

RESUMEN DE LA SOLUCIÓN

Cumplimiento del Reglamento DORA con Confianza

La solución de Pure Storage y Commvault ayuda a las instituciones a cumplir con los requisitos más estrictos del reglamento DORA.

Las entidades financieras han dedicado mucho tiempo y recursos a diseñar y desarrollar infraestructuras de detección, prevención y mitigación de los sucesos imprevistos que pueden suponer un riesgo. Sin embargo, la interconexión del sector financiero global, la frecuencia y la gravedad de las ciberamenazas y la sofisticación de los agentes malintencionados siguen aumentando por momentos. Estos sucesos nefastos suponen un riesgo que ya no se limita a las entidades individuales, sino que afecta a todo el sector financiero y pone en peligro a todos los sectores adyacentes. El cambio de mentalidad del “sí” al “cuando” se ha generalizado y ha hecho que los organismos regulatorios de todo el mundo introduzcan unas directrices y mandatos estrictos, diseñados para garantizar la resiliencia cibernética y operativa, con el fin de proteger la integridad del sector financiero. Algunas de estas normativas son el Reglamento sobre la resiliencia operativa digital (DORA, por sus siglas en inglés) de la UE, la Directiva NIS 2 y la norma APRA CPS 230.

Resumen de la situación

Los mandatos y las directrices de estas normativas son muy amplios y para algunas empresas resultan ambiguos, lo que lleva a un ciclo constante de formación, modernización de la infraestructura e inversión estratégica, con el fin de prepararse para afrontar las amenazas inminentes y para demostrar la ciberresiliencia y el cumplimiento de las mejores prácticas operativas. El Reglamento DORA introduce un marco detallado para garantizar que las entidades financieras, en especial los bancos globales, y sus proveedores externos no solo están preparados para los acontecimientos imprevistos, sino que también son capaces de recuperarse rápidamente en caso de que se produzcan. A medida que la sofisticación de las amenazas aumenta, los mandatos de DORA se han ido haciendo más urgentes. Una sola disrupción no prevista en las aplicaciones y los datos críticos para la empresa puede desestabilizar el funcionamiento de ésta y la red de instituciones que dependen de ella, y producir unos daños potencialmente irreparables en la reputación de la compañía y en la estabilidad financiera a escala global.

DORA constituye un imperativo estratégico en un mundo en el que la resiliencia operativa es una necesidad para proteger la viabilidad de un sector financiero y una economía global muy interdependientes. Las empresas que consigan cumplir y superar los requisitos del Reglamento DORA no solo evitarán las sanciones administrativas y/o penales, sino que también lograrán una importante ventaja competitiva. En cambio, aquellas que no los cumplan correrán un grave riesgo de sufrir unos ciberataques y disrupciones que podrían paralizar e incluso provocar la desaparición de su negocio.

Protección y prevención

- Basada en los principios de confianza cero con autenticación avanzada, cifrado y bloqueos de cumplimiento de normativas.
- Capas de inmutabilidad, incluidos los snapshots SafeMode™, que proporcionan capacidad de recuperación y protección frente a las ciberamenazas.

Detección

- Descubra y corrija los riesgos y detecte las amenazas con el escaneado de riesgos, la detección de anomalías asistida por IA y la tecnología de señuelo cibernético.
- Las alertas tempranas de Commvault permiten que las organizaciones coordinen la respuesta y aceleren la recuperación.

Respuesta y recuperación

- Cumpla los estrictos objetivos de tiempo de recuperación exigidos por las regulaciones con unos snapshots basados en el almacenamiento.
- Commvault se integra con Pure Storage para proporcionar una recuperación rápida de los sistemas de misión crítica a partir de los snapshots inmutables.

Pruebas de resiliencia

- Cumpla las exigencias en materia de pruebas de resiliencia operativa con unas pruebas de recuperación cibernética automatizadas y continuas.

Nos estamos acercando rápidamente a la importante fecha límite del 17 de enero de 2025, que es cuando entrará plenamente en vigor la obligación de cumplir con los mandatos del Reglamento DORA, y la Autoridad Europea de Supervisión ya ha realizado varios simulacros para evaluar la preparación de algunas entidades financieras seleccionadas. Más de 22 000 entidades financieras y proveedores de servicios TIC que operan en la UE estarán sujetos al Reglamento DORA. Solo las empresas que se preparen e implementen las soluciones tecnológicas y operativas adecuadas podrán salir adelante en este estricto entorno regulatorio.

La colaboración de Pure Storage y Commvault

Pure Storage y Commvault llevan años colaborando para proporcionar unas soluciones únicas y diferenciadas que resuelven los retos del mundo real en materia de protección, gestión y recuperación de todo tipo de datos. La combinación del software de ciberresiliencia líder en el sector de Commvault y de la plataforma segura y de alto rendimiento de Pure Storage permite que las organizaciones protejan sus datos y aplicaciones de misión crítica y presten unos servicios ininterrumpidos a sus clientes y empleados, a pesar del aumento de la frecuencia y la complejidad del ransomware y otras amenazas.

Si eligen a Commvault y Pure Storage, las compañías financieras pueden sacar el máximo partido de sus datos, impulsar la excelencia operativa, resolver el cumplimiento de sus obligaciones y lograr una ventaja competitiva.

La solución de cumplimiento del Reglamento DORA

Dada la profundidad y amplitud de los requisitos relacionados con DORA y los diversos sistemas y soluciones que las instituciones financieras puedan tener ya instalados, la solución de Pure Storage y Commvault se diseñó desde el principio para ser modular. Una vez que los clientes han implementado los componentes básicos, pueden elegir qué funcionalidades adicionales necesitan. Con este enfoque no solo se protegen los datos, sino que, si se vulneran los sistemas, las aplicaciones y los servicios pueden restaurarse en el menor plazo de tiempo posible.

La solución de Pure Storage y Commvault ayuda a los clientes a recuperarse de los ciberataques con confianza

BENEFICIOS	DETALLES DE LA SOLUCIÓN
Almacén ciberresiliente Este almacén aislado lógicamente sirve de base de la solución. Proporciona un repositorio aislado e inmutable que protege los datos críticos. La conectividad con el almacén se controla desde dentro del propio almacén y cuando no está en uso, la comunicación con el almacén se desactiva.	Almacén ciberresiliente - Replicación segura de Commvault en una red aislada gestionada - Copias de datos inmutables de Pure Storage con SafeMode - Comprobación de la integridad de los datos con Threat Scan de Commvault
Entornos de recuperación aislados Estas zonas son áreas aisladas completamente autónomas, en las que los datos pueden restaurarse para realizar análisis forenses y de las aplicaciones, con el fin de validar que dichos datos están limpios antes de volver a la producción y para probar continuamente las prácticas de recuperación cibernética para asegurar la preparación organizativa.	Entornos de recuperación aislados - Zonas de validación para los equipos de respuesta a incidentes y de aplicaciones - Zona de recuperación tras desastres para restablecer el servicio - Zona aislada localmente con el software de Commvault y FlashBlade™ y FlashArray™ de Pure Storage o instancias aisladas bajo demanda usando Commvault Cleanroom
Recuperación rápida del Nivel 1 Si se produce un incidente cibernético, conservar las pruebas debe ser la prioridad número uno del equipo de respuesta a incidentes, pero la restauración rápida del servicio en las aplicaciones de Nivel 1 también es igual de importante. Por eso, la restauración en un sitio secundario, ya sea en las propias instalaciones o en la nube, es sumamente importante.	Restauración rápida de la producción - Recuperación operativa mejorada con Pure Storage - Inmutabilidad de las copias de seguridad primarias con los snapshots SafeMode - Transferencia de datos mejorada al almacén ciberresiliente
Recuperación con RTO extremadamente corto del Nivel 0 de misión crítica En los sistemas críticos (como los pagos), la única manera de cumplir los objetivos de tiempo de recuperación más estrictos que las normativas en materia de resiliencia operativa exigen es recuperar usando snapshots (instantáneas) basadas en el almacenamiento.	Recuperación con snapshots inmutables - Snapshots de FlashArray de Pure Storage en el almacenamiento primario para un RTO extremadamente corto - Coherencia de la aplicación con Commvault IntelliSnap - Replicación segura y eficiente en el almacén ciberresiliente



Los resultados de la solución

La solución de cumplimiento del Reglamento DORA de Pure Storage y Commvault ayuda a las organizaciones a ser más ciberresilientes y a cumplir dos grandes categorías de normas técnicas definidas por DORA.

La gestión del riesgo de las TIC

La solución conjunta descrita en este documento ayuda a identificar, gestionar y reducir el riesgo en el ámbito de las tecnologías de la información y las comunicaciones (TIC). Esto incluye la ayuda para cumplir los artículos siguientes del **Capítulo II del Reglamento DORA**:

- **Artículo 8—Identificación:** la solución proporciona a las entidades financieras la capacidad de identificar y clasificar fácilmente los datos sensibles y en riesgo.
- **Artículo 9—Protección y prevención:** la solución se basa en los principios de confianza cero con controles de seguridad MFA, MPA, PAM, SAML, RBAC y granulares. Proporciona unas copias de datos cifradas e inmutables para la seguridad y protección de los datos y, al mismo tiempo, ayuda a prevenir las fugas de datos.
- **Artículo 10—Detección:** la solución proporciona una detección de amenazas proactiva asistida por IA que reconoce y avisa de las conductas anómalas. También contiene unas funcionalidades de búsqueda activa de amenazas mediante dispositivos señuelo, para identificar aún más las conductas sospechosas.
- **Artículo 11—Respuesta y recuperación:** la solución permite una recuperación probada, rápida y flexible de los datos limpios e incluye la capacidad de pasar a entornos de recuperación aislados y espacios limpios (cleanrooms), como parte de las pruebas de preparación.
- **Artículo 12—Políticas y procedimientos de respaldo y procedimientos y métodos de restablecimiento y recuperación:** la solución ofrece una copia de seguridad de los datos completa e inmejorable, con opciones de configuración flexibles, aplicación automática de políticas, la capacidad de cumplir varios objetivos RTO y RPO, comprobaciones de integridad incorporadas y la capacidad de probar los sistemas de forma fácil y frecuente en entornos aislados o espacios limpios.

Las pruebas de resiliencia operativa digital

La solución también ayuda a cumplir los requisitos de resiliencia que se describen en los **artículos 24-26 del Capítulo IV**, relacionados con las pruebas de resiliencia operativa digital. Para cumplir estos requisitos, Commvault y Pure Storage proporcionan unas pruebas automatizadas y continuas de la recuperación cibernética, para que las organizaciones puedan mejorar sus procedimientos de recuperación y su preparación para las vulneraciones y las interrupciones. Tanto si las pruebas se realizan bajo demanda en inquilinos aislados en la nube mediante la solución Cleanroom Recovery de Commvault como si se efectúan dentro de entornos de recuperación aislados con el software de Commvault y los sistemas FlashArray o FlashBlade® de Pure Storage, las organizaciones pueden proporcionar una recuperación rápida y sin problemas de los datos limpios en entornos aislados.

La resiliencia operativa global

Los principios de resiliencia operativa inicialmente se centraron en el cumplimiento del Reglamento DORA que próximamente será aplicable al sector financiero europeo, pero son de aplicación universal a todos los sectores. Los gobiernos de todo el mundo reconocen esta importancia y están desarrollando o implementando de forma activa estas normativas, con vistas a garantizar la continuidad operativa y la resiliencia en los sectores críticos, como la sanidad, las comunicaciones, la energía y otros.

Commvault y Pure Storage se comprometen a proporcionar una solución globalmente escalable que permita que las organizaciones logren la resiliencia operativa digital. Gracias a la combinación de nuestra experiencia en la gestión de los datos, una tecnología de plataforma de datos innovadora y un profundo conocimiento de la infraestructura, ofrecemos un enfoque completo de la protección, la recuperación y la optimización del valor de los datos, a pesar de las interrupciones.

Recursos adicionales

- Obtenga más información sobre [El fortalecimiento de la resiliencia operativa en los servicios financieros](#).
- Siga leyendo sobre [Las soluciones de preparación y recuperación cibernéticas de Commvault](#).
- Conozca mejor la [Colaboración entre Pure Storage y Commvault](#).