

LA SEGURIDAD COMO FOCO DE ATENCIÓN

La clave para la estrategia de nube híbrida empresarial

Resumen ejecutivo

Las organizaciones de TI modernas que adoptan una visión integral de su infraestructura tecnológica, incluidos los modelos “*on-premises*” (en el sitio) y en la nube, estarán mejor posicionadas para hacer frente a las vulnerabilidades de seguridad. En la actualidad, las organizaciones enfrentan más incertidumbre que nunca. A medida que las amenazas del ciberespacio aumentan en número y complejidad, la necesidad de contar con un entorno digital seguro es primordial. A su vez, las organizaciones buscan adaptar sus estrategias de infraestructura para brindar un mejor soporte a sus clientes y a cargas de trabajo cada vez más complejas sin sacrificar la seguridad.

En enero de 2020, IBM publicó un estudio que había encargado a Forrester Consulting en septiembre de 2019. En él se evalúa cómo las organizaciones desarrollan e implementan sus estrategias de infraestructura de TI. Para explorar el tema, Forrester realizó una encuesta en línea a 350 encargados de tomar decisiones de TI en empresas multinacionales de distintos sectores. Descubrimos que las organizaciones crean entornos de nube híbrida con distintas nubes públicas, nubes privadas alojadas e infraestructura *on-premises*.

Las empresas de TI realizan grandes inversiones en infraestructura para superar los desafíos de seguridad actuales y futuros.

Las organizaciones se centran no solo en atender las crecientes demandas de la infraestructura de TI existente, sino también en garantizar la seguridad al tiempo que migran hacia las nuevas tecnologías.

El 58 %

mencionan atender las crecientes demandas de la infraestructura de TI *existente* como una de las principales cinco prioridades de este año.

El 56 %

están ampliando o implementando *nuevas* tecnologías de infraestructura este año.

El 77 %

consideran que la *seguridad* es un factor importante a la hora de realizar una compra de infraestructura.

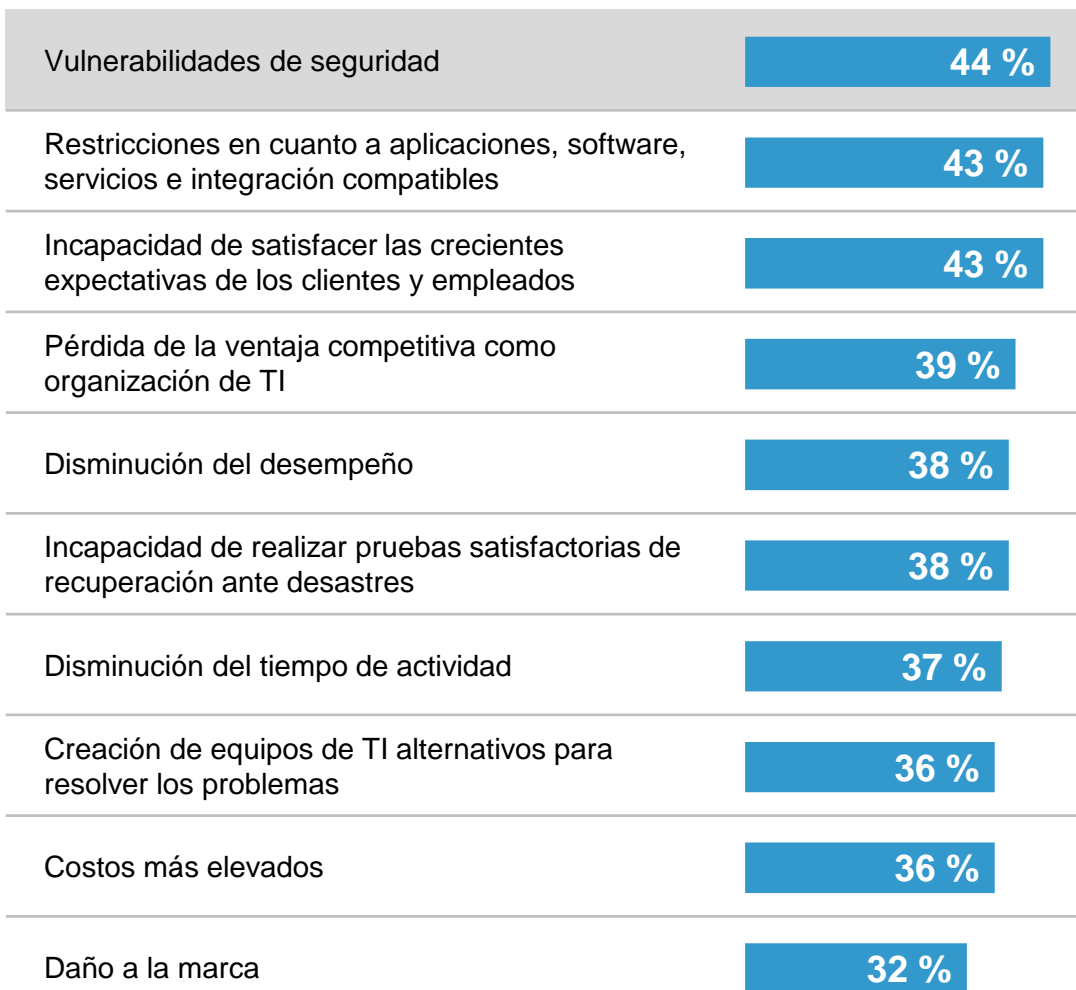
En tiempos de incertidumbre, con cargas de trabajo crecientes y cambiantes, las organizaciones de TI deben abordar la seguridad de manera integral al adaptar su infraestructura.

Refuerce la seguridad ante la incertidumbre al modernizar la estrategia de infraestructura de su empresa:

- Actualice continuamente su estrategia de protección contra las vulnerabilidades de seguridad
- Mantenga la infraestructura *on-premises* como parte de su estrategia de seguridad integral
- Aproveche la infraestructura *on-premises* para mejorar la seguridad de las cargas de trabajo y las aplicaciones críticas

Los principales riesgos de retrasar la renovación de la infraestructura

(Se muestran los 10 primeros, calificados del 1 al 5)



Base: distintos responsables de la toma de decisiones a nivel mundial sobre entornos de infraestructura de TI
Fuente: Estudio realizado por Forrester Consulting por encargo de IBM, septiembre de 2019

© 2020 Forrester. Se prohíbe la reproducción

No estar al día con las actualizaciones de la infraestructura crea amenazas

El 38 % de los responsables de la toma de decisiones afirman que sus empresas se han enfrentado a pruebas fallidas de recuperación ante desastres tras una demora en la actualización.

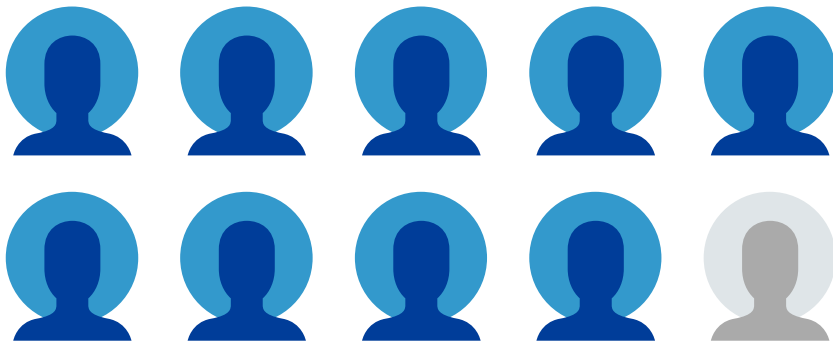
El 61 % han postergado la renovación de la infraestructura unas cuantas veces o más en los últimos cinco años.

Mantenga la infraestructura *on-premises* como parte de su estrategia de seguridad integral

Las empresas siguen diversificando su infraestructura con plataformas de nubes privadas, incluso *on-premises*. La infraestructura *on-premises* sigue siendo fundamental y una parte crítica de una estrategia de nube híbrida segura y resiliente.

9/10

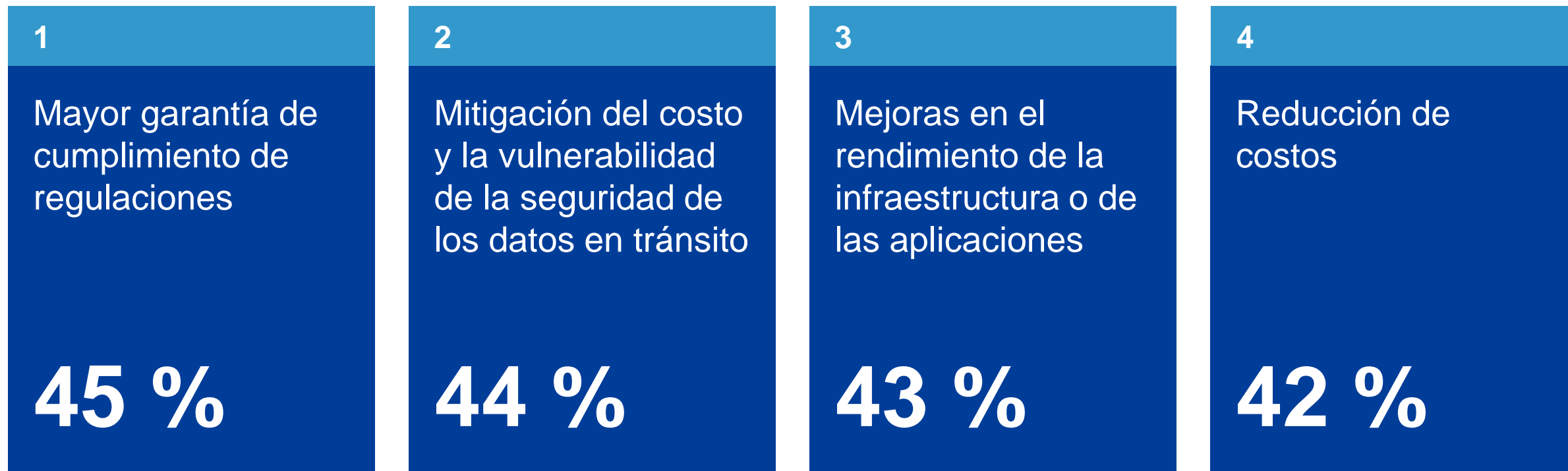
coinciden en que la infraestructura *on-premises* es una parte fundamental de las estrategias de nube híbrida de sus empresas.



El **40 %** señalan que la incapacidad de la nube pública de satisfacer las **necesidades de seguridad** es una razón para mantener la infraestructura fuera de la plataforma de dicha nube.

Aproveche la infraestructura *on-premises* para mejorar la seguridad de las cargas de trabajo y las aplicaciones críticas

Principales motivos para utilizar recursos *on-premises* para determinadas cargas de trabajo y aplicaciones:



Recomendaciones clave



Dé prioridad a la actualización de la infraestructura. Establezca una estrategia de infraestructura clara e integral que reconozca el compromiso permanente con las cargas de trabajo *on-premises* y se centre en las cuestiones de seguridad como motor principal de las decisiones de actualización. Incluso las empresas que luchan por sobrevivir en la pandemia deberían considerar la actualización de la infraestructura relacionada con la seguridad como prioridad máxima.



Establezca una estrategia de datos para fundamentar las decisiones sobre la carga de trabajo para promover la seguridad y el desempeño. Evite caer en la trampa de considerar únicamente los costos al tomar decisiones sobre la carga de trabajo. Mantenga en primer lugar la repercusión de la ubicación de los datos y ajuste el desempeño general en función de la gestión de los problemas de seguridad y de latencia a través de los datos y las grandes cargas de trabajo asociadas en la misma plataforma.



Desarrolle un modelo comercial irrefutable. El desempeño es especialmente crítico, ya que tiene un impacto significativo en la experiencia del cliente (CX) y en la percepción de la marca. Los ejecutivos que no pueden comprometerse a una actualización completa pueden aprovechar las opciones de actualización de la infraestructura basadas en suscripciones para contar con un futuro más flexible si su estrategia cambia.



Descargue el estudio completo

Metodología

En este estudio, Forrester realizó una encuesta en línea a 350 responsables de la toma de decisiones a nivel mundial sobre los entornos de la infraestructura de TI para evaluar la forma en que las organizaciones desarrollan y aplican sus estrategias de infraestructura. En la encuesta participaron los responsables de la toma de decisiones en materia de TI en las áreas de infraestructura y operaciones, gestión o mantenimiento de aplicaciones, o desarrollo de software. Se formularon preguntas a los participantes sobre los entornos utilizados para las diferentes cargas de trabajo y la inversión en infraestructura. Se ofreció a los encuestados un pequeño incentivo como muestra de agradecimiento por el tiempo dedicado a la encuesta. El estudio comenzó en agosto de 2019 y finalizó en septiembre del mismo año.

ACERCA DE FORRESTER CONSULTING

Forrester Consulting presta servicios de consultoría basados en análisis objetivos e independientes para ayudar a los líderes a cosechar éxitos en sus organizaciones. Forrester Consulting ofrece desde reuniones estratégicas hasta proyectos personalizados y lo pone en contacto directo con analistas e investigadores centrados en abordar las dificultades concretas a las que se enfrenta su empresa. Para obtener más información, visite forrester.com/consulting.

© 2020, Forrester Research, Inc. Todos los derechos reservados. Queda estrictamente prohibida la reproducción no autorizada. La información está basada en los recursos disponibles. Las opiniones expresadas reflejan juicios de valor válidos en su momento y están sujetas a cambios. Forrester®, Technographics®, TechRankings, Forrester Wave, RoleView, TechRadar, Total Economic Impact y el logotipo de CX son marcas comerciales de Forrester Research, Inc. El resto de marcas comerciales son propiedad de sus respectivas empresas. Para obtener más información, visite forrester.com. [E-45084]

Directora del proyecto:

Cynthia Hicks,
Asesora de Impacto en el Mercado

Colaboraron en la investigación:

Grupo de investigación de CIO de Forrester