IBM Cloud

Industria Bancaria Argentina

Camino hacia la nube

Guía de normativas locales y recomendaciones para la adopción de la nube.

IBM

Introducción

¿Qué beneficios tiene la nube?

El mundo está experimentando una transformación digital y móvil: más información disponible rápidamente a través de diversos medios. En este contexto, la nube se ha convertido en una herramienta fundamental para la innovación bancaria. Existen un sinnúmero de beneficios de operar en la nube; entre ellos se destacan:

- Flexibilidad de costos
- Escalabilidad
- Adaptabilidad
- Complejidad enmascarada
- Variabilidad contextual
- Conectividad con el ecosistema

Estos atributos, sumados a la agilidad y la reducción del *time-to-market*, son facilitadores de negocios que permiten mejorar la sofisticación de productos y servicios sin complejizar la experiencia de usuario o las integraciones con el ecosistema. Además, impulsan la innovación a través de propuestas de valor para clientes, mejoran la eficiencia y respaldan la transformación de las organizaciones.

¿Qué se entiende por nube o Cloud? ¿Cómo puede ayudar a las organizaciones? ¿Qué beneficios implica? ¿Cómo se puede implementar respetando las normativas locales?

> **“Operar en la nube es el primer paso para la mejora de la eficiencia y la optimización de procesos.**

Índice

01. Sobre este documento

02. ¿Por qué mover cargas a la nube?

03. Mitos sobre la nube en la industria

04. Transformación de la industria

05. Seguridad en la nube

06. Normativa local

07. Glosario

01.

Sobre este documento

Un poco sobre la nube

La industria bancaria (al igual que las demás industrias) se encuentra en una carrera constante para aprovechar las ventajas y oportunidades de los avances tecnológicos. Sin embargo, debe adaptarse a sus propias dinámicas y normativas, lo cual representa un desafío en sí mismo. A veces, incluso dificulta la adopción de nuevas iniciativas.

Este documento surge como resultado de las reuniones que tuvieron lugar durante 2019 en el marco de la Mesa de Innovación Financiera, en las que participaron proveedores de nube, representantes de los bancos, fintech y organismos gubernamentales (como el Banco Central de la República Argentina -BCRA- y la Dirección Nacional de Protección de Datos Personales).

Su objetivo es **iniciar el camino hacia la adopción de servicios de nube** según diferentes modelos de arquitectura e identificar la combinación que mejor se adapte a cada institución.

También se analizarán aspectos de seguridad, tendencias, mitos y su relación con la normativa local.

02.

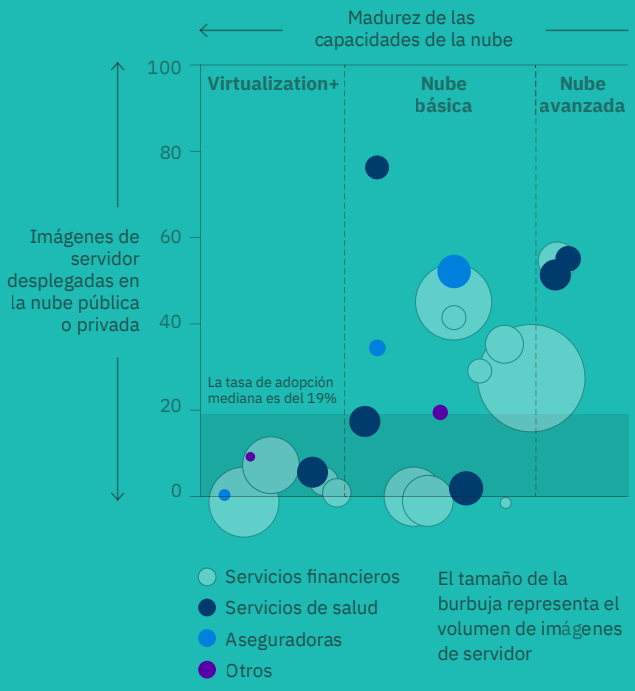
¿Por qué mover cargas a la nube?

Los bancos se encuentran en un escenario en el que deben convertirse en líderes digitales, para diferenciarse eficazmente de sus competidores. La nube resulta ser un elemento indispensable en sus estrategias digitales.

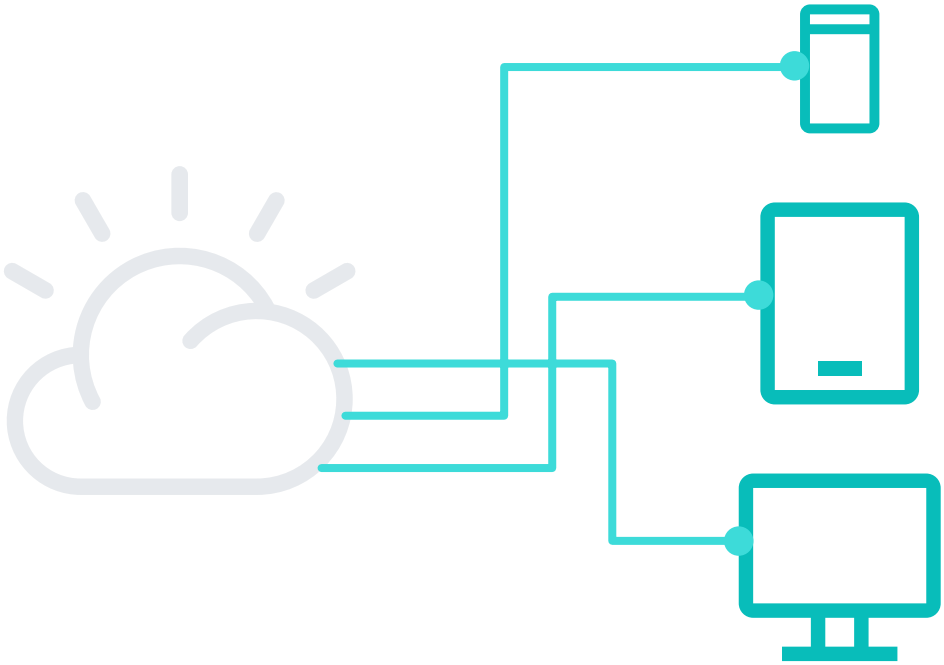
Si bien son muchos los bancos que reconocen las ventajas de desarrollar soluciones ágiles y nuevas aplicaciones en plataformas de datos en la nube, solo unos pocos poseen una estrategia definida y robusta para la adopción de la nube. Generalmente, los bancos utilizan la nube para algunas cargas no críticas o alternativas de infraestructura tradicional, como soluciones de respaldo o recupero de datos, pero esto no resulta suficiente para escalar de forma ágil y bajo demanda en un mercado dinámico y en constante cambio.

Por su parte, los clientes demandan servicios más personalizados y eficientes, accesibles en cualquier momento y a través de múltiples plataformas. Esto genera una presión adicional en la infraestructura instalada y una necesidad de escalabilidad y elasticidad que solo son posibles gracias a la transformación digital con un enfoque de banca digital.

Volumen de imágenes de servidor desplegadas por industria en comparación con la madurez de las capacidades de la nube.



> **La nube se convirtió en un elemento indispensable en las estrategias digitales de los bancos.**



Las compañías financieras son las primeras en experimentar con nuevas tendencias tecnológicas; sin embargo, sus largos tiempos de implementación, regulaciones y burocracia son causantes de que sean las últimas en adoptarlas. Los sistemas bancarios tradicionales son continuamente actualizados con código personalizado para hacer frente a los cambios en las prácticas comerciales y la evolución tecnológica. Como resultado, aparecen sistemas saturados con capas adicionales de funcionalidad, lo que los hace complicados y más difíciles de manejar.

Esta dinámica resulta poco práctica y la falta de interconexión de los sistemas alojados en silos inhibe el crecimiento de los negocios. Además, las aplicaciones *legacy* se caracterizan por tener datos de clientes y productos en el mismo sistema, lo que impide que los bancos que ejecutan múltiples carteras de productos puedan proporcionar una visión clara y única del cliente.
Estas dificultades impulsan a las empresas del sector financiero a buscar alternativas basadas en nube que les permitan:

1. Proporcionar servicios únicos. Generar experiencias personalizadas para clientes y usuarios que se traduzcan en una ventaja competitiva en un sector extremadamente homogéneo en su cartera de productos.

2. Adoptar prácticas eficientes. Las prácticas tradicionales no permiten asimilar rápidamente los cambios que generan las nuevas tendencias. Esto puede revertirse gracias a plataformas basadas en nube, escalables bajo demanda y rápidas de modificar. Incorporar prácticas como DevOps permite reducir los ciclos de desarrollo y generar valor constantemente.

3. Reducir costos. La eficiencia en los costos asociados a la innovación tecnológica es la clave para la competitividad. El primer paso en la implementación de nuevas prácticas es posible gracias a la migración a la nube.

03.

Mitos sobre la nube en la industria

Causas de su lenta adopción

Durante el año 2019, el BCRA convocó a una mesa de especialistas y profesionales del mundo financiero y tecnológico con el objetivo de identificar las causas por las que el sector financiero argentino mostraba una lenta adopción de los servicios de nube.

¿El resultado? Se demostró que esa tendencia era consecuencia de un sinnúmero de percepciones que no tenían sustento desde el punto de vista legal y operativo. A continuación, las abordamos e intentamos aclararlas.

Mito:
Existe un proveedor de servicios de nube homologado por BCRA.

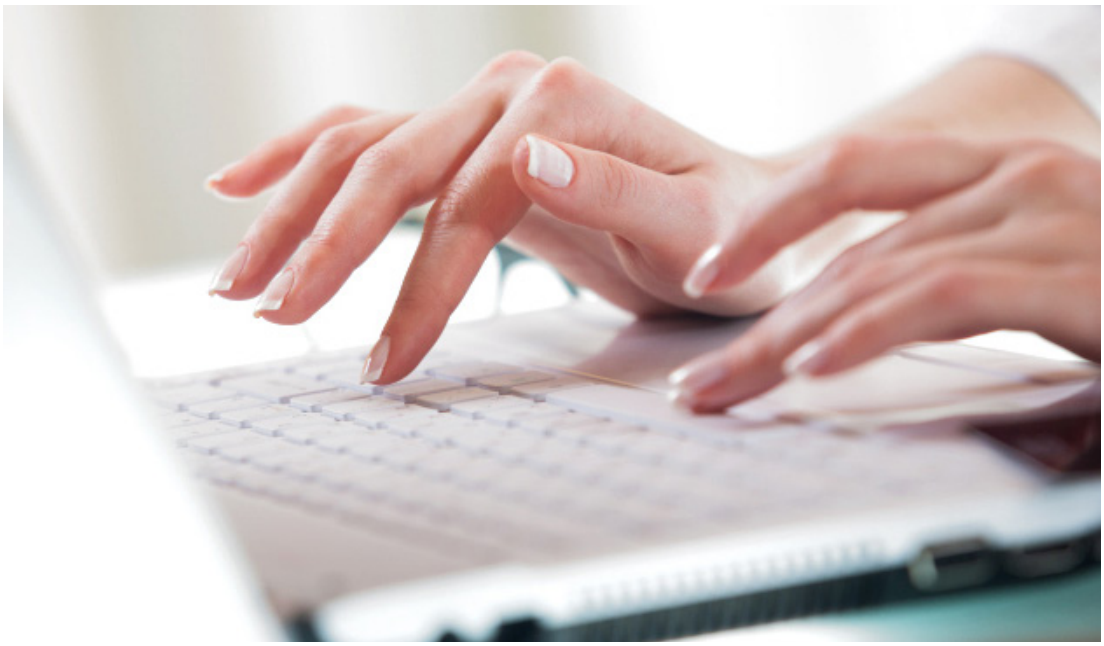
Realidad:
El BCRA y la Dirección Nacional de Protección de Datos Personales no homologan a los proveedores. Solo establecen los requerimientos mínimos que un proveedor de cualquier servicio (incluyendo servicios de nube) debe cumplir para que una entidad financiera pueda hacer uso de ellos. En este contexto, todos los grandes proveedores cumplen con el requerimiento.

Mito:
Las leyes argentinas limitan o no permiten el uso de nube a las entidades financieras.

Realidad:
En la actualidad, no existen disposiciones que prohíban o restrinjan el uso de la nube en el sector financiero argentino. Según la Comunicación A 6354 del BCRA, las entidades financieras se encuentran habilitadas para contratar servicios en la nube siempre que se cumplan una serie de requisitos (los detallaremos más adelante).

Mito:
Alojar datos en la nube dificulta la capacidad de las entidades financieras para acceder a ellos.

Realidad:
En IBM Cloud el cliente es el titular de sus datos y conserva los derechos sobre ellos. Cualquier cliente puede solicitar una copia o la eliminación de sus datos en cualquier momento.



Mito:
No es posible garantizar la seguridad de los datos alojados en una plataforma de nube.

Realidad:
La protección de los datos es prioridad para IBM Cloud.
IBM está sujeto a las exigencias de GDPR (Reglamento de Protección de los Datos, por su sigla en inglés) a nivel global y posee servicios y mecanismos diseñados para proteger los datos propietarios y sensibles de las personas. El acceso a los datos está estrictamente monitoreado y controlado no solo por medio de encriptado y control de acceso, sino también siguiendo lineamientos de entes certificadores internacionales y programas de auditoría sujetos a certificación anual del cumplimiento con las normas ISO 27001 o SSAE SOC 2 (o ambas).

Mito:
No es posible garantizar que los datos de los clientes sean correctamente borrados si se encuentran alojados en una plataforma de nube.

Realidad:
IBM saneará de forma segura los soportes físicos para su reutilización y destruirá aquellos que no se reutilizarán, de conformidad con las directrices del Instituto Nacional de Estándares.
IBM puede proporcionar evidencia y acreditación del cumplimiento con lo indicado, tales como certificados, declaraciones o informes procedentes de auditorías externas independientes y acreditadas (como normas ISO 27001, SSAE SOC 2 y otras normas del sector).

Mito:
Subir cargas productivas a una nube es complejo porque luego es muy difícil evitar quedar atrapado con un único proveedor (*vendor lock-in*).

Realidad:
IBM Cloud soporta todo tipo de plataformas y lenguajes de desarrollo, lo cual permite la portabilidad de las aplicaciones que se desarrollen o alberguen en sus centros de datos. Además, IBM posee soluciones multinube e híbridas con componentes en IBM Cloud, entornos físicos del cliente o en cualquiera de los demás proveedores de nube del mercado.

Mito:
No es posible utilizar servicios de IBM Cloud porque IBM no admite visitas de auditoría (requeridas por el BCRA) a sus centros de cómputos.

Realidad:
El cliente podrá solicitar a IBM Cloud auditorías a sus centros de cómputos en la medida que no comprometan la seguridad de los datos de IBM o de cualquiera de sus clientes. Deberán coordinarse con el equipo de soporte local. Asimismo, IBM puede proveer certificados, declaraciones o informes procedentes de auditorías externas independientes y acreditadas (como normas ISO 27001, SSAE SOC 2 y otras normas del sector).

Mito:
IBM posee muchos centros de datos. Es imposible asegurar en dónde está alojada la información de nuestros clientes o sus réplicas.

Realidad:
Al momento de crear la infraestructura o contratar un servicio de IBM Cloud, el cliente decide en dónde desea ubicar su infraestructura de nube y sus datos (ya sea por necesidades de regulación o por requerimientos de arquitectura), lo cual no se modificará a menos que sea solicitado expresamente.
El origen y destino de las réplicas de alta disponibilidad también puede seleccionarse según los requerimientos. Podrán ser réplicas en un mismo centro de datos y en una misma o distintas regiones.

Mito:
Mi empresa no posee personal digital y no está preparada para acompañar un proceso de migración a la nube.

Realidad:
Existen diversas formas de migrar cargas a la nube, algunas implican *refactoring* para adaptarlas a nuevos enfoques de arquitectura (por ejemplo, las basadas en microservicios, contenedores, etc.), pero existen contextos en los que por la modalidad de uso, antigüedad de las aplicaciones o la arquitectura sobre la que se ejecutan resulta más conveniente migrar a un entorno de nube sin realizar cambios de arquitectura (Lift and Shift).
Cada caso tiene sus particularidades, por lo que siempre es recomendable recurrir a especialistas para determinar la mejor opción.

Mito:
El proceso de migrar las aplicaciones vigentes que, no son “Cloud Ready”, no tiene un retorno de inversión claro.

Realidad:
Existen diversas formas de migrar cargas a la nube, algunas implican refactoring para adaptarlas a nuevos enfoques de arquitectura (por ejemplo, las basadas en microservicios, contenedores, etc.), pero existen contextos en los que por la modalidad de uso, antigüedad de las aplicaciones o la arquitectura sobre la que se ejecutan resulta más conveniente migrar a un entorno cloud sin realizar cambios de arquitectura (Lift and Shift).
Cada caso tiene sus particularidades, por lo que siempre es recomendable recurrir a especialistas para determinar la mejor opción.

Mito:
Mi empresa no puede adoptar nube porque nuestra infraestructura no tiene una buena conectividad a internet.

Realidad:
Existen múltiples formas de desplegar una nube. Históricamente se trataba de algo que se encontraba en un centro de cómputos externo, pero hoy existen alternativas para desplegar nube en un centro de cómputos propio, una solución híbrida o una que se encuentre 100% en IBM Cloud. Cada caso debe ser analizado; muchas veces la solución final implica una combinación de todas estas opciones.

04.

Transformación de la industria

Más que una moda, una tendencia.

Las instituciones financieras buscan mejorar la experiencia de sus clientes y modernizar sus aplicaciones básicas.

Transformarse e innovar con mayor rapidez, crear experiencias bancarias personalizadas y desarrollar servicios bajo demanda que superen a los de la competencia y que sean más inteligentes es fundamental cuando el servicio se encuentra estandarizado.
Para esto se necesitan la agilidad, resiliencia, elasticidad y facilidad de aprovisionamiento que ofrece la nube. Sin embargo, a medida que las instituciones financieras se esfuerzan por ser más innovadoras también necesitan cumplir con las obligaciones normativas y de seguridad.

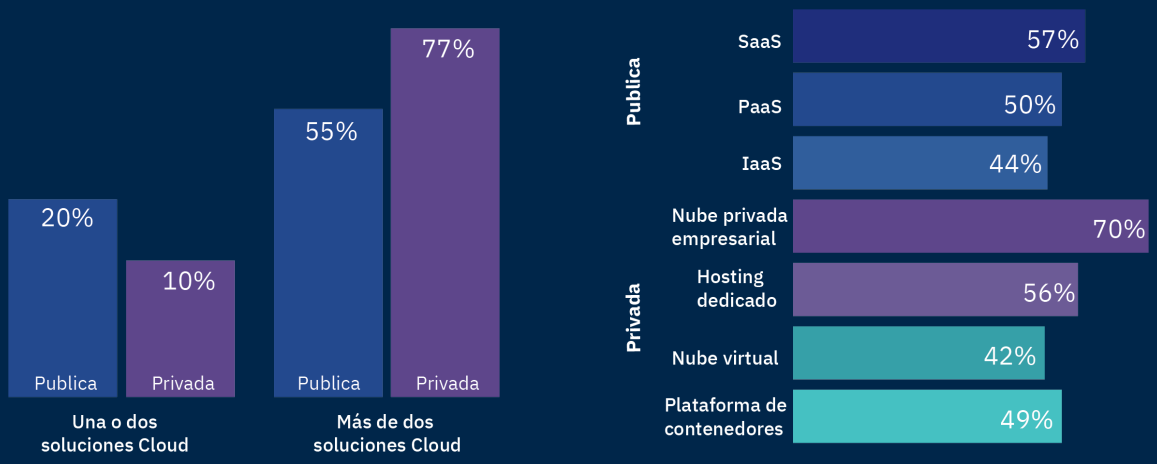
Las instituciones bancarias, junto con los proveedores que prestan servicios a la industria, requieren un marco seguro que infunda confianza y seguridad al trasladar las cargas de trabajo y las aplicaciones a la nube pública.

Las entidades financieras argentinas también se encuentran en un fuerte proceso de conversión digital (camino iniciado hace varios años cuando los procesos todavía dependían de tareas manuales y físicas). El progreso de la tecnología y el cambio en el comportamiento de los clientes ha creado en los bancos la necesidad de transformarse en organizaciones digitales.

> **“Las entidades financieras se encuentrar en un fuerte proceso de conversión digital, camino iniciado hace varios años.**

El proceso de transformación se sustenta en tres pilares fundamentales:

1. Conocer al cliente.
2. Optimizar los procesos de negocios y TI.
3. Aprovechar capacidades tecnológicas como la nube, economía de APIs o la inteligencia artificial para mejorar la experiencia de los clientes.



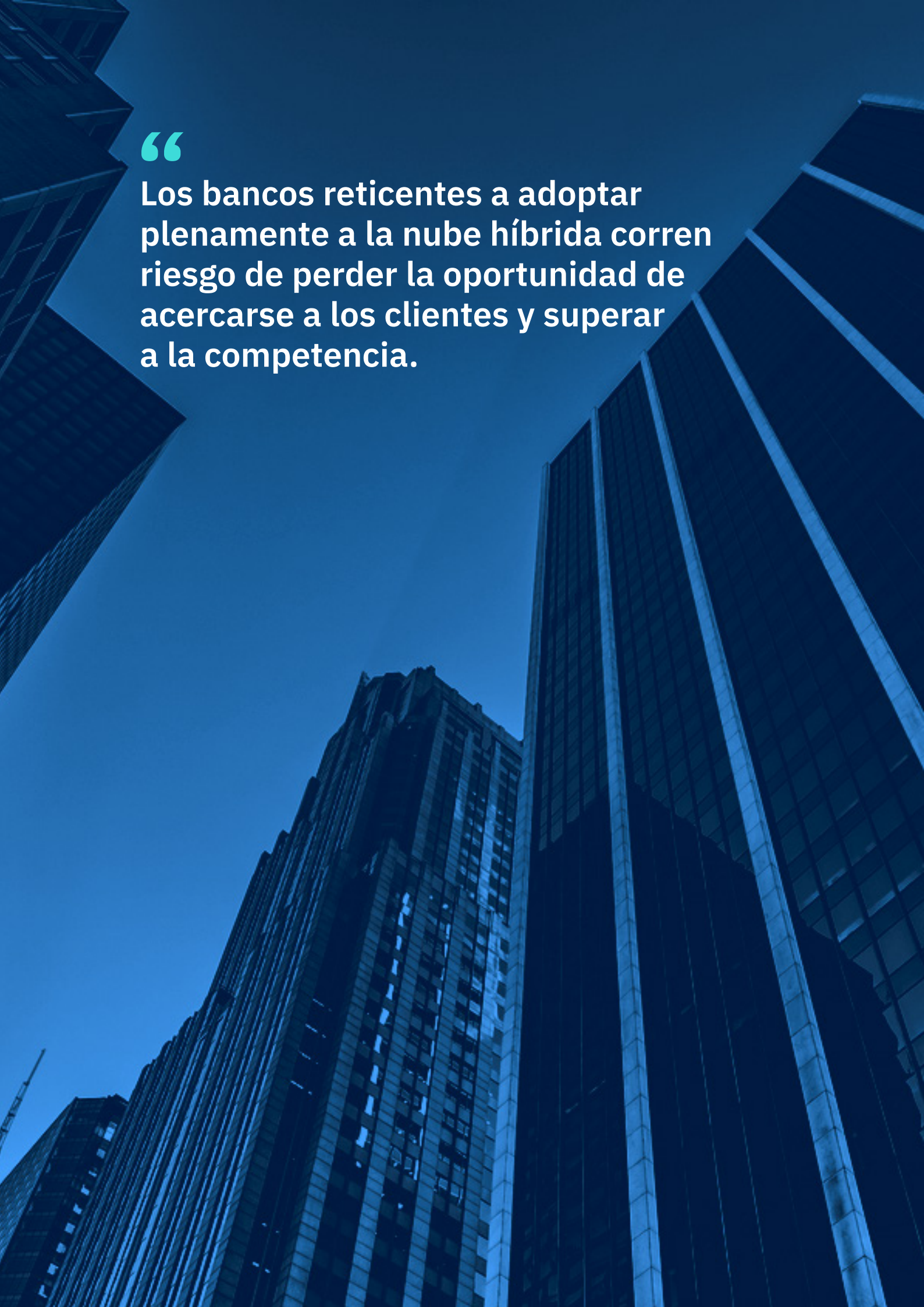
Principales usos de la Nube en clientes de la Industria Bancaria mundial

Transformación hacia modelos Cloud

Además de las ventajas del modelo financiero de nube (pago por uso), la transformación de las compañías hacia la nube es mucho más intensa: las empresas Cloud oriented pueden poner en marcha metodologías ágiles que permitan extender la agilidad de la nube a otras capas de la organización.

Un ejemplo es el caso de las metodologías de Integración Continua (utilizadas desde hace años) que pueden extenderse con las de Despliegue Continuo sobre entornos Cloud y permitir que las compañías no solo desarrollen el código más rápido: una vez que el código está listo y ha superado la batería de pruebas predeterminadas puede pasar a producción de manera automática y permitir que los clientes dispongan de las mejoras tan pronto como estén listas, sin necesidad de esperar a la puesta en producción de una gran versión final. Un ejemplo clásico de esta metodología se observa en las aplicaciones que tenemos en nuestros celulares: nos envían actualizaciones constantes que no implican necesariamente cambios drásticos.

Uno de los elementos transformadores para este tipo de metodologías es el uso de arquitecturas de desarrollo como los microservicios. Están muy ligados también a los modelos de nube, ya que permiten que las aplicaciones se dividan en pequeñas áreas funcionales (en lugar de un gran bloque monolítico) que se conectan entre sí mediante APIs. De esta manera, el desarrollo de cada módulo es independiente del resto y la actualización de uno de ellos no afecta a los demás, por lo que los cambios realizados pueden ponerse en marcha de una manera mucho más ágil.



> Los bancos reticentes a adoptar plenamente a la nube híbrida corren riesgo de perder la oportunidad de acercarse a los clientes y superar a la competencia.

El informe “Tailoring Hybrid Cloud for Banking” del IBM Institute for Business Value revela las tres principales razones por las cuales las entidades bancarias están adoptando la nube híbrida:

01. Reducción de costos

La nube híbrida puede generar una disminución en los costos aprovechando las economías de escala que proporcionan los centros de datos de las nubes: ofrecen menores costos de hardware, energía, mantenimiento de las instalaciones y personal de infraestructura. En lugar de congelar fondos en equipamiento tradicional se puede realizar una inversión en otras iniciativas de negocio.

02. Eficiencia operativa

El 47 % de los bancos encuestados citó la eficiencia operativa como una de las principales razones para implementar nube.
La nube permite aprovisionar rápidamente recursos en todo un ecosistema para montar soluciones a medida, acelerar los tiempos de resolución de problemas y agilizar la respuesta a las demandas de un mercado en constante cambio.
También permite mayor eficiencia operativa mediante la optimización de la infraestructura, el *middleware* y las aplicaciones más recientes. De esta manera, los bancos pueden dejar atrás los sistemas *legacy* de menor calidad.

03. Impulsar la innovación

La adopción de la nube permite derribar las barreras de la geografía, la industria y la organización. Además, facilita la creación rápida de prototipos para una rápida experimentación. Sorprendentemente, al menos el 75 % de los bancos encuestados sostuvo que a través de sus iniciativas de nube más exitosas lograron expandirse hacia nuevas industrias, crear nuevas fuentes de ingresos e incrementar su cartera de productos y servicios.

No solo Lift-and-Shift

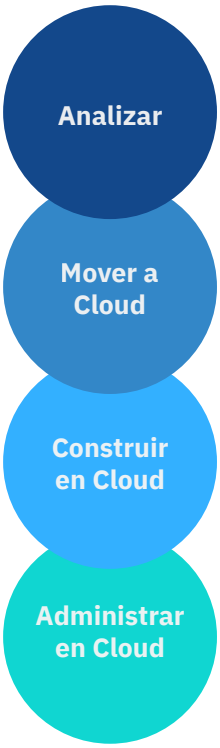
Lo primero que se debe tener en cuenta es que una empresa no se vuelve digital únicamente por migrar cargas: la nube es un medio, no un fin.
La mayoría de las empresas tiende a confundir el traslado de los sistemas de TI a la nube con una estrategia de transformación; si bien es posible tener un modelo exitoso de SaaS o PaaS, estas no son las únicas alternativas y no siempre permiten extraer el máximo beneficio de la nube.
Tomar las aplicaciones *legacy* y trasladarlas a la nube (Lift and Shift) puede no representar grandes beneficios para la solución; en algunos casos ese enfoque puede dar lugar a arquitecturas de TI más complejas, engorrosas y costosas que dificultan la obtención de financiamiento para proyectos más afines a nube.

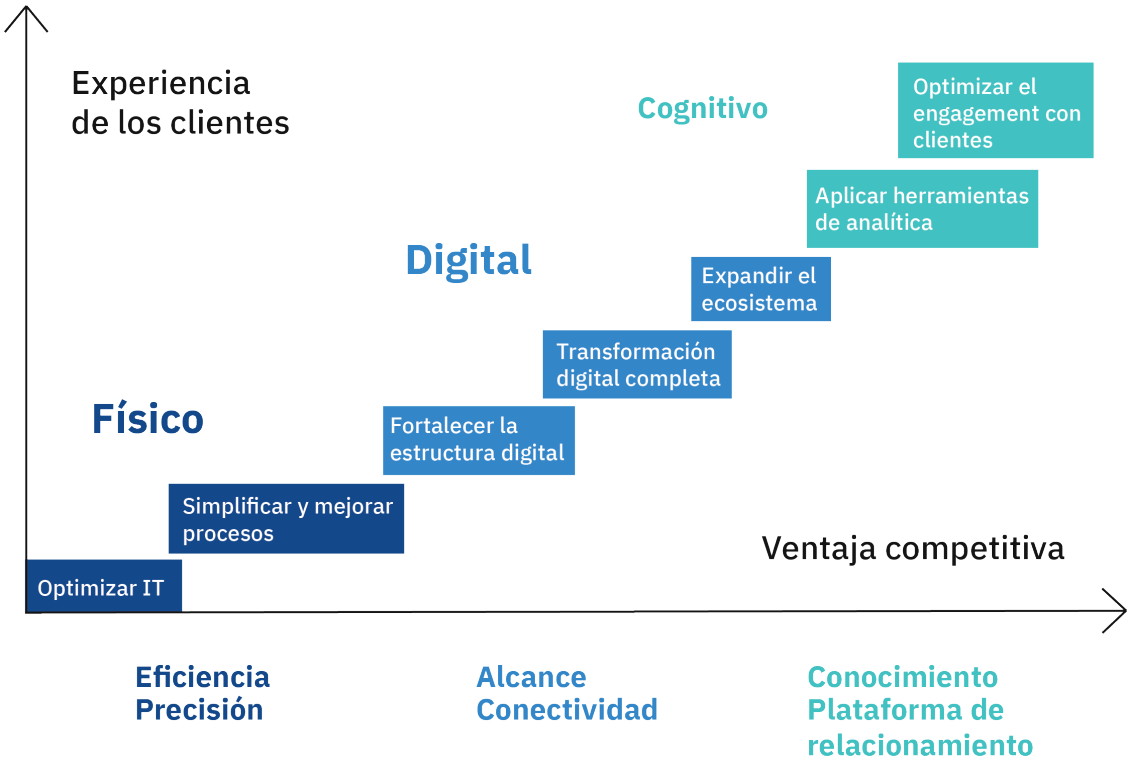
El camino hacia la nube es difícil sin ayuda

Desde IBM entendemos que migrar a la nube no es tarea una sencilla: requiere planeamiento, seguimiento y una guía de ruta clara.

Para eso creamos el Journey To Cloud (J2C): una solución que ayuda a nuestros clientes en todo el proceso de adopción, basada en nuestro profundo conocimiento de la industria, experiencia, metodología y tecnología probada.

IBM guía al negocio a través de la transición a infraestructura de Cloud y en la adopción de la transformación digital.





Beneficios del Journey to Cloud

- Visibilidad y control de cualquier combinación de nube (on-premise, híbrida, multinube, pública, privada o la tradicional TI).
- Método Garage para ayudar a adquirir nuevos conocimientos, innovar y ofrecer verdadero valor empresarial haciendo que las migraciones a la nube sean predecibles, seguras y rápidas.
- Aplicaciones abiertas desde el nacimiento, que permiten la portabilidad y reducen el *vendor lock-in*.
- Agilidad y reducción del *time-to-market* de los nuevos desarrollos.
- Migración y modernización a plataformas multinube un 25 % más rápidas.
- Herramientas cognitivas para la migración a nube y automatización para impulsar soluciones que mejoran el rendimiento y reducen el costo.
- Mejor experiencia del cliente y mayor participación de los socios.
- Procesos comerciales optimizados con una mayor productividad y calidad.
- Nuevos modelos de negocio a partir de un nuevo panorama de empresa digital.

05.

Seguridad en la nube

La seguridad de los datos alojados en la nube

Hasta ahora nos enfocamos en cuestiones de infraestructura o tendencias a nivel global; incluso derribamos algunos mitos. Pero nada de esto es factible si tanto IBM como las entidades financieras no pueden garantizar la seguridad de los datos.

La nube de IBM es segura y de nivel empresarial

IBM Cloud posee más de 60 centros de cómputos distribuidos por todo el mundo. Todos contemplan medidas de seguridad de (al menos) Tier III con control de acceso 24/7, fuentes de alimentación, red y refrigeración redundantes.

Con un catálogo que se destaca por las amplias opciones de despliegue de servicios (como VMware as a service, servicios nativos de nube y Red Hat OpenShift) está equipada para satisfacer los requisitos específicos de las instituciones de servicios financieros.

IBM Cloud está preparada y diseñada para aprovechar todas las capacidades de protección de datos, seguridad y servicios, lo que la hace ideal para cargas de trabajo de misión crítica y manipulación de datos altamente sensibles.

Un marco normativo sólido para los servicios financieros

IBM ayuda a las instituciones financieras a cumplir con sus obligaciones legales en un marco de políticas seguro y rentable pensado para abordar las medidas de seguridad y reglamentos de los bancos siguiendo las mejores prácticas de nube. El cumplimiento se puede demostrar en forma continua.

Para garantizarlo se despliega un modelo de responsabilidad compartida para la aplicación de controles aprovechando IBM Promontory® para la gobernanza: una solución diseñada en base a más de 450 políticas bancarias, reglamentos de la industria y mejores prácticas de nube que permite asegurar que la plataforma se mantenga a la vanguardia de los cambios en las regulaciones.

¿Por qué adoptar IBM Cloud para las cargas operativas?

IBM Cloud es la opción predilecta para soluciones de arquitectura híbrida y multinube. IBM ofrece la escalabilidad, seguridad, integración y resistencia necesarias para ejecutar las cargas de trabajo más críticas de los clientes sin comprometer la visibilidad o el control garantizando el aislamiento de datos necesario y con el respaldo de las certificaciones y reglamentos de protección más exigentes del mercado.

Tanto si se trata de aplicaciones basadas en contenedores sobre Kubernetes y RedHat OpenShift, como de entornos completos virtualizados con VMware, las políticas de seguridad y cifrado son transversales a toda la plataforma.

Centros de datos globales

Con casi 60 centros de datos en 6 continentes, IBM ofrece una arquitectura de nube que permite identificar en dónde están los datos y las aplicaciones.

IBM está comprometida con la protección de la privacidad de los datos. Si bien no hay un enfoque único, cumple con leyes de privacidad de datos en todos los países y territorios en los que opera.

Al momento de crear la infraestructura, contratar un servicio de IBM Cloud o crear réplicas para alta disponibilidad o *backup* (en un mismo *data center*, en una misma o distintas regiones) es el cliente quien decide en dónde ubicar su infraestructura de nube y sus datos, ya sea por necesidades de regulación o por requerimientos de arquitectura, lo cual no se modificará a menos que sea expresamente solicitado.

Liderazgo en seguridad de los datos con soluciones líderes de mercado para protección de la información

La protección de datos es una misión crítica para IBM. Los servicios de IBM Cloud están diseñados para proteger el contenido y datos propietarios. El acceso a los datos se controla estrictamente, en línea con los programas internos de monitoreo y auditoría de usuarios privilegiados de IBM.

IBM está alineada a los requerimientos del nuevo Reglamento General de Protección de Datos de la Unión Europea (GDPR) y refuerza su compromiso permanente con la privacidad por diseño. Esto permite mejorar los controles para limitar el acceso a los datos personales, incluso en lo que respecta a las aplicaciones móviles que se basan en configuraciones predeterminadas.

IBM Cloud fue diseñada teniendo en cuenta las exigentes demandas de las organizaciones más grandes y complejas del mundo. Utiliza la misma tecnología criptográfica en la que confían las instituciones financieras más prestigiosas.
Los datos que un cliente almacena en IBM Cloud son de su propiedad, por lo que puede disponer de ellos. De hecho, los clientes pueden poseer sus propias llaves sin las que nadie puede acceder - ni siquiera IBM - y pueden construir y ejecutar aplicaciones comerciales básicas y cargas de trabajo con visibilidad de un solo tablero y portabilidad multiplataforma.

1. **Encriptación de datos End-to-End, con un control exhaustivo:** IBM ofrece la tecnología criptográfica de punta más fuerte de la industria por medio de IBM Cloud Hyper Protect Crypto Services. Este servicio proporciona la capacidad única de “guardar su propia clave” (KYOK) basada en la certificación FIPS 140-2 Nivel 4 y otorga a los clientes la posibilidad de mantener el control de sus propias claves de encriptación y los módulos de seguridad de *hardware* que las protegen.

2. **IBM Security Advisor:** detecta configuraciones vulnerables para que las organizaciones puedan evaluar mejor sus posturas de seguridad y tomar medidas correctivas.

3. **Seguridad centrada en el *workload*:** Cada carga de trabajo requiere varias reglas de acceso y seguridad; IBM permite a las organizaciones definir y aplicar dichas directrices mediante la seguridad integrada de los contenedores y DevSecOps para aplicaciones nativas en la nube con IBM Cloud Kubernetes Service.

06.

Normativa local

Comunicación A 6354/17 del BCRA

IBM, como parte de la mesa de innovación financiera, colaboró con la revisión de la normativa, responsabilidades y formas de acompañar a sus clientes de la industria en el proceso de transformación en consonancia con el cumplimiento de las reglamentaciones vigentes.

Requerimiento:
Las entidades financieras podrán tercerizar servicios de TI previa comunicación a la Superintendencia de Entidades Financieras y Cambiarias ("SEFyC") con al menos 60 días de anticipación al inicio de dichos servicios.

¿Cómo ayuda IBM a cumplir?
IBM puede ayudar a las entidades financieras durante el proceso de notificación a la SEFyC brindando toda la información necesaria sobre los productos y servicios de IBM Cloud que requiera el ente regulador.

Requerimiento:
En el contrato de tercerización de servicios de TI deberá indicar:
- El compromiso de ambas partes de cumplir con las regulaciones técnicas correspondientes.
- La facultad de la SEFyC para auditar periódicamente el cumplimiento de dichas condiciones.

¿Cómo ayuda IBM a cumplir?
IBM cumple con leyes de privacidad de datos en todos los países y territorios en los que opera. El servicio de IBM Cloud adhiere a todas las legislaciones que la afectan como prestadora de servicios informáticos para entidades financieras.

Del mismo modo, los contratos de IBM Cloud para entidades financieras incluyen aclaraciones particulares que apuntan a la necesidad de realizar visitas de auditorías a aquellos centros de cómputos donde el cliente tenga almacenada su infraestructura y datos, previa coordinación con el equipo de soporte local y en la medida que dicha auditoria no comprometa la seguridad de los datos de IBM o de cualquiera de sus clientes.

Requerimiento:
Las entidades financieras deben implementar un Punto de Acceso Unificado emplazado en la República Argentina.

¿Cómo ayuda IBM a cumplir?
Los servicios de IBM Cloud permiten que los usuarios controlen y monitoreen tanto los servicios de nube que se encuentran en el catálogo como su información. Asimismo, IBM Argentina cuenta con personal especializado que puede validar el cumplimiento de este punto o crear las políticas de acceso y seguridad que se requieran.

Requerimiento:
Las entidades financieras deben desarrollar, planificar y ejecutar un Programa de Seguridad de la Información con el objetivo de proteger los activos, procesos, recursos técnicos y humanos relacionados con los Servicios de Tecnología Informática ("STI") tercerizados.

¿Cómo ayuda IBM a cumplir?
IBM tiene un fuerte foco en la seguridad como premisa de base. Los servicios de IBM Cloud se encuentran sujetos a las normas más estrictas de seguridad y privacidad de los datos, control de accesos y auditorías periódicas de carácter internacional (como CSA STAR, ISO, SOC, entre otras). Información adicional sobre las características de seguridad de la información en IBM Cloud:
https://www.ibm.com/ar-es/cloud/security
https://www.ibm.com/cloud/compliance/global

Requerimiento:
Las entidades deben adquirir y desarrollar los mecanismos para la verificación de la identidad y privilegios de los usuarios internos y externos estableciendo una estrategia basada en la disponibilidad, la reducción de la complejidad de uso y la maximización de la protección de la información del cliente.

¿Cómo ayuda IBM a cumplir?
IBM Cloud ofrece alternativas para que sus clientes puedan monitorear y administrar identidades y accesos.

Requerimiento:
Las entidades deben garantizar un registro y trazabilidad completa de las actividades de los STI tercerizados en un entorno seguro para su generación, almacenamiento, transporte, custodia y recuperación.

¿Cómo ayuda IBM a cumplir?
En IBM Cloud los datos son propiedad de los clientes, quienes tienen total control sobre ellos. IBM Cloud prioriza la confidencialidad de los datos de sus clientes; por este motivo, está diseñada a partir de patrones de arquitectura que impiden, incluso a IBM, acceder a los datos que sus clientes poseen en su infraestructura.
Cumplido el ciclo de vida del servicio o del equipamiento, IBM saneará de forma segura los soportes físicos para su reutilización y destruirá aquellos que no se reutilizarán, de conformidad con las directrices del Instituto Nacional de Estándares y Tecnología.
Si se lo solicita, IBM puede proporcionar evidencia y acreditación del cumplimiento con lo indicado, como certificados, declaraciones o informes procedentes de auditorías externas independientes y acreditadas (como normas ISO 27001, SSAE SOC 2 y otras normas del sector).

Requerimiento:
Las entidades deben contar con recursos técnicos y humanos dispuestos para asegurar un control permanente y continuo de todos sus STI tercerizados y una clasificación de los eventos registrables, así como patrones de búsqueda y correlación.

¿Cómo ayuda IBM a cumplir?
Los servicios de IBM Cloud cuentan con mecanismos personalizables para el registro, auditoría y control de acceso para cumplir con los requerimientos de monitoreo y control.

Requerimiento:
Las entidades deben contar con recursos técnicos y humanos especializados en la atención, diagnóstico, análisis, contención, resolución, escalamiento e informe de los incidentes de seguridad de todos sus STI tercerizados.

¿Cómo ayuda IBM a cumplir?
IBM cuenta con recursos locales y globales para asistir a los clientes durante el eventual caso en que se deba investigar cualquier tipo de falla en el servicio y proporcionar información detallada sobre causas, mecanismos de control, medidas de mitigación y cualquier otra acción que deba tomarse a fin de resolver el problema, alineados con un estricto protocolo de Gestión de Incidentes.

Requerimiento:
Las entidades financieras deben establecer criterios de continuidad y recuperación para cada uno de los STI tercerizados y contar con los recursos técnicos y humanos, así como los planes necesarios para garantizar la continuidad operativa según la demanda de cada servicio, el soporte técnico y logístico, la recuperación de datos y sistemas aplicativos y el procesamiento alternativo en contingencia.

¿Cómo ayuda IBM a cumplir?
Para ello es importante conocer la criticidad de la solución en términos de la continuidad del negocio del cliente. IBM, por su parte, cuenta con sistemas de redundancia y continuidad de servicio a nivel centro de cómputos, tanto para accesos de red, como de energía y refrigeración. Cada arquitectura debe ser analizada al momento de su diseño, con el objeto de validar requerimientos como una copia de alta disponibilidad para fortalecer estos aspectos. Los especialistas y arquitectos de IBM Argentina pueden acompañarlos en este análisis y ofrecer las mejores alternativas para garantizar la continuidad de los entornos y del servicio.

Requerimiento:
La entidad financiera y el prestador del STI tercerizado deberán cumplir con la Ley de Protección de los Datos Personales cuando el servicio involucre la recolección y uso de datos personales, lo que deberá reflejarse en los acuerdos del STI .

¿Cómo ayuda IBM a cumplir?
El contrato de servicios de IBM Cloud posee aclaraciones y adendas incorporadas específicamente para cumplir con los requisitos de privacidad y seguridad establecidos por la Ley de Protección de los Datos Personales.

Ley de protección de datos personales

Conforme lo establecido en la Ley de Protección de Datos Personales de Argentina y sus normas reglamentarias, cuando una entidad transfiera datos de sus clientes a un proveedor de Servicios en la Nube cuyos centros de cómputos se encuentren en el exterior de Argentina se requiere que la transferencia sea efectuada a países que proporcionan niveles de protección adecuados según la ley argentina o, en caso que la jurisdicción no sea reconocida como tal (por ejemplo, Estados Unidos de América), la entidad y su proveedor de servicios en la nube deberán firmar un acuerdo de transferencia internacional de datos -también conocido como DTA por sus siglas en inglés- de conformidad con el texto requerido por la ley argentina a tal efecto.

IBM ofrece para todos sus servicios en nube un DTA que satisface los requerimientos de la ley argentina, incluyendo la Disposición 60/2016 de la Autoridad de Protección de Datos de Argentina en donde se compromete a tomar medidas exhaustivas para que los datos de los clientes estén seguros y sean procesados conforme a la ley.

IBM presta sus servicios de nube a un gran número de empresas argentinas, tanto del sector financiero como de otras industrias; en todos los casos se rige por las mismas normativas y regulaciones de seguridad y protección de los datos, las cuales adhieren a la legislación argentina, incluyendo las medidas de seguridad técnicas y organizacionales a las que se refiere la Disposición 11/2006 de la Autoridad de Protección de Datos de Argentina y otras de carácter internacional.

Conclusión

¿Qué nos llevamos de este documento?

- La seguridad de que no existe una normativa que impida a las empresas del sector financiero argentino hacer uso de servicios de nube.

- IBM es un socio estratégico para acompañar a sus clientes en el proceso de adopción de la tecnología de nubey para ofrecer guía sobre el cumplimiento de los requerimientos de la normativa local.

Recomendaciones finales

- **La renovación de los sistemas centrales es esencial para responder a la demanda de los clientes y adaptarse rápidamente a los entornos cambiantes.** Permite trabajar directamente en la experiencia de usuario, excelencia operacional y cumplimiento al mismo tiempo.

- **Una arquitectura de tres capas, estándares modulares, orquestación y la integración con soluciones de terceros** son características que definen una solución moderna y escalable con visión de futuro y asegurarán una arquitectura flexible, abierta y segura.

- **La migración del *core* bancario a la nube presenta una rara oportunidad** para lograr objetivos que podrían parecer contradictorios: reducir los costos y aumentar la agilidad, flexibilidad y escalabilidad. Basándose en la nube, la banca puede acelerar el crecimiento y automatizar las operaciones y los flujos de trabajo, lo que resulta en una mayor eficiencia y seguridad.
Una adopción efectiva de metodología y tecnología de nube será el punto de inflexión que determinará qué bancos emergerán y cuáles se quedarán atrás de sus competidores.

- **La arquitectura de contenedores y basada en microservicios** permite implementaciones elásticas y escalables bajo demanda, con la libertad que otorga la capacidad de desplegarlas en donde sea necesario. Además, puede centrarse en el desarrollo de nuevas soluciones integradas a las preexistentes, para luego migrar y ajustar las arquitecturas.

- **La estandarización, configuración y la automatización** permiten dar un giro a la operatoria de TI de la industria bancaria, acelerar la innovación, la digitalización y todo el ecosistema de fintech.

07.
Glosario

API: "Application Programming Interface". Interfaz que permite a las aplicaciones de terceros solicitar datos y recibirlos en un formato predefinido y de acuerdo a normas específicas. Constituye el mecanismo más utilizado de comunicación entre aplicaciones.

App: Término utilizado comúnmente como abreviatura de *application software*, un programa informático diseñado para ayudar al usuario a realizar una serie de tareas específicas. Las aplicaciones pueden ser estándares o desarrolladas a medida para cubrir necesidades particulares.

***Backup*:** Copia de seguridad que se realiza sobre ficheros o aplicaciones contenidas en un ordenador con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales. Los dispositivos más empleados para llevar a cabo la técnica de *backup* pueden ser cintas magnéticas, DVDs, discos duros, discos ópticos, USBs o servicios remotos de copias de seguridad.

BPM: "Business Process Management". Tipo de gestión empresarial que consiste en la integración de los procesos, las personas y los sistemas tecnológicos de una compañía en aras de facilitar el desarrollo de las estrategias de negocio.

Ciberseguridad: Sistemas y principios que tienen como objetivo proteger los sitios y las aplicaciones web de los atacantes que quieren interrumpir, retrasar, modificar o redirigir el flujo de datos. Los atacantes pueden tener objetivos, niveles de organización y capacidad técnica diferente, por lo que las empresas públicas y privadas deben adoptar cada vez más medidas para evitar los ciberataques.

Cloud Ready: Arquitecturas, soluciones, *software* o servicios que están preparados para que una aplicación sea desplegada independientemente de la infraestructura subyacente.

Datos del cliente: Toda información personal/financiera del cliente que permita revelar o inferir su identidad, credenciales personales, relación comercial y/o posición financiera, limitada, restringida y/o protegida por la Ley de Datos Personales (Ley 25.326), la Ley de Entidades Financieras (Ley 21.526) y normas particulares del BCRA.

GDPR: Es el Reglamento General de Protección de Datos (GDPR por sus siglas en inglés). Es el nuevo marco legal en la Unión Europea que regula el uso de datos personales y la forma en la que las organizaciones los procesan, almacenan y destruyen.

ISO27001: Estándar para la seguridad de la información. Especifica los requisitos necesarios para establecer, implementar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según la metodología del Plan-Do-Check-Act (Planificar-Hacer-Verificar-Actuar).

Nube pública: Modelo tradicional de nube en donde el prestador de estos servicios pone a disposición de cualquier usuario su infraestructura. Cabe destacar que aunque este servicio esté disponible para todos, los archivos que estén alojados en esta nube son privados.

Nube privada: Ofrece los mismos servicios que la nube pública, pero en infraestructura dedicada y no compartida. Ya sea en un centro de cómputos propio, alquilado o externo.

Nube híbrida: Combinación de las mejores características de los modelos de nube privada y pública.

***On-premise*:** Modelo referido al esquema tradicional de licenciamiento. La empresa adquiere las licencias que le otorgan derecho de uso de los sistemas del proveedor, los integra en sus propias instalaciones y mantiene sus datos dentro de su propia infraestructura de tecnología.

PaaS: "Platform as a Service". Plataforma como Servicio es una oferta de computación en nube que proporciona a los usuarios un entorno de nube en el que pueden desarrollar, gestionar y entregar aplicaciones.

SaaS: "Software as a Service". *Software* como Servicio es una aplicación completa ofrecida como un servicio.

TI: Tecnologías de la Información.

***Virtualization*:** Representación basada en *software* (o virtual) de una entidad física. Puede ser una plataforma de *hardware*, un sistema operativo, un dispositivo de almacenamiento o cualquier otro recurso de red.

Más información

Servicios de IBM Cloud
https://www.ibm.com/ar-es/cloud

Seguridad en IBM Cloud
https://www.ibm.com/ar-es/cloud/security

Certificaciones IBM Cloud
https://www.ibm.com/ar-es/cloud/compliance

Servicios de IBM para industria bancaria
https://www.ibm.com/ar-es/cloud/banking

Casos de referencia y recursos
https://www.ibm.com/industries/banking-financial-markets/resources/back-office/secure/

IBM Cloud Paks
https://www.ibm.com/cloud/paks/

Sobre IBM Argentina
https://www.ibm.com/ar-es/about

Contacto

Román Zambrano
CTO
romazan@ar.ibm.com

Santiago Bisso
Business Development Executive
bissourr@ar.ibm.com

Estefanía Zmaragdis
Cloud Architect
zmara@ar.ibm.com

Créditos

Autor:
Germán Santini
Solutions Architect
Banking and Finance Industry

Colaboradores:
Estefanía Zmaragdis
IBM Cloud Architect

Juliana Moriones
Hybrid Cloud Specialist

Julieta Romero
Hybrid Cloud Specialist

Camila Scalzo
Content Writer

Sabrina Cinzer
IBM Media Design

Verónica Casillo
IBM Media Design

IBM Corporation
IBM Global Markets (o división apropiada, o ninguna división)

IBM Argentina
IBM Catalinas: Ingeniero Butty 275.CP: C1001AFA, Buenos Aires Argentina
IBM Campus Tecnológico: Hipólito Yrigoyen 2149, Martínez. CP:1640

Producido en Argentina, junio 2020.

IBM Cloud Services