

DOCUMENTO TÉCNICO

Administración distribuida frente a administración centralizada de la ciberprotección para empresas con varias ubicaciones

Cómo la administración distribuida de la ciberseguridad y la protección de datos puede hacer que su empresa sea más ciberresiliente



Las empresas, sea cual sea su magnitud, luchan por proteger el tiempo de actividad de sus sistemas y la integridad de los datos contra una gran cantidad de amenazas, desde ciberataques basados en IA hasta fallos de hardware, problemas de software y errores humanos. Si bien muchas empresas optan por centralizar la administración de sus operaciones de TI y de ciberseguridad, existen otros casos de uso en los que ceder parte de ese control al personal de TI y ciberseguridad ubicado en sitios remotos puede generar una mejor ciberresiliencia.

En este documento técnico se examinan los escenarios en los que una empresa puede lograr un mayor tiempo de actividad, prevenir de forma más eficaz la pérdida de datos y reducir los costes de administración y protección de la infraestructura de TI y de los datos al delegar parte del control a sus ubicaciones regionales y remotas. Además, se sopesan los puntos a favor y en contra de este enfoque y se consideran las formas en que las empresas pueden lograr sus objetivos de cumplimiento y gobernanza sin una administración totalmente centralizada de las operaciones de TI y de la ciberseguridad.

Muchas empresas están distribuidas

En torno a una cuarta parte de las empresas estadounidenses operan desde más de una ubicación. Y aunque la Unión Europea (UE) no facilita información específica sobre las empresas en función del número de ubicaciones, la prevalencia del comercio minorista, la hostelería, los servicios médicos y financieros y otros segmentos empresariales —que suelen tener múltiples ubicaciones— sugiere que las empresas con múltiples ubicaciones también conforman una parte importante de la economía de la UE. Es aún más probable que las empresas de mayor tamaño tengan múltiples ubicaciones, entre las que se incluirían oficinas regionales, plantas de producción, almacenes y centros de distribución.

Las empresas que llevan a cabo fusiones y adquisiciones para expandirse dentro de su sector, hacia otras líneas de negocio y otras regiones geográficas, probablemente también cuenten con una gran cantidad de ubicaciones que estén físicamente alejadas del personal centralizado de TI y ciberseguridad.

Ejemplos de empresas distribuidas

El sector minorista constituye un ejemplo claro de empresas altamente distribuidas. El comercio minorista típico incluye sedes globales y regionales, almacenes de distribución y tiendas físicas orientadas al consumidor. No obstante, muchas empresas de otros sectores también están organizadas como empresas minoristas, ya que tienen muchas tiendas u oficinas distribuidas geográficamente, como sucede en los siguientes ejemplos:

- Prestación de servicios de atención sanitaria, como servicios de óptica, centros médicos de atención primaria, clínicas dentales, centros de atención de urgencia sin cita previa, farmacias y clínicas veterinarias.
- Empresas de banca minorista, de seguros y de servicios financieros orientadas al consumidor con numerosas sucursales.

- Empresas de envío/recepción, transporte y logística con numerosos centros de distribución y un gran número de tiendas minoristas de envío y servicios empresariales.
- Empresas de juegos y apuestas con múltiples ubicaciones para casinos, salas de bingo, salas de apuestas fuera del hipódromo, salones de pachinko e instalaciones similares.
- Servicios en carretera, que a menudo combinan el suministro de combustible para automóviles y la carga de vehículos eléctricos con tiendas de conveniencia y restaurantes de servicio rápido.
- Empresas organizadas en virtud de una arquitectura federada, en la que un equipo centralizado puede supervisar las operaciones de TI, la ciberseguridad y el cumplimiento normativo de toda la empresa. Sin embargo, las instalaciones individuales tienen sus propios presupuestos, responsabilidad de contratación de personal y autonomía local para administrar la infraestructura de TI de la unidad empresarial.

La administración centralizada de TI y de la ciberseguridad puede ser un desafío

Las empresas con un alto grado de distribución suelen tener una mezcla heterogénea de hardware, virtualización y sistemas operativos, además de aplicaciones como sistemas de inventario o de puntos de venta de diferentes proveedores

de tecnología. La combinación de infraestructura tecnológica y niveles de revisión de software puede variar significativamente de una ubicación a otra. La necesidad de mantener aplicaciones heredadas, software de diseño personalizado y ordenadores utilizados para controlar entornos tecnológicos operativos estables puede dificultar la estandarización de TI en toda la empresa, lo que lleva a una proliferación de herramientas de TI y ciberseguridad.

Al personal centralizado le puede resultar difícil dominar a la perfección todas las herramientas necesarias para proteger, administrar y asegurar aplicaciones y datos en toda la organización. Por su parte, la complejidad y diversidad de las aplicaciones, así como las herramientas necesarias para gestionarla y protegerla, no deja de crecer.

Es posible que sea necesario aislar físicamente las ubicaciones remotas con altos requisitos de seguridad, como p. ej., los entornos de fábricas, de la red corporativa y de internet pública para minimizar la exposición a ciberamenazas. Esto limitaría la capacidad del personal centralizado para diagnosticar y resolver problemas mediante la administración de escritorio remoto y otras herramientas basadas en red, ya que requeriría viajar a las ubicaciones remotas para resolver los problemas en cuestión.

Además, podría suponer costes extra inasumibles y requerir demasiado tiempo en el caso de lugares de difícil acceso, como refinerías en el desierto, plataformas petrolíferas en alta mar, instalaciones mineras y otros sitios alejados de centros de transporte comercial aéreo y terrestre.



Gestionar la protección y seguridad de los datos en una empresa grande con una sola ubicación es menos complejo y requiere menos tiempo que proteger la misma cantidad de aplicaciones y endpoints dispersos en múltiples ubicaciones separadas geográficamente. Si los datos de las copias de seguridad no están separados por ubicación, la restauración a partir de la copia de seguridad en una ubicación puede afectar negativamente al rendimiento en todas las demás ubicaciones.

La conectividad de red WAN (red de área amplia) y las velocidades de red en ubicaciones remotas pueden variar de forma considerable según la geografía, lo que hace que los tiempos de restauración sean impredecibles e incluso demasiado lentos para cumplir con los estándares de tiempo de recuperación.

A la hora de administrar sitios remotos, es posible que el personal de TI deba iniciar sesión en repositorios de datos locales y consolas de administración de seguridad por separado y de forma repetida, lo que no solo puede resultar ineficaz, sino también provocar errores y lentitud. Muchas herramientas tradicionales de copia de seguridad, recuperación ante desastres y seguridad están especializadas en entornos de determinadas aplicaciones particulares, lo que dificulta la estandarización en herramientas comunes en toda la organización.

La proliferación resultante de operaciones de TI y herramientas de seguridad es costosa y dispara los costes de incorporación y formación del personal de soporte técnico, un problema creciente en un mundo donde los costes de personal de TI y ciberseguridad siguen siendo elevadísimos.

El cumplimiento normativo puede ser difícil de gestionar de forma centralizada

Los requisitos de cumplimiento normativo también varían significativamente de un país a otro y, en algunos casos, incluso según el estado, la provincia y el municipio. Por ejemplo, es posible que las empresas que desempeñen su actividad económica en Estados Unidos tengan que cumplir con normativas en materia de privacidad impuestas por el gobierno federal, por varios estados del país e incluso por algunas ciudades específicas.

El cumplimiento de normativas sobre soberanía de datos también es un desafío creciente. Estas normativas limitan las ubicaciones físicas, los centros de datos y las redes en las que se pueden almacenar datos confidenciales o permitir su tránsito a través de una red, bajo la premisa de que algunos gobiernos nacionales podrían infringir la privacidad de los datos con vigilancia encubierta. Respetar estos requisitos en una empresa ampliamente distribuida es una tarea compleja de gestionar y puede influir de forma negativa en el rendimiento de las aplicaciones.

Estar al tanto de qué datos deben protegerse y en qué dispositivos, qué elementos de la infraestructura de TI están certificados por cumplir con diversos estándares normativos y de seguridad, y qué empleados tienen acceso autorizado a esos datos, puede generar confusión y costosas infracciones en toda la organización por incumplir normativas. Esta complejidad surge en un momento en el que la mayoría de las empresas tienen presupuestos congelados o incluso decrecientes para el personal de TI y ciberseguridad, mientras que el número de aplicaciones y el volumen de datos que deben administrar y proteger están creciendo.

Las autoridades reguladoras ahora imponen sanciones cuantiosas para fomentar el cumplimiento de las normativas. Por ejemplo, la UE suele imponer multas de entre el dos y el cuatro por ciento de los ingresos anuales de una empresa por no proteger los datos de los consumidores como es debido de forma reiterada.

Esto puede presentar problemas importantes para algunas empresas distribuidas geográficamente y con múltiples ubicaciones, incluidos posibles desafíos de conexión a redes y dificultades para encontrar alojamiento de aplicaciones y almacenamiento de terceros que cumpla con las normativas y sea seguro, con funciones como control de acceso seguro y almacenamiento inmutable.

Acronis aborda los desafíos de administrar y proteger empresas distribuidas

Acronis Cyber Protect aborda el desafío de brindar soluciones de seguridad y protección de datos en entornos distribuidos al integrar la administración remota, la copia de seguridad, la recuperación ante desastres y la seguridad en una sola plataforma. El personal local puede configurar y administrar ubicaciones remotas individuales por separado desde una única consola exclusiva para su ubicación, ya sea instalada in situ o alojada en la nube.

Por otro lado, se pueden personalizar los planes de protección de datos y las opciones de planificación de copias de seguridad para cada ubicación, o bien se pueden implementar planes y opciones de planificación estandarizados en más de una ubicación. Además, la protección de datos y la seguridad de todos los recursos locales se pueden administrar desde una única consola sin tener que cambiar entre pantallas o aplicaciones.

Todas las funciones de seguridad y protección de datos se administran a través de un único agente instalado en cada endpoint. El cifrado completo de datos y la transferencia segura a través del protocolo de seguridad de la capa de transporte (TLS) garantizan que los datos estén seguros en tránsito. Además, la compresión de datos, la deduplicación y la limitación del ancho de banda se gestionan automáticamente para optimizar el tráfico a cualquier velocidad de conexión razonable y garantizar un impacto mínimo en las operaciones activas.

Mientras tanto, el personal de TI y ciberseguridad de las sedes centrales puede supervisar ubicaciones remotas desde un panel de control centralizado para evaluar el riesgo general de sufrir ciberataques, el estado de la protección de datos y el cumplimiento normativo en toda la organización, tal y como se muestra en la Figura 1.

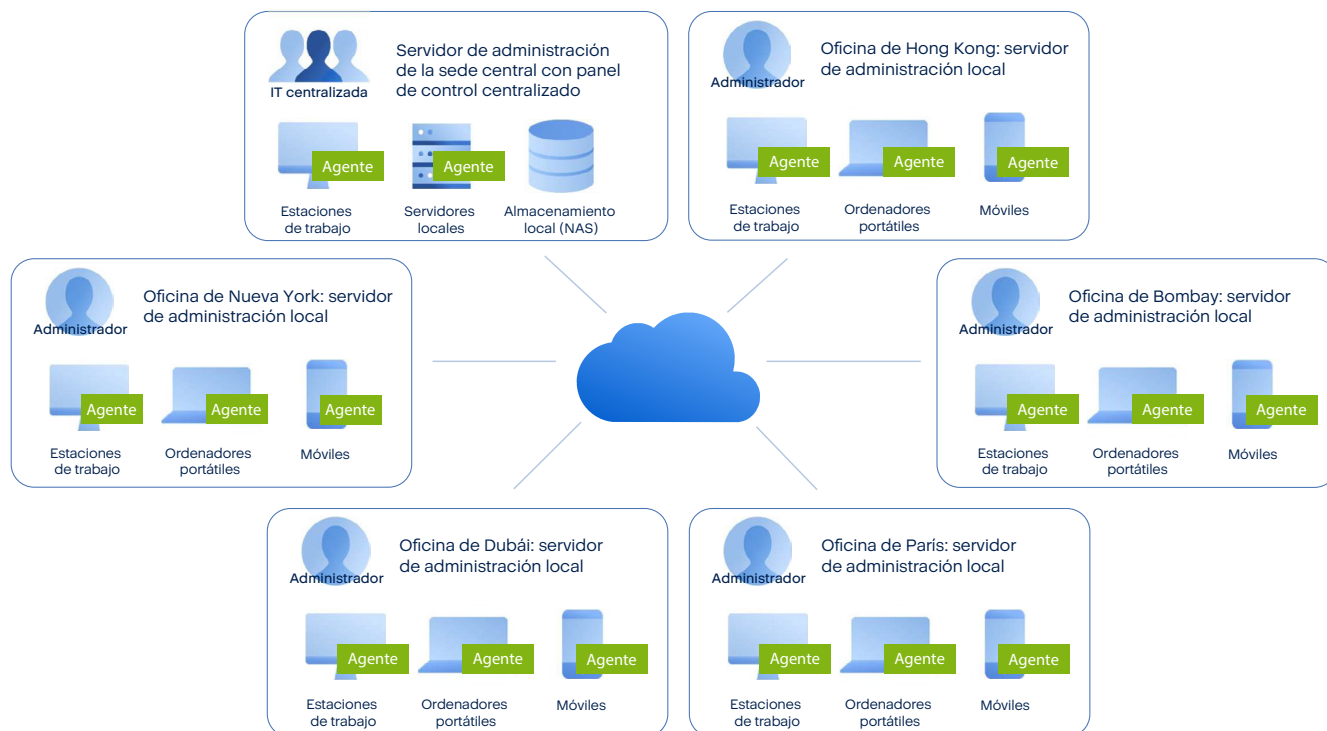


Figura 1. Administración multisitio de operaciones de ciberseguridad y TI con control local y supervisión centralizada

Principales ventajas de Acronis Cyber Protect

- Aísla el almacenamiento y la seguridad de los datos por ubicación.
- Reduce o elimina posibles problemas de compatibilidad en ciberseguridad relacionados con hardware, software y virtualización.
- Resuelve problemas de soberanía de datos y facilita el cumplimiento normativo.
- Elimina problemas relacionados con diferentes configuraciones y conexiones de red.
- Reduce o elimina la necesidad de múltiples entornos de alojamiento para la protección de datos.
- Crea costes coherentes y predecibles en todas las ubicaciones físicas.
- Optimiza la implementación de almacenamiento georredundante.
- Permite supervisar de forma centralizada la evaluación del riesgo de sufrir ciberataques, el estado de la protección de datos y el estado de cumplimiento normativo de toda la empresa.



Las soluciones de Acronis se basan en imágenes y archivos, y utilizan un agente multiplataforma compatible con la mayoría de los entornos informáticos que se utilizan en empresas y fábricas. Acronis también protege plataformas de colaboración y correo electrónico basadas en la nube, como por ejemplo, Microsoft 365 y Google Workspace, además de plataformas basadas en entornos in situ, como p. ej., Microsoft Exchange.

Entornos compatibles con Acronis

VMware vSphere 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0

Microsoft Hyper-V Server 2022, 2019, 2016, 2012/2012 R2, 2008/2008 R2

Citrix XenServer / Citrix Hypervisor 8.2 – 4.1.5

Linux KVM 8 – 7.6

Scale Computing HyperCore 8.8, 8.9, 9.0

Red Hat Enterprise Virtualization (RHEV) 3.6 – 2.2

Red Hat Virtualization (RHV) 4.0, 4.1

Red Hat Virtualization (oVirt) 4.2, 4.3, 4.4

Virtuozzo 7.0.14 – 6.0.1.0

Virtuozzo Infrastructure Platform 3.5

Oracle Linux Virtualization Manager (Oracle LVM) 4.3

Nutanix Acropolis Hypervisor (AHV) 20160925x – 20180425x

Virtuozzo Hyper Server 7.5

Virtuozzo Hybrid Infrastructure 4.3 – 3.5

Soberanía de datos y cumplimiento normativo para entornos distribuidos

Acronis opera una red global e independiente de centros de datos con presencia en todo el mundo industrializado, lo que proporciona a las empresas distribuidas una gran flexibilidad para almacenar datos de forma segura, con el fin de optimizar el rendimiento de la protección de datos y ayudar a cumplir las normativas sobre soberanía de datos. En las ubicaciones remotas individuales se puede administrar la protección y seguridad de sus datos por ubicación, además de mantener los datos de sus servidores, endpoints, correos electrónicos y apps de colaboración en determinados países cuando y donde sea necesario con el fin de cumplir con las normativas.

Al integrar la administración de endpoints, la protección de datos y la ciberseguridad en una única plataforma con consolas locales se pueden reducir los costes operativos de TI hasta en un 60 %. Las empresas conseguirán ahorrar aún más gracias a la reducción de los gastos generales asociados con la formación del personal y con el mantenimiento de múltiples herramientas de TI y de ciberseguridad, así como gracias a los menores costes de almacenamiento y tránsito de datos de terceros que cumplen con las normativas geográficas.

Por su parte, las empresas distribuidas y con múltiples ubicaciones han de enfrentarse a desafíos peculiares a la hora de implementar y mantener soluciones de seguridad, copia de seguridad y recuperación ante desastres. Entre dichos desafíos se incluyen la administración de soluciones en múltiples ubicaciones, la navegación por los servicios y el mantenimiento de los mismos en innumerables combinaciones de tecnologías de hardware y software, garantizar el cumplimiento de las normativas en materia de privacidad y soberanía de datos, y prestar tales servicios en un entorno con recursos y presupuestos limitados. Asimismo, estos desafíos se amplifican cuando las empresas ejercen su actividad económica a nivel internacional.

Ventajas de la administración multisitio

Consolas locales para ubicaciones remotas con agentes independientes

- Consola única alojada en la nube o in situ para cada ubicación, departamento, unidad de negocio o marca.
- Limitación del ancho de banda, compresión de datos y deduplicación, siempre incremental, con transporte de disco físico opcional.
- Agente en origen con cifrado de datos y transferencia segura a través del protocolo TLS; sin necesidad de utilizar red corporativa.

Panel de control centralizado en la sede corporativa para supervisar todas las consolas de Acronis del sitio remoto

- Supervise todas las consolas de Acronis del sitio remoto de forma colectiva o individual.
- Obtenga una vista consolidada de todos los dispositivos remotos, alertas y actividades.
- Descargue datos de los widgets de las consolas de Acronis del sitio remoto.
- Acceda a dispositivos específicos en cualquier consola remota de Acronis.

Consolidación de múltiples herramientas

Un solo agente y una única consola para administrar:

- Funciones de copia de seguridad y recuperación ante desastres.
- Seguridad del correo electrónico y de endpoints con Detección y respuesta para endpoints (EDR).
- Aplicación de parches, inventario, asistencia remota, scripting y supervisión.

Recursos informáticos protegidos

- Servidor, máquina virtual, máquina virtual en la nube y estaciones de trabajo.
- Ordenadores de escritorio, portátiles y dispositivos móviles.
- Windows (hasta 2003/XP), Mac, Linux.
- Microsoft 365 y Google Workspace.

Cumplimiento local mejorado

Más de 50 centros de datos globales.

- 11 centros de datos en Europa.
- 2 centros de datos en Alemania.

Datos cifrados en origen mediante AES-256 con contraseñas gestionadas por la empresa.

Datos cifrados en tránsito a través de SSL/TLS.

Almacenamiento inmutable.

Autenticación multifactor.

Acceso basado en roles.

Certificaciones de cumplimiento de normativas globales.

Reducción de costes y complejidad para los proveedores

La consolidación en Acronis puede ahorrar hasta un 60 % en comparación con una variedad de herramientas de múltiples proveedores.

Mitigación de las limitaciones de recursos

Una única consola, una única administración.

Inteligencia artificial y aprendizaje automático (ML) para brindar ayuda en las tareas cotidianas.

- Supervisión de dispositivos y soluciones automatizadas.
- Investigación y corrección de incidentes de seguridad con IA.
- Copia de seguridad automatizada y pruebas de recuperación ante desastres.
- Biblioteca de scripts automatizada para tareas de mantenimiento.



Reflexiones finales

Si bien la mayoría de las empresas administran las operaciones de TI y la ciberseguridad con personal centralizado, algunas empresas llegarán a la conclusión de que delegar algunas funciones de administración de TI y seguridad a equipos presentes en ubicaciones regionales o remotas puede generar una mayor ciberresiliencia.

Distribuir la administración de las defensas de una empresa contra posibles ciberamenazas y contra otros problemas que causen tiempos de inactividad y pérdida de datos, así como su capacidad para restaurar rápidamente los datos y el tiempo de actividad cuando ocurran incidentes, puede reducir el riesgo empresarial de forma más eficaz que un control centralizado.

En estos escenarios multisitio y administrados localmente, las empresas deben facilitar a sus equipos regionales y de sitios remotos herramientas que integren de forma nativa la ciberseguridad, la protección de datos y la administración de endpoints. Añadir una supervisión centralizada de las consolas que se utilizan a nivel regional

y en los sitios remotos puede ayudar a los equipos de TI y de ciberseguridad de la sede central a auditar y aplicar los estándares de la empresa para la gobernanza y el cumplimiento normativo de TI.

Esta combinación de supervisión centralizada y administración distribuida de las operaciones de TI y de ciberseguridad puede optimizar la capacidad de respuesta del soporte técnico (en particular para instalaciones aisladas y muy remotas) y mejorar el cumplimiento de las normativas regionales en materia de seguridad y de TI, así como reducir el riesgo empresarial general.

Más información

Para obtener una consulta gratuita con un ingeniero de soluciones de Acronis y comprobar si una topología de control distribuida y con supervisión centralizada tiene sentido para su negocio a la hora de administrar operaciones de TI y ciberseguridad, póngase en contacto con Acronis [aquí](#).

Consiga una prueba gratuita de 30 días de Acronis Cyber Protect [aquí](#).

Acerca de Acronis

Acronis es una empresa global de ciberprotección que ofrece ciberseguridad, protección de datos y administración de endpoints integradas de forma nativa para proveedores de servicios gestionados (MSP), pequeñas y medianas empresas (pymes) y departamentos de TI de empresas. Las soluciones de Acronis son muy eficaces y están diseñadas para identificar, prevenir y detectar ciberamenazas modernas, así como responder ante ellas, corregir los sistemas afectados y recuperarse de los ciberataques, todo ello con un tiempo de inactividad mínimo, lo que garantiza la integridad de los datos y la continuidad de la actividad empresarial. Además, Acronis ofrece la solución de seguridad más completa del mercado para MSP, con su capacidad exclusiva para satisfacer las necesidades de entornos de TI diversos y distribuidos.

Acronis es una empresa suiza fundada en Singapur en 2003 que cuenta con 45 ubicaciones en todo el mundo. Acronis Cyber Protect Cloud está disponible en 26 idiomas en más de 150 países y la utilizan más de 20 000 proveedores de servicios para proteger más de 750 000 empresas. Obtenga más información en www.acronis.com.

