporte lógico y los datos que maneja se alojan en servidores de una compañía de tecnologías de información y comunicación (TIC), a los que se accede vía Internet desde un cliente. La empresa proveedora TIC se ocupa del servicio de mantenimiento, de la operación diaria y del soporte del software usado por el cliente.

SMS — Servicio de Mensajes Cortos o Servicio de Mensajes Simples. Puede enviarse entre teléfonos celulares o móviles.

Software — Es un conjunto de programas y rutinas que le permiten a la computadora realizar determinadas tareas.

***Start-ups* —** Este término hace referencia a empresas o compañías emergentes que buscan arrancar, emprender o montar un nuevo negocio; aluden a ideas de negocios que están empezando o están en construcción, y generalmente se trata de empresas emergentes apoyadas en la tecnología.

Resumen

La arquitectura de seguridad para la gestión del riesgo bajo un esquema fintech está enfocada en generar un modelo que sirva de referencia a la industria financiera colombiana; esta desea incursionar de forma segura en los modelos financieros, bajo un esquema de computación en la nube. Además, este informe quiere demostrar que la amenaza que representan las fintech para el sector financiero puede convertirse en una oportunidad para mejorar los servicios financieros, de forma acorde con el mercado actual, garantizando la seguridad de la información de los clientes.

Este trabajo, aunque deja ver la problemática actual de los bancos ante la evolución de las fintech, tiene un propósito que va más allá de la evolución del modelo de negocio que el sector financiero debe llevar a cabo. Su objetivo principal es plantear los retos de seguridad que trae esta evolución y presentar un modelo viable, que sirva de insumo para cualquier entidad financiera colombiana que desee incursionar en un modelo de arquitectura en la nube. Este modelo debería cumplir con las normas colombianas y los estándares de seguridad requeridos, para garantizar la confidencialidad, la autenticidad, el no repudio y, ante todo, nunca poner en riesgo el patrimonio de los clientes.

Palabras clave: Computación en la nube, banca digital, seguridad en la nube, tecnología financiera, compañías emergentes

Abstract

The security architecture for risk management under a fintech scheme is focused on generating a model that serves as reference to the Colombian financial industry, that wants to penetrate financial models under a cloud computing scheme in a secure way. It is evident that the threat that fintech represents to the financial sector can become an opportunity to improve and evolve financial services according to the current market, always guaranteeing the security of customer information.

This work, while showing the current problems of the banks with the evolution of fintech, has a purpose that goes beyond the evolution of the business model that must be carried out by the financial sector. Its main objective is to raise the security challenges that this evolution brings and to present a viable model, that serves as the basic input for any Colombian financial institution that wishes to enter a model of architecture in the cloud that complies with Colombian norms and security standards. Such a model is always required to guarantee the confidentiality, authenticity, non-repudiation and, above all, never jeopardize the patrimony of the clients.

Keywords: cloud computing, digital bank, cloud security, fintech, Strauss

Introducción

Este trabajo tiene un doble propósito: mostrar los retos de las entidades bancarias ante la incursión de las *fintech* en el entorno financiero y describir las implicaciones de seguridad que estas traen consigo. Para esto, es importante entender que una fintech es una empresa tecnológica que busca ofrecer algunos servicios financieros. Este tipo de negocios representa un gran reto para las entidades financieras, debido a que las regulaciones de los bancos son muy estrictas; sin embargo, las fintech no están reguladas y demuestran mayor flexibilidad y agilidad a la hora de ofrecer algunos productos financieros.

La aparición de las fintech en el mundo financiero ha generado lo que podría llamarse un despertar de los bancos: buscan formas de trabajo más eficientes y, en algunos casos, convertirse ellos mismos en bancos fintech. Esto se presenta especialmente en Europa y Asia, donde las principales entidades financieras están adoptando esta innovación. No obstante, este cambio ha causado alarma en los bancos; se han descubierto algunos temas de seguridad que deben resolverse para proteger la información de los clientes y de sus productos financieros.

A nivel de seguridad, las entidades financieras tienen el reto de garantizar la confidencialidad de la información de sus clientes, así como de sus productos y servicios, bajo esquemas más agiles —como son los despliegues en la nube—. En este punto, surgen algunas dudas: por ejemplo, si el país donde está la nube es considerado un país seguro por la Superintendencia Financiera de Colombia. Este es solo el primer paso; después es necesario verificar cuál es el esquema de almacenamiento en la nube que más se ajuste a las necesidades del banco, y, además, hay que saber si cumple con los estándares de seguridad necesarios para

una entidad financiera. Una vez aclaradas estas cuestiones debe decidirse cuál es la posición de la entidad: ¿son las fintech una amenaza o una oportunidad?

Al respecto, es claro que el entorno ha cambiado y que los bancos deben cambiar. El concepto de banca fintech es una realidad y una oportunidad, que les permitiría a los bancos incursionar en un sector del mercado financiero que antes no era evidente, con nuevos actores y aliados. Aun así, dentro de esta evolución hay temas que deben abordarse de forma más detallada: la seguridad desde todos los ámbitos, como cumplimiento regulatorio, como confidencialidad y como seguridad de la información; el servicio; la disponibilidad, y la confianza de los clientes.

Planteamiento del problema

Problema**: seguridad y privacidad de la información en una arquitectura fintech para la evolución de la Banca Digital.**

Para entender los problemas de seguridad y privacidad en el sector y los bancos fintech, es necesario tener claridad sobre el fenómeno fintech y sobre cómo está influenciando el sector bancario. Por esto, a continuación, se presentará un breve contexto de la evolución de las fintech y del impacto que estas han generado en el sector financiero; asimismo, se describirá cómo ha repercutido en la seguridad y privacidad de la información.

En años recientes, el mundo ha sido testigo del crecimiento de las fintech y de cómo cobran cada vez más fuerza. Una señal clara de este crecimiento es que la inversión global en empresas fintech pasó de 4.050 millones de dólares, en 2013, a 12.200 millones, en 2014, y a 22.000 millones, en 2015 (Skan, Dickerson & Masood, 2014). El crecimiento acelerado de estas compañías tecnológicas, sumado al hecho de que muchos bancos tradicionales no están preparados para hacer frente a la revolución digital, ha encendido las alarmas de las principales entidades financieras.

El hecho de que muchos bancos no estén preparados para hacer frente a la revolución digital se debe en gran medida a su rigidez, complejidad y a las altas regulaciones del sector, que no permiten que tengan la flexibilidad para innovar que sí poseen las fintech (Skan et al., 2014; Sriram, 2011). Además del tema regulatorio, hay que tener en cuenta otro factor que es igual o más importante: la seguridad de la información. Sobre este tema no se encuentra mucha información acerca de las implementaciones realizadas, debido al nivel de confidencialidad y criticidad tanto para las fintech como para la banca. Por este motivo, no es posible identificar o

tener referencias del modelo de seguridad de una fintech o de una entidad financiera; esta información es sensible y puede ser usada para vulnerar la seguridad.

Actualmente, la mejor referencia para poder desarrollar un modelo de seguridad con arquitectura en la nube en una entidad financiera es la arquitectura de referencia de seguridad del NIST. Este, junto con otros organismos, es el encargado de plantear las actividades específicas encaminadas a acelerar la adopción de la computación en la nube. Estas actividades incluyen la creación de las Publicaciones Especiales del NIST (NIST SP), las cuales se ocupan de las definiciones, la arquitectura de referencia y de otros aspectos de seguridad (Primorac, 2015).

Ninguna entidad del sector financiero está exenta de esta realidad, como se pudo evidenciar en la duodécima edición del *World Retail Banking Report* (WRBR) de 2015, en donde se explica que la probabilidad de que los clientes dejen sus bancos ha aumentado en todas partes, desde casi 4 puntos porcentuales a más de 12 puntos porcentuales en el último año. Este problema también fue descrito en el artículo *Los retos de la banca tradicional*. En este documento puede apreciarse que la banca tradicional tiene una relación más débil con los clientes; allí es donde las fintech han surgido como grandes amenazas del modelo financiero tradicional (Noya, 2016).

Los datos mencionados anteriormente corresponden a las fintech de Europa y Estados Unidos; en estas regiones, las entidades han sido afectadas y prevén pérdidas de empleos financieros. La edición del primero de abril de 2016 del Financial Times señala que

> Los bancos europeos y estadounidenses eliminarán 1.7 millones de puestos de trabajo en la próxima década, conforme las compañías de tecnología financiera o fintech se enfocan en las

áreas de crecimiento rentable, como los préstamos y pagos, según predice un nuevo informe de Citigroup. (Noonan, 2016)

Justificación

Actualmente, las entidades financieras están afrontando una pérdida de mercado cercana al 24 %, a causa de la proliferación de las fintech (Price Waterhouse Cooper, 2016). Por esto, algunas han optado por incursionar en la digitalización de la banca mediante modelos de computación en la nube. Sin embargo, al tratar de cubrir la materialización de un riesgo se está abriendo la puerta a otros tipos de riesgo relacionados con la seguridad en la nube. En consecuencia, en este momento, las entidades financieras afrontan un gran reto: diseñar un modelo de arquitectura en la nube que garantice la seguridad de la información y que, al mismo tiempo, les permita mitigar el impacto de las fintech. Para poder tener una mejor perspectiva al respecto, se debe revisar el impacto que las fintech pueden tener en el negocio financiero y los riesgos de seguridad que afrontan las entidades financieras con la adopción de modelos de computación en la nube.

Hoy, las entidades financieras creen que el fenómeno fintech está transformando el sector financiero y que este podría poner en riesgo casi el 25 % de su negocio actual, concretamente, el 23 % en los próximos cinco años. Sin embargo, las fintech consideran que este porcentaje puede ser todavía mayor: podría llegar hasta el 33 % del negocio actual de las entidades financieras tradicionales. La banca *retail*, los medios de pago y los servicios relacionados con la gestión de activos y de patrimonio son, en este orden, los que van a experimentar un cambio más radical (Price Waterhouse Cooper, 2016).

El 83 % de los encuestados pertenecientes al sector financiero tradicional —bancos, compañías de seguros, agencias de valores, gestoras de activos, *brokers*, entre otros— reconoce que la llegada de nuevos competidores —como empresas tecnológicas, de comercio electrónico,

compañías de telecomunicaciones, *start-ups* y proveedores de infraestructuras— está teniendo un efecto disruptivo en el sector, hasta el punto de poner en riesgo parte de su negocio. La proporción anterior aumenta hasta el 95 %, cuando se les pregunta solo a los directivos de la banca (Price Waterhouse Cooper, 2016). Además de la pérdida de cuota de mercado, las fintech están presionando a la baja los márgenes y la rentabilidad de las entidades financieras, como reconoce el 67 % de los encuestados (Price Waterhouse Cooper, 2016).

Todos estos datos hacen parte de la *Encuesta Global Fintech 2016*; en esta, puede verse que un alto porcentaje del negocio financiero estará en riesgo en los próximos cinco años, como consecuencia de la aparición de las fintech. Aquí, se presenta este fenómeno con más detalle en la **FIGURA 1**; de igual manera, los detalles acerca de las principales amenazas que representan las fintech para las organizaciones financieras se pueden consultar en la **FIGURA 2**.

FIGURA 1: PORCENTAJE DEL NEGOCIO EN RIESGO EN LOS PRÓXIMOS CINCO AÑOS **COMO CONSECUENCIA** DE LA APARICIÓN DE LAS FINTECH **(PRICE WATERHOUSE COOPER, 2016).**

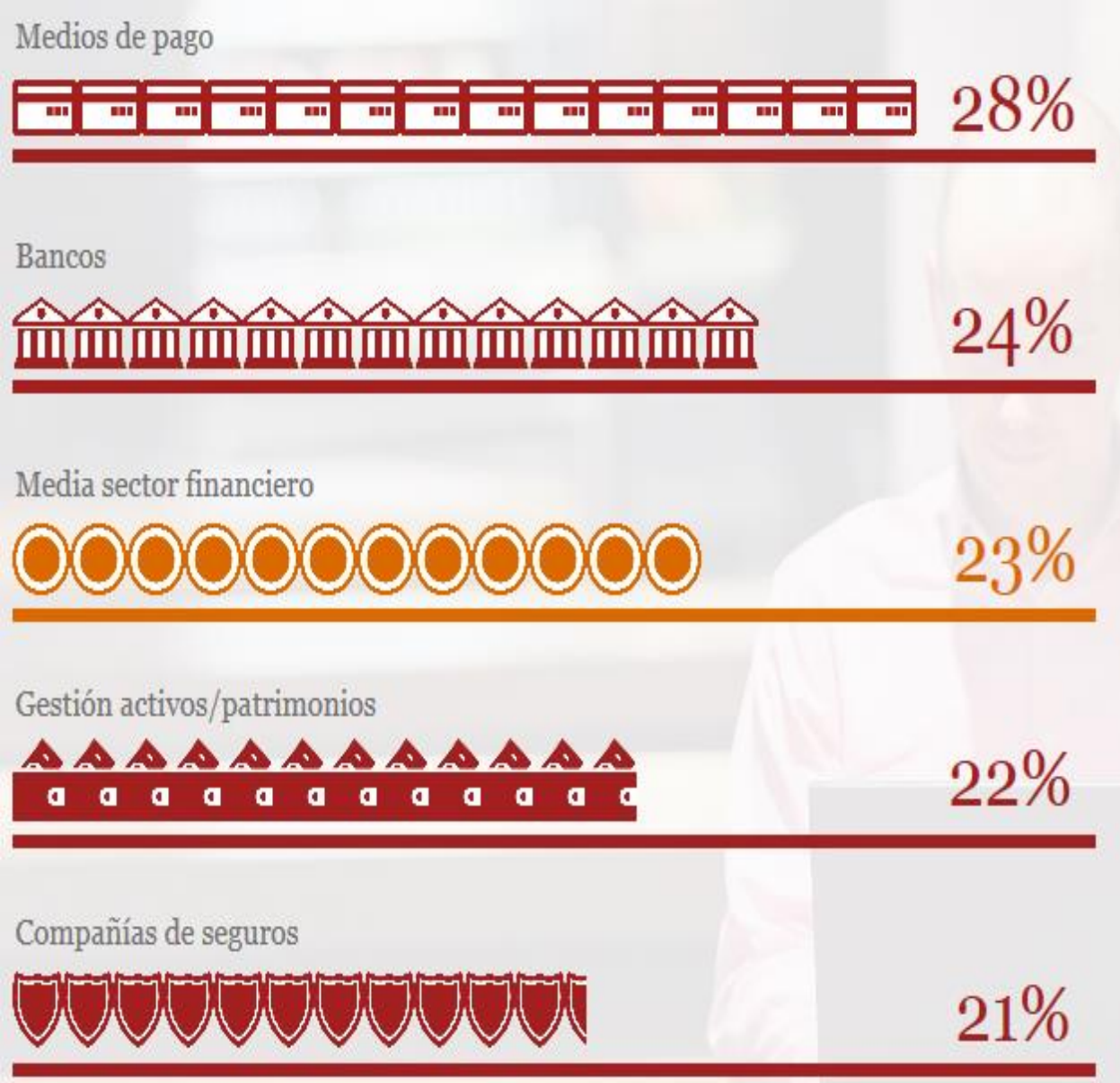
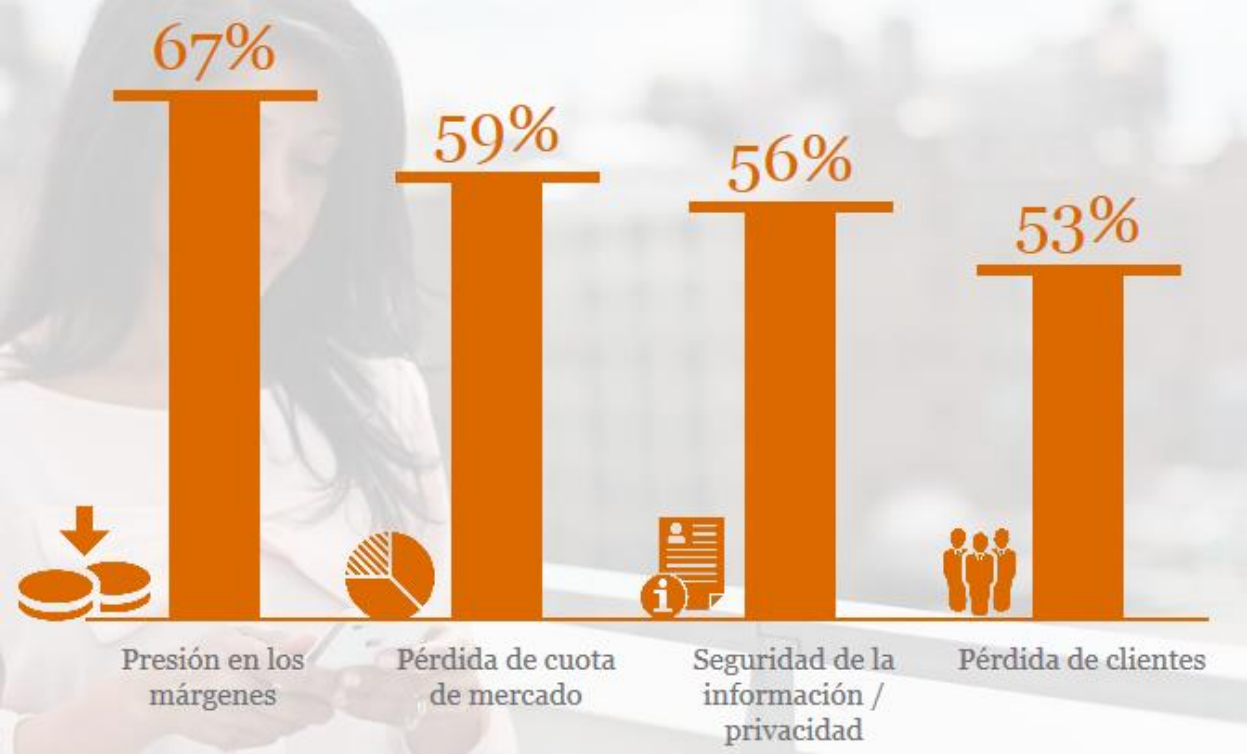


FIGURA 2: PRINCIPALES AMENAZAS QUE REPRESENTAN LAS FINTECH EN LAS ORGANIZACIONES FINANCIERAS (PRICE WATERHOUSE COOPER, 2016).



Considerando el fuerte impacto que han tenido las fintech en el sector financiero y la manera cómo han reaccionado los bancos con la digitalización de la banca, es importante entender los riesgos que implica la evolución de la banca hacia los modelos de nube, especialmente en los temas de seguridad. Actualmente, se calcula que el impacto económico por el cibercrimen es de unos USD $3 trillones a nivel mundial, una cifra incluso superior a la del narcotráfico (USD $1 trillón) ("El cibercrimen es un delito más rentable que el narcotráfico", 2015). Estos datos son mucho más alarmantes cuando se sabe que el número total de arremetidas cibernéticas por día supera los 6.600.000 millones y sigue creciendo. El sector financiero es el más afectado por este delito, con un 75.29 % de los ataques realizados, según la **TABLA 1**, presentada a continuación.

TABLA 1: ATAQUES INFORMÁTICOS EN AMÉRICA LATINA Y SU TENDENCIA A FUTURO ("EL CIBERCRIMEN ES UN DELITO MÁS RENTABLE QUE EL NARCOTRÁFICO", 2015).

SECTORES	ATAQUES POR DÍA	PORCENTAJE	TENDENCIA A FUTURO
Financiero	6.600.000	75,29%	Aumentarán
Gobierno	925.600	10,56%	Aumentarán
Comunicaciones	737.200	8,41%	Se mantendrá
Energía	325.347	3,71%	Descenderán
Industria	173.900	1,98%	Aumentarán
Comercio	3.600	0,05%	Aumentarán
TOTAL	8.765.647	100%	

Las estadísticas mencionadas anteriormente son impactantes, teniendo en cuenta el enfoque de la amenaza de las fintech a las entidades financieras y el alto crecimiento de ataques informáticos en Latinoamérica durante el 2015 y sus proyecciones. Aun así, es importante resaltar que hay un vacío sobre el que no se tiene información: la seguridad informática en la nube. Esto se explica porque no es posible conseguir información sobre ataques o vulnerabilidades en los grandes proveedores de nube como Amazon, Microsoft, Google, IBM u Oracle. A causa de su reputación y de la confianza con sus clientes, ninguno de estos proveedores revela qué ataques han recibido o cuáles vulnerabilidades han sido detectadas. Estos datos rara vez se hacen públicos, por lo que no puede saberse qué tan segura es la nube, excepto por las recomendaciones de las empresas de consultoría.

Objetivos

Objetivo general

Diseñar la arquitectura de seguridad para la gestión del riesgo en esquemas de banca digital que operen bajo un modelo fintech, en el contexto de la banca en Colombia.

Objetivos específicos

1. Plantear el desarrollo de una estrategia de banca digital que opere bajo un enfoque fintech, cuya arquitectura cumpla con los estándares de seguridad de confidencialidad, integridad y no repudio.

2. Elaborar un análisis de escenarios con tres modelos de nube (pública, privada e híbrida), que permita identificar los que más se ajusten a una arquitectura de seguridad bajo un modelo fintech.

3. Diseñar un modelo de arquitectura de seguridad en la nube para la banca digital, que opere bajo un esquema fintech.

4. Implementar una prueba de concepto en la nube del modelo de arquitectura diseñado, enfocado en las capacidades de autenticación.

Marco referencial

Marco contextual

La revolución digital se extiende de forma imparable en todos los sectores socioeconómicos, a través de *smartphones*, *tablets*, *wearables* y empresas fintech. En estas últimas es donde se nota una mayor relación con la trasformación que enfrenta el sector financiero (Pacheco Jiménez, 2016).

La denominación "fintech" es el acrónimo de "financial" y "technology": tecnología financiera. Se trataría, pues, de innovación tecnológica en los servicios financieros. En los últimos años, empresas de esta naturaleza, aprovechando las nuevas demandas de los usuarios en un contexto de evolución tecnológica, se especializaron en distintos campos de acción: pagos y transferencias, banca online, negociación, financiación colectiva o *crowdfunding*, seguridad y privacidad, criptomonedas, monederos digitales, entre otros. Entre sus peculiaridades destacan su enorme flexibilidad para incorporar cambios, debido a su reducida estructura de costes, y la falta de un marco legal que regule su actividad.

Así las cosas, y conscientes de que no pueden dejar pasar el tren de la revolución digital, la banca y el sector financiero están haciendo inversiones estratégicas en este ámbito. Su propósito es fomentar sus negocios mediante los servicios creados por los *startups* que deseen añadir a su cartera (Pacheco Jiménez, 2016)

Sin embargo —y son varias las voces que así lo consideran— la banca, además de proceder a la revolución digital, necesitaría reinventar su modelo de negocios sin descuidar su principal pilar: la seguridad. Debido a la difusión de las tecnologías de la información, la

mayoría de las organizaciones actuales están expuestas a una serie de riesgos derivados de una protección inadecuada o inapropiada de la información o de sus sistemas de tratamiento. En gran medida, esto puede explicarse por la evolución hacia entornos con acceso global y múltiple, con un aumento de la conectividad entre organizaciones y personas, cosa que plantea retos importantes para la gestión de la seguridad (Benítez Hernández, 2009).

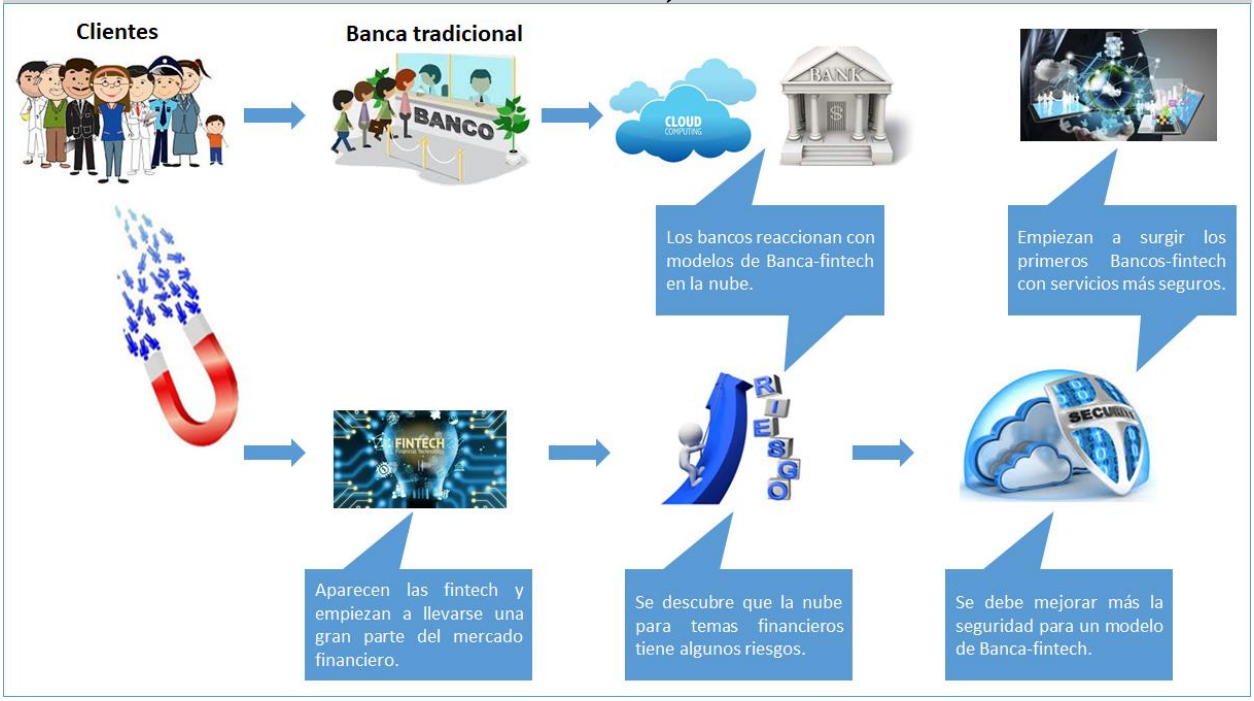
Ese cambio de rumbo tiene que ver con varios factores, como el alarmante aumento de los clientes dispuestos a abandonar sus bancos habituales; la aparición de sitios web de *crowdfunding*, y el desarrollo de prestamistas *peer-to-peer*, de proveedores de servicios online y de nuevos sistemas de pago (Pacheco Jiménez, 2016).

Marco conceptual

Para abordar el planteamiento del problema, es necesario aclarar los conceptos relacionados y sus diferencias. De esta forma, primero debe definirse el concepto de banca tradicional; luego, abordar cada uno de los conceptos necesarios para entender y analizar las diferencias que hay entre la banca tradicional y las fintech; finalmente, debe considerarse el impacto que estas generan en el sector bancario, especialmente en los aspectos de seguridad.

A continuación, la **FIGURA 3** mostrará cómo ha sido la evolución de la banca hacia el mundo fintech. Más adelante, se explicará de forma más detallada cada uno de los aspectos descritos en este marco conceptual.

FIGURA 3: MODELO CONCEPTUAL DE LA EVOLUCIÓN DE LA BANCA FINTECH (ELABORACIÓN PROPIA).



La gráfica anterior refleja la problemática que se pretende abordar en este proyecto. A continuación, un breve resumen.

La banca tradicional estaba acostumbrada a ofrecerles unos productos y servicios básicos especializados a todos sus clientes. Sin embargo, en los últimos 5 años han surgido las fintech, ofreciendo algunos de esos productos básicos bajo un esquema mucho más ágil y sencillo. Al ver esto, la banca empezó a ofrecer servicios que evolucionaron a modelos de nube, para poder competir de forma más oportuna con las fintech. Por otro lado, esto aumentó el nivel de riesgo de la banca, debido a los problemas de seguridad de la nube y el nivel de ataques recibido. Con el fin de contrarrestar estos peligros, los bancos decidieron mejorar la seguridad y convertirse en bancos fintech, mejorando la seguridad de los servicios ofrecidos.

Un banco es una institución de tipo financiero que se dedica a administrar el dinero, mediante servicios como el ahorro, la financiación y la inversión (Definición ABC, s.f). Estas

entidades conforman el sistema bancario, también conocido como banca, y son las que operan en una economía. Los bancos, normalmente, trabajan bajo normas legales estrictas y con tecnologías monolíticas bastante rígidas; por esto, la evolución de las entidades bancarias es muy lenta

Esta capacidad de respuesta paulatina ha generado mayor presión en los bancos para adaptarse a los nuevos cambios en el ambiente tecnológico; en consecuencia, ha aumentado la insatisfacción de los clientes con los niveles de calidad del servicio prestado. Los clientes actuales son más afines a la tecnología y demandan más servicios que estén al alcance de su mano. Ante esta oportunidad aparecieron las Fintech, para cautivar a los clientes insatisfechos, gracias a su agilidad, productos innovadores y pocas regulaciones.

La denominación “fintech” es el acrónimo de *financial* y *technology* o tecnología financiera; se trata de innovación tecnológica en los servicios financieros. En los últimos años, han proliferado las empresas de esta naturaleza, aprovechando las nuevas demandas de los usuarios en un contexto de evolución tecnológica (Skan et al., 2015; Pacheco Jiménez, 2016). Estas iniciativas se han especializado en distintos campos de acción: pagos y transferencias, banca online, negociación, financiación colectiva o *crowdfunding*, seguridad, privacidad, criptomonedas y monederos digitales. Entre sus peculiaridades, destaca su enorme flexibilidad para incorporar cambios, debido a su reducida estructura de costes y la falta de un marco legal que regule su actividad.

Teniendo en cuenta estos riesgos potenciales, las entidades financieras han visto la necesidad imperiosa de adaptarse a los nuevos tiempos. En consecuencia, los bancos están apostándole firmemente a la *digitalización de la banca* o la *banca digital* (Pacheco Jiménez,

2016). Los bancos han identificado que la banca digital es más que la transición de lo analógico a procesos digitales. Se trata de ser una empresa que crea valor digitalizado e ingresos de los activos digitales. La tecnología digital está transformando las instituciones financieras y requiere de un cambio estructural en la banca.

Por otra parte, la penetración de internet y de la telefonía móvil ha transformado profundamente los hábitos y preferencias de los consumidores, cada vez más acostumbrados a interactuar a través de medios digitales (Cuesta, Ruesta, Tuesta & Urbiola, 2015). Esto ha creado nuevas oportunidades para los bancos: pueden proporcionar una conveniente experiencia al cliente y multiplicar el número de clientes que pueden ser alcanzados.

Un objetivo clave de la banca digital es ofrecer una experiencia segura, digital e integrada para todos los clientes y socios, a través de todos los canales (en la sucursal, en casa o en la carretera). Si esto se logra, impulsa la lealtad y la repetición de negocios para los bancos. Por ejemplo, en una reciente conferencia bancaria en New York, se dijo que los bancos exitosos en el futuro tendrán que ser fintech o bancos fintech, ya que solo con la mezcla de sus servicios financieros con la tecnología específica dirigida a sus clientes se lograría innovar y ofrecer productos acordes con las necesidades del mercado y de la competencia actuales.

Bajo esta nueva premisa de la banca digital ha surgido el *cloud computing.* Este modelo permite el acceso bajo demanda —en forma ubicua, conveniente, compartida y a través de la red— a un conjunto de recursos informáticos configurables: redes, servidores, almacenamiento, aplicaciones y servicios. Dichos servicios se pueden aprovisionar o liberar rápidamente, con un esfuerzo mínimo de gestión e interacción por parte del proveedor de servicios (Noceti & Freijo, 2015). El término “ubicuo” da idea de la disponibilidad permanente en el tiempo, desde

cualquier lugar y a través de cualquier dispositivo, para hacer uso de los servicios de IT ofrecidos en el modelo *cloud*.

Características del Cloud Computing.

El concepto de *cloud computing* también se asocia a las siguientes características:

Abstracción de toda implementación física. Permite que los usuarios finales y los desarrolladores de aplicaciones en la nube no necesiten conocer la ubicación física de los servidores y sistemas de almacenamiento de datos, así como tampoco la administración y operación de esos entornos.

Virtualización de la tecnología. Esto posibilita que pueda ejecutarse más de un servidor lógico o virtual en un mismo servidor físico, con diferentes sistemas operativos y compartiendo los recursos de procesamiento disponibles.

De esta manera, la computación en la nube —*cloud computing*— se convierte en un aliado estratégico para apoyar el rápido crecimiento de las fintech y de los bancos que estén incursionando en el mundo de la banca digital. Esto puede explicarse porque "la computación en la nube no sólo tiene el potencial de llegar a ser la tecnología que definirá el siglo veintiuno, sino que es el servicio definidor, como fue la electricidad en el siglo veinte" (Merrill & Kang, 2014). Es el equivalente a volver a alambrar el mundo, desde Edison hasta Google.

> Lo que sucedió con la generación de energía eléctrica un siglo atrás está sucediendo ahora con el procesamiento de información. Los sistemas privados de computación, construidos y operados por compañías individuales, están siendo suplantados por servicios prestados a través de una malla común por plantas procesadoras de datos centralizadas. Sin embargo, cuando se habla de la

> nube, se debe tener presente que, en función de las necesidades de cada organización, los servicios ofrecidos a través de la nube pueden ser de diversa naturaleza y, por lo tanto, la sensibilidad de los datos a procesar, así como el acceso a los mismos también difieren.

En consecuencia, no debería extrañar el hecho de que las organizaciones que hacen uso del *cloud computing* requieran tipologías con distintas políticas de acceso, por lo cual se hace importante enfocar el análisis en los tipos de nube —pública, privada e hibrida— que más se adapten a las entidades bancarias, teniendo como foco principal los siguientes criterios y características (Camps & Oriol, 2012):

Nube privada o Private Cloud. La infraestructura de una nube privada es gestionada y utilizada por una única organización. La gestión puede delegarse en un tercero, pero bajo supervisión directa de la organización. Asimismo, la nube puede estar dentro de los límites físicos de la organización o fuera de la misma.

El rasgo distintivo de este tipo de implementación es que la seguridad física y lógica, así como la operación y administración, es realizada por la misma organización propietaria de la nube privada. Esta organización es la que adopta las características del modelo de la tecnología de *Cloud Computing*, para concentrar el acceso de todos los usuarios, locaciones y departamentos de una organización a un conjunto de recursos que se brindan a través de la nube (Noceti & Freijo, 2015).

Nube pública o public cloud. Se trata de infraestructura tecnológica (hardware, software de base, aplicaciones y servicios) que está disponible para el uso del público general. Este tipo de "nube" puede ser gestionado por una empresa, por una entidad académica o gubernamental o por combinaciones de estas. Por lo general, una *public cloud* se aloja en más de un *data center* del

cloud provider, ubicado en diferentes sitios geográficos; los servicios se ofrecen a múltiples consumidores de nubes que comparten los mismos recursos. La gestión de seguridad, la provisión de los recursos y el mantenimiento en funcionamiento de la infraestructura ofrecida es responsabilidad directa del proveedor de nube (Noceti & Freijo, 2015).

Nube híbrida o hybrid cloud. Es la composición de dos o más nubes (ej. privada y pública) que siguen siendo entidades únicas, pero que se integran entre ellas por tener tecnologías compatibles que les permiten compartir datos y aplicaciones y ser portables entre ellas.

Este modelo de despliegue de la tecnología de nube es aplicable por aquellas organizaciones que, por motivos de seguridad, deciden implementar una nube privada. En esta instalan sus aplicaciones críticas y datos de producción sensibles. Por otro lado, integran las nubes privadas con nubes públicas, con la finalidad de que estas últimas provean recursos en casos de picos de demanda, para la instalación de ambientes no productivos (ej.: desarrollo y *testing* de aplicaciones) y para uso de aplicaciones no críticas, aplicaciones de apoyo al negocio, ambientes de recuperación de desastres, entre otros (Noceti & Freijo, 2015).

Para entender un poco mejor los modelos de despliegue de nube, se presenta a continuación la **TABLA 1: CRITERIOS DE SELECCIÓN DE NUBE**. En esta figura se evalúan los escenarios de nube previamente mencionados, teniendo en cuenta sus principales características, ventajas y desventajas, para facilitar la selección de un modelo de nube acorde con las necesidades de una organización.

TABLA 2: CRITERIOS DE SELECCIÓN DE NUBE

	Privada	Pública	Híbrida
Visibilidad y acceso	Organización	Todo el mundo	Depende de la información a la que se quiera acceder
Gestión de la infraestructura	Organización/ Proveedor	Proveedor	Organización/ Proveedor
Localización	Organización/ Proveedor	Proveedor	Organización/ Proveedor
Aplicación típica	Es una nube que trabaja con datos especialmente sensibles; por ejemplo, bancos.	Es un servicio que se contrata para publicar información que debe transmitirse al mayor número de personas; por ejemplo, el *streaming*.	Se usa cuando se quiere distinguir el tratamiento de la información dentro de una organización, según el tipo de servicio. Por ejemplo, se usa la parte pública para el correo electrónico, y parte privada, para datos analíticos.

	Privada	Pública	Híbrida
Escalabilidad	**Media–Baja** Necesidad de invertir en nuevos equipos, a medida que aumente la capacidad.	**Alta** Fácil escalado de aplicaciones sobre múltiples servidores.	**Media-Alta** Posibilidad de derivar picos de procesos y sobrecargas de trabajo sobre la nube pública, en caso de necesidad.
Rendimiento	**Alto** Gran capacidad de la red (local) al servicio *Cloud*.	**Medio-Bajo** Recursos compartidos por gran número de usuarios. Dependencia de la capacidad de la red de acceso al servicio *Cloud*.	**Medio-Alto** El contenido en el caché se almacena localmente.
Fiabilidad	**Alta** Todos los equipos pertenecen a la organización.	**Media** La fiabilidad depende de la conectividad a internet y de la disponibilidad del servicio ofrecido por el proveedor.	**Media-Alta** El contenido en el caché se almacena localmente. La fiabilidad depende de la conectividad a internet y de la disponibilidad del servicio ofrecido por el proveedor.

	Privada	Pública	Híbrida
Costo	**Alto** Requiere de equipamiento a nivel local (*Data Center*, electricidad y refrigeración). Al costo se agrega la implementación y el mantenimiento de los equipos. Se agregan nuevos procesos operativos en la gestión de activos IT.	**Bajo** Modelo de pago *pay-as-you-go*; no necesita almacenamiento local (infraestructura *off-site*).	**Medio** Permite migrar a la nube gran parte de los equipos, hacia un modelo *pay-as-you-go*.
Características generales	El negocio gira en torno a los datos de la empresa y a las aplicaciones (la seguridad es crucial). Aparece la necesidad de respetar estructuras y políticas de seguridad y confidencialidad de datos. Hay un alto número de usuarios a nivel interno. Se adquiere la capacidad de gestionar de manera autónoma, eficiente y efectiva *Data Centers* de nueva generación.	La carga de trabajo estándar necesita de aplicaciones empleadas por muchos usuarios (p. ej. e-mail). Es necesario probar y desarrollar las aplicaciones. Se dispone de aplicaciones SaaS con un alto nivel de seguridad. Se necesita una capacidad incremental (en otras palabras, añadir capacidad de computación en picos de carga). Se realizan proyectos de colaboración con otros usuarios y/o organizaciones.	Empleo de aplicaciones SaaS; pero con la exigencia de cumplir con estrictas medidas de seguridad. Existen datos privados de crucial importancia, así como información menos crítica.

Hoy siguen existiendo una serie de riesgos legales y de seguridad, a pesar de la rapidez en el crecimiento de las estas empresas y de la gran cantidad de innovaciones introducidas en multitud de productos y servicios financieros, innovaciones de las que ya muchos se benefician actualmente. Estos riesgos necesitan ser tomados en cuenta; obviarlos podría suponer penalizaciones no sólo económicas, sino de reputación, y, en el peor de los casos, causar el cierre de la empresa (Signaturit, 2016).

Por este motivo, para no caer en estos riesgos, las entidades bancarias deben ser muy cuidadosas al momento de evolucionar hacia el mundo fintech con tecnologías en la nube. Entre las posibles complicaciones se incluyen el riesgo de incumplimiento normativo, el riesgo de infringir el derecho a la privacidad de los clientes y el riesgo de sufrir un ciberataque. Como puede verse, los riesgos son altos y, si se considera un poco más lo hasta ahora expuesto, tanto en el segundo como en el tercer riesgo la seguridad es el factor clave: es ahí donde hay que hacer el mayor esfuerzo (Signaturit, 2016).

Marco legal

Para conocer los aspectos legales implicados, es importante partir de lo que ha manifestado la Superintendencia Financiera — la institución gubernamental encargada de regular todos los temas normativos asociados con las entidades financieras, según la legislación colombiana—. Para esto, se comenzará con los conceptos 2015019296-001 del 16 de abril de 2015 (*Servicios en la nube, contratación de servicios de terceros*) y el 2017059546-001 del 20 de junio de 2017 (*Servicios en la nube, seguridad y calidad de la información*).

Las reglas citadas son una muestra de que en la legislación colombiana no existe una norma que regule de manera específica la contratación de servicios en la nube por parte de

entidades financieras. Sin embargo, es importante señalar que la Ley 1341 de 2009 consagra los principios sobre "la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones". Entre estos, se encuentra el de neutralidad tecnológica, previsto en el numeral 6, artículo 2.

Acerca de la contratación de personas naturales o jurídicas bajo la modalidad de *outsourcing* o tercerización, debe aplicarse el numeral 2.3.6 del Capítulo I, Título II, Parte I de la Circular Básica Jurídica (CE 029 de 2014). Este reglamento establece los requerimientos mínimos que una empresa debe cumplir en estos casos. Las entidades financieras requieren este tipo de contratación para la atención parcial o total de los distintos canales o dispositivos usados en ellos o durante el desarrollo actividades en las que se acceda a información confidencial de la entidad o de sus clientes.

Además, debe considerarse que, en materia de seguridad y calidad de la información, hay normas de control interno para la gestión de la tecnología, así como reglas relativas a la administración del riesgo operativo SARO, entre otras. Todas estas son de obligatorio cumplimiento por parte de las entidades vigiladas por la Superintendencia Financiera. La Circular Externa 029 de 2014 (Circular Básica Jurídica) y la Circular Externa 100 de 1995 de Superintendencia Financiera (Circular Básica Contable y Financiera) regulan cada uno de estos aspectos. Esta normativa tiene plena aplicación en los servicios de computación en la nube implementados por las entidades vigiladas.

En consecuencia, puede decirse que el Estado garantiza la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia; estas permiten fomentar la prestación eficiente de servicios,

contenidos y aplicaciones que usen Tecnologías de la Información y Comunicación. Además, el Estado vela por la libre y leal competencia, y porque su adopción sea armónica con el desarrollo ambiental sostenible.

Además de los aspectos mencionados anteriormente, es necesario tener en cuenta que en "el tratamiento de la información bancaria en la nube o *cloud computing* a nivel bancos" deben considerarse las exigencias previstas para la transferencia de datos internacionales. Sobre este punto es preciso indicar que Ley 1581 de 2012, artículo 26 y la Ley 1266 indican bajo qué criterios debe tratarse esta información, entre otras leyes de seguridad informática y del sector financiero que se verán más adelante (Superfinanciera, 2017).

Es un paso muy importante que resuelvan todos los temas de seguridad. Sin embargo, para garantizar la seguridad, no basta con identificar los factores de riesgo. Además, al escoger el tipo de nube que se va a implementar, también deben identificarse las normas legales pertinentes. Esto podrá apreciarse con más detalle a continuación, al recopilar las normas legales que las entidades financieras deben tener en cuenta en Colombia cuando adoptan alguno de estos servicios.

Leyes de seguridad informática y del sector financiero.

En primer lugar, se analizará la Ley de Protección de Datos Personales o Ley Estatutaria 1581 de 2012. Los antecedentes de esta normativa se basan en que la información es el activo más importante en el mundo actual; por ello, era necesario dictar las disposiciones generales para la protección de datos personales.

Esta ley regula el derecho fundamental del *habeas data* y señala la importancia del mismo, tal como lo corrobora la Sentencia C–748 de 2011 de la Corte Constitucional, donde se estableció el control de constitucionalidad de la ley en mención. Esta nueva ley busca proteger la información personal registrada en cualquier base de datos que les permita a entidades públicas y privadas realizar diferentes operaciones: recolección, almacenamiento, uso, circulación o supresión (en adelante, se aludirá a todas estas acciones como tratamiento). Esta ley también enumera los países que se consideran seguros para almacenar información de los clientes colombianos, esto fue avalado por la circular 005 del 2017, sobre el *habeas data* (Congreso de la República, 2012).

Esta misma ley ampara el Decreto 1377 de 2013, cuyo objetivo es facilitar la implementación y el cumplimiento de la Ley 1581, reglamentando aspectos relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, las políticas de tratamiento de los responsables y encargados, el ejercicio de los derechos de los titulares de la información, entre otros.

Ya esbozada brevemente la Ley de Protección de Datos Personales, es pertinente presentar la Ley de Delitos Informáticos: la Ley 1273, también conocida como Ley de la Protección de la Información y de los Datos (Congreso de la República, 2009); sin embargo, no se explicará cada uno de sus artículos. En este caso, se señalarán los artículos que mencionan los riesgos más factibles de materializarse en la computación en la nube.

Los riesgos identificados son los siguientes:

Artículo 269A: acceso abusivo a un sistema informático

Artículo 269C: interceptación de datos informáticos.

Artículo 269D: daño informático.

Artículo 269F: violación de datos personales.

Artículo 269J: transferencia no consentida de activos.

También puede encontrarse una revisión a alto nivel de la ley 1266 de 2008, por la cual se dictan las disposiciones generales del *habeas data* y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países. Finalmente, se dictan otras disposiciones.

Sobre esta ley en particular se mencionarán algunos de los artículos, pero solo van a considerarse en detalle los más relevantes. Los artículos más importantes son para esta investigación se enumeran a continuación (Congreso de la República, 2008):

Artículo 4: principios de la administración de datos.

Artículo 5: circulación de información.

Artículo 10: principio de favorecimiento a una actividad de interés público.

Artículo 11: requisitos especiales para los operadores.

Artículo 12: requisitos especiales para fuentes.

Artículo 13: permanencia de la información.

Artículo 14: contenido de la información.

Artículo 15: acceso a la información por parte de los usuarios.

Por último, hay que incluir una de las normativas más importantes para la privacidad de la información en la nube: “ISO27018”, publicada el 29 de julio de 2014. Este documento establece criterios sobre controles y directrices, en relación con las medidas de protección de información de identificación personal (PII), en conformidad con los principios de privacidad en la norma ISO / IEC 29100. Estos principios están orientados a entornos de trabajo con sistemas de almacenamiento público en la nube.

La ISO 27018 es un código de buenas prácticas para los controles de protección de datos en servicios de computación en la nube. Esta norma se complementa con la norma ISO 27001 e ISO 27002, en el ámbito de gestión de la seguridad de la información, y se dirige de forma específica a los proveedores de servicios de nube.

El objetivo perseguido por la norma ISO 27018 es crear un conjunto de normas, procedimientos y controles. Mediante estos, los proveedores de servicios en la nube que actúan como “procesadores de datos” podrían garantizar el cumplimiento de las obligaciones legales en materia de tratamiento de los datos personales. Al mismo tiempo, esta normativa les proporciona a los consumidores potenciales de servicios en nube una herramienta comparativa útil, para que estos ejerzan su derecho de verificar y auditar los niveles de cumplimiento de las regulaciones establecidas por el proveedor (Camps & Oriol, 2012).

Conpes 3854**.** El Consejo Nacional de Política Económica y Social (Conpes), busca establecer las bases y lineamientos futuros de la seguridad en el entorno digital. Este objetivo se persigue teniendo en cuenta que el creciente uso del entorno digital en Colombia, en donde se desarrollan actividades económicas y sociales, acarrea incertidumbres y riesgos inherentes de seguridad digital; estos riesgos deben ser permanentemente gestionados.

Por estos motivos, la Política Nacional de Seguridad Digital —objeto principal del documento Conpes 3854— cambió el enfoque tradicional, incluyendo la gestión de riesgo como uno de los elementos más importantes para abordar la seguridad digital. Esto se hizo bajo cuatro principios fundamentales y cinco dimensiones estratégicas, que regirían el desarrollo de esta política. Entre los primeros destaca que la Política Nacional de Seguridad Digital debe involucrar activamente a todas las partes interesadas y asegurar una responsabilidad compartida entre las mismas. Cada uno de los principios se refleja en las dimensiones en las que actuará esta política; estas determinan las estrategias para alcanzar su objetivo principal: fortalecer las capacidades de las múltiples partes interesadas. Su objetivo es identificar, gestionar, tratar y mitigar los riesgos de seguridad digital, en el marco de las actividades socioeconómicas del entorno digital (Conpes, 2016).

Estado del arte

Se puede concluir, según lo explicado anteriormente, que la amenaza de las fintech es un hecho global y contundente para las entidades bancarias; Colombia no está exenta de este desafío. Esto se hizo evidente en marzo de 2016, durante el evento de *Finnosummit*, en dónde se concluyó que Colombia es un país donde el ecosistema emprendedor fintech está emergiendo a una velocidad vertiginosa. En el mapeo que realizó esta institución, se identificaron 70 *startups* fintech colombianas que están cambiando las reglas del juego. No es casual que los dos startups fintech más prometedoras de Sudamérica —ganadoras de la reciente competencia regional *Finnosummit Challenge*— sean de Colombia (Martin, 2016).

Para entender un poco mejor hacia dónde se están enfocando las fintech colombianas, puede consultarse la **FIGURA 4**. Esta es una adaptación de la información tomada del Radar

Fintech Colombia, donde se pueden identificar los mercados a los que actualmente apuntan las fintech.

FIGURA 4: PRINCIPALES FINTECH EN COLOMBIA (MARTIN, 2016)

Las entidades financieras son poco flexibles y agiles para realizar cambios; además, las fintech pueden tener un alto impacto en sus modelos de negocio. Teniendo en cuenta esta problemática, es importante que las entidades financieras evalúen cuál de los modelos de nube se adapta mejor a este entorno de la digitalización de la banca, para crear sinergias con aliados estratégicos: medios de transporte, cadenas de supermercados, estaciones de gasolina, peajes, impuestos, etc. Además, esto mejoraría su agilidad, servicio personalizado y capacidad de respuesta a las crecientes fintech (Skan et al., 2015; Noya, 2016).

Esto lleva a las entidades bancarias a preguntarse si la evolución hacia el mundo fintech con tecnologías en la nube es la mejor forma, garantizando siempre la seguridad, de afrontar la amenaza de las fintech. Sin embargo, para poder tener claridad sobre este panorama, es necesario entender cómo ha sido la evolución de las fintech y su impacto en las entidades bancarias. Para esto, es necesario hacer un análisis detallado de cómo ha sido el surgimiento y evolución de las fintech; esto permitirá entender el impacto que están teniendo sobre el sector financiero y la manera en la que producen una revolución digital. En consecuencia, las entidades bancarias se están viendo obligadas a iniciar un proceso disruptivo que les permita rediseñar su negocio para poder seguir siendo competitivos. Parte de ese proceso disruptivo es la adopción de la nube, como un mecanismo que les permita ser más agiles y oportunos en los despliegues de nuevas soluciones y en la evolución de su negocio.

Surgimiento **de** las fintech**.** Las fintech son una nueva forma de ofrecer servicios financieros a través de la tecnología. Ya sea directamente con los clientes (B2C) o proporcionando a los bancos soluciones innovadoras de marca blanca (B2B), las empresas fintech crean una experiencia financiera más atractiva y transparente. Esto incluye desde

intercambio de divisas (*TransferWise*) hasta billeteras móviles (*mobile wallets*) o la gestión de finanzas personales (Gardiner, 2016). Sin embargo, el término "fintech" no es tan nuevo como se cree normalmente; fue concebido en el año de 1972 por David Stolin, profesor de finanzas en la Toulouse Business School, a quien se le atribuye la primera mención del término "fintech".

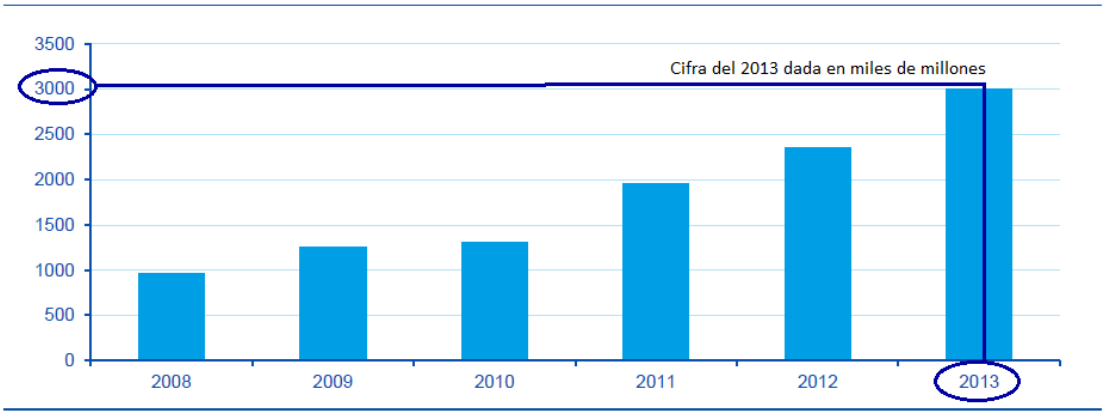
Hasta donde se sabe, el término fintech se dejó de lado hasta su moderno resurgimiento, durante el siglo XXI; sin embargo, no hay registros de la fecha exacta de su resurgimiento.

El impacto de las fintech en la banca**.** En los últimos años, *startups* de alto componente tecnológico han irrumpido en el sector financiero, aprovechando la brecha existente entre las nuevas demandas de los clientes y los servicios, en ocasiones obsoletos, que ofrecen los bancos tradicionales, lastrados por el peso de su regulación, estructura y cultura corporativa. Estos nuevos competidores, conocidos como compañías fintech, desagregan la cadena de valor de los bancos al especializarse en sus distintos componentes: pagos, cambio de divisas, crédito, acceso a los mercados de capitales, asesoramiento financiero, etc.

Basándose en las nuevas tecnologías, las fintech se caracterizan por disponer de una gran flexibilidad y agilidad para incorporar cambios y por tener una estructura de costos reducida. Además, en la mayoría de los casos, presentan modelos de negocio profundamente redefinidos, que suponen auténticas disrupciones respecto al negocio tradicional. Este es el caso, por ejemplo, de las plataformas de *crowdfunding* financiero y de las monedas virtuales, que tienen el potencial de des-intermediar completamente a los bancos.

Las expectativas generadas por las compañías fintech han atraído un volumen creciente de inversión en los últimos años, cercano a los 3.000 millones de dólares en 2013. Estos datos pueden dimensionarse a continuación, en la **FIGURA 5**.

FIGURA 5: INVERSIÓN GLOBAL EN EMPRESAS FINTECH (CUESTA ET AL., 2015)



La apuesta de los bancos más digitales**.** Una vez planteados los potenciales riesgos y siendo conscientes de la necesidad imperiosa de acoplarse a los nuevos tiempos, los bancos se percataron de que deben hacer una apuesta firme por la banca digital. De esta forma, necesitan promover que sus operaciones y procesos se puedan realizar a través de *smartphones*, *tablets* u ordenadores. El problema práctico es que conviven dos realidades diferentes difíciles de sostener económicamente: por un lado, la inversión que los bancos necesitan para competir con las fintech; por otro, la banca tradicional, con toda su infraestructura física y monolítica (Pacheco Jiménez, 2016; Niazmand, 2015).

La computación en la nube ***(cloud computing)*.** La computación en la nube es una práctica que contempla el acceso por demanda de *hardware*, *software* y servicios de un tercero, por medio de internet, con el objetivo de reducir costos de infraestructura. Bajo una perspectiva global a nivel empresarial, las entidades financieras que adopten la computación en la nube no solo reducirán costos en el área de tecnología, sino que también podrán enfocar sus procesos y recursos en profundizar sus actividades de negocio. En consecuencia, podrán orientarse a maximizar la cartera de productos ofrecidos a sus clientes actuales y, además, a captar otros nuevos.

Tener una capacidad tecnológica ágil y flexible, con capacidad de responder adecuadamente a las demandas del negocio, favorecería la alineación del área de tecnología informática (T.I.) con el negocio. Esto se lograría generando una ventaja competitiva que acelere el aumento de rentabilidad.

Todo esto les permite a las entidades bancarias tener un modelo para habilitar el acceso ubicuo, conveniente y bajo demanda, por medio de la red, a un *pool* compartido de recursos computacionales configurables. Estos pueden ser rápidamente aprovisionados y liberados, con un esfuerzo mínimo de administración o de interacción del proveedor (Camps & Oriol, 2012; Fielder & Brown, 2012; Cuesta et al., 2015).

La nube como una opción para la transformación digital**.** La computación en la nube ha experimentado un rápido crecimiento durante los últimos años, y se espera que se siga desarrollando cada vez más. Los servicios en la nube serán más rentables en aplicaciones de negocio; transformarán los servicios en servicios basados en la nube. Este cambio es especialmente necesario para aplicaciones del tipo ERP (*Enterprise Resource Planning*) o CRM (*Customer Relationship Management*).

Los bancos son un segmento importante en el área del negocio de la computación en la nube, debido a que los bancos estarían incursionando en estos modelos durante los próximos años. Hay muchas ventajas que ofrece la nube para los bancos como clientes: en primer lugar, el ahorro de costos que se lograría utilizando servidores en la nube en lugar de servidores tradicionales; por otra parte, la nube ofrece la facturación basada en el uso, la continuidad del negocio, la agilidad del negocio, TI verde, entre otros (Bogdan, 2015).

Viabilidad de la computación en la nube para las entidades financieras**.** La utilización de la computación en nube es una realidad innegable para los usuarios individuales y corporativos. El interés por su implementación ha llevado a que se realicen esfuerzos para aprovechar su potencial en diversas industrias, entre ellas la actividad financiera, en la que ya se ha comenzado a experimentar su uso.

En las entidades financieras —donde se da un uso significativo de la información—, la computación en la nube puede brindar importantes ventajas para mejorar la gestión. Entre estas se cuenta la posibilidad de usar diferentes servicios computacionales, en función de las necesidades de cada momento: almacenamiento, capacidad, ancho de banda, etc. Como resultado, las organizaciones adquirían mayor agilidad mediante la expansión o reducción en el aprovisionamiento y el uso de recursos de *hardware* y *software*, atendiendo a los picos operacionales (López, 2014).

Modelos de despliegue**.** Cuando se habla de computación en la nube, es importante entender que existen varios tipos de despliegue; algunos de ellos se evaluarán durante el desarrollo del proyecto. A continuación, se describirán los tres modelos de nube seleccionados para ser evaluados.

Nube privada. La infraestructura de nube es operada únicamente para una organización, esta puede estar dentro de la misma empresa o con un tercero.

Nube pública. La infraestructura de nube se pone a disponibilidad del público en general o de un gran grupo industrial. Es propiedad de una organización que vende servicios de nube; no hay separación física de la infraestructura, solo hay separación lógica.

Nube híbrida. La infraestructura de nube es una composición de dos o más modelos de despliegue de nube; estos permanecen como entidades únicas, pero son unidos entre sí por medio de una tecnología estandarizada o propietaria, que permite portabilidad de datos y aplicación (Bruno, 2013).

Evolución de los aspectos legales en los temas de la nube**.** Gracias al vertiginoso incremento a nivel mundial en el almacenamiento de datos de carácter personal a través de diversos medios digitales y virtuales, el intercambio de información entre personas y empresas se basa en un único objetivo: mantener la confidencialidad, integridad y disponibilidad de la información personal.

Muchos países en el mundo han establecido leyes cuyo principal objetivo es proteger la información. En 1973, Suecia fue el primer país en el mundo en definir una ley de protección de datos; luego Estados Unidos, en 1974; más adelante, Canadá, Francia, Dinamarca, Noruega, Austria, entre otros países, empezaron a promulgar leyes de este tipo.

Sin embargo, en el análisis de estas leyes, se observa que estas no contemplan el tratamiento de datos personales en servicios de computación en la nube. Países como UE, Argentina, Suiza o Canadá consideran "puertos seguros" a los países donde es posible transferir datos de forma segura, considerando que, si entre estos se almacena información, estará cobijada por la ley de su país. Adicionalmente, en los contratos deberá existir una clausura que garantice esta legislación.

Muchos de los proveedores de *cloud computing* ofrecen sus servicios, pero no indican en qué país están alojada la información. Sabiendo esto, Francia está invirtiendo millones de euros

en el diseño de su propia nube, para evitar que empresas o personas de su país almacenen información en otras nubes por fuera de su jurisdicción (Jiménez Hidalgo, s.f).

Colombia no es ajena a la necesidad de leyes de protección de datos, con las que pueda estar en el grupo de los países que participan en "Puerto seguro", acreditados por la Comisión Europea. Por ello, hoy cuenta con un conjunto de leyes que facilitará el desarrollo de la computación en la nube (*cloud computing*) en las empresas colombianas. A continuación, se mencionan estas:

Ley 1266 de 2008 (Colombia). Mediante esta ley se dictan las disposiciones generales y se regula el manejo de la información contenida en bases de datos personales; en especial, se estipula el manejo de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones (Alcaldía de Bogotá, 2008).

Ley 1273 de 2009 (Colombia). Mediante esta ley se modifica el Código Penal, se crea un nuevo bien jurídico tutelado —denominado "de la protección de la información y de los datos— y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones (Alcaldía de Bogotá, 2009).

Ley 1581 de 2012 (Colombia). Mediante esta ley se dictan disposiciones generales para la protección de datos personales (Certicámara, 2013). Además de estas leyes, Colombia cuenta con la Norma ISO 27018, que proporciona orientación destinada a garantizar que los proveedores de servicios en la nube puedan ofrecer **controles adecuados de seguridad de información**, con el objetivo de proteger la privacidad de los clientes.

Riesgos a nivel de seguridad de la nube en entidades financieras**.** Hoy, los servicios informáticos en la nube tienen algunas desventajas que detienen a los bancos en el momento de adoptar la nube: seguridad, confidencialidad de los datos y calidad de los servicios.

En el sector financiero, la principal barrera para la implementación de los servicios en la nube es la inseguridad. Esto se explica por el volumen significativo de datos sensibles que se manejan. Los bancos son obligados a utilizar aplicaciones basadas en normativas y rigurosos marcos de referencia; por esto, se enfrentan a las mayores restricciones para la utilización de la nube. Hay quienes consideran este riesgo como uno de los principales obstáculos para la utilización de estas tecnologías, debido a que las complicaciones sobre la protección y confidencialidad de los datos preocupa al mercado (Joint, Baker & Eccles, 2009; Niazmand, 2015; López, 2014).

Algunos de estos riesgos son inherentes a la naturaleza de la computación en nube, en especial los riesgos sobre cuestiones jurídicas y contractuales, la protección de datos, la interoperabilidad y las normas. Otras cuestiones importantes no son nuevas, pero se han intensificado aún más, debido a la naturaleza de la computación en nube. Entre estas, destacan la privacidad de la información y la protección de datos ().

Estado actual y proyecciones de la digitalización de la banca en Europa**.** Para tener una mayor claridad sobre la problemática actual y la manera como la están afrontando los grandes bancos, es necesario tomar como referencia las siguientes entidades. En estas se podrá ver el estado actual de la digitalización de la banca y las proyecciones que tienen estas entidades (Pacheco Jiménez, 2016; Galdo, 2015).

CaixaBank. El 55 % de sus operaciones se realizan por la red o el móvil; el 28 %, en cajeros, y solo el 8 %, en oficinas. Por consiguiente, entre el 2011 y el 2014, este banco destinó 666 millones a los desarrollos digitales. Esta entidad apuesta principalmente por el desarrollo interno de productos y servicios, utilizando las nuevas tecnologías y apoyándose menos en alianzas externas. Cuenta con varias sociedades dedicadas a la innovación tecnológica: e-aCaixa, que se ocupa del desarrollo de la multicanalidad para el grupo; MoneytoPay, para los productos de prepago, y CaixaCard, para desarrollar tecnológicamente el negocio de tarjetas del grupo. Además, CaixaBank es copropietaria del 49 %, de Comercial Global Payments, firma especializada en servicios de pago electrónicos para comercios. Muchos expertos consideran a esta entidad como de las más avanzadas tecnológicamente en la banca española.

BBVA. En palabras de la propia entidad, “el 15 % no va nunca, o casi nunca, a la oficina; apostamos por la convivencia entre lo digital y las oficinas para rentabilizar ambas inversiones”. Al cierre del 2015, el 19,2 % de los préstamos al consumo en España se concedieron a través de canales digitales; en el mismo lapso, las transacciones en oficinas cayeron hasta los 40 millones en operaciones, frente a los 67 millones de 2009. En vista de ello, desde 2008, este banco ha invertido unos 6.500 millones en tecnología; así, se convirtió en la entidad que más apuesta por la revolución digital.

Santander. Según sus datos de 2014, en España tiene más de 6 millones de clientes activos; entre ellos, aproximadamente el 27 % son digitales. El objetivo de este banco es tener 25 millones de clientes digitales en 2017. En 2014 lanzó su propio fondo de *venture capital*, con el que se plantea invertir unos 100 millones de dólares en dos o tres años. Entre sus principales inversiones se encuentran iZettle, especializada en pagos vía móvil y *tablet*; MiCheck, para pagos en hostelería; Cyanogen, el sistema operativo de código abierto para móviles; Ripple,

dedicado a la tecnología *blockchain*, y Kabbage, especializada en el crédito directo a empresas. Asimismo, tiene su propia factoría tecnológica para desarrollo de *software* bancario: Isban. Esta última les da servicio a todos los bancos del grupo. No obstante, la propia entidad considera que "la oficina sigue siendo el punto principal de gestión con los clientes".

Bankia. En 2014, el 30 % de sus clientes eran multicanal; este porcentaje se estaba incrementando paulatinamente.

Banco Popular. Sus datos de 2014 ponen de manifiesto que "los clientes activos de banca multicanal son 830.888", el 15 % del total; los de Banca móvil, 142.517, con un crecimiento de 44 % al año; las transacciones mensuales por Internet y móvil suman 62 millones; la penetración de Internet en empresas es del 70 %".

Banco Sabadell. Sus datos de 2014 señalan que "más del 35 % de los clientes utilizan de forma recurrente web y móvil para acceder a la entidad; y más del 50 % de la operativa ya se realiza a través de Internet/móvil sobre el total de procesos, sin tener en cuenta las consultas".

Eurostat público en el 2015 un informe sobre el uso individual en España de la banca *online* por personas de entre 16 y 74 años. Según este documento, el 39 % emplea esta vía (Cuesta et al., 2015). Respecto a los 28 países de la UE, la media en 2015 sería del 46 %. Sin embargo, España tendría un porcentaje más bien bajo, situándose por detrás de Noruega (con un 90 %), Finlandia (con un 86 %), Dinamarca (con un 85 %), Estonia (con un 81 %), Suecia (con un 80 %), Luxemburgo (con un 65 %), Bélgica (con un 62 %), Francia y Reino Unido (con un 58 %), Alemania e Irlanda (con un 51 %).

A partir de los datos expuestos, resulta más que evidente que los grandes bancos no están haciendo todo lo posible para enfrentar el fomento de las nuevas tecnologías. Lo peor de todo es que, según expertos en la materia, aquellos que no se transformen digitalmente pueden estar en peligro. La previsión actual es que la banca tradicional desaparezca en unos 4 o 5 años, pasando a tener naturaleza digital. Esta transformación le facilitará al cliente muchas operaciones. Aún más, se estima que en el 2020 alrededor del 70 % de los servicios financieros serán digitales. Hay que añadir que el nuevo panorama tecnológico ha propiciado la aparición de nuevos competidores como Google, Apple y Amazon, los cuales llegan con servicios financieros alternativos (Pacheco Jiménez, 2016).

Estado actual y proyecciones de la digitalización de la banca en Latinoamérica**.** Como se puede deducir del punto anterior, en Europa las entidades bancarias ya están haciendo esfuerzos para incorporar la transformación digital dentro de sus *road map* estratégicos. No obstante, esto podría no ser suficiente y pondría en peligro a los bancos tradicionales (Pacheco Jiménez, 2016).

Si se traslada esto al contexto de Latinoamérica, la situación es mucho más preocupante. No es posible encontrar información sobre las entidades bancarias colombianas y de la región que reflejen esfuerzos similares por incursionar en el mundo de la banca digital. Solo hay algunos intentos de billeteras virtuales, a los que todavía les falta mucho por madurar; además, estos son solo un componente de la banca digital.

Pasos hacia la transformación**.** Tomando un ejemplo concreto de una entidad inmersa en la denominada revolución digital, se analizará el BBVA, el segundo mayor banco español. Se seguirá el balance de su transformación, desde una perspectiva tanto nacional como internacional.

Ya desde el 2007, BBVA comenzó a construir una nueva plataforma tecnológica, con la intención de anticiparse al impacto venidero para la banca. Concluida esta primera etapa, en el 2014 creó la División de Banca Digital, con la doble misión de acelerar la transformación del grupo e impulsar el desarrollo de nuevos negocios digitales. Para lograr esos objetivos, era preciso desarrollar una cultura dirigida a la ejecución y gestión por proyectos, a través de pequeños equipos con autonomía plena, incorporando talento interno y externo. Y, en la búsqueda de este talento, la entidad ha adquirido varios negocios: Simple y Madiva Soluciones en 2014; Spring Studio y Atom en 2015; Cisco y Holvi en 2016. Además, Simple Finance Technology Corp, empresa estadounidense propietaria de la plataforma de Banca online del mismo nombre, fue adquirida por 117 millones de dólares. La unión de BBVA y Simple supone ventajas para ambas: a Simple le proporciona recursos y presencia internacional, expandiéndose más allá de EE. UU. y entrando en nuevos mercados; a BBVA, un valioso apoyo tecnológico que le permitirá reinventar los servicios financieros.

Madiva Soluciones —fundada en diciembre del 2008 y con sede en Madrid, especializada en servicios de procesamiento masivo de datos (*big data*) y computación en la nube (*cloud computing*)— seguirá operando como una compañía independiente, atendiendo a BBVA y a otros clientes.

Spring Studio —compañía californiana especializada en diseño digital para procesos online o móviles— fue adquirida por BBVA, con la finalidad de potenciar el diseño como una de sus diferencias competitivas en el mercado (Pacheco Jiménez, 2016; Gibson, 2015).

Por último —pero no menos importante—, aunque en los puntos mencionados anteriormente se hable de seguridad en la nube y de su importancia para las entidades

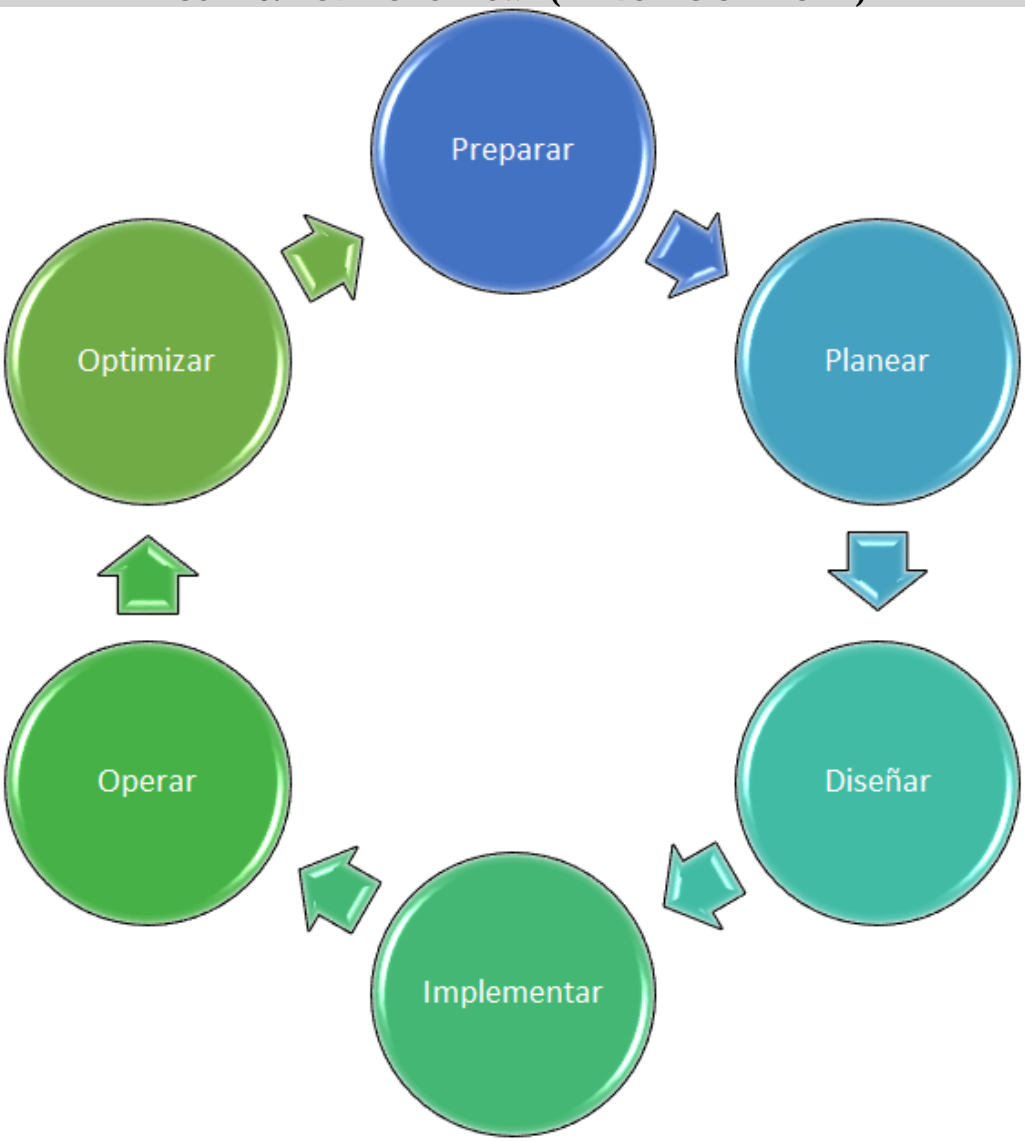
financieras, es complejo encontrar información detallada que revele los modelos de seguridad recomendados. Esto se explica porque esta información puede exponer la seguridad de la organización; también es muy difícil encontrar información sobre los problemas de seguridad sufridos por las entidades financieras o por las fintech, debido a que esto podría causar una perdida reputacional en las organizaciones, motivo por el que no dan a conocer esa información de manera detallada.

Metodología

El marco metodológico para la realización de este proyecto se fundamenta en la metodología *Top Down*. El esquema de diseño *Top Down* consiste en fijar los criterios y especificaciones iniciales del proyecto en un nivel jerárquico superior. Estas especificaciones de nivel superior se transfieren sucesivamente, de un modo hereditario, a todas las partes del proyecto de los niveles inferiores. Esta transferencia se realiza a través del llamado esqueleto del producto, que se construye en la fase preliminar del proyecto.

A continuación, la **FIGURA 6** muestra la secuencia del modelo *Top Down* (“Metodología Top Down”, s.f).

FIGURA 6: MODELO TOP DOWN **(ELABORACIÓN PROPIA)**



A continuación, se ofrecerá una breve explicación sobre cómo se abordará cada uno de los objetivos incluidos en las fases de la **METODOLOGÍA**.

Preparar y planear

En esta fase se abordará el primer y segundo objetivos: elaborar el plan de requisitos de la arquitectura bajo lineamientos fintech e identificar el modelo de nube que más se ajuste a las necesidades del sector bancario.

Diseñar

En esta fase se abordará el tercer objetivo: se realizará el modelo de arquitectura que cumpla con los lineamientos de seguridad y las necesidades bancarias bajo lineamientos fintech.

Implementar y operar

Aquí se tomará el cuarto objetivo: realizar una prueba de concepto en la nube, implementando un par de servicios existentes y valorando su operatividad.

Optimizar

Esta es la última fase; en ella se va a revisar el objetivo cinco, que consiste en analizar los resultados de la prueba y terminar de documentar el todo el proyecto.

Presentación y análisis de resultados

Diseñar la Arquitectura de Seguridad para la Gestión del Riesgo en esquemas de Banca Digital que operan bajo un modelo fintech, en el contexto de la banca en Colombia.

Este proyecto se enfoca en diseñar una arquitectura que cumpla con los lineamientos de seguridad para la gestión del riesgo en esquemas de Banca digital que operen bajo un modelo fintech, en el contexto de la Banca en Colombia. Por consiguiente, durante el desarrollo del mismo, se hará un análisis y evolución del mundo de la industria financiera, la computación en la nube y la evolución de los bancos hacia esta tecnología. Finalmente, se verán los retos y consideraciones de seguridad que deben tenerse en cuenta cuando una entidad financiera decide dar el paso a la nube.

Como podrá comprobarse a continuación, el siguiente análisis se enfoca en el desarrollo de los objetivos que se plantearon durante la primera parte de este documento. Cada objetivo propone una alternativa a los problemas mencionados anteriormente.

Primer objetivo: plantear el desarrollo de una estrategia de banca fintech

Este objetivo consiste en plantear el desarrollo de una estrategia de Banca digital que opere bajo un enfoque fintech, cuya arquitectura cumpla con los estándares de seguridad de confidencialidad, integridad y no repudio.

Para lograrlo, fue necesario realizar las actividades que involucraran a expertos del sector financiero y de industrias tecnológicas. De esta manera, se podía obtener una percepción cuantitativa de la seguridad en la nube para las entidades financieras. A continuación, se presentan las preguntas realizadas y los resultados obtenidos. Hay que agregar que, debido a la

confidencialidad de la información, no es posible revelar los datos personas de las personas que contestaron esta encuesta, publicada en www.portalencuestas.com

La encuesto se envió a 50 personas expertas en seguridad y en el sector financiero, también se incluyó a proveedores tecnológicos enfocados en atender al sector financiero. 20 personas contestaron la encuesta. Estos fueron los resultados.

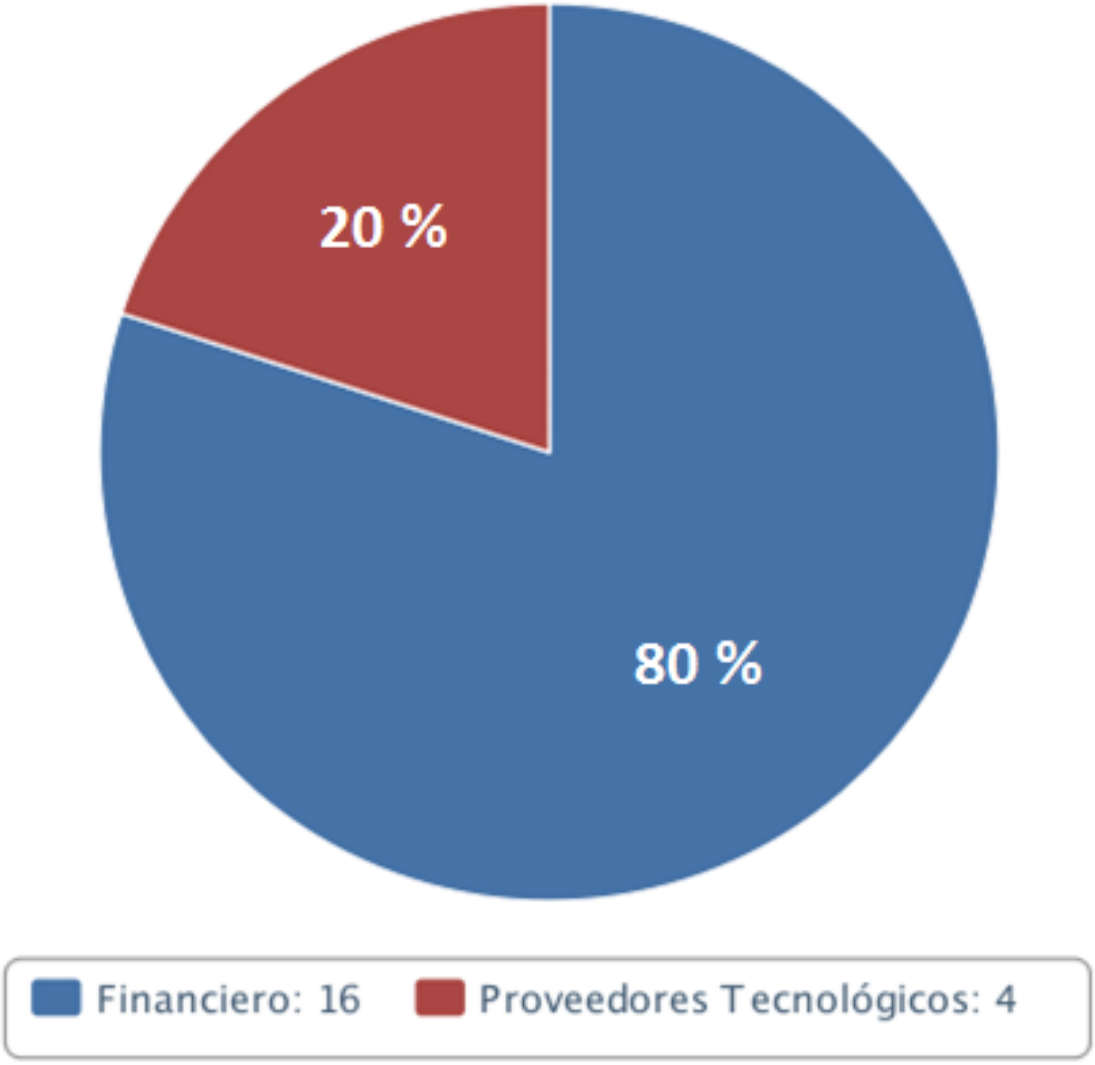
Encuesta de percepción de seguridad en la nube en las entidades financieras**.** A continuación, se revisará el resultado de cada una de las preguntas realizadas a todos los encuestados. Cada una se hizo teniendo en cuenta los principales factores necesarios para el desarrollo de este proyecto; en su gran mayoría, se recurrió a preguntas relacionadas con la computación en la nube y sus factores críticos de seguridad.

Cuando se plantean este tipo de preguntas, deben considerarse varios factores críticos. El primero es conocer el entorno en que hará la encuesta; en este caso, se trata del entorno financiero. En segundo lugar, hay que identificar las preguntas más valiosas para la encuesta: no pueden ser demasiado técnicas o dificultar la respuesta de los encuestados. Por último, es necesario moderar la cantidad de preguntas realizadas, para que la encuesta no se vuelva tediosa; por lo general, una encuesta no debe sobrepasar las 10 preguntas. Sin embargo, en este caso, se usaron 14; se tuvo en cuenta que la mayoría eran de opción múltiple o de seleccionar la respuesta, motivo por el que eran más fáciles de contestar. Solo hubo dos preguntas abiertas, para que la encuesta no fuera demasiado extensa o compleja para el público seleccionado.

*Pregunta **número** 1: ¿**a qué** sector pertenece la empresa en **donde** trabaja?* Como se puede ver en la **FIGURA 7**, la gran mayoría de las personas que contestaron la encuesta

pertenecen al sector financiero. Para los propósitos de este análisis, esto convierte a los encuestados en un grupo más representativo respecto al problema estudiado.

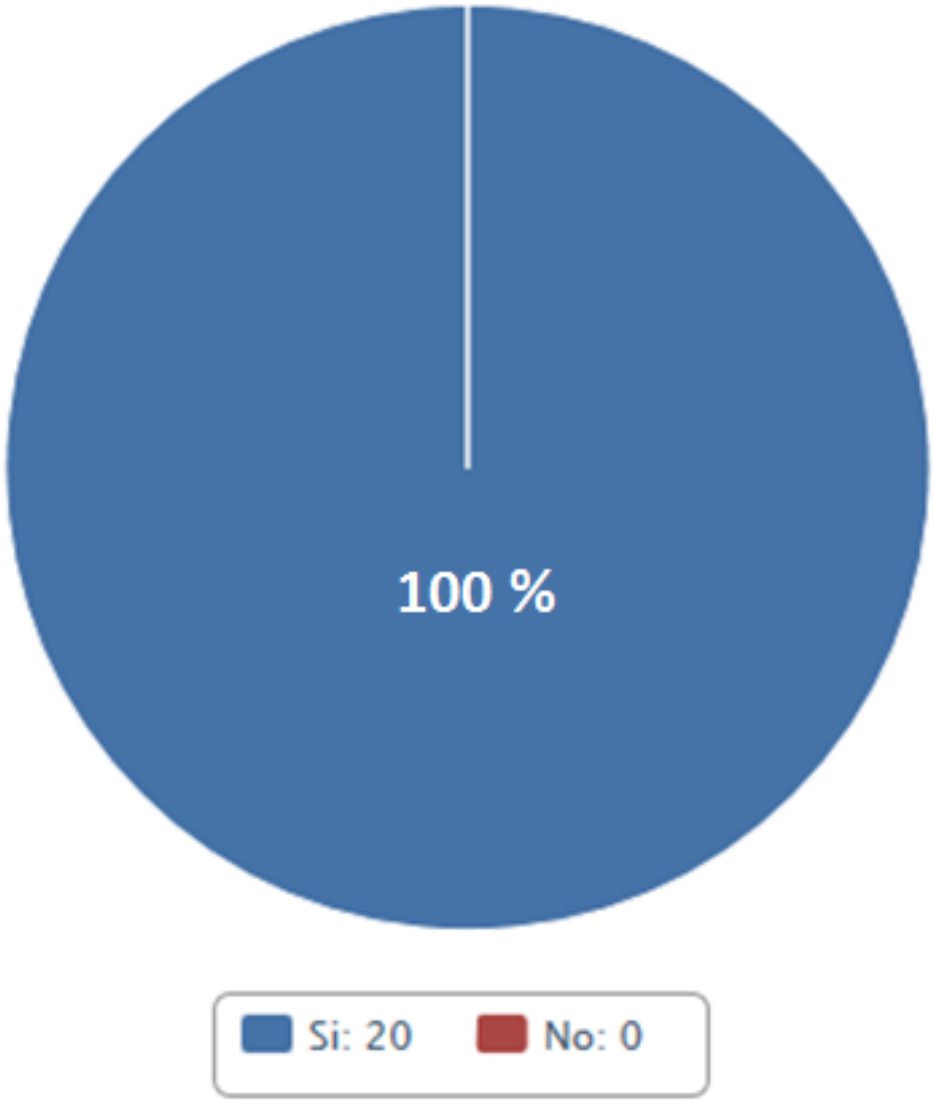
FIGURA 7: RESULTADO DE LA PRIMERA PREGUNTA (ELABORACIÓN PROPIA, BASADA EN LA INFORMACIÓN DE PORTALDEENCUESTAS.COM)



Pregunta numero 2: ¿En tu organización se contempla la nube como parte de la visión estratégica de la compañía? Como podrá comprobarse, esta pregunta es de gran importancia, aunque parezca simple: muestra cómo las entidades financieras y empresas tecnológicas perciben la importancia de la adopción de los modelos en la nube en la estrategia de su organización.

La **FIGURA 8** muestra que todos los encuestados tienen claro que la nube hace parte de la visión estratégica de sus organizaciones y que se están moviendo o se deben mover hacia ese camino.

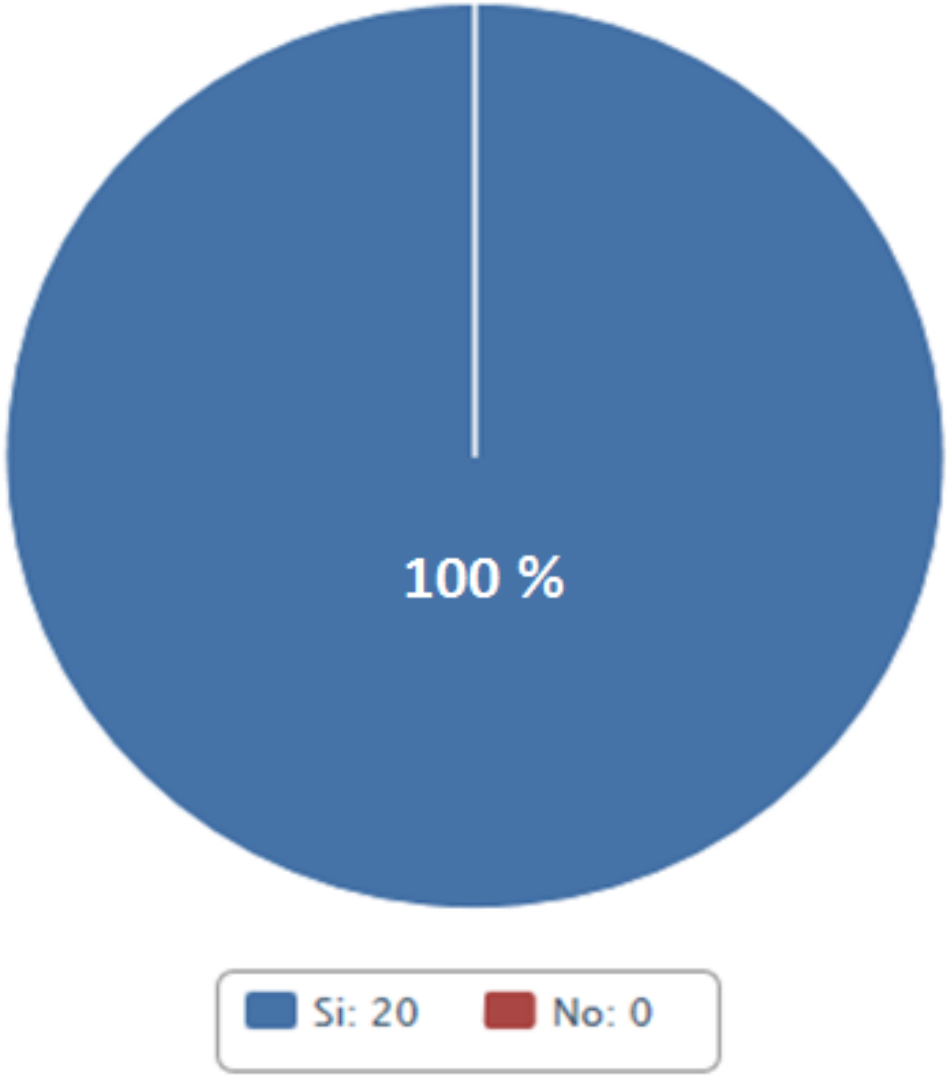
FIGURA 8: RESULTADO DE LA SEGUNDA PREGUNTA (ELABORACIÓN PROPIA, BASADA EN LA INFORMACIÓN DE PORTALDEENCUESTAS.COM)



Pregunta número 3: ¿Considera usted que las tecnologías de la nube son necesarias y que serán cada vez más importantes en todos los sectores de la industria, incluyendo la banca?

Esta pregunta es un complemento a la pregunta anterior. Además de reconocer la importancia que tiene la nube en su estrategia, las compañías toman en cuenta que cada vez estas tecnologías son más necesarias y que cobran más fuerza este tipo de soluciones. Lo anterior no solo aplica para la industria financiera: los modelos de nube llegaron para quedarse y son cada vez más importantes en todas las industrias de la economía. Así lo expresan los encuestados en la tercera pregunta, como puede verse en la **FIGURA 9**.

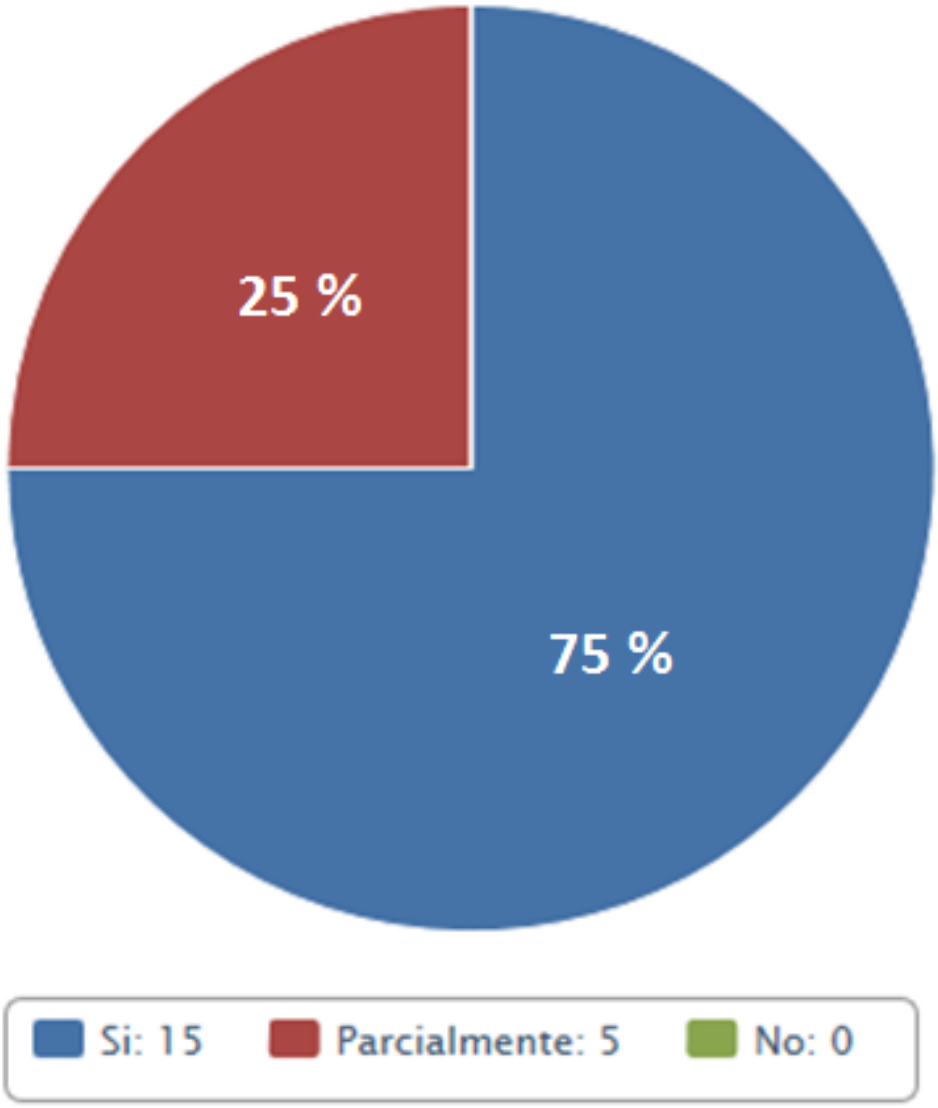
FIGURA 9: RESULTADO DE LA TERCERA PREGUNTA (ELABORACIÓN PROPIA, BASADA EN LA INFORMACIÓN PORTALDEENCUESTAS.COM)



*Pregunta numero 4: ¿**considera** usted que una planeación estratégica exitosa debe contemplar la computación en la nube como un modelo de evolución del sector financiero?* Esta pregunta es la última de una serie de tres, incluidas las dos anteriores; esta serie de preguntas buscaba dejar en evidencia la importancia de la nube en el sector financiero y en su planeación estratégica. La nube no es un componente más de la arquitectura; es una base fundamental para las nuevas arquitecturas de las entidades financieras. Es por eso por lo que los bancos tradicionales deben mutar a arquitecturas más flexibles, que les permitan ser más competitivos y

agiles, para concentrar sus esfuerzos en lo que realmente les genera valor. Esto puede apreciarse a continuación, en la **FIGURA 10**.

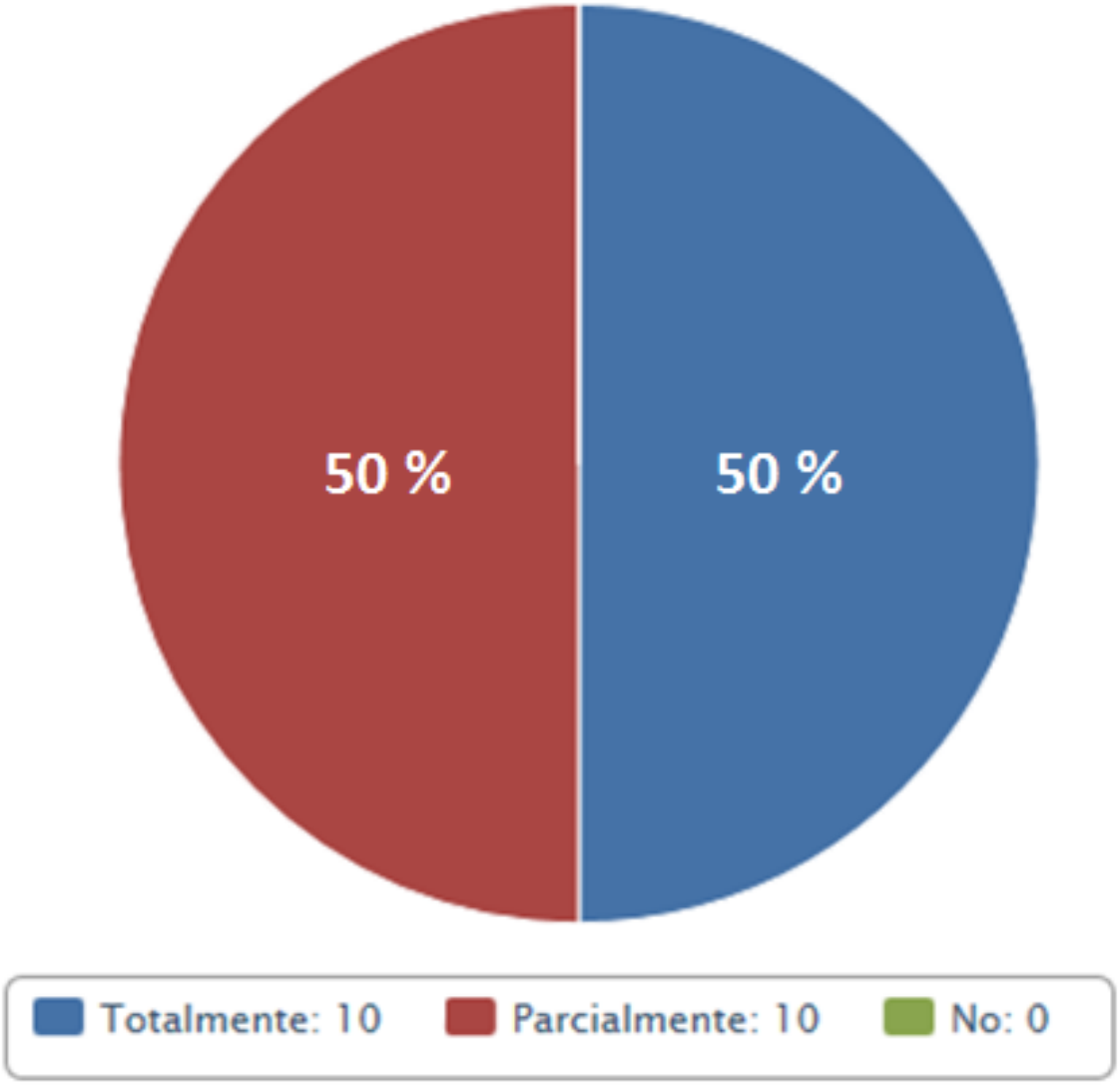
FIGURA 10: RESULTADO DE LA CUARTA PREGUNTA (ELABORACIÓN PROPIA, BASADA EN LA INFORMACIÓN DE PORTALDEENCUESTAS.COM)



*Pregunta numero 5: ¿**cree** usted que los servicios de la nube les permiten a las entidades financieras concentrar sus esfuerzos en oportunidades **de** negocio y, al mismo tiempo, seguir cumpliendo con el manejo de riesgos bajo la regulación colombiana?* Como se pudo entrever en el punto anterior, esta pregunta permite evidenciar que, si las entidades financieras se apoyan en

tecnologías en la nube, podrán enfocar sus esfuerzos y recursos en el *core* de su negocio. Aunque las respuestas están divididas, lo que sí queda claro es que se prevén beneficios con el uso de la nube, ya sea total o parcialmente. Esta tecnología le ayudaría a las organizaciones a enfocar esfuerzos en su *core* de negocio, como puede verse en la **FIGURA 11**.

FIGURA 11: RESULTADO DE LA QUINTA PREGUNTA (ELABORACIÓN PROPIA, BASADA EN LA INFORMACIÓN DE PORTALDEENCUESTAS.COM)



Pregunta numero 6: ¿Cree usted que la nube es viable para los bancos en Colombia? A diferencia de las anteriores, esta es una pregunta abierta. Por esto, se incluirá un resumen de las

respuestas dadas por los encuestados, en donde destaca la gran diversidad de respuestas, pero con una tendencia: se reconoce la viabilidad de la nube en el sector financiero colombiano.

- De los 20 usuarios, 6 contestaron que les parece totalmente viable.

- Uno expresó que es viable en una nube privada.

- Si es viable. De acuerdo con el tipo de clasificación de los datos, se podría analizar e implementar este esquema bajo el modelo de riesgos definido.

- Es viable para soluciones críticas en el mediano plazo.

- Es parcialmente viable, debido a la falta de conocimiento de los entes regulatorios; la falta de actualización de las normas que rigen estas entidades, según la realidad tecnológica del mundo, y el temor de adoptar nuevas tecnologías que aún se vive aún dentro de las entidades bancarias **colombianas**.

- Si, ante la creciente necesidad de optimizar el uso de la infraestructura requerida en la gestión bancaria, lo que podría llevar a ser más eficientes en costos. Las soluciones en la nube se presentan como una alternativa ideal para lograrlo, focalizando más la atención en el negocio.

- Si es viable, y el regulador debe adaptar las normas para garantizar dicha viabilidad, al mismo tiempo que continuamos protegiendo la confidencialidad de la información y operaciones de los clientes y usuarios.

- Es totalmente viable; se deben revisar las capacidades que se quieren tener en la nube, dado que es posible que algunas de ellas sigan siendo más generadoras de valor en modelos *OnPremise*.

- Si, aunque se debe reforzar el tema regulatorio, tanto de los reguladores locales como de los internacionales, como la Bolsa de NY, ya que a veces estos pueden generar contradicciones.

- Es viable utilizarla en diferentes procesos, siempre y cuando se garantice la seguridad e integridad de la información; ya hoy se hace en algunos casos.

- Sí, es viable. Debemos aprender más del tema, para saber cómo enfrentar los obstáculos en su implementación.

- Es viable para algunos servicios, especialmente para la colocación de productos financieros. Sin embargo, existen *issues* regulatorios que no permiten que la banca evolucione.

- Si, es completamente viable, por la oportunidad de entrar en los mercados de una manera temprana y poderse enfocar realmente en los procesos que generan valor.

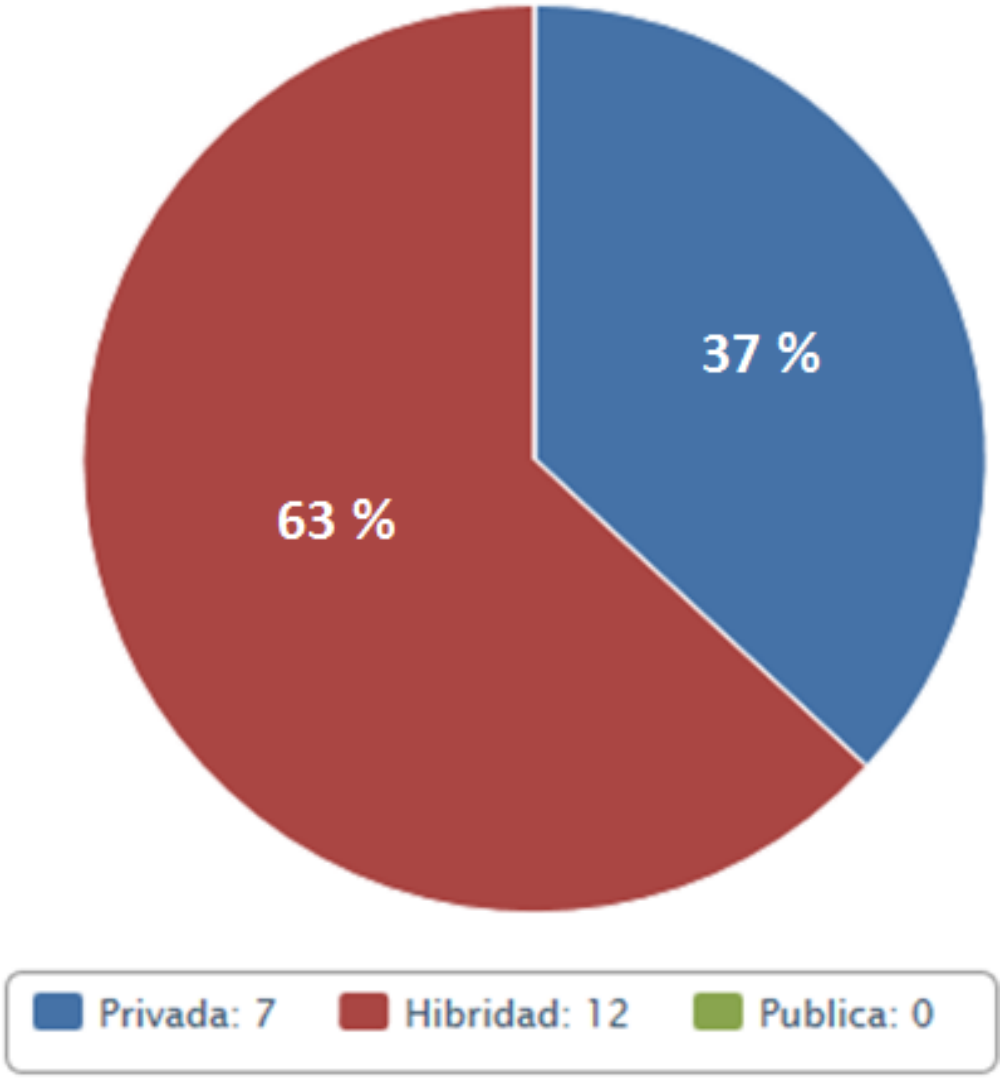
- Si me parece viable, sin conocer en detalle la legislación; pero lo que, en mi opinión, hay que considerar es el modo de implementación más que el implementarla o no.

- Si, teniendo en cuenta que servicios se desean llevar a la nube.

Pregunta numero 7: ¿cuál de los siguientes modelos de nube considera usted que más se adapta a las necesidades de una entidad financiera en Colombia? Con esta pregunta, ya se empieza a profundizar en los modelos de nube, dentro de que se evaluaron los modelos de nube pública, privada e híbrida. La primera gran conclusión es que las nubes públicas no les parecen viables a las entidades financieras; además se nota una gran aceptación de los modelos de nube híbrida incluso por encima de la nube privada, como puede verse a continuación en la **FIGURA**

12. Esta información podrá contrastarse más adelante, cuando se realice la evaluación detallada de los modelos de nube.

FIGURA 12: RESULTADO DE LA SÉPTIMA PREGUNTA (ELABORACIÓN PROPIA, BASADA EN LA INFORMACIÓN DE PORTALDEENCUESTAS.COM)



Pregunta numero 8: ¿cuáles considera usted que deben ser los factores críticos al momento de evaluar si se debe llevar una aplicación financiera a la nube? Esta pregunta es un poco más compleja que las anteriores, porque busca entender los factores críticos de los modelos en la nube y su relevancia. En la siguiente tabla se encuentra los factores seleccionados y la manera cómo fueron calificados; sin embargo, es necesario tener más detalles sobre los

principales factores. Por esa razón, se incluyen 5 graficas más, especificando los factores más relevantes.

TABLA 3: RESULTADO DE LA OCTAVA PREGUNTA (ELABORACIÓN PROPIA, BASADA EN LA INFORMACIÓN DE PORTALDEENCUESTAS.COM)

	Muy importante	Importante	Poco importante	Nada importante	No se requiere
Disponibilidad	18 (95%)	1 (5%)	0 (0%)	0 (0%)	0 (0%)
Confidencialidad	19 (100%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
Escalabilidad	16 (84%)	3 (16%)	0 (0%)	0 (0%)	0 (0%)
Fiabilidad	14 (74%)	5 (26%)	0 (0%)	0 (0%)	0 (0%)
Seguridad	18 (95%)	1 (5%)	0 (0%)	0 (0%)	0 (0%)
Integración	11 (58%)	7 (37%)	1 (5%)	0 (0%)	0 (0%)
Flexibilidad	11 (58%)	7 (37%)	1 (5%)	0 (0%)	0 (0%)
Beneficio Economico	7 (37%)	9 (47%)	3 (16%)	0 (0%)	0 (0%)
Accesibilidad	10 (53%)	8 (42%)	1 (5%)	0 (0%)	0 (0%)

De la tabla anterior es muy importante resaltar los resultados de los primeros 5 factores: están altamente correlacionados y son calificados como muy importantes. Estos datos indican que la seguridad de los modelos en la nube para las entidades financieras es un factor muy relevante. Por eso, a continuación, se verán con más detalle los resultados de **disponibilidad, confiabilidad, escalabilidad, fiabilidad y seguridad** en las gráficas dadas en las **FIGURAS 13**, **14**, **15**, **16** y **17**, respectivamente.

FIGURA 13: FACTOR DE DISPONIBILIDAD **- COMPLEMENTO DE LA FIGURA 8 (ELABORACIÓN PROPIA, BASADA EN LA INFORMACIÓN DE PORTALDEENCUESTAS.COM)**

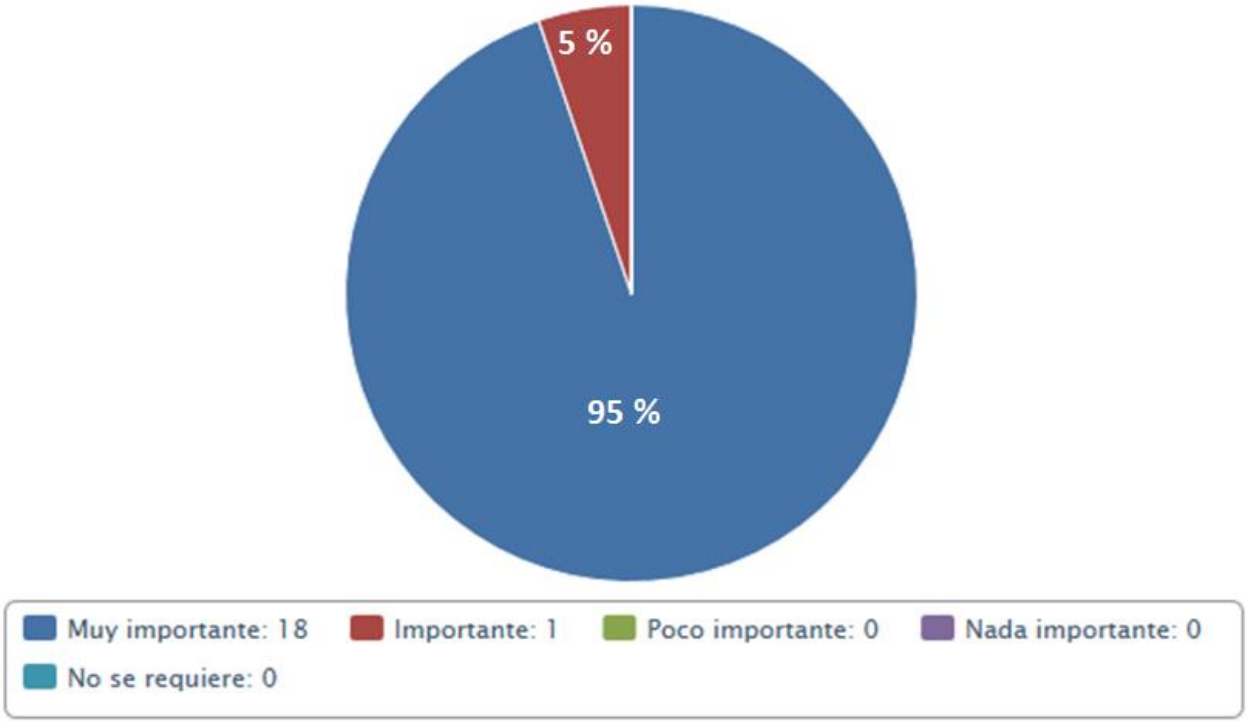


FIGURA 14: FACTOR DE CONFIDENCIALIDAD **– COMPLEMENTO DE LA FIGURA 8 (ELABORACIÓN PROPIA, BASADA EN LA INFORMACIÓN DE PORTALDEENCUESTAS.COM)**

FIGURA 15: FACTOR DE ESCALABILIDAD **– COMPLEMENTO DE LA FIGURA 8 (ELABORACIÓN PROPIA, BASADA EN LA INFORMACIÓN DE PORTALDEENCUESTAS.COM)**

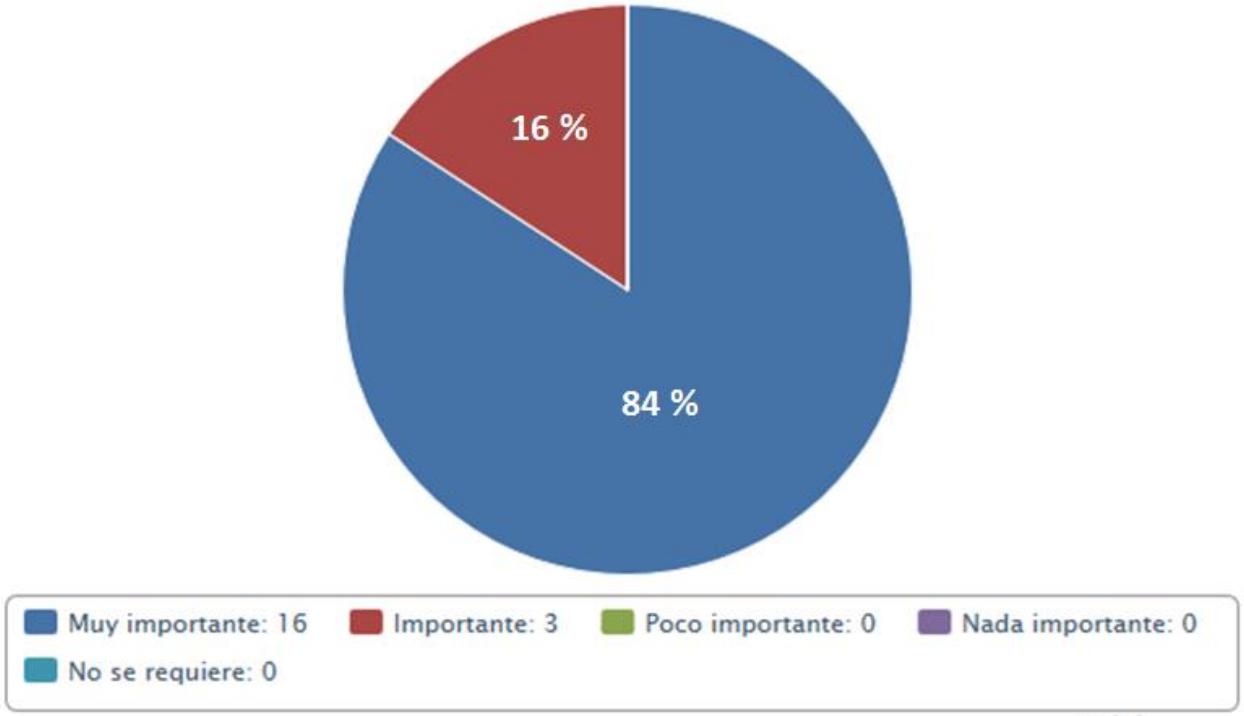


FIGURA 15: FACTOR DE FLEXIBILIDAD **– COMPLEMENTO DE LA FIGURA 8 (ELABORACIÓN PROPIA, BASADA EN LA INFORMACIÓN DE PORTALDEENCUESTAS.COM)**

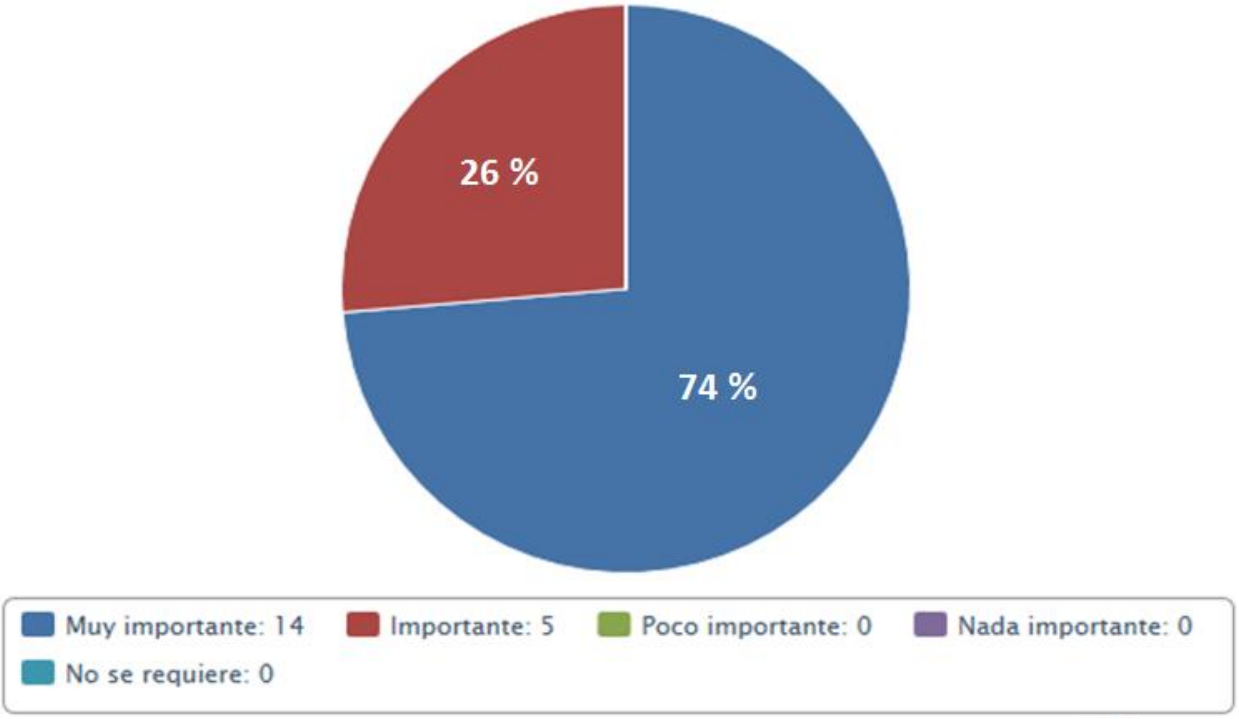
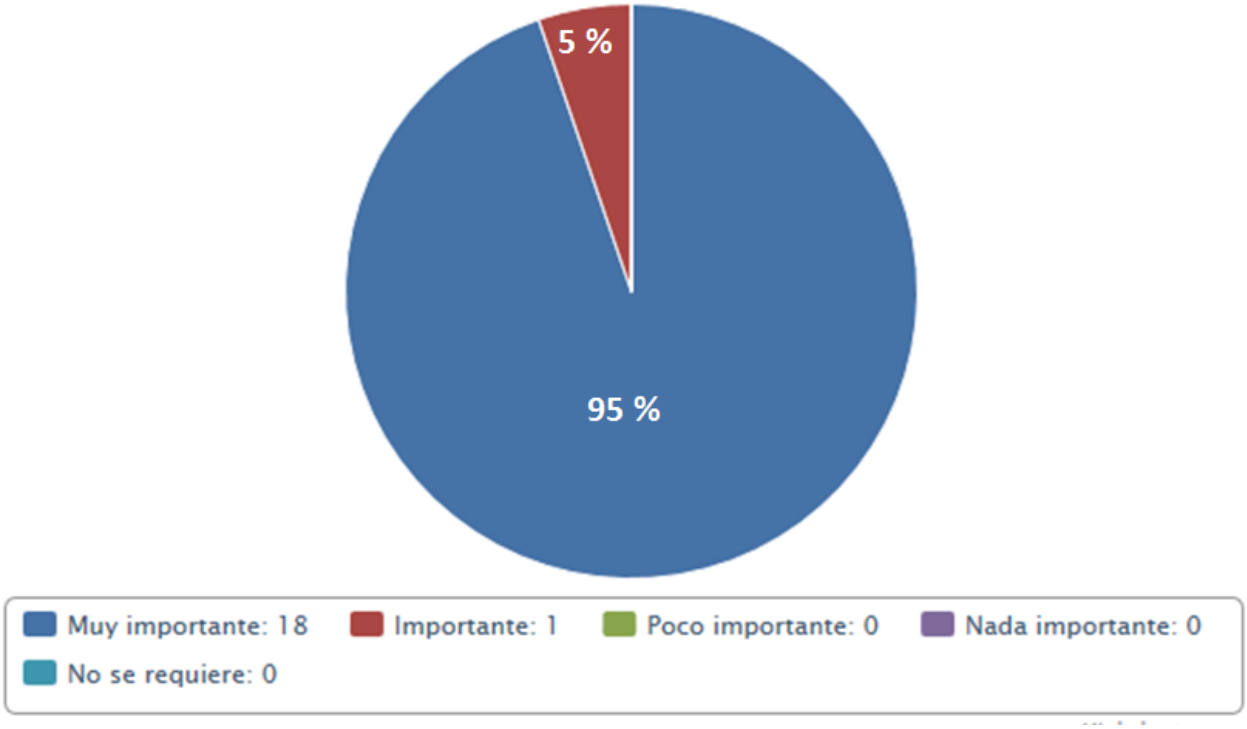


FIGURA 16: FACTOR DE SEGURIDAD – COMPLEMENTO DE LA FIGURA 8 (ELABORACIÓN PROPIA, BASADA EN LA INFORMACIÓN DE PORTALDEENCUESTAS.COM)



Pregunta numero 9: ¿según las características esenciales de la nube (esta les provee a los clientes autoservicio a demanda, acceso amplio a la red, agrupación de recursos, elasticidad rápida y servicio medido), está de usted de acuerdo en que estas capacidades son importantes en el negocio financiero para hacer frente a la evolución de las fintech? Esta pregunta, a diferencia de las anteriores, es una pregunta abierta. A continuación, se incluye un resumen de las respuestas dadas por los encuestados. Destaca la gran diversidad de respuestas, pero con una tendencia marcada a la importancia de la nube para el sector financiero colombiano.

- De los 20 usuarios, 4 contestaron solamente que sí.

- De los 20 usuarios, 4 contestaron estar de acuerdo.

- Si, apoya las necesidades tecnológicas orientadas a TI, según el ritmo que requiere un sector cambiante como el financiero.

- Completamente de acuerdo, porque las tecnologías tradicionales no ofrecen el *time to market* que se requiere para mantenerse vigentes.

- Todas estas características, y muchas más que ofrecen las soluciones en nube, son esenciales para que cualquier empresa pueda responder a la velocidad y oportunidad que exige el mercado, y más a un mercado tan sensible como el financiero.

- Frente a las fintech, la opción de la nube es un factor entre muchos. Frente a las *bigtech*, la nube es imprescindible.

- Completamente, la estrategia centrada en la nube les permite a las organizaciones poder "andar" a un ritmo diferencial al que normalmente están acostumbradas a hacerlo. Las plataformas de nube le apuntan a la bimodalidad, a tener un ritmo más ágil y dinámico, que les permitiría poder crear plataformas y soluciones de cara a las nuevas necesidades de nuestros clientes, aliados estratégicos y —¿por qué no?— de las fintech, para convertirnos en su aliado de servicios financieros.

- Si, aportaría al tema de seguridad y confidencialidad.

- Faltaría la seguridad.

- Totalmente, todas estas capacidades apalancan una mayor flexibilidad, para evolucionar tecnológicamente y desde el punto de vista de negocio.

- El paradigma, y más en el sector financiero, es la facilidad de adquirir productos y servicios financieros, de la forma más cercana al cliente, mejorando la experiencia y acompañamiento en todos lados: *customers first*[1].

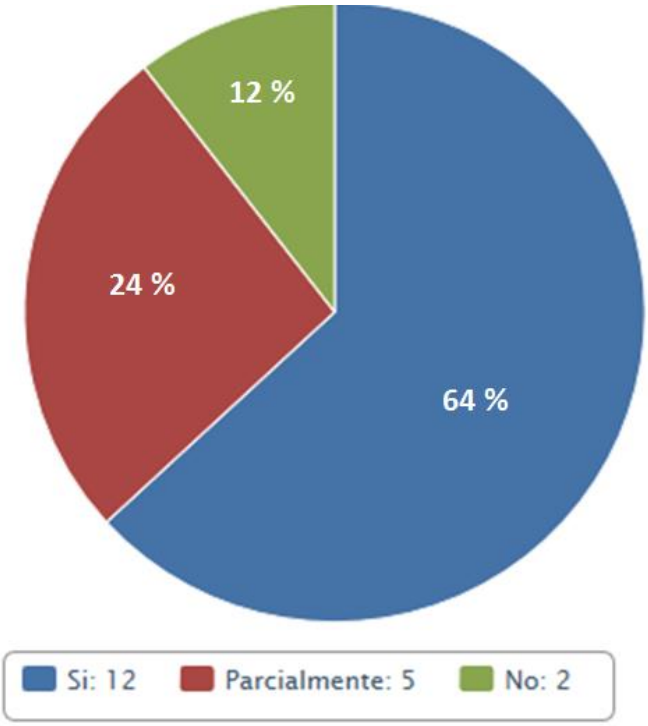
- Si, para agilizar implementaciones, incrementar la flexibilidad y proveer ambientes maleables.

- Si, ya que las entidades financieras deben evolucionar mucho más rápido, de forma acorde con la situación actual.

Pregunta numero 10: ¿Cree usted que los niveles de seguridad pueden variar de una industria a otra, respecto a la tecnología utilizada? Como puede notarse a continuación, en la **FIGURA 18**, gran parte de los encuestados considera que la seguridad puede variar de una industria a otra. No obstante, otros creen que no o que la variación puede ser parcial. Esto último se debe en gran medida a que hay temas asociados a la confidencialidad de la información que son estándares entre industrias. Aun así, es importante aclarar que la industria financiera tiene que cumplir con normas muy propias del sector financiero, que no aplican para otros sectores de la industria.

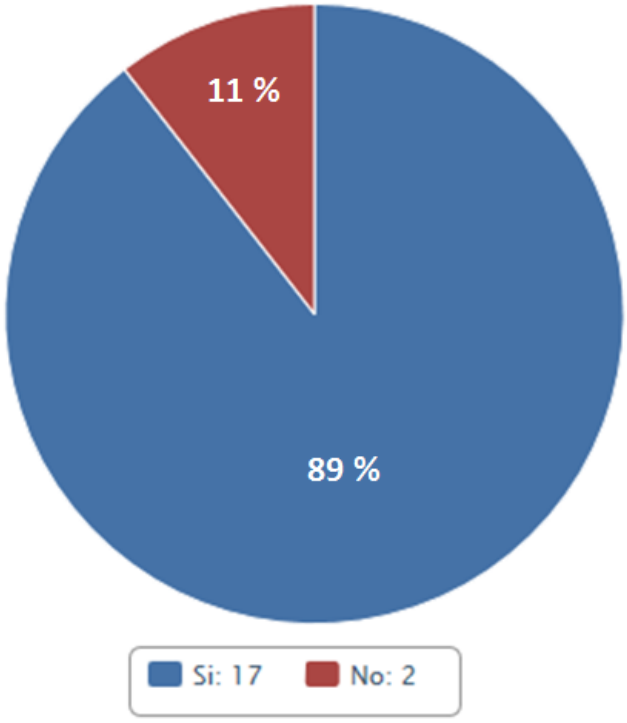
1. En inglés, esto traduce “clientes primero”.

FIGURA 18: RESULTADO DE LA DÉCIMA PREGUNTA (ELABORACIÓN PROPIA, BASADA EN LA INFORMACIÓN DE PORTALDEENCUESTAS.COM)



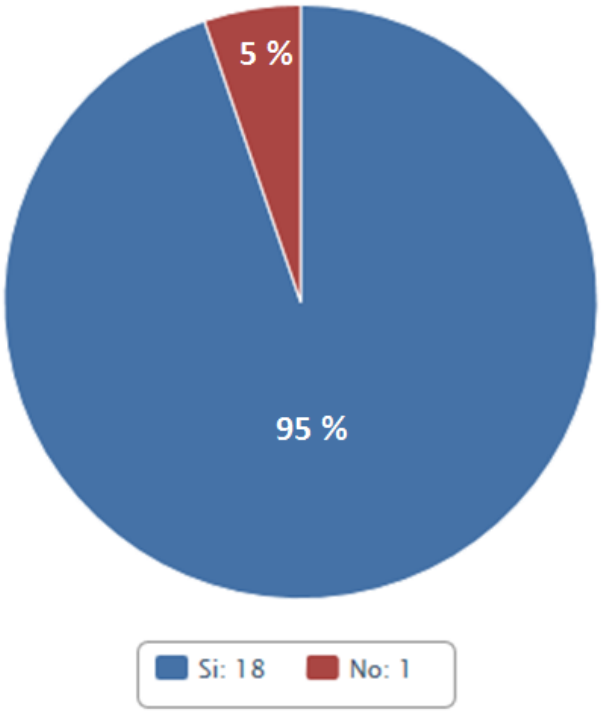
*Pregunta **número** 11: ¿**cree** usted que introducir medidas de seguridad en la red de la nube puede reducir el riesgo de un banco que lleve sus servicios a la nube?* La gran mayoría de los encuestados considera que agregar medidas de seguridad en la red ayuda a disminuir los riesgos; sin embargo, esta es solo una de las muchas variables de seguridad que se deben tener en cuenta al momento de adoptar una estrategia de computación en la nube. A partir de estos datos, se diseñó la **FIGURA 19**.

FIGURA 19: RESULTADO DE LA UNDÉCIMA PREGUNTA (ELABORACIÓN PROPIA, BASADA EN LA INFORMACIÓN DE PORTALDEENCUESTAS.COM)



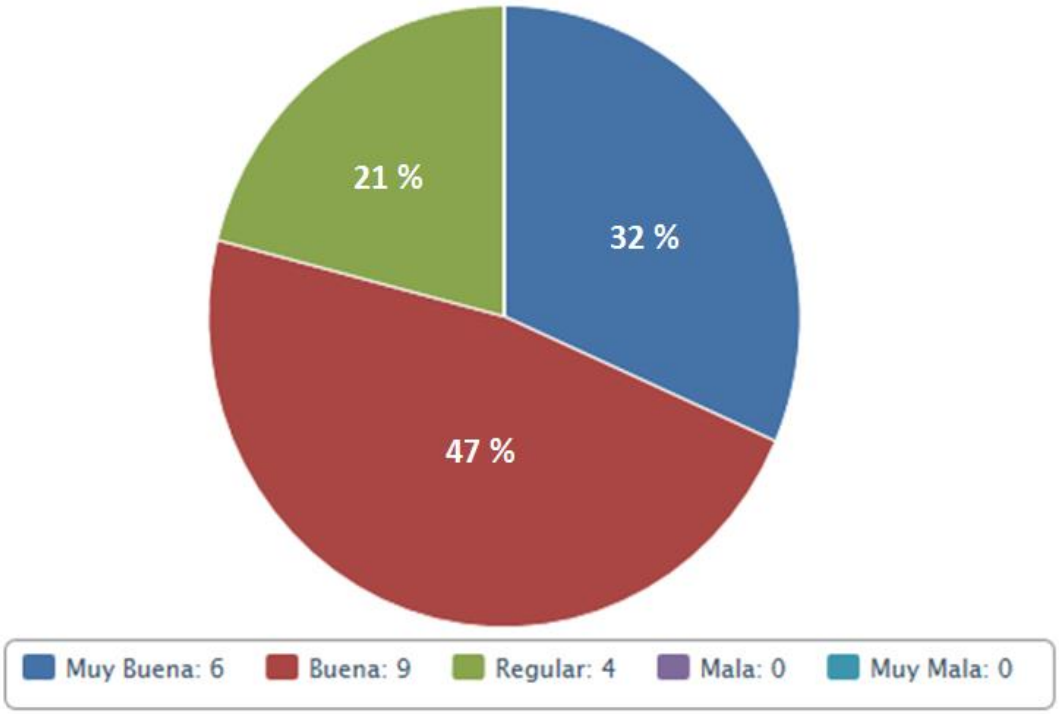
Duodécima pregunta: ¿cree *usted que están usando los proveedores de la nube algunos estándares de seguridad y/o mejores prácticas?* Como puede comprobarse en la **FIGURA 20**, el 95 % de los encuestados considera que los proveedores de la nube usan estándares de seguridad y buenas prácticas. Hay que aclarar que esto siempre debe comprobarse en el momento de contratar un servicio en la nube, el cual debe conformarse a las necesidades del negocio y a los requisitos de seguridad. Además, la nube debe ser acorde al tipo de información que se desee llevar a la nube; esto significa la criticidad de información, la confidencialidad, los temas regulatorios y los acuerdos contractuales adquiridos con los clientes.

FIGURA 20: RESULTADO DE LA DUODÉCIMA PREGUNTA (ELABORACIÓN PROPIA, BASADA EN LA INFORMACIÓN DE PORTALDEENCUESTAS.COM)



*Pregunta numero 13: ¿**cuál** es su percepción de la seguridad en la nube para los negocios financieros en Colombia?* Como se explicita en la **FIGURA 21**, la percepción de seguridad en la nube para los negocios financieros en Colombia es relativamente buena. En la gráfica que sigue, se puede notar que aún quedan aspectos por mejorar; estas mejoras garantizarían que las entidades financieras se migren en un 100 %, con total tranquilidad, a los modelos de nube.

FIGURA 21: RESULTADO DE LA DECIMOTERCERA PREGUNTA (ELABORACIÓN PROPIA, BASADA EN LA INFORMACIÓN DE PORTALDEENCUESTAS.COM)



Pregunta numero 14: De una breve explicación de su respuesta anterior. Esta pregunta es complementaria a la anterior: busca más detalles que permitan entender en que se basa la percepción de la seguridad en la nube para los negocios financieros en Colombia. A continuación, se incluyen las respuestas dadas en la encuesta.

- Aún la legislación no es muy clara.

- Respondí "sí" a la pregunta 13, porque estoy convencido que los CSP son más estrictos en sus estándares de seguridad que lo que pueden serlo las entidades financieras.

- La seguridad es una característica fácilmente verificable en los prestadores de nube.

- Los principales proveedores de nube están certificados en los temas de seguridad requeridos para contener información de los servicios financieros.

- Los proveedores de nube cuentan con todos los controles de seguridad físicos y lógicos necesarios para garantizar la confidencialidad y seguridad de la información que los clientes alojan en su infraestructura. Su negocio se basa en la calidad con que ofrezcan su servicio: es su foco, su producto, se dedican a eso. Por lo tanto, cada día será mucho mejor, a diferencia de una entidad financiera, cuyo foco es el negocio, no la tecnología. De igual forma como los bancos confían en las transportadoras de valores por su experticia, de igual forma ocurre con la información y los proveedores de servicios *cloud*.

- Más que una percepción, diría que es una necesidad. Que el esquema de seguridad sea muy bueno es algo que debe garantizar cualquier proveedor de nube, pues en este aspecto las empresas del sector financiero han sido bastante recelosas.

- Los oferentes actuales de nube han elevado la vara de los estándares de seguridad de forma contundente.

- Grandes compañías a nivel mundial han confiado muchos de sus procesos de negocio y soluciones a plataformas de nube. Progresivamente, las nubes han ido afinando y considerando mejores opciones de seguridad, para proteger la información y las soluciones que se hospedan en ellas. Se deben superar algunas paradojas y creencias de que la nube es más insegura, porque estudios han demostrado que los *datacenters* de grandes competidores —como AWS, Azure, Bluemix, entre otros— tienen instalaciones que cuentan con mejores mecanismos de seguridad que las de los *datacenters* de las organizaciones tradicionales.

- Si aún no se ha masificado en todas las aplicaciones de un negocio financiero (por ejemplo, depósitos, canales, clientes, contabilidad, etc.), es porque aún hay brechas regulatorias o de seguridad.

- Creo que los temas de nube están más enfocados en otras características —como elasticidad, pago por uso, entre otros— que en los mismos temas de seguridad. Al menos eso es lo que he notado. Creo que, en Colombia, por eso mismo la nube no ha incursionado mucho en el tema financiero.

- Pienso que técnicamente los proveedores de nube ofrecen todos los mecanismos de seguridad, y depende más del diseño que realice cada empresa, según el riesgo que decida asumir.

- Las herramientas son estándares y la regulación pide muchas cosas por fuera del estándar.

- Debido a la proliferación de nuevas tecnologías, protocolos y mecanismos de seguridad, hay mucho desconocimiento. Por esto, no se atreven a explorar dichos mecanismos para que los servicios financieros sean expuestos a terceros o *plataformas cloud*.

- La verdad, existen riesgos más en la transmisión de la información que en su disposición en las bases de datos. Pienso que esta última se encuentra cubierta; pero en los medios de comunicación no están tan claros los esquemas de seguridad.

- Solo conozco el caso de Nequi; hasta el momento, según tengo entendido, no han presentado problemas de seguridad.

- Los servicios en nube hoy ya alojan servicios masivos que funcionan en línea. En algunos casos, incluyen transacciones financieras, como pueden ser los pagos, y estas son características similares a las del sector financiero.

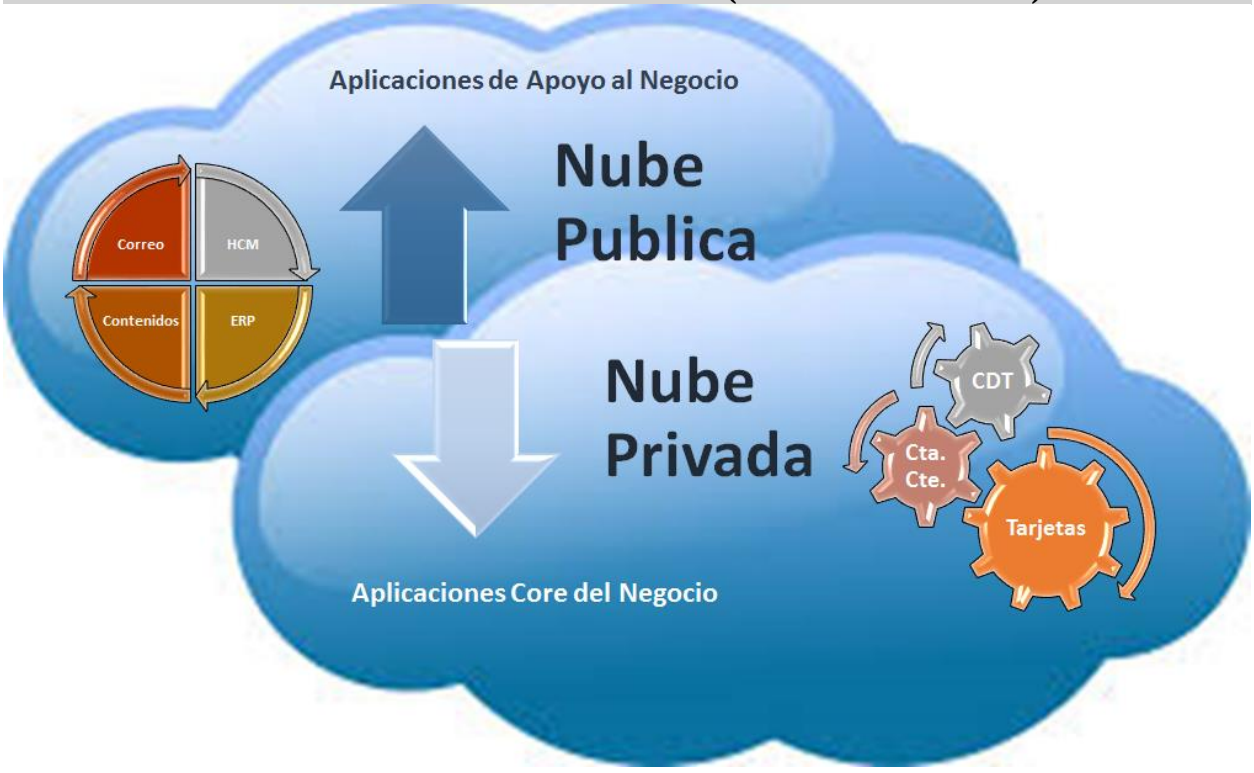
- La seguridad es buena, pero depende del proveedor de nube seleccionado.

- Los proveedores de la nube, en su gran mayoría, ya trabajan bajo estándares de seguridad alta.

Estrategia de banca digital bajo un enfoque fintech**.** Según la información recopilada en la encuesta, un modelo híbrido es el tipo de nube más recomendado para una arquitectura bajo un esquema fintech. En este sistema encuentran las bondades de una nube pública, para aquellas aplicaciones de apoyo al negocio, y de una nube privada, para sus capacidades *core*.

Modelo de nube hibrida. En la siguiente gráfica, se puede ver un modelo de nube híbrida. Esta cuenta con capacidades desplegadas en una nube pública, para aquellas aplicaciones de apoyo al negocio, y con capacidades desplegadas en una nube privada, para las capacidades *core* del negocio y que por el momento no se recomienda que sean llevadas a una nube pública.

FIGURA 22: MODELO DE NUBE **HÍBRIDA (ELABORACIÓN PROPIA)**



Teniendo en cuenta los resultados de la encuesta, se descubre una tendencia hacia el modelo de nube hibrido. Es importante resaltar que, de acuerdo con el segundo objetivo, se evaluarán los tres modelos de nube desde una perspectiva distinta, con un modelo de referencia de industria. Una vez realizada esta evaluación, se comprobará si se conserva la tendencia o si, por el contrario, arroja un resultado distinto.

Planteamiento del desarrollo de una estrategia de banca fintech**.** De forma acorde con el resultado de la encuesta y el análisis realizado, es oportuno decir que el planteamiento de una estrategia de banca fintech es un escenario valido y recomendado. Por ese motivo, se describirá brevemente cómo debería ser ese planteamiento de un banco fintech, el cual parte de una premisa de innovación abierta y de unos pilares estratégicos.

Computación en la nube. Para poder desarrollar una banca fintech, es indiscutible que las capacidades de despliegue de la nube son un recurso que los bancos tendrán que usar. Según el análisis realizado, esto es totalmente viable siempre y cuando, se garantice una buena estrategia de seguridad, la cual está dada en el siguiente pilar estratégico.

Seguridad. La seguridad es el aspecto más importante en cualquier entidad financiera, y esto no cambia en un banco-fintech. Es incluso más importante, dado que se debe garantizar en todo momento que la confidencialidad de la información, el cumplimiento de las normativas legales, la autenticación y el no repudio. De esta forma, se podrá cumplir la normativa legal en todo momento y, más importante aún, garantizar los recursos de los clientes.

Conocimiento y decisión. Bajo un modelo de banca fintech, el conocimiento de los clientes es un factor de vital importancia. Gracias a este, se podrán tomar decisiones más

asertivas, para así brindarle a los clientes lo que realmente necesitan en el momento en que lo necesitan.

Movilidad. La movilidad es otro factor muy importante para tener en cuenta en un esquema de banca fintech: este es precisamente el canal de comunicación por excelencia con los clientes en un modelo de banca fintech. Esta característica les permite a los usuarios interactuar con la banca en todo momento y desde cualquier lugar.

Además de tener en cuenta la premisa de una banca fintech y sus pilares estratégicos, es importante destacar que un buen ecosistema de integración es de vital importancia para garantizar un correcto funcionamiento de la banca fintech. Esto implica que sea un modelo flexible y eficiente, que les permita a los socios y aliados estratégicos integrarse de forma sencilla y rápida al ecosistema del banco. La importancia de esto es que la parte vital de un banco fintech son los socios y aliados estratégicos, los cuales son impulsadores importantes bajo este modelo.

Por consiguiente, el banco no es quien debe hacer todo: se apoya en aliados y socios estratégicos, que son conocedores y expertos de un sector de la industria, y en su conocimiento para generar valor en el banco. En consecuencia, la sinergia entre distintos actores se vuelve parte fundamental del modelo de banca fintech. Con este esquema, los bancos fintech lograrán ser habilitadores de servicios para el crecimiento del país; de esta forma, el papel que actualmente juegan los bancos en una economía nacional se complementaría y evolucionaría, dejando a un lado el rol de promotor de la economía y evolucionando hasta convertirse en el eje central de la economía de principio a fin.

Sin embargo, este solo es el planteamiento del desarrollo de una estrategia de banca fintech. Su desarrollo a nivel conceptual se irá presentando durante el desarrollo de los siguientes objetivos. El análisis de los modelos de nube y en el diseño del modelo de arquitectura se resumen en la **FIGURA 27**.

Segundo objetivo: análisis de modelos de nube

Este objetivo consiste en elaborar un análisis de escenarios con tres modelos de nube (pública, privada e híbrida), para identificar cuál es el modelo que más se ajusta a las necesidades del entorno financiero bajo una arquitectura de un banco fintech que cumpla con los lineamientos de seguridad requeridos por la industria.

Evaluación de modelos de nube**.** A continuación, en la **TABLA 4** se presenta cada una de las variables evaluadas en el análisis de los diferentes tipos de nube, con su respectivo significado y las calificaciones de los modelos de nube seleccionados: pública, privada e híbrida. Las calificaciones se dan en los valores uno, tres y cinco, con el propósito de evidenciar de forma más clara las diferencias entre un modelo y otro. Esta evaluación se realizó teniendo en cuenta el modelo de industria de Oracle y los criterios definidos por este, tal como estaba contemplado previamente.

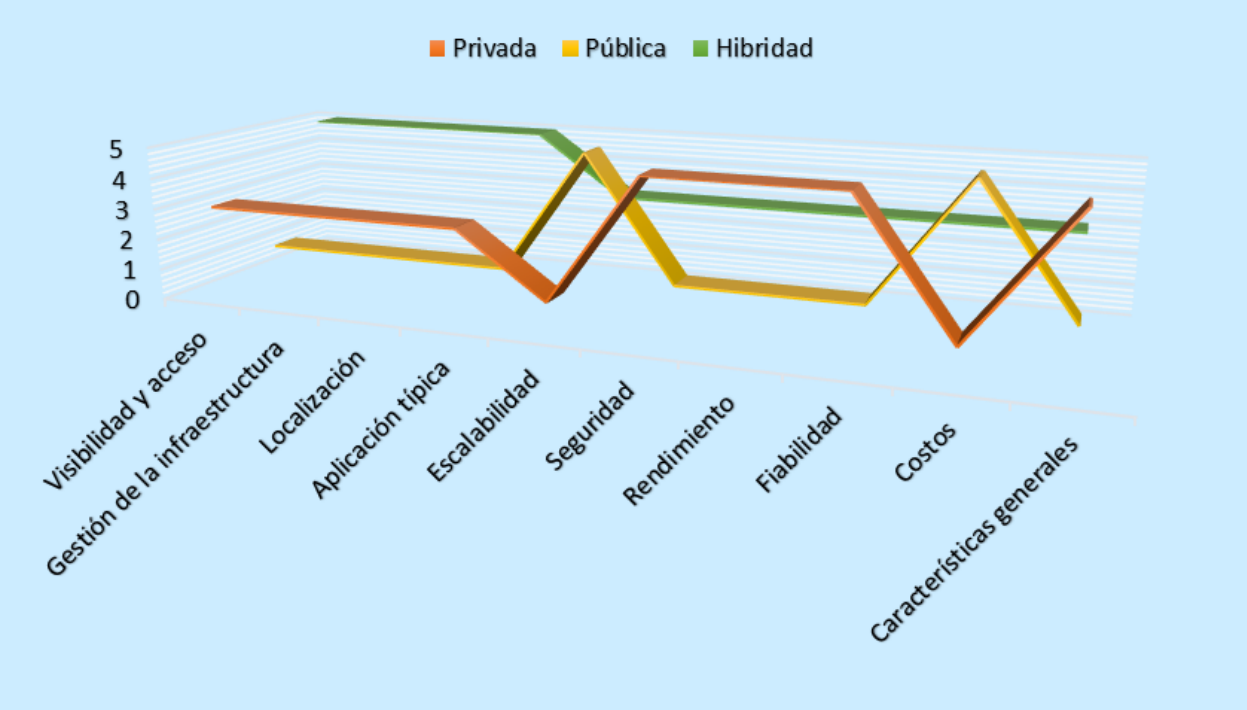
Cada una de las variables definidas se evaluó con un mismo peso. En el momento de realizar un análisis detallado para una entidad específica, el peso de cada variable puede cambiar según las necesidades, la situación tecnológica y económica y las políticas de la organización.

TABLA 4: RESULTADOS DE LA EVALUACIÓN DE MODELOS DE NUBE (ELABORACIÓN PROPIA)

Evaluación de Modelos de Nube						
Nombre de Criterio	**Descripción del Criterio**	**Opciones**	**Privada**	**Pública**	**Hibridad**	**Descripción opción**
Visibilidad y acceso	Hace referencia a quien puede tener acceso a la información	Organización	3			Solo la organización tiene acceso a la información
		Depende de la Información			5	Depende de la información que se quiera acceder
		Todo el Mundo		1		Todos pueden ver la información
Gestión de la infraestructura	Permite identificar de quien depende la gestión de la infraestructura	Proveedor		1		El proveedor es quien gestiona la infraestructura
		Organización	3			La organización es quien gestiona la infraestructura
		Organización y Proveedor			5	La gestión de la infraestructura es compartida
Localización	Permite identificar donde esta ubica la infraestructura	Proveedor		1		El proveedor es quien tiene la infraestructura
		Organización	3			La organización es quien tiene la infraestructura
		Organización y Proveedor			5	La ubicación de la infraestructura es compartida
Aplicación típica	Permite distinguir el tratamiento de la información dentro de una organización	Datos Sensibles	3			Todos los datos son sensibles
		Datos Parcialmente Sensibles			5	Gran parte de los datos son sensibles
		Datos no Sensibles		1		Los datos no son sensibles
Escalabilidad	Es la capacidad de aumentar la capacidad de computó en caso de que se requiera	Alta		5		Fácil escalado de aplicaciones
		Media Alta			3	Posibilidad de picos de procesos y sobre cargas
		Media Baja	1			Necesitad realizar inversiones
Seguridad	Es el nivel de seguridad que se puede obtener en autenticación, confidencialidad, almacenamiento entre otros	Alta	5			Se tiene control completo sobre la seguridad
		Media Alta			3	Capas opcionales de seguridad, seguridad compartida
		Media		1		Depende de la seguridad ofrecida por el proveedor
Rendimiento	Es el nivel de respuesta esperado en los servicios ofrecidos del Banco	Alta	5			Gran capacidad de la red (local) al servicio Cloud
		Media Alta			3	El contenido en la caché se almacena localmente
		Media Baja		1		Recursos compartidos por gran número de usuarios
Fiabilidad	Es el nivel de confiabilidad esperado en los servicios ofrecidos del Banco	Alta	5			Todos los equipos pertenecen a la organización
		Media Alta			3	El contenido en la caché se almacena localmente, hay dependencia del servicio
		Media		1		Dependiente de la conectividad a internet y de la disponibilidad del servicio
Coste	Son los costos asociados el tipo de nube que se desea trabajar	Alto	1			Requiere equipamiento en el Data Center
		Medio		5		Permite migrar a la nube gran parte de los equipos hacia un modelo de pago por uso
		Bajo			3	Permite migrar a la nube todos los equipos hacia un modelo de pago por uso
Características generales	Estas características generales están enfocadas los niveles de seguridad que requiere la organización	Estrictas	5			El negocio gira en torno a los datos de la empresa (la seguridad es crucial)
		Moderadas			3	Empleo de aplicaciones SaaS con necesidad de cumplir estrictas medidas de seguridad
		Flexibles		1		Los niveles de seguridad pueden varias según las aplicaciones
Resultado Consolidado de los Criterios Evaluados			**34**	**18**	**38**	**El modelo con mejores resultados es el Modelo Hibrido.**

El cuadro anterior es bastante extenso: tiene todas las variables con sus múltiples opciones y calificaciones. Por eso, se incluye otra gráfica resumida: la **FIGURA 23**. En este resumen, se pueden ver las opciones de nube y su tendencia de forma más accesible.

FIGURA 23: CONSOLIDADO DE LA EVALUACIÓN DE MODELOS DE NUBE (ELABORACIÓN PROPIA)



Como se puede comprobar en el cuadro de análisis de modelos de nube y en la gráfica de resumen (**TABLA 4** y **FIGURA 23**, respectivamente), el modelo de nube híbrida es el que cuenta con un mejor resultado en la calificación de todas sus variables. Aun así, esto no quiere decir que sea un modelo que cumpla al 100 % en cada una de sus variables, pero sí es el que más se acerca a tener un cumplimiento integral.

Seleccionar el modelo de nube es el primer paso, aunque este por sí solo no garantiza una implementación exitosa. Para eso se deben abordar otros aspectos de igual importancia, que deben estar enmarcados en el modelo de arquitectura, enfocados en la estrategia del negocio y en el diseño de seguridad de la solución. Dicho de otra forma, todo modelo debe ser acorde con las

necesidades del negocio y con las normativas legales que rigen en Colombia. Estos aspectos se podrán apreciar en el desarrollo de los siguientes objetivos de este proyecto.

Teniendo presentes estos resultados y extrapolándolos con lo realizado en el primer objetivo, se recomienda adoptar un modelo de nube híbrida para la banca fintech. Esto le abre la puerta a un análisis adicional: es necesario entender el estado actual de las nubes públicas, desde todos los aspectos. Por ese motivo, se hará una evaluación de nubes públicas, donde se revisen todas sus capacidades desarrolladas hasta la fecha, para no recomendar un modelo de nube hibrido, si no también ver qué nube pública puede complementar este modelo.

Evaluación de nubes públicas**.** A continuación, la **TABLA 5** resumirá el análisis de los principales proveedores de nube que hay actualmente en el mercado. Este informe se basa en un reporte publicado el 1 de octubre del 2017 (Cloud Comparer, 2017); este último documento contiene todas las categorías mencionadas con un alto nivel de detalle. A partir de ahí, se procedió a evaluar una por una y a consolidar las categorías en mención.

TABLA 5: RESULTADOS DE LA EVALUACIÓN DE NUBES PÚBLICAS (ELABORACIÓN PROPIA, BASADA EN CLOUD COMPARER (2017))

Categoria/Proveedores de Nube	Amazon	Microsfot Azure	Google Cloud Platform	IBM Bluemix	Oracle
Computo	4	4	3	4	3
Almacenamiento	5	5	3	3	3
Base de Datos	4	5	3	3	3
Migración de Servicios	5	4	1	2	1
Redes y Entrega de Contenido	5	5	5	3	5
Herramientas de Desarrollo	5	3	4	3	2
Herramientas de Administración	5	4	3	1	2
Recuperación de Desastres	5	5	1	1	1
Seguridad, Idedntidad y Cumplimiento	5	4	3	2	1
Big data y analitica	5	5	3	2	2
Inteligencia Artificial	4	4	4	5	1
Servicios de Dispositivos Moviles	5	5	3	2	2
Servicios de Aplicaciones	5	5	2	2	2
Productividad Empresarial	5	5	3	1	1
Software MarketPlace	5	5	5	5	5
Internet de las cosas	5	4	3	3	3
Desarrollo de Juegos	5	5	1	1	1
Desarrollo y Pruebas	5	5	1	1	1
Consolidado	**87**	**82**	**51**	**44**	**39**
Promedio	**4.83**	**4.56**	**2.83**	**2.44**	**2.17**

De este cuadro puede concluirse que, actualmente, hay cinco grandes proveedores de nubes públicas; se enumeran a continuación:

- Amazon Web Services

- Microsoft Azure

- Google Cloud Platform

- IBM Bluemix

- Oracle

Estas empresas son las que están marcando las tendencias en el desarrollo de capacidades en la nube; estos son los proveedores que se van a considerar. No obstante, este es un mundo

altamente cambiante; en corto tiempo pueden presentarse muchos cambios. La realidad actual es que cualquier entidad que quiera incursionar en la nube tendrá que recurrir a estas compañías.

Teniendo esto como punto de referencia, es importante notar que para el entorno financiero solo hay dos nubes que cumplen con todas las necesidades requeridas, especialmente con las variables de seguridad: Amazon Web Services y Microsoft Azure. Principalmente, esto se explica por su nivel de madurez, desarrollo de capacidades y evolución constante; por estos motivos, el modelo de arquitectura que se desarrollará en el transcurso de esta tesis tendrá como uno de sus componentes la nube publica de cualquiera de estos proveedores.

Aunque en este caso se recomienda trabajar con las nubes de Amazon o de Microsoft, pueden presentarse situaciones donde se requiera implementar otra nube. Por ejemplo, si se habla de servicios de inteligencia artificial, la recomendación es hacerlo sobre la nube de IBM con Watson. Cada nube tiene unas características especializadas, y en ocasiones es mejor tener dos o tres proveedores de nube, para poder aprovechar estas características.

Tercer objetivo "diseñar un modelo de arquitectura"

En este objetivo se debe diseñar un modelo de arquitectura que cumpla con los lineamientos de seguridad requeridos para una banca fintech bajo un esquema de nube hibrida.

Para poder realizar este objetivo y profundizar en el análisis, es necesario tener claridad sobre cuáles son los componentes del negocio —técnicos y de seguridad— que harán parte de la arquitectura y del modelo conceptual requerido.

Componentes de un modelo conceptual de arquitectura**.** Antes de crear un diseño de arquitectura de seguridad en la nube, hay que definir la estrategia organizacional. Por eso, a

continuación, se puede ver un modelo conceptual definido y elaborado a la luz de este proyecto. Este modelo cuenta con cinco grandes focos, planteados de forma acorde con un modelo de nube híbrido. Los focos de este modelo son los siguientes:

Aplicaciones críticas de un banco. Este foco incluye las aplicaciones del negocio que se deben mantener dentro de la organización, a causa de su criticidad, confidencialidad y seguridad. Por el otro lado, también permite decidir cuáles pueden ser llevadas a un modelo de nube. Para el caso de un modelo de banca fintech, se pueden clasificar estas aplicaciones en dos grandes grupos:

Aplicaciones core. En este grupo de aplicaciones están todas aquellos que son el *core* del negocio: aplicaciones de productos (cuenta corriente, ahorros, CDT, entre otros), aplicaciones de mesa dinero y todas aquellas aplicaciones especializadas o de valor estratégico para la entidad. La selección de las aplicaciones *core* dependerá de un proceso de evaluación interno en cada organización; pero un buen referente es tomar aquellas aplicaciones que, en caso de un desastre o catástrofe, son necesarias para ofrecerles a los clientes los servicios básicos mientras se normaliza la emergencia presentada.

Aplicaciones de apoyo al negocio. En este grupo figuran todas aquellas aplicaciones que son necesarias para el funcionamiento del negocio, pero que no hacen parte del *core* financiero. Estas aplicaciones están más estandarizadas en la industria y no tienen un valor diferenciador para el negocio financiero. Algunas de estas aplicaciones son, por ejemplo, las de gestión humana, gestión documental, correo, contenidos, ERP, entre otras. Es importante aclarar que, sin estas aplicaciones, el negocio puedo seguir funcionando por un tiempo, ofreciendo los servicios básicos.

Pilares estratégicos de un modelo ***Fintech.*** Los pilares estratégicos de un modelo fintech tienen como objetivo sentar las bases de la banca Fintech, para que la organización pueda realizar sus despliegues de forma óptima y eficiente. Este proceso se realiza considerando las necesidades del cliente y a la evolución del entorno, circunstancias a las que se enfrentan las entidades financieras. Por eso, se identificaron y plantearon los siguientes pilares:

Conocimiento y decisión. Este pilar tiene como propósito maximizar el conocimiento de la organización, clientes, proveedores, aliados e incluso de los no clientes, para poderles brindar una experiencia personalizada y satisfactoria en todo el ecosistema de la entidad financiera a quien lo requiera.

Esto se logra a través de la recopilación de información en todos los canales de la entidad, las redes sociales y los socios estratégicos. Esta información se debe llevar a un modelo de *big data*, para que sea posteriormente analizada mediante modelos analíticos especializados; como resultado, dicha información generará valor para la organización y los clientes.

Actualmente, los temas de *big data*, analítica, computación cognitiva, análisis de redes, análisis de sentimiento —todo lo relacionado con el conocimiento de los clientes, su entorno y sus decisiones— son de vital importancia para maximizar los resultados y minimizar los riesgos, con el fin de lograr arquitecturas y despliegues más eficientes.

Computación en la nube. Este pilar es el más importante para este proyecto, debido a que tiene como propósito habilitar esquemas de despliegue más eficientes para las organizaciones financieras. En consecuencia, estas podrían competir de forma eficiente con las fintech y darles soluciones más oportunas a los clientes.

La nube no es una moda: las nubes llegaron y cada día cobran más fuerzas. Por consiguiente, es necesario que las organizaciones se muevan bajo este mismo entorno; aunque hay que aclarar que los cambios deben ser paulatinos y acordes con las evoluciones que presenten en los proveedores de nube. Es muy probable que en 10 o 15 años sea viable decir que una entidad financiera tradicional este 100 % montada en una nube pública. Sin embargo, las organizaciones se deben mover con cautela: dando pasos firmes hacia la nube, pero de forma segura y estructurada.

Movilidad. Aunque ya hace parte de la vida diaria de todos, es importante este pilar: actualmente presenta una evolución vertiginosa, y está presente en casi cualquier solución que se base en un modelo de nube. Además, cuando se considera el conocimiento del cliente y de su movilidad, este concepto va más allá de un dispositivo móvil; implica saber dónde han estado y están los clientes, para saber que ofrecerles según sus preferencias y sus ubicaciones.

Conocer dónde está el cliente vas más allá de ofrecerle productos y servicios o campañas de mercadeo; conocer la ubicación del cliente les permite a las organizaciones mejorar su esquema de seguridad de acuerdo con la ubicación de cliente y de dónde está tranzando. Esta información es vital para las organizaciones; por eso es uno de los pilares que se revisarán a continuación.

Seguridad. Es la base angular en cualquier arquitectura de una entidad financiera. Cuando se habla de seguridad, es necesario profundizar y entrar en un nivel de detalle superior, ya que en la seguridad hay muchas aristas que se deben tener en cuenta. A continuación, se explicarán en detalle algunas cuestiones que es necesario revisar.

- *Autenticación y control de acceso*. Se debe garantizar que el usuario que ingresa al sistema sea quien dice ser. El servicio de autenticación debe funcionar en cualquier medio usado por los usuarios: canales digitales, físicos, móviles, etc. Es importante tener en cuenta que el mecanismo de autenticación puede variar de una canal a otro, para garantizar un mayor nivel de seguridad. Se pueden usar diferentes mecanismos de autenticación biométrica (voz, huella, facial, etc.), doble factor de autenticación, autenticación con contraseña de un solo uso (OTP), entre otros.

- *No repudio*. Es un servicio de seguridad que debe garantizar en todo momento que el mensaje recibido sí corresponda a quien lo envió y viceversa. Con esto se busca que ambas partes tengan certeza de la comunicación establecida entre ellos, para evitar suplantaciones y reclamaciones indebidas.

- *Confidencialidad*. La confidencialidad de la información es un factor de alta importancia en las entidades financieras, motivo por el cual el acceso debe ser restringido, según roles y responsabilidades. Además de esto, se requiere que la información sensible quede cifrada en reposo, que se transmita mediante canales seguros o cifrados y que los datos también viajen cifrados. Para estos fines, pueden aplicarse uno o varios de los mecanismos, según se requiera, para garantizar en todo momento la confidencialidad de la información de los clientes.

- *Integridad*. Es un servicio de seguridad que garantiza que la información solo sea modificada, creada o borrada por los procesos del cliente y del personal autorizado. El sistema no debe modificar o corromper la información que almacene, ni tampoco permitir que alguien no autorizado lo haga. El problema de la integridad no sólo se refiere a modificaciones intencionadas, sino también a cambios accidentales.

- *Disponibilidad*. La disponibilidad es el servicio que garantiza que los usuarios tengan acceso a la información en el momento y la forma que lo requieran. Esto se debe garantizar a nivel de *hardware* y *software* para que funcione eficientemente y sea capaz de recuperarse ante una eventual falla.

- *Monitoreo*. El monitoreo en seguridad de TI es un factor de vital importancia, y se debe abordar tanto desde un monitoreo interno como externo. Las amenazas de seguridad en una entidad financiera pueden llegar a través de una persona, una circunstancia, un evento o un fenómeno malicioso que pueda provocarles daño a los sistemas y producir pérdidas materiales, financieras y de reputación Cuando se hace un monitoreo, normalmente se buscan las siguientes amenazas:

    - Amenazas humanas
    - Amenazas de hardware
    - Amenazas de red
    - Amenazas lógicas
    - Amenazas por fenómenos naturales

- *Evolución constante*. Para garantizar la seguridad en una entidad financiera, es importante estar evolucionado constantemente, ya que las amenazas cada día son más y más sofisticadas. Por esta razón, las entidades financieras deben contar con equipos especializados en todo lo relacionado con seguridad, cuya característica principal sea la evolución constante. La seguridad no da espera; debe ser abordada con seriedad y total compromiso, ya que está en juego la reputación de la entidad y los activos de los clientes.

- *IOT*. El internet de las cosas es el último pilar necesario en un modelo Fintech. Cada vez son más los objetos o cosas a los que se les agregan capacidades de comunicación por internet y capacidades cognitivas. Esto implica que cada vez van a ser más los componentes o cosas que van a interactuar con las entidades financieras. En ese orden de ideas, los bancos deben estar preparados para ofrecer estos servicios de integración de forma segura, para así poder aprovechar un nicho de mercado que es relativamente nuevo, pero que va a tener un gran auge en los próximos años.

Capa de integración y mediación. En cualquier arquitectura, y especialmente en una hibrida, la capa de integración es uno de los factores más complejos y, a su vez, claves en una implementación. La importancia de este elemento se explica porque en esta capa se realiza toda la orquestación entre las aplicaciones *core* del banco, los servicios de la nube y los socios estratégicos. Por este motivo, en esta capa se identifican cinco grandes aspectos que deben considerarse para un modelo de banca fintech:

Conexión transaccional en tiempo real. La conexión en tiempo real de cualquier aplicación financiera es de vital importancia. Al estar cada vez más conectados, los clientes esperan poder transar desde cualquier parte y de forma rápida. Hoy no se está hablando de segundos para que una transacción monetaria o no monetaria sea realizada; se está hablando de milisegundos. Lo anterior hace que los diseños de arquitectura sean más eficientes y optimizados, para garantizar una óptima respuesta en todo momento. Además de usar cada vez más capacidades de computo en memoria, conexiones virtualizadas, entre otras, estas capacidades también se complementan con modelos de aplicaciones basadas en contenedores, microservicios y Apis. En consecuencia, estas capacidades están dejando atrás las aplicaciones monolíticas y complejas.

Microservicios. Los microservicios son un enfoque diseñado para desarrollar una aplicación de *software* como una serie de pequeños servicios, cada uno ejecutándose de forma autónoma y comunicándose entre sí. Además, cuentan con la capacidad para ser reusados en múltiples soluciones contenerizadas.

Una aplicación se diseña en múltiples microservicios, que luego se integran. Esto genera facilidades en el despliegue, en los cambios, en las pruebas y en las futuras mejoras que se requieran. Las aplicaciones que triunfan evolucionan por serles útiles a sus usuarios; las que fracasan no evolucionan y terminan por entrar en desuso. Por eso, las aplicaciones construidas bajo un esquema de microservicios generan valor para las organizaciones, ya que su mecanismo de evolución es más eficiente.

Contenedores. Cuando se está hablando de contenedores, normalmente se piensa en esos contenedores que cargan los camiones en los puertos. La verdad es que este concepto no es muy diferente: lo que se hizo fue extrapolar ese concepto al desarrollo de aplicaciones, para hacer las aplicaciones más portables, ligeras y autosuficientes. Con este nuevo esquema de desarrollo, se puede decir que una aplicación es construida por partes y, luego, se sitúa todo dentro de un contenedor que se despliega como aplicación. La ventaja de este sistema es que puede usar cualquier componente en múltiples contenedores y que puede cambiar un componente sin afectar todo el contenedor.

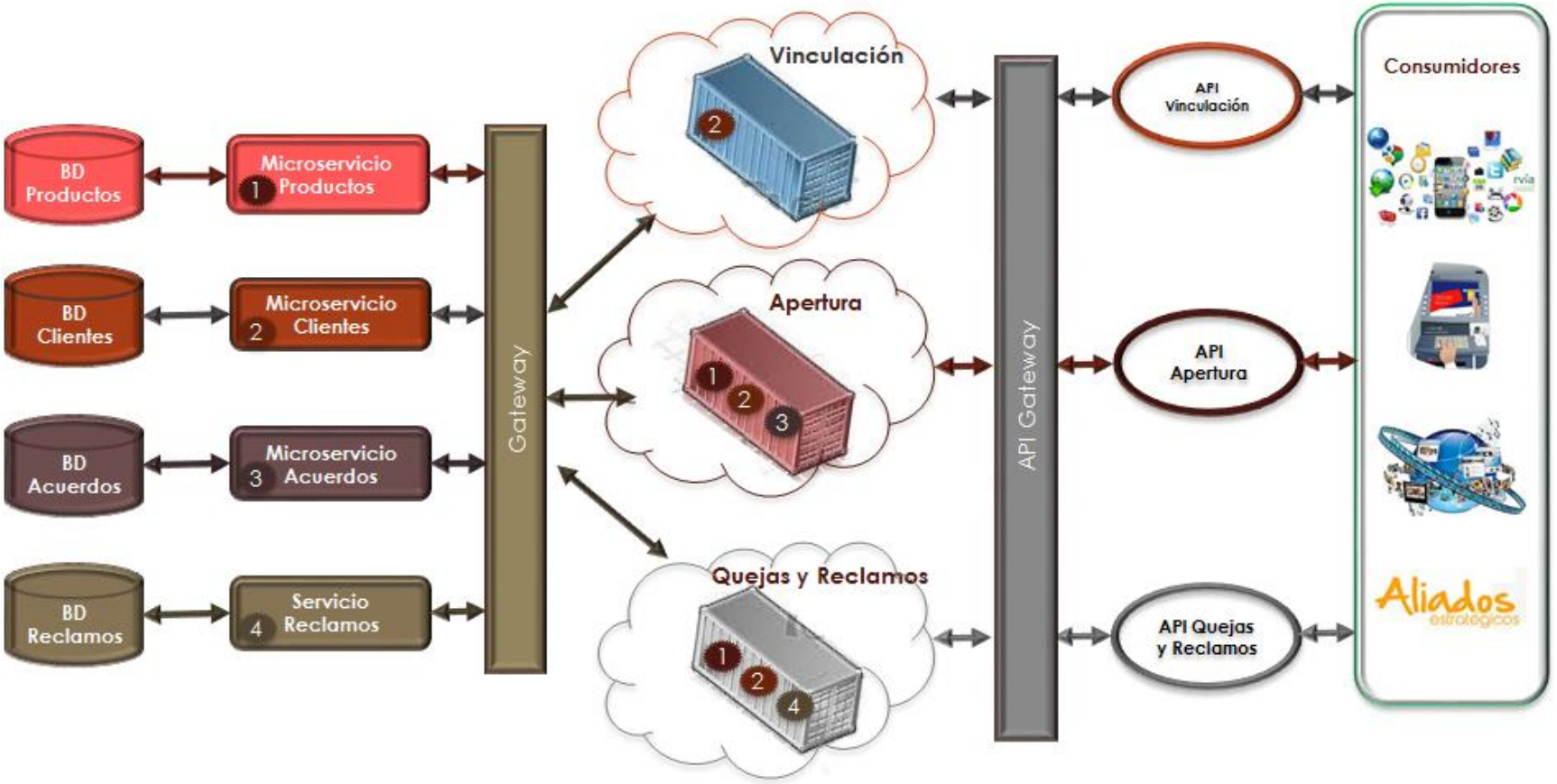
Un contenedor es un proceso para el sistema operativo, que internamente la aplicación que se desea ejecutar, junto con todas sus dependencias. La aplicación contenida solamente tiene visibilidad sobre el sistema de ficheros virtual del contenedor y utiliza indirectamente el *Kernel* del sistema operativo principal para ejecutarse. Esta herramienta permite probar aplicaciones o

sistemas en un entorno seguro e igual al de producción, reduciendo así tiempos de pruebas y adaptaciones a cambios de hardware desde el entorno de prueba al de producción.

APIs. Es una interfaz de programación de aplicaciones, que en sí es un conjunto de subrutinas, procedimientos y funciones de una programación orientada a objetos. Esta característica les permite a las APIs tener una capa de abstracción y conectar software entre sí para el intercambio de información. Precisamente esta capacidad es la que hace que el modelo de desarrollo de APIs encaje también con el esquema de microservicios y contenedores. Como resultado, produce un ecosistema de integración simple, pero eficiente para las necesidades de las organizaciones financieras, como sucede en este caso o en cualquier otro tipo de institución.

´A continuación, la **FIGURA 24** muestra un breve ejemplo sobre cómo interactúan estas tres capacidades entre sí para generar un ecosistema de integración más robusto, moderno y eficiente, acorde con las necesidades actuales y con la evolución tecnológica que se ha dado en los últimos años. Este modelo le permite las organizaciones competir de forma más eficiente y coherente con lo que necesitan los usuarios de esta generación, muy enfocados en la tecnología.

FIGURA 24: DIAGRAMA DE CORRELACIÓN DE MICROSERVICIOS CON LOS CONTENEDORES Y EL MUNDO DE LAS APIS (ELABORACIÓN PROPIA)

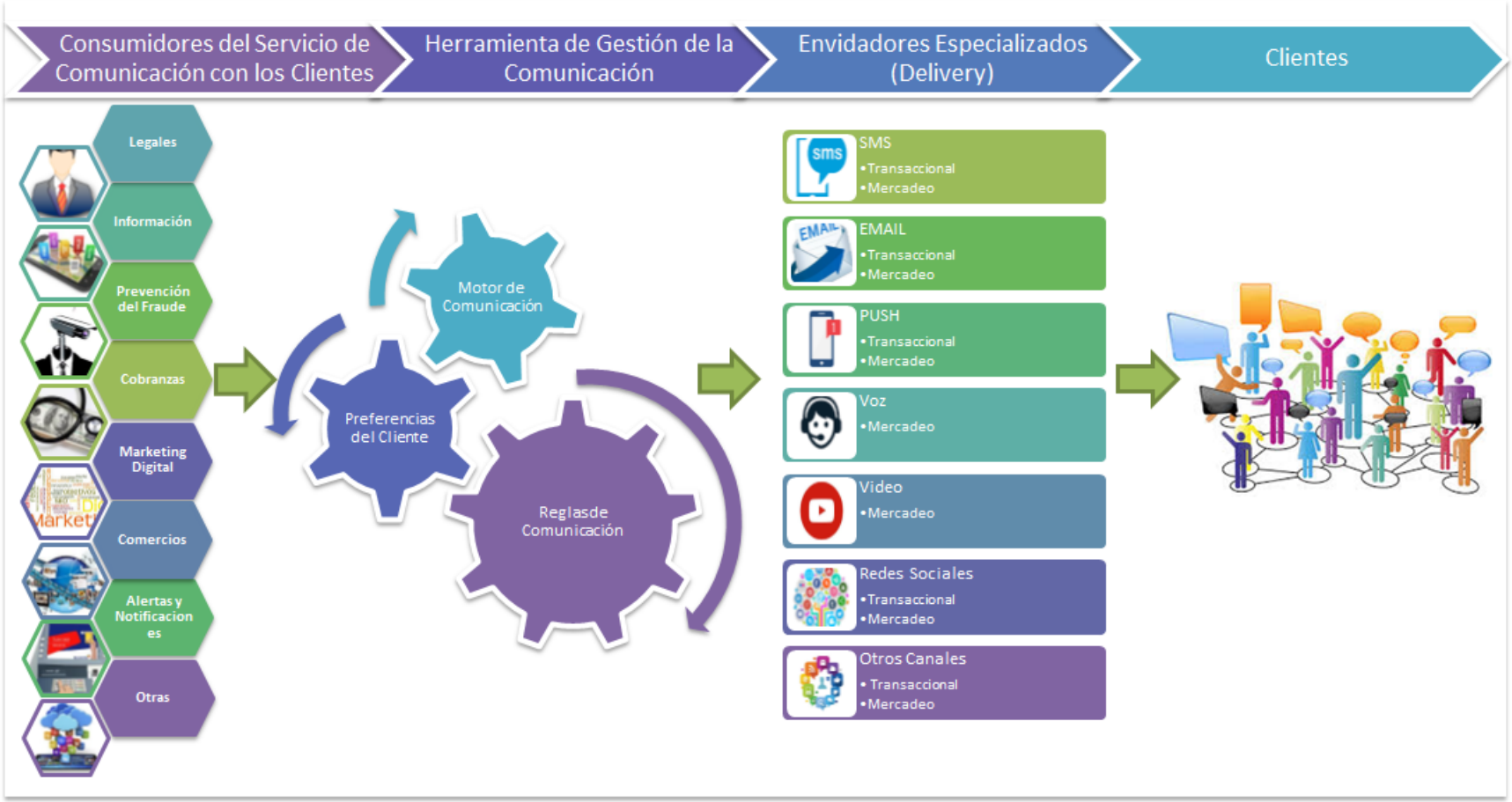


Servicios de seguridad. Cuando se habla de servicios de seguridad, hay múltiples opciones a nivel de red, *hardware* o *software*. Sin embargo, el propósito de este trabajo es que se tengan como foco los pilares más definidos en el nivel de las necesidades funcionales y de las aplicaciones, independientemente de que herramientas los soporten. Para hablar de las capacidades de seguridad, es necesario retomar lo que explicó previamente sobre los microservicios, contenedores y APIs. Bajo este mismo esquema se pueden desarrollar las capacidades de seguridad, para que sean reutilizadas por cualquier canal, con la meta de mejorar el tiempo de detección y de respuesta ante amenazas.

En temas de seguridad siempre es importante tener productos de mercado que estén a la vanguardia tecnológica y que brinden el soporte de expertos técnicos para adaptarse al cambiante mundo de la seguridad.

Gestión de la comunicación. La gestión de la comunicación es un concepto que todavía es infravalorado y desconocido por muchos. Hoy, la comunicación, en la mayoría de los casos, es caótica y poco eficiente, por lo que se hace necesario que un modelo de banca fintech tenga un mecanismo de gestión de la comunicación eficiente. De esta forma, podrá tener proveedores especializados en la contactabilidad con los clientes, ya sea vía email, SMS, Push, redes sociales, canales digitales y video, entre otros. Por otro lado, con un buen sistema de comunicación siempre se podría saber por cuál medio se está comunicando el cliente, que tan seguro y eficiente es el contacto y las preferencias de comunicación de los clientes. La comunicación impersonal ya no es suficiente: el cliente requiere una comunicación personalizada y que responda a sus necesidades. A continuación, se incluye la **FIGURA 25**: un diagrama de gestión de la comunicación con los clientes.

FIGURA 25: DIAGRAMA DE GESTIÓN DE LA COMUNICACIÓN CON LOS CLIENTES (ELABORACIÓN PROPIA)



Aliados estratégicos. Cuando se piensa en aliados estratégicos, se parte de que la banca tradicional monolítica ya no es eficiente; el mundo actual es altamente cambiante y ninguna organización financiera puede asumir estos cambios por si sola, a la velocidad que exige el mercado. Las entidades financieras deben abrir su campo de visión y generar sinergias con aliados estratégicos en múltiples sectores, tanto del negocio como de TI. Este es uno de los grandes impulsadores de la transformación digital: las sinergias permiten obtener una mayor velocidad de respuesta y aprovechar la experticia de cada uno de los aliados en su campo de acción, ya sea seguridad, nube, gestión de la comunicación, de sectores de industria o cualquier otro aliado que se tenga.

De esta manera, los aliados estratégicos pasan a ser parte del ecosistema financiero; se convierten en uno de los motores que ayudan a impulsar el mundo financiero. A su vez, los bancos se transforman en los impulsores de la transformación digital del país, generando una simbiosis donde todas las partes involucradas se benefician. Si los bancos logran entender esto y adoptan esta cultura, se verá una transformación del sector como no se ha visto en muchos años; tal vez aún no se ha visto una transformación así.

El sector bancario siempre ha sido unos de los motores de la economía; sin embargo, siempre se ha comportado de forma monolítica y cerrada. Ahora están dadas las condiciones para que siga siendo el motor de la economía, pero con una relevancia mayor y con una apertura que puede cambiar lo que hoy se conoce como el mundo financiero. A continuación, la figura 26 alude a algunos de los sectores que podrían ser aliados estratégicos de las entidades financieras y que deberían empezar a generar sinergias para un mayor beneficio de la economía y de los usuarios.

FIGURA 26: ALIADOS ESTRATÉGICOS PARA LAS ENTIDADES FINANCIERAS. (ELABORACIÓN PROPIA)

Servicios externos. Para las entidades financieras los servicios externos son de gran importancia. Normalmente, esta categoría incluye a los entes regulatorios como la Superintendencia Financiera de Colombia, el Banco de la República, la Bolsa de Valores de Colombia e incluso las bolsas de otros países; además, aquí se suma el cumplimiento de otro sinfín de normas que deben cumplir todas las entidades financieras. No se entrará en detalle sobre estas; aunque esto hace parte de la cotidianidad de los bancos, solo se hace mención por su relevancia en el momento de un diseño de arquitectura.

Modelo de arquitectura de un banco **Fintech.** Antes de entrar en detalle con respecto a una arquitectura de banca Fintech, hay que pensar desde un enfoque más conceptual qué es un banco fintech. En los puntos anteriores se ha revisado cada uno de los componentes de este modelo conceptual; sin embargo, esto se ha hecho de forma independiente; ahora es el momento de comenzar con un panorama completo de lo que se requiere para un banco fintech: cómo encaja cada uno de los componentes y la importancia que tiene cada uno. Todos tienen un rol que deben cumplir para poder desarrollar un diseño de arquitectura bajo un modelo de nube híbrida, con un esquema de seguridad acorde al entorno que enfrentan las entidades financieras actualmente. Además, todo lo anterior debe hacerse teniendo en cuenta la apertura que deben tener los bancos para formar alianzas con socios estratégicos, que les permitan evolucionar según el entorno actual. Para esto, se presenta a continuación un diagrama conceptual en la **FIGURA 27** y una vista general en la **FIGURA 28**, que ilustran la arquitectura de un banco fintech a alto nivel. Luego se ilustrará con más detalle la descripción y recomendación de los servicios de seguridad requeridos para este tipo de implementaciones.

FIGURA 27: MODELO CONCEPTUAL DE UN BANCO FINTECH **(ELABORACIÓN PROPIA)**

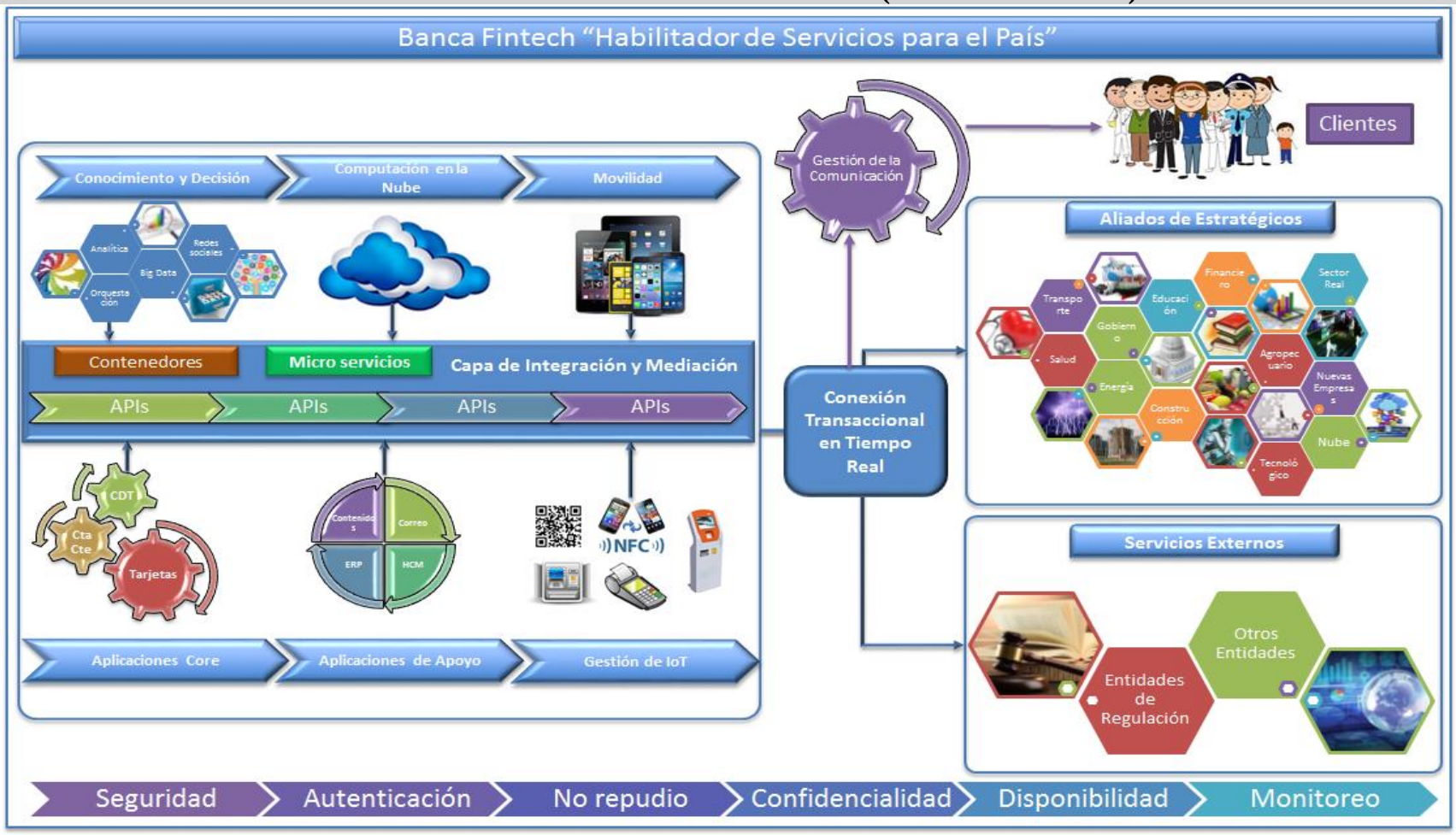


FIGURA 28: DIAGRAMA DE ARQUITECTURA BAJO UN ESQUEMA DE NUBE HÍBRIDA (ELABORACIÓN PROPIA)

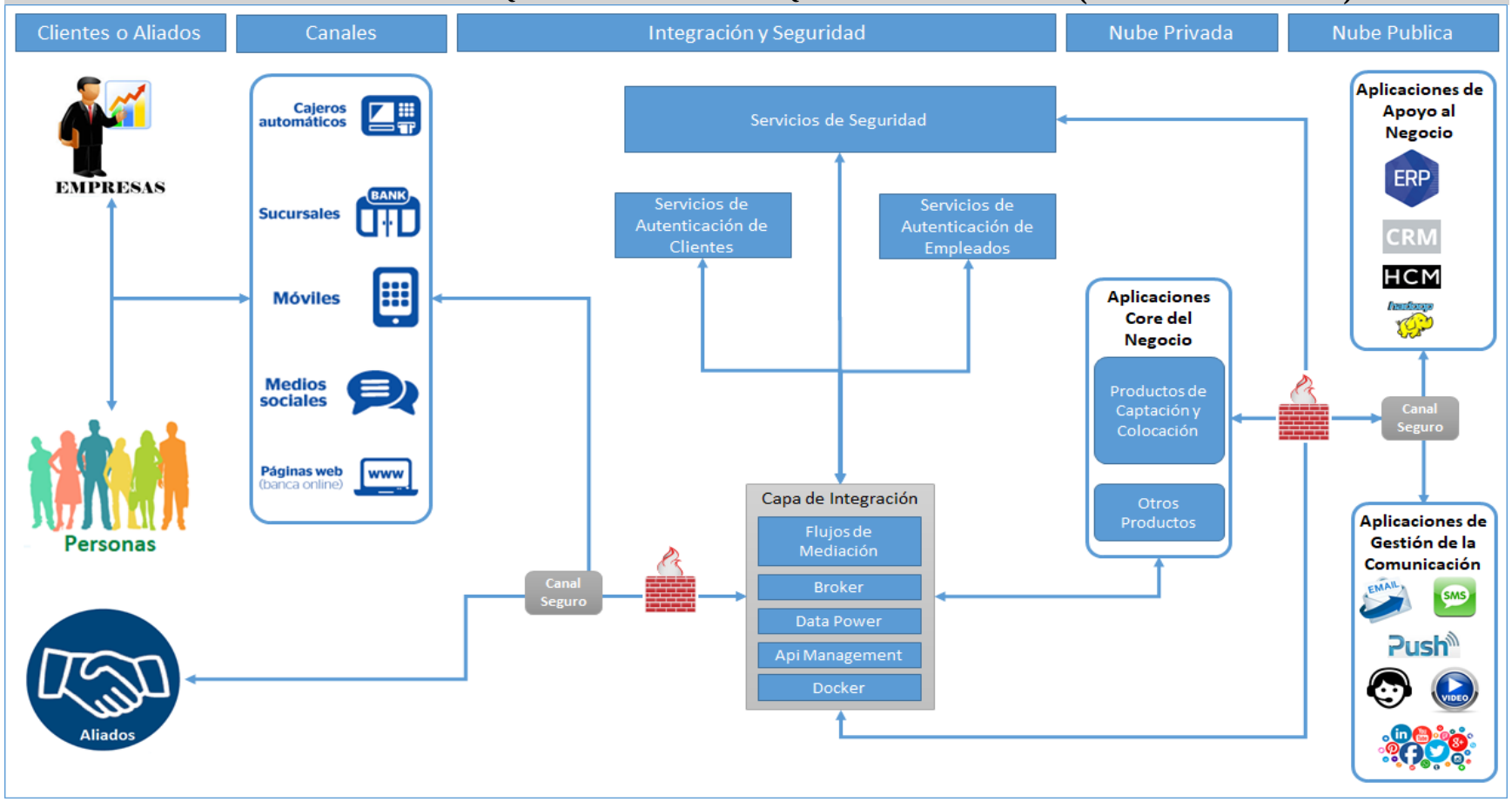


FIGURA 29: DIAGRAMA DEL PERÍMETRO DE SEGURIDAD DE UN MODELO DE BANCA FINTECH (ELABORACIÓN PROPIA)

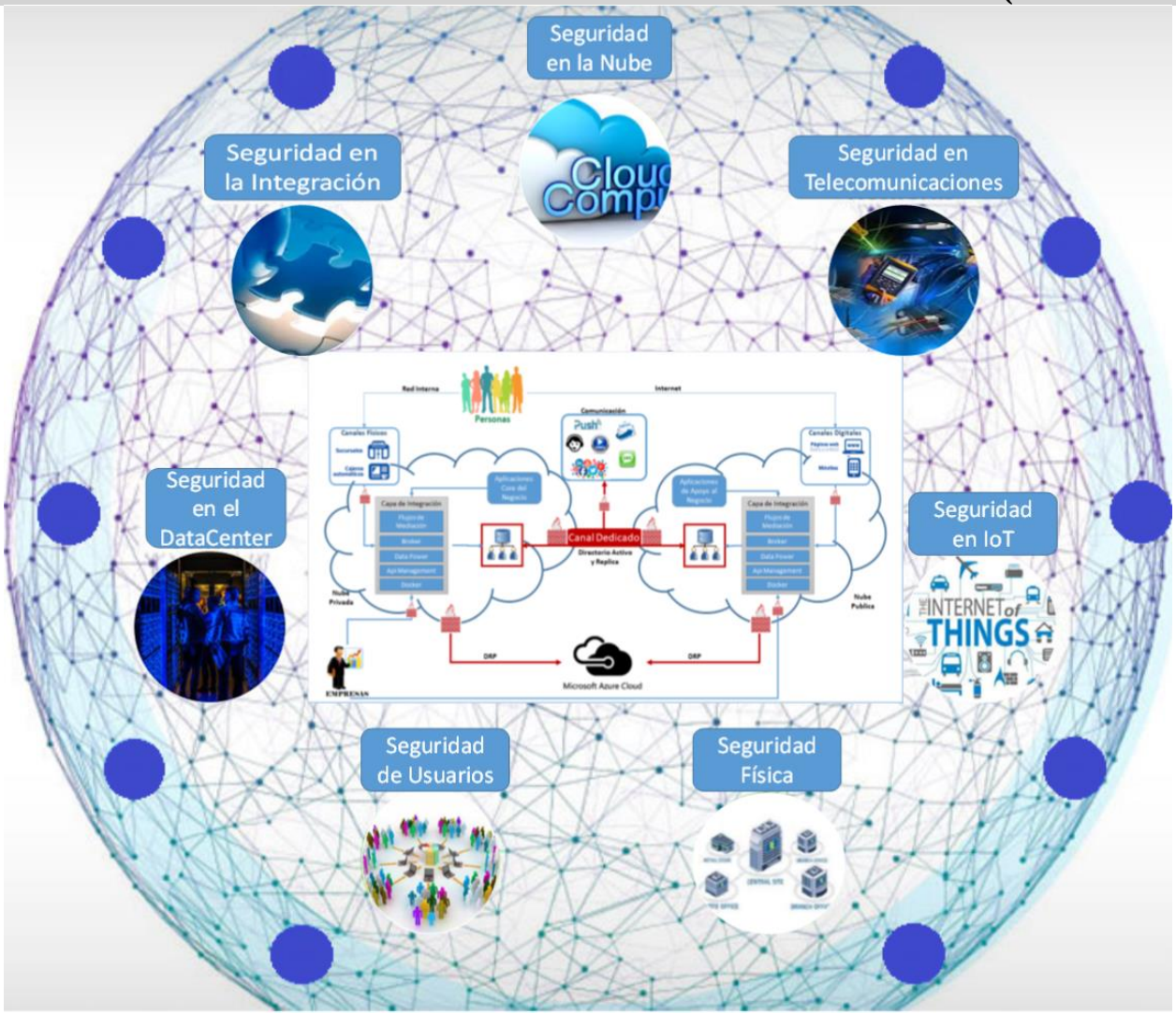
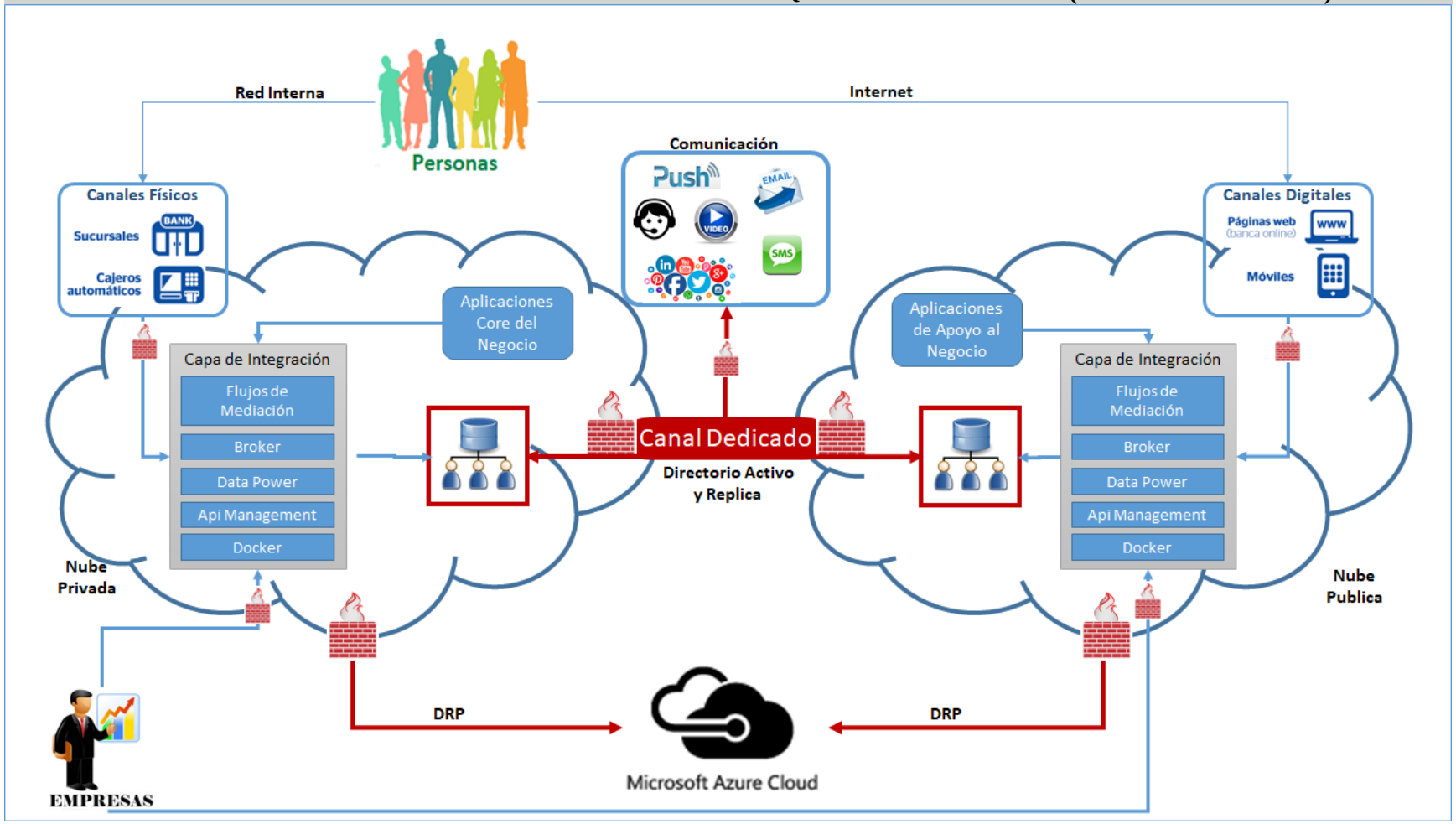


FIGURA 30: MODELO CONCEPTUAL DE SEGURIDAD BAJO UN ESQUEMA DE NUBE HÍBRIDA (ELABORACIÓN PROPIA)



Requisitos de negocio de un banco fintech**.** Los requisitos de negocio que se mencionan a continuación están pensados a la luz de un banco fintech. No se hace mención de otra serie de requisitos que debe un cumplir un banco, debido a que estos hacen parte del funcionamiento tradicional de la banca. Para este caso es relevante enfocarse en aquellos requisitos que generan transformación y disrupción en las entidades financiera y apalancan el modelo de banco fintech.

Innovación abierta. La innovación es un prerrequisito para cualquier fintech; de igual manera, un banco fintech debe adquirir esta mentalidad y sumarse a soluciones tecnológicas externas. Incluso podría abrir su propia propiedad intelectual, con el fin de ayudar a generar nuevas ideas, identificar y atraer nuevas habilidades y descubrir nuevas áreas de crecimiento.

Un banco fintech debe estar en la capacidad de repensar su negocio y las tecnologías que lo soportan de forma más abierta y ágil. La evolución de la tecnología y de la competencia es una constante, y, como tales, los bancos deben evolucionar según esa misma corriente.

*Colaboración***.** La colaboración es un aspecto fundamental en una banca-fintech. este desafío consiste en colaborar con otras industrias para identificar nuevas formas de generar valor; las entidades financieras ya no tienen que ser los expertos en todo, pueden apoyarse en compañías que son expertas en ciertos nichos de mercado o tecnologías. Además, es muy importante que las entidades financieras busquen colaboración con el entorno, para así lograr sinergias en toda la cadena de valor y ser los apalancadores tecnológicos de la industria colombiana.

*Computación en la nube***.** La computación en la nube es uno de los aspectos cruciales para un banco-fintech, a causa de que esta le da la una capacidad de despliegue acorde con las

necesidades del negocio. La inversión se realiza dependiendo de la necesidad, para alcanzar de sa manera un crecimiento más estructurado.

Para el caso de un banco fintech, se estará trabajando con un modelo de nube híbrida, esto según los resultados previos de los modelos de nube y evaluación de nube. En esa sección de este documento, se optó por trabajar la parte de nube publica con el servicio de Amazon o de Microsoft: son las que mejor se adaptan a las necesidades de este proyecto, tanto por los niveles de seguridad como por los servicios que ofrecen.

Movilidad. La banca-fintech debe tener como canal de interacción con los clientes los dispositivos móviles y todo lo relacionado con estos. Esta innovación permite aprovechar las capacidades propias de los usuarios y la oportunidad de prestar el servició donde el usuario lo necesita y cuando lo necesita.

Conocimiento y decisión. Un banco fintech debe poder aprovechar la información para conocer a sus clientes; esto significa incursionar en el mundo del *big data* y de la analítica. El cliente como parte de un segmento ya no es una opción; cada cliente por sí mismo es único y tiene un comportamiento particular. Entender y aprovechar esto es lo que realmente va a generar valor para la organización en todos los aspectos: desde sus productos tradicionales de captación y colocación hasta las campañas de mercadeo y la gestión de la comunicación. Esto no solo trae ahorros para la organización, también trae mayores ingresos; cosa que en gran medida se explica por la asertividad en la interacción con el cliente, la confianza que alcanza y el costo de oportunidad de los servicios ofrecidos por la entidad.

Requisitos de seguridad de un banco fintech. La seguridad es el aspecto más importante en cualquier entidad financiera, también en los bancos fintech. Por ese motivo, la seguridad se

vuelve el requisito más importante de todos, y debe estar incluido en todos los aspectos vistos anteriormente, para garantizar el servicio y la seguridad de los mismos. A continuación, se verán los factores claves que se deben tener en cuenta y que hacen parte de la capa de servicios de seguridad en el diagrama de vista general.

Administración de identificación y acceso. Esta es la primera línea de defensa en la organización, ayudando a prevenir el ingreso de personas no autorizadas. La administración de identificación y acceso es la base de la mayor parte de los controles de acceso y del seguimiento de las actividades de los usuarios. Para el caso de un modelo de nube, se podría optar por un servicio en la nube de identidad y acceso; hay dos en particular que se adaptan a esta necesidad: uno es el de Amazon AWS Identify and Access Management (IAM) y otro es el de Microsoft Azure Active Directory.

Servicio de evaluación de seguridad en la nube. Este es un servicio de valoración de seguridad y protección avanzada contra amenazas de aplicaciones montadas en esquemas de nube híbrida. Estos servicios funcionan como procesos automáticos que valoran automáticamente las aplicaciones en busca de vulnerabilidades y desviaciones con respecto a las practicas recomendadas. Operan produciendo una lista detalla de las vulnerabilidades encontradas, ordenadas según su criticidad. Para el modelo que se está trabajando, se recomienda trabajar con Amazon Inspector o Microsoft Azure Security Center.

Certificados SSL. Los certificados SSL son un mecanismo de protección de la comunicación en red, los cuales permiten establecer la identidad de sitios web a través del internet. Para un modelo de banca fintech, se recomienda adquirir esto como servicio; dicha medida permite dejar a un lado el proceso contante de carga y renovación de certificados. En este

escenario específico, se proponen los servicios de Amazon AWS Certificate Manager y el de Microsoft App Service Certificate.

Componente de seguridad basado en hardware. Este componente es esencial para poder implementar el servicio de autenticación de clientes, ya que les permite generar y usar sus propias claves de cifrado y se conecta bajo mecanismos de API estándar. Este módulo puede ser implementado dentro de una nube privada o incluso en una nube pública, debido a sus mecanismos de cifrado por hardware. Para este caso, se recomiendan los servicios de Amazon AWS CloudHSM, el de Microsoft Azure KeyVault o las cajas Atalla de HP.

Directorio de servicios. El directorio de servicios permite salvaguardar el acceso a datos y aplicaciones; ayuda a satisfacer la demanda de los clientes en un proceso de inicio de sección con múltiples opciones de validación. Para esta necesidad se podrían usar los servicios de Amazon AWS Directory Service, los de Microsoft Azure Active Directory o algunas de sus variantes B2C, Multi Factor o Domain, dependiendo de la necesidad. Para este caso, con alguna de las dos primeras es suficiente.

*Servidor de seguridad de aplicaciones **web.*** Esto básicamente es un firewall web, que ayuda a proteger las aplicaciones web de ataques que podrían afectar la disponibilidad de la aplicación. Teniendo en cuenta que el modelo de banca fintech se apalanca en la web, esto se vuelve relevante, por lo cual se recomienda implementar este servicio con Amazon AWS, WAF o con Microsoft Azure WAF.

Servidor de seguridad y cumplimiento. Este es un servicio de auditoria y conformidad que permite descargar informes bajo demanda según los acuerdos seleccionados. Estos pueden ser informes de control de organización de servicios, validación y eficacia de los mecanismos de

control, entre otros. Este sistema se puede implementar con Amazon AWS Artifact o con Microsoft Azure Security & Compliance.

Requisitos técnicos de un banco **Fintech.** Los requisitos técnicos para la implementación de un banco fintech son múltiples. En esta sección se agruparán los distintos aspectos que hay que revisar. En este aparte no se abordará ningún aspecto de seguridad, ya contemplados en el punto anterior; al igual que en esa sección, se recomienda usar las capacidades ofrecidas por Amazon o Microsoft, según el análisis de nubes realizado más atrás.

Cómputo. Las capacidades de computo de un modelo de banco fintech tienen una connotación distinta a la tradicional. En este caso, se habla de capacidades de computo en la nube que, en algunos casos, no hacen parte de las capacidades tradicionales. Las capacidades de un banco fintech se pueden desplegar en una nube pública o privada, según las necesidades del negocio, y son escalables según la necesidad. Para que esto funcione correctamente, se deben tener en cuentas las siguientes capacidades:

Servidores virtuales. Este es un servicio web que proporciona capacidad informática en la nube, de forma segura y según el tamaño requerido; también puede ser escalable. Además, está diseñado para facilitarles a los desarrolladores el uso de la informática en la nube a escala de la Web. Los mejores servidores virtuales en este momento son el de Amazon EC2 y los de Azure Virtual Machine o Virtual Machine Scale Sets.

Servicio de registro de contenedores. Este en un servicio que permite el registro de contenedores Docker. Se administra totalmente de una forma que les facilite a los desarrolladores las tareas de gestión, almacenamiento e implementación de imágenes de contenedores. Para esto

se recomienda usar las soluciones de Amazon EC2 Container Registry o Azure Container Registry.

Servicio de gestión de contenedores. Este debe ser un servicio de administración de contenedores de alto desempeño y escalabilidad, que sea compatible con *docker* y que, además, permita ejecutar aplicaciones distribuidas en un *cluster* administrado. Para estos se recomienda usar los servicios de Amazon EC2 Container Service y Azure Container Service o Azure Container Instances.

Plataforma de desarrollo de aplicaciones basada en microservicios. Estas plataformas permiten ejecutar código sin aprovisionar o administrar servidores. En estas solo se paga por el tiempo de cómputo consumido; cuando el código no se está ejecutando, no hay cobro. Las más recomendadas son AWS Lambda y Azure Service Fabric.

Servidores privados virtuales. Este es un servicio que proporciona un entorno totalmente asilado y dedicado para ejecutar de forma segura aplicaciones que son críticas para el negocio, es un buen esquema de montar una nube privada con un proveedor de nube garantizando aislamiento, acceso a redes seguro y un alto nivel de escalabilidad, esto se puede hacer con servicios como los de Amazon Lightsail y Azure App Service Environment.

Herramientas para procesos Batch. Estas herramientas permiten ejecutar de manera fácil y eficiente múltiples trabajos, en lotes que son requeridos por la organización, garantizando el uso eficiente de los recursos informáticos. Para este tipo de trabajo se pueden usar herramientas como AWS Batch y Azure Batch.

Capacidades de desarrollo y despliegue de aplicaciones en Java, .Net, PHP, Python entre otros. Estas herramientas permiten el desarrollo, despliegue y empaquetado de información. También ofrecen la ventaja de que, una vez implementada la aplicación, se incluye el servicio de aprovisionamiento, balance de carga y monitoreo. Para esto se pueden usar los servicios de AWS Elastic Beanstalk, Azure Web Apps o Azure Cloud Services.

Computación impulsada por eventos. Este servicio permite conectar aplicaciones, datos y dispositivos en cualquier lugar para así poder acceder a los datos y mantener sistemas dispares actualizados en tiempo real, para esto se recomienda usar AWS Lambda o Azure Functions Logic Apps.

Almacenamiento. La gestión de almacenamiento es de vital importancia en las organizaciones financieras, ya sean imágenes, documentos o cualquier otra información. Esta debe almacenarse según las regulaciones establecidas, por lo que se deben tener en cuenta los siguientes servicios de almacenamiento:

Almacenamiento de objetos. Este es un esquema de almacenamiento que permite almacenar cualquier tipo de archivos o de información: estructurada o no estructurada, en forma de videos, imágenes, audio, documentos u otros. Para esto se recomiendan los servicios como Amazon Simple Storage Service (S3) o Azure Blob Storage.

Almacenamiento en disco de la máquina virtual. Este servicio proporciona volúmenes de almacenamiento de bloques persistentes para utilizar en la nube. Cada bloque se replica automáticamente dentro de una zona de disponibilidad, para protegerlo frente a errores de componentes. Como esta alternativa ofrece alta disponibilidad y durabilidad, genera un desempeño constante y de baja latencia, el cual es necesario para ejecutar las cargas de trabajo de

las entidades financieras. Además, el almacenamiento en disco de la máquina virtual ofrece la capacidad de escalar el uso hacia arriba o hacia abajo, en cuestión de minutos. Los servicios que se recomiendan para esto son Amazon Elastic Block Storage (EBS) y Azure Page Blobs / Premium Storage.

Almacenamiento de archivos. Este es un servicio más estándar que se puede utilizar para almacenar archivos; se paga por la cantidad de almacenamiento mensual; se puede implementar con Amazon Elastic File System y Azure File Storage.

Almacenamiento en frio a largo plazo. Este servicio es el equivalente a llevar información a una cinta para ser usada en una posible restauración o requerimiento legal. A esto se le agrega la ventaja de que es un sistema más duradero, seguro y de bajo costo para archivar datos y realizar *backups*. Para esto se recomienda usar los servicios de Amazon Glacier o de Azure Cool Storage.

Bases de datos**.** A nivel de bases de datos, es importante tener presente cuál es el uso que se le va a dar a esta tecnología, para así poder definir de forma óptima qué tipo de base de datos implementar. En las entidades financieras, es normal encontrar bases de datos relacionales, no relacionales, en memoria y, por supuesto, bodegas de datos. Esta variedad se debe a la complejidad de las entidades financieras y a sus múltiples necesidades. En consecuencia, se revisaran los siguientes servicios de bases de datos:

Servicio de gestión de bases de datos relacionales. Estos son servicios de motores de bases de datos relacionales, que combinan la velocidad y fiabilidad de los motores de bases de datos tradicionales o de gama alta con la sencillez y rentabilidad de las bases de datos de código abierto. En este caso, los servicios son tan amplios que se recomienda escoger el motor de base

de datos más adecuado a la necesidad del cliente y no definir un único motor de base de datos para todo. Los siguientes son los más recomendados: Amazon Aurora, Amazon RDS, Azure SQL Database, SQL Server Stretch Database, Azure CosmosDB, Azure Database for MySQL, Azure Database for PostgresSQL, Cloud SQL, Cloud Spanner, dashDB for Transactions SQL, Database IBM DB2 on Cloud, entre otros.

Servicio de gestión de bases de datos no relacionales. Este es un servicio rápido y flexible para aquellas aplicaciones que requieren latencias constantes (en el rango de milisegundos). Esta característica hace de este servicio una alternativa ideal para algunas aplicaciones financieras de cara al cliente. En este caso, se recomienda optar por alguno de los siguientes servicios: Amazon DynamoDB, Amazon DynamoDB Accelerator (DAX), Azure CosmosDB, Azure Time Series Insights.

Almacenamiento de datos en memoria. Este tipo de servicios facilita la implementación de un almacén de datos en memoria, de manera mucho más rápida y sin depender de las bases de datos en disco. Este tipo de implementaciones es un poco más costoso, motivo por el que no se recomienda usarlas para todo. Es necesario encontrar el balance entre las bases de datos relacionales, no relacionales y las capacidades en memoria, para esto se recomienda usar Amazon ElastiCache o Azure RedisCache.

Redes y entrega de contenido. Respecto a las redes, también se pueden hacer implementaciones en la nube con secciones dedicadas, mediante la facilidad de uso de los protocolos IPV4 e IPV6 (según sea requerido). En la nube se puede trabajar todo lo relacionado con los siguientes servicios:

- Redes virtuales con Amazon VPC y Azure VNet.

- Gateway de red con Amazon VPN y Azure VPN Gateway.

- Red de entrega de contenidos con Amazon CloudFront, Azure CDN, Amazon Route 53, Azure DNS y Azure Traffic Manager

- Conectividad privada con AWS Direct Connect y Azure Express Route.

- Balanceadores de carga con Elastic Load Balancing y Azure Load Balancer.

Estas herramientas de red siempre se deben revisar, según el modelo de red definido que se vaya a implementar; asimismo puede cambiar según cada necesidad.

Herramientas de desarrollo. El propósito de esta tesis no es abordar cuales herramientas de desarrollo usar o no; sin embargo, si se quiere dejara la puerta abierta para ver el mundo de desarrollo con otros ojos y contemplar formas más eficientes de desarrollar. El mundo de la nube, los microservicios, los contenedores y las Apis generan un sinfín de posibilidades. Si estas posibilidades se saben explotar, les permitirán a las organizaciones evolucionar a la velocidad que se requiere y con unas mejores capacidades de reuso. Para esto existen herramientas especializadas, como las de AWS Code Star, AWS CodeCommit, AWS CodeBuild, Visual Studio Team Services, AWS SDK, Azure SDK Visual Studio, entre otros.

Recuperación de desastres. Cualquier entidad financiera requiere de un esquema eficiente de recuperación de desastres, que no requiera de gastos adicionales en infraestructuras en un segundo sitio físico. La nube admite numerosas arquitecturas de recuperación de desastres (DR) populares, más aun si la arquitectura que soporta el negocio ya está en la nube. En este caso, se facilita el montaje de un DR; se pueden utilizar los servicios de AWS Disaster Recovery, Azure Site Recovery o Azure Backup.

Big data y analítica. El mundo del *big data* y analítica se encuentra presente en todas aquellas organizaciones que manejan grandes volúmenes de información y que desean usarla para generar valor. Los bancos no son la excepción y, debido a los volúmenes y el tipo de información que manejan, se vuelve muy importante la gestión de la información. Por eso, un modelo de banca fintech debe tener en cuenta los siguientes conceptos y herramientas para gestionar correctamente su información.

- Las *query* de *big* data: Amazon Athena y Azure Data Lake Analytics.

- Los *clusters* de *big data*: Amazon EMR, Azure HDInsight.

- Servicio de *streaming*: Amazon Kinesis o Azure Event Hub.

Inteligencia artificial. Los temas relacionados con la inteligencia artificial están en pleno apogeo, debido en gran medida a la evolución tecnológica que se ha presentado en los últimos años y a las bondades de la IA en automatización de procesos con capacidades cognitivas. La inteligencia artificial no es la automatización tradicional; es una automatización inteligente donde los modelos definidos aprenden y evolucionan de forma constante, según los resultados obtenidos previamente. Esto hace que, en el sector financiero tradicional o en un modelo de banca Fintech, se deba incursionar en los temas de IA. Para alcanzar ese objetivo, es recomendable usar capacidades como las de IBM Watson, Amazon Lex o Microsoft Luis, que en este momento son los más especializados en el mercado. En caso de no recurrir a estas empresas, desarrollar estas capacidades es muy costoso para cualquier compañía.

Otros servicios. Cómo se ha comprobado al exponer los requisitos técnicos requeridos para un banco fintech, hay muchos servicios especializados. Hablar de todos no es posible; solo

se abordaron los servicios más importantes. En este capítulo se va a hacer mención de otras herramientas, sin entrar a describirlas en detalle, con el fin de que se tenga en cuenta que puede haber servicios adicionales según la necesidad: servicios para dispositivos móviles, servicios de aplicación, servicios de desarrollo y pruebas, internet de las cosas, entre otros. Todos estos servicios se ofrecen dentro de las capacidades de Amazon y Microsoft, que fueron las dos nubes mejor calificadas durante el proceso de evaluación de nube realizado previamente.

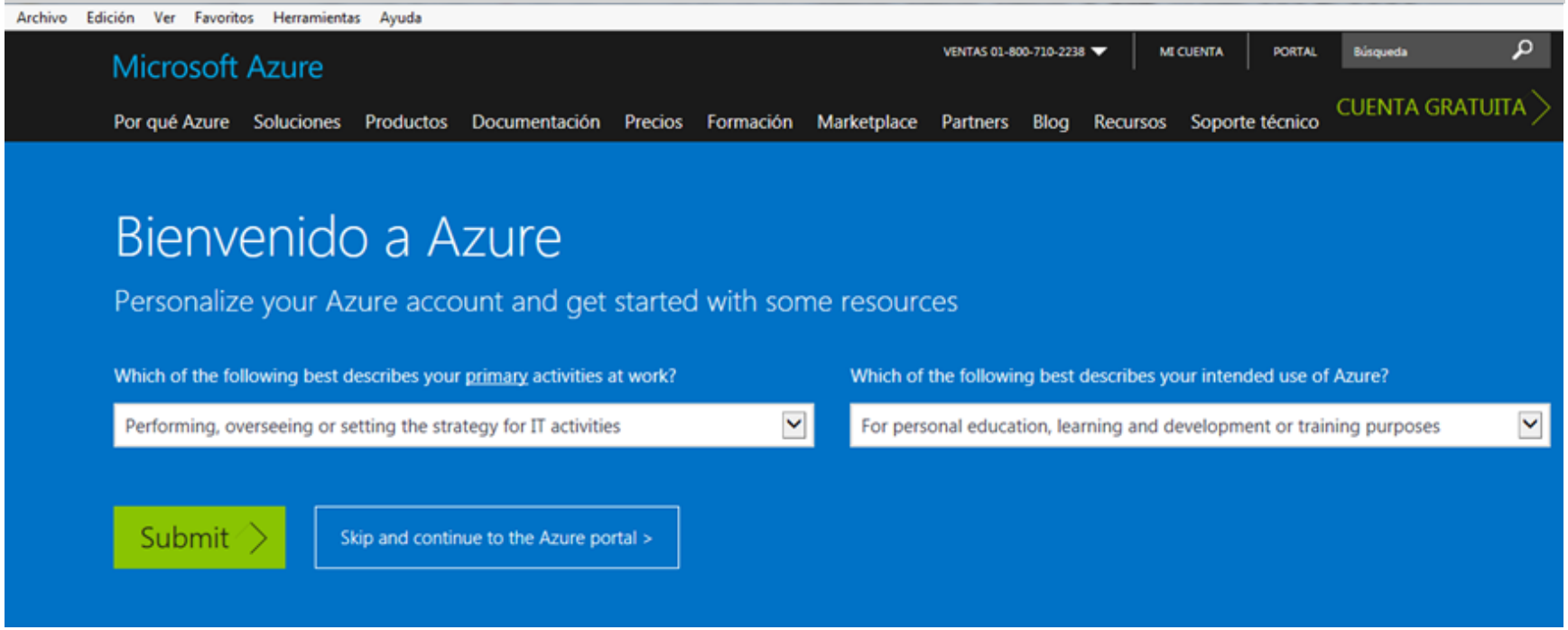
Durante la evaluación de estos requisitos funcionales, de seguridad y técnicos, se pudo confirmar que los proveedores de nube seleccionados son los más maduros para este tipo de implementaciones.

Cuarto objetivo: implementar una prueba de concepto de la nube

Este objetivo consiste en probar una de las nubes evaluadas, para lo cual se optó por evaluar la nube de Azure. Esta, al igual que la de AWS, ofrece capacidades muy robustas y completas. La decisión de usar una o la otra en este caso no es relevante; ambas cumplen lo que se requiere para la prueba. Se escogió la nube de Azure más por un tema de facilidad.

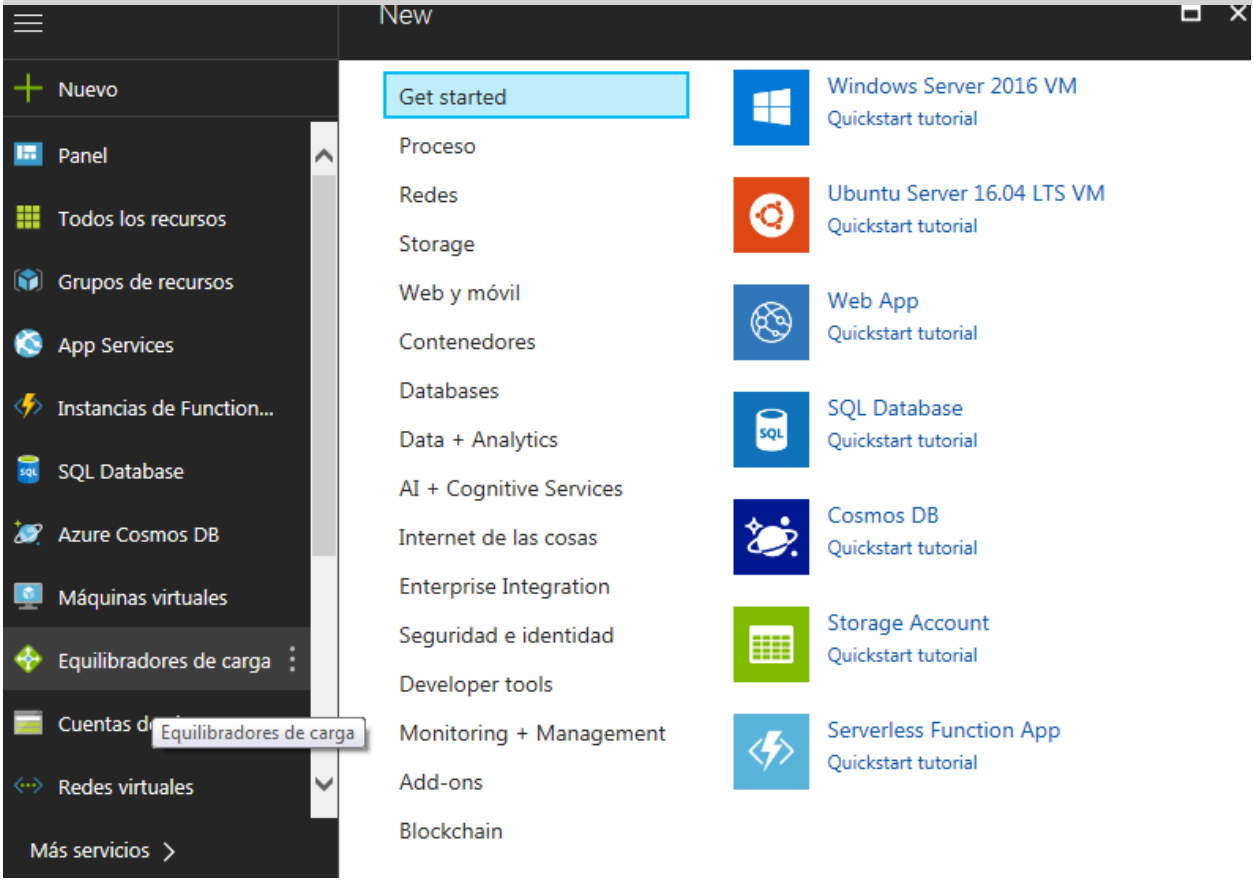
Lo primero que se realizó para cumplir este objetivo fue el proceso de inscripción, cuyo costo fue de apenas un dólar estadounidense. En esta etapa se requirieron los datos de cuenta de correo, una tarjeta de crédito y un numero de celular. Una vez ingresados los datos, apareció la pantalla que se puede ver en la **FIGURA 31**, a continuación.

FIGURA 31: PROCESO DE REGISTRO E INGRESO A MICROSOFT AZURE



Una vez realizado el proceso de registro e ingreso a Microsoft Azure, se despliega el panel de control —incluido en la **FIGURA 32**—, donde se pueden crear todos los componentes que se requieran a nivel de máquinas virtuales, bases de datos, aplicaciones, instancias y servicios de seguridad, desarrollo o integración, entre otros.

FIGURA 32: PANEL DE CONTROL DE MICROSOFT AZURE



Para la realización de la prueba se realizaron varias actividades, desde la creación de una máquina virtual, creación de aplicación y configuración de usuarios en el directorio activo.

Configuración de máquina virtual**.** En este caso, se configuró una máquina virtual Windows Server, versión 1709, para uso de contenedores. Este sistema está diseñado para correr aplicaciones sobre una infraestructura robusta y acorde con las capacidades de contenerización, según la necesidad de este proyecto. La máquina se creó con las siguientes características, como indica más adelante la **FIGURA 33**.

- Nombre de la maquina: Máquina Tesis

- Tipo de disco de máquina virtual: SSD

- Nombre de usuario: Juan

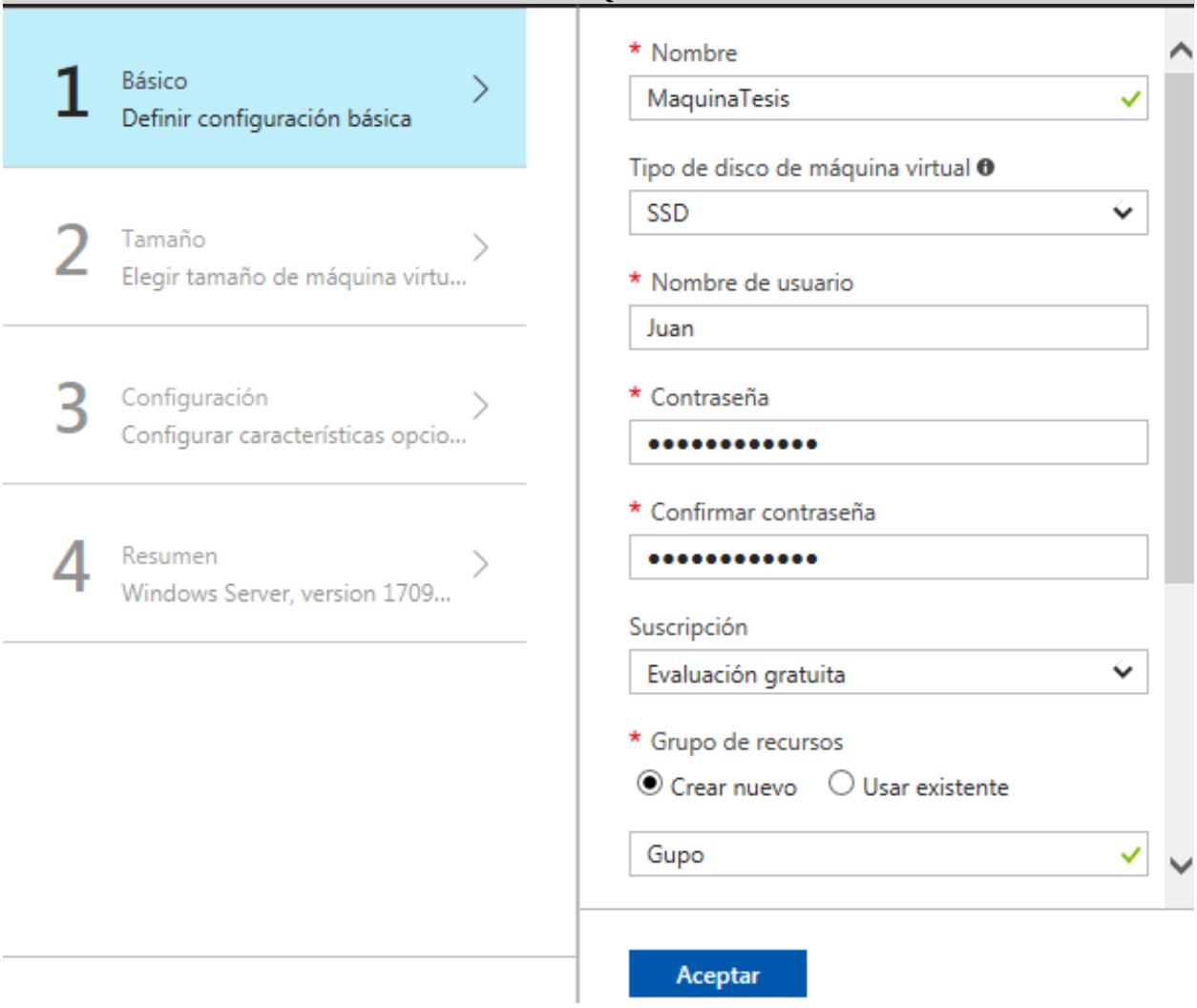
- Contraseña: Juan87910000

- Suscripción: evaluación gratuita

- Grupo de recursos: grupo

- Ubicación: centro-Sur de EE.UU

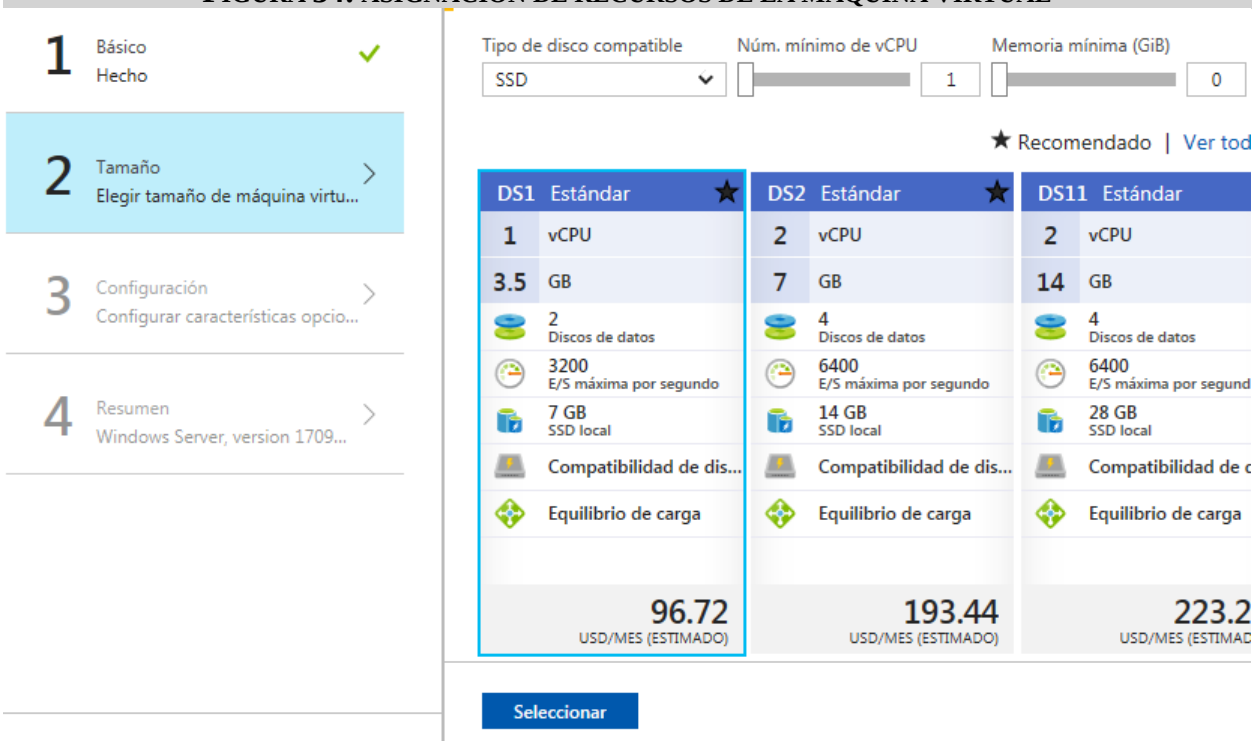
FIGURA 33: MÁQUINA VIRTUAL



Una vez creada la configuración básica, se configuró el tamaño de la máquina virtual, la cual tiene un costo de 96 dólares mensuales, como aparece en la **FIGURA 34**. Esto es acorde con

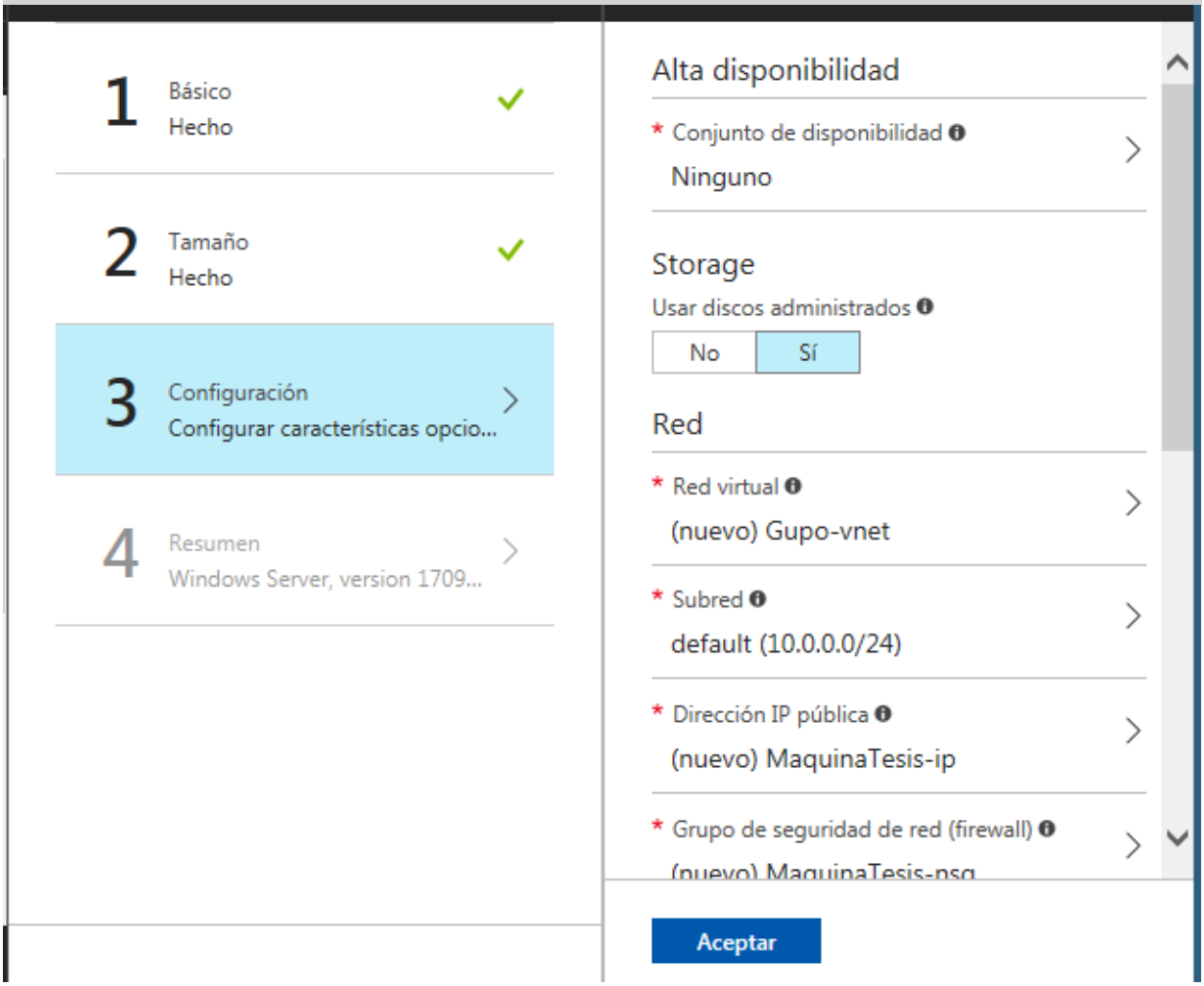
las características de la maquina seleccionada, que, en este caso, fue la más económica, ya que los recursos para las pruebas son de 290 dólares.

FIGURA 34: ASIGNACIÓN DE RECURSOS DE LA MÁQUINA VIRTUAL



Con los recursos asignados se realizaron las configuraciones de red, de alta disponibilidad y de almacenamiento, junto con otras configuraciones adicionales. A continuación, se incluyen los detalles en la **FIGURA 35**.

FIGURA 35: CONFIGURACIONES ADICIONALES



Una vez creada la máquina virtual, con todas sus configuraciones y asignación de recursos, se revisó un resumen de todas las configuraciones, antes de proceder con la implementación. Esta información se incluye en las **FIGURAS 36** y **37**, que contienen el resumen de la configuración de las máquinas virtuales y los recursos asignados.

FIGURA 36: RESUMEN DE LA CONFIGURACIÓN DE LA MÁQUINA VIRTUAL 1

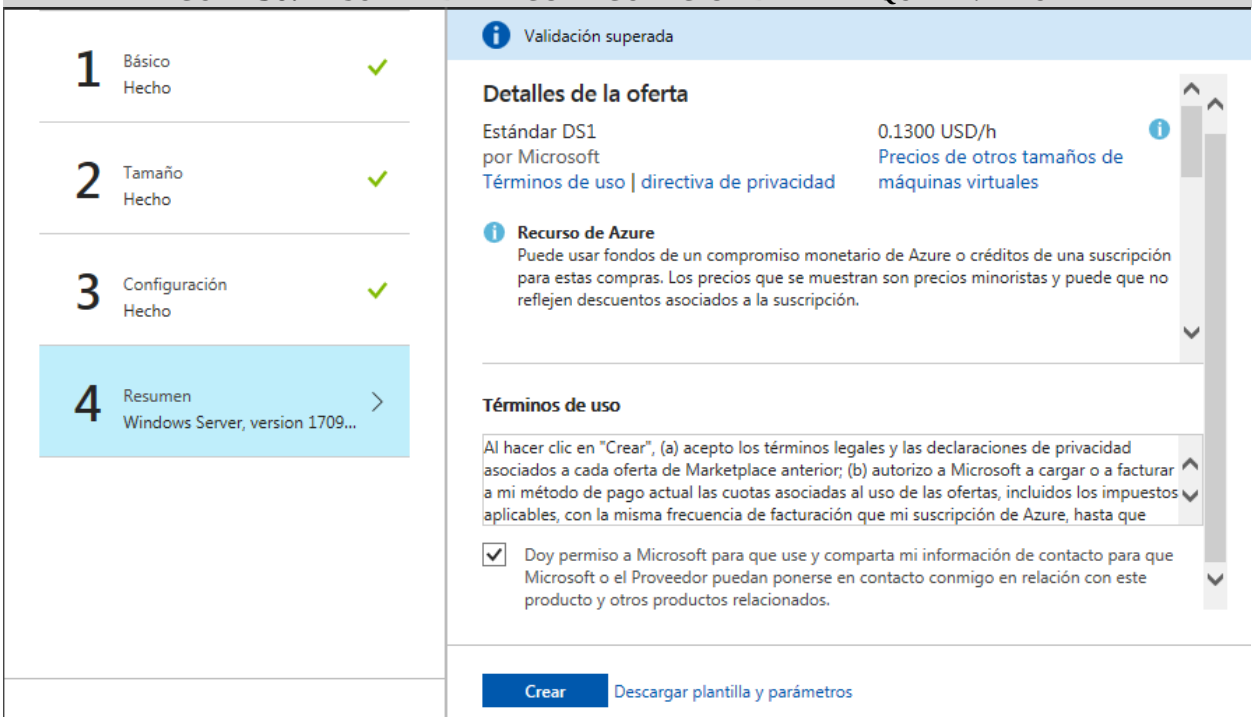
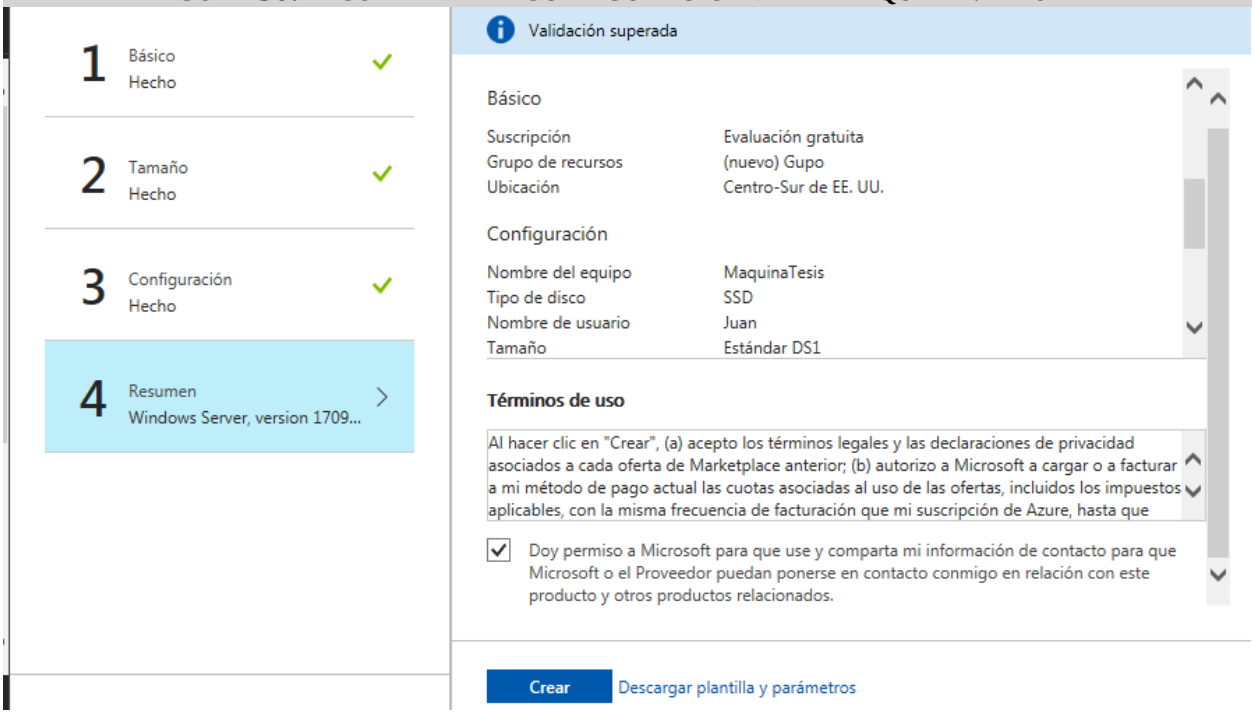


FIGURA 36: RESUMEN DE LA CONFIGURACIÓN DE LA MÁQUINA VIRTUAL 2



Con toda la información en orden, se procedió a la implementación de la máquina virtual. Este proceso puede demorarse algunos minutos, mientras es realizado de forma automática. La totalidad del proceso no toma más de 5 minutos para tener un servidor Windows Server. A continuación, en la **FIGURA 38**, se puede ver la imagen del proceso de implementación de la máquina virtual.

FIGURA 38: PROCESO DE IMPLEMENTACIÓN DE LA MÁQUINA VIRTUAL

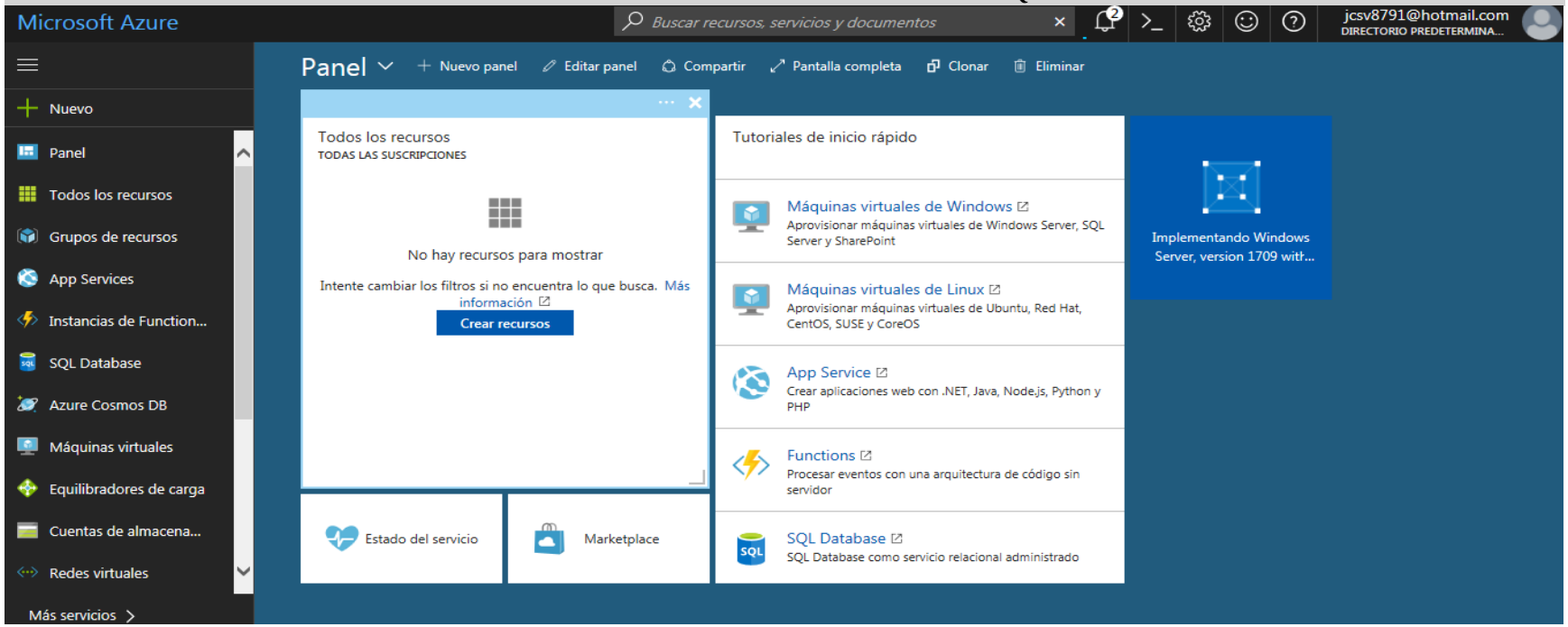
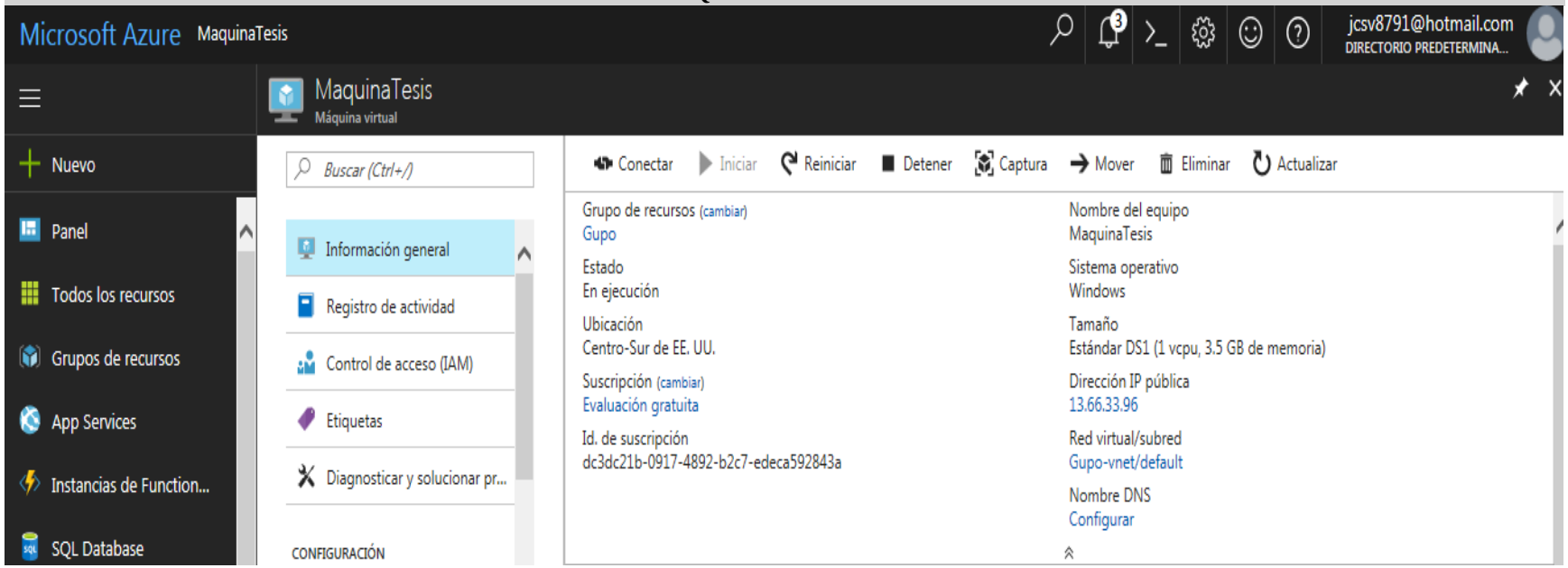
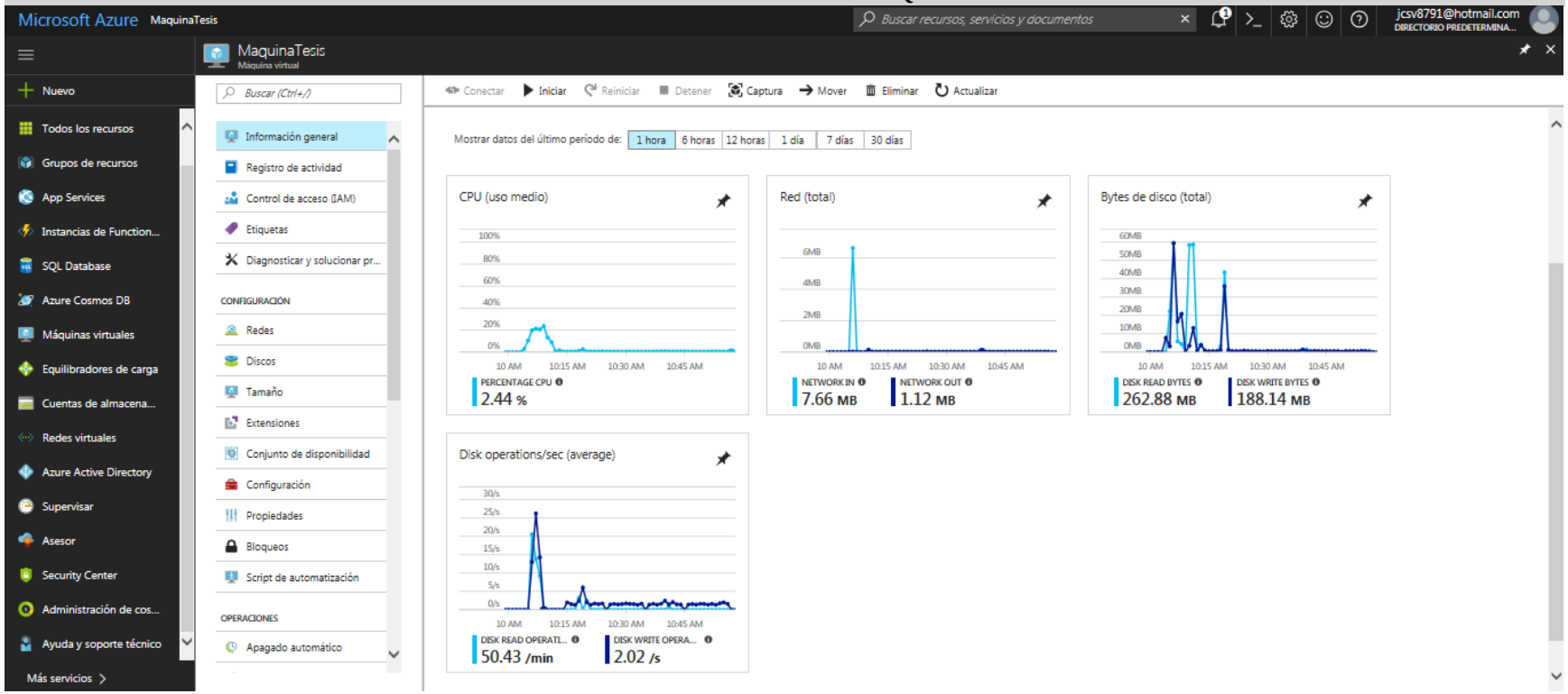


FIGURA 39: MÁQUINA VIRTUAL EN EJECUCIÓN



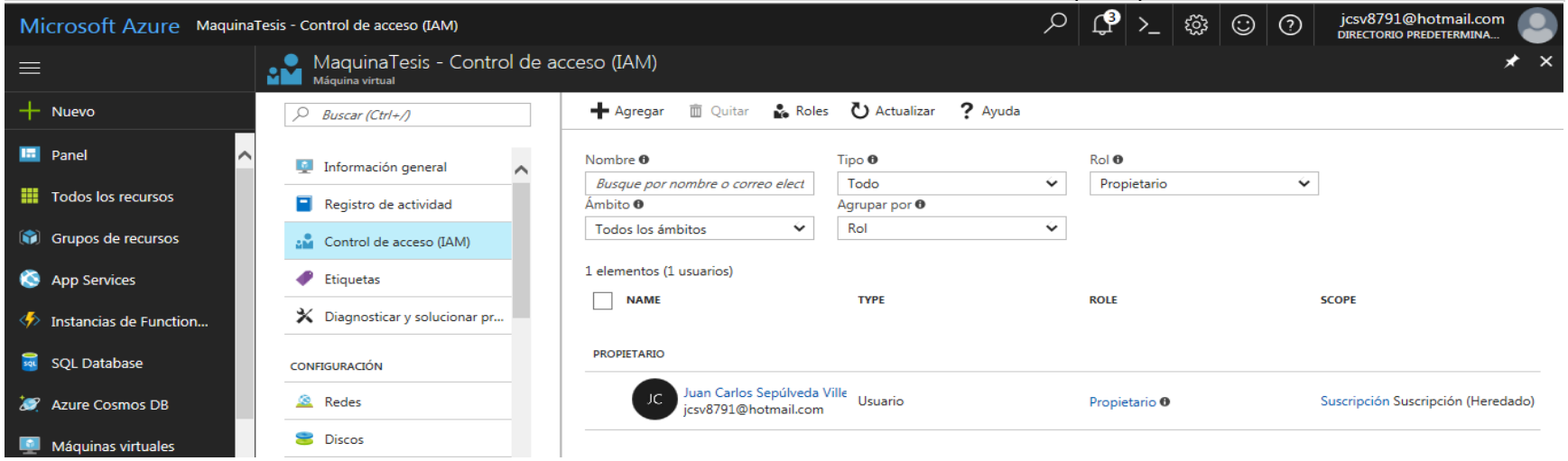
Una vez la máquina virtual fue implementada y se encontró en proceso de ejecución, se habilitaron los procesos de monitoreo y estado de la máquina, como puede comprobarse en las **FIGURAS 39** y **40**.

FIGURA 40: MONITOREO DE LA MÁQUINA VIRTUAL



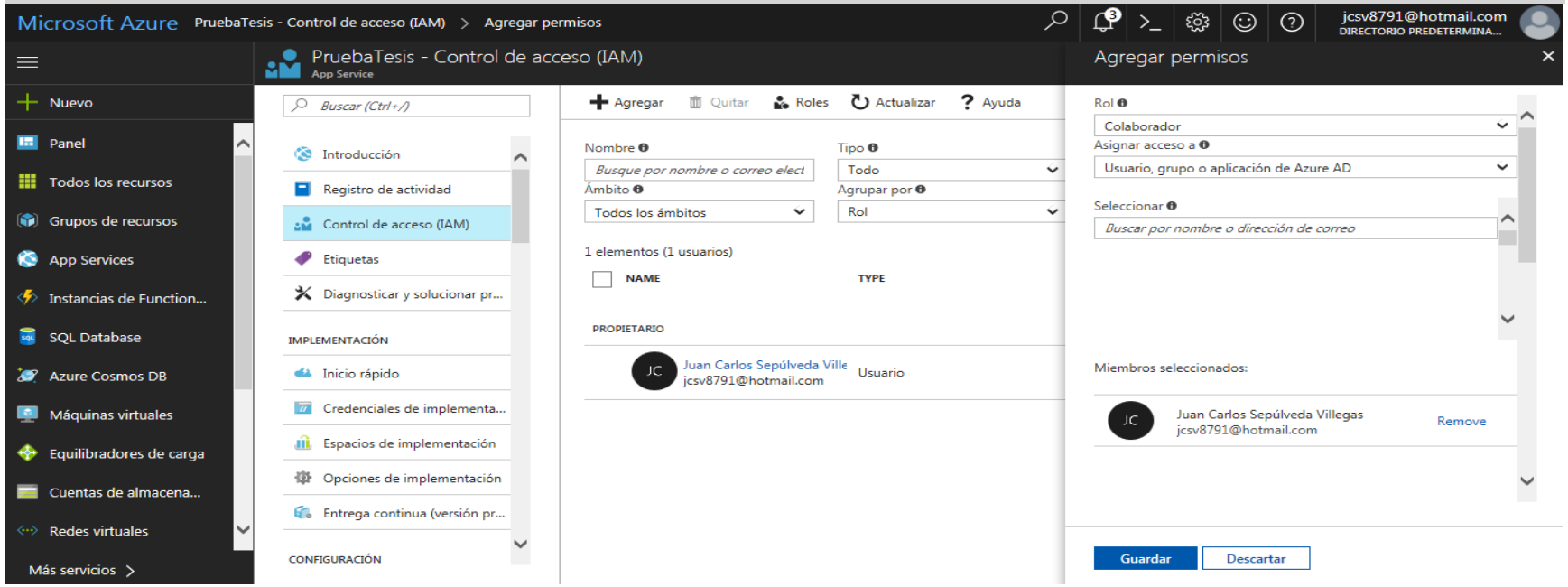
Configuración de seguridad**.** Una de las principales ventajas de la nube es su facilidad de despliegue, debido a que permite realizar despliegues de infraestructura e implementar soluciones de forma muy rápida. Esto pudo comprobarse en el despliegue del Windows Server que se instaló en el paso anterior; sin embargo, esta facilidad se puede replicar en todos los servicios que se ofrecen en la nube. A continuación, se realizará la configuración de control de acceso, usando las capacidades de IAM de la nube de Azure. Este proceso se explica en la **FIGURA 41**, presentada a continuación.

FIGURA 41: CONFIGURACIÓN DE CONTROL DE ACCESO (IAM)



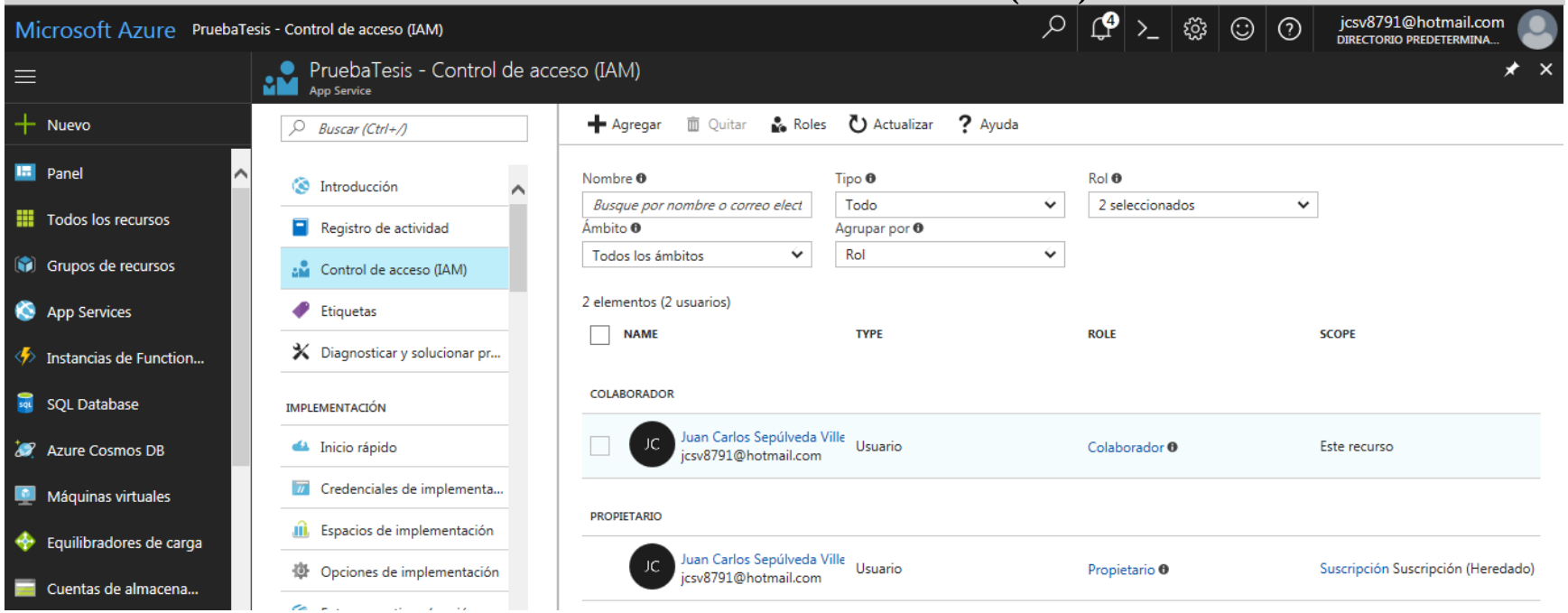
La gráfica anterior muestra que se inicia con el usuario propietario, con permisos completos sobre el servidor y todo su entorno. Además, crear otro usuario es relativamente sencillo, y puede ser controlado por quien tiene acceso a la infraestructura, de forma muy similar a la de un modelo *on premise*. De igual forma, se realizó la asignación de permisos a las aplicaciones. La **FIGURA 42** ofrece detalles sobre cómo es la creación del usuario propietario.

FIGURA 42: CREACIÓN DE NUEVO USUARIO PROPIETARIO



El usuario se crea con datos muy similares a los del usuario propietario. La diferencia radica en que se creó como un usuario colaborador y en que solo tiene permisos para atender esa máquina virtual en particular, como puede comprobarse en la **FIGURA 43** a continuación.

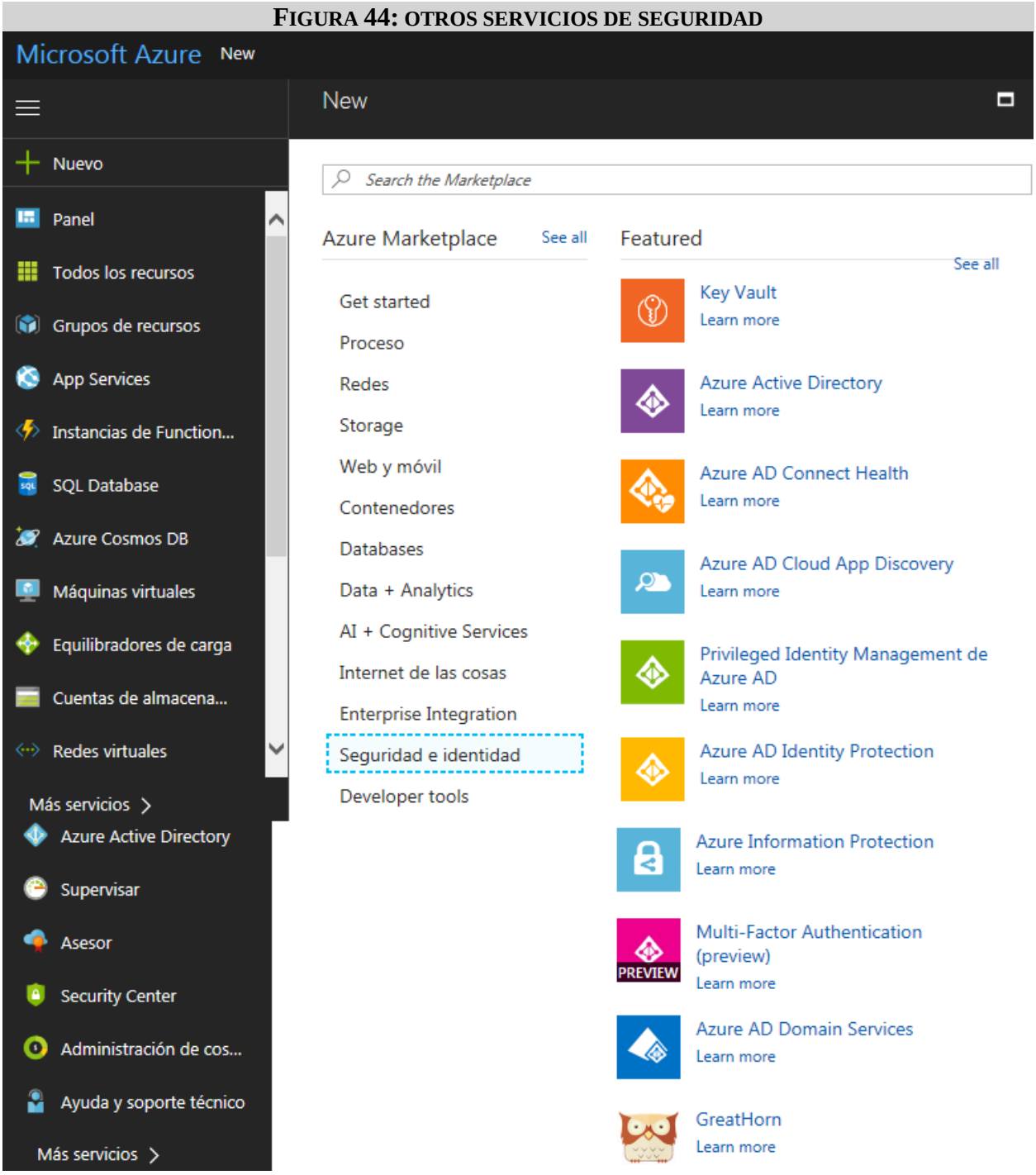
FIGURA 43: CREACIÓN DE NUEVO USUARIO EN (IAM) 2



Configuración de otros servicios de seguridad

Una vez creada una aplicación, se pueden crear recursos adicionales: por ejemplo, los recursos de seguridad e identidad que recoge la **FIGURA 44**.

FIGURA 44: OTROS SERVICIOS DE SEGURIDAD



Dentro de los servicios de seguridad que aparecen en la gráfica anterior cabe destacar los de bóveda de llaves, directorio activo, privilegios y administración de identidad, protección de identidad, protección de información, múltiple factor de autenticación, entre otros. Para darle continuidad a la prueba, se procedió a configurar el servicio de directorio activo con los siguientes datos de prueba:

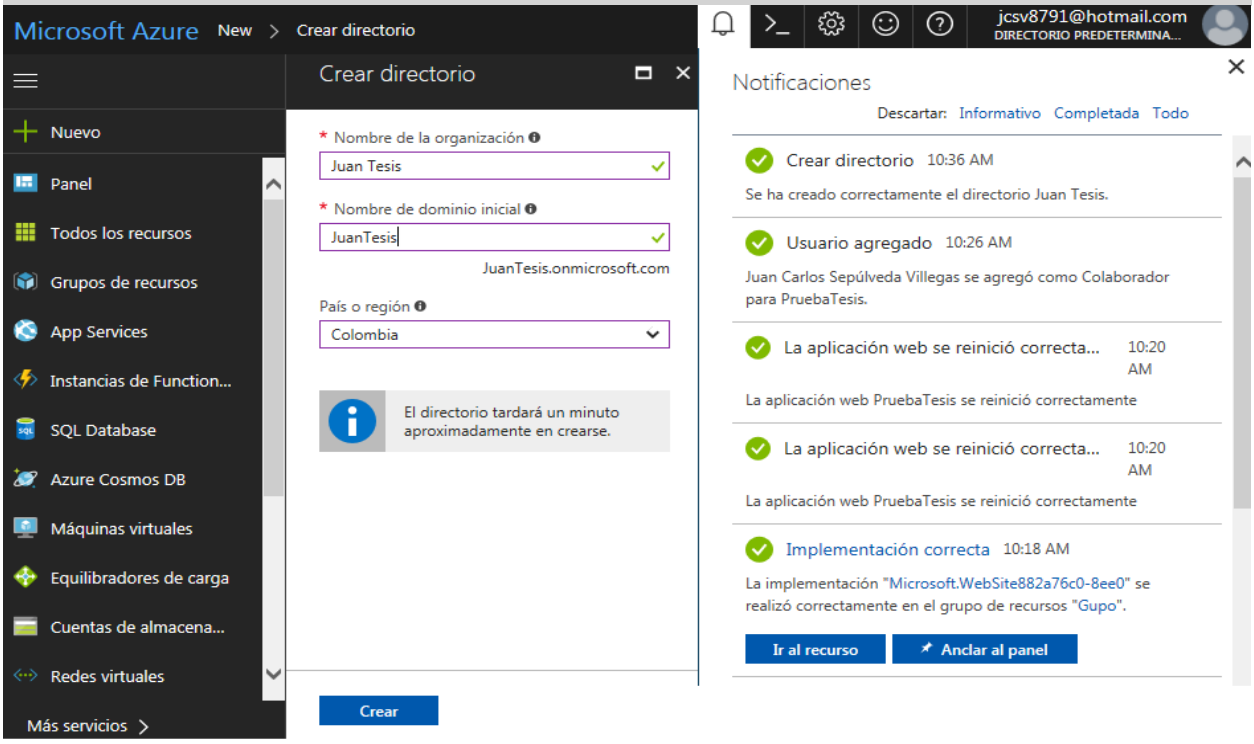
Nombre de la organización: Juan Tesis

Nombre de dominio inicial: JuanTesis.onmicrosoft.com "de forma predeterminada, se incluye el dominio básico onmicrosoft.com con el directorio; sin embargo, más adelante se puede personalizar con un dominio propio, si se tiene".

País: Colombia

La **FIGURA 45** resume a continuación cómo se crea un directorio.

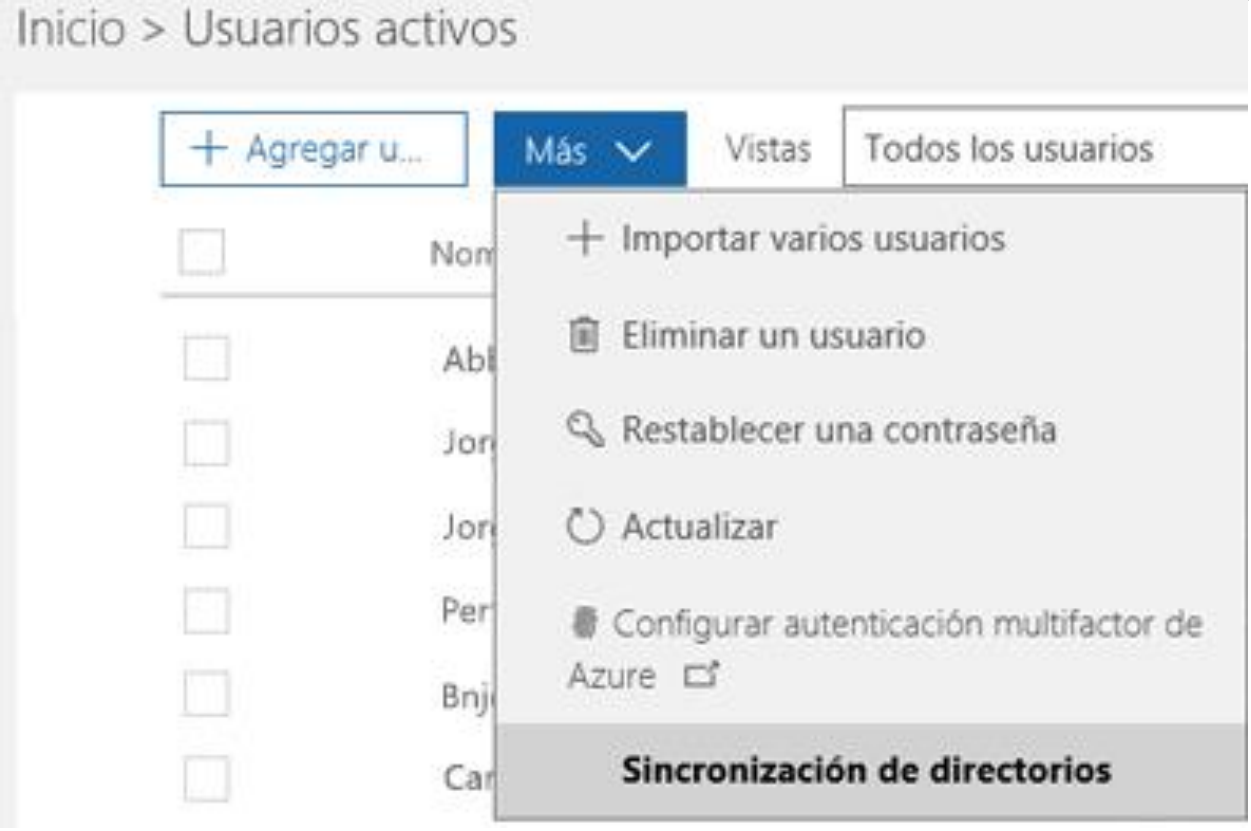
FIGURA 45: CREACIÓN DE DIRECTORIO



Una vez realizada la configuración del directorio activo, hay que iniciar el proceso de sincronización de directorios. En este ejercicio se parte de la premisa de un modelo de nube hibrido, por eso es indispensable realizar la sincronización del directorio activo. Con este fin, se instaló Azure Active Directory Connect, en uno de los servidores previamente configurados. La configuración de directorios se realizó siguiendo el manual de configuración de la cuenta de soporte de Microsoft. Es importante seguir paso a paso la configuración; de lo contrario, se podrían presentar inconvenientes.

1. Se debe realizar el inicio de sesión en el Centro de administración de Office 365 y elegir *Usuarios* **>** *Usuarios activos* en la navegación de la izquierda. Luego, en la página *Usuarios activos* del Centro de administración de Office 365, hay que elegir *Más* > *Sincronización de directorios***.**

Figura 46: creación de directorios



La sincronización de directorios no es obligatoria, esto dependerá del tamaño de la organización. No obstante, para una entidad financiera este es un requisito indispensable, debido principalmente al tamaño de la organización y a su razón social. Una vez se realiza la comprobación del directorio, se debe ejecutar un análisis para revisar la sincronización, esto incluye la configuración de dominios. Para esto, es necesario instalar Azure Active Directory Connect, el cual permite manejar dos configuraciones: *Sincronización de directorios*, con la sincronización de contraseñas *hash*, o Azure AD Connect, con la configuración de *express* que es usada para varios bosques, autenticación de paso, identidad federada y opciones SSO.

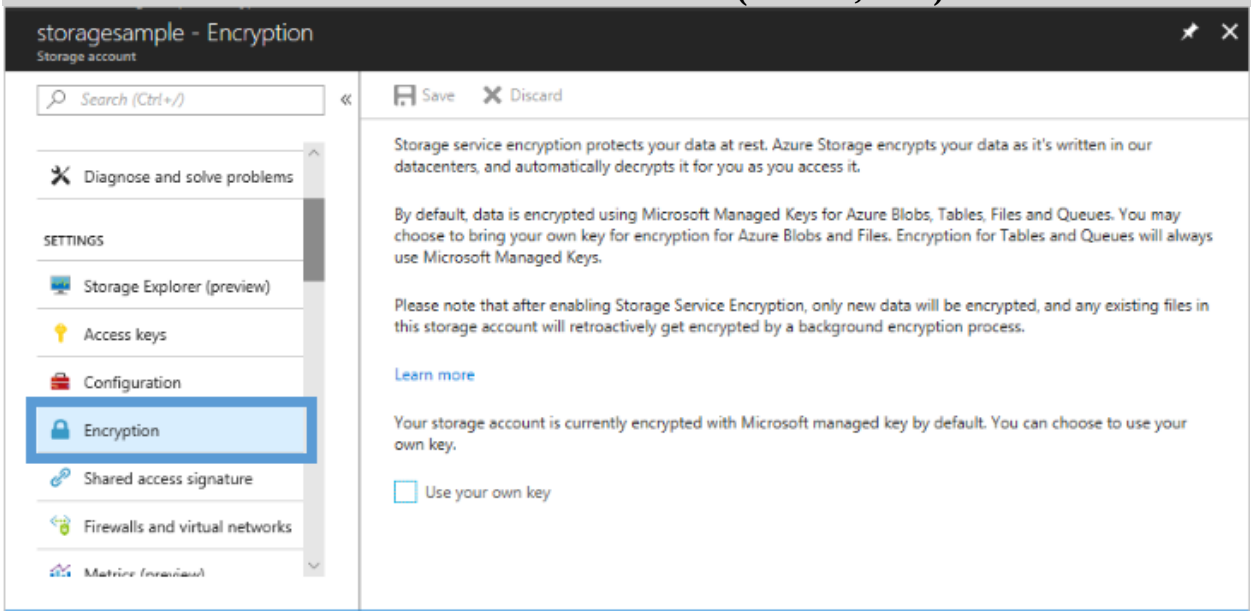
*Cifrado en reposo en **Azure.*** El cifrado en reposo es otro servicio de seguridad indispensable en una arquitectura de nube híbrida. Este servicio es un requisito de seguridad habitual, ya que las organizaciones pueden lograr el cifrado en reposo sin el costo de implementación y administración, sin el riesgo de una solución de administración de claves personalizadas[2]. Las organizaciones tienen la opción de permitirle a Azure administrar completamente el cifrado en reposo[3] Los diseños del cifrado en reposo de Azure utilizan cifrado asimétrico para cifrar o descifrar rápidamente grandes cantidades de datos, según un modelo conceptual sencillo. Para esta prueba de concepto, se utilizará el esquema de cifrado en reposo para SaaS de Azure, más conocido como Azure Storage Services Encryption para datos en reposo. Este sistema ayuda a proteger los datos en reposo en los esquemas de almacenamiento de Azure —como Azure Blob Storage, Azure Files o Azure Queue Storage, entre otros— y los descifra antes de recuperarlos[4].

2. “
3. “
4. “

El control del cifrado, el cifrado en reposo, el descifrado y la administración de claves en cifrado del servicio Storage es transparente para los usuarios[5]. Todos los datos escritos en la plataforma de almacenamiento de Azure se cifran mediante cifrado AES de 256 bits, uno de los cifrados de bloques más fuertes disponibles; el cifrado del servicio Storage está habilitado para todas las cuentas de almacenamiento nuevas y existentes y no se puede deshabilitar[6].

Dado que los datos están protegidos de forma predeterminada, no es necesario modificar el código o las aplicaciones para aprovechar el Cifrado del servicio Storage. Esto último es uno de los motivos por los que no se pudo contemplar la configuración del cifrado en reposo en la herramienta; sin embargo, a continuación, se verá cómo se visualiza la configuración del cifrado en Azure.

FIGURA 47: CIFRADO **EN REPOSO (CONPES, 2016)**



Centro de seguridad de la nube de ***Azure.*** Además de los servicios que se han revisado, también es posible acceder al centro de seguridad que ofrece la nube Azure como parte de su

5. “”.
6. “”.

solución. Esto se ve con más claridad en las **FIGURAS 44** y **45**, a continuación; con estas capacidades, es posible ver cómo se están comportando las capacidades de computo, el almacenamiento en redes y las aplicaciones instaladas en la nube.

FIGURA 48: CENTRO DE SEGURIDAD DE AZURE 1

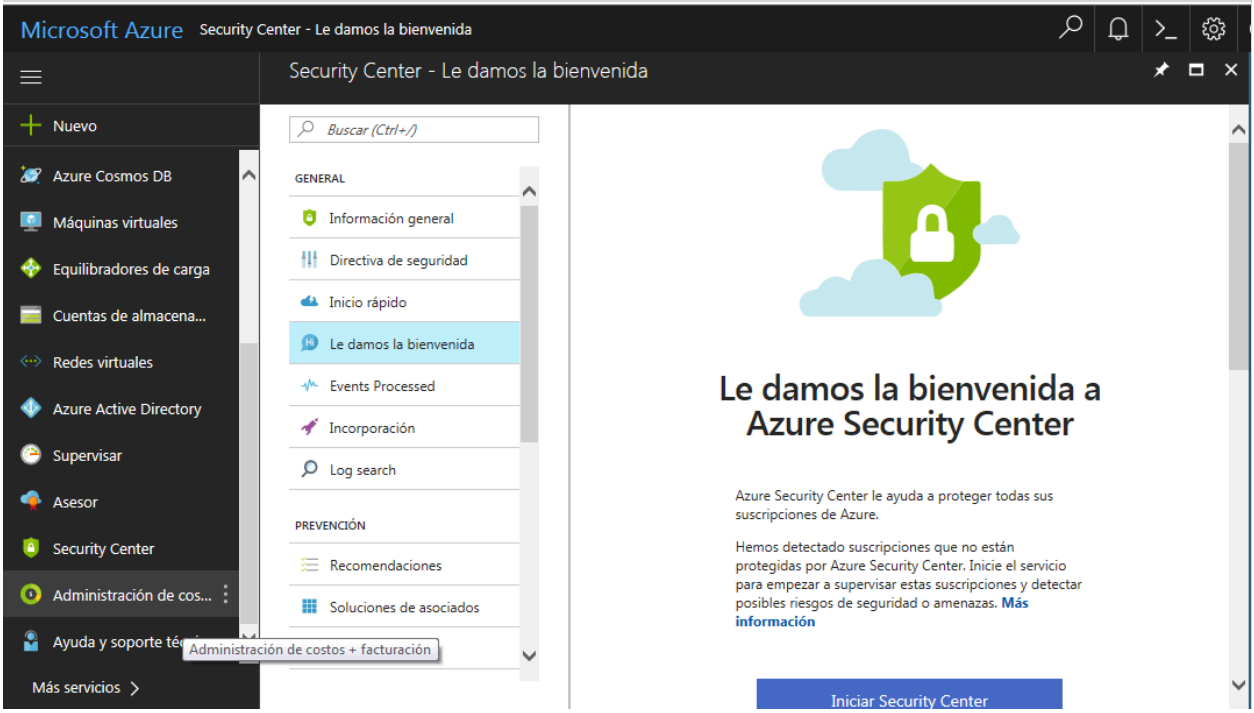
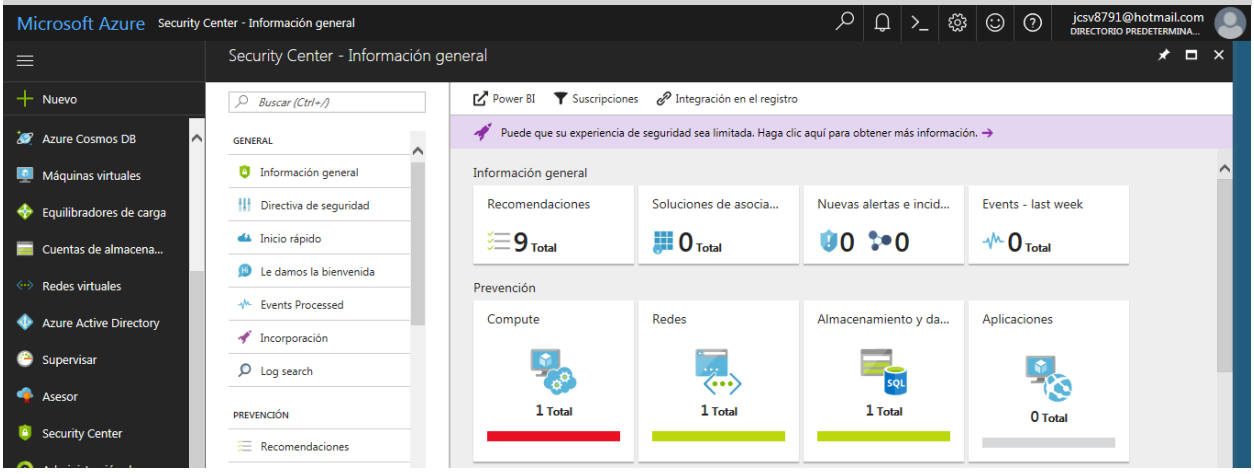


FIGURA 49: CENTRO DE SEGURIDAD DE AZURE 2

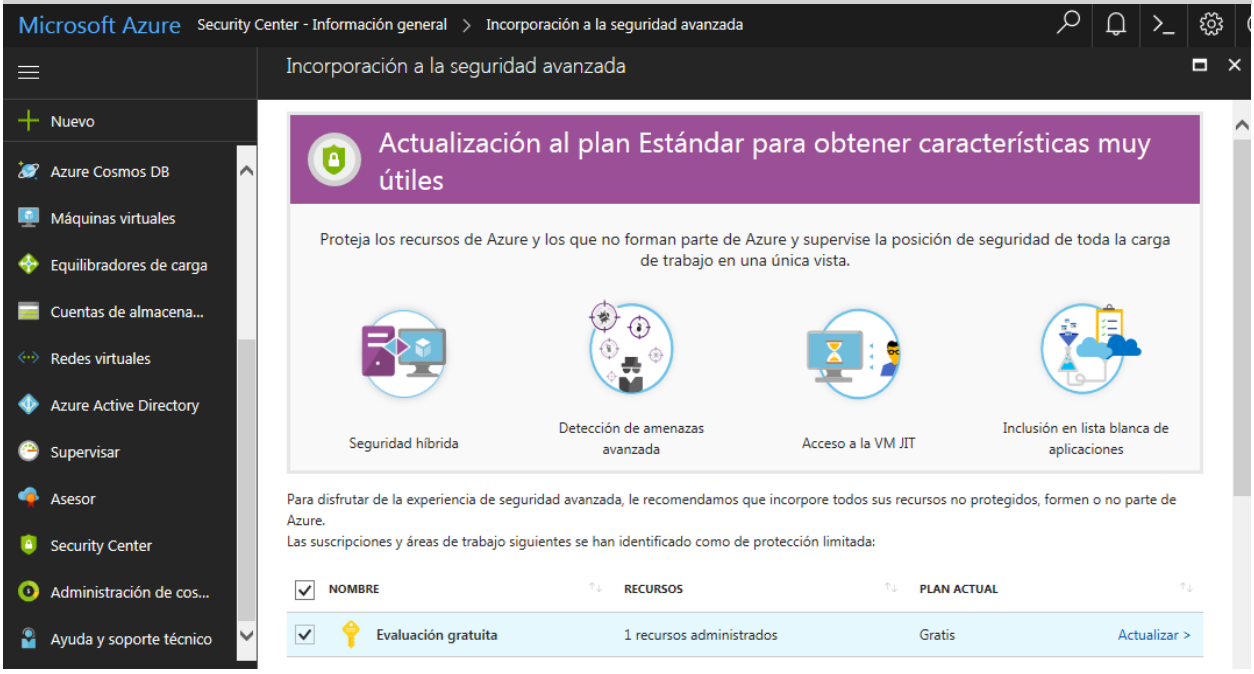


Estas capacidades mencionadas y esbozadas en las gráficas anteriores son las capacidades básicas; por otra parte, se recomienda realizar una actualización del plan estándar, para adquirir

otras capacidades adicionales: seguridad híbrida, detección de amenazas avanzadas, inclusión de listas blancas de las aplicaciones, entre otras. Como como puede comprobarse en la **FIGURA 46**, esto permite tener un mayor nivel de seguridad en las aplicaciones y en todo el ecosistema en general.

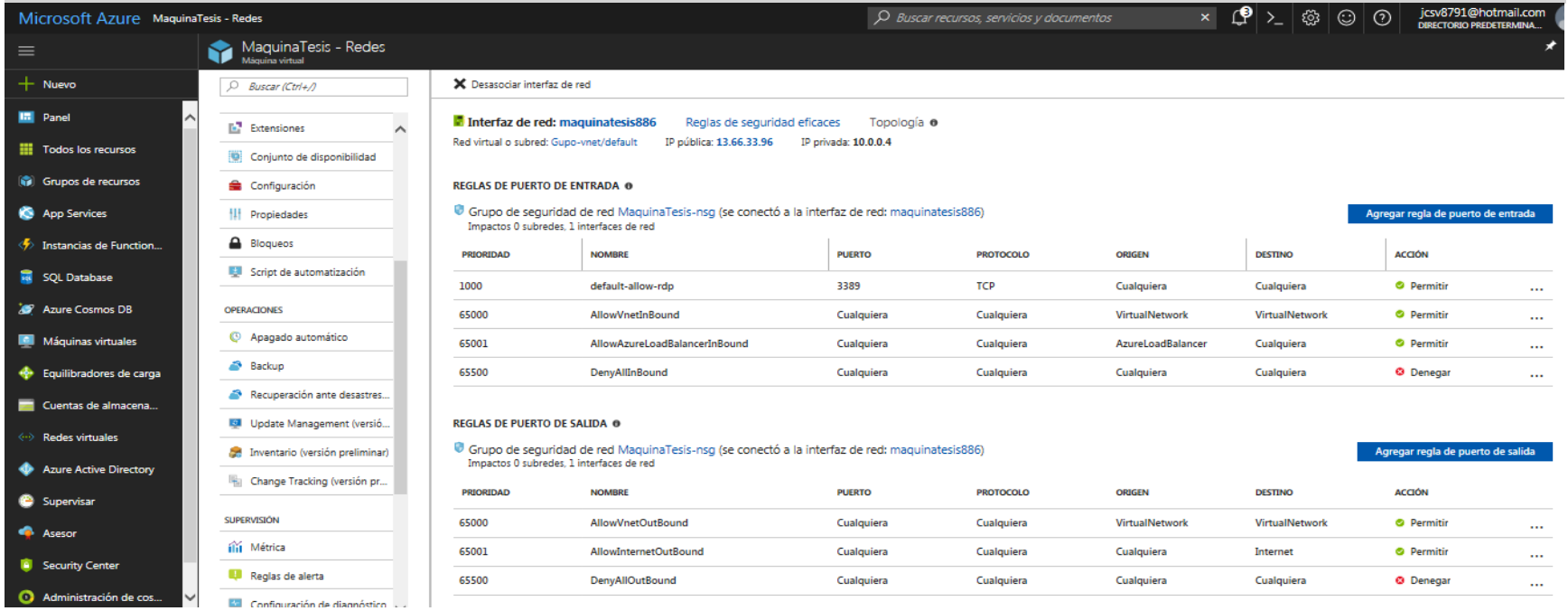
Cualquiera de los servicios mencionados solo se adquiere una vez; el resto depende la infraestructura de la nube que se esté utilizando y de las capacidades requeridas. Lo anterior implica que, si un servicio de monitoreo se usa para una sola aplicación, puede ser un poco costoso; pero, cuando se tienen múltiples aplicaciones, se genera una economía de escala.

FIGURA 50: ACTUALIZACIÓN DEL PLAN ESTÁNDAR DE SEGURIDAD



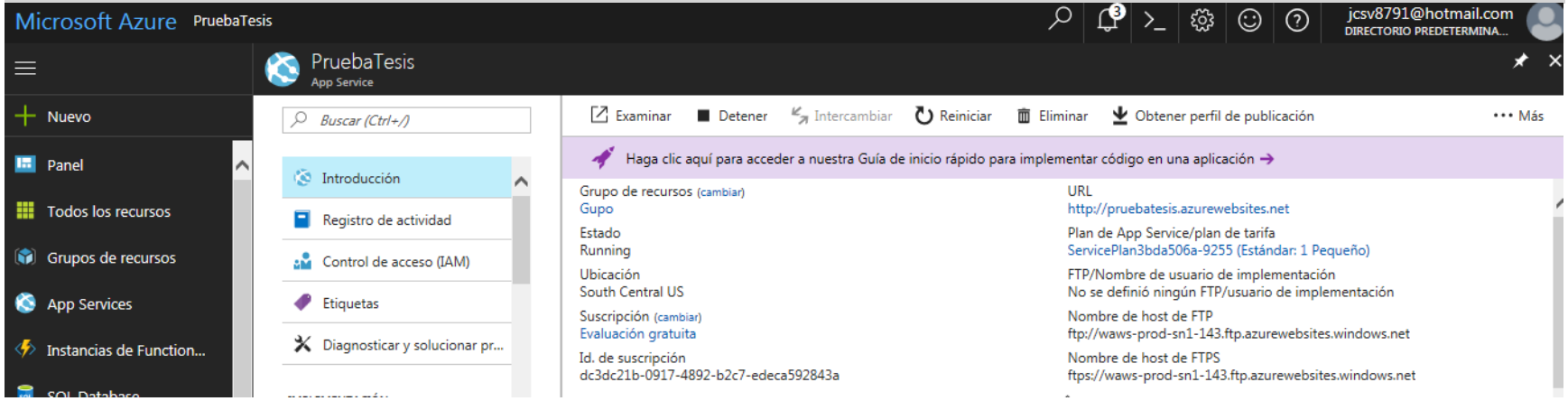
Configuración de reglas de puertos de entrada y de salida**.** A continuación, en la **FIGURA 47**, se mostrará cómo se pueden configurar los puertos de entrada y de salida. La configuración es sencilla, y se deja en modo estándar para efectos de la prueba. Aun así, en el momento de una implementación, se pueden seleccionar los puertos que se desean utilizar y aumentar la seguridad.

FIGURA 51: REGLAS DE PUERTO DE ENTRADA Y SALIDA.



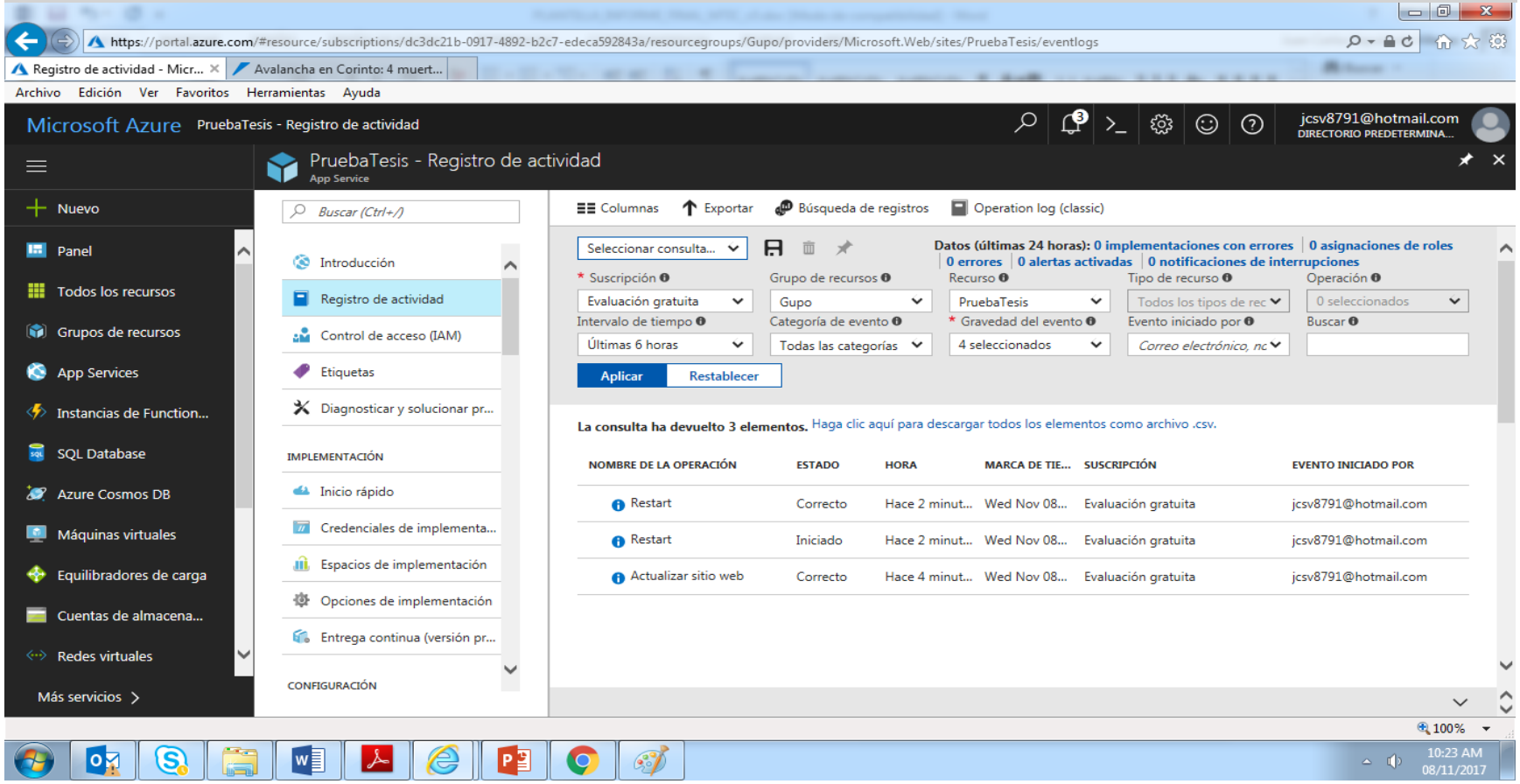
Creación de aplicaciones**.** Cuando se requiere crear una aplicación, el proceso es relativamente sencillo: se pueden usar las interfaces propias de la nube y agregar aplicaciones o paquetes ya existentes; lo único que se debe hacer es crear la aplicación dentro de la configuración de la nube. En otro caso, si se va a desarrollar, se trabaja con los servicios que ofrece la nube o con las herramientas propietarias que ya se tengan; luego, se importa para hacerla parte del servicio y realizar todo el despliegue y ejecución en la nube. Dicho proceso se ve con más claridad en la **FIGURA 52**.

FIGURA 52: CREACIÓN DE APLICACIÓN



Como se puede ver en la gráfica anterior, se procedió a crear la aplicación; posteriormente, se ejecutó y comprobó su comportamiento, según lo muestra la **FIGURA 53**.

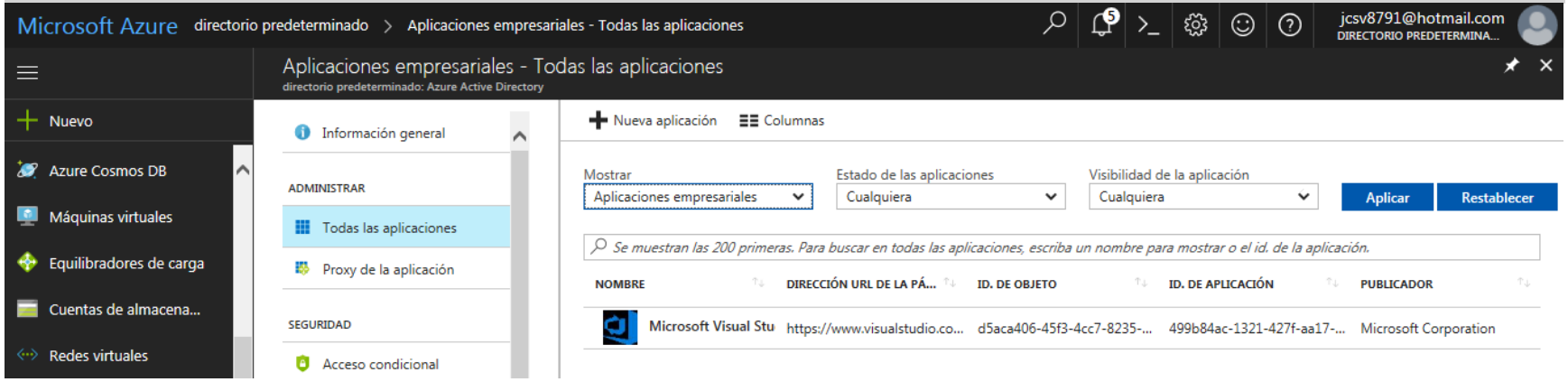
FIGURA 53: ESTADO DE LA APLICACIÓN



Como se puede ver en las dos graficas anteriores, se creó y ejecutó la aplicación para comprobar su comportamiento. Por otro lado, si se quiere crear una aplicación desde cero, también se puede hacer importando un lenguaje de desarrollo, como una aplicación;

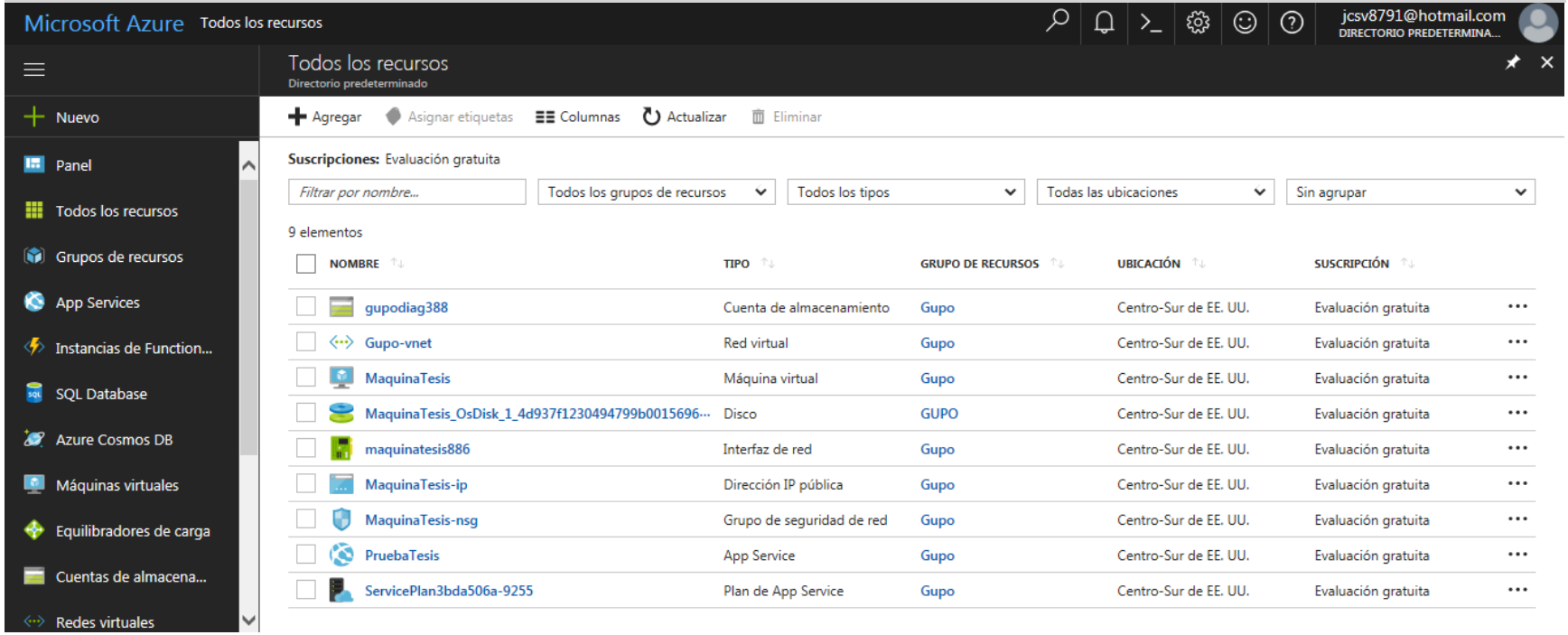
sobre este se desarrolla la aplicación, que luego será creada en esta misma pantalla de administración de aplicaciones. Lo anterior se explica a continuación, en la Figura 54.

FIGURA 54: MICROSOFT VISUAL STUDIO



Estado de la prueba**.** Para realizar esta prueba, se creó un total de servicios que, se pueden ver en la siguiente gráfica: la **FIGURA 55**. Estos servicios se dispusieron para ser ejecutados sobre el *datacenter* de la nube de Microsoft, en el centro-sur de EE. UU.

FIGURA 55: SERVICIOS CREADOS



Conclusiones

La realización de este trabajo arroja varios resultados interesantes, que dejan ver cómo las tecnologías son agentes de cambio en las entidades financieras. Estos cambios generan dudas y temores, principalmente en los temas de seguridad; no obstante, estos temores son cada vez menores, en comparación con los beneficios que brinda la nube. Para entender de forma más clara y concisa todos los temas abordados en este trabajo, se incluyen varias conclusiones que aportarán precisión sobre el tema tratado.

Lo primero es que la seguridad nunca se puede garantizar al 100 %. Cuando se habla de seguridad informática, en especial en el mundo financiero, es necesario tener presente que hay un sinfín de variables que pueden afectar la seguridad de un banco o entidad financiera; los ataques externos que estas entidades reciben diariamente suman el 75 % del total de los ataques cibernéticos. A esto también hay sumarle que las entidades financieras son susceptibles de fraude interno, ya sea por personas que se infiltraron en estas organizaciones con este fin o por trabajadores que se dejaron tentar por el dinero fácil. La realidad es que siempre existirán posibilidades de un ataque para robar información de los clientes, para robar dinero o para atacar la infraestructura que soporta los servicios de la organización.

Ninguna organización —gubernamental o privada— puede garantizar el 100 % de la seguridad. Lo que sí se puede hacer es mantener un buen nivel de seguridad e identificar los posibles riesgos; revisar constantemente todos los parámetros y la arquitectura de seguridad, en busca de brechas o posibles fallas; mantener equipos de seguridad interna y de seguridad externa, que permitan descubrir cualquier problema y que, a su vez, garanticen que no haya alguien

dentro la organización que pueda ser juez y parte. A todo lo anterior se suman los equipos de auditoria.

Otro aspecto, no menos importante, es tener en cuenta que una entidad financiera tiene un propósito: facilitarles a sus clientes la administración, gestión y uso de su dinero, además de otros productos que ofrecen estas entidades. Por ese motivo, la probabilidad de que alguien se aproveche de clientes sin mucho conocimiento o clientes ingenuos es muy alta; cada vez son más los ladrones que logran defraudar a sus clientes a través de engaños o de ingeniera social. Este sin duda es el factor más crítico; como se ha mencionado antes, los seres humanos son el eslabón más débil de la cadena, es indiscutible que siempre estarán ahí. Por consiguiente, los bancos deben buscar formas más eficientes, simples y seguras para que los clientes puedan interactuar con sus productos financieros.

Cuando se habla de buscar formas más eficientes y simples para estas operaciones, las implementaciones en la nube pueden ser muy buena opción: estas pueden ser tan o incluso más seguras que las implementaciones *on premise*. Esta afirmación puede ser un poco polémica para muchos, especialmente para aquellas personas que no han incursionado en el mundo de la nube: para aquellos que están acostumbrados a implementaciones *on premise*, donde creen tener el control de todo su *datacenter*.

Sin embargo, esto no es totalmente cierto: si un *datacenter* tiene unos costos muy altos en implementación, soporte y mantenimiento, esto implica que su velocidad de adecuación y mejora es mucho más lenta que la de un servicio en la nube, a causa del impacto económico que supondría actualizarlo. Esto se debe a que todas las empresas deben cuidar primero su *core* de negocio y, después, aquellos componentes que lo soportan. En este punto es donde son expertos

los proveedores de nube. Aquí surge una pregunta de gran relevancia: ¿cuál es el *core* de negocio de una empresa que ofrece servicios en la nube?

La respuesta es clara, y es la razón por la que estas empresas ofrecen cada vez servicios de nube más especializados y en un menor tiempo: los proveedores de servicios en la nube son compañías dedicadas a soportar estos servicios. En consecuencia, cuando encuentran un problema de seguridad, son capaces de solucionarlo y de replicarlo fácilmente para todos clientes. Si se compara esto con la capacidad de una organización para encontrar un problema —suponiendo que lo encuentre de forma oportuna— y con el tiempo que se demora en corregirlo, resultan obvias las ventajas de la seguridad en la nube.

No obstante, al hablar de seguridad también hay que tener en cuenta otros aspectos: las personas, los temas contractuales y la implementación realizada. En primer lugar, se reflexionará sobre las personas: el ser humano siempre será el punto más débil de la cadena, ya sea por omisión o por acción. Normalmente, cuando hay problemas de seguridad, siempre hubo participación de las personas: fallas de los clientes, por descuido o desconocimiento; errores de los empleados, por falencias humanas o mala intención, o acciones perjudiciales de un tercero. Esto no va a cambiar en los modelos de nube: el factor humano siempre va a estar presente; sin embargo, este riesgo puede mitigarse un poco, mediante los controles adicionales que ofrecen los servicios de la nube.

Lo anterior se complementa con los temas contractuales, donde siempre deben quedar claros todos lo relacionado con la seguridad y con las consecuencias del no cumplimiento por parte del prestador de servicios.

Por último, el factor más importante es la implementación: cuáles componentes se van a usar, cuál o cuáles serán los proveedores de nube y cuál va a ser el modelo operativo. Si esto no está claro y bien definido, será una incubadora de problemas de seguridad para el futuro, ya sea en cualquier modelo de nube o en un modelo *on premise*. La nube es tan segura como la arquitectura que utilice. Si la arquitectura es débil —sin controles, sin monitoreo, sin el correcto cumplimiento de los estándares y sin un buen modelo de gobierno—, no importa cómo se implemente, sea en la nube u *on premise*; tarde o temprano, habrá una puerta abierta para que la seguridad sea vulnerada.

Teniendo en cuenta lo explicado sobre la nube, puede decirse que los modelos de nube llegaron para quedarse y que cada día cobran más fuerza. Llegar a esta conclusión no ha sido fácil y no es algo que se deba tomar a la ligera. Cuando se piensa en la nube y en su masificación, es necesario tener en cuenta los costos, además de pensar en la seguridad. Como puede leerse la Revista Dinero, Andrew Nazareth, el líder de desarrollo de negocios con *startups* de Amazon Web Services (AWS), explico que AWS ha rebajado precios 62 veces, desde que fue presentado en 2006. Paralelamente, en el segundo trimestre de 2017, los ingresos de esta compañía aumentaron 42 % hasta alcanzar los USD $4.100 millones, cosa que convirtió a AWS en un negocio con más de USD $ 16.000 millones de tasa de manejo de negocio.

Además, AWS ha expandido continuamente sus servicios para admitir una nube de carga. Hoy tiene más de 90 servicios, que van desde el almacenamiento hasta el internet de las cosas (IoT[7]) y la inteligencia artificial. Actualmente, esta empresa opera 44 zonas de disponibilidad, en 16 regiones de infraestructura repartidas por todo el mundo; hay planes anunciados para otras 16

7. Internet of Things.

zonas de disponibilidad en seis regiones de AWS: Hong Kong, Francia, Suecia, China, Oriente Medio y la segunda región de GovCloud) (“El almacenamiento en la nube marcó un antes y un después en el mundo de las startups”, 2017).

Los datos anteriores contribuyen a la confiabilidad de esta compañía, y permiten afirmar con mayor certeza que la nube llego para quedarse; esta tecnología cobra cada día más fuerza, ofreciendo servicios especializados y con un nivel muy alto de seguridad. A estas ventajas es muy importante sumarles un excelente proceso de selección del proveedor de nube; ya se ha señalado en este trabajo que, en la actualidad, los dos proveedores líderes en el mercado de nube son Amazon —con AWS— y Microsoft —con Azure—, en ese orden.

Habiendo aclarado el potencial de la nube y los retos que traen las fintech, es acertado decir que el futuro de los bancos está en ser bancos-fintech; esta aseveración se respalda con los aspectos antes mencionados: primero, nunca se puede garantizar la seguridad al 100 %; segundo, la nube puede ser tan o incluso más segura que una implementación *on premise*, y, tercero, la nube cada día cobra más fuerza; estos factores son innegables. Si a esto se le suma la popularidad que siguen adquiriendo las fintech y las exigencias actuales de los clientes, puede decirse que las entidades financieras deben evolucionar.

La banca tradicional, donde el objetivo de un banco era el dinero, ya no existe; en la actualidad, un banco se mueve basado entre grandes ejes: la tecnología, la información y la seguridad. Estos tres factores son el corazón del negocio; en todo momento se deben garantizar unas tecnologías adecuadas, un correcto uso de la información y un muy buen esquema de seguridad. Lo anterior se entiende al considerar que el dinero cada día se hace más digital y los

clientes son más digitales a cada momento; con el paso del tiempo, las bóvedas de los bancos tienen menos dinero y sus *datacenter* son cada vez más grandes.

Esto se puede corroborar cuando se analiza lo que sucede en Europa y Asia: los bancos hacen grandes inversiones en tecnología, especialmente en cuatro grandes aspectos: nube, seguridad, información y movilidad. Estas entidades financieras han creado sus propias compañías fintech, que les ayudarían a desarrollar esta tecnología en el futuro. Este fenómeno también se está dando en Colombia, donde Bancolombia desarrolló Nequi —su primera *app*—, que funciona como un banco de cuentas de bajo monto, totalmente independiente y con el 80 % montado en una nube pública. Al ser un primer intento, Nequi todavía tiene muchos aspectos de mejora; aun así, en las cuentas de bajo monto se minimiza el riesgo y, además, son un laboratorio de nuevas tecnologías, que puedan ser llevadas a Bancolombia para luego ser masificadas.

De esta manera, los bancos que no evolucionen pueden ver seriamente comprometida su participación en el mercado o, incluso, podrían desaparecer. Las entidades financieras deben optimizar el uso de sus sucursales físicas, llevando muchas de sus operaciones al mundo digital. Para alcanzar ese objetivo, los bancos deben entender que no hay que ver a las fintech como una amenaza; por el contrario, deben tomarse como aliados estratégicos.

Es claro que, en primera instancia, las fintech se tomaron como una amenaza para las entidades financieras; sin embargo, también están abriendo el mundo financiero a niveles que antes no se contemplaban: esta es la oportunidad de entrar en una competencia abierta. De esta forma, lo que deben hacer las entidades financieras es generar sinergias con estas compañías, aprovechando su velocidad para el cambio y esa visual diferente del entorno financiero. Las fintech pueden ser grandes aliados, si se gestionan de la forma correcta. Su implementación

abriría el mundo de la banca a todos los sectores y a múltiples modelos de industria, interconectando a los clientes con estos servicios: transporte, salud, gobierno, energía, educación, construcción, entre otras. En consecuencia, se lograría que la banca le pueda decir al cliente, en todo momento, “acá estoy”, “este es tu comportamiento financiero”, “¿cómo puedo ayudarte a conseguir lo quieres?”, “esto es lo que debes hacer”, “así es como lo puedes hacer”.

Hacer esto una realidad en el entorno financiero es demasiado complejo. Visto desde otra perspectiva es posible, pero el costo de oportunidad se pierde; es necesario llegarles a los clientes en el momento en el que realmente lo necesitan y con lo que necesitan. Por eso, el modelo de banco-fintech se ha hecho tan necesario.

Por último, puede decirse que las entidades financieras deben aprovechar los servicios de la nube para apalancar la transformación del mundo financiero. No hay que temer a los aspectos de seguridad, ya que el tipo de nubes de Amazon y Microsoft cumplen con unos estándares de seguridad que incluso podrían ser más altos que los de muchos *datacenters*. Hay que dejar atrás los temores de seguridad y plantear escenarios de nube con arquitecturas robustas y confiables, que contemplen todos los controles necesarios y que, además, tengan en cuenta todos los temas regulatorios que deben ser cumplidos por los bancos. Esto podría ser incluso un poco más complejo que las mismas implementaciones de seguridad.

Los bancos deben ser bancos fintech y trabajar con otros sectores de la industria; esto incluye a las fintech, para lograr así apalancar la transformación digital del país. El pilar fundamental es la seguridad, analizada desde todos los puntos de vista posibles: seguridad de la información, seguridad de la infraestructura, seguridad de las aplicaciones, seguridad en la

autenticación, seguridad interna, arquitectura de seguridad, aspectos de seguridad en los contractos, seguridad a nivel de cumplimiento normativo, entre otros aspectos.

Trabajos futuros

En el futuro, puede surgir un trabajo complementario al que aquí se presenta: un análisis de la seguridad del Internet de las Cosas en la nube. El Internet de las Cosas (IoT) cada día cobra más fuerza, y, por los volúmenes de información que maneja, lo más viable es trabajarlo en la nube. Sin embargo, en ese caso la seguridad es un factor crítico. ¿Qué puede pasar con los carros autónomos si la información está en la nube?, ¿qué pasaría con la información de las empresas de energía, acueducto, gas, transporte público, entre otras?, ¿qué puede esperarse si alguien manipula esta información? En estos escenarios, ya no solo se hablaría de perder la información de los clientes, de perder su dinero o de ver un servicio financiero afectado; esto pondría en riesgo vidas humanas.

¿Cómo debe ser la seguridad del IoT en la nube?

Referencias

Alexos, N., Company, P. & Contero, M. (). Integrated modeling with top-down approach in subsidiary industries. *Computers in Industry, 53* (1), 97-116. https://doi.org/10.1016/S0166-3615(03)00122-2

Banco. (s.f.). En *DefiniciónABC*. Recuperado de http://www.definicionabc.com/economia/banco.php

Benítez Hernández, I. (2009). Problemas éticos y de la seguridad informática asociados al uso de esta tecnología [artículo de revista en línea]. *Infodir* (8). Recuperado de http://www.revinfodir.sld.cu/index.php/infodir/article/view/375

Bruno, G. (2013). Cloud computing en la industria financiera. *Ciencia y Tecnología, 1*(13). Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=4843852

Camps, C. & Oriol, A. (2012). *La nube. Oportunidades y retos para los integrantes de la cadena de valor.* Madrid, España: Management Solutions. Recuperado de https://www.managementsolutions.com/sites/default/files/publicaciones/esp/La-nube.pdf

Cloud Comparer. (2017, 1 de octubre). *Public Cloud Serrvices Comparison*. Recuperado de https://ilyas-it83.github.io/CloudComparer/

Congreso de la República. (2008, 31 de diciembre). Ley Estatutaria 1266 de 2008. *Diario Oficial* (47.219), . Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

Congreso de la República. (2009, 5 de enero). Ley 1273 de 2009. *Diario Oficial* (47.223). Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Congreso de la República. (2012, octubre 17). Ley Estatutaria 1581 de 2012. *Diario Oficial* (48.587). Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Conpes. (2016, 11 de abril). *Política nacional de seguridad digital* [documento oficial]. Recuperado de https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

Cuesta, C., Alonso, J., Tuesta, D. & Fernández de Lis, S. (2015). *El desarrollo de la industria del cloud computing: impactos y transformaciones en marcha*. Recuperado de https://www.bbvaresearch.com/publicaciones/el-desarrollo-de-la-industria-del-cloud-computing-impactos-y-transformaciones-en-marcha/

Cuesta, C., Ruesta, M., Tuesta, D. & Urbiola, P. (2015, 16 de julio). *La transformación digital de la banca*. Recuperado de https://www.bbvaresearch.com/wp-content/uploads/2015/07/Observatorio—Banca—Digital2.pdf

El almacenamiento en la nube marcó un antes y un después en el mundo de las startups. (2017, 11 de noviembre). *Revista Dinero*. Recuperado de http://www.dinero.com/emprendimiento/articulo/el-almacenamiento-en-la-nube-multiplico-emprendimientos/252039

El cibercrimen es un delito mas rentable que el narcotrafico. (2015, 28 de septiembre). *Revista Dinero*. Recuperado de http://www.dinero.com/internacional/articulo/principales-cifras-del-cibercrimen-mundo-colombia/213988

Erika Maria Jimenez Hidalgo, F. d. (s.f.). Legal aspects of cloud computing.

Fielder, A. & Brown, I. (2012, mayo). Computación en nube [estudio solicitado por el Parlamento Europeo]. Berlin, Alemania: Civic Consulting. Recuperado de http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO—ET(2012)475104—ES.pdf

Galdo, M. (2015, julio). *Multicanalidad y digitalización bancaria* [Tesis de Maestría en Finanzas]. Madrid, España: Universidad Pontificia de Comillas. Recuperado de : https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/6338/TFM000186.pdf?sequence=1&isAllowed=y

Gardiner, G. (2016, 2 de abril). *Fintech o internet, ¿qué llegó antes?* Recuperado de https://www.kantox.com/es/fintech-internet-que-llego-antes/

Gibson, J. (2015, 20 de agosto). *The Impact fintech is having on the Financial Services Industry in Ireland* [Tesis de Maestría en Administración de Negocios - MBA]. Dublin, Irlanda: Dublin Business School. Recuperado de http://esource.dbs.ie/bitstream/handle/10788/2906/mba—gibson—j—2015.pdf?sequence=1

ISO 27018 [resumen en blog]. (2015, 25 de febrero). Recuperado de http://www.normas-iso.com/iso-iec-27018-2014-requisitos-para-la-proteccion-de-la-informacion-de-identificacion-personal/

López, M. A., Albanese, D. E. & Sánchez, M. A. (2014). Gestión de riesgos para la adopción de la computación en nube en entidades financieras de la República Argentina. *Contaduría y*

administración, 59(3), 61-88. Recuperado de http://www.redalyc.org/articulo.oa?id=39531264004

Martin, J. (2016, 18 de marzo). *El mapa imperdible de las startups fintech en Colombia.* Recuperado de http://pulsosocial.com/2016/03/18/el-mapa-imperdible-de-las-startups-fintech-en-colombia/

Merrill, T. & Kang, T. (2014, abril). *Computación en la nube:. ¿está considerando su empresa tanto los beneficios como los riesgos?* Recuperado de http://www.acegroup.com/latam-es/assets/whitepaper-cloud-computing-esp.pdf

Nedelcu, B., Stefanet, M. E., Tamasescu, I. F., Tintoiu, S. E. & Vezeanu, A. (2015). Cloud Computing and its Challenges and Benefits in the Bank System. *Database Systems Journal, 5*(1), 45-58. Recuperado de http://www.dbjournal.ro/archive/19/19_5.pdf

Niazmand, N. (2015). The impact of Cloud Computing in the banking industry resources. *International Journal of Information, Security and System Management, 4* (2), 436-440. Recuperado de http://www.ijissm.org/article_12900_4.html

Noceti, H. & Freijo, A. (2015, septiembre). Cloud Computing. Su Aplicación en la Banca Privada Argentina. En *II Simposio Argentino sobre Tecnología y Sociedad*. Buenos Aires, Argentina: Sociedad Argentina de Informática e Investigación Operativa. Recuperado de http://hdl.handle.net/10915/59784

Noonan, L. (2016, 31 de marzo). Tecnología financiera elimina millones de empleos. *Financial Times*. Recuperado de http://www.elfinanciero.com.mx/financial-times/tecnologia-financiera-elimina-millones-de-empleos

Noya, E. (2016, 4 de abril). ¿Es el 'fintech' el mayor desafío que afronta la banca? *Harvard Deusto Business Review* (254), 22-29. Recuperado de http://gref.org/nuevo/docs/economia_digital_280416.pdf

Pacheco Jiménez, M, N. (2016, 16 de marzo). *Bancos, bienvenidos a la revolución digital*. Recuperado de http://blog.uclm.es/cesco/files/2016/03/Bancos-bienvenidos-a-la-revoluci%C3 %B3n-digital.pdf

Presidencia de la República. (2013). Decreto 1377 de 2013. *Diario Oficial* (48.834). Recuperado de http://wsp.presidencia.gov.co/Normativa/Decretos/2013/Documents/JUNIO/27/DECRETO%201377%20DEL%2027%20DE%20JUNIO%20DE%202013.pdf

Price Waterhouse Cooper. (2016). *Fintech 2016*. Recuperado de http://informes.pwc.es/fintech/

Primorac, C. R. (2015). *Seguridad en la computación en la nube* [Monografía de Licenciatura en Sistemas de Información]. Corrientes, Argentina: Universidad Nacional del Nordeste. Recuperado de http://exa.unne.edu.ar/informatica/SO/primorac_monografia_computacion_en_nube.pdf

Signaturit. (2016, 14 de enero). *¿A qué riesgos legales y de seguridad se enfrentan las fintech?* [publicación en blog]. Recuperado de https://blog.signaturit.com/es/riesgos-legales-y-de-seguridad-para-las-fintech

Skan, J., Dickerson, J. & Masood, S. (2015). *The Future of fintech and Banking. Digital disrupted or reimagined?* Recuperado de https://www.accenture.com/_acnmedia/Accenture/Conversion-

Assets/DotCom/Documents/Global/PDF/Dualpub_11/Accenture-Future-Fintech-Banking.pdf#zoom=50

Sriram, S. (2011). *Cloud Computing in Banking. What banks need to know when considering a move to the cloud*. Recuperado de https://www.capgemini.com/wp-content/uploads/2017/07/Cloud_Computing_in_Banking.pdf

Superintendencia Financiera de Colombia. (2017). Servicios en la nube, seguridad y calidad de la información [Concepto 2017059546-001]. Recuperado www.superfinanciera.gov.co%2Fdescargas%3Fcom%3Dinstitucional%26name%3DpubFile1012860%26downloadname%3D2015019296.docx&usg=AOvVaw12Dc0dyZ7Jwvp24tBu4jck

Anexos

Evaluación modelos de nube.xlsx

Evaluación nubes publicas.xlsx

Graficas propias.pptx

Análisis de riesgos-pdf