

# Migración/transformación en la nube

Construya redes críticas seguras y resilientes

Servicios para acelerar la adopción de la nube

## RESUMEN DEL IMPACTO



### Simplifica la transformación en la nube

Agiliza las migraciones al combinar visibilidad total, aprovisionamiento automatizado e integración directa con diversos partners de la nube.



### Mejora la gobernanza y el cumplimiento en la nube

Mantiene un inventario exhaustivo de los activos para simplificar las auditorías, exponer riesgos ocultos y reducir el despilfarro de recursos.



### Reduce la complejidad operativa

Acelera los despliegues y minimiza los errores y las interrupciones mediante la gestión de los servicios de red fundamentales en entornos híbridos y multinube desde una única API e interfaz.



### Refuerza la postura de seguridad

Utiliza inteligencia predictiva para detectar el tráfico sospechoso y malicioso en todo el entorno híbrido y multinube, lo que detiene las amenazas antes de que se propaguen.

## 63 %

más confianza en la visibilidad de la nube<sup>1</sup>

## 44 %

menos interrupciones en la nube, con una velocidad de recuperación un 38 % mayor<sup>1</sup>

## 82 %

de mayor rapidez en la resolución de problemas<sup>2</sup>

## 75 %

menos tiempo dedicado a gestionar recursos de red<sup>2</sup>

## INTRODUCCIÓN

En su afán por ser más rápidas, ágiles y competitivas, las organizaciones están trasladando una mayor parte de su infraestructura de TI empresarial a la nube. A medida que avanzan en su transición a la nube (ya sea mediante migraciones de tipo «lift-and-shift», refactorización de aplicaciones o con la adopción de aplicaciones nativas en la nube), muchas se enfrentan a una barrera importante: la complejidad operativa fuera de control. Sin una forma sencilla y sistemática de controlar los servicios de red críticos en la empresa — tanto en entornos de nube como on-prem—, esa complejidad empieza a dificultar la visibilidad y la gobernanza de TI, amplía la superficie de ataque y hace que los nuevos despliegues sean más lentos, arriesgados y costosos.

## DESAFÍO

Casi toda transición a la nube comienza por integrar los entornos y aplicaciones en la nube con las operaciones tradicionales de TI. Este cambio a entornos de TI híbridos introduce complejidad y riesgos importantes, y a menudo interrumpe flujos de trabajo bien establecidos en múltiples equipos. Es especialmente así en el caso de los servicios fundamentales del DNS, DHCP y gestión de direcciones IP (IPAM), que interconectan ubicaciones, dispositivos y aplicaciones.

Cada proveedor de servicios en la nube utiliza sus propias convenciones de nomenclatura, conjuntos de herramientas y flujos de trabajo dedicados para aprovisionar nuevos entornos y llevar a cabo otras operaciones básicas de red, ninguno de los cuales se aplica a las cargas de trabajo locales o a las plataformas en la nube de la competencia. El resultado es un entorno de TI altamente fragmentado que aumenta los errores de configuración y las interrupciones, introduce puntos ciegos peligrosos y añade tiempo, esfuerzo y riesgo adicionales a casi todas las tareas de red.

### Operaciones complejas y aisladas

En las primeras etapas de transición a la nube, muchas organizaciones optan por utilizar las herramientas nativas de cada proveedor de la nube para administrar el DNS, DHCP y la gestión de direcciones IP en el nuevo entorno, al tiempo que mantienen los flujos de trabajo tradicionales para las redes on-prem. Aunque este enfoque permite a la organización avanzar en sus objetivos relativos a la nube, añade capas adicionales de complejidad que dificultan la centralización y la automatización de las operaciones.

Los equipos deben cambiar constantemente entre distintas herramientas en la nube y el entorno on-prem para aprovisionar y supervisar los servicios de red críticos en cada entorno — un esfuerzo manual y duplicado que aumenta significativamente la probabilidad de cometer errores de configuración, principal causa de las interrupciones. A medida que la empresa añade más proveedores de nube para evitar puntos únicos de fallo y acceder a las ventajas de cada proveedor, la complejidad no hace sino aumentar (figura 1).

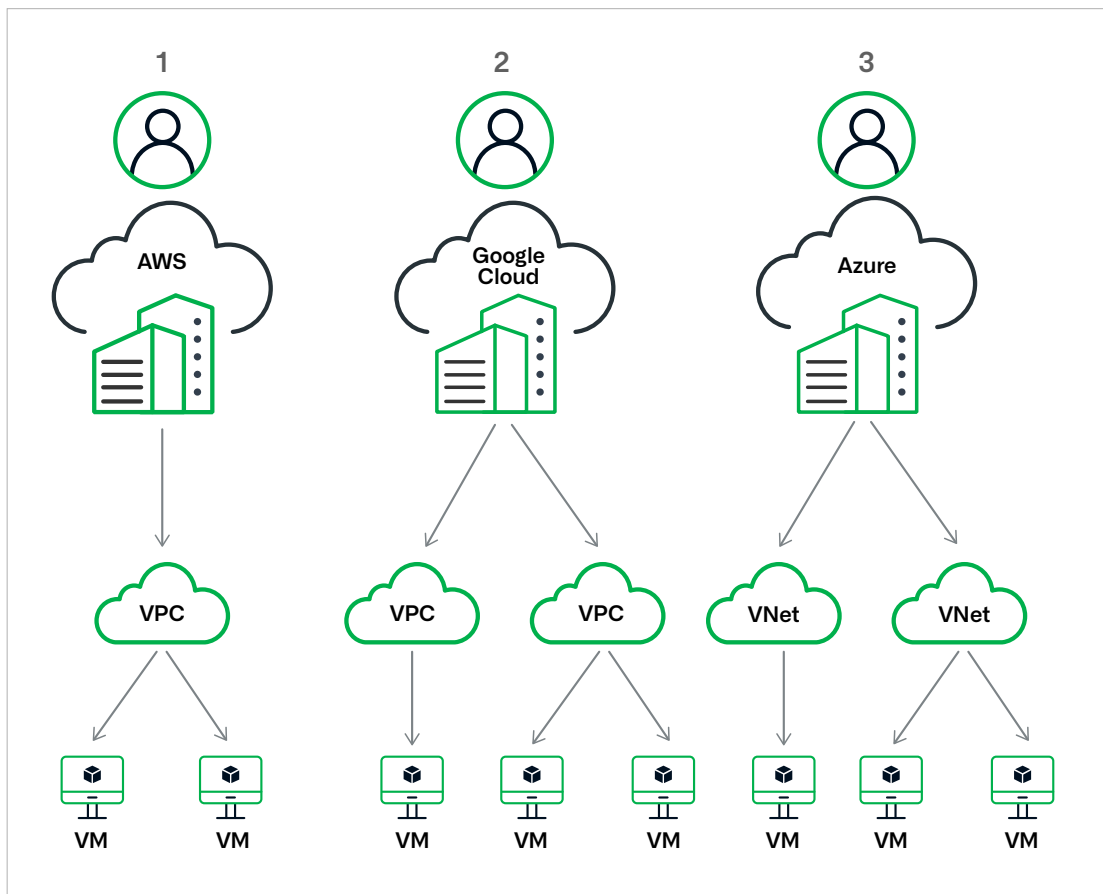


Figura 1. La fragmentación híbrida y multinube obliga a los equipos a duplicar el esfuerzo entre proveedores para cada nube privada virtual (VPC), red virtual (VNet), subred y máquina virtual (VM) que se despliega

### Visibilidad fragmentada

La fragmentación de TI obliga a los equipos a depender de múltiples conjuntos de herramientas especializadas para supervisar el entorno híbrido, con los que solo captan una visión parcial. Como resultado, entender qué está conectado a la red —y no digamos monitorizar servicios empresariales críticos— resulta excepcionalmente difícil. Estos puntos ciegos complican las auditorías de cumplimiento y aumentan el riesgo de que se produzcan solapamientos de rangos de IP y la inactividad asociada. También debilitan la gobernanza efectiva de la nube, lo que da lugar a recursos huérfanos, crean incoherencias en las políticas y, en muchos casos, dan lugar a una importante infrautilización de los costosos rangos de direcciones IP públicas.

## Los procesos lentos y manuales socavan los objetivos de la nube

En ausencia de visibilidad centralizada y de información de IP autoritativa, los equipos de TI tienen dificultades para seguir el ritmo que exige una empresa basada en la nube. Los equipos de NetOps y CloudOps terminan por trabajar en silos y comunicarse mediante tickets de soporte y procesos manuales fuera de banda, que ralentizan los despliegues y erosionan el retorno de la inversión (ROI) de la nube. Si aún se requieren semanas para proporcionar nuevas zonas de aterrizaje en la nube, la organización no puede virar rápidamente para captar nuevas oportunidades ni superar a los competidores que acceden a nuevos mercados, si bien esos factores son los que impulsaron la adopción de la nube en primer lugar.

### Riesgo elevado

Las empresas innovadoras crecen en la nube, ya que pueden crear nuevos entornos y aplicaciones en cuestión de minutos. Sin embargo, con el tiempo, esa agilidad da lugar a nuevos desafíos, ya que los recursos de la nube se generan y luego se abandonan, lo que plantea importantes riesgos de seguridad y cumplimiento. Por ejemplo, es común que los equipos desactiven aplicaciones en la nube o sitios web que ya no se utilizan, pero a menudo olvidan eliminar los registros del DNS que apuntan a ellos, lo que deja un blanco fácil para los ciberatacantes que buscan secuestrar los dominios de la organización y comprometer la marca. La fragmentación de TI también ralentiza la velocidad a la que los equipos pueden responder a los problemas de red y a los incidentes de seguridad.

## SOLUCIÓN

Infoblox ayuda a las organizaciones a reducir la complejidad de la nube híbrida para simplificar las migraciones, minimizar el riesgo y acceder a todo el valor que cabe esperar de la transformación en la nube. Con un único plano de gestión centralizado para servicios de red críticos en entornos híbridos y multinube, las empresas obtienen la visibilidad, agilidad y control de extremo a extremo que conforman la base de una empresa de éxito en la nube.

### Migraciones a la nube simplificadas

Infoblox unifica las complejas operaciones de TI híbridas y multinube, lo que permite a los equipos aprovisionar y gestionar de forma centralizada los servicios de red fundamentales en todo el entorno digital desde una sola API e interfaz. Ya efectúen migraciones de tipo «lift-and-shift», refactoricen aplicaciones o empleen una combinación de estrategias, los equipos pueden utilizar convenciones de nomenclatura y flujos de trabajo coherentes tanto en entornos de nube como on-prem, lo que simplifica enormemente las migraciones.

Además, las integraciones nativas con los principales proveedores de nube (AWS, Microsoft Azure, Google Cloud), sistemas de bases de datos de gestión de la configuración (ServiceNow) y soluciones de red y seguridad de terceros (Meraki, CrowdStrike) aceleran la rentabilización de las inversiones en la nube, al tiempo que permiten a las empresas trabajar sin problemas con los socios de nube de su elección.

### Visibilidad total

Mediante un único punto de control universal para todo el entorno híbrido, las organizaciones pueden supervisar de forma centralizada los servicios de red críticos a fin de eliminar puntos ciegos y optimizar la gobernanza en la nube. Los equipos de TI obtienen visibilidad casi en tiempo real y en un solo panel de control de todos los activos en la huella de nube híbrida —cargas de trabajo, dispositivos IoT/OT y endpoints en todos los espacios IP—, lo que simplifica drásticamente las auditorías de cumplimiento.

Los equipos pueden monitorizar el uso de direcciones IP y subredes para identificar rápidamente recursos olvidados e infrautilizados, mejorar la planificación de la capacidad y detectar rangos de IP superpuestos y otros antes de que estos riesgos provoquen interrupciones de los servicios. Además, al mantener un inventario exhaustivo de activos e información autorizada sobre la IP de los dispositivos de toda la empresa, los equipos pueden responder a los problemas de la red y a los incidentes de seguridad con mucha más rapidez. En lugar de revisar manualmente hojas de cálculo para emparejar los registros de red con puntos de conexión específicos, los equipos pueden localizar instantáneamente los dispositivos afectados, conocer su ubicación y el contexto asociado en segundos, y solucionar problemas antes de que se conviertan en crisis.

### Operaciones rápidas y eficientes

Cuando las organizaciones parten de una amplia visibilidad empresarial en entornos híbridos y luego añaden una capa de gestión común, adquieren la base para simplificar y optimizar la colaboración entre equipos. La asignación automatizada de direcciones IP, basada en políticas, permite que los equipos de CloudOps pueden actuar con mayor rapidez, sin tener que esperar a que NetOps responda a solicitudes en tickets. Reducir los trasposos manuales también reduce el riesgo de errores e interrupciones.

La capacidad de mantener flujos de trabajo y políticas coherentes en toda la empresa facilita enormemente la automatización de los entornos de red híbridos. Al automatizar con una única API (en lugar de mantener scripts independientes para cada nube y entorno on-prem), las organizaciones pueden acelerar los despliegues gracias a herramientas de infraestructura-como-código (IaC) —como Terraform y Ansible— que normalizan y automatizan la provisión de recursos (Figura 2).

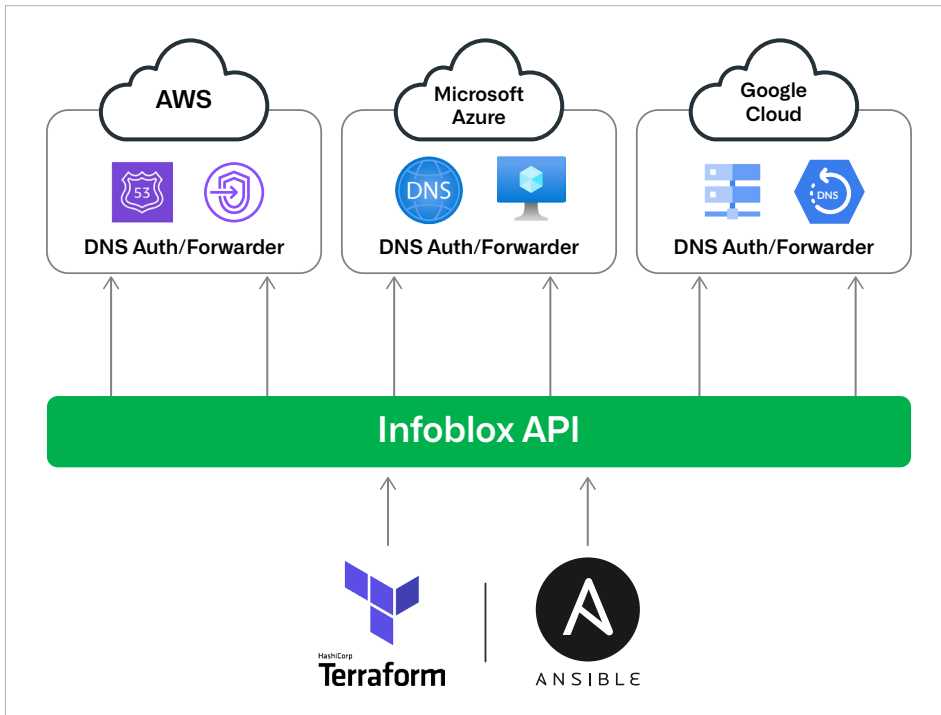


Figura 2. La API de Infoblox permite una configuración e implementación más rápida de todos los proveedores de nube

### Postura de seguridad mejorada

Expandirse a nuevos entornos en la nube puede abrir la puerta a capacidades potentes, pero también aumenta la superficie de ataque, puesto que la complejidad añadida dificulta monitorizar y proteger el entorno. Infoblox proporciona capacidades avanzadas de Protective DNS para bloquear preventivamente las amenazas tan pronto como tratan de comunicarse con el mundo exterior. Al supervisar cada consulta del DNS en todo el entorno híbrido, estas defensas detectan inmediatamente los intentos de conexión de dominios sospechosos o maliciosos, rastrean el origen y bloquean la actividad, lo que proporciona una protección integrada contra los ataques originados en cualquier carga de trabajo en la nube o on-prem.

## UNIFIQUE LAS OPERACIONES DE TI HÍBRIDAS PARA ACELERAR LA TRANSFORMACIÓN EN LA NUBE

En el mercado digital moderno, la velocidad y la agilidad definen cada vez más el éxito de una empresa. Mantenerse competitivo significa poder acceder rápidamente a nuevos mercados, cambiar de estrategia e incorporar nuevas innovaciones digitales y de IA. Por todo ello, migrar a la nube es una prioridad empresarial urgente. Sin embargo, si las organizaciones no construyen una base ágil y automatizada para los servicios de red críticos de los que dependen todas las cargas de trabajo en la nube y on-prem, sus iniciativas en la nube pueden verse rápidamente inmersas en la complejidad.

Infoblox proporciona la gestión unificada, la visibilidad y la agilidad necesarias para sustentar una transformación de éxito en la nube. Gracias a unas operaciones de red automatizadas y basadas en políticas, así como a una visibilidad completa en todo el entorno híbrido, las empresas pueden reducir errores e interrupciones, acelerar las implementaciones y garantizar resiliencia y seguridad sin cortes en cada proceso de transición a la nube.

## Ejemplos reales de clientes:

- Un proveedor de servicios financieros identificó y eliminó 847 recursos huérfanos en la nube, lo que le permitió ahorrar 180 000 USD al año y reducir los riesgos de seguridad mediante la detección proactiva de activos y gobernanza.
- Una institución sanitaria redujo los tiempos de respuesta en un 75 % utilizando la asignación universal de direcciones IP y la visibilidad de activos de Infoblox, lo que garantizó una recuperación más rápida de las interrupciones y los incidentes.
- Un minorista estadounidense aceleró enormemente las implementaciones, al lanzar nuevas tiendas de forma remota en cuestión de minutos, lo que permitió una expansión comercial más rápida con unos gastos operativos mínimos.

## PRESTACIONES CLAVE

**Control unificado en redes híbridas:** Reduzca los errores y las interrupciones con flujos de trabajo consistentes y normalizados para las operaciones del DNS, DHCP e IP tanto en la nube como en entornos on-prem.

**Visibilidad total:** Supervise de forma centralizada todos los recursos en la nube y on-prem desde una única interfaz para simplificar las auditorías, optimizar la gobernanza y exponer riesgos ocultos.

**Migraciones más rápidas y sencillas:** Acelere el aprovisionamiento de nuevos entornos de nube con automatización de laC basada en políticas, que reduce los plazos de implementación de semanas a minutos.

**Seguridad del Protective DNS:** Amplíe el footprint de la nube con confianza y bloquee preventivamente las amenazas en todo el entorno antes de que se propaguen.

1. *9 Pitfalls of Not Using Enterprise-Grade DDI*, Enterprise Strategy Group (ESG), febrero de 2025.

<https://www.infoblox.com/es/resources/analyst-report/network-modernization-ddi-report/>

2. *Infoblox Authoritative IPAM for DNS and DHCP*, junio de 2022.

<https://www.infoblox.com/resources/analyst-report/tolly-report-infoblox-authoritative-ipam-for-dns-and-dhcp/>



Infoblox integra redes, seguridad y nube con una plataforma DDI protectora que ofrece resiliencia y agilidad empresarial. Nos integramos en entornos híbridos y multinube, automatizamos los servicios de red críticos y protegemos la empresa de forma preventiva, proporcionando la visibilidad y el contexto necesarios para avanzar rápidamente sin compromiso.

**Sede corporativa**  
2390 Mission College Blvd, Ste. 501  
Santa Clara, CA 95054 (EE. UU.)

+1.408.986.4000  
[www.infoblox.com/es](http://www.infoblox.com/es)