



Conocimientos extraídos de la investigación

Dominio del cloud híbrido



Cómo puede ayudar IBM Consulting

IBM Consulting es un nuevo socio para las nuevas reglas de la empresa moderna. Nosotros adoptamos una forma de trabajar abierta que reúne un conjunto diverso de voces y tecnologías. Colaboramos estrechamente, pensamos con libertad y somos ágiles al aplicar innovaciones revolucionarias que generan un impacto exponencial capaz de cambiar la manera de hacer negocios. Creemos que los ecosistemas, tecnologías, innovación y culturas de carácter abierto son claves para que tanto las empresas modernas como el mundo accedan a nuevas oportunidades y avancen. Queremos trabajar juntos, crear juntos y replantear juntos los límites de lo posible. Para obtener más información, visite: ibm.com/es-es/consulting.

Dominio del cloud híbrido

En IBM tenemos la suerte de conocer el panorama global de los resultados que están obteniendo las empresas con la adopción del cloud híbrido para generar valor empresarial. Nuestro trabajo más interesante y desafiante es con los clientes que están dejando atrás las primeras fases de adopción del cloud y avanzando hacia un dominio del cloud híbrido mucho más profundo y orientado a los negocios.

Sentemos las bases con algunas grandes ideas.

John Granger

Vicepresidente sénior, IBM Consulting

Dominio del cloud híbrido: grandes ideas

El cloud híbrido es una estrategia poderosa para la transformación de los negocios y la innovación en una empresa moderna.

Para dar paso a la mejora transformadora del rendimiento empresarial, debemos ser capaces de emplear software y datos a escala, de forma segura y rápida, en todo el entorno informático de la empresa. Para esto, por supuesto, está el cloud. Para una empresa grande, especialmente una que se esté transformando rápidamente en una empresa virtual, el listón está más alto. Presentamos la empresa virtual como el destino deseado para la transformación empresarial de nueva generación en un informe relacionado.¹

Debido a la gravedad de los datos, los requisitos de seguridad y normativos, y la complejidad de las aplicaciones críticas para la misión, es poco común que un solo cloud público sea la opción adecuada. La transformación de empresas exige innovación abierta y un mayor valor empresarial. Eso es lo que ofrece el cloud híbrido. Una solución que abarca los centros de datos convencionales, sistemas mainframe, múltiples clouds (privados y públicos), aplicaciones de software como servicio (SaaS) y aplicaciones o datos que se ejecutan en el Edge.

Este pragmático enfoque del cloud híbrido multiplica por 2,5 el valor que ofrece el uso de un único cloud público.² Una plataforma de cloud híbrido puede integrar aplicaciones que se ejecutan en múltiples clouds, con lo cual mueve los datos de forma segura en todo el patrimonio de cloud, mejorando así los procesos y flujos de trabajo empresariales que abarcan múltiples clouds. Una plataforma de cloud híbrido simplifica e integra diversos elementos de un patrimonio de cloud de gran magnitud, y los convierte en una sola estructura coherente de prestaciones.

Por lo tanto, la simplificación e integración del entorno de TI es el objetivo principal de dominar el cloud híbrido, y ese dominio puede otorgar cuatro palancas distintivas de valor:

- Desarrolle las aplicaciones una vez e impleméntelas en cualquier parte.
- Gestione las aplicaciones una vez y alójelas en cualquier parte.

- Desarrolle competencias una vez e impleméntelas en cualquier parte.
- Inove en cualquier parte con tecnología de terceros.

La simplificación e integración del cloud híbrido también proporcionan un mayor acceso a un rango más amplio de propuestas de valor. Veamos esto en detalle.

Cuando hablamos de un mayor acceso, nos referimos a que más personas pueden desarrollar e implementar más software, así como acceder a los datos subyacentes y usarlos. Entonces, ¿cómo se combina ese mayor acceso con el cloud híbrido? Pensemos en el cloud híbrido como la red de transporte de una ciudad: del mismo modo que tener múltiples rutas expande el acceso de la población, contar con múltiples formas de cloud hace que las prestaciones valiosas del cloud estén a disposición de todas las personas de la empresa.

Cuando hablamos de un rango más amplio de propuestas de valor, nos referimos a que el cloud híbrido puede llevarle a muchos más destinos de su lista durante su búsqueda de valor empresarial. Actualmente, puede mover fácilmente solo una pequeña porción de sus aplicaciones al cloud público. Por eso vemos este gran movimiento hacia el cloud híbrido.

Somos muy optimistas con respecto al camino para obtener valor con el cloud híbrido.

En las primeras etapas de la adopción del cloud se obtiene valor, pero creemos que el cloud híbrido orientará sus planes basados en datos y software más transformadores de cara a mejorar la prestación de servicios y la entrega de productos a sus clientes.

Además, al fomentar la apertura y la cohesión en todo el ecosistema, el cloud híbrido abre la puerta a un mayor valor empresarial mediante la expansión de la innovación.

Considere algunos de los datos recientes:

- El cloud híbrido se ha convertido en la forma de abordar el cloud entre las grandes empresas: el 97 % de las organizaciones ya usan más de un único cloud.³
- El cloud híbrido se ha convertido en una inversión empresarial de primer nivel. Nuestros datos más recientes

muestran que el gasto en cloud híbrido como cuota del gasto en TI ha aumentado en dos cifras, mientras que el gasto en el cloud público como cuota del gasto en TI ha disminuido recientemente en algunos sectores.

- Dominar el cloud híbrido se ha convertido en un motor central de la transformación. De hecho, otro estudio reciente de IBM estima que el valor de las inversiones en el cloud híbrido se multiplica hasta por 13 en promedio cuando se combina con otras palancas de transformación. En algunos sectores, el valor llega a multiplicarse por cifras tan altas como 20.⁴

Si la transición al cloud no llega al dominio del cloud híbrido, las fuentes profundas de valor siguen quedando fuera del alcance.

Algo que sucede con demasiada frecuencia es que los programas de adopción del cloud pierden impulso antes de que las inversiones del programa comiencen a dar frutos. La adopción a nivel aficionado no llega a alcanzar el punto de inflexión en el cual el ROI de las mejoras en rendimiento empresarial se equilibra y sobrepasa los costes de implementación del cloud.

A modo ilustrativo: en una encuesta reciente, casi un tercio de los que adoptaron el cloud indican que están estancados en la mitad de sus transiciones y otro 37 % comenta que no quiere seguir adelante después de migrar tan solo una mínima carga de trabajo.⁵ ¿Por qué? Uno de los motivos es que están observando aumentos imprevistos en los costes operativos a medida que añaden más proveedores de cloud o pasan al cloud más funciones empresariales.

Existen muchos motivos por los cuales la adopción del cloud híbrido puede no alcanzar las expectativas, pero hay una temática que se mantiene constante en cada historia del terreno: la archienemiga de la transición al cloud híbrido es la complejidad. Como sucede con todos los archienemigos, la complejidad se puede vencer. Hemos identificado cinco desafíos clave y lo que puede hacer para sortearlos, además de cómo el dominio del cloud híbrido puede acelerar el valor empresarial con mayor apertura, innovación y transformación.

La palabra definitiva

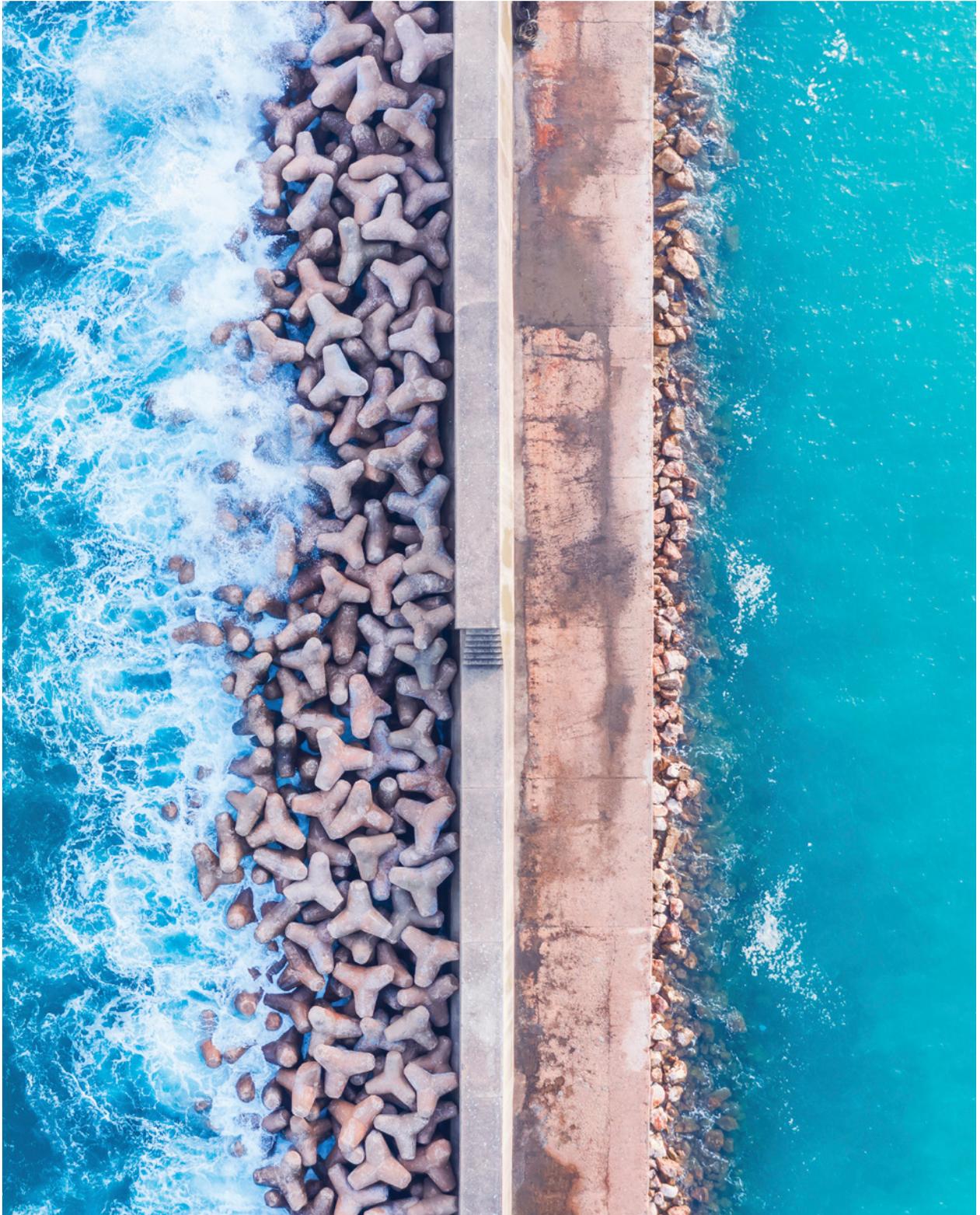
¿Qué es el cloud híbrido?

Usamos el término *cloud híbrido* para describir una combinación de entornos de cloud que incluye cloud público, cloud privado y multicloud, así como infraestructura local. Nuestros datos demuestran que durante la pandemia muchas organizaciones empezaron a usar el cloud híbrido como consecuencia de decisiones tácticas tomadas por los departamentos de usuarios, TI y compras.

Sin embargo, más allá de esta combinación de entornos, usamos el término *plataforma de cloud híbrido* para describir cierto nivel de integración que abarca infraestructura local, cloud público, cloud privado y multicloud, y cada vez más edge computing y cloud distribuido. Si se hace bien, la plataforma de cloud híbrido proporciona un tejido para la orquestación, gestión y portabilidad de aplicaciones en todos estos entornos. El resultado puede ser un entorno informático distribuido flexible, abierto, unificado y único donde la organización puede ejecutar y escalar sus cargas de trabajo tradicionales y nativas en cloud en el modelo informático más adecuado.

Por último, usamos el término *dominio del cloud híbrido* para describir una forma altamente evolucionada de utilizar su plataforma de cloud híbrido que mejora (e incluso transforma) el rendimiento empresarial de base.

Cinco desafíos comunes en la transición hacia el cloud híbrido.



Los cinco desafíos

El camino hacia el dominio del cloud híbrido

En nuestro trabajo con clientes de todo el mundo observamos cinco desafíos comunes en la transición hacia el cloud híbrido. Pero estos no son insuperables. La verdad es que probablemente haya resuelto desafíos similares en el pasado, solo que no lo ha hecho en el contexto específico de una estrategia de cloud híbrido. Hay cinco cosas pragmáticas y simples que puede hacer hoy para llegar a dominar el cloud híbrido.

		Desafío	Adopción	Dominio
1	El desafío de la arquitectura	Cómo poner orden en un patrimonio de cloud saturado, simplificar el entorno de TI y definir una arquitectura para ofrecer una única plataforma segura de cloud híbrido.	La adopción del cloud simplemente apila cloud sobre cloud.	El dominio del cloud híbrido integra los activos de cloud de acuerdo con una visión clara y convincente del cloud híbrido, comenzando con una arquitectura de plataforma de cloud híbrido que define un tejido de servicios cloud en múltiples entornos.
2	El desafío de las personas y las operaciones	Cómo domesticar al monstruo de Frankenstein de cada cloud generando su propio silo operativo y limitando la eficiencia y eficacia del trabajo de las personas.	La adopción del cloud simplemente monta piezas de talento en el cloud en prácticas de trabajo aisladas.	El dominio del cloud híbrido desarrolla equipos de creativos inteligentes y expertos en el cloud, diseña flujos de trabajo que descargan de tareas a esas personas para que hagan su mejor trabajo (de forma eficiente y eficaz) en toda la plataforma y guía la evolución de un único modelo operativo de cloud híbrido.
3	El desafío de seguridad	Cómo gestionar y promover el avance de la seguridad del cloud híbrido como deporte de equipo, integrando los dominios separados de seguridad en el cloud para formar un plan de juego integral con el fin de defenderse de los adversarios cibernéticos.	La adopción del cloud genera el riesgo de ampliar la superficie de ataque a la seguridad y es susceptible de fallar en un entorno multicloud.	El dominio del cloud híbrido desarrolla un programa de seguridad unificado que orienta las iniciativas empresariales, optimiza los recursos de seguridad y transforma la cultura operativa para poner la seguridad en primer lugar.
4	El desafío financiero	Cómo entender las inversiones, los costes y los retornos del cloud, y gestionar todo el patrimonio híbrido como una cartera unificada.	La adopción del cloud simplemente gestiona las facturas de cloud individuales.	El dominio del cloud híbrido gestiona todos los costes del cloud en una sola vista y captura las oportunidades para optimizar costes y reasignar recursos.
5	El desafío del ecosistema de socios	Cómo llevar nuevos socios a una mesa de capitanes dedicada para generar capital social y priorizar el éxito de los clientes sobre los intereses de cada actor.	La adopción del cloud administra simplemente los contratos individuales con socios.	El dominio del cloud híbrido reúne a todos los socios en un ecosistema voluntario y multilateral, alineados bajo una estrategia para el éxito.

El dominio del cloud híbrido integra los activos de cloud según una visión clara y convincente del cloud híbrido.



Desafío 1

El desafío de la arquitectura

Cómo poner orden en un patrimonio de cloud saturado, simplificar el entorno de TI y definir una arquitectura para ofrecer una única plataforma segura de cloud híbrido.

El proceso de adopción del cloud se limita a apilar un cloud sobre otro. *El **dominio del cloud híbrido** integra los activos de cloud de acuerdo con una visión clara y convincente del cloud híbrido, comenzando con una arquitectura de plataforma de cloud híbrido que define un “tejido” de servicios cloud en múltiples entornos.*

La COVID-19 ha actuado como detonante de la adopción del cloud híbrido. La pandemia ha exigido que más empresas ofrezcan una mayor parte de sus productos y servicios por internet, y que lo hagan con urgencia. Tanto es así que ahora el 97 % de las organizaciones afirman que están en varios clouds.⁶ De hecho, se prevé que la empresa promedio pase de los ocho clouds que tenía en 2020 a diez clouds para 2023.⁷ Las aplicaciones de SaaS también han explotado: muchos procesos empresariales estándar se migraron al cloud.

Lamentablemente, esta necesidad urgente de acción incitó a las organizaciones a montar sus entornos de cloud actuales en una combinación ad hoc de recursos públicos, privados y locales, los cuales podrían funcionar juntos de forma útil o no. Sin guardarrailles arquitectónicos, las presiones relativas a la implementación llevan a tomar atajos, lo cual hace que el entorno de TI sea más complejo y costoso, menos seguro y con menos probabilidades de dar mejores resultados empresariales. No sorprende que, por ejemplo, el 71 % de los ejecutivos vean la integración de datos en el patrimonio de cloud como un problema.⁸

El problema no yace en los recursos informáticos en sí. Los clouds públicos forman los cimientos de una estrategia de cloud híbrido y hay buenos motivos para tener más de un cloud público. Los clouds privados son esenciales en los sectores altamente regulados. Algunos recursos no se pueden mover a un cloud público, pero de igual forma pueden beneficiarse de los principios básicos del cloud computing. Por ejemplo, un sistema mainframe se puede ejecutar “como un servicio” que los consumidores pagan a medida que usan.

Poner orden en un patrimonio de cloud saturado

Si tiene una colección de componentes cloud individuales, pero no hay una estructura cohesiva detrás, es como si tuviera un taller desordenado con piezas de coches aleatorias desperdigadas. Es probable que tenga todo lo necesario para construir un vehículo que funcione, pero está muy lejos de tener uno en realidad, mucho menos de conducirlo hacia el destino que quiere alcanzar.

Una arquitectura de aplicaciones y una única plataforma integral de cloud híbrido son el chasis sobre el cual montará y conectará todas las piezas. En lugar de los componentes específicos que logran poco de forma individual, es el sistema completo lo que puede llevarlo hacia donde desea ir: es decir, una mejora drástica en el desarrollo y la producción de aplicaciones de software. Puede implicar una mayor agilidad, velocidad e innovación empresarial. Sus inversiones en el cloud podrían comenzar a generarle un valor empresarial real. Quizás incluso mayor de lo que preveía.

Comience con estos tres pasos para poner en orden un patrimonio de cloud saturado.

Paso 1: Visualice una arquitectura de aplicaciones y una única plataforma integral de cloud híbrido totalmente alineadas con la empresa.

El dominio implica pasar de un “híbrido de clouds” (varios clouds que compiten en lugar de complementarse) a una plataforma única integral de cloud híbrido. La plataforma presta servicios de producción de software altamente automatizados e integrados a los usuarios de toda la empresa. La plataforma optimiza la prestación y el consumo de servicios a través de un “mercado” conveniente y rentable para servicios de cloud híbrido. También define las zonas de aterrizaje que permiten a los usuarios empezar a usar la plataforma con un nivel reducido de carga técnica y administrativa.

Complemente la plataforma con una arquitectura de aplicaciones alineada con la empresa que respalde una innovación abierta. Una arquitectura de plataforma de cloud híbrido necesita un marco complementario orientado a los negocios que guíe las decisiones respecto al funcionamiento de las aplicaciones en un entorno de cloud híbrido. ¿Una aplicación va a un cloud público? Si es así, ¿qué cloud público? ¿Pertenece a un cloud privado? ¿Es necesario que permanezca en el centro de datos? ¿Se puede retirar la aplicación? ¿Y cómo se interconectan las aplicaciones y los datos en diversos dominios y ecosistemas empresariales?

El dominio del cloud híbrido ofrece una opción muy diferente. Idealmente, algunas aplicaciones deberían rediseñarse como un conjunto de componentes reutilizables para que la aplicación se convierta en un conjunto de pequeños fragmentos de lógica empresarial que admite “composición”. Esta idea no es nueva (busque “arquitectura orientada a servicios” en sus libros de historia de TI), pero las tecnologías actuales de plataforma de cloud híbrido,

contenedores y microservicios hacen que sea factible a escala empresarial. Esta es una de las formas en las que entra en juego el superpoder que tiene el cloud híbrido para “desarrollar aplicaciones una vez e implementarlas en cualquier parte”. Los desarrolladores crean los microservicios una vez y pueden reutilizarlos posteriormente en aplicaciones que se ejecuten en cualquier lugar del patrimonio de cloud.

Las aplicaciones que admiten composición no son solo para los desarrolladores, sino que hay una gran idea de valor empresarial bajo la superficie de tono tecnológico. Ver las aplicaciones como fragmentos de lógica empresarial requiere comprender profundamente lo que deben hacer las aplicaciones para incrementar el rendimiento empresarial: ¿de qué forma las prestaciones de desarrollo de software que está creando devolverán valor a los patrocinadores de la empresa? Realizar esta conexión es el objetivo principal de prácticas como el diseño guiado por el dominio (DDD), pues el “dominio” es un dominio empresarial que estamos mejorando con lanzamientos rápidos de aplicaciones que admiten composición. Y dichas aplicaciones son productos montados a partir de microservicios.

Lumen Technologies, una empresa multinacional de telecomunicaciones con sede en EE. UU., buscaba expandir y mejorar la compatibilidad con nuevos conjuntos de aplicaciones de proceso intensivo de clientes en el Edge, pero le preocupaban la resiliencia y la velocidad de sus prestaciones actuales.

Luego de adoptar potentes prestaciones de cloud híbrido para incrementar la velocidad y seguridad, Lumen consiguió ofrecer a los clientes una nueva consola de cloud centralizada a través de la cual se podían desarrollar y orquestar fácilmente aplicaciones Edge en toda la empresa a nivel global.⁹

Paso 2: Desarrolle su plataforma de cloud híbrido de la misma forma que desarrollaría un producto orientado al cliente.

Todo lo que sabe sobre desarrollar productos digitales (como tratamos en el paso 1) se transfiere directamente al trabajo de desarrollar una plataforma de cloud híbrido. Tenga en cuenta que la plataforma de cloud híbrido (el producto que está desarrollando) está destinada a la prestación de servicios. Está prestando esos servicios de la plataforma cloud a los clientes, y son los clientes quienes definen qué es “valor”. Definir los principios de design thinking centrados en el cliente al inicio del desarrollo de la plataforma puede generar un gran beneficio a la hora de empezar a lanzar servicios de la plataforma.

Para ilustrar esto, una *postal desde el terreno*: vemos a muchas empresas grandes con plataformas cloud grandes, costosas y que hacen mucha publicidad de su TI. Sin embargo, casi nadie está usando la plataforma. A pesar de que parece un método estándar en la empresa, no funciona de esa forma.

¿Por qué? Es posible que los desarrolladores de la plataforma olvidaran obtener las opiniones de sus clientes (los desarrolladores que deben usar el sistema). Para alcanzar el nivel óptimo de utilidad, la plataforma de cloud híbrido abierta debería usar una estrategia de “crowdsourcing”, es decir, estar creada por desarrolladores para desarrolladores. Han dado con la manera de distribuir software en su entorno actual, así que su nueva plataforma tiene que ofrecerles formas mejores, más rápidas y más sencillas de hacer su trabajo. Como indica Andrew Clay Shafer de Red Hat, “Si *uno* la desarrolla, huirán. Si uno deja que *ellos* la desarrollen, vendrán”.

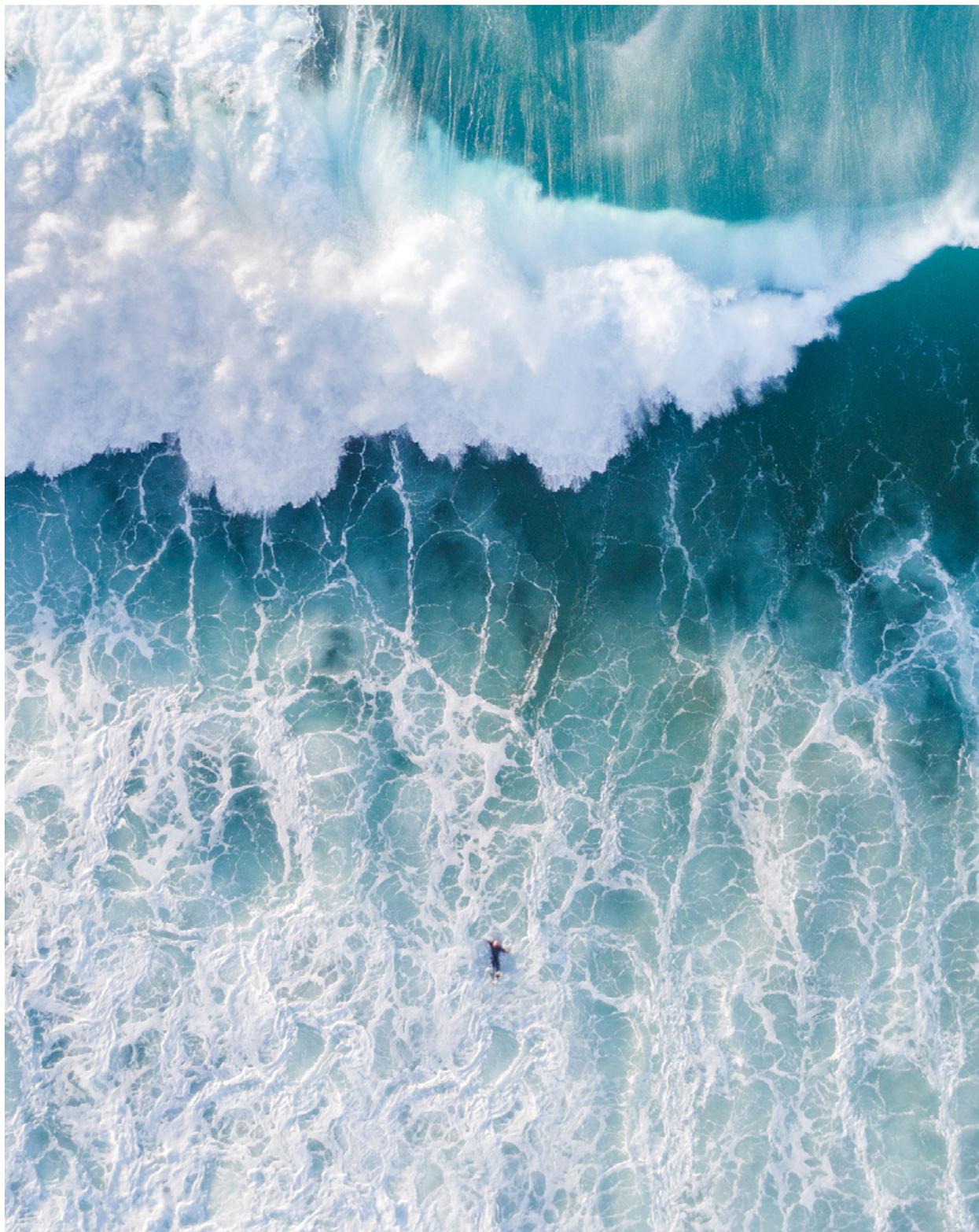
Concentrarse en los trabajos pendientes de los desarrolladores de la misma forma en que desarrolla productos para los clientes de pago no implica que no se puedan satisfacer también las necesidades de TI de la empresa. Simplemente haga que el método de trabajo apropiado en la plataforma sea el más sencillo. Adapte el diseño del servicio de la plataforma para que el camino con menos obstáculos sea desarrollar en la plataforma nueva en lugar de en los antiguos silos. Después, la plataforma comenzará a funcionar de una manera constante y conforme que incrementa la seguridad.

Paso 3: Defina el punto óptimo en el que el plan de TI de la empresa para el desarrollo de la plataforma de cloud híbrido avanza al ritmo del plan de la empresa para incrementar el rendimiento.

El punto óptimo es aquel donde el desarrollo de su plataforma, la prestación de servicios, las prácticas técnicas nativas en el cloud, etc., se limitan a igualar las iniciativas de mejora del rendimiento e innovación orientadas al cloud que patrocina la empresa.

A medida que desarrolla su plataforma de cloud híbrido, la regla de oro es diseñar, probar, construir y prestar el servicio que más necesita la empresa en ese momento para que muchos clientes lo consuman rápidamente. A continuación, siga experimentando para validar sus decisiones en cuanto al diseño arquitectónico, proporcione pruebas de concepto de ingeniería y arquitecturas técnicas de MVP que pongan a prueba las alternativas de diseño de la plataforma. Mientras tanto, puede generar más valor empresarial.

El dominio del cloud híbrido desarrolla equipos de creativos inteligentes y expertos en el cloud, y diseña flujos de trabajo que descargan de tareas a esas personas para que hagan su mejor trabajo.



Desafío 2

El desafío de las personas y las operaciones

Cómo domesticar al monstruo de Frankenstein de cada cloud generando su propio silo operativo y limitando la eficiencia y eficacia del trabajo de las personas.

La adopción del cloud simplemente monta piezas de talento en el cloud en prácticas de trabajo aisladas. *El dominio del cloud híbrido desarrolla equipos de creativos inteligentes y expertos en el cloud, diseña flujos de trabajo que descargan de tareas a esas personas para que hagan su mejor trabajo (de forma eficiente y eficaz) en toda la plataforma y guía la evolución de un único modelo operativo de cloud híbrido.*

El monstruo de Frankenstein es el resultado de operaciones cloud remendadas con piezas de habilidades, prácticas, métodos y flujos de trabajo. El trabajo se hace en focos y silos pequeños a medida en toda la empresa. Las formas de trabajar previas al cloud han quedado obsoletas con el transcurso del tiempo, las formas de trabajo nativas en el cloud todavía no han echado raíces, pero están emergiendo diferentes silos de habilidades. Por lo tanto, todavía estamos lejos de la integración e interoperabilidad que promete el cloud híbrido. El monstruo de Frankenstein es enorme, fuerte y difícil de matar. A menudo es una fuerza abrumadora que bloquea el progreso hacia el dominio del cloud híbrido.¹⁰

Los datos de las investigaciones validan el poder del monstruo. En una encuesta reciente, el 84 % de los ejecutivos reconocieron las dificultades de sus empresas para eliminar las transferencias de silo a silo.¹¹ Y un 78 % de los ejecutivos dicen que un modelo operativo inadecuado impide la adopción exitosa de su plataforma multicloud.¹²

La escasez de talento es una de las formas en que se presenta el monstruo. Simplemente no hay suficientes arquitectos de cloud, desarrolladores de microservicios e ingenieros de datos a los que recurrir, sobre todo si el grupo de talentos está disperso en silos del cloud. De hecho, en nuestra investigación, 4 de cada 5 ejecutivos dicen que no cuentan con profesionales suficientes para gestionar una plataforma de cloud híbrido.¹³

El monstruo también puede ser una fuente de confusión para el modelo operativo. No es difícil entender el modelo operativo actual; y siempre hay uno, aunque no esté volcado por escrito. Tampoco es un desafío insuperable la tarea de definir el estado deseado del futuro. Gestionar cómo ir del punto A al punto B puede ser difícil: ¿Cómo se ven los estados intermedios? Y ¿cómo abre el camino cada estado intermedio para la siguiente evolución?

Si se hace bien, el diseño del modelo operativo puede convertirse en el superpoder de la organización para incorporar prácticas de trabajo conectadas, eficientes y nativas en cloud en todo el entorno híbrido, abordando la falta de habilidades, talento y experiencia.

Estos son tres pasos que puede dar hoy para continuar su transición al dominio del cloud híbrido.

Paso 1: Facilite herramientas a un centro de excelencia de cloud para que ponga en marcha un modelo operativo de cloud híbrido y acelere la ejecución.

Los modelos operativos de cloud híbrido tienen muchas piezas móviles, y la mayoría de las empresas no tienen demasiada experiencia en el diseño y ejecución de modelos operativos. Si intenta abordar todo a la vez —el diseño, el trazado de la hoja de ruta y la implementación del modelo operativo—, posiblemente le resulte abrumador. Recomendamos crear un centro de excelencia de cloud (CCoE) para alojar a los expertos en la materia de diversas disciplinas que definan y dirijan la transición a un nuevo modelo operativo y nuevas prácticas de trabajo.

El CCoE debe contar con las herramientas para trabajar en todos los silos de cloud del monstruo de Frankenstein; de lo contrario, hay pocas probabilidades de domar a ese monstruo. Si su programa tiene silos que han tenido tiempo de crecer y segurizarse, retomar la ruta hacia un modelo operativo con un único cloud híbrido podría requerir un alto grado de intervención por parte del CCoE. La meta es disolver los silos en una forma de trabajar común e integrada que sirva a los clientes y empleados mejor que un método fragmentado.

Tenga en cuenta que cambiar cómo trabaja la gente genera fricción. A medida que diseña flujos de trabajo de prestación de servicios en el cloud híbrido y aplica los resultados de la experimentación, trate a los equipos de prestación como clientes. Ayúdelos a responder las siguientes preguntas: ¿Por qué el nuevo modo de hacer las cosas es mejor que el anterior? ¿En qué sentido mi experiencia trabajando de este modo aumenta mi predisposición a probar algo nuevo, aunque sea incómodo?

Para acelerar la ejecución de un modelo operativo de cloud híbrido, es útil tener la capacidad de predecir y anticipar el rango de resultados que se pueden obtener a raíz de los cambios operativos. Ver lo que hay a la vuelta de la esquina requiere invertir en exploradores: un equipo pequeño que esté uno o dos pasos por delante de la implementación actual. La función del explorador es validar los siguientes pasos en el plan de implementación de acuerdo con la marcha del trabajo actual. Esto incluye prever lo que vendrá, recabar datos y aplicar las lecciones aprendidas durante la ejecución del programa. Si es necesario alterar el plan, los exploradores deben justificarlo.

Paso 2: Proporcione a su gente las habilidades y la experiencia que necesitan para prosperar en un modelo operativo de cloud híbrido.

Hay grandes diferencias entre los programas de formación convencionales sobre cómo trabajar en el cloud y los programas que otorgan a las personas las herramientas para dominar el cloud híbrido. La diferencia más sustancial es que con el cloud híbrido, una cadena de herramientas de DevSecOps uniforme y un modelo operativo coherente no es necesario que forme a nadie en cada silo de tecnología y práctica. Puede desarrollar habilidades y ofrecer formación de modo más eficiente y a escala dentro de un entorno de garaje o en otro lugar.

Este dividendo de integración implica que puede emplear algunos principios de diseño de programa de capacitación que, de otro modo, hubieran sido inasequibles, como:

- Ofrecer formación, acreditaciones y certificaciones sobre cloud híbrido “justo a tiempo”, para que los estudiantes apliquen esas habilidades nuevas con rapidez. Hacer el aprendizaje más experiencial asegurándose de que los estudiantes reciben formación sobre cómo aplicar las nuevas habilidades directamente en el contexto de su función en el modelo operativo de cloud híbrido.

- Dirigirse hacia las prácticas verdaderas de DevSecOps enfatizando la manera de aplicar los conjuntos de habilidades y prácticas en un modelo operativo integral e interdisciplinario.
- Ir más allá de formar y entrenar a la gente para que trabaje en equipo; formarla y entrenarla para que trabaje con otros tipos de equipos. Muchas organizaciones comienzan preparando equipos de desarrollo nativos en cloud, ágiles e interdisciplinarios, pero esto es solo el principio. A medida que evoluciona el modelo operativo del cloud híbrido, se torna claro que esos equipos nativos en cloud no trabajan de forma aislada. Tienen que trabajar con una red de diferentes tipos de equipos: equipos de analistas de negocios y responsables de producto, equipos de TI convencionales de back-office, equipos de la oficina de gestión de proyectos (OGP), centros de excelencia, etc. La calidad de la interacción entre esas diversas “topologías de equipos” es al menos tan importante como la interacción de las personas dentro de cada equipo.

A continuación se ofrece un ejemplo de cómo conectar talento y tecnología:

Orange France desarrolló un programa integral de Orange Campus para incrementar las competencias digitales de los empleados. Con estudios de cocreación, se redujeron 150 funciones diferentes a 30, al tiempo que se identificaron 80 competencias digitales para la fuerza laboral del futuro. Orange France reestructuró las vías de formación y elevó la movilidad profesional ayudando a los empleados a adquirir habilidades digitales nuevas (y críticas). ¿Los resultados? El 50 % de la fuerza laboral adquirió nuevas habilidades digitales y hubo un aumento del 150 % en las ventas a clientes en los canales digitales con más de 10 puntos de Net Promoter Score (NPS).¹⁴

Paso 3: Diseñe primero el trabajo necesario para las operaciones de cloud híbrido y después ajuste la gráfica de su organización.

No confunda su modelo operativo de cloud híbrido con la gráfica de su organización.

El diseño del modelo operativo no es nuevo, sino que es una fusión de diseño de modelo de negocios, diseño de flujo de trabajo y diseño de servicio, con algunos principios de producción eficiente incorporados. Pero, para la mayoría de las empresas, la última vez que hicieron algo como diseñar un modelo operativo fue cuando prepararon los mapas de procesos empresariales para admitir implementaciones de ERP. Nuestra experiencia en el sector revela una confusión genuina con respecto a la diferencia entre un modelo operativo y una gráfica de organización.

Los modelos operativos y las estructuras de organización son animales distintos. La principal preocupación del modelo operativo es cómo fluye el trabajo de la prestación de servicios desde la solicitud del cliente hasta la entrega. En contrapartida, la principal preocupación de una gráfica de organización es cómo se estructura la jerarquía y cómo se distribuyen el poder y el control.

En la fase inicial del trabajo de diseño del modelo operativo, algunas partes interesadas se concentrarán en qué nombres (y cuántos) aparecerán en qué recuadros de la gráfica de la organización. No sorprende, pues están evaluando si la nueva forma de operar les será útil o no. Sin embargo, puede coartar una exploración nueva y objetiva del diseño del modelo operativo y debe gestionarse con destreza.

Deje muy claro que el trabajo del modelo operativo es lo primero. Luego, a medida que define no solo el estado deseado, sino también la hoja de ruta de implementación del modelo operativo, piense en los cambios que son necesarios en la gráfica de la organización.

El dominio del cloud híbrido requiere poner a prueba las presunciones de ejecución, aprender rápido y estar siempre preparado para alejarse de los problemas y orientarse hacia las oportunidades.



Desafío 3

El desafío de seguridad

Cómo gestionar y promover el avance de la seguridad del cloud híbrido como deporte de equipo, integrando los dominios separados de seguridad en el cloud para formar un plan de juego integral con el fin de defenderse de los adversarios cibernéticos.

La adopción del cloud genera el riesgo de ampliar la superficie de ataque a la seguridad y es susceptible de fallar en un entorno multicloud. *El dominio del cloud híbrido desarrolla un programa de seguridad unificado que orienta las iniciativas empresariales, optimiza los recursos de seguridad y transforma la cultura operativa para poner la seguridad en primer lugar.*

Amenazas para la seguridad en un entorno híbrido

Antes de que las empresas comenzaran a usar los clouds públicos, sus inquietudes de seguridad aunque eran significativas se limitaban a las aplicaciones, el centro de datos y la red. Añadir incluso un primer cloud público creó un nuevo conjunto de riesgos de seguridad y una necesidad de compartir las responsabilidades de seguridad con un proveedor de servicios cloud. Las cosas se tornaron un poco más complejas y surgieron algunos incidentes notorios. ¿Por qué? Según nuestra investigación, el 80 % de los ejecutivos tiene dificultades para incorporar las disciplinas de operaciones y seguridad de la información con la suficiente antelación como para prevenir el reacondicionamiento y este tipo de incidentes.¹⁵

Avancemos hasta la pandemia, cuando la mayoría de las grandes empresas están migrando a entornos de cloud híbrido, multicloud y con un alto volumen de SaaS; cuando numerosas funciones empresariales se han movido al mundo online; y cuando la fuerza laboral trabaja desde casa o desde la cafetería local. Hemos ampliado drásticamente la superficie de ataques de seguridad, creando un lugar para los actores malintencionados del negocio del phishing y los ataques de ransomware. Y, dicho sea de paso, algunos de estos actores malintencionados son expertos en ciberconflictos patrocinados por el estado.

Las empresas que han montado un patrimonio de cloud saturado y no integrado han asumido mayores riesgos de seguridad: riesgos que son un obstáculo para el dominio del cloud híbrido y que pueden amenazar la resiliencia de la empresa.

Seguridad de cloud moderna: salir de la obstrucción y pasar a la abstracción

El nuevo modelo de seguridad necesario para dominar el cloud híbrido consiste en pasar de la obstrucción a la abstracción. Si se hace correctamente, la seguridad se convierte en una abstracción de la misma forma que la “infraestructura como código” ha convertido la infraestructura física en una abstracción. La complejidad técnica no ha dejado de existir, pero el usuario no se enfrenta a esta directamente.

A modo ilustrativo: en la actualidad, los desarrolladores, científicos de datos y arquitectos de datos pueden aprovisionar un servidor, máquina virtual (MV) o contenedor en pocos minutos. Y no pueden esperar semanas o meses para que la seguridad obstructiva se ponga al día. Por lo tanto, un modelo de seguridad moderno debe alinearse con una infraestructura dinámica de cloud híbrido, mientras avanza al mismo ritmo que la innovación que se produce en la capa de datos y aplicaciones. La seguridad moderna se está convirtiendo en algo ambiental, funciona en segundo plano en todo el patrimonio de cloud híbrido.

Un enfoque ambiental incorpora la seguridad en el proceso de desarrollo de productos de cloud híbrido. Mantiene a los propietarios de sistemas y desarrolladores como responsables del empleo de buenas prácticas en materia de seguridad y privacidad en cada versión del código, hasta el nivel de la carga de trabajo.

El dominio del cloud híbrido exige un abordaje de la seguridad por parte de todo el equipo

Nuestra investigación nos indica que una mayoría significativa de los ejecutivos empresariales (un 73 %, para ser precisos) cree que mejorar la ciberseguridad y reducir los riesgos de seguridad es fundamental para la ejecución exitosa de las iniciativas digitales en su cartera de cloud.¹⁶ Pero no siempre están vinculados directamente en la ejecución. Es común ver un programa de modernización de la seguridad que funciona en paralelo con un programa de adopción del cloud, pero lo hacen bajo distintos patrocinios y sin hojas de ruta integradas explícitamente.

No obstante, la ruta hacia el dominio del cloud híbrido exige que la seguridad empresarial y la seguridad del cloud híbrido jueguen en el mismo equipo, con responsabilidades de seguridad compartidas y una guía de estrategias de seguridad creada en conjunto. En un escenario ideal, las inversiones en el cloud híbrido actúan como disparador para mejorar la seguridad empresarial y vincular las inversiones en seguridad con valor empresarial tangible.

La lista de actores en un equipo de seguridad del cloud híbrido va mucho más allá del CISO, el CIO y el CTO. Incluye patrocinadores del programa de la línea de negocio y responsables de producto. Incluye directores de seguridad, desarrolladores de plataformas cloud y desarrolladores de software de todo el patrimonio de cloud híbrido, así como responsables de activos de cloud de la empresa. Jugar en equipo implica que la seguridad se convierte en una responsabilidad explícitamente compartida, se deja atrás la mentalidad de “Tenía protegidas mis cosas en el cloud; debe haber sido tu culpa”.

Proteger los data fabrics es un ejemplo ilustrativo de trabajo de todo el equipo. Una de las ideas detrás del data fabric es dejar de pensar en las bases de datos (o data lakes, almacenes de datos, data marts, etc.) como almacenes fijos de datos y comenzar a ver los datos más como una red amplia mediante la cual estos fluyen libremente por todo el entorno de TI. Los data fabrics y los clouds híbridos bien dominados son una combinación natural y potente, dado que los primeros reducen el nivel de “gravidad de los datos” que puede limitar las iniciativas de modernización de aplicaciones.

Esta descentralización de los datos facilita la explotación del potencial de mejora del rendimiento del cloud híbrido, pero exige reimaginar cómo proteger esos datos en casos de uso específicos centrados en la empresa. Entonces, no importa quién lidere la iniciativa de data fabric (CDO, CTO, CIO, etc.), diseñar e implementar un data fabric seguro requiere la participación de todo el equipo.

Un método que abarque todo el equipo es más fácil y eficaz si se basa en una cultura consciente de la seguridad más amplia y que dé prioridad a la seguridad. La creación de esta cultura requiere que se proporcionen recursos de aprendizaje que reconozcan las necesidades de diversos públicos de partes interesadas. Los líderes de negocio podrían responder bien al aprendizaje a nivel de concienciación basado en simulaciones. Para las partes interesadas que pertenezcan a la generación digital quizás sea mejor una formación en modo de juego. Los directores de seguridad quizás necesiten una certificación de cloud formalizada. Aproveche plenamente los beneficios de tener una única plataforma cloud, así como políticas y procedimientos de seguridad uniformes y armonizados: los recursos de formación que proporcione pueden ser mucho más específicos, prácticos y relevantes para la función que desempeña cada estudiante del equipo.

Perspectiva

Innovación guiada por el cloud híbrido

Vale la pena resolver los cinco desafíos que plantea el dominio del cloud híbrido descritos en este documento debido a la innovación que hacen posible. El valor económico de las empresas actuales depende en gran medida de su capacidad para llevar a cabo experimentos en el mercado con mucha rapidez usando datos, software y plataformas. Una plataforma de cloud híbrido bien dominada hace que esta innovación de ciclo rápido sea mucho más flexible, rápida y productiva, así como menos costosa, al tiempo que pone los datos al alcance de más innovadores de la empresa. En realidad, la plataforma de cloud híbrido puede permitirle innovar en cualquier lugar con la tecnología de cualquiera.

El funcionamiento del cloud híbrido con datos es fundamental para la innovación basada en software. El dominio del cloud híbrido da acceso a datos de toda la empresa, abriendo así la puerta a una innovación que de otro modo se hubiera visto obstaculizada por silos de datos inaccesibles. Además, la plataforma de cloud híbrido permite que los innovadores vean los datos a través de distintas lentes: los datos que residen en un entorno de ERP (como SAP), en un sistema mainframe o en el Edge ahora pueden verse como información conectada que genera nuevos conocimientos potenciales sobre los clientes, nuevas oportunidades de mercado o la viabilidad de nuevos modelos de negocio.

En entornos aislados, las empresas pueden usar herramientas de automatización para optimizar *partes* de un flujo de trabajo. Reinventar los flujos de trabajo de extremo a extremo en entornos muy heterogéneos (con IA, automatización y datos de clientes) simplemente no es posible sin *un dominio del cloud híbrido*.

El dominio del cloud híbrido le permite innovar en un nivel totalmente superior:

- Reúna la fuerza de diferentes plataformas y tecnologías cloud.
- Organice equipos multidisciplinarios y formados por distintos socios para crear o ejecutar en colaboración.
- Genere conocimientos multiplataforma sobre procesos y socios de flujo de trabajo para promover una transparencia prácticamente instantánea.
- Otorgue a los usuarios acceso a plataformas de ecosistemas y datos más diversas.
- Deje lugar para la inteligencia artificial y humana de siguiente nivel, obtenida gracias a algoritmos y datos multiplataforma.
- Establezca y ejecute mercados con mucha rapidez.
- Permita que las empresas realicen experimentos rápidos de no superado-superado.

Para dominar la seguridad del cloud híbrido, comience con estos tres pasos.

Paso 1: Armonice la postura de seguridad en todo el patrimonio.

La postura de seguridad es la suma de las políticas, prestaciones y procedimientos de seguridad en diversos componentes del patrimonio de cloud híbrido: clouds individuales, plataformas cloud y controles de gestión, entornos de producción de software, red, datos, contenedores, zonas de aterrizaje y otros.

En una condición previa al dominio, la posición de seguridad del cloud híbrido no es coherente. Podría parecer que algunos componentes (por ejemplo, un cloud privado) tienen una posición de seguridad firme, pero otros quizás no. Algunos tal vez se ajusten a los estándares específicos de cumplimiento normativo, pero otros quizás no. Por lo tanto, cuando pulsamos el botón de “inicio” y solicitamos al cloud o los componentes específicos que interoperen de forma productiva, la falta de armonía entre las posiciones de seguridad puede exponer problemas graves.

Por ejemplo, las funciones empresariales a menudo dependen de múltiples componentes del cloud híbrido, y un actor malintencionado puede atacar cualquier parte de la superficie del cloud híbrido. Si la posición de seguridad de esos componentes no está armonizada, es difícil dilucidar cuál es el eslabón más débil de la cadena de seguridad. Y, sin saberlo, es casi imposible tomar medidas preventivas.

Desde un punto de vista arquitectónico, la armonización requiere enclaves de seguridad fuertes y segmentados de forma lógica que controlen el acceso de los usuarios y protejan los activos alojados. Requiere un método zero trust que regule rigurosamente el acceso a los datos, aplicaciones y componentes protegidos del patrimonio de cloud.

Armonizar la posición de seguridad en todo el cloud híbrido genera un tejido de protección que ayuda a evitar que los malos accedan por el eslabón más débil. Y puede hacer que responder a las exigencias normativas sea más fácil y menos costoso.

Una postal desde el terreno: *Con el objetivo de avanzar con una transformación digital de gran magnitud, un importante banco europeo tomó la decisión estratégica de introducir un nuevo cloud público en su entorno híbrido. Pero a medida que el banco aceleraba la migración, su CISO se alarmó al descubrir que no se estaba contemplando la seguridad desde la fase inicial, ni se estaba implementando de modo uniforme en toda la organización. No llegaba a satisfacer los requisitos normativos y dejaba al banco en una posición de vulnerabilidad a explotaciones por configuraciones incorrectas y TI invisible en el cloud. Era necesario remediar esa situación con urgencia. El banco también se dio cuenta de que el dominio del cloud híbrido era crucial para garantizar que los datos y servicios de todo el ecosistema cloud se estaban gestionando uniformemente y con un alto nivel tanto de seguridad como de cumplimiento normativo. Se adoptó un enfoque de plataforma de cloud híbrido. Se aplicaron prácticas de seguridad coherentes en todos los clouds públicos, clouds privados y centros de datos. Y, como consecuencia, el banco pudo demostrar fácilmente su cumplimiento ante los organismos de control.¹⁷*

Paso 2: Cree visibilidad a través de un solo panel de cristal.

Incluso con una posición de seguridad integral, es difícil proteger lo que uno no puede ver, así como alejar al malhechor si no se tiene información de seguridad precisa de todo el patrimonio de cloud. Ese es el desafío de visibilidad en la seguridad del cloud híbrido.

En el mercado de herramientas de control y comando de seguridad del cloud, hay muchos tipos de motores de fusión de datos y paneles de instrumentos disponibles para iluminar las amenazas a la seguridad. Pero, como sucede con la posición de seguridad del cloud híbrido en general, estas herramientas y la información que generan deben agregarse para poder detectar, evaluar y resolver las anomalías de seguridad a gran velocidad. Esta prestación de visibilidad agregada se conoce como un “solo panel de cristal”.

Tener un solo panel de cristal es especialmente importante cuando se produce un incidente de seguridad: ¿Cuál es la fuente del ataque? ¿Qué impacto tiene? Tener un solo panel de cristal puede permitir a los responsables determinar rápidamente qué sucedió, dónde, cuándo y quién es responsable del incidente para poder iniciar las acciones de mitigación.

Paso 3: Aproveche la IA para predecir las vulnerabilidades y tomar acciones preventivas.

Una vista coherente de la seguridad del cloud híbrido y un solo panel de cristal son más potentes si también podemos hacernos pronto una idea mejor de la seguridad que estamos observando. La inteligencia artificial (IA), el machine learning y la automatización pueden consumir altos volúmenes de datos de seguridad complejos, así como permitir la detección y predicción de amenazas casi en tiempo real. Estas herramientas y métodos proporcionan a los directores de seguridad información validada sobre las amenazas y recomendaciones de acción, lo cual los libera de la carga de buscar cada anomalía detectada.

Específicamente, las herramientas de IA se pueden entrenar para que detecten patrones de ciberataque previos a incidentes del pasado. Si esos patrones son recurrentes, la IA puede desencadenar alertas o incluso proporcionar acciones para la autorreparación mucho antes de lo que un operario humano habría podido detectarlos y actuar para abordar el posible incidente.

Recuerde que en un entorno de cloud híbrido, los operadores de seguridad se convierten en una comunidad de socios que incluyen proveedores de servicios en el cloud, responsables de activos y terceros como proveedores de software independientes (ISV). Un solo panel de cristal alimentado por una predicción proactiva de amenazas ayuda a coordinar las acciones de respuesta de seguridad en todo el ecosistema de cloud híbrido.

El dominio del cloud híbrido gestiona todos los costes del cloud en una sola vista y captura las oportunidades para optimizar costes y reasignar recursos.



El desafío financiero

Cómo entender las inversiones en el cloud, sus costes y rentabilidades, y gestionar todo el patrimonio híbrido como una sola cartera unificada.

La adopción del cloud solo gestiona las facturas de cloud individuales.

El dominio del cloud híbrido gestiona todos los costes del cloud en una sola vista y captura las oportunidades para optimizar costes y reasignar recursos.

Nuestra investigación revela que el 81 % de los ejecutivos tienen dificultades para gestionar y optimizar el gasto en el cloud.¹⁸ El código de software, los contenedores y los datos no son las únicas cosas que se mueven en un modelo operativo de cloud híbrido. También se mueve dinero (mucho) y, a medida que el ámbito de adopción del cloud híbrido sigue creciendo, el lado financiero del cloud puede convertirse en una oportunidad mayor para generar ventajas competitivas basadas en las operaciones. No obstante, a menudo es el elemento menos comprendido y menos supervisado del dominio del cloud híbrido.

La ruta hacia el dominio del cloud híbrido conlleva algunos desafíos financieros, incluidos los siguientes:

- Durante las primeras etapas de la adopción del cloud, las partes interesadas esperan que los costes bajen cuando las cargas de trabajo pasen del centro de datos al cloud de una empresa hiperescalable. Pero, con frecuencia, esos costes suben y eso genera mucha angustia e incluso remordimiento en el comprador.
- El coste de mover los datos (que en el pasado estaban mayormente ocultos en centros de datos locales) en un entorno de cloud puede impulsar el alza de los costes de los datos hasta en un 50 %, según conversaciones recientes que hemos tenido con clientes.
- El ROI en los casos de negocio requiere predecir los costes de prestación de servicios y del cloud con fiabilidad. Pero cuando los costes del cloud demuestran ser impredecibles, se erosiona la confianza en las nuevas inversiones y en la transición global al cloud híbrido. No sorprende, entonces, que el 79 % de los ejecutivos de una reciente encuesta reconocieran tener dificultades a la hora de desarrollar casos de negocio para sus iniciativas de cloud híbrido.¹⁹

Si se combinan y no se abordan, estos desafíos financieros pueden impedir la transformación empresarial y generar una gran cantidad de fricción, lo que menoscabará la energía y el impulso del programa.

Emplee prácticas de FinOps para diseñar una prestación de gestión financiera del cloud híbrido

Las operaciones financieras (FinOps) en el cloud son un conjunto de prácticas financieras y de aprovisionamiento que ayudan a las empresas a gestionar y optimizar el consumo y el gasto en servicios cloud. FinOps es crucial para el dominio del cloud híbrido porque permite que las empresas vean cómo y dónde se están consumiendo sus servicios cloud en todo el patrimonio de cloud. FinOps hace que sea posible prever la demanda de servicios cloud y optimizar el gasto para que los costes del cloud sean acordes con las prioridades empresariales. Además, FinOps ayuda a los equipos de ingeniería, finanzas, tecnología y negocios a colaborar en decisiones de gasto basadas en datos relativas a todo el patrimonio de cloud híbrido de la empresa. Con el tiempo, FinOps de cloud se puede combinar totalmente con las prácticas de gestión financiera existentes.

La visión integral de las operaciones y las finanzas que proporciona FinOps es importante para la mayoría de los ejecutivos de TI. En una encuesta reciente, un 79 % indicó que lograr visibilidad, gobierno y control en múltiples clouds es crucial para establecer una plataforma eficaz de orquestación multicloud.²⁰

Estos son los tres pasos que puede dar ahora para abordar el desafío financiero.

Paso 1: Comience con el desarrollo de una prestación de FinOps.

Cuando FinOps se convierte en parte de un modelo operativo de cloud híbrido, proporciona visibilidad financiera en cada uno de los componentes del entorno híbrido. FinOps no gira únicamente en torno al coste, sino que trata de obtener el mayor valor de cada unidad de coste. No se trata solo de ahorrar dinero: se trata de usar el dinero para generar más dinero.

No obstante, FinOps no es una cura milagrosa ni algo que uno pueda comprar, instalar y olvidarse. Un buen lugar para hacer crecer las competencias de gestión financiera es el centro de excelencia del cloud híbrido antes mencionado, donde las prácticas de FinOps pueden evolucionar y convertirse en un conjunto bien definido de servicios de apoyo a la toma de decisiones que las partes interesadas consumen en todo un modelo operativo de cloud híbrido.

Los líderes de negocio y de TI deberían reconocer que, inicialmente, los conocimientos de FinOps probablemente estén limitados debido a la falta de habilidades, talento o experiencia. Entonces, en el corto plazo, concentre los servicios de FinOps en los desafíos financieros y costes de mayor riesgo o impacto del centro de excelencia del cloud híbrido. E inicie la formación, educación y selección de personal para FinOps.

Paso 2: Optimice los costes ahora. A medida que crezcan sus prestaciones de FinOps, úselas para sumergirse más a fondo en la optimización del gasto en el cloud.

Una vez que el centro de excelencia del cloud haya comenzado a prestar servicios de gestión financiera del cloud conforme a principios de FinOps, desarrolle y proporcione una versión única de la verdad para todos los proveedores externos de servicios cloud en el patrimonio de cloud híbrido. Haga que la facturación del cloud y la elaboración de informes de costes sean lo más sencillas y fáciles de entender posible. Sea capaz de explicar las facturas de sus proveedores de servicios cloud y comience a optimizar esos costes variables proponiendo cambios simples en la forma de generar esos costes. Por ejemplo, ¿los servicios de la plataforma cloud están facilitando que los clientes (desarrolladores e ingenieros) eleven los costes sin darse cuenta? ¿Todavía quedan silos de cloud en los que no hay controles reales sobre las compras de servicios cloud (y la responsabilidad sobre estas)?

A medida que crecen sus prestaciones de FinOps, úselas para abordar un amplio espectro de costes del cloud híbrido y relacionados con el modelo operativo del cloud. Algunos podrían estar disponibles en forma de mayores descuentos en servicios cloud habilitados por el ingenio financiero de FinOps. Contemple esta *postal desde el terreno* que muestra que las prácticas de FinOps ayudan a identificar ahorros de costes del 20 % o más de las fuentes, lo que incluye:

- Reducción en costes de servicios gestionados
- Reducción en costes de infraestructura
- Reducción de incidencias de software
- Obtención de beneficios de la automatización
- Mejora en la economía gracias al autoservicio
- Proyectos de cumplimiento y certificación de seguridad menos costosos y mejores
- Menos personas que dedican su tiempo a tareas de prestación de servicios automatizadas

Paso 3: Combine FinOps con AIOps.

AIOps hace referencia a la aplicación de la IA para mejorar las operaciones de TI. Específicamente, AIOps usa prestaciones de Big Data, análisis y machine learning para realizar un seguimiento y comprender los datos relativos al rendimiento de las aplicaciones que las operaciones de cloud híbrido generan en abundancia. Y, como sucede con la mayoría de las tecnologías prometedoras que avanzan por la curva de madurez, las inversiones en AIOps requieren cierta experimentación y desarrollo de casos de prueba.

Como el resultado deseado de muchos casos de uso de AIOps es la reducción de costes, AIOps se combina naturalmente con FinOps. Básicamente, la combinación de FinOps y AIOps sirve para mantener a AIOps en el punto óptimo en el cual el programa realiza la implementación suficiente para facilitar la obtención de los beneficios empresariales deseados. FinOps puede proporcionar los conjuntos de problemas y las hipótesis iniciales para la experimentación (“las incidencias de gestión de recursos de aplicaciones están costando X euros, pero con la automatización de AIOps este importe se puede reducir a Y euros”). También puede proporcionar los datos necesarios para medir la eficacia de las inversiones en AIOps. Y cuando AIOps logra reducir los costes operativos, las ganancias se pueden volver a invertir en otras partes del programa.

TSB Bank, que está pasando rápidamente de una estrategia con muchas sucursales a una que prioriza el mercado digital, invirtió 120 millones de libras a lo largo de tres años para desarrollar una solución de cloud híbrido que simplificara la infraestructura tecnológica y permitiera el movimiento y la gestión de datos, servicios y flujos de trabajo en múltiples clouds. TSB, que opera en una plataforma cloud unificada para todos los canales y aplicaciones bancarios, lanzó nuevos canales como banca de conversación y añadió funciones digitales en los canales móvil y web con mayor frecuencia para impulsar más de un 90 % de autoconsumo digital, sin dejar de reforzar la seguridad y confidencialidad de los datos críticos de los clientes.²¹

El dominio del cloud híbrido reúne a todos los socios en un ecosistema voluntario y multilateral, alineados bajo una estrategia para el éxito.



Desafío 5

El desafío del ecosistema de socios

Cómo llevar nuevos socios a una mesa de capitanes dedicada para generar capital social y priorizar el éxito de los clientes sobre los intereses de cada actor.

La adopción del cloud administra simplemente los contratos individuales con socios. *El dominio del cloud híbrido reúne a todos los socios en un ecosistema voluntario y multilateral, alineados bajo una estrategia para el éxito.*

Las transiciones empresariales al cloud pueden ser como una cocina repleta de cocineros en la cual cada uno piensa que debería ser el chef principal. La competencia que se produce en consecuencia hace que los comensales tengan que esperar mucho tiempo por su plato y que la calidad de la comida sea regular.

El diverso elenco de actores del ecosistema involucrados en su transición al cloud híbrido puede generar una dinámica similar. A nivel interno, líderes de múltiples líneas de negocio y una variedad de líderes de la organización de TI intentarán usar los recursos del programa en su beneficio. A nivel externo, los socios de implementación, las empresas hiperescalables, los proveedores de SaaS y los ISV aportarán sus propios sesgos, perspectivas divergentes e intereses particulares. Pero una cosa es segura y, en nuestra reciente encuesta, un 88 % de los ejecutivos están de acuerdo en lo siguiente: la colaboración en el ecosistema es crucial para una gestión eficaz del multicloud.²²

La tarea de gestionar estos intereses diversos podría abordarse parcialmente mediante las estructuras de gobierno de TI y empresariales existentes y las OGP, pero solo de forma parcial. Las prioridades de las partes interesadas que compiten entre sí, los incentivos en conflicto y las acusaciones de socios, entre otros factores similares, a menudo requieren una solución más directa: algo que cambie las reglas del juego.

Considere esta *postal desde el terreno*: un enfoque exitoso que hemos visto en el terreno podría llamarse “la mesa de capitanes”.²³ Imagínese una mesa redonda donde cada sector de su transición al dominio del cloud híbrido (su ecosistema de cloud híbrido) está representado por un capitán sénior. Con un ejecutivo de la empresa a la cabeza y supervisando la transición al cloud híbrido, los ejecutivos interesados internos y los ejecutivos de los socios externos sentados a la mesa mantienen el programa en la trayectoria correcta acordando que las decisiones más críticas del programa (y la resolución de conflictos) se deben tomar de forma colaborativa, coherente y con suficiente transparencia para preservar la confianza de todas las partes.²⁴

Uno de los objetivos de la mesa es convertir lo que podría ser un juego en el que no gana ningún capitán en un conjunto más amplio de valor para todos los que participan y todo el ecosistema. El dominio del cloud híbrido toma los intereses que compiten naturalmente (sectores de línea de negocios, TI, integrador principal y proveedor de tecnologías) y logra que adopten una innovación abierta y la creación conjunta para conseguir un programa exitoso.

Estos son tres pasos que puede dar para crear una mesa de capitanes eficaz.

Paso 1: Seleccione los participantes de su mesa de capitanes.

Para comenzar, decida qué organizaciones del ecosistema deberían sentarse a la mesa. Las opciones obvias son, entre otras, los patrocinadores principales de las líneas de negocio, su integrador principal, sus proveedores de servicios cloud principales y los proveedores de servicios gestionados que desempeñan una función en la producción de software, la gestión de aplicaciones y las operaciones de centros de datos. Piense en una mesa de capitanes del tamaño aproximado de un equipo ágil.

Seleccione al ejecutivo sénior específico que desee que represente a cada socio. Probablemente ya conozca a varios ejecutivos de cada socio, pero hable con los directores de su programa de socios antes de enviar las invitaciones. El ejecutivo que elija como participante debe tener la antigüedad adecuada y capacidad para representar al socio en la toma de las decisiones necesarias para resolver cuestiones actuales y futuras del ecosistema.

Si sus socios son organizaciones de gran magnitud, no se deje impresionar por los cargos. Seleccione ejecutivos que puedan “actuar por encima de los silos” de sus organizaciones. Es necesario que puedan tomar decisiones sobre el trabajo del socio y hacer que queden en firme. Ya tiene un contacto de cada socio que puede “consultar con la oficina central”. Para su mesa, necesita a alguien que pueda *actuar como* la oficina central. “Tengo buena relación con tal y cual” no es suficiente.

Paso 2: Desarrolle una visión y un documento funcional de la mesa de capitanes.

La mesa de capitanes necesita un razonamiento compartido muy claro con respecto a los objetivos, las normas y los procesos de la mesa. Para ese fin, recomendamos que incorpore a profesionales de design thinking para que planifiquen y faciliten un sprint para desarrollar una visión y un documento funcional creado conjuntamente entre sus patrocinadores ejecutivos y los participantes que haya seleccionado. La visión y el documento funcional deberían prever preguntas provocadoras y críticas como:

- ¿Cómo están afectando los incentivos al rendimiento de los capitanes (planes de bonificaciones, KPI de la empresa, asignaciones presupuestarias, objetivos y resultados clave, SLA, objetivos de ingresos, objetivos de “aterrizaje y expansión”, etc.) en la toma de decisiones y en la ejecución del programa?
- ¿Qué tal están alineadas las hojas de ruta de mejora del rendimiento de las líneas de negocio con la hoja de ruta de implementación del cloud híbrido? ¿Las demandas de TI de las líneas de negocio tienen que repriorizarse con el fin de obtener el valor óptimo de las inversiones en el cloud híbrido?
- ¿Cómo deberían comunicar los capitanes sus expectativas de colaboración de todo el programa y capacitar a su personal para que pueda aplicarlas en sus interacciones diarias?

Recomendamos incorporar a un facilitador formado y cualificado para que diseñe las reuniones e interacciones para los miembros de la mesa de capitanes. Mantenga el foco en mejorar la comunicación y colaboración, así como la calidad de las reuniones y los resultados en general. Defina un tono y una cultura para la mesa de capitanes. Enfatique constantemente que la calidad de su programa no puede superar la calidad de las conversaciones que tiene con respecto a ese programa.

Paso 3: Use la mesa de capitanes para enfocarse en los principales desafíos para dominar el cloud híbrido.

Una vez que la mesa de capitanes esté en funcionamiento, es momento de obtener un gran retorno de su inversión. Una clara recompensa de una mesa de capitanes eficaz es que puede ayudar a que su programa aborde los desafíos del dominio del cloud híbrido que hemos explorado en este documento. Si revisamos esos desafíos que dificultan el dominio, está claro que todos se entrecruzan con la totalidad de su ecosistema de socios. Sin duda, la mejor forma de integrar a cada socio pasa por trabajar en una zona gris que probablemente no estará cubierta por el contrato de cada socio. Entonces, cada desafío presenta una gran manera de centrar su mesa de capitanes en el abordaje de cuestiones que podrían generar mucha fricción si no se tratan. Un modelo de garaje de colaboración abierta puede ser muy eficaz. A modo ilustrativo:

- Para el desafío de la arquitectura: defina la función que desempeña cada actor en la arquitectura de la plataforma de cloud híbrido, prestando mucha atención a las inevitables superposiciones entre los socios y a las dependencias que surgen al diseñar una plataforma única e integrada.
- Para el desafío de las personas y las operaciones: defina la función que desempeña cada socio en la formación del personal en cuanto a la tecnología y las prácticas que incorporan a la plataforma. Cada socio tendrá servicios de asistencia a los usuarios, pero ¿cómo se puede hacer que acepten una forma integrada adaptada a su programa? ¿Cuánta formación y asistencia directa sobre el terreno proporcionará cada socio?
- La mesa de capitanes no puede estar involucrada en el trabajo diario de diseñar e implementar un modelo operativo de cloud híbrido, pero debería participar cuando uno o más socios se enfrenten a un gran cambio en los servicios que prestan a medida que evoluciona el modelo operativo.

- Para el desafío de seguridad: hemos argumentado que un programa de seguridad transformador tiene que ser un deporte de equipo, y una mesa de capitanes puede ser una forma excelente para conseguir que lo sea. Armonizar la posición de seguridad del cloud híbrido y adoptar una mentalidad que priorice la seguridad requiere concesiones mutuas sustanciales entre todos los miembros del ecosistema de socios, y puede sacar a la superficie problemas que requieran la atención de la mesa.
- Y, por último, para el desafío financiero: los esfuerzos del programa por desarrollar una prestación de FinOps deberían engranarse directamente con las inquietudes de la mesa de capitanes. Al capturar una versión única de la verdad financiera, los datos de FinOps proporcionan al capitán una forma de incorporar a los socios en conversaciones constructivas sobre la optimización de costes que apliquen el principio de FinOps de sacar el máximo valor de cada unidad de coste.

Ante una demanda al alza de datos con una tasa de crecimiento anual compuesta (CAGR) superior al 70 %, Airtel (una de las empresas de telecomunicaciones integradas más grande de India) ha adoptado la arquitectura de cloud híbrido moderno para ofrecer redes más rápidas, más grandes y más reactivas a los clientes. La plataforma abierta de cloud híbrido de Airtel permite la generación de nuevos flujos de ingresos al incorporar servicios de terceros, como juegos, producción remota de medios y otros servicios empresariales. Airtel está mejorando el tiempo de comercialización de los servicios y reduciendo los gastos operativos y de capital. El cloud de la red posiciona a los socios del ecosistema, incluidos los desarrolladores de aplicaciones B2B y B2C, para que creen servicios de valor añadido, como nuevas ofertas de Edge.²⁵

Alcanzar el dominio.



En conclusión, ahora está preparado para

Alcanzar el dominio

Este documento ha dejado claro que el cloud híbrido es una estrategia poderosa para la transformación empresarial. Como se destacó al inicio, somos muy optimistas en cuanto al recorrido para la obtención de valor con el cloud híbrido. Y más allá de los beneficios a corto plazo del cloud híbrido, considere que las tecnologías empresariales exponenciales (IA, IoT y edge computing, seguidas de blockchain y la computación cuántica) exigen un dominio del cloud híbrido como requisito previo a la generación de valor nuevo. Incluso los primeros en adoptar las nuevas tecnologías no pueden pasar por alto el trabajo de formar correctamente su cloud híbrido.

Así, cuando vemos que las transiciones de las empresas no llegan al punto de dominio del cloud híbrido (dejando las fuentes profundas de valor fuera del alcance), nos lleva a preguntarnos qué frena a los programas. Los cinco desafíos que hemos abordado (de forma no exhaustiva) captan los obstáculos más comunes que vemos en el terreno y las “decisiones correctas” que pueden inclinar la balanza con más fuerza a su favor.

Vamos a concluir con una llamada a la acción para todas las empresas que estén recorriendo este camino hacia el dominio, sobre todo para aquellas que ya van por el segundo o tercer intento de captar el valor que ofrece el cloud híbrido. Considere los cinco desafíos y cambie su trayectoria actual para abordarlos. Una vez que haya alcanzado el equilibrio inicial entre una hoja de ruta para desarrollar prestaciones de cloud híbrido y una hoja de ruta para mejorar el rendimiento de su empresa en un mundo guiado por el software, manténgase en ese punto óptimo y siga aportando valor. Y no se conforme con menos de lo que se ha demostrado que es posible.

Un estudio reciente del IBM Institute for Business Value estima que el valor de las inversiones en el cloud híbrido se multiplica hasta por 13 de promedio cuando se combina con otras palancas de transformación. En algunos sectores, el valor llega a multiplicarse por cifras tan altas como 20.²⁶

Notas y referencias bibliográficas

- 1 Foster, Mark y John Granger. "The Virtual Enterprise Blueprint". IBM Institute for Business Value. Enero de 2022. <http://ibm.co/virtual-enterprise>
- 2 Hurwitz, Judith y Daniel Kirsch. "Outperforming Businesses: Realize 2.5-x value with a hybrid cloud platform approach". Hurwitz & Associates. 2020. <https://www.ibm.com/es-es/downloads/cas/LVGDJE9N>
- 3 Boville, Howard, Hillery Hunter y Richard Warrick. "Cloud's next leap". Octubre de 2021. <https://www.ibm.com/es-es/thought-leadership/institute-business-value/report/cloud-transformation>
- 4 Payraudeau, Jean-Stéphane, Anthony Marshall y Jacob Dencik. "Unlock the business value of hybrid cloud: How the Virtual Enterprise drives revenue growth and innovation". IBM Institute for Business Value. Julio de 2021. <https://www.ibm.com/es-es/thought-leadership/institute-business-value/report/hybrid-cloud-business-value>
- 5 Boville, Howard, Hillery Hunter y Richard Warrick. "Cloud's next leap". Octubre de 2021. <https://www.ibm.com/es-es/thought-leadership/institute-business-value/report/cloud-transformation>
- 6 *Ibidem*.
- 7 Comfort, Jim, Blaine Dolph, Steve Robinson, Lynn Kesterson-Townes y Anthony Marshall. "The hybrid cloud platform advantage". IBM Institute for Business Value. Junio de 2020. <https://www.ibm.com/es-es/thought-leadership/institute-business-value/report/hybrid-cloud-platform>
- 8 Boville, Howard, Hillery Hunter y Richard Warrick. "Cloud's next leap". Octubre de 2021. <https://www.ibm.com/es-es/thought-leadership/institute-business-value/report/cloud-transformation>
- 9 Lumen Technologies. Caso práctico de IBM.
- 10 Datos no publicados del IBM Institute for Business Value.
- 11 *Ibidem*.
- 12 *Ibidem*.
- 13 Comfort, Jim, Blaine Dolph, Steve Robinson, Lynn Kesterson-Townes y Anthony Marshall. "The hybrid cloud platform advantage". IBM Institute for Business Value. Junio de 2020. <https://www.ibm.com/es-es/thought-leadership/institute-business-value/report/hybrid-cloud-platform>
- 14 Orange France. Caso práctico de IBM.
- 15 Datos no publicados del IBM Institute for Business Value. T4 de 2021.

- 16 Boville, Howard, Hillery Hunter y Richard Warrick. "Cloud's next leap". Octubre de 2021. <https://www.ibm.com/es-es/thought-leadership/institute-business-value/report/cloud-transformation>
- 17 Basado en un caso práctico interno de IBM.
- 18 Payraudeau, Jean-Stéphane, Anthony Marshall y Jacob Dencik. "Unlock the business value of hybrid cloud: How the Virtual Enterprise drives revenue growth and innovation". IBM Institute for Business Value. Julio de 2021. <https://www.ibm.com/es-es/thought-leadership/institute-business-value/report/hybrid-cloud-business-value>
- 19 *Ibidem*.
- 20 Comfort, Jim, Blaine Dolph, Steve Robinson, Lynn Kesterson-Townes y Anthony Marshall. "The hybrid cloud platform advantage". IBM Institute for Business Value. Junio de 2020. <https://www.ibm.com/es-es/thought-leadership/institute-business-value/report/hybrid-cloud-platform>
- 21 TSB Bank. Caso práctico de IBM.
- 22 Comfort, Jim, Blaine Dolph, Steve Robinson, Lynn Kesterson-Townes y Anthony Marshall. "The hybrid cloud platform advantage". IBM Institute for Business Value. Junio de 2020. <https://www.ibm.com/es-es/thought-leadership/institute-business-value/report/hybrid-cloud-platform>
- 23 Chillingworth, Mark. "BP CIO oils outsourcing future". CIO. 4 de junio de 2013. <https://www.cio.com/article/200265/bp-cio-oils-outsourcing-future.html>
- 24 Contrariamente a lo que propone la clásica mesa del capitán donde los participantes se juntan para reunirse con el capitán de la organización principal, debería tener una mesa de capitanes en la que todos los capitanes clave de la empresa, la plataforma, la tecnología y los proveedores se reúnen para colaborar en condiciones de igualdad.
- 25 Bharti Airtel. Caso práctico de IBM.
- 26 Payraudeau, Jean-Stéphane, Anthony Marshall y Jacob Dencik. "Unlock the business value of hybrid cloud: How the Virtual Enterprise drives revenue growth and innovation". IBM Institute for Business Value. Julio de 2021. <https://www.ibm.com/es-es/thought-leadership/institute-business-value/report/hybrid-cloud-business-value>

Acerca de los autores

John Granger

Vicepresidente sénior
IBM Consulting
[linkedin.com/in/grangerjohn](https://www.linkedin.com/in/grangerjohn)
john.granger@ibm.com

John ha sido arquitecto jefe de la estrategia para IBM Consulting, un motor de crecimiento clave de IBM. Con una firme alineación con la estrategia de IA y cloud híbrido de IBM, IBM Consulting está ejecutando su estrategia mediante la contratación y el desarrollo de talentos cualificados, adquisiciones de objetivos, ofertas líderes en el mercado y asociaciones estratégicas profundas con proveedores de servicios cloud líderes, proveedores de software independientes e IBM Technology, incluido Red Hat OpenShift.

Shai Joshi

Socio gerente y líder de la plataforma de crecimiento Servicios globales de cloud híbrido
IBM Consulting
[linkedin.com/in/shaijoshi](https://www.linkedin.com/in/shaijoshi)
shailesh@us.ibm.com

Shai es responsable de los servicios globales de asesoría, migración, modernización, desarrollo, gestión y seguridad, así como de las plataformas cloud para toda la plataforma de crecimiento. Además, es responsable de los acuerdos de gran magnitud y empresas adscritas. En esta función, Shai se encarga de todos los aspectos del negocio, incluidas la estrategia, las ofertas, la transformación de habilidades y talentos, las ventas y la ejecución, lo cual abarca más de 80 000 profesionales a nivel global.

Thais Lima de Marca

Socia gerente, Gestión del cloud híbrido
IBM Consulting
[linkedin.com/in/thais-marca-88b45a2](https://www.linkedin.com/in/thais-marca-88b45a2)
tmarca@br.ibm.com

Thai es responsable de aproximadamente un 45 % de todos los ingresos de IBM Consulting a nivel mundial. Su objetivo es ayudar a los clientes a migrar al cloud y a mejorar tanto su CTP como el tiempo de comercialización. Thais forma parte del equipo acelerado de IBM Global y de la academia del sector. Antes de su reciente nombramiento, era directora general de IBM Consulting para Latinoamérica y se centraba en ayudar a los clientes a transformar sus empresas mediante soluciones digitales.

Varun Bijlani

Socio gerente global, Transformación del cloud híbrido
IBM Consulting
[linkedin.com/in/varunbijlani](https://www.linkedin.com/in/varunbijlani)
varun.bijlani@uk.ibm.com

Varun dirige el negocio de servicios globales de transformación del cloud híbrido de IBM y ayuda a los clientes a diseñar su estrategia y arquitectura de cloud, así como a ejecutarlas por medio de la migración, la modernización y nuevas prestaciones nativas en cloud. Cuenta con más de 26 años de experiencia, durante los que ha combinado conocimientos del área y de gestión de programas globales con un liderazgo estratégico y operativo tanto en asesoría como en el sector.

Shue-Jane Thompson, D.M.

Socia sénior, Crecimiento y estrategia de seguridad
Líder distinguida del sector
IBM Consulting
[linkedin.com/in/shuejane](https://www.linkedin.com/in/shuejane)
shuejane@us.ibm.com

La Dra. Shue-Jane supervisa la innovación, integración, ventas de servicios y prestación de soluciones de ciberseguridad a clientes en más de 170 países del mundo. Tiene más de 30 años de experiencia en entornos de administración de empresas y tecnologías de ámbito académico, comercial, gubernamental e internacional. Además, ha ganado y gestionado muchos programas a gran escala de TI, cibernéticos, de cloud y de operaciones de la misión.

Más información

Si desea saber más sobre este estudio o sobre el IBM Institute for Business Value, póngase en contacto con nosotros en el correo electrónico iibv@us.ibm.com. Siga a @IBMIBV en Twitter. Y si desea obtener un catálogo completo de nuestras investigaciones o suscribirse a nuestro boletín mensual, visite: ibm.com/es-es/ibv.

Acerca de los conocimientos extraídos de la investigación

El IBM Institute for Business Value, que forma parte de IBM Consulting, desarrolla conocimientos estratégicos basados en hechos para los altos ejecutivos de empresa sobre cuestiones críticas de los sectores público y privado.

© Copyright IBM Corporation 2022

IBM España, S.A.

Santa Hortensia, 26-28

28002 Madrid

Producido en los Estados Unidos de América

Mayo de 2022

IBM, el logotipo de IBM e ibm.com son marcas comerciales de International Business Machines Corp., registradas en muchas jurisdicciones del mundo. Los demás nombres de productos y servicios pueden ser marcas registradas de IBM u otras empresas. Puede consultar una lista actual de las marcas comerciales de IBM en «Copyright and trademark information», en ibm.com/legal/copytrade.shtml.

Este documento se actualizó por última vez 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.

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.

Este informe está destinado a servir de orientación general. No pretende sustituir a una investigación detallada ni al ejercicio del juicio profesional. IBM no será responsable de ninguna pérdida sufrida por cualquier organización o persona que se base en esta publicación.

Los datos utilizados en este informe pueden proceder de fuentes de terceros e IBM no verifica, valida ni audita dichos datos de forma independiente. Los resultados de la utilización de estos datos se proporcionan “tal cual” e IBM no ofrece ninguna declaración ni garantía, expresa o implícita.

Este documento se ha impreso en papel reciclado sin cloro en una imprenta certificada con la Cadena de Custodia del Consejo de Administración Forestal (FSC) utilizando tintas biológicas. La energía utilizada para fabricar este papel e imprimirlo procede de energías ecológicas renovables. Por favor, recicle.





IBM.