

LIBRO BLANCO

# Centros de datos resilientes

Gestión del riesgo de contratistas  
y proveedores a lo largo de todo  
el ciclo de vida del activo

Agosto de 2026

[www.achilles.com](http://www.achilles.com)

 **Achilles**  
Global Risk Management

# Contenido

---

## **Sección uno**

Introducción

## **Sección dos**

El papel crítico de las cadenas de suministro en la resiliencia de los centros de datos

## **Sección tres**

Entorno de riesgo uno: construcción

## **Sección cuatro**

Entorno de riesgo dos: resiliencia operativa

## **Sección cinco**

Gestión dinámica del riesgo de la cadena de suministro

## **Sección seis**

De la homologación de proveedores a la inteligencia continua de la cadena de suministro

## **Sección siete**

Cinco preguntas que todo operador de centros de datos debería poder responder

## **Sección ocho**

El futuro de la resiliencia de la cadena de suministro





# Introducción

---

**La carrera mundial por construir infraestructuras preparadas para la inteligencia artificial ha desencadenado una de las mayores oleadas de inversión en centros de datos de la historia. Los operadores hiperescalables, los proveedores de colocación y las grandes empresas están ampliando su capacidad a una velocidad sin precedentes, a menudo en regiones geográficas completamente nuevas.**

McKinsey estima que las empresas invertirán casi 7 billones de dólares en infraestructuras de centros de datos en todo el mundo de aquí a 2030, y que más del 40 % de esa inversión se realizará en Estados Unidos. A medida que se acelera el despliegue de capital, también aumentan la escala y la complejidad del ecosistema de contratistas y proveedores necesario para materializarlo.

Un centro de datos moderno depende de cientos de organizaciones especializadas a lo largo de todo su ciclo de vida. Durante la construcción, suministran infraestructuras altamente técnicas bajo una intensa presión de plazos. Una vez que el centro entra en operación, un ecosistema diferente de proveedores de mantenimiento, ingenieros y contratistas especializados resulta esencial para

mantener en funcionamiento una infraestructura crítica.

Históricamente, los contratistas se consideraban proveedores externos de servicios que apoyaban las actividades de construcción y mantenimiento. Hoy, su función se ha convertido en una parte integral de la resiliencia y la disponibilidad de la infraestructura digital. A medida que los centros de datos son más complejos, la capacidad, la fiabilidad y la resiliencia operativa de los contratistas influyen directamente en la continuidad de los servicios digitales de los que dependen las economías modernas.

Cada fase introduce riesgos diferentes, pero ambas dependen de una capacidad común: la visibilidad continua de la cadena de suministro.



# El papel crítico de las cadenas de suministro en la resiliencia de los centros de datos

El rápido crecimiento de la inteligencia artificial, la computación en la nube y los servicios digitales está impulsando uno de los mayores programas de expansión de infraestructuras de la historia reciente. En Norteamérica, Europa y Asia-Pacífico, los propietarios y operadores de centros de datos están invirtiendo miles de millones de dólares en nueva capacidad para responder a una demanda de potencia de computación sin precedentes.

Las instalaciones actuales también son considerablemente más grandes y complejas. Hace solo unos años, los centros que requerían alrededor de 20-30 MW de potencia se consideraban desarrollos a gran escala. Hoy, los campus hiperescalables se diseñan cada vez más para soportar 100 MW o más, y varios proyectos anunciados prevén alcanzar varios cientos de megavatios. Estos proyectos requieren amplias obras civiles, infraestructuras eléctricas especializadas, sistemas avanzados de refrigeración, conexiones de alta tensión, generación eléctrica de respaldo y sofisticadas medidas de seguridad física y cibernética, todo ello ejecutado en plazos reducidos.

Se trata, además, de un entorno de

seguridad de graves consecuencias. Los datos laborales de Estados Unidos recopilados por la Electrical Safety Foundation International muestran que la construcción concentró 907 de las 2.070 muertes laborales por electrocución registradas entre 2011 y 2024.

Al mismo tiempo, la disponibilidad de terrenos adecuados y de capacidad eléctrica está redefiniendo dónde se construyen los centros de datos. En lugar de concentrarse únicamente en polos tecnológicos consolidados, los operadores se expanden cada vez más hacia mercados secundarios y emergentes, donde la disponibilidad energética, las condiciones de planificación y los costes de desarrollo pueden resultar más favorables.

JLL señala que el 64 % de los 35 GW de capacidad de centros de datos en construcción en Norteamérica se encuentra ya en “mercados frontera”, fuera de los polos consolidados. El oeste de Texas, Tennessee, Wisconsin y Ohio figuran entre los principales beneficiarios de este cambio geográfico. Al mismo tiempo, el 92 % de la capacidad norteamericana en construcción ya está comprometida de antemano. JLL la identifica como capacidad arrendada



Más de 35 GW de nueva capacidad están en construcción en Norteamérica, frente a los 39 GW que ya se encuentran operativos.

mediante contratos vinculantes o como desarrollos hiperescalables para uso propio.

Esta expansión se produce en un contexto de escasez persistente de mano de obra en los sectores de la construcción y la ingeniería. La demanda de electricistas con experiencia, ingenieros de puesta en marcha, especialistas mecánicos y otros perfiles cualificados sigue superando a la oferta. Esto aumenta la competencia por los contratistas adecuados y añade presión a la ejecución de los proyectos. Como resultado, las organizaciones dependen con frecuencia de amplias redes de subcontratistas y proveedores especializados para cumplir los plazos, lo que crea cadenas de suministro cada vez más complejas y difíciles de supervisar de forma eficaz.

El reto va más allá de la construcción. Una vez que una instalación entra en operación, mantener una disponibilidad continua depende de un ecosistema de proveedores diferente, pero igual de crítico. Los contratistas de mantenimiento, los proveedores de gestión de instalaciones, los especialistas en generadores y sistemas de alimentación ininterrumpida (SAI/UPS), los ingenieros de refrigeración, los

contratistas de protección contra incendios, los proveedores de seguridad y los socios de infraestructura de red desempeñan una función esencial en la resiliencia operativa. Muchas de estas organizaciones trabajan en varios emplazamientos, con personal, subcontratistas, certificaciones y coberturas de seguro que cambian durante la vida útil del activo.

Para los operadores de centros de datos, la disponibilidad (uptime) es la medida definitiva del rendimiento. Cada contratista que trabaja en una infraestructura crítica puede influir en la resiliencia operativa, ya sea por la calidad de la instalación durante la construcción o por la fiabilidad de las actividades de mantenimiento una vez que el centro está activo. A medida que las redes de contratistas crecen, resulta cada vez más difícil mantener la visibilidad sobre las cualificaciones de los proveedores, su resiliencia financiera, sus seguros, su cumplimiento y sus relaciones con subcontratistas mediante procesos manuales o revisiones periódicas.

A diferencia de lo que ocurre en muchos proyectos de infraestructura, el riesgo de los proveedores no termina cuando finaliza la construcción. Simplemente cambia.

# Entorno de riesgo uno: construcción

## Los proyectos complejos dependen de redes de contratistas especializados

Construir un centro de datos moderno exige coordinar miles de actividades en una compleja red de contratistas, proveedores y subcontratistas especializados. Desde el movimiento de tierras y la ingeniería estructural hasta los sistemas eléctricos de alta tensión, las instalaciones mecánicas, la infraestructura de refrigeración, la protección contra incendios, la seguridad, la instalación de fibra y la puesta en marcha, cada fase depende de que los conocimientos especializados se aporten de forma segura, conforme a la normativa y dentro de plazo.

A diferencia de muchos grandes proyectos de infraestructura, la construcción de centros de datos se desarrolla bajo una presión comercial excepcional. La capacidad no puede entrar en funcionamiento con la rapidez necesaria para satisfacer la demanda, lo que comprime los plazos de ejecución y deja poco margen para los retrasos. Al mismo tiempo, la escasez de mano de obra cualificada obliga a menudo a contratar simultáneamente a varios especialistas y subcontratistas, aumentando la complejidad de la supervisión de proveedores.

## Cada contratista incorpora un nuevo perfil de riesgo

Cada nuevo contratista incorpora su propio perfil de riesgo. Antes de que empiecen los trabajos, las organizaciones deben comprobar las cualificaciones, certificaciones, coberturas de seguro,

estabilidad financiera y cumplimiento normativo adecuados. También necesitan mantener la confianza en que esos requisitos siguen siendo válidos durante todo el proyecto. A medida que este evoluciona, los contratistas pueden recurrir a nuevos subcontratistas, las pólizas pueden caducar o cambiar, el personal clave puede ser sustituido y los proveedores pueden atravesar dificultades financieras. Cualquiera de estos cambios puede introducir riesgos operativos o comerciales si no se detecta a tiempo.

## La visibilidad se fragmenta a medida que crecen los proyectos

A medida que los ecosistemas de contratistas se amplían, la visibilidad suele fragmentarse. La información se reparte entre los equipos de Compras, los responsables de proyecto, las funciones de salud y seguridad, los equipos de instalaciones y los socios externos de ejecución, mientras que los registros se mantienen en hojas de cálculo, cadenas de correos electrónicos y sistemas locales. Cada equipo puede conocer una parte de la situación, pero pocas organizaciones disponen de una visión única y continuamente actualizada de la homologación, el cumplimiento y el riesgo de los contratistas en todo el programa.

## El riesgo de construcción se convierte rápidamente en riesgo para todo el programa

Las consecuencias van mucho más allá de la ineficiencia administrativa. Un contratista que no puede acceder al emplazamiento porque sus cualificaciones han caducado,

un proveedor que entra en dificultades financieras durante una fase crítica de la construcción o un subcontratista sin seguro implicado en un accidente laboral pueden alterar la ejecución del proyecto.

La limitación es especialmente grave en los oficios especializados. La Oficina de Estadísticas Laborales de Estados Unidos prevé unas 81.000 vacantes de electricistas al año durante el periodo 2024-2034, incluidas las que se generan por la salida de trabajadores y los cambios de ocupación. Los retrasos en los trabajos especializados suelen producir un efecto en cascada sobre las actividades posteriores, elevando los costes del programa, retrasando la puesta en marcha y prolongando el tiempo necesario para que una valiosa capacidad de computación pueda entrar en operación.

Estas presiones ya están afectando a la ejecución. JLL señala que más de la mitad de los proyectos de centros de datos sufrieron retrasos en 2025, lo que refuerza la necesidad de incorporar márgenes de entrega realistas y de mejorar la supervisión de las cadenas de suministro que sostienen cada construcción.

El análisis de McKinsey indica que las perturbaciones en la cadena de suministro pueden erosionar casi el 45 % del EBITDA de un año a lo largo de una década, mientras que una única interrupción prolongada de la producción puede costar entre el 30 % y el 50 % del EBITDA anual. En los grandes proyectos de centros de datos, donde los contratistas especializados pueden ser difíciles de sustituir y las actividades de puesta en marcha siguen programas estrictamente secuenciados, incluso las interrupciones relativamente pequeñas pueden tener consecuencias comerciales desproporcionadas.

Estos riesgos son cada vez más frecuentes a medida que se amplían las redes de contratistas. La Encuesta de Riesgo y

Sostenibilidad 2025 de Achilles reveló que el 31 % de las organizaciones había sufrido, durante los 12 meses anteriores, la quiebra o dificultades financieras de un proveedor con impacto en su cadena de suministro. El dato subraya la importancia creciente de supervisar continuamente la resiliencia de los proveedores, en lugar de depender únicamente de la diligencia debida realizada durante su incorporación.

Para los responsables de construcción, el reto ya no consiste únicamente en homologar a los contratistas antes de que empiecen los trabajos. Consiste en mantener la confianza en que todas las organizaciones que participan en el proyecto siguen cumpliendo los requisitos, conservan su resiliencia financiera y mantienen su capacidad de ejecución durante toda la obra. Alcanzar ese nivel de control exige una visibilidad continua, no periódica, que permita detectar los riesgos emergentes antes de que afecten a la entrega del programa.

## EN LA PRÁCTICA Apoyo a operaciones de centros de datos hiperescalables

Los principales operadores hiperescalables ya reconocen este reto. A medida que los ecosistemas de contratistas son más amplios y están más dispersos geográficamente, mantener una visibilidad continua sobre su homologación y cumplimiento se convierte en una capacidad estratégica, no en un ejercicio administrativo. Achilles ayuda a organizaciones como Google a gestionar ecosistemas complejos de contratistas en sus operaciones globales de centros de datos, contribuyendo a mantener la confianza en el cumplimiento de los proveedores y en su preparación operativa.

# Entorno de riesgo dos: resiliencia operativa

## La construcción termina. Comienza el riesgo operativo

Completar la construcción marca el comienzo de un nuevo reto para la cadena de suministro, no el final del anterior. Cuando un centro de datos entra en operación, el foco pasa de entregar la infraestructura a mantener una disponibilidad continua. Aunque los contratistas implicados pueden cambiar, la necesidad de supervisar eficazmente a los proveedores se vuelve todavía más crítica.

## Las instalaciones críticas dependen de proveedores de servicios especializados

Los centros de datos operativos dependen de un amplio ecosistema de proveedores especializados que trabajan en entornos de alta sensibilidad. La encuesta de personal 2025 de Uptime Institute, basada en 864 respuestas, reveló que el 42 % de los participantes consideraba la contratación de nuevo personal uno de los mayores retos de su organización. Este ecosistema incluye proveedores de gestión de instalaciones, contratistas de mantenimiento eléctrico y mecánico, especialistas en SAI/UPS y generadores, ingenieros de refrigeración, expertos en protección y extinción de incendios, proveedores de seguridad, socios de infraestructura de red, proveedores de combustible e ingenieros de servicio especializados de fabricantes de equipos originales (OEM). En conjunto, realizan el mantenimiento, las inspecciones y las reparaciones que protegen la resiliencia de una infraestructura crítica.

## El riesgo operativo cambia continuamente

A diferencia de los proyectos de construcción, donde las relaciones con contratistas suelen ser temporales, las relaciones con proveedores operativos pueden prolongarse durante décadas. Los contratistas acceden periódicamente al centro para realizar mantenimientos planificados, responder a incidencias o apoyar mejoras de la infraestructura. El personal cambia, se incorporan subcontratistas, las certificaciones caducan, las pólizas de seguro se renuevan y las circunstancias financieras evolucionan. Cada cambio puede afectar a la resiliencia operativa si no se identifica y gestiona.

Las consecuencias de una visibilidad deficiente también son fundamentalmente distintas. Durante la construcción, los fallos de los proveedores pueden retrasar la finalización del proyecto o elevar sus costes. Cuando la instalación ya está activa, los mismos fallos pueden afectar directamente a la continuidad del negocio. Un contratista sin la cualificación adecuada que trabaje en una infraestructura eléctrica crítica, un proveedor de mantenimiento sin seguro implicado en un accidente laboral o un proveedor con dificultades financieras que no pueda cumplir sus obligaciones contractuales pueden provocar interrupciones operativas, aumentar los riesgos de seguridad y comprometer la disponibilidad del servicio.

Estos riesgos adquieren mayor importancia a medida que los operadores se expanden geográficamente y estandarizan sus operaciones en múltiples centros. La

**El error humano** interviene de algún modo en aproximadamente dos tercios de las interrupciones de centros de datos, según 25 años de datos de Uptime Institute.

Aproximadamente **uno de cada diez** señaló que la interrupción había tenido un impacto grave o muy grave.

En el análisis de 2026 de Uptime Institute, el 57 % de los participantes afirmó que su interrupción grave más reciente había costado más de **100.000 dólares**, mientras que uno de cada cinco indicó un coste superior al **millón de dólares**.

Uptime Institute también informa de que **los fallos de infraestructuras externas** ganan peso en las interrupciones comunicadas públicamente, mientras aumentan las relacionadas con fibra y conectividad, que tienen más probabilidades de provocar una **afectación prolongada**.

población de contratistas aumenta con el tiempo y muchos proveedores trabajan en varios emplazamientos, unidades de negocio y regiones. Mantener la confianza en que cada contratista sigue estando debidamente cualificado, asegurado, financieramente resiliente y conforme a la normativa resulta cada vez más difícil cuando la información está fragmentada entre diferentes sistemas, departamentos y equipos locales.

Los procesos tradicionales de homologación y control no se diseñaron para este nivel de complejidad. Las revisiones anuales solo ofrecen una fotografía del cumplimiento de los proveedores en un momento concreto, aunque el riesgo operativo evoluciona cada día. La cobertura de un seguro puede vencer, el rendimiento financiero puede deteriorarse, la situación regulatoria puede cambiar y pueden incorporarse nuevos subcontratistas mucho antes de la siguiente revisión programada. Por tanto, las organizaciones que dependen de evaluaciones periódicas pueden desconocer los riesgos emergentes hasta que ya han afectado a las operaciones.

Para las organizaciones responsables de infraestructuras críticas, la resiliencia

operativa no depende únicamente de la fiabilidad de los activos físicos, sino también de la resiliencia de las organizaciones encargadas de mantenerlos. La visibilidad continua sobre las cualificaciones de los contratistas, su salud financiera, sus seguros, su cumplimiento y sus relaciones en la cadena de suministro permite detectar los cambios cuando se producen y adoptar medidas correctivas antes de que el rendimiento operativo se vea afectado.

## La continuidad del negocio depende de la resiliencia de los proveedores

A medida que los centros de datos sostienen servicios digitales cada vez más críticos, desde cargas de trabajo de IA y plataformas en la nube hasta sistemas financieros, sanidad y telecomunicaciones, la resiliencia de la cadena de suministro operativa se convierte en una capacidad estratégica. Las organizaciones capaces de supervisar y comprender continuamente su ecosistema de contratistas están mejor posicionadas para reducir las interrupciones, proteger la disponibilidad y mantener la confianza en el rendimiento a largo plazo de sus instalaciones.



# Gestión dinámica del riesgo de la cadena de suministro

## El riesgo de los proveedores no permanece inmóvil

Los modelos tradicionales de homologación y control de contratistas se diseñaron para un entorno operativo muy distinto. Cuando los proyectos eran más pequeños, las redes de contratistas relativamente estables y las cadenas de suministro cambiaban de forma gradual, las revisiones anuales de cualificación y los controles periódicos de cumplimiento ofrecían un nivel razonable de garantía.

El entorno actual de los centros de datos es fundamentalmente diferente. Las organizaciones gestionan poblaciones de contratistas más amplias en múltiples emplazamientos, recurren a proveedores especializados para trabajos cada vez más complejos y operan instalaciones donde una disponibilidad ininterrumpida es crítica para el negocio. En este contexto, el riesgo de los proveedores evoluciona de manera continua, no anual.

A lo largo de las fases de construcción y operación, los perfiles de los contratistas

cambian constantemente. Se incorporan nuevos proveedores y subcontratistas; las pólizas de seguro se renuevan o vencen; la salud financiera fluctúa; los requisitos normativos evolucionan; y el personal clave cambia de organización. Cada variación puede modificar el perfil de riesgo de un proveedor mucho antes de la siguiente revisión programada.

## Los controles estáticos crean puntos ciegos operativos

Las revisiones periódicas solo ofrecen una fotografía del nivel de control de un contratista en un momento concreto. Confirman que el proveedor cumplía los estándares exigidos el día de la evaluación, pero aportan poca información sobre lo que puede haber cambiado después. La continuidad de la plantilla forma parte de este riesgo cambiante. La investigación de Uptime Institute sobre personal en 2025 reveló que los puestos operativos junior y de nivel intermedio presentaban las tasas de rotación más elevadas, especialmente entre los proveedores de colocación.

A medida que los ecosistemas de contratistas crecen, estas brechas son más difíciles de gestionar. La información suele repartirse entre Compras, Ejecución de Proyectos, Gestión de Instalaciones, Salud y Seguridad, Cumplimiento y Finanzas, y cada función mantiene sus propios registros y procesos. Sin una visión continuamente actualizada, las organizaciones pueden no saber que el seguro de un contratista ha caducado, que una certificación crítica ha vencido o que un proveedor clave muestra señales de dificultades financieras hasta que esos cambios empiezan a afectar a la ejecución del proyecto o al rendimiento operativo.

El ritmo de cambio del sector de los centros de datos agrava el reto. Las instalaciones se amplían, las infraestructuras se actualizan con mayor frecuencia y los contratistas suelen trabajar simultáneamente en varios proyectos y emplazamientos operativos. Cuanto más dinámica es la cadena de suministro, menos eficaces resultan los procesos estáticos de homologación y control.

## De las revisiones periódicas a la inteligencia continua sobre proveedores

Las organizaciones líderes reconocen que la homologación y el control de contratistas ya no deben entenderse como un ejercicio

puntual de cumplimiento, sino como una capacidad continua de gestión del riesgo.

En lugar de preguntar “¿cumplía este contratista los requisitos cuando se incorporó al proyecto?”, las organizaciones necesitan plantearse cada vez más “¿qué ha cambiado desde entonces?”.

La visibilidad continua permite identificar los riesgos emergentes mientras se desarrollan, y no después de que hayan interrumpido un proyecto o afectado a las operaciones. Permite supervisar los cambios en las cualificaciones de los contratistas, los seguros, la resiliencia financiera, el estado de cumplimiento y las relaciones con subcontratistas durante todo el ciclo de vida del proveedor. De este modo, quienes toman las decisiones disponen de una visión actualizada de dónde está aumentando el riesgo y dónde puede ser necesario intervenir.

Para las organizaciones que construyen y operan infraestructuras críticas, esto representa un cambio de enfoque fundamental. La supervisión de contratistas ya no consiste solo en verificar documentación, sino en mantener una confianza continua en que las organizaciones responsables de entregar y sostener instalaciones críticas siguen siendo capaces, cumplen los requisitos y conservan su resiliencia.



# De la homologación de proveedores a la inteligencia continua de la cadena de suministro

La rápida expansión de las infraestructuras de centros de datos está transformando la forma en que las organizaciones entienden el riesgo de los proveedores. A medida que las instalaciones aumentan de tamaño y complejidad, y adquieren un papel más crítico en la economía digital mundial, gestionar contratistas y proveedores deja de ser una simple actividad operativa o de cumplimiento. Se convierte en un componente fundamental de la resiliencia de la organización.

Históricamente, la homologación de contratistas se ha centrado en recopilar documentación, verificar a los proveedores durante su incorporación y realizar revisiones periódicas para demostrar el cumplimiento. Aunque estas actividades siguen siendo esenciales, se diseñaron para cadenas de suministro relativamente estables y que cambiaban lentamente. Los entornos actuales de los centros de datos son fundamentalmente distintos.

Durante todo el ciclo de vida de un centro de datos, el ecosistema de proveedores evoluciona continuamente. En la construcción se incorporan nuevos contratistas, subcontratistas y proveedores

especializados conforme avanza el proyecto. Una vez en operación, los proveedores de mantenimiento, los socios de ingeniería y los contratistas de servicios críticos siguen cambiando por movimientos de personal, renovaciones contractuales, reestructuraciones organizativas y variaciones en su situación financiera.

Al mismo tiempo, el propio riesgo de los proveedores cambia constantemente. El rendimiento financiero fluctúa, las pólizas de seguro caducan, surgen ciberamenazas, evolucionan los requisitos normativos, los acontecimientos geopolíticos alteran las redes de suministro y nuevos subcontratistas entran en la cadena. Considerados por separado, estos cambios pueden parecer manejables. En conjunto, crean una imagen dinámica de la resiliencia de los proveedores que puede influir de forma significativa en el rendimiento operativo.

Esto exige que las organizaciones vayan más allá de mantener listas de proveedores aprobados o revisar periódicamente la documentación de los contratistas. Necesitan confiar en que los proveedores conservan su cualificación, resiliencia

financiera, cobertura de seguro y capacidad operativa durante toda la relación. Alcanzar esa confianza depende de mantener una visibilidad continua sobre el ecosistema de proveedores, para identificar los riesgos emergentes antes de que afecten a la ejecución del proyecto, al rendimiento operativo o a la continuidad del negocio.

Por este motivo, las organizaciones líderes están evolucionando desde la homologación tradicional de proveedores hacia una inteligencia continua de la cadena de suministro. En lugar de tratar la salud financiera, los seguros, la competencia de los contratistas, el riesgo cibernético, el desempeño ESG, las auditorías, las noticias adversas y la exposición geopolítica como actividades de cumplimiento independientes, reúnen estas señales para desarrollar una visión continuamente actualizada de la resiliencia de los proveedores.

Este enfoque permite que los equipos de Compras, Operaciones, Gestión de Instalaciones, Salud y Seguridad y Cumplimiento trabajen a partir de una visión compartida del riesgo de los proveedores, prioricen las intervenciones con mayor eficacia y adopten decisiones operativas mejor informadas.

A medida que la inversión en centros de datos siga acelerándose, esta capacidad será una fuente de ventaja competitiva cada vez más importante. Las organizaciones mejor posicionadas para el éxito a largo plazo no se limitarán a construir instalaciones más rápido u operarlas con mayor eficiencia. Desarrollarán cadenas de suministro transparentes, resilientes y comprendidas de forma continua, reconociendo que unos centros de datos resilientes dependen, en última instancia, de ecosistemas de proveedores resilientes.





# Cinco preguntas que todo operador de centros de datos debería poder responder

Construir centros de datos resilientes exige algo más que una infraestructura resistente. Requiere confianza continua en las organizaciones que la construyen, mantienen y sostienen. Estas cinco preguntas ofrecen una prueba sencilla de la resiliencia de la cadena de suministro.

1

## ¿Conocemos a todas las organizaciones que trabajan en nuestra infraestructura crítica?

La visibilidad debe ir más allá de los contratistas principales e incluir a los subcontratistas, proveedores especializados y prestadores de servicios que participan tanto en la construcción como en las operaciones.

2

## ¿Podemos confiar en que hoy siguen cualificados, asegurados y cumplen los requisitos?

La homologación y el control de proveedores no son actividades puntuales. Las certificaciones, los seguros, la salud financiera y el cumplimiento normativo cambian con el tiempo.

3

## ¿Entendemos qué proveedores representan nuestro mayor riesgo operativo?

No todos los proveedores tienen la misma criticidad. Las organizaciones deben saber dónde existen dependencias y en qué casos el fallo de un proveedor tendría un mayor impacto operativo.

4

## ¿Con qué rapidez podemos responder cuando cambia nuestro panorama de proveedores?

Los nuevos contratistas, los cambios regulatorios, las dificultades financieras y la escasez de personal exigen que las organizaciones se adapten sin comprometer la gobernanza ni la ejecución.

5

## ¿Podemos detectar los riesgos emergentes de los proveedores antes de que provoquen interrupciones operativas?

Las organizaciones más resilientes no se limitan a responder a las interrupciones. Reconocen con suficiente antelación los cambios en los perfiles de riesgo para actuar antes de que los proyectos o las operaciones se vean afectados.

Si alguna de estas preguntas no puede responderse con confianza, es posible que existan riesgos ocultos en la cadena de suministro que resulten difíciles de identificar mediante revisiones periódicas.



# El futuro de la resiliencia de la cadena de suministro

La infraestructura que sostiene este crecimiento, desde la generación y transmisión eléctrica hasta los sistemas de refrigeración, la construcción y los proveedores especializados, es cada vez más crítica e interconectada. La Agencia Internacional de la Energía prevé que la demanda mundial de electricidad de los centros de datos supere los 945 TWh en 2030. En Estados Unidos, se espera que los centros de datos representen casi la mitad del crecimiento de la demanda eléctrica durante el mismo periodo.

Para desplegar con éxito la próxima generación de centros de datos hará falta algo más que capacidad técnica e inversión. A medida que los proyectos aumenten de tamaño, los plazos se compriman y los ecosistemas de proveedores se vuelvan más complejos, la gestión eficaz de contratistas y proveedores será un factor cada vez más importante para el éxito de la ejecución y de las operaciones posteriores.

A medida que la IA impulse la demanda de campus más grandes, la expansión geográfica y una mayor complejidad operativa, la resiliencia de la cadena de suministro adquirirá importancia junto con la disponibilidad de energía, la seguridad física y la conectividad de red. Las organizaciones con mayor visibilidad sobre la capacidad, el riesgo y el rendimiento de sus proveedores estarán mejor preparadas

para gestionar las interrupciones, mantener la disponibilidad y apoyar un crecimiento sostenible.

La resiliencia de los centros de datos del futuro no dependerá únicamente de la fiabilidad de su infraestructura física, sino también de la solidez y la resiliencia de las cadenas de suministro que los sostienen.

## Cómo ayuda Achilles a los operadores de centros de datos a reforzar la resiliencia de su cadena de suministro

Achilles hace posible este enfoque al reunir múltiples fuentes de inteligencia sobre proveedores, entre ellas la salud financiera, los seguros, el cumplimiento, la competencia de los contratistas, el desempeño ESG, el riesgo cibernético, las auditorías, las noticias adversas y la exposición geopolítica. Así, ofrece a las organizaciones una visión continuamente actualizada del riesgo de los proveedores durante todo el ciclo de vida del centro de datos.



## Fuentes

1. McKinsey & Company, *The Data Center Balance: How US States Can Navigate the Opportunities and Challenges*, 8 de agosto de 2025. [Ver fuente \[mckinsey.com\]](#)
2. McKinsey & Company, *Scaling Bigger, Faster, Cheaper Data Centers with Smarter Designs*, 1 de agosto de 2025. [Ver fuente \[mckinsey.com\]](#)
3. JLL, *North America Data Center Report: Year-end 2025*, 17 de febrero de 2026. [Ver fuente \[jll.com\]](#)
4. JLL, *2026 Global Data Center Market Outlook*, 5 de enero de 2026. [Ver fuente \[jll.com\]](#)
5. Uptime Institute, *Annual Outage Analysis 2026: The Causes and Impacts of IT and Data Center Outages*, mayo de 2026. [Ver fuente \[datacenter.uptimeinstitute.com\]](#)
6. Uptime Institute, *Outages: Understanding the Human Factor*, 8 de junio de 2022. [Ver fuente \[journal.uptimeinstitute.com\]](#)
7. Uptime Institute, *Data Center Staffing and Recruitment Survey 2025: Staffing Crisis Persists as Colos Struggle to Retain Junior Operators*, octubre de 2025. [Ver fuente \[intelligence.uptimeinstitute.com\]](#)
8. Agencia Internacional de la Energía, *Energy and AI: AI Is Set to Drive Surging Electricity Demand from Data Centers*, 10 de abril de 2025. [Ver fuente \[iea.org\]](#)
9. Electrical Safety Foundation International, *Workplace Injury and Fatality Statistics: 2011–2024*, publicado el 5 de marzo de 2026 a partir de datos de la Oficina de Estadísticas Laborales y de la Administración de Seguridad y Salud Ocupacional de Estados Unidos. [Ver fuente \[esfi.org\]](#)
10. Achilles, *Encuesta de Riesgo y Sostenibilidad 2025*.





**Dirección**

Achilles Information, LLC.,  
5271 California Ave, Suite 290  
Irvine, CA 92617



**California**

+1 949 899 6850



**Texas**

+1 281 809 4400



**Correo Electrónico**

[enquiries@achilles.com](mailto:enquiries@achilles.com)



**Web**

[www.achilles.com](http://www.achilles.com)