COHESITY

DOCUMENTO TÉCNICO

Topologías modernas de seguridad y gestión de datos: Una guía para líderes de TI

Guías y mejores prácticas para reducir el riesgo y fortalecer la resiliencia empresarial

ÍNDICE

Introducción

Tres factores están impulsando la necesidad de contar con un enfoque nuevo hacia la seguridad y la gestión de datos. En primer lugar, el imperativo de la transformación digital y la infraestructura basada en API. Los líderes de TI están modernizando todos los aspectos de su infraestructura tecnológica para apoyar una mayor automatización, escalabilidad en la nube, arquitecturas definidas por software, extensibilidad y los principios de seguridad "shift left".

En segundo lugar, el panorama de amenazas cibernéticas está evolucionando de maneras complejas e impredecibles. Los conjuntos de datos existentes de muchas organizaciones están aislados, lo que resulta en un mayor riesgo operativo de sufrir un ciberataque. Una encuesta reciente indica que el 32 % de las organizaciones cree que los tiempos de recuperación rápidos se ven obstaculizados por los sistemas anticuados de copia de seguridad y recuperación. Del mismo modo, el 34 % dice que la falta de integración entre los equipos de TI y de seguridad también prolonga los tiempos de recuperación.

Y en tercer lugar, la llegada de la IA ha hecho que los líderes busquen plataformas de datos modernas que hagan que los datos empresariales sean accesibles para las tecnologías de IA generativa.

Todo ejecutivo de TI que lidere un proyecto de modernización de datos puede beneficiarse de "pararse en los hombros de gigantes". En este informe técnico, describimos las consideraciones de diseño más importantes y cómo llegar al mejor enfoque de resiliencia de datos en vista de los requisitos empresariales comunes. Nuestra experiencia en miles de implementaciones y nuestro conocimiento de las mejores prácticas han dado forma a nuestras perspectivas.

La siguiente guía pretende ser independiente de los proveedores, pero usaremos los nombres de marca Cohesity para simplificar.

Factores clave de diseño

Todo proyecto de modernización que valga la pena conlleva riesgos. Esto ciertamente se aplica al transformar la seguridad de los datos empresariales y los procesos y herramientas de gestión. Pero hay buenas noticias: puede construir a partir del trabajo que otros han hecho antes que usted. Muchas organizaciones han modernizado con éxito su patrimonio de datos; en este documento, hemos catalogado estas mejores prácticas.

Los líderes de TI y ciberseguridad tienen la tarea de equilibrar la agilidad, el riesgo y el costo en toda su infraestructura tecnológica. Este patrimonio es dinámico y ahora abarca datos y aplicaciones que se ejecutan en centros de datos locales, nubes públicas, instalaciones de colocación y ubicaciones de borde. Los esfuerzos de modernización crecen en escala y alcance con el tiempo a medida que aumenta el volumen de las aplicaciones, datos y fuentes de datos.

Modernizar el patrimonio de datos empresariales se complica aún más debido a:

- Diversos objetivos de infraestructura en diferentes ubicaciones y múltiples cargas de trabajo, lo que resulta en la fragmentación de datos y procesos ineficientes de copia de seguridad y recuperación
- Falta de suficientes habilidades de TI y ciberseguridad dentro de la mayoría de las organizaciones
- Un panorama de ciberseguridad que cambia rápidamente, con cientos de ataques por minuto. La evolución y sofisticación de los ataques hace que la identificación temprana sea de vital importancia.

Dicho esto, hay algunos "primeros principios" a tener en cuenta.

La regla 3:2:1 sigue siendo aplicable

La regla 3:2:1 establece que debe conservar al menos tres copias de datos, que estas copias de seguridad deben almacenarse en dos tipos diferentes de medios o plataformas y que al menos una de las copias debe conservarse fuera del sitio.

El valor perdurable de la regla 3:2:1 proviene de tres conceptos que continúan impulsando el diseño de la topología del sistema en la era nativa de la nube:

- Requisitos comerciales
- Dominios de falla
- Casos fortuitos

Describiremos cada uno de estos conceptos en detalle. Siempre han sido enfoques clave en la industria y lo siguen siendo en la actualidad, especialmente con la intensificación de las preocupaciones en torno a los ciberataques. Los ciberataques no siempre fueron los protagonistas, pero ciertamente lo son ahora.

Definiremos cómo estos tres conceptos han dado forma a los diseños de las copias de seguridad y la recuperación a lo largo del tiempo y analizaremos cómo las inquietudes en torno a los ciberataques están obligando a nuestros clientes a preguntarse si sus topologías de implementación existentes siguen siendo suficientes (o no).

Analicemos cada uno:

Requisitos comerciales

Las empresas deben cumplir con un amplio conjunto de requisitos comerciales, regulatorios y de cumplimiento. Muchos de estos requisitos impulsan la necesidad de retener copias de datos actuales y pasadas. Por ejemplo, es posible que un equipo de cumplimiento deba obtener un contrato de tres años para responder a una solicitud de un

regulador de la industria. O un equipo de impuestos puede necesitar recuperar archivos para una auditoría en curso. O, de forma más identificable, tal vez un archivo crítico fue eliminado accidentalmente y debe restaurarse.

Dominios de falla

Es bien sabido en la industria de las tecnologías de la información que tanto el software como el hardware fallarán. Los proveedores de hardware y software hacen esfuerzos extraordinarios para diseñar en torno a esta inevitabilidad, pero las fallas persisten. Los equipos de TI deben planificar para las fallas y asegurarse de que estas fallas no afecten negativamente a la organización o al negocio. Algunos ejemplos de fallas incluyen fallas en la carga de trabajo, como la corrupción de una máquina virtual o un volumen de almacenamiento, o la implementación fallida de un parche del sistema operativo. En ambos casos, el equipo de TI necesita recuperarse de la falla y, como parte de esa recuperación, es probable que necesite datos de su sistema de copia de seguridad y recuperación.

Décadas atrás, los líderes no tenían que preocuparse por fallas causadas por actores malintencionados. Hoy en día, los ciberataques no solo son un factor clave de fallas en los sistemas, sino quizás la causa de falla más visible, y una que atrae la atención de la junta directiva.

Casos fortuitos

Este término se refiere a desastres naturales u otros eventos que están fuera del control humano y no se pueden prever o prevenir por medios razonables. Los eventos adversos como incendios, terremotos, inundaciones y cortes de cables pueden considerarse "casos fortuitos". Al igual que con los dominios de falla, las organizaciones de TI deben considerar la posibilidad de que ocurran casos fortuitos y diseñar sistemas que sean resilientes frente a ellos.

La regla 3:2:1 ofrece orientación práctica frente a los casos fortuitos.

Los sistemas fallan, por lo que es razonable tener varias copias de los datos disponibles. Debido a los dominios de falla, también es razonable mantener las copias de seguridad en dos tipos o sistemas de medios diferentes. Por último, debido a los casos fortuitos, es responsable mantener al menos una de estas copias en una ubicación remota, tal vez como parte de un sitio de recuperación ante desastres o centro de datos remoto.

Sus requisitos pueden variar, pero existen similitudes

Si bien la regla 3:2:1 es una práctica sólida, las organizaciones pueden optar por contar con implementaciones que hagan uso de menos de tres copias. Otros se adhieren más estrictamente a la regla 3:2:1, mientras que otros conservan más de tres copias. (Más adelante en este documento, le explicaremos la justificación de estas opciones de diseño).

Con respecto al diseño, hemos agrupado las topologías de implementación ("guías") en tres tipos.

Tipo	Description
Básico	Una topología de implementación con dos copias o menos
Mejorado	Una topología de implementación con tres copias
Misión crítica	Una topología de implementación con cuatro o más copias

Las arquitecturas de disponibilidad conocidas siguen siendo relevantes hoy en día

Pasemos a un término que los líderes y profesionales de TI con experiencia encontrarán más familiar: arquitectura de disponibilidad.

Una arquitectura de disponibilidad describe cómo un equipo de TI puede organizar sus sistemas de hardware y software para que sean resilientes ante una posible interrupción. En nuestra experiencia, la mayoría de las implementaciones empresariales consisten en una de tres arquitecturas de disponibilidad de clientes: ***activo-activo, activo-en espera y Hub and Spoke***.

Cada uno de estos enfoques se muestra en la página siguiente.

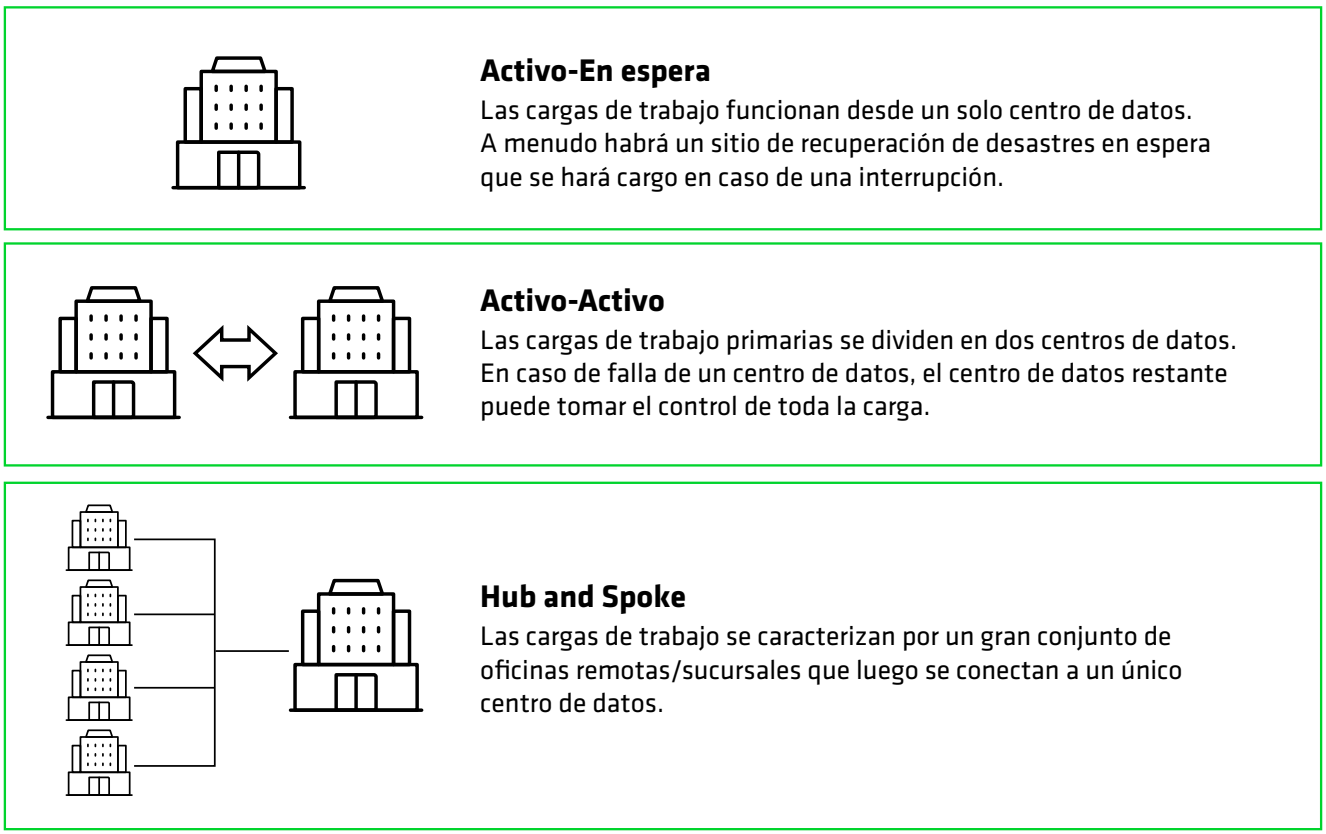


Fig. 1: Arquitecturas de disponibilidad del cliente

En cada caso, la arquitectura de disponibilidad está diseñada para garantizar que las operaciones comerciales puedan continuar en caso de una falla. Cuando el lado "activo" de una arquitectura **activa-en espera** tiene una falla, todo el procesamiento cambia al otro sistema en espera. Cuando falla cualquiera de los lados de un sistema **activo-activo**, el otro lado asume el 100 % de la carga de trabajo. Y cuando hay una falla en un sistema tipo **Hub and Spoke**, como cuando los datos se destruyen por una falla de hardware u otro problema en una oficina sucursal, el sistema y sus datos pueden restaurarse desde el hub una vez que se resuelve la causa de la falla.

Los equipos responsables de las tecnologías de la información han diseñado estas arquitecturas de disponibilidad y las prueban de manera rutinaria para garantizar que los mecanismos de resiliencia funcionen correctamente.

Nuestro conjunto de mejores prácticas de guías se basa en estas arquitecturas de disponibilidad comprobada. En Cohesity, no implementamos sistemas de copia de seguridad y recuperación en un vacío. Los diseñamos para que se alineen estrechamente con la infraestructura de TI subyacente. Verá esto en detalle más adelante en este documento, cuando cubramos varias topologías de copia de seguridad y recuperación, y cómo esas topologías se mapean a las arquitecturas de disponibilidad de TI.

Guías para la seguridad y gestión de datos modernos: Tipos y topologías

Ya hemos analizado los tipos de copias de seguridad básicas, mejoradas y de misión crítica. Ahora le presentaremos las topologías asociadas con estos tipos.

Pero primero, mencionaremos algunas definiciones. Los sistemas de gestión y seguridad de datos pueden almacenar datos a través de diferentes métodos. Las copias de los datos pueden conservarse como ***copias de seguridad, réplicas*** o ***archivos***.

Algunas reglas generales son las siguientes:

- **Las copias de seguridad** se forman a partir de una copia primaria y dan como resultado datos desduplicados, comprimidos y cifrados. Este procesamiento se realiza una vez a los datos y luego los datos de copia de seguridad procesados pueden ser copiados a una réplica o un archivo.
- **Las réplicas** generalmente se utilizan para la retención a corto plazo, generalmente meses, pero no años. Estas réplicas a menudo admiten arquitecturas de disponibilidad de TI como activo-activo o activo-en espera.
- **Los archivos** generalmente se utilizan para la retención a largo plazo y a menudo se conservan durante años. Los archivos a menudo se utilizan para fines de cumplimiento y regulatorios, pero en algunos casos también se utilizan para arquitecturas de disponibilidad de TI.
- **La restauración desde una copia de seguridad o réplica** es un proceso de un solo paso y es más rápida que la restauración desde un archivo, que es un proceso de dos pasos. El archivo debe descargarse en el sistema de copia de seguridad y recuperación del proveedor antes de ser restaurado al sistema de TI.
- **La restauración de un ataque de ransomware** se complica por la necesidad de restaurar a una copia limpia y no infectada que probablemente no sea la copia de seguridad más reciente. Una organización no puede simplemente restaurarse de un ataque de ransomware de la misma manera que se restaura de una falla o interrupción del dominio causada por un acto de la naturaleza. La organización afectada tendrá que analizar el entorno y asegurarse de que las copias que están siendo recuperadas estén libres de la infección por malware que causó el ataque en primer lugar.

En la tabla a continuación aparece la lista de topologías. Tenga en cuenta que cada topología tiene una única copia de seguridad donde los datos se deduplican, comprimen y cifran. Además de la copia de seguridad, las diversas topologías pueden conservar una o más réplicas y uno o más archivos también. Hemos dado un descriptor (B1, B2, E1, E2, M1, M2, etc.) a cada tipo de topología para ayudar a llevar un registro de ellas.

Tipo	Copias	Topología/Tipo de copias
Básico	1	B1 - Copia de seguridad
	2	B2 - Copia de seguridad y archivo
	2	B3 - Copia de seguridad y replicación
Mejorado	3	E1 - Copia de seguridad, replicación y archivo
	3	E2 - Copia de seguridad y réplica doble
Misión crítica	4	M1 - Copia de seguridad y réplica doble con archivo
	4	M2 - Copia de seguridad, replicación y archivo doble
	5	M3 - Copia de seguridad, réplica doble y archivo doble

Una combinación de tipo/topología se define tanto **por la cantidad de copias como por la naturaleza de esas copias**. Por ejemplo, un tipo mejorado, que siempre incluye tres copias, puede tener dos topologías distintas. Una topología es copia de seguridad, replicación y archivo, mientras que la otra es copia de seguridad y réplica doble. Tenga en cuenta que no todas las permutaciones de copias de datos han sido enumeradas; esta lista simplemente representa las implementaciones más comunes. Algunas combinaciones simplemente no tienen sentido comercial o técnico.

Es útil comprender qué topologías se utilizan comúnmente y cuáles no. La popularidad relativa de cada patrón puede ofrecer rutas de "actualización" útiles a medida que los equipos de TI consideran una protección adicional para su patrimonio de datos.

Guías: La lista completa de topologías

Ahora que hemos descrito los tipos, las topologías y las arquitecturas de disponibilidad de los clientes, expongamos la lista completa de guías de la industria.

Esta tabla une todos los conceptos que analizamos anteriormente. Todas las configuraciones representan una opción popular en el mundo real, con empresas reales que operan a escala con Cohesity.

Tipo	Topología/Tipo de copias	Arquitectura de disponibilidad del cliente		
		Activo-En espera	Activo-Activo	Hub and Spoke
Básico	B1 Copia de seguridad (1)	•	•	
	B2 Copia de seguridad y archivo (2)	•	•	
	B3 Copia de seguridad y replicación (2)	•	•	
Mejorado	E1 Copia de seguridad, replicación y archivo (3)	•	• •	•
	E2 Copia de seguridad y réplica doble (3)	•	•	
Misión crítica	M1 Copia de seguridad y réplica doble con archivo (4)	•		
	M2 Copia de seguridad, replicación y archivo doble (4)	•	•	
	M3 Copia de seguridad, réplica doble y archivo doble (5)		•	

Una advertencia sobre las topologías de misión crítica. Estas topologías han sido implementadas, demostradas, probadas o analizadas en detalle con empresas u otros clientes grandes. Anteriormente observamos que muchos clientes buscan una mayor resiliencia en sus implementaciones. Las discusiones implican formas prácticas de proteger las copias adicionales de los datos. Una solución común es mejorar la implementación con un repositorio cibernético. Por ese motivo, muchas de las topologías de misión críticas contienen un archivo configurado como un repositorio cibernético. (Ofrecemos Cohesity FortKnox para este escenario). Muchas topologías pueden ser más resilientes a nivel cibernético con la adición de un repositorio cibernético.

Ahora analizaremos los tipos y las topologías en detalle, un grupo a la vez.

Básico

Topología	Centro de datos principal	Activo-Activo
B1 - Copia de seguridad	✓	✓
B2 - Copia de seguridad y archivo	✓	✓
B3 - Copia de seguridad y replicación	✓	✓

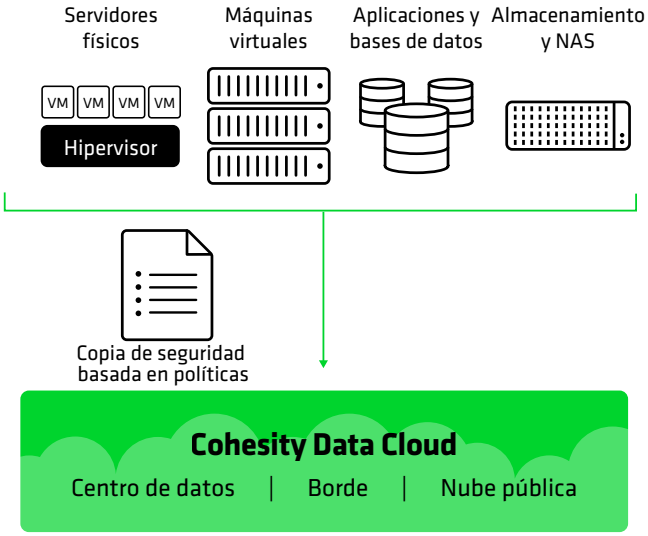
Un tipo básico es popular con datos de valor bajo y moderado, o en casos en los que el cliente ya cuenta con varias copias de sus datos. Las topologías básicas se utilizan cuando hay un único centro de datos primario y también para enfoques activo-activo.

¿Qué es un repositorio cibernético?

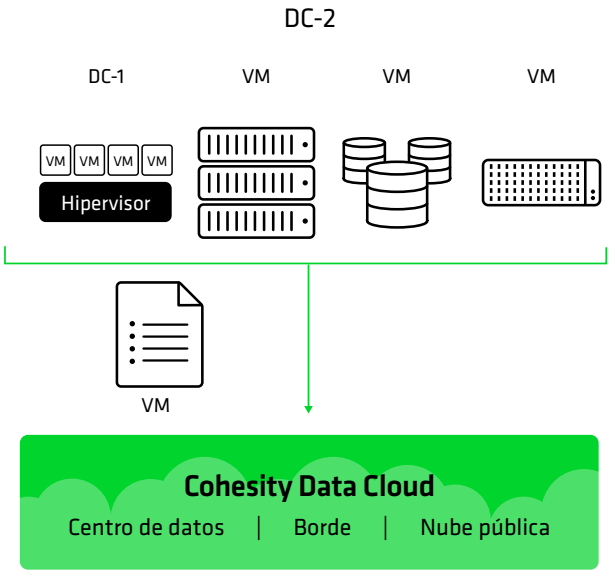
Un repositorio cibernético almacena una copia aislada de los datos de producción, a menudo fuera del sitio. Con una copia de datos limpia, independiente y protegida siempre disponible, las organizaciones pueden recuperar rápidamente los datos a su fuente original o a ubicaciones de respaldo alternas en caso de un ataque de ransomware u otro incidente que comprometa los sistemas de producción o las copias de seguridad principales. Una estrategia moderna de repositorio cibernético utiliza tecnología de "brecha de aire virtual" que protege las copias de seguridad pero permite conexiones de red temporales para habilitar el acceso remoto necesario, aunque con controles muy estrictos, al tiempo que aísla aún más los datos utilizando la nube según se requiera. Un repositorio cibernético bien diseñada puede ser una parte eficaz de una estrategia sólida de aislamiento de datos y resiliencia cibernética.

Básico: B1 - Copia de seguridad local

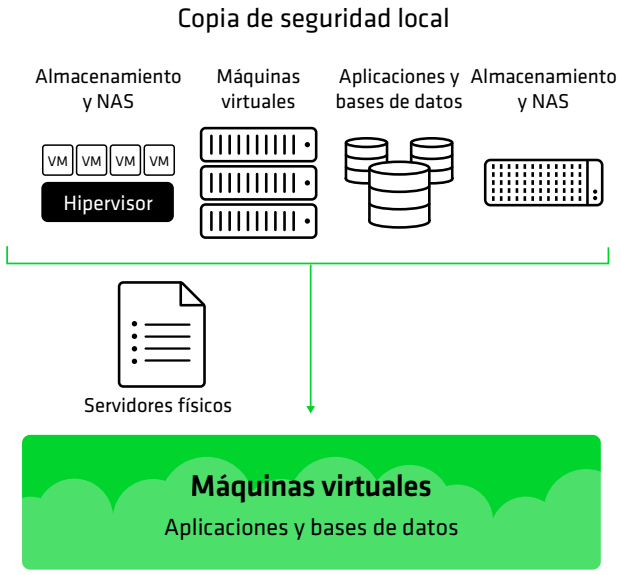
Este es un enfoque básico, con solo una copia de seguridad de los datos. Muchos centros de datos de TI aún utilizan este enfoque, aunque no tiene ninguna previsión para la recuperación ante desastres o la retención a largo plazo de los datos de copias de seguridad. Este enfoque generalmente se utiliza para datos de bajo valor.



Básico: B1 - Copia de seguridad (Activo-Activo)



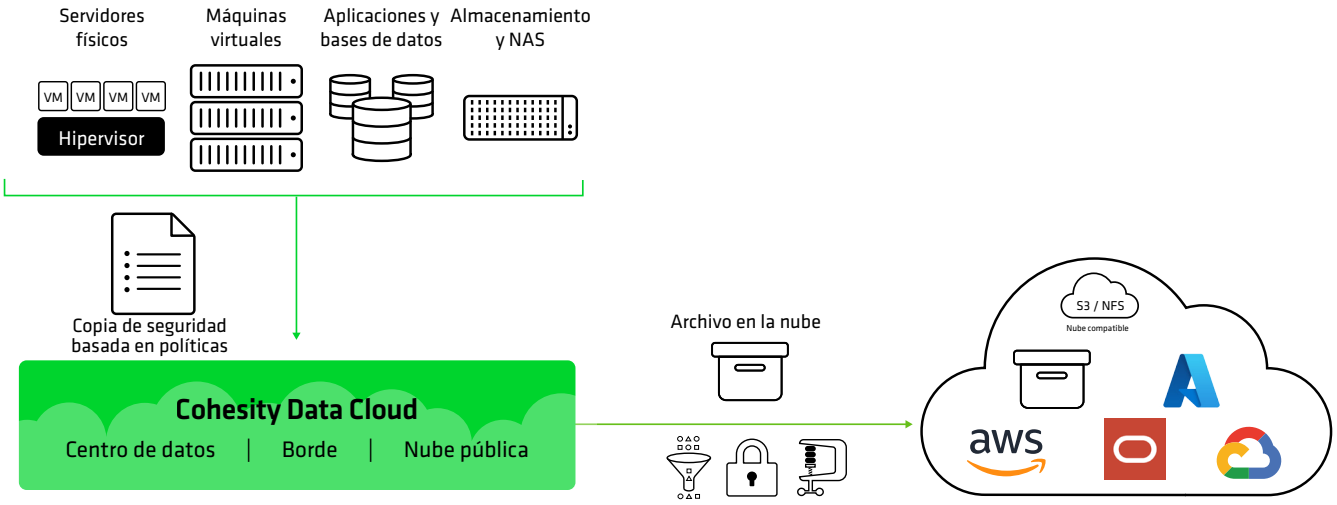
Copia de seguridad local



Copia de seguridad basada en políticas

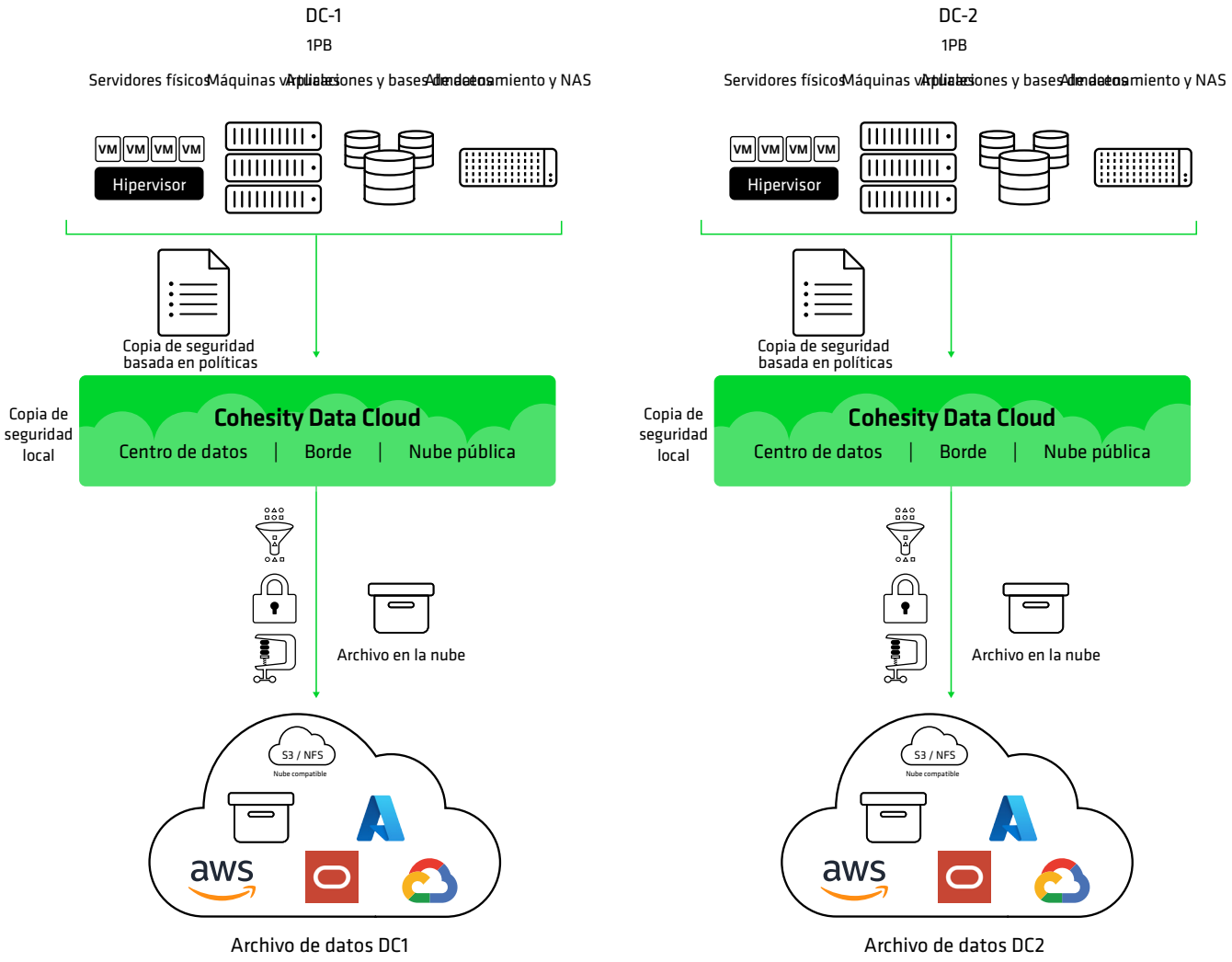
Muchos tipos y topologías se prestan a un enfoque activo-activo. Un enfoque activo-activo consiste efectivamente en dos instancias de un mismo tipo de topología, reflejadas y dispuestas de manera inversa. En esta topología, tenemos un par de centros de datos activo-activo, cada uno con su propia copia de seguridad. Cualquier centro de datos puede asumir el control en caso de interrupción. Cada centro de datos también tiene una copia de seguridad completa de sus datos y cargas de trabajo. Para los clientes con una gran cantidad de ancho de banda WAN disponible, incluso la copia de seguridad puede separarse geográficamente del centro de datos para proporcionar prevención adicional de desastres. Toda replicación de cargas de trabajo y datos ocurre en la capa de carga de trabajo, por lo que esta topología no requiere replicación.

Básico: B2 - Copia de seguridad y archivo



En este caso, la copia de seguridad se combina con un archivo con un período de retención mucho más largo que la copia de seguridad. Cohesity FortKnox es una opción popular en este sentido, ya que proporciona seguridad adicional para esta topología. FortKnox es un archivo aislado y solo se conecta cuando se realiza una escritura en el archivo o una restauración desde el archivo. El archivo también puede ser a una nube privada dentro/fuera de las instalaciones o a una nube pública como AWS, Google Cloud, Microsoft Azure, Oracle Cloud o cualquier servicio de nube compatible con S3/NFS.

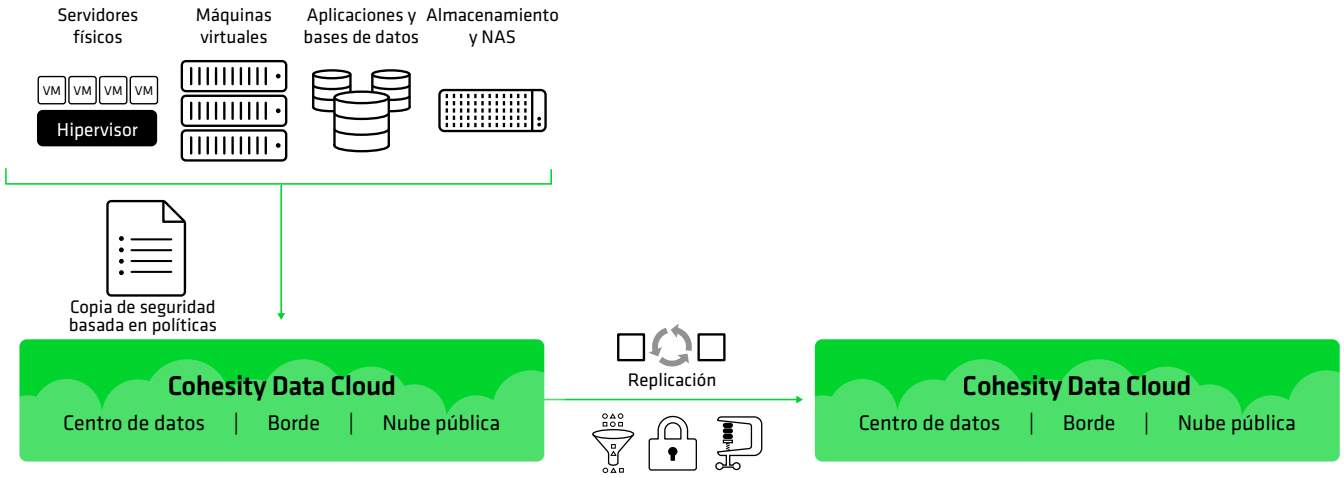
Básico: B2 - Copia de seguridad y archivo (Activo-Activo)



En esta topología, tenemos un par de centros de datos activo-activo, cada uno con su propia copia de seguridad y archivo. Cualquier centro de datos puede asumir el control en caso de una interrupción, y cada centro de datos también cuenta con una copia de seguridad completa de sus datos y cargas de trabajo en todo el archivo.

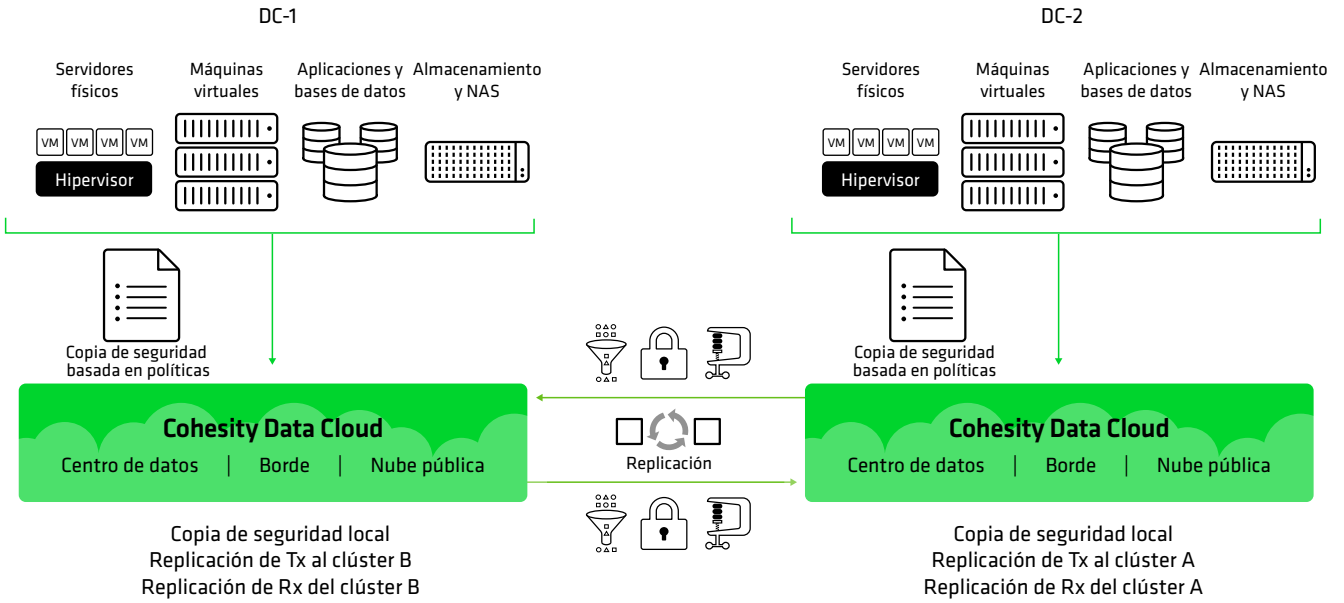
Toda replicación de cargas de trabajo y datos ocurre en la capa de carga de trabajo, por lo que esta topología no requiere replicación. FortKnox sería una opción útil para un archivo, debido a su aislamiento y seguridad adicional.

Básico: B3 - Copia de seguridad y replicación (recuperación ante desastres)



En esta topología, la copia de seguridad y la réplica están aproximadamente alineadas en cuanto al período de retención. La réplica se distribuye geográficamente y se utiliza para la recuperación ante desastres. Para los clientes con una gran cantidad de ancho de banda WAN disponible, incluso la copia de seguridad puede separarse geográficamente del centro de datos para proporcionar prevención adicional de desastres. El enfoque de esta topología está en la continuidad del negocio en caso de que la copia de seguridad no esté disponible. Las réplicas pueden restaurar los datos directamente, sin requerir el proceso de dos pasos que se necesita cuando se utiliza un archivo.

Básico: B3 - Copia de seguridad y replicación cruzada (Activo-Activo)



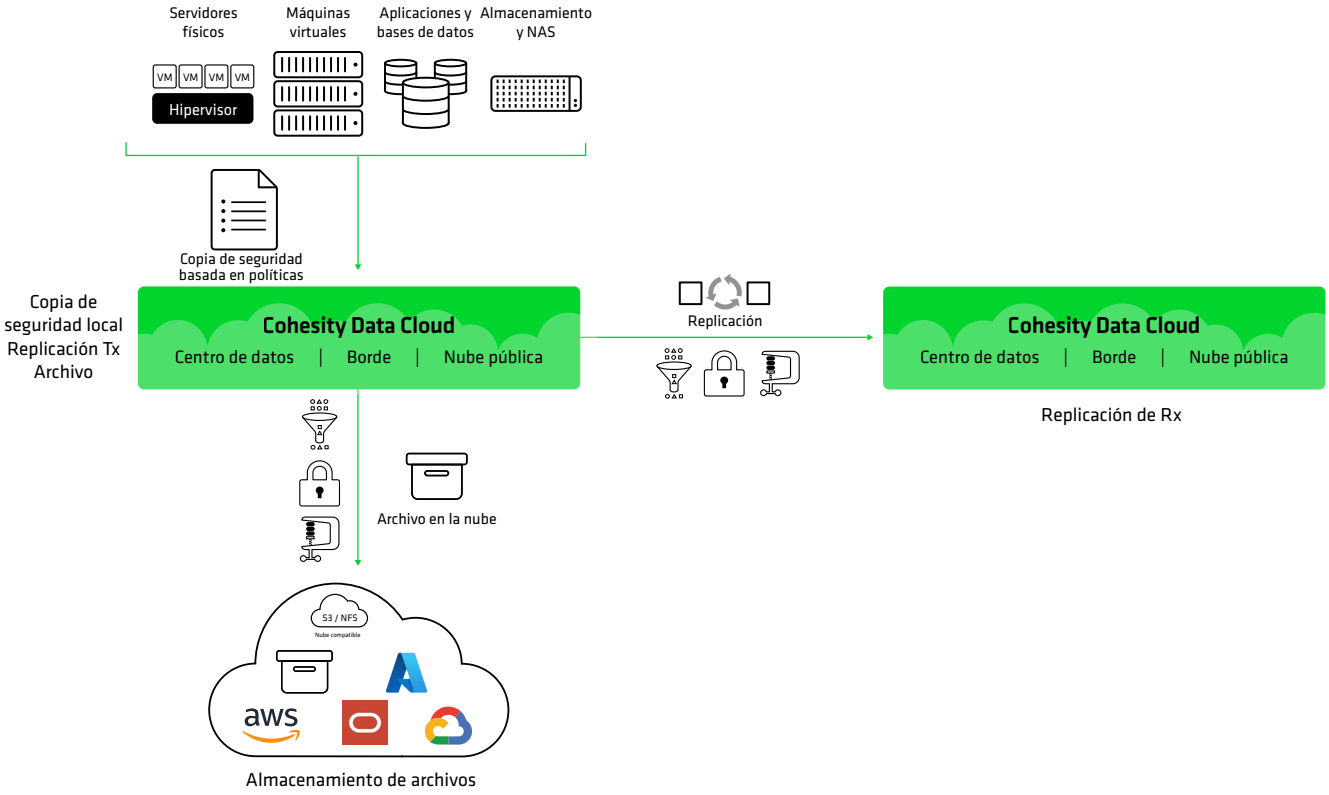
En este caso, los clústeres de copias de seguridad y replicación se replican de forma cruzada. La copia de seguridad del primer sitio es la réplica del segundo sitio y viceversa.

Topologías mejoradas (incluida la adopción por industria)

Las topologías mejoradas son populares para los datos de alto valor. Copia de seguridad, replicación y archivo (E1) es lo más popular, mientras que copia de seguridad y la réplica doble (E2) es menos popular. A continuación se marcan las topologías de uso común, junto con los favoritos destacados por industria.

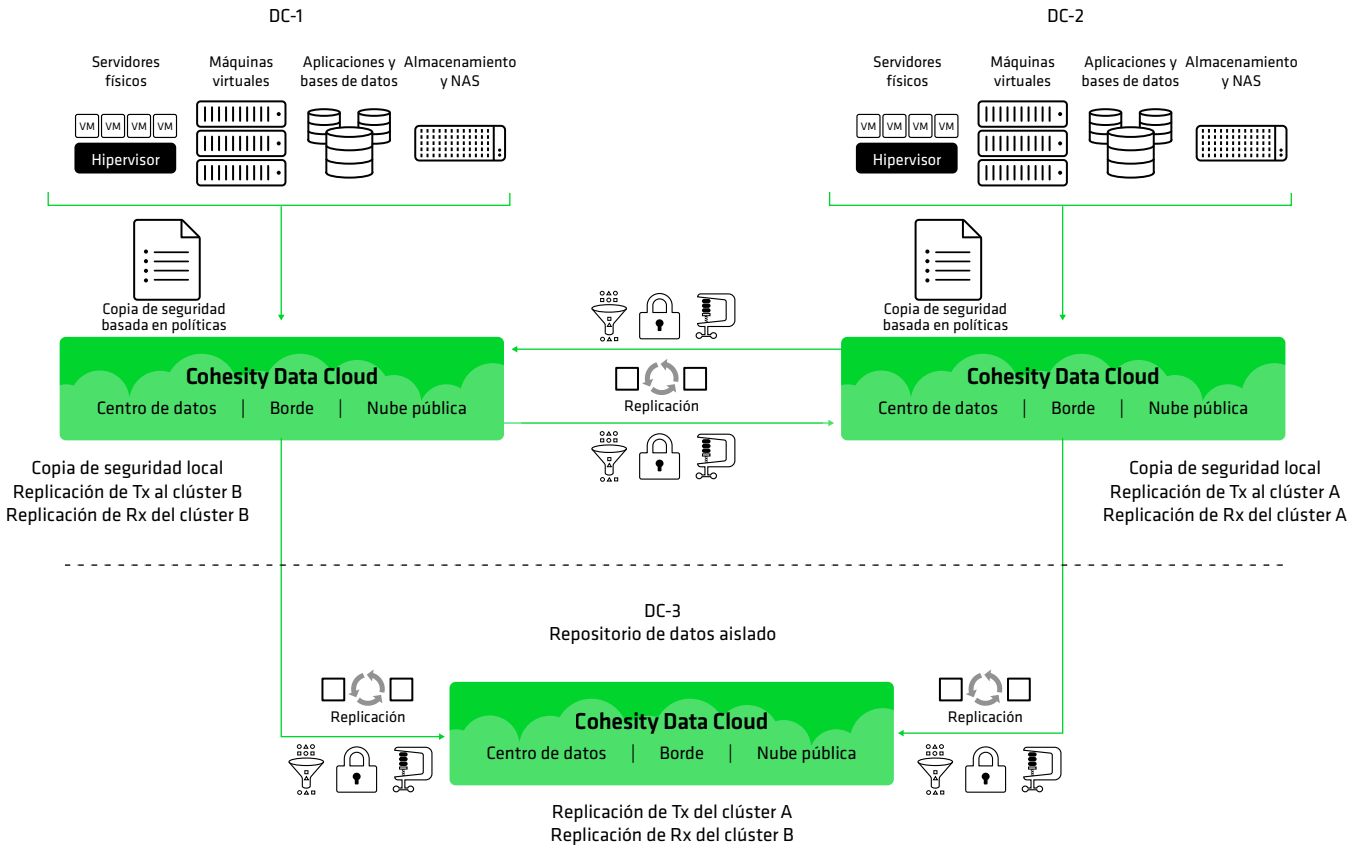
Topología	Centro de datos principal	Activo-Activo	Hub and Spoke
E1 - Copia de seguridad, replicación y archivo	✓ Todos los tipos	✓ Instituciones financieras	
E2 - Copia de seguridad y réplica doble	✓ Agencias gubernamentales	✓ Cadenas de venta minorista, algunas agencias gubernamentales que utilizan un modelo este-oeste	

Mejorado: E1 - Copia de seguridad, replicación y archivo



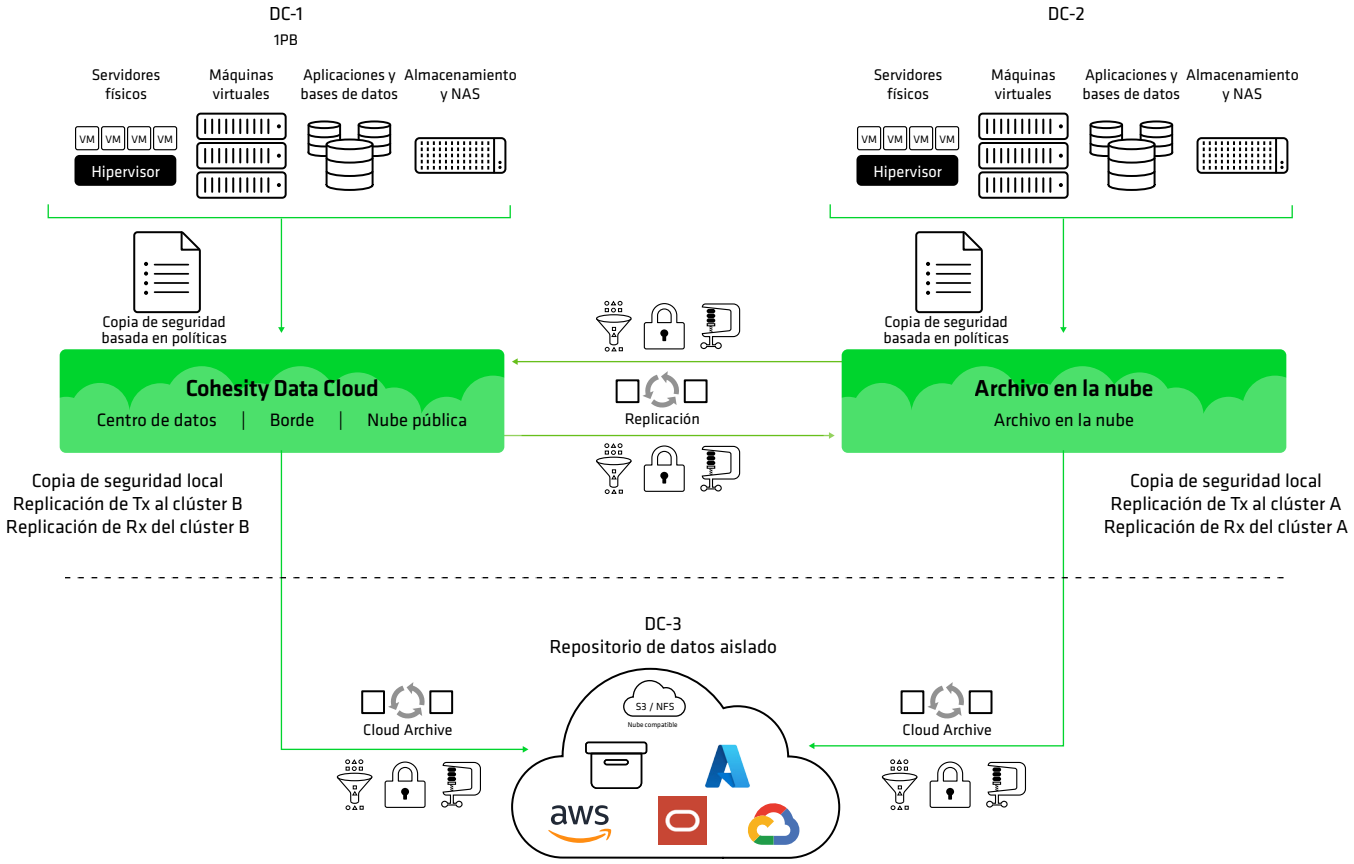
La copia de seguridad y la réplica están aproximadamente alineados (p. ej., dos veces al día durante 90 días), mientras que el archivo puede cubrir meses o incluso años. La recuperación a partir de una copia de seguridad o réplica es un proceso de un solo paso, mientras que la recuperación desde un archivo implica dos pasos: una lectura del archivo y luego una restauración de los datos. El archivo puede ser a una nube privada dentro/fuera de las instalaciones o a una nube pública como AWS, Google Cloud, Microsoft Azure, Oracle Cloud o cualquier servicio de nube compatible con S3/NFS. FortKnox también sería una excelente opción para esta topología debido a su aislamiento y seguridad adicionales. Tenga en cuenta que con Cohesity Data Cloud, se puede restaurar un archivo a través de un clúster primario o secundario.

Mejorado: E1 - Activo-Activo con un repositorio de datos



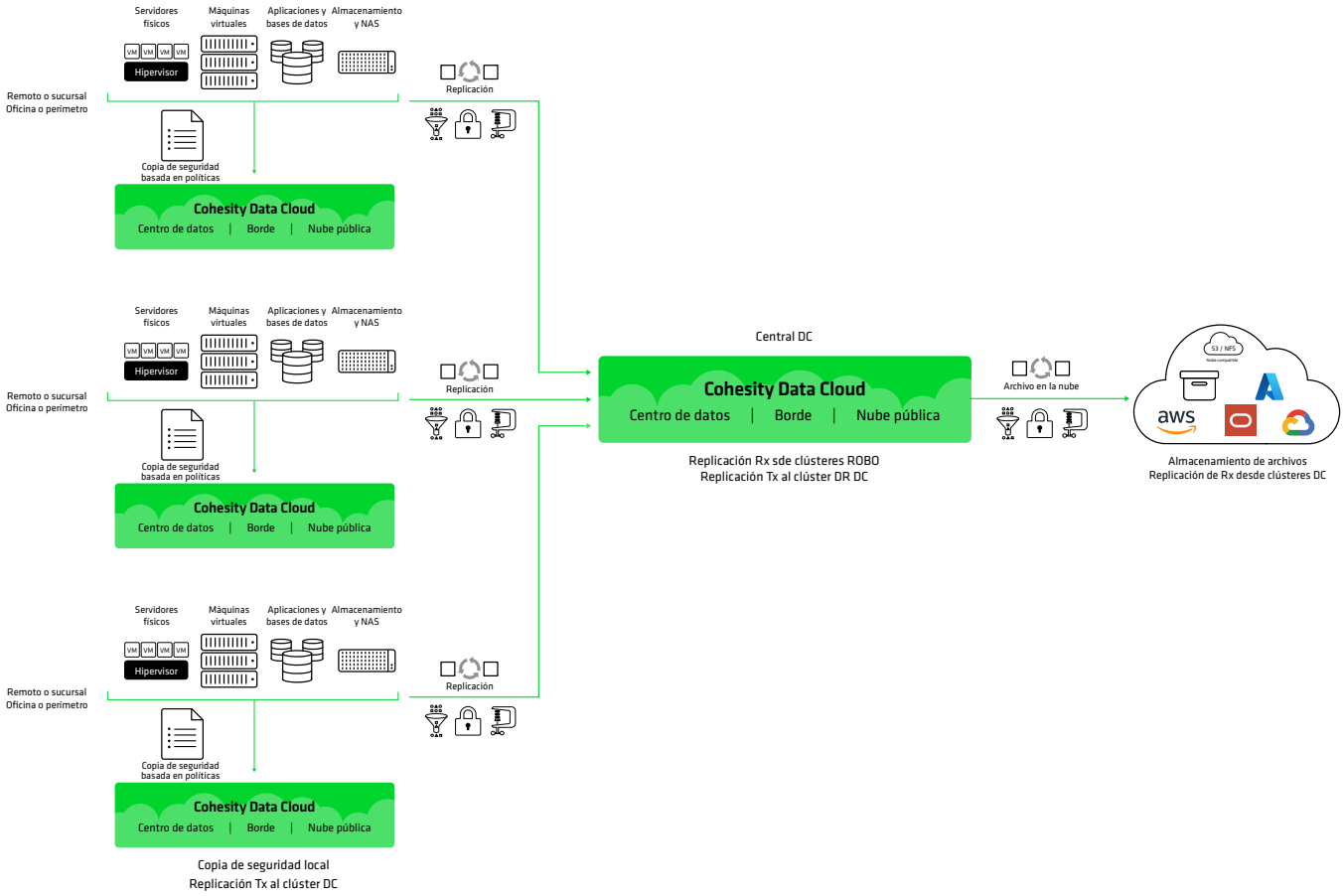
Esta topología es otro enfoque **activo-activo**. Aquí, los centros de datos de replicación cruzada comparten un único repositorio de datos aislada. El aislamiento es físico, con el repositorio de datos desconectada de la red cuando no está en uso. Tenga en cuenta que la bóveda es una réplica, lo que permite una recuperación de un paso de cualquiera de los centros de datos desde la réplica. Esta arquitectura también puede extenderse, con múltiples pares activo-activo que utilizan el mismo repositorio de datos.

Mejorado: E1 - Activo-activo con un archivo aislado



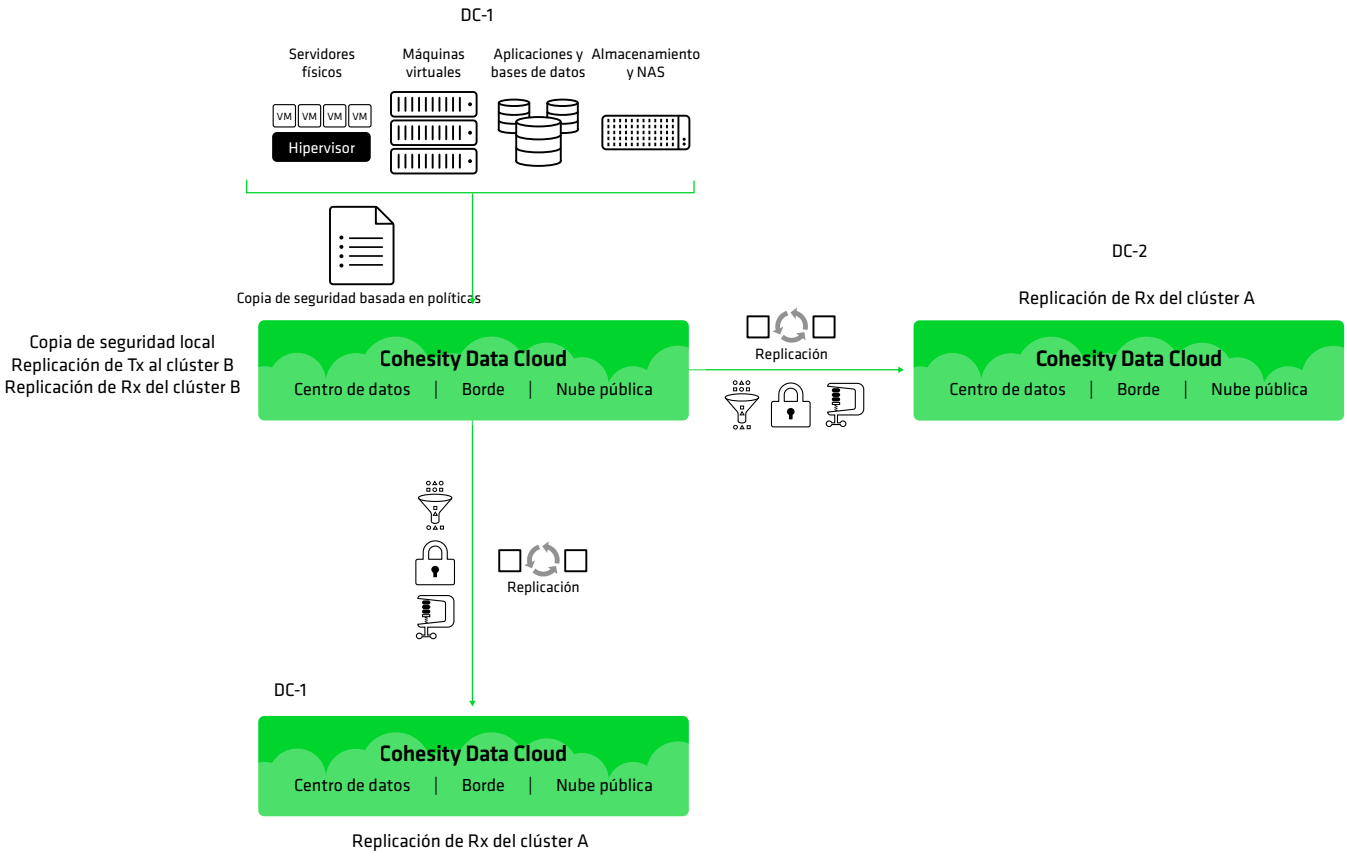
El gráfico anterior es otro enfoque **activo-activo**. En este caso, los centros de datos de replicación cruzada compartieron un único archivo aislado. Este caso de uso funcionaría bien con nuestro enfoque de archivo FortKnox debido a su aislamiento y seguridad adicionales. Esta arquitectura también puede extenderse, con varios pares activo-activo, todos con el mismo archivo aislado. Con Cohesity Data Cloud, se puede restaurar un archivo a partir de cualquiera de las copias de seguridad o réplicas.

Mejorado: E1 - Copia de seguridad, replicación y archivo (Hub and Spoke)



Muchas topologías también pueden extenderse a **Hub and Spoke**, lo que también se conoce como topología fan-in. En el modelo Hub and Spoke, las sucursales individuales tienen sus propias copias de seguridad, y esas copias de seguridad se replican en una sola nube de datos Cohesity Data Cloud integrada en un centro de datos central. Desde el centro de datos central, la réplica se archiva a través de FortKnox o a otro archivo privado o público. FortKnox sería una gran opción aquí, ya que proporciona aislamiento completo en caso de que tanto las copias de seguridad como la réplica se vieran comprometidas. Con Cohesity Data Cloud, se puede restaurar un archivo a través de un clúster primario o secundario.

Mejorado: E2 - Copia de seguridad y réplica doble



Esta topología es para aquellos casos en que el proceso de restauración de dos pasos de un archivo no proporciona un RTO suficientemente bajo. Las tres copias (la copia de seguridad y ambas réplicas) se pueden utilizar para restaurar los datos en un proceso de un solo paso en esta configuración.

Mejorado: E2 - Hub and Spoke con Hubs activo-activo

Esta topología combina varios modelos diferentes. Cada una de las sucursales remotas realiza sus propias copias de seguridad, y esas copias de seguridad se replican en un centro de datos central. Este centro de datos central también tiene un centro de datos de recuperación ante desastres como copia de seguridad. Todo está reflejado, con el centro de datos principal a la izquierda sirviendo como sitio de recuperación ante desastres para el centro de datos a la derecha y viceversa.

Misión crítica

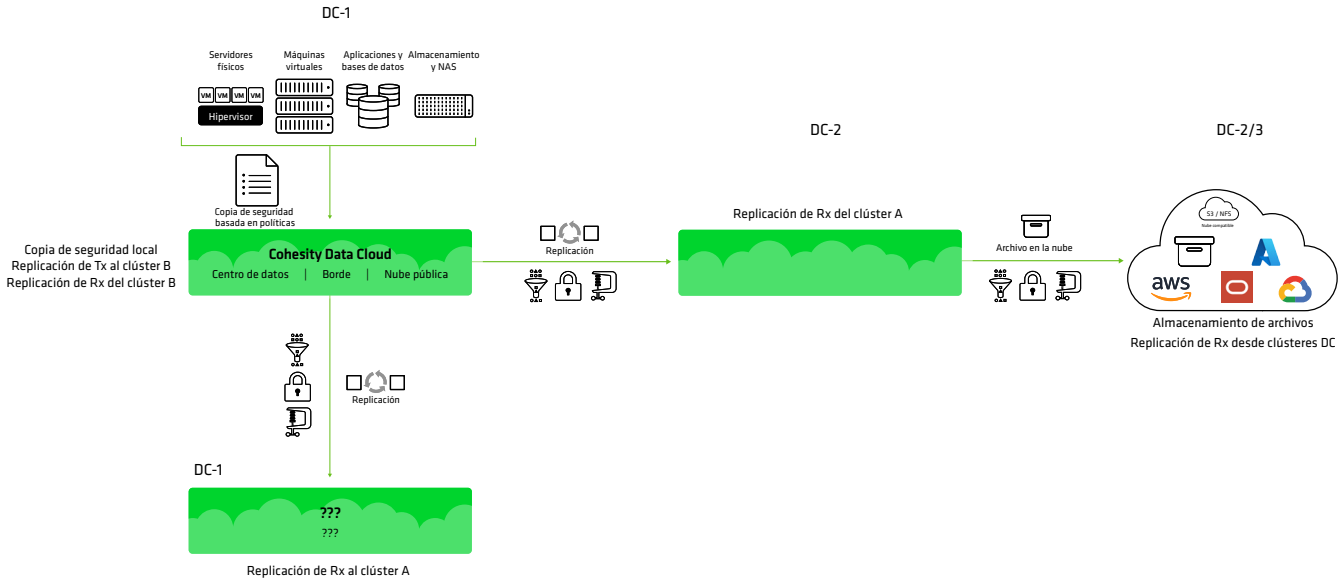
Topología	Centro de datos único	Activo-Activo	Hub and Spoke
Copia de seguridad y réplica doble con archivo	✓		✓
Copia de seguridad, replicación y archivo doble	✓	✓	
Copia de seguridad, réplica doble y archivo doble		✓	

El modo Misión crítica está emergiendo como una topología para los datos más valiosos en una empresa determinada. Estos son los datos necesarios para ejecutar la viabilidad mínima de una empresa (Minimum Viable Company, MVC).

¿Cuál es la viabilidad mínima de una empresa?

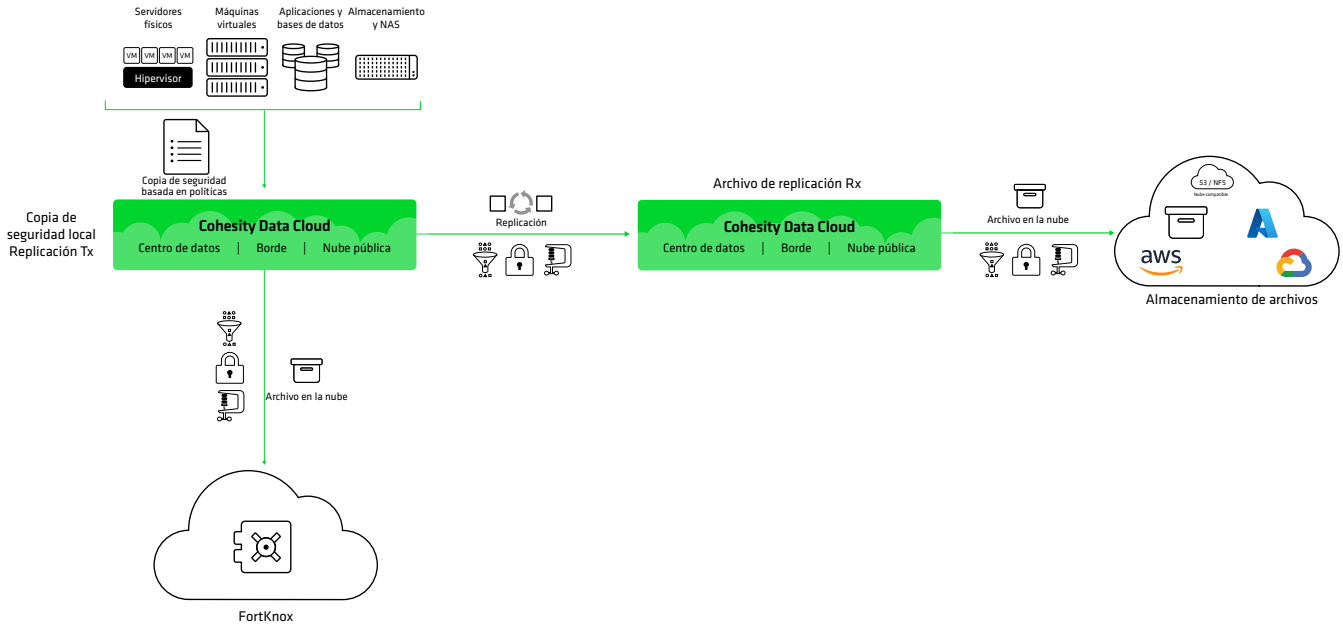
Una MVC es la recopilación de aplicaciones, infraestructura y procesos que deben restaurarse para que el negocio funcione a un nivel mínimamente viable. Estos sistemas deben volver volver a estar en línea primero; todos los demás sistemas son una prioridad secundaria. Los líderes de TI deben emplear la MVC cuando planifiquen sus estrategias de respuesta ante incidentes y recuperación, así como su topología de datos.

Misión crítica: M1 - Copia de seguridad y réplica doble con archivo



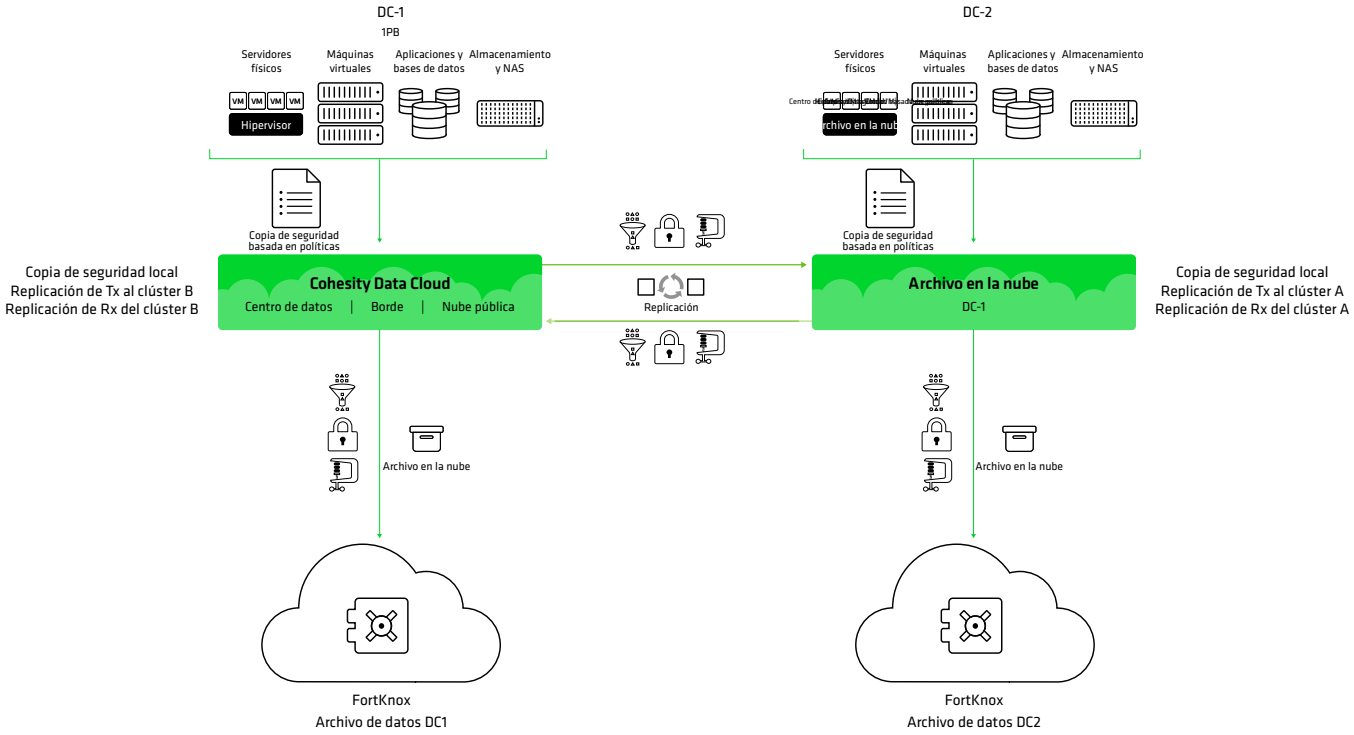
Esta arquitectura tolerante a fallas cumple con estrictos requisitos de RTO y RPO y se combina con un requisito de retención a largo plazo. La segunda réplica proporciona recuperación adicional ante desastres y protección contra ransomware. Con Cohesity Data Cloud, se puede restaurar un archivo a través de un clúster primario o secundario. Agregar una brecha de aire a la segunda réplica proporciona resiliencia adicional.

Misión crítica: M2 - Copia de seguridad y replicación con archivo doble usando FortKnox (desde copia de seguridad local)



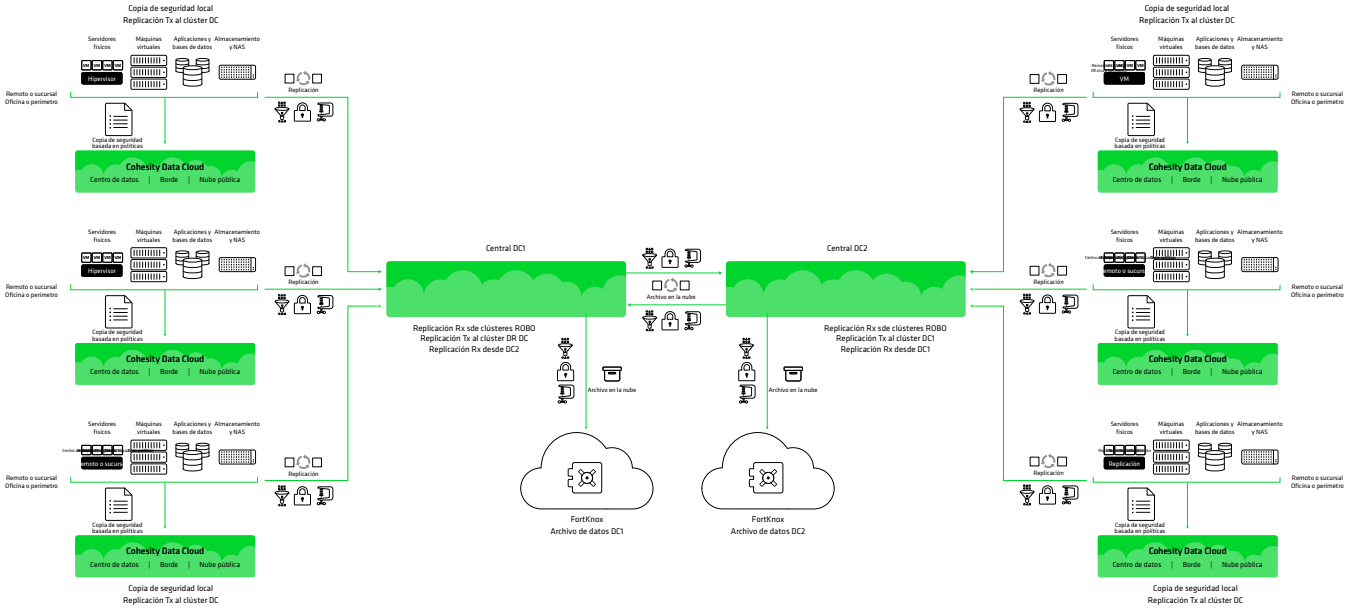
Esta arquitectura tolerante a fallas utiliza FortKnox en lugar de una segunda réplica, ya que FortKnox proporciona seguridad y aislamiento adicionales. El primer archivo se puede utilizar para actividades de cumplimiento, mientras que el archivo FortKnox proporciona resiliencia adicional anti-ransomware. Con Cohesity Data Cloud, se puede restaurar un archivo a través de un clúster primario o secundario.

Misión crítica: M2 - Replicación cruzada y archivo desde Local con FortKnox



Este es el modelo **activo-activo** que vimos en las topologías **básicas**, con la adición de archivos dobles de FortKnox. Dado que cada clúster contiene copias DC1 y DC2, cada instancia de FortKnox también contiene copias DC1 y DC2. Con Cohesity Data Cloud, se puede restaurar un archivo a través de un clúster primario o secundario.

Misión crítica: M3 - Hub and Spoke con Hubs activo-activo y el archivo FortKnox



Esto es similar a lo que vimos en los tipos **mejorados**, pero en este caso, cada una de las réplicas está conectada a FortKnox como un archivo a largo plazo. Dado que las réplicas tienen copias de los spokes izquierdo y derecho, cada uno de los archivos de FortKnox también cuenta con ambos conjuntos de copias. Con Cohesity Data Cloud, se puede restaurar un archivo a través de un clúster primario o secundario.

Conclusiones y próximos pasos

Muchos líderes empresariales buscan fortalecer la protección de sus datos críticos. A medida que analizamos nuevos enfoques con estos responsables de la toma de decisiones, las guías se tornan fundamentales. Los diseños analizados en este informe técnico ayudarán a los ejecutivos a comprender lo que sus colegas han hecho en situaciones similares con requisitos de protección de datos parecidos.

"Más" no siempre es mejor cuando se trata de las copias de datos. Tanto Cohesity como nuestros clientes entienden que agregar más copias de datos agrega costos operativos, de licencias y, a menudo, de hardware. En algunos casos, no abogamos por agregar una copia adicional, sino que alentamos el uso de diferentes tipos de copias.

A menudo recomendamos el uso de archivos para actividades de cumplimiento de la empresa y para promover la resiliencia cibernética. Por lo tanto, nuestros clientes a menudo eligen conservar la misma cantidad de copias de datos, pero cambian el tipo de copias que utilizan. Pueden, por ejemplo, reemplazar un archivo in situ no seguro con un archivo aislado como FortKnox para proporcionar copias que se pueden utilizar tanto con fines de cumplimiento como con fines de resiliencia de ransomware.

Las guías son poderosas porque le permiten revisar todas las opciones relevantes y comprobadas, y tomar una decisión informada sobre cuál de estas opciones utilizará en su implementación.

El siguiente cuadro proporciona una vista simplificada y agregada del beneficio de cada topología en relación con los dominios de falla, los casos fortuitos y la protección cibernética.

Tipo	**Básico**		**Mejorado**	**Misión crítica**	
Copias	**1**	**2**	**3**	**4**	**5**
Topología	**Solo copia de seguridad**	**Copia de seguridad y repositorio** (Réplica o archivo)	**Copia de seguridad y repositorio doble** (Réplica y archivo, o réplica doble)	**Copia de seguridad y réplica doble y archivo**	**Copia de seguridad y réplica doble y archivo doble**
Protección contra dominios de falla HW y SW	★	★ ★	★ ★ ★	★ ★ ★ ★	★ ★ ★ ★
Protección contra "casos fortuitos"		★	★ ★ ★	★ ★ ★ ★	★ ★ ★ ★
Protección cibernética	★	★ ★	★ ★ ★	★ ★ ★ ★	★ ★ ★ ★

El recorrido hacia la seguridad y la gestión de datos modernos puede parecer abrumador. Reunimos esta información del plan maestro para facilitar el proceso y ayudarte a acelerar la consecución de mejores resultados empresariales, reduciendo al mismo tiempo riesgos y costos.

A partir de aquí, recomendamos los siguientes pasos:

1. Determine qué guías son las más relevantes para su situación.
2. Evalúe el ROI y el TCO de una plataforma de datos moderna con respecto a su solución actual. Los puntos clave de comparación deben ser:
    a. Eficiencia de protección de datos
    b. Eficiencia operativa
    c. Riesgo y cumplimiento
3. Seleccione su solución en función de las demostraciones de productos, los cálculos comprobados de ROI y TCO, y el soporte para las prioridades de la hoja de ruta.
4. Implemente la solución elegida siguiendo las guías más relevantes y proceda a ejecutar la hoja de ruta del paso anterior.

Una vez que su plataforma moderna esté implementada, genere un conjunto inicial de KPI con respecto a la resiliencia cibernética y mida regularmente su progreso en relación con esta línea de referencia. Desde allí, sabrá cuándo avanzar a la siguiente fase de su recorrido.

Acerca de Cohesity

Cohesity es el líder en seguridad de datos impulsada por IA. Más de 13 600 clientes empresariales, incluidos más de 85 de las empresas Fortune 100 y casi el 70 % de las empresas Global 500, confían en Cohesity para fortalecer su resiliencia y, al mismo tiempo, proporcionar información sobre la inteligencia artificial generativa en sus vastas cantidades de datos. Formadas a partir de la combinación de Cohesity con el negocio de protección de datos empresariales de Veritas, las soluciones de la empresa aseguran y protegen los datos en las instalaciones, en la nube y en el borde. Con el respaldo de NVIDIA, IBM, HPE, Cisco, AWS, Google Cloud y otros, Cohesity tiene sede en Santa Clara, CA, con oficinas en todo el mundo. Para obtener más información, siga a Cohesity en **LinkedIn**, **X** y **Facebook**.

Obtenga más información en Cohesity

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000050-002 ES 4-2025