# Conservación de la protección de datos en el mundo de la multicloud híbrida

UN DOCUMENTO ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™)
PREPARADO PARA IBM
POR PAULA MUSICH
JUNIO 2020

EMA™
TI Y GESTIÓN DE DATOS
INVESTIGACIÓN | ANÁLISIS DE LA INDUSTRIA | CONSULTORÍA

# Tabla de contenido

# MANTENER LA PROTECCIÓN DE DATOS EN EL MUNDO DE LA MULTICLOUD HÍBRIDA

La colaboración digital y su intercambio de datos inherente son una realidad en la empresa moderna conectada a la nube. La premisa tradicional de la confianza que se otorga a los empleados y contratistas debidamente acreditados que operan dentro del perímetro reforzado de la empresa se ha extendido a las arquitecturas modernas basadas en la nube. Los equipos que trabajan juntos para avanzar en los objetivos empresariales pueden compartir datos libremente a través de aplicaciones privadas en el entorno local, de multicloud y de nube híbrida. En la mayoría de los casos, tales datos se comparten en texto plano. La investigación sobre los datos en la nube muestra que solo el 9,4% de los datos de la nube están cifrados. Si dichos datos se exponen en Internet o se filtran de otro modo, la organización tiene poco o ningún medio para recuperarlos o eliminarlos. En los casos de robo, la ausencia general de cifrado implica que una vez que los datos son robados, no hay remedio posible.

Todas estas actividades se basan en compartir datos en un ecosistema de confianza débil que podría verse fortalecido por el cifrado. Desafortunadamente, es frecuente que el cifrado no se utilice debido a la compartimentación de tecnologías que protegen los datos en sus diversos estados y al aumento de la fricción para el usuario en ambos extremos de la transacción. Para empeorar las cosas, si un destinatario de los datos rompe la confianza y comparte los datos con otros (ya sea a propósito o por accidente), el propietario/custodio de los datos no tendrá conocimiento de la vulneración de la confianza a menos que la parte infractora se lo informe. Es necesario que los datos empresariales estén mejor protegidos y de manera más amplia a través de un conjunto integral de tecnologías altamente integradas. Esto ayudará a los propietarios/custodios de los datos a mantener el control y rastrear los datos durante todo su ciclo de vida.

## El cubo de McCumber y las tres dimensiones del riesgo

En 1991, John McCumber lanzó un modelo de riesgo de ciberseguridad ahora conocido como el cubo de McCumber. Este modelo fue revolucionario por la forma en que describía los factores de riesgo de ciberseguridad como un cubo tridimensional. Cada una de las caras visibles del cubo tiene tres aspectos diferentes del riesgo cibernético que deben gestionarse. Cada una de las intersecciones tridimensionales representa la unión de tres componentes, uno de cada cara. El minicubo más al frente, delineado en rojo, es la intersección de la confidencialidad, la tecnología y el procesamiento. Esto representa la idea de un control tecnológico para proteger la privacidad de los datos en el procesamiento.

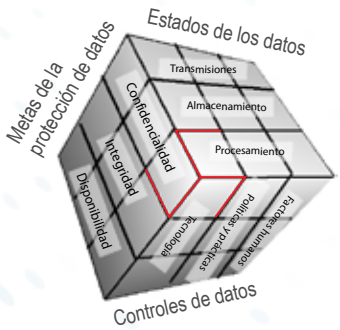


*Figura 1: Cubo de McCumber*

Este documento analizará cómo la implementación adecuada del cifrado en cada etapa del ciclo de vida, la transmisión, el almacenamiento y el procesamiento de los datos puede crear controles más avanzados que mejoren la protección y la privacidad. En la era de la colaboración y el intercambio de datos digitales, estos controles reducen el riesgo de exposición, fuga, pérdida y robo de los datos. Este documento se centra en el concepto de ofrecer confidencialidad a través de nuevos controles de cifrado y cómo los controles de datos afectan y se ven afectados por el uso del cifrado en todo lugar durante el ciclo de vida de los datos.

# CIFRADO DE DATOS EN LA TRANSMISIÓN

## La intersección de la confidencialidad, la tecnología y la transmisión

La implementación adecuada del cifrado puede reducir significativamente las pérdidas por el robo de datos. En el cubo de McCumber, la intersección de la tecnología, la confidencialidad y la transmisión se ha abordado mediante el uso del protocolo Transport Layer Security (TLS) y su predecesor, Secure Sockets Layer (SSL). A finales de 2019, la protección de los datos durante la transmisión a través de Internet había mejorado enormemente, con el cifrado de casi el 95% del tráfico centrado en los sitios web.

Existen ventajas y desventajas de utilizar el cifrado basado en el transporte en todo el entorno interno. El principal beneficio para quienes poseen los datos es el mayor nivel de confidencialidad que brinda al transferir datos con fines empresariales legítimos. El principal problema para quienes poseen los datos es el mayor nivel de confidencialidad que el cifrado aporta a los infiltrados cuando trasladan datos robados. Con frecuencia, quien supervisa la seguridad es incapaz de ver lo que hay en el tráfico, o debe invertir en herramientas de proxy de puerta de enlace para interceptar el tráfico con un ataque de "man in the middle" autorizado para ver lo que hay. Este tipo de inspección también puede agregar latencia a las aplicaciones, creando otros problemas y haciendo que la elección de utilizar el cifrado basado en el transporte sea difícil y, a menudo, costosa.

Crear e implementar los estándares de cifrado de transporte de datos para SSL y TLS en todos los navegadores es logísticamente más fácil que la creación y la aplicación de políticas internacionales y el intercambio de claves. Sin embargo, el cifrado crea una falsa sensación de seguridad para muchos usuarios de Internet. Creen que los datos transportados están seguros porque están cifrados, pero una vez que los datos pasan de la transmisión al procesamiento o almacenamiento, la seguridad del transporte TLS se disuelve y los datos son más susceptibles a los ataques.

También es interesante observar que, incluso antes del auge del cifrado de transporte, el número de ataques exitosos al cifrado de transporte era bajo, y el número de registros robados de los datos en reposo era alto. Robar datos sobre la marcha es una tarea más compleja que requiere una configuración más técnica y precisión, especialmente a la hora de robar datos específicos, que la configuración técnica para robar datos en reposo.

# CIFRADO DE DATOS EN REPOSO/ALMACENAMIENTO

## La intersección de la confidencialidad, el almacenamiento y la tecnología

Los datos en reposo son, con mucho, el mayor objetivo de los ladrones. Aunque las cifras varían considerablemente según la organización que las informa, las prestigiosas cifras de Risk Based Security identifican más de cuatro mil millones de registros en 2016, más de siete mil millones de registros en 2017, más de cinco mil millones de registros en 2018 y poco menos de ocho mil millones de registros vulnerados en 2019. El informe de amenazas de los datos de 2019 de Thales Security estimó que menos del 30% de las organizaciones implementan cifrado en entornos críticos, y la cantidad de datos cifrados no supera un solo dígito.

Históricamente, los sistemas de cifrado han resultado ser costosos y difíciles de instalar, configurar, operar y mantener. Los usuarios empresariales que interactúan con los datos critican la fricción que trae a su trabajo y los impactos negativos en el rendimiento, incluso hasta el punto de causar fallos/pérdidas en las solicitudes. Por lo tanto, en la batalla de la usabilidad contra la seguridad, la usabilidad sigue ganando.

En el caso del almacenamiento, la conquista de estos problemas requiere abordar la usabilidad subyacente del sistema de cifrado mediante el enfoque en la gestión de claves de cifrado. La usabilidad de las herramientas de cifrado de datos para eliminar la fricción de los clientes de datos, ya sean empleados internos o clientes externos, también es importante.

# CIFRADO DE DATOS EN USO Y PROCESAMIENTO

## La intersección de la confidencialidad, el procesamiento y la tecnología

El modelo de cubo de McCumber identifica el procesamiento de los datos, que puede aplicarse al procesamiento automatizado dentro de un sistema informático o al manejo manual de los datos antes o después de su digitalización.

### Cifrado de datos en el procesamiento

Proteger los datos a medida que fluyen a través de una aplicación es probablemente el aspecto más difícil del control de riesgos de los datos. La primera puerta de control es el aprovisionamiento de acceso normal. Si alguien no tiene acceso a la puerta de entrada de la aplicación, acceder a los datos es mucho más difícil. Más allá de eso, el enfoque del control se centra más a menudo en la protección física de los servidores o el reforzamiento de los componentes electrónicos que componen el sistema. Los ataques a los datos en procesamiento requieren acceso directo al sistema para realizar sondeos, acceso directo a los datos que se están operando o malware insertado en la aplicación o controladores del sistema para canalizar los datos mientras la aplicación está en funcionamiento.

### Cifrado de datos en uso

Dependiendo de cómo esté estructurado el procesamiento, es posible que sea necesario agregar controles para la defensa contra las personas que desvían los datos durante su manejo/procesamiento. Se debe tener precaución para garantizar que los datos correctos lleguen a la persona adecuada. Tradicionalmente, aquí es donde más se ha implementado el cifrado. En tanto solo se incluyeron a las personas adecuadas en el círculo de confianza, el propietario o el custodio de los datos podía estar seguros de que los datos estaban seguros. Sin embargo, hasta hace poco, la limitación crucial era que una vez que los datos dejaban de estar en posesión del propietario o el custodio, aún era posible que alguien descifrara la información y la reenviara a otra persona sin el conocimiento del propietario/custodio de los datos.

### Defensa contra los ataques de uso y procesamiento

Si bien el antimalware es útil para enfrentar el malware utilizado en los ataques, los bloqueos y los guardias de seguridad sirven más para mantener a las personas alejadas de los sistemas de procesamiento. El cifrado puede aplicarse al procesamiento e incluso a algunas áreas de uso para limitar la exposición de los datos durante el procesamiento. Existen proyectos de investigación en curso, como aquellos con cifrado homomórfico, que exploran cómo se puede extraer información de consultas relevantes de los datos cifrados sin revelar los datos en sí. Son prometedores, pero lo más probable es que falten años para su uso comercial.

Recientemente, las capacidades de cifrado evolucionaron para vincular derechos de forma persistente con los datos a lo largo de todo su ciclo de vida. Este es un gran avance que les permite al propietario de los datos agregar, cambiar o revocar permisos de uso a cualquier usuario, incluso después de que los datos se hayan compartido.

## REDUZCA LOS RIESGOS MEDIANTE EL CIFRADO EN TODO LUGAR

### Protección de los datos y privacidad en todas las ubicaciones y estados de los datos

En 2018, las pérdidas causadas por los robos de identidad se estimaron en 1700 millones de dólares solo en los EE. UU. La Comisión sobre el Robo de la Propiedad Intelectual Estadounidense estima que los robos de propiedad intelectual de empresas estadounidenses por parte de China cuestan unos 600 mil millones de dólares anuales. Para evitar estas pérdidas y obtener la promesa de una verdadera protección a lo largo del ciclo de vida de los datos, se requiere un cambio de enfoque fundamental. Hasta hace poco, una vez que los datos se entregaban al objetivo, estos dejaban de estar bajo el control del custodio original de los datos. Se otorgaba plena confianza a la siguiente persona en la cadena de posesión de datos. Si dicha persona decidía ampliar aún más el círculo de confianza, no tenía que obtener el permiso del propietario original.

Los custodios de los datos tienen el mandato de compartir solo la información requerida, a menudo tomando decisiones sobre lo que se requiere mientras los aspectos de los requisitos aún son variables. Esto los pone en una situación precaria. Lo que se aprobó para compartir internamente en el pasado, puede determinarse que está fuera del alcance más adelante. En el contexto actual de los datos compartidos, con o sin cifrado, proteger la organización mediante la implementación de una política modificada y recuperar los datos ya fuera de alcance es algo cuya anulación requiere un esfuerzo significativo. En la mayoría de los casos, es imposible verificar que todas las copias internas hayan sido devueltas o destruidas. Incluso sin intención malintencionada, las copias de datos compartidos pueden haber quedado capturadas en repositorios alternativos, como copias de seguridad, correos electrónicos, carpetas compartidas y unidades personales. El concepto de cifrado en todo lugar resuelve este problema al mantener la protección y la privacidad de los datos en toda la empresa, ya sea en reposo, en vuelo, en almacenamiento o en la nube.

## *La intersección de la confidencialidad, las políticas y los procesos, y el factor humano*

Las políticas y los procesos son los elementos fundamentales de cualquier sistema de cifrado sólido. La política dicta qué se puede y qué no se puede compartir, así como quiénes forman parte del círculo de confianza para cada elemento de datos protegido. Desafortunadamente para los sistemas de cifrado tradicionales, las políticas se basan más a menudo en un nivel de confianza según el cual los seres humanos seguirán las políticas prescritas para garantizar que los datos permanezcan donde y con quien pertenecen. Si los factores humanos cometen un error, pueden ocurrir fugas y exposición de los datos.

Sin importa cuán irrompible sea un algoritmo de cifrado y qué tan bien estén documentadas las políticas, si una persona decide operar intencionalmente fuera de ellas o comete un error, los datos protegidos corren riesgo. En la mayoría de los casos esto es simplemente una molestia, pero en otros puede ser devastador, causando enormes impactos financieros y de reputación. El robo de propiedad intelectual en American Semiconductor es un excelente ejemplo del daño que las organizaciones pueden sufrir. El precio de las acciones de American Semiconductor cayó casi un 50% después de que se descubrió el robo.

El primer paso para proteger los datos de los factores humanos es reducir la cantidad de seres humanos que pueden revelar o compartir los datos desprotegidos. El propietario de los datos siempre puede conservar el control de los derechos de los datos y mantener ese control aparte de cualquier mecanismo de entrega o entornos de uso compartido. Esto crea dos controles que pueden evitar una liberación de datos no deseada.

El concepto de cifrado en todo lugar requiere un control proactivo de los datos a lo largo de su ciclo de vida. La protección de datos debe transformarse en políticas aplicables que creen un sistema de cifrado integrado en los datos. Si las políticas se aplican a los datos antes de la distribución interna y se adhieren a dichos datos a medida que se trasladan, los propietarios de los datos pueden estar seguros de que los derechos que definieron en los datos permanecerán con ellos en cualquier estado en el que se encuentren. El propietario también debe definir el período de validez de los derechos antes de que se requiera una nueva comprobación del servidor de control, manteniendo así un control constante sobre quién puede acceder a los datos compartidos sin importar a dónde viajen los datos dentro de la empresa. Luego se utiliza la tecnología para supervisar y aplicar políticas a lo largo del ciclo de vida de los datos. Esto proporciona una protección persistente que cumple con las demandas cambiantes de la empresa, desde cambios en el personal y socios comerciales hasta otros requisitos operacionales.

Los permisos asignados son válidos y se mantienen residentes y protegidos dentro de datos no estructurados. Cuando se intenta acceder a los datos, se envía una solicitud al sistema de gestión de claves dentro del entorno del propietario de los datos. Si el solicitante tiene los derechos correspondientes asignados, se envía un token temporal para desbloquear la información y permitir que se ejerzan los derechos. En los datos estructurados, los datos se pueden proteger a nivel de atributo o tabla. Los datos mantenidos en la ubicación del destinatario permanecen bajo el control del propietario/custodio de los datos todo el tiempo. Si en algún momento el propietario de los datos determina que los parámetros de acceso deben cambiar o ser revocados por completo, todo lo que debe hacer es cambiar la política y esta se aplicará a las copias remotas de los datos.

## *Aplicación de políticas adaptativas para la protección vitalicia de los datos*

En cualquier momento en el que termine la relación de uso compartido o el propietario de los datos determine que los derechos requieren un cambio, es posible actualizar los derechos en el motor de políticas. Los permisos actualizados se aplican en la siguiente solicitud de comprobación de derechos. Los permisos actualizados se aplican a las copias que se crearon antes de acceder a ellas. Si se aplica la revocación completa, las claves se destruyen y los datos cifrados quedan inertes. Dado que el destinatario no tiene acceso a las claves, los datos permanecen seguros contra el uso no autorizado.

## PROTECCIÓN DE DATOS CON CIFRADO EN TODO LUGAR

Una política aplicada por la tecnología, derechos persistentes de los datos, un sistema de gestión de claves robusto y un conjunto de cifrado sólido crean una base sólida para una defensa exhaustiva. Lo que hace que el cifrado en todo lugar sea único en concepto y aplicación es la aplicación persistente de políticas al crear una protección continua en los centros de datos y la nube para mantener el control de los datos elegibles, a los que se puede acceder a través de una conexión JDBC. Para que el concepto de cifrado en todo lugar sea una realidad funcional, los propietarios de los datos deben aprovechar un ecosistema tecnológico y no solo soluciones puntuales. Hoy en día, las soluciones puntuales son buenas en lo que hacen, pero no están diseñadas para un cifrado completo en todo el ecosistema. Las integraciones amplias no están donde deben estar. Por lo tanto, lograr una protección integral de los datos requiere integraciones compactas con alta interoperabilidad como objetivo de diseño. Con esto, los datos pueden estar protegidos en cada fase de su existencia.

## CASOS DE USO DEL CIFRADO EN TODO LUGAR

Los casos de uso enumerados identifican una combinación de componentes de IBM y ajenos a IBM que se pueden usar para ofrecer privacidad y protección continua de los datos. Si bien todas las fases del concepto de cifrado en todo lugar se pueden lograr utilizando otras soluciones de proveedores, IBM es el único proveedor que actualmente ofrece un ecosistema de soluciones estrechamente integrado en IBM Z para ofrecer privacidad y protección continua de los datos elegibles. Los siguientes son componentes utilizados en los casos de uso:

1. IBM z15 que ejecuta z/OS o bien Linux en Z con capacidades de cifrado integral
2. IBM Data Privacy Passports
3. Adaptadores Fibre Channel de IBM Z
4. Almacenamiento IBM DS8900F
5. IBM Z Fibre Channel Endpoint Security
6. IBM Hyper Protect Virtual Servers
7. TLS o IPSec
8. Su elección de nube(s) pública(s) o privada(s)
9. IBM Data Privacy for Diagnostics (vendedores y proveedores)
10. Un módulo de seguridad de hardware (HSM)
11. Hardware básico para el procesamiento y almacenamiento de datos

### Caso de uso 1: Privacidad y protección de los datos dentro de la familia de soluciones locales de IBM

Para muchos entornos exigentes, como el comercio minorista de gran volumen, los grandes bancos, el procesamiento de tarjetas de crédito y otros pagos a escala, lo más probable es que ya exista una infraestructura de procesamiento de IBM y el z15 sea una tecnología fundamental. En z15, es posible habilitar el cifrado integral para proteger el procesamiento y los datos elegibles dentro del sistema. La privacidad y la protección de los datos elegibles pueden ampliarse desde los entornos IBM z15 al resto de la empresa con los controles de políticas adecuados de Data Privacy Passports.[1] Es posible instalar un controlador de pasaportes en IBM Data Privacy Passports para mantener y gestionar derechos y comprobaciones de derechos para datos elegibles de fuentes de datos a los que se puede acceder a través de una conexión JDBC. Con los datos elegibles bajo la protección del cifrado integral, el enfoque puede pasar a la protección de los datos que deben fluir dentro y fuera del sistema.

Una vez que se habiliten las políticas, los datos no tienen que permanecer en IBM Z para recibir protección. Los datos asociados con las políticas se cifran antes de abandonar su almacenamiento de host. Cuando se opera dentro del ecosistema completo de IBM, los adaptadores y conmutadores de IBM Fibre Channel con rendimiento ultra alto se pueden usar para mover datos muy rápidamente dentro del centro de datos. Estos son compatibles con otros sistemas interconectados de Fibre Channel, pero si se usan con el almacenamiento IBM DS8900F, las protecciones se pueden aumentar al agregar IBM Fiber Channel Endpoint Security, que protege los datos en tránsito a nivel de hardware. La combinación de Fibre Channel y DS8900F también agrega cifrado y autenticación para los datos en vuelo.

1 Exención de responsabilidad: Data Privacy Passports soporta fuentes de datos a las que se puede acceder a través de una conexión JDBC.

## Caso de uso 2: Privacidad y protección de los datos en centros de datos empresariales heterogéneos

La mayoría de las organizaciones con otras plataformas informáticas ya implementadas no están en condiciones de extraer y reemplazar por completo su infraestructura informática actual. Data Privacy Passports está diseñado para proteger de manera sólida los datos críticos y confidenciales que residen en prácticamente cualquier hardware conectado a la red en esos centros de datos. Una vez que se realice la conexión a IBM z15, la protección de los datos elegibles se puede aplicar en cualquier lugar del centro de datos durante la existencia de los datos. IBM z15 está diseñado con la seguridad del HSM criptográfico FIPS 140-2 de nivel 4. También está diseñado para la velocidad y es capaz de procesar más de 19 mil millones de transacciones cifradas por día.[2]

## Caso de uso 3: Privacidad y protección de los datos en cualquier nube y en los datos compartidos

IBM z15 con Linux en Z ofrece IBM Hyper Protect Virtual Servers para crear una infraestructura segura de nube privada. Con Hyper Protect Virtual Servers, los propietarios de cargas de trabajo mantienen un control completo sobre los datos y las cargas de trabajo. Ni siquiera los administradores del sistema o de la nube tienen acceso a las cargas de trabajo a menos que el propietario de los datos lo permita. Es posible aplicar Data Privacy Passports a los datos elegibles incluso en entornos hiperconvergentes y multicloud altamente distribuidos, siempre que dicha nube tenga acceso al controlador de pasaportes que aplica las políticas. Los túneles TLS se pueden agregar en las puertas de enlace de Internet para aumentar la seguridad de transporte donde los puntos finales de comunicación deben ocultarse de la vista de Internet.

Con los controles de datos establecidos, cualquier propietario de los datos puede compartirlos con cualquier persona en toda la empresa. Independientemente de las necesidades de la empresa, el acceso a los datos, la distribución y la caducidad dentro de la empresa están bajo el control total del administrador de políticas. Los propietarios de los datos pueden tener la seguridad de que cuando cambien las necesidades, la política podrá cambiarse fácilmente para adaptarse a dichas necesidades. Cuando la necesidad ya no exista, tanto la protección como la privacidad pueden permanecer intactas. Los datos elegibles en cualquier ubicación dentro de la empresa pueden quedar inertes al destruir las claves locales a través de la gestión de políticas mediante el uso de Data Privacy Passports.

## Caso de uso 4: Minimización de los impactos de la TI paralela

La TI paralela tiene lugar cuando alguien en la organización decide mover o copiar los datos a una ubicación no autorizada. Moverlos o copiarlos sin permiso crea brechas de seguridad y aumenta los riesgos empresariales. Si se producen fugas o exposición de los datos, incluso por accidente, se pueden incurrir en graves consecuencias financieras y de reputación. La implementación de Data Privacy Passports en todos los datos estructurados críticos o confidenciales minimiza en gran medida el impacto de la TI paralela. Incluso si los datos se copian y se mueven, siguen siendo inútiles sin los permisos correspondientes. Si alguien con acceso a una base de datos controlada pero sin permisos de acceso a los datos los mueve a una ubicación no autorizada, los datos permanecen cifrados, minimizando la exposición de la empresa.

2 Exención de responsabilidad: Esta velocidad de transacción se basa en mediciones internas de una configuración z15 que consta de dos LPAR de 8 vías y un ICF de 4 vías que se ejecuta con cifrado de conjunto de datos y cifrado CF habilitado. Con estos resultados, se proyectaron las velocidades de transacción de tamaño completo de z15 utilizando LSPR MIPS estándar. El rendimiento que puede experimentar cualquier usuario puede variar.

## RESUMEN: PROTEJA LOS DATOS A LO LARGO DE SU CICLO DE VIDA CON EL CIFRADO EN TODO LUGAR

Mantener la confidencialidad de los datos proporciona a los propietarios ventajas empresariales y operativas. A pesar de este hecho, prácticamente todas las organizaciones subutilizan el cifrado para proteger sus datos y muchas son víctimas de actores de amenazas malintencionadas y personas descuidadas.

Dentro de una organización, el problema principal al proteger los datos es que las herramientas más populares y comunes requieren diferentes interfaces y políticas independientes para defender los datos en sus diferentes estados. Las herramientas y las interfaces de gestión funcionan de forma independiente, con solo algunas integraciones débiles. La independencia dificulta la cohesión total y las pruebas y la aplicación de las políticas, y a menudo deja brechas en la protección.

En entornos colaborativos, la fricción del usuario y la conservación del control de los datos son dos de los aspectos más difíciles. El aumento de la fricción del usuario aleja a las personas de las plataformas de cifrado tradicionales. La falta de flexibilidad en el control y la aplicación de políticas en los datos sobre el terreno hace que los propietarios y custodios de los datos sean reacios a implementar protecciones.

Si bien las tecnologías para proteger los datos en cada etapa del ciclo de vida son comunes, los cambios periódicos que experimentan los datos a lo largo de su ciclo de vida dificultan ciertos aspectos de la gestión del cifrado. Independientemente de los impedimentos, las empresas deben definir sus requisitos comerciales para proteger todos sus datos confidenciales en la transmisión, el procesamiento y el almacenamiento. Siempre deben realizarse análisis de costo/beneficio, pero una evaluación realista casi siempre mostrará que hay un beneficio en ampliar el uso del cifrado en los datos privados y confidenciales.

Esté preparado. En algunos casos, la transición a los almacenes de datos cifrados puede llevar años. Aunque la cantidad de datos es un factor, no es el más impactante. Los requisitos más difíciles de incorporar implican catalogar y definir el tipo de datos y la diversidad de ubicaciones, los derechos de los usuarios y las aplicaciones, y las interfaces de las aplicaciones para la interacción y el intercambio de datos. Las aplicaciones heredadas necesitan una actualización o reemplazo para funcionar con el cifrado, pero si los datos brindan una verdadera ventaja empresarial u operativa y, por lo tanto, vale la pena conservarlos, entonces también vale la pena protegerlos.

Para las organizaciones con datos altamente confidenciales o sistemas transaccionales de alto volumen, ejecutar IBM z15 con z/OS o Linux en Z con cifrado integral y Data Privacy Passports debería ser una consideración primordial. El ecosistema IBM z15 proporciona un rendimiento incomparable para aplicaciones internas o como la base para cualquier tipo de entorno de nube que se esté construyendo. Su arquitectura de seguridad nativa incluye chips de aceleración de cifrado integrados, chips y servicios de módulos de seguridad de hardware integrados, servicios de creación y gestión del ciclo de vida de las claves de cifrado, interfaces cifradas de varios Gbps y almacenamiento de alta velocidad compatible con cifrado. La plataforma ofrece confidencialidad persistente de los datos y gestión y aplicación de políticas que respaldan cualquier requisito de cifrado. Actualmente, no hay disponible un sistema de producción en masa más completo y eficiente.

Independientemente de las soluciones elegidas, la implementación de una estrategia de cifrado en todo lugar reduce significativamente los costos de las vulneraciones relacionadas con la privacidad y el cumplimiento. Si el propietario/custodio de los datos puede proporcionar pruebas razonables de que cualquier dato se filtró, fue robado o quedó de alguna manera comprometido, la notificación, el análisis forense, la reparación a las víctimas y las multas se reducen significativamente y, a veces, se eliminan. El impacto negativo a la marca también puede reducirse/eliminarse significativamente. La reducción de estos factores ayuda a disminuir las repercusiones en los beneficios finales.

Para obtener más información sobre cómo su organización puede beneficiarse del enfoque de IBM para un ecosistema completo de cifrado de datos utilizando IBM z15 con cifrado integral y Data Privacy Passports, visite: https://www.ibm.com/it-infrastructure/z/capabilities/enterprise-security.

## Acerca de Enterprise Management Associates, Inc.

Fundada en 1996, Enterprise Management Associates® (EMA) es una firma líder de analistas de la industria que brinda una visión profunda de todo el espectro de tecnologías de TI y de gestión de datos. Los analistas de EMA aprovechan una combinación única de experiencia práctica, comprensión de las mejores prácticas de la industria y un profundo conocimiento de las soluciones actuales y planificadas de los proveedores para ayudar a los clientes de EMA a alcanzar sus objetivos. Obtenga más información sobre los servicios de investigación, análisis y consultoría de EMA para la línea empresarial de usuarios corporativos, profesionales de TI y proveedores de TI en www.enterprisemanagement.com o bien blog.enterprisemanagement.com. También puede seguir a EMA en Twitter, Facebook o LinkedIn.

---



**Sede central corporativa**:
1995 North 57th Court, Suite 120
Boulder, CO 80301
**Teléfono**: +1 303.543.9500
www.enterprisemanagement.com

3933.03022020-06032020.revision9