



IBM Cloud for Financial Services

Acelere la innovación y responda a sus necesidades
de seguridad y cumplimiento



Un sector que se enfrenta a la disrupción

Hoy en día, la industria de servicios financieros se enfrenta a numerosas fuerzas disruptivas, lo que incluye la demanda cada vez mayor de los clientes de servicios innovadores y personalizados; la intensa competencia de las empresas tecnológicas, las fintech y los operadores tradicionales; la creciente presión regulatoria; el aumento de las amenazas de ciberseguridad; y la necesidad de talento cualificado para hacer frente a todo lo anterior.

Para innovar más rápido y transformarse, muchas instituciones financieras buscan cada vez más el cloud para ayudarles a modernizar las aplicaciones existentes, otorgar mayor flexibilidad y agilidad, y asociarse con distribuidores de software independientes (ISV), proveedores de software como servicio (SaaS) y fintechs. Al aprovechar al máximo las tecnologías del cloud, las instituciones financieras pueden remodelar las experiencias de los clientes, optimizar las operaciones y desbloquear potencialmente nuevos modelos de ingresos.

Sin embargo, IBM ha observado que muchas instituciones financieras se abstienen de mover sus cargas de trabajo principales y datos confidenciales al cloud debido al tremendo riesgo para la seguridad cibernética y las crecientes complejidades normativas. Según un informe patrocinado por IBM Security, el coste promedio de una megavulneración en los servicios financieros fue de 401 millones de dólares a partir de 2021 y el coste promedio de una vulneración de datos aumentó un 10 % de 2020 a 2021.¹ Comprometer la seguridad o el cumplimiento normativo simplemente no es aceptable.

Para que las instituciones financieras sean competitivas, deben continuar migrando las cargas de trabajo principales al cloud para ayudar a acelerar la transformación digital y reducir sus costes, al tiempo que mantienen sus datos confidenciales y las cargas de trabajo críticas seguras y en conformidad. Para lograr esto, las instituciones financieras necesitan un cloud creado con las prestaciones específicas de supervisión del cumplimiento normativo y de seguridad que requiere la industria.

Las instituciones financieras necesitan una opción que permita la transparencia en el traslado de sus cargas de trabajo y aplicaciones al cloud y, con IBM Cloud for Financial Services™, el cloud público se convierte en una opción cada vez más estratégica para acelerar eficientemente la transformación digital.

Un cloud desarrollado para la industria

IBM Cloud for Financial Services es el primer cloud público de este tipo desarrollado para el sector con las capacidades de seguridad y control necesarias para ayudar a los clientes a mitigar el riesgo y acelerar la adopción del cloud, incluso para sus cargas de trabajo más confidenciales, mientras trabajan.

Nuestro cloud está diseñado para ayudar a los clientes a automatizar su posición de seguridad y cumplimiento y supervisarla con seguridad y controles integrados en la plataforma, que no se ofrecen como herramientas adicionales ni funciones personales. También cuenta con prestaciones de seguridad y privacidad líderes en la industria y se ve reforzado por el profundo conocimiento de las operaciones de TI de IBM, su experiencia en la industria y un amplio conjunto de socios de ecosistema seleccionados.

El resultado es un entorno seguro diseñado para ayudar a los clientes a reducir el riesgo y el coste de migrar datos confidenciales al cloud, modernizar las cargas de trabajo e integrar rápidamente las prestaciones necesarias para hacer avanzar su negocio.

Las instituciones financieras ahora pueden aprovechar los beneficios del cloud público al mismo tiempo que abordan sus requisitos de ciberseguridad y cumplimiento normativo. Ya no es necesario elegir entre innovación y gestión de riesgos.

Acelere la innovación, mitigue su riesgo

IBM Cloud for Financial Services, el primer cloud creado en colaboración con la industria, está diseñado para acelerar la innovación y ayudar a reducir el riesgo y el coste de migrar datos al cloud.



Aborde sus requisitos de cumplimiento con una plataforma de controles comunes creada en la industria.



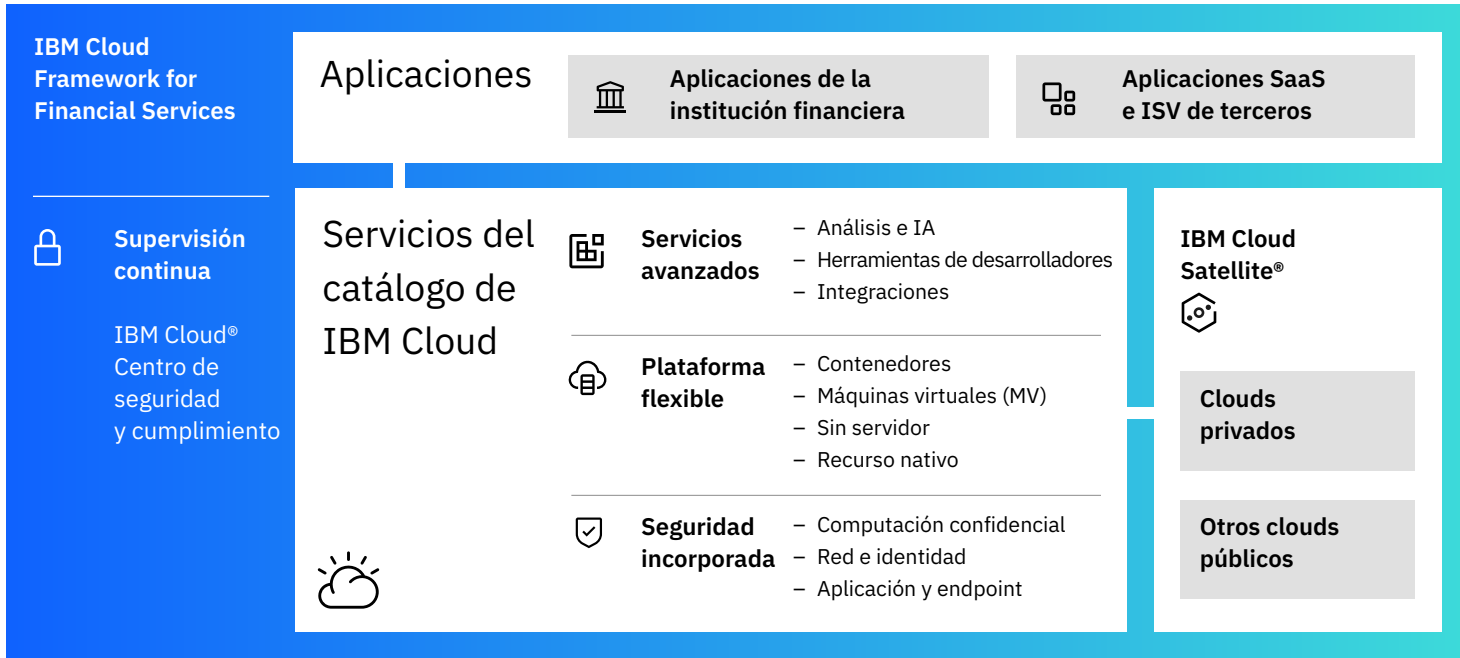
Acelere la innovación con un ecosistema de ISV, fintechs y proveedores de SaaS.



Proteja los datos con prestaciones de seguridad líderes en la industria.



Opere con alternativas y agilidad a través de las opciones de implementación del cloud híbrido.



IBM Cloud for Financial Services aprovecha un marco respaldado por la industria con seguridad y controles preconfigurados que IBM aplica mediante programación a los servicios de IBM Cloud, las aplicaciones de terceros y las cargas de trabajo de la institución.

El marco de control, central para nuestra plataforma

El núcleo de nuestra oferta es un marco de control llamado IBM Cloud Framework for Financial Services. El marco se desarrolló para ayudar a las instituciones financieras a automatizar su posición de seguridad y cumplimiento para que les resultase más fácil a ellas y a sus socios de la cadena de suministro digital simplificar su gestión de riesgos y demostrar su cumplimiento normativo.

El marco de control proporciona una estructura de seguridad y cumplimiento para todo el ecosistema a través de un conjunto común de controles preconfigurados y automatizados que se aplican en servicios de IBM Cloud®, aplicaciones de terceros y cargas de trabajo de instituciones financieras. Los controles, creados en colaboración con las principales instituciones financieras, están alineados con los estándares de la industria y los organismos reglamentarios globales. Se valida continuamente con el asesoramiento del IBM Financial Services Cloud Council, compuesto por los principales CIO, CTO, CISO y responsables de cumplimiento y riesgo de instituciones financieras, y con la orientación de Promontory Financial Group®, una empresa de IBM y líder mundial en consultoría de cumplimiento normativo. El marco evoluciona y los controles se adaptan a los requisitos emergentes de la industria y las obligaciones reglamentarias para ayudar a las instituciones financieras a mitigar el coste y la complejidad del cumplimiento en un panorama normativo y de seguridad cibernética en constante evolución. El amplio conjunto de controles dentro de IBM Cloud Framework for Financial Services incluye, entre otros, seguridad, protección de datos, gestión de acceso y gestión de configuración.

Controles integrales alineados con los estándares de la industria y las reglamentaciones globales

<p>7</p> <p>Áreas de atención</p> <ul style="list-style-type: none"> – Cumplimiento y gestión de riesgos prioritarios – Protección de datos avanzada – Autenticación mejorada y administración de acceso – Protección automatizada de aplicaciones y cargas de trabajo – Resiliencia y seguridad de infraestructura unificada – Excelencia operativa – Supervisión de respuesta activa <p>A partir de abril de 2022</p>	<p>21</p> <p>Familias de control únicas</p>
	<p>280</p> <p>Controles</p>
	<p>565</p> <p>Requisitos de control</p>

[Más información sobre IBM Cloud Framework for Financial Services →](#)

Un amplio catálogo de soluciones ISV, fintech y SaaS

IBM Cloud for Financial Services cuenta con el respaldo de un selecto ecosistema de ISV, fintech y proveedores de SaaS para ayudar a que las instituciones financieras incorporen aplicaciones y servicios de terceros de manera más fácil y rápida, y comiencen a trabajar con ellos en nuestro cloud.

A través del Centro de seguridad y cumplimiento de IBM Cloud®, las posiciones de seguridad y cumplimiento de las aplicaciones y los servicios de los socios se pueden automatizar y supervisar continuamente y, a su vez, recoger pruebas. Como resultado, se pueden reducir los pasos manuales en el proceso de gestión del cumplimiento de las aplicaciones de los socios, se puede minimizar el potencial de error humano y se pueden mejorar la consistencia, la trazabilidad, la auditabilidad y la escalabilidad. Con la automatización, las organizaciones también pueden reducir la variabilidad entre auditorías, proporcionando informes valiosos y consecuentes y eliminando demoras mientras mantienen un cumplimiento constante.

El Centro de seguridad y cumplimiento de IBM Cloud

El Centro de seguridad y cumplimiento de IBM Cloud ayuda a los clientes a supervisar y hacer cumplir sus controles para proteger datos y activos y administrar vulnerabilidades en entornos de cloud. Para permitir que las instituciones financieras supervisen la posición de seguridad y cumplimiento de sus servicios cloud, además de las aplicaciones y los servicios de los socios, IBM proporciona la plataforma y el panel de control de seguridad y cumplimiento como parte de una cuenta de IBM Cloud. Los clientes y socios pueden definir perfiles de cumplimiento, administrar controles y mantener un extenso registro de datos para auditoría. Esto puede ayudar a promover una cultura de cumplimiento dentro de la organización que comienza con la configuración de recursos y se mantiene a través de la recopilación de pruebas de auditoría.

La reciente integración de Tanium Comply en el Centro de seguridad y cumplimiento de IBM Cloud permite a los clientes con cargas de trabajo reguladas analizar su experiencia al tener la capacidad de ver los resultados de la evaluación de cumplimiento de Tanium desde dentro del Centro de seguridad y cumplimiento de IBM Cloud. Con Tanium Comply, los clientes pueden ver sus datos de cumplimiento asociados con IBM Cloud y Tanium en el mismo formato en una sola ubicación. La integración de Tanium permite a los clientes de IBM Cloud ampliar las capacidades de gestión de endpoints de su organización para incluir el análisis de vulnerabilidades y errores de configuración según los estándares de seguridad de la industria y las definiciones de vulnerabilidad.

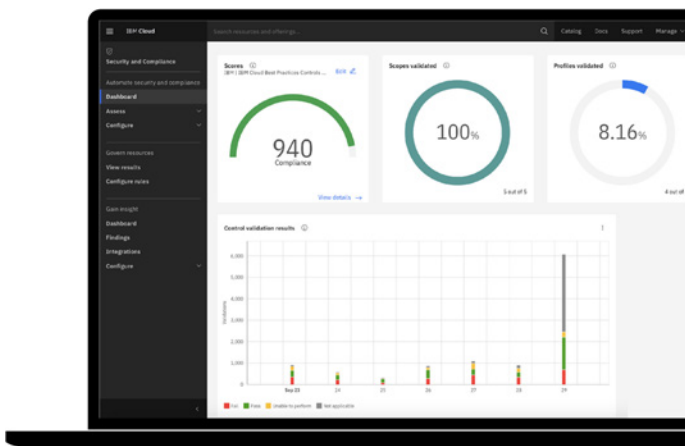
Controles de seguridad y protección de datos líderes de la industria, con un enfoque zero trust

IBM Cloud for Financial Services se ha diseñado teniendo en cuenta las necesidades exactas de las organizaciones más grandes y complejas del mundo. Se basa en todas las prestaciones y los servicios de seguridad y protección de datos integrados en el cloud público de IBM, lo que permite su uso para cargas de trabajo críticas y datos altamente confidenciales. IBM ofrece un cloud público de nivel empresarial con amplias opciones de implementación de servicios, como VMware y Red Hat® OpenShift® como servicio, y está equipado para cumplir con los requisitos específicos de los servicios financieros.

Dentro de IBM Cloud for Financial Services se incluyen tecnologías fundamentales para administrar el riesgo de seguridad y el cumplimiento normativo con un enfoque zero trust centrado en los datos.

Computación confidencial

IBM adopta un enfoque holístico de la computación confidencial, que abarca la informática, los contenedores, las bases de datos y el cifrado. La computación confidencial ayuda a los clientes a eliminar la confianza implícita que las aplicaciones depositan en la pila de software subyacente y los proveedores del cloud, para que pueda pasar de medidas operativas a medidas técnicas y proteger la privacidad de sus datos confidenciales en reposo, en tránsito y en uso. Esto puede permitir a los clientes migrar datos confidenciales y cargas de trabajo al cloud, con lo cual crean nuevas formas de colaborar e innovar. Si bien es imposible prevenir por completo las filtraciones de datos en el entorno de cloud híbrido conectado actual, un enfoque zero trust centrado en los datos puede ayudar a las instituciones financieras a modernizar las operaciones e incorporar controles de seguridad, y está diseñado para mitigar el impacto y el coste de una vulneración de datos.

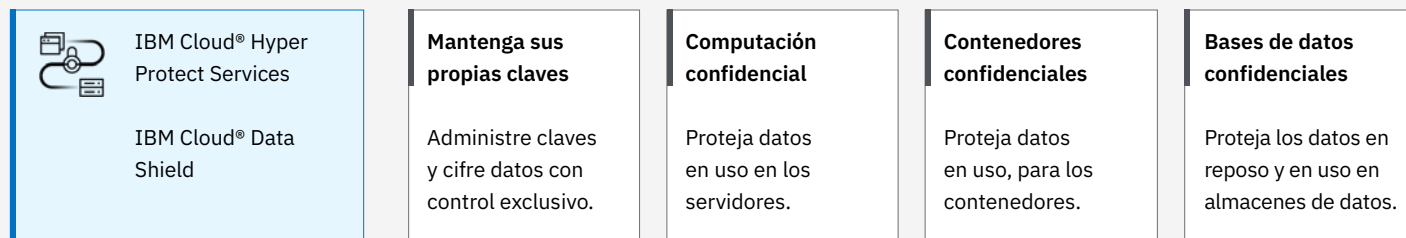


Centro de seguridad y cumplimiento de IBM Cloud

Zero trust: seguridad integrada en la red, la identidad, los endpoints y las aplicaciones

Computación confidencial de IBM: un enfoque holístico para proteger los datos en tránsito, en reposo y en uso

Tecnologías y prestaciones habilitadas



Cifrado de extremo a extremo con amplio control

Nuestro cloud de servicios financieros también ofrece un enfoque de administración de claves líder en la industria que técnicamente brinda a los clientes un control exclusivo de sus datos. Ni siquiera IBM puede acceder a ellos.² IBM Cloud® Hyper Protect Crypto Services permite el cifrado de datos en el cloud en un módulo de seguridad de hardware (HSM) dedicado del cloud. El servicio ofrece tecnología como “KYOK” (Mantener sus propias claves), un servicio de gestión de claves de un solo arrendatario que cuenta con almacenamiento de claves proporcionado por HSM dedicados y controlados por el usuario y que está diseñado para admitir los estándares de cifrado de la industria, como los estándares de criptografía de clave pública (PKCS) n.º 11. También es el único servicio cloud de la industria basado en hardware con certificación FIPS 140-2 de nivel 4. En este nivel de seguridad, los mecanismos de seguridad física pueden proporcionar una envoltura de protección alrededor del módulo criptográfico con la intención de detectar y responder a los intentos no autorizados de acceso físico.

Con este tipo de protección de datos, el cliente es el único que gobierna y controla el acceso a sus datos privados. Estas prestaciones pueden cambiar las reglas del juego de la industria de servicios financieros, que necesita cumplir con estrictos requisitos normativos de protección de datos.

IBM Cloud for Financial Services se basa en servicios adicionales integrados en el cloud público de IBM que también pueden utilizarse para cargas de trabajo críticas y datos confidenciales.

Seguridad centrada en la carga de trabajo por defecto

Cada carga de trabajo requiere varias reglas de acceso y seguridad. IBM permite que las organizaciones definan y apliquen dichas pautas mediante la seguridad integrada de contenedores y DevSecOps para aplicaciones nativas del cloud con Red Hat OpenShift como servicio.

Regiones multizona (MZR)

Los clientes pueden aprovechar las prestaciones subyacentes de IBM Cloud for Financial Services para mejorar la capacidad de



resiliencia empresarial y la recuperación tras desastres. Las MZR comprenden múltiples zonas de disponibilidad interconectadas de alta velocidad y baja latencia que son independientes entre sí para ayudar a limitar el impacto de los eventos de falla única a una sola zona de disponibilidad, únicamente. Permiten a las instituciones financieras ubicar cargas de trabajo en puntos geográficos específicos para satisfacer sus necesidades.

Reglas de registro y auditoría

Los proveedores de SaaS e ISV deben registrar todas las acciones realizadas a través del portal en el cloud, la API o la interfaz de línea de comandos para que se registren en detalle utilizando el rastreador de actividad de IBM Cloud®. Esto proporciona un registro estándar de actividad en sistemas y servicios y un registro de sesión completa de exactamente qué acciones realizan los operadores. Esta información se almacena y analiza centralmente. El proceso de registro es auditable para permitir el seguimiento de todos los pasos, incluido el registro de eventos correctos e incorrectos, y brinda protección basada en roles en todos los puntos de intervención. Los registros de acceso se almacenan junto con marcas de tiempo para facilitar el análisis y la investigación forense.

Modernización y transformación del negocio más rápido con IBM Cloud for Financial Services

Para ayudar a los clientes a modernizar y transformar su negocio más rápido con IBM Cloud for Financial Services, IBM confluye con los clientes “en el punto en que se encuentren” en la transición para adoptar el cloud al abordar los casos de uso más importantes para ellos, lo que incluye:

- Tratamiento del cumplimiento normativo en los datos y las cargas de trabajo de la cadena de suministro interna y digital
- Protección de datos confidenciales en el cloud con un enfoque zero trust centrado en los datos
- Migración segura de cargas de trabajo virtualizadas al cloud
- Desarrollo y gestión seguros de aplicaciones nativas del cloud en contenedores

Hable con su representante de IBM para realizar nuestra evaluación de controles sin coste y comprender cómo el cloud o el marco de control de seguridad y la tecnología de su institución financiera se alinean con IBM Cloud Framework for Financial Services. Para obtener más información y acceder a recursos adicionales, visite la página web [IBM Cloud for Financial Services](#).

Notas finales

1. *Informe Coste de la vulneración de datos 2021*, IBM Security y Ponemon Institute, julio de 2021. <https://www.ibm.com/es-es/downloads/cas/OJDVQGRY>
2. Basado en IBM Hyper Protect Crypto Services, el único servicio cloud de la industria basado en hardware con certificación FIPS 140-2 de nivel 4. En este nivel de seguridad, los mecanismos de seguridad física pueden proporcionar una envoltura de protección alrededor del módulo criptográfico con la intención de detectar y responder a los intentos no autorizados de acceso físico.

© Copyright IBM Corporation 2022©

IBM España, S.A.

Santa Hortensia, 26-28
28002 Madrid

Producido en los Estados Unidos de América
Julio de 2022

IBM, el logotipo de IBM, IBM Cloud for Financial Services, IBM Cloud, IBM Cloud Satellite y Promontory Financial Group son marcas comerciales o marcas comerciales registradas de International Business Machines Corporation, en los Estados Unidos y/o en otros países. Los demás nombres de productos y servicios pueden ser marcas comerciales de IBM u otras empresas. Puede consultar una lista actualizada de las marcas comerciales en ibm.com/trademark

VMware es una marca comercial registrada o marcas comerciales de VMware, Inc. o sus filiales en los Estados Unidos y/u otras jurisdicciones.

Red Hat y OpenShift son marcas comerciales o marcas registradas de Red Hat, Inc. o sus filiales en los Estados Unidos y otros países.

Este documento está actualizado en la fecha inicial de publicación e IBM puede modificarlo en cualquier momento. No todas las ofertas están disponibles en todos los países en los que opera IBM.

Es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier otro producto o programa con los productos y programas de IBM. LA INFORMACIÓN DE ESTE DOCUMENTO SE OFRECE "TAL CUAL ESTÁ" SIN NINGUNA GARANTÍA, NI EXPLÍCITA NI IMPLÍCITA, INCLUIDAS, ENTRE OTRAS, LAS GARANTÍAS DE COMERCIALIZACIÓN, ADECUACIÓN A UN FIN CONCRETO Y CUALQUIER GARANTÍA O CONDICIÓN DE INEXISTENCIA DE INFRACCIÓN. Los productos de IBM están garantizados según los términos y condiciones de los acuerdos bajo los que se proporcionan.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

El cliente es responsable de garantizar el cumplimiento de las leyes y reglamentos aplicables. IBM no presta asesoramiento legal ni declara o garantiza que sus servicios o productos aseguren que el cliente cumpla con cualquier ley o reglamento. Las declaraciones relativas a la dirección e intención futuras de IBM están sujetas a cambios o a su retirada sin previo aviso, y representan únicamente metas y objetivos.

