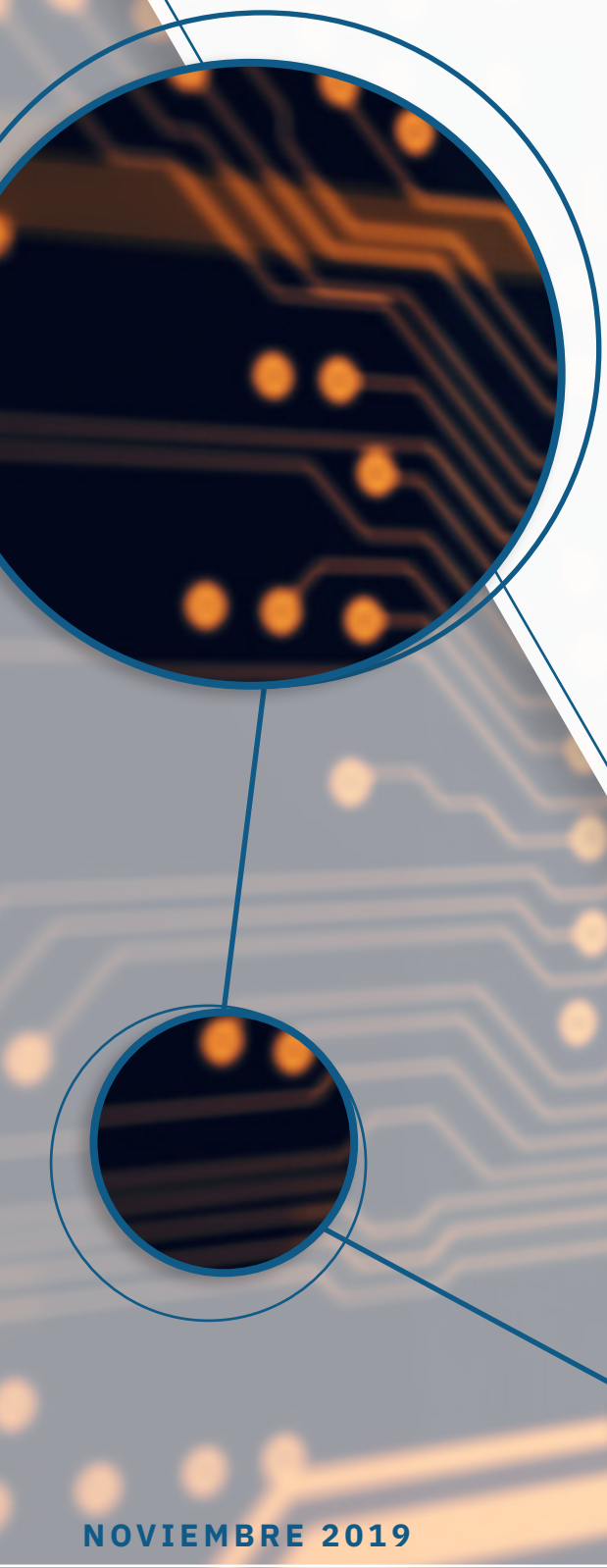
451 Research® | PATHFINDER REPORT



Mitigar los riesgos durante el proceso hacia un entorno híbrido de múltiples nubes

IMPERATIVOS DE RESISTENCIA

POR ENCARGO DE

IBM

NOVIEMBRE 2019

Acerca de este documento

Un documento Pathfinder ofrece las opciones a los que tienen que tomar las decisiones frente a los problemas de una tecnología o un caso de empresa especifico, explora el valor comercial de esta adopción, y recomienda la gama de consideraciones y pasos concretos a seguir en el proceso de toma de decisiones.

ACERCA DEL AUTOR

ERIC HANSELMAN

JEFE ANALISTA

Eric Hanselman es el jefe analista en 451 Research. Tiene un vasto conocimiento práctico de una amplia gama de áreas de TI y una experiencia directa en las áreas de redes, virtualización, seguridad y semiconductores. Coordina el análisis de la industria mediante la cartera amplia de las disciplinas de 451 Research. La convergencia de fuerzas en el paisaje tecnológico está causando movimientos en las placas tectónicas en la industria, incluyendo las redes definidas por software (SDN), la virtualización de funciones de red (NFV), la hiperconvergencia y el Internet de las cosas (IoT). Eric ayuda a los clientes de 451 Research a navegar por estas aguas turbulentas para determinar sus impactos y la mejor forma para capitalizarlos. También es miembro del Centro de Excelencia para Tecnologías Cuánticas de 451 Research.

Resumen ejecutivo

El avance hacia un entorno híbrido de múltiples nubes ya podría ser una realidad para algunos y puede parecer inevitable para muchos. Ese cambio trae de manera involuntaria un conjunto de complejidades que pueden forzar los enfoques tradicionales a la disponibilidad, la seguridad y el cumplimiento. La expansión natural que atrae en estos momentos a las empresas a entornos fuera de sus centros de datos tradicionales también está llevando a componentes críticos de aplicación y datos más allá de las protecciones que implementaron. Es necesario establecer esas protecciones en estos nuevos lugares; sin embargo, puede ser intensivo en recursos y desafiante para las organizaciones que no hayan tenido el tiempo de desarrollar la profundidad técnica para hacerlo de manera efectiva.

Hallazgos principales

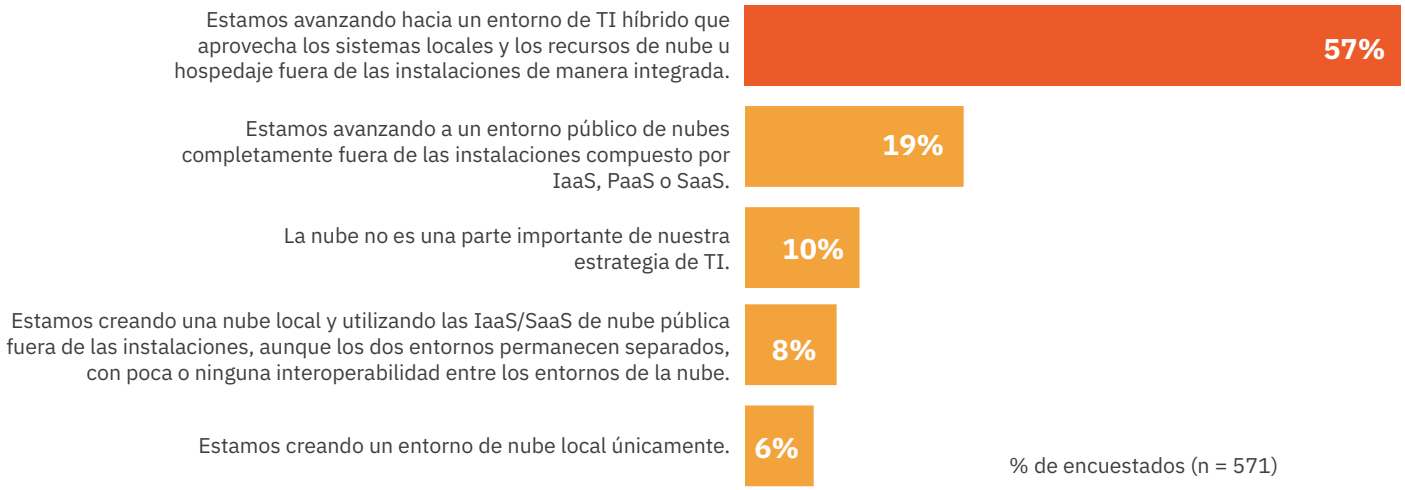
- Los entornos híbridos de múltiples nubes requieren nuevas estrategias para manejar los riesgos.
- La resistencia requiere acciones en el ahora para mitigar los riesgos de las empresas.
- Los cambios en los patrones de ataque y en las herramientas requieren la protección para los datos que puedan mitigar nuevas amenazas.
- La protección de datos en la de múltiples nubes híbrida requiere una mayor vigilancia de los nuevos riesgos.
- Las mejoras en la gestión de datos híbridos son imprescindibles bajo la órbita de las fuerzas reguladoras como el Reglamento General de Protección de Datos de la UE y la Ley de Privacidad del Consumidor de California.
- La automatización y la orquestación son necesarias para abordar la escala de los entornos híbridos de manera efectiva.

Beneficios del entorno híbrido de múltiples nubes

A medida que la transformación digital y la nube se expanden, las empresas están ampliando su infraestructura a escala masiva. La creación de un entorno híbrido de múltiples nubes debería aumentar la interoperabilidad y permitir una gran variedad de asociaciones y colaboraciones entre nubes. Según la encuesta Voice of the Enterprise: Cloud, Hosting Managed Services, Workloads and Key Projects 2019 de 451 Research, el 57% de las organizaciones describieron su enfoque y estrategia de TI como de carácter híbrido.

Figura 1: El futuro es híbrido para la mayoría

Fuente: 451 Research, Voice of the Enterprise: Cloud, Hosting & Managed Services, Workloads and Key Projects 2019
P: ¿Cuál de las siguientes opciones describe mejor el enfoque y la estrategia de TI general de su organización?



Puede ser difícil para el 19 % de los encuestados que informan que avanzan hacia un entorno de nube pública, existir exclusivamente en nubes públicas. Anticipamos que los entornos híbridos se extenderán demasiado para que las empresas no tengan un cierto nivel de colaboración híbrida, incluso si fuera solo para unas pocas aplicaciones.

El uso creciente de la infraestructura de la nube crea un entorno en el que se podrían utilizar innumerables configuraciones de recursos virtuales. Una amplia gama de recursos disponibles significa que para tener éxito, las empresas deben ser capaces de crear activos que puedan existir en múltiples entornos. Una estrategia híbrida de TI permite más espacio para la colaboración y la interoperabilidad.

Para operar con éxito en un modo híbrido de múltiples nubes, las organizaciones deben poder mover los datos a través de la infraestructura sin sacrificar la fluidez. A medida que avanzan hacia el uso de arquitecturas de contenedores y microservicios, los componentes de la aplicación liviana se pueden transferir fácilmente a través de las nubes. En un entorno donde los datos pueden necesitar almacenarse al margen, como una implementación de IoT o una fábrica inteligente, es imperativo que esos datos se puedan transferir fácilmente a través de las nubes para permitir un uso más eficiente de la infraestructura distribuida.

Las tecnologías para permitir el funcionamiento híbrido de múltiples nubes están disponibles y en uso generalizado. Las estrategias para el movimiento y la disponibilidad de datos se pueden adaptar a las necesidades de las aplicaciones que respaldan. Las técnicas de replicación y publicación/suscripción ofrecen enfoques básicos para garantizar que los datos estén disponibles donde se necesiten. Las rutas más complejas, como las bases de datos distribuidas como MongoDB o Cassandra, pueden abarcar ubicaciones mientras automatizan la tarea de distribución de datos.

Un impulsor más del cambio a la tecnología híbrida es la expansión del ecosistema tecnológico de una organización. Hay dos caminos comunes: la adopción de una tecnología importante y la presencia de un socio o proveedor. En cualquier caso, la organización establece una presencia en un nuevo lugar para aprovechar la tecnología o el servicio. Los proveedores de la nube pública ofrecen tecnología especializada, como el reconocimiento de imagen o de voz y las capacidades de aprendizaje automático. Para usarlos, los datos deben estar disponibles en ese entorno de nube, y los resultados también se entregan allí. Los servicios que ofrecen los socios del ecosistema, como el marketing o la participación del cliente, pueden estar alojados en un proveedor en particular, lo que hace que sea atractivo tener componentes de la aplicación alojados allí para mejorar el rendimiento. Todos estos son factores que pueden exigir a las organizaciones a múltiples entornos donde necesitan gestionar la confiabilidad y disponibilidad de los datos.

Complejidades del entorno híbrido de múltiples nubes

A medida que la infraestructura de la nube se expande, se vuelve cada vez más complicada, abriendo la puerta a errores y fallas. Una empresa que opera en un modo híbrido de múltiples nubes puede desarrollar exposiciones de riesgo en su infraestructura sin estar operativamente consciente de su existencia. Este es un desafío que puede aparecer con el crecimiento de la infraestructura orgánica. Si la organización no tiene procesos para incorporar nuevos recursos que reevalúen el riesgo en cada paso, pueden aparecer amenazas a la resistencia. No es raro que el uso de varios entornos de nube o hosting no esté coordinado, y que mucho volumen de trabajo conectado pueda crear vectores de ataque que son ajenos a los equipos y software de seguridad informática existentes.

Trabajar en entornos de nube también crea una dependencia particular de la interconexión, con una confiabilidad que dista de ser perfecta. Los entornos híbridos extienden las rutas a los datos a través de tecnologías típicamente diferentes y con herramientas que no son consistentes para administrar y monitorear a estas. Administrar rutas de datos clave puede ser lo suficientemente desafiante dentro de un centro de datos. Una vez que los datos se dispersan en una infraestructura a escala masiva, se vuelve un desafío aún mayor.

Una de las mayores dificultades que presenta la interconexión es que los modos de falla que se introducen pueden ser mucho más complejos. Eso puede dificultar la detección de las fallas y recuperarse de ellas. Por ejemplo, una ruta que comparte tráfico de varias fuentes puede congestionarse, creando aumentos en la latencia o en la pérdida de paquetes. Para las aplicaciones que dependen de la sincronización en el tiempo, los aumentos en la latencia por encima de su umbral de rendimiento pueden tener un efecto similar al fallo de la ruta, pero incluso así para las herramientas de monitoreo aún pueden parecer que funcionan. Diagnosticar problemas como estos es una complicación, especialmente porque a menudo se experimentan solo bajo una carga significativa, lo que puede hacer que su aparición sea intermitente.

Los modos de falla de una aplicación pueden complicarse por factores en los diferentes entornos donde se encuentran los componentes. Los problemas de rendimiento local pueden ser impulsados por una serie de problemas que van desde errores de aplicación, variabilidad E/S de almacenamiento, errores de tamaño de instancia y fallas simples. La complejidad surge al tratar de determinar que

se ha producido un error y luego recuperarse, en entornos donde los mecanismos de detección y recuperación son únicos. Si una organización quiere resolver este problema, puede terminar en un gasto considerable de recursos para desarrollar habilidades en cada nuevo entorno en el que opera.

La infraestructura de TI híbrida también puede ser un dolor de cabeza para los equipos de operaciones que tienen que monitorear más ambientes que nunca. Si bien los expertos en operaciones de TI pueden tener mucha experiencia en la administración de los servidores locales privados de su empresa, en una configuración híbrida de múltiples nubes, deberán interoperar con nubes públicas y, posiblemente, con una nube privada de otro proveedor. Es difícil mantener la eficiencia operativa cuando los equipos tienen la tarea de dominar diferentes conjuntos de habilidades e integrar los resultados en un proceso de trabajo.

Uno de los riesgos más grandes de los entornos híbridos es que los riesgos subyacentes pueden estar enmascarados por la complejidad de las estructuras de aplicación que se construyen en ellos. La combinación de todos estos factores puede acumular un conjunto oculto de problemas potenciales que no se tienen en cuenta en la planificación de la continuidad de la empresa y la recuperación ante desastres, que analiza cada entorno de forma independiente.

Imperativos de resistencia

Con la combinación de expansiones del ecosistema y un conjunto de beneficios que impulsan la adopción de entornos híbridos, las organizaciones tienen un fuerte imperativo para abordar la resistencia de este nuevo entorno para garantizar que puedan mantener los mismos niveles de disponibilidad en aplicaciones clave que hayan tenido tradicionalmente. Esta tendencia de expansión no es un evento único sino una nueva realidad. Los nuevos entornos continuarán ofreciendo valor de nuevas maneras. Las nubes IaaS tradicionales han dado paso a entornos de contenedores, y los entornos funcionales y sin servidor están teniendo un rol más destacado. Esto significa que las organizaciones tienen que crear capacidades que simplifiquen la extensión de las protecciones necesarias para brindar resistencia a los nuevos servicios o lugares de ejecución.

Este imperativo tiene que cumplirse hoy. No se trata simplemente de retrasar un solo proyecto para hacer que un nuevo entorno sea resiliente. Cualquier retraso es aplazar el desarrollo de una habilidad importante que puede respaldar una estrategia de infraestructura ágil cuando garantiza que, sin importar cómo se satisfagan las necesidades de infraestructura, se asegure la solidez de los servicios y de las aplicaciones que se ejecutan en ella. Existe un debate sobre la orquestación y la automatización que se necesita para una infraestructura ágil, pero la resistencia ágil es igual de importante.

Hay una serie de componentes en este imperativo que se deben cubrir para brindar una capacidad de recuperación efectiva de manera que sea operacionalmente eficiente en las implementaciones híbridas de múltiples nubes. Algunos de ellos pueden abordarse expandiendo la continuidad del negocio existente y la recuperación ante desastres para incluir recursos de los socios. La mayoría de los ejercicios de planificación de la continuidad del negocio y la recuperación ante desastres consideran los activos propios, lo que limita el alcance en que se tiene en cuenta la capacidad entregada por los proveedores de alojamiento o las nubes públicas. Algo de esto se debe a que, históricamente, esto era complicado de lograr: la mayoría de las prácticas tradicionales de continuidad del negocio y la recuperación ante desastres no podían extenderse fácilmente fuera de las instalaciones, y aquellas que sí podían hacerlo, requerían de una intervención manual importante. Con la automatización y la orquestación adecuadas, la infraestructura local y externa ahora puede tener los mismos niveles de protección.

Otro componente importante del imperativo de la resistencia es impulsado por las necesidades de seguridad de la información. Los entornos híbridos de múltiples nubes tienen una superficie de ataque mucho mayor. Debido al rápido aumento en el uso de herramientas de ataque automatizadas por parte de la comunidad de atacantes, se ha vuelto mucho más fácil encontrar y apuntar a diferentes elementos de una infraestructura de aplicaciones de mayor distribución. Un beneficio adicional de las capacidades de resistencia que admiten múltiples entornos es que hacen posible la recuperación en la infraestructura que no está bajo ataque. Esto puede reducir el riesgo de que cualquier elemento individual de la implementación del proceso completo de la empresa pueda eliminar una aplicación.

Requisitos para la resistencia

Para ofrecer los niveles de funcionalidad necesarios para respaldar entornos híbridos de múltiples nubes, existe un conjunto de requisitos que debe cumplir cualquier enfoque de resistencia. En primer lugar, tiene que extender el conocimiento y la visibilidad en todo el entorno híbrido. Tener un punto de referencia común que pueda actuar como un recurso compartido puede reunir a los equipos y proporcionar una perspectiva más completa del estado actual de la infraestructura de una organización. Para lograr esto, tiene que abarcar recursos físicos y virtuales y brindar perspectivas equivalentes. En todos estos ámbitos, tiene que crear abstracciones de servicio que puedan simplificar las operaciones cuando traduce las capacidades de alto nivel a la funcionalidad nativa de cada entorno. Los enfoques que requieren conocimiento especializado para diferentes dominios no se pueden escalar y harán que el proceso de incorporación de nuevos entornos sea costoso. Tener servicios comunes que los equipos de aplicaciones puedan esperar en diferentes centros tiene múltiples beneficios: las aplicaciones y los servicios se pueden entregar más rápidamente porque se tiene que hacer una pequeña adaptación nueva, y reducen la posibilidad de bloquearse en un entorno particular debido a una reducción de la independencia en la funcionalidad específica del entorno.

Cualquier enfoque también debe ser lo suficientemente flexible como para funcionar bien en diferentes entornos operativos. Tener la agilidad para desplegarse rápidamente puede significar que el establecimiento de protecciones no frena la experimentación o las reacciones rápidas a los cambios del mercado. La escalabilidad debe ser un subproducto natural de este nivel de agilidad. Uno de los principales desafíos de los entornos híbridos es la escala.

Uno de los aspectos de las capacidades de resistencia que debería impulsar el apoyo a una escala mayor es la automatización y orquestación. Vale la pena considerarlo como su propio requisito porque es un elemento importante de cualquier implementación. La automatización y la orquestación efectivas deben ser el vehículo que ofrece abstracciones al tiempo que reduce el volumen de trabajo del equipo de operaciones.

La puntualidad de la recuperación y la amplitud de las opciones de recuperación también son requisitos importantes. En muchos casos, los dos van de la mano porque tener más opciones de recuperación puede permitir la optimización del proceso de recuperación para satisfacer las necesidades de diferentes situaciones. En entornos híbridos, las interrupciones pueden tener muchos factores que están entrelazados, creando dependencias que pueden impedir ciertas rutas de recuperación. Los enfoques eficaces podrán ofrecer alternativas para evitar cualquier problema de bloqueo.

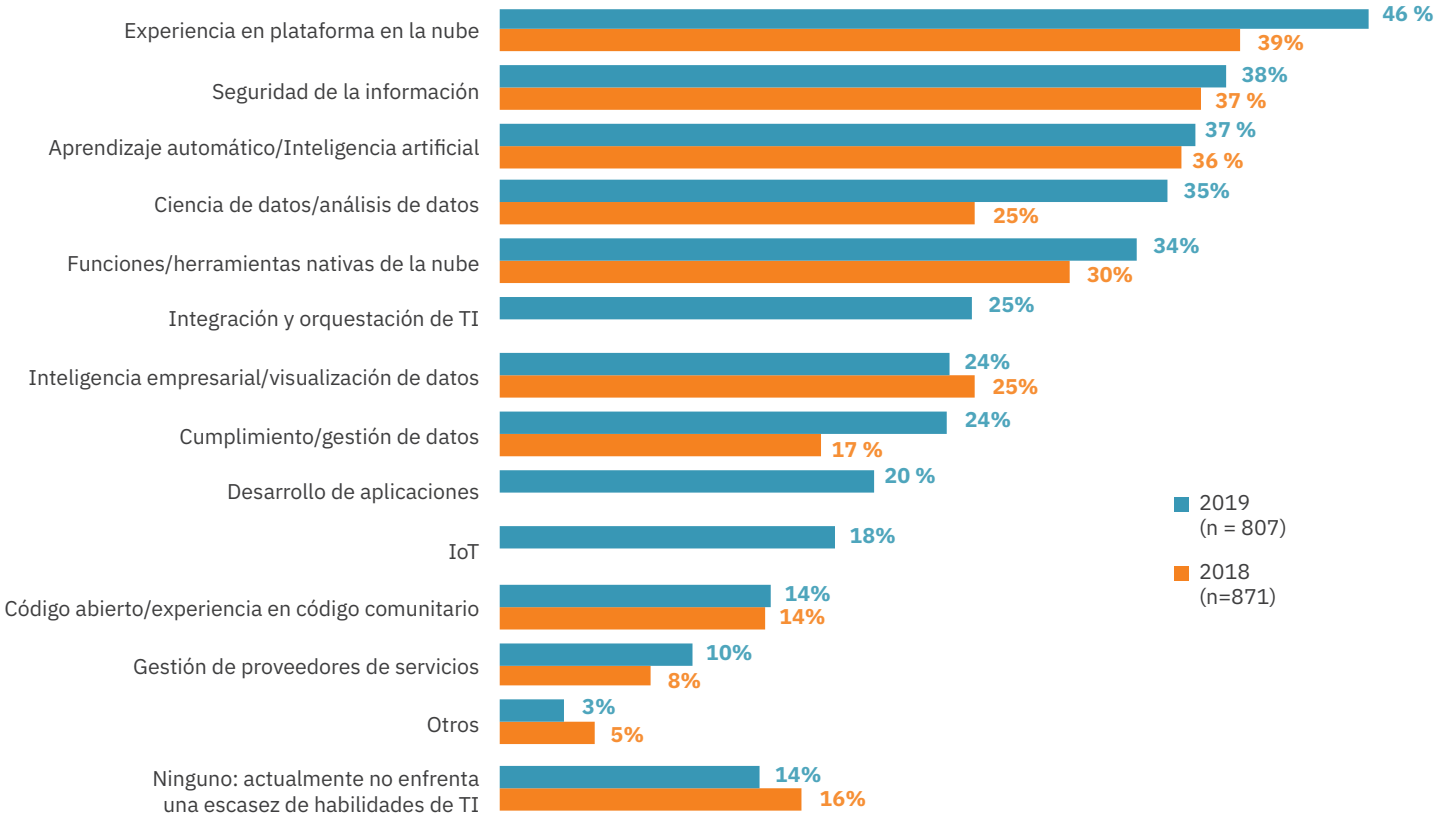
Un enfoque de resistencia que aborde estos requisitos puede hacer que las organizaciones sean más ágiles permitiéndoles adaptarse más rápidamente y recuperarse de los problemas más rápido.

Enfoques para una mayor resistencia

Los entornos híbridos de múltiples nubes tienen suficientes facetas diferentes que pueden ser difíciles de identificar para garantizar la resistencia general. Decidir si extender las protecciones de datos existentes, capitalizar los servicios nativos en nuevos entornos o adoptar métodos completamente nuevos no es sencillo. Tomar decisiones detalladas también puede requerir un conocimiento profundo de los detalles técnicos de los diversos entornos que pueden estar fuera del conjunto de habilidades de los equipos de TI. Es muy probable que no sean expertos en servicios en la nube o alojamiento que sean nuevos para la organización, y tomarse el tiempo para desarrollar esas habilidades retrasaría nuevos servicios y aplicaciones o dejaría abierta la posibilidad de que los riesgos operativos no se identifiquen y mitiguen. Esta es un área en la que un socio proveedor de servicios capaz puede ser útil en particular para identificar problemas y para proporcionar perspectivas sobre cómo tratarlos.

Figura 2: Escasez actual de habilidades por categoría de TI - 2019 y 2018

Fuente: 451 Research's Voice of the Enterprise: Digital Pulse, Organizational Dynamics Quarterly Advisory Report
P: ¿En cuál de las siguientes categorías de TI, si las hay, su organización enfrenta actualmente una grave escasez de habilidades? Indique la que corresponda.



La mayoría de las organizaciones están luchando para mantenerse al día con las habilidades para administrar nuevos modelos de infraestructura. En el estudio del primer trimestre de 2019 Voice of the Enterprise: Digital Pulse de 451 Research, los encuestados dijeron que la experiencia en plataforma en la nube era su mayor falta de habilidades, superando la seguridad de la información (en un 46% a 38%), que fue el líder en encuestas anteriores. En situaciones como esta, puede ser difícil contratar y retener el talento necesario para satisfacer las necesidades operativas, y mucho menos los equipos de personal para tomar decisiones estratégicasTrabajar con un socio proveedor de servicios especializado puede ampliar las habilidades del personal existente y reforzarlas con capacidades de servicio que puedan abordar las complejidades que presentan los modelos híbridos.Una asociación de trabajo permitirá a las organizaciones lograr la escala necesaria en sus propios términos.

Este es un proceso que puede tener beneficios importantes para la organización.La implementación de capacidades integrales de resistencia híbrida puede ayudar a las organizaciones a adelantarse a las necesidades de sus equipos de desarrollo.Pueden administrar las necesidades de resistencia de datos hoy en día, pero, lo que es más importante, pueden proporcionar una base que los equipos de desarrollo puedan aprovechar con el tiempo, lo que hace que los desarrolladores sean menos dependientes de las opciones nativas y propietarias que existen en los proveedores individuales de la nube.Puede ampliar las opciones de una organización para la elección de infraestructura, lo que facilita la optimización de los entornos para adaptarse a las necesidades de la empresa.Al mismo tiempo, puede permitir que las organizaciones respondan más rápidamente a las condiciones cambiantes del mercado y las relaciones con los proveedores.

Conclusiones y recomendaciones

El cambio a modelos de infraestructura híbrida de múltiples nubes está en marcha para muchas organizaciones.Ofrece beneficios que pueden ser convincentes, y muchas organizaciones elegirán ese modo de operación sin tener en cuenta su impacto en la confiabilidad y en la resistencia de sus entornos de aplicación.

Todas las organizaciones, particularmente aquellas que aún no han adoptado por completo este modelo, deben considerar cómo abordar los riesgos asociados y controlarlos de una manera operativa eficiente.Abordar esto ahora puede ayudar a controlar el entorno actual, así como brindar un medio para manejar con confianza la expansión de la infraestructura.Es un proceso cuyo valor puede maximizarse trabajando con un socio capaz que pueda brindar orientación en un área donde a menudo hay brechas considerables de las habilidades.

El aumento de la resistencia de las aplicaciones en un mundo híbrido tiene muchas complejidades, y es un objetivo extremadamente valioso de alcanzar.

Perfil del patrocinador

Lograr la resistencia en un entorno híbrido de múltiples nubes requiere una plataforma integrada para proteger los datos, mantener una alta disponibilidad y recuperar rápidamente la infraestructura y los sistemas de tecnología vital en caso de un desastre. La construcción de una plataforma de este tipo comienza con una estrategia de resistencia integrada y un plan que abarca tecnologías, procesos comerciales, personas y políticas.

IBM Services ayuda a los clientes a desarrollar e implementar estrategias y soluciones de resistencia en toda la empresa para ayudar a eliminar el riesgo de su proceso hacia un entorno híbrido de múltiples nubes. Ayuda a los clientes a optimizar la disponibilidad y la continuidad de la empresa y de TI, ya sea en el día a día de las operaciones comerciales y de TI o en condiciones inesperadas, como ataques cibernéticos, fallas de hardware y software, fallas de proveedores y desastres naturales o provocados por el ser humano.Es compatible con empresas en entornos híbridos de múltiples nubes, incluidos entornos de nube pública, nube privada, colocación y centros de datos locales. También cuenta con una práctica sólida de múltiples nubes en los proveedores de nube populares, incluidos Red Hat OpenShift, AWS, Azure, Google Cloud e IBM Cloud.

La cartera de ofertas de resistencia de IBM incluye servicios de asesoramiento, infraestructura, diseño o construcción, implementación y gestión, que van desde la protección de datos, la virtualización, la recuperación ante desastres y la resistencia cibernética hasta el cálculo a gran escala, la resistencia de datos y aplicaciones, la alta disponibilidad y las instalaciones y centros de datos eficientes. Utilizando enfoques definidos por software, herramientas basadas en la nube y soluciones de orquestación, los servicios de IBM están diseñados para ayudar a los clientes a proteger los sistemas de TI, mantener las aplicaciones críticas en funcionamiento y lograr una recuperación rápida y confiable en el caso de interrupciones. Para obtener más información, visite: *ibm.biz/multicloud-resiliency*.

CONTENIDO PROPORCIONADO POR: IBM

Acerca de 451 Research

451 Research es una empresa líder en investigación y asesoramiento en tecnología de la información que se centra en la innovación tecnológica y la disrupción del mercado.Más de 100 analistas y consultores brindan información esencial a más de 1000 organizaciones de clientes a nivel mundial a través de una combinación de investigación y datos sindicados, servicios de asesoramiento y comercialización, y eventos en vivo. Fundada en 2000 y con sede en Nueva York, 451 Research es una división de The 451 Group.

NUEVA YORK
Chrysler Building
405 Lexington Avenue,
9.o Piso
Nueva York, NY 10174
+1 212 505 3030

SAN FRANCISCO
505 Montgomery Street,
Suite 1052
San Francisco, CA 94111
+1 212 505 3030

LONDRES
Paxton House
30, Artillery Lane
Londres, E1 7LS, Reino Unido
+44 (0) 203 929 5700

BOSTON
75-101 Federal Street
Boston, MA 02110
+1 617 598 7200