PURESTORAGE®
Uncomplicate Data Storage, Forever

WHITE PAPER

El fortalecimiento de la resiliencia operativa en los servicios financieros

Soluciones para abordar las nuevas normativas sobre riesgos

Índice

"El 90 % de los profesionales de la resiliencia esperan que las amenazas para sus organizaciones aumenten en los próximos tres años".

THE CONFERENCE BOARD, AGOSTO DE 2023[1]

Introducción

Para las empresas de servicios financieros, la gestión del riesgo es una responsabilidad que aumenta constantemente y que evoluciona sin cesar. Desde la crisis financiera de 2007-2008, los ministros y los reguladores financieros de todo el mundo no han parado de elevar los estándares de la gestión del riesgo y han ido incluyendo cada vez más áreas en sus definiciones de las actividades cubiertas. Al mismo tiempo, la aparición de nuevas tecnologías y las novedades del mercado plantean retos adicionales que deben abordarse para garantizar la resiliencia operativa de una empresa.

Los reguladores y el mercado en general han acabado reconociendo que el hecho de que el ecosistema de servicios financieros sea cada vez más complejo, interconectado y expansivo exige que la gestión del riesgo vaya mucho más allá de las medidas puramente financieras para incluir todo la actividad y el ecosistema en el que se encuentra. Cada vez más, la gestión del riesgo en el siglo XXI engloba todos los aspectos de una actividad, con un énfasis particular en los datos y la tecnología, que constituyen la base de las empresas modernas. De cara al futuro, la resiliencia operativa es una frontera que una empresa debe gestionar y mantener con disciplina y diligencia, y no solo porque así lo exijan los reguladores. La resiliencia operativa puede aportar otras ventajas, desde demostrar a los clientes y a otras partes interesadas que la empresa (y sus inversiones) son seguras hasta diferenciarse de los competidores o garantizar la estabilidad de la empresa frente a las pérdidas, los fallos o la inestabilidad laboral. La resiliencia operativa es un ingrediente esencial de una empresa moderna.

La resiliencia operativa se refiere a la capacidad de las empresas, las infraestructuras de los mercados financieros (IMF) y el sector en su conjunto para mantener o recuperar su actividad y sus servicios ante las disrupciones, los desastres u otros riesgos operativos. En líneas generales, engloba las estrategias, los procesos y los sistemas que las entidades financieras adoptan para garantizar que pueden seguir prestando los servicios críticos a sus clientes, pase lo que pase. La resiliencia operativa ha ido adquiriendo una importancia cada vez mayor para las empresas de servicios financieros, ya que estas se enfrentan a unos riesgos crecientes, incluidos ciberataques, ransomware, desastres naturales y pandemias.

Contemplar este asunto complejo desde el punto de vista de los reguladores ofrece una perspectiva muy útil sobre la resiliencia operativa en los servicios financieros. Si partimos del estado actual de las normativas y analizamos las similitudes y las diferencias entre las regiones geográficas y dónde centran su atención los reguladores, podemos estudiar los retos y los enfoques para gestionar este tema difícil. Al final, obtendremos una imagen nítida de hacia dónde se dirige la cuestión de la resiliencia operativa.

Perspectivas globales de la resiliencia operativa para los servicios financieros

La resiliencia operativa como responsabilidad y función de gestión del riesgo es un fenómeno relativamente reciente. Si bien el campo relacionado de la continuidad operativa surgió en la década de 1970 (véase el recuadro lateral), la resiliencia operativa no empezó a tener relevancia hasta principios de 2017. Los reguladores de Europa, Singapur, Hong Kong, los Estados Unidos y otros países, como reacción a una epidemia de problemas de ciberseguridad y al auge del ransomware, reconocieron que la gestión del riesgo en la empresa tenía que ir más allá de los indicadores financieros para englobar todos los aspectos de la actividad, sobre todo porque las tecnologías de la información y las comunicaciones (TIC) se han convertido en la columna vertebral de la empresa moderna. Como es lógico, la ciberresiliencia ha sido un elemento central de estos esfuerzos; una preocupación cada vez más destacada en una constelación de cuestiones críticas, a medida que los reguladores y las empresas han reconocido las interconexiones y las concentraciones que han surgido, junto con el concepto de "demasiado grande para caer", tras las crisis financieras globales. En realidad, el aumento de la concentración y los mayores avances en las operaciones digitales lo que han hecho es aumentar lo que hay en juego.

Desde 2017, la resiliencia operativa ha seguido evolucionando de manera heterogénea, ya que cada jurisdicción le ha dado un sello propio a su regulación. Este enfoque y está adopción desiguales tienen su reflejo en las formas en las que las empresas privadas han abordado el reto y son un buen indicador de por dónde es probable que vayan las cosas en el futuro.

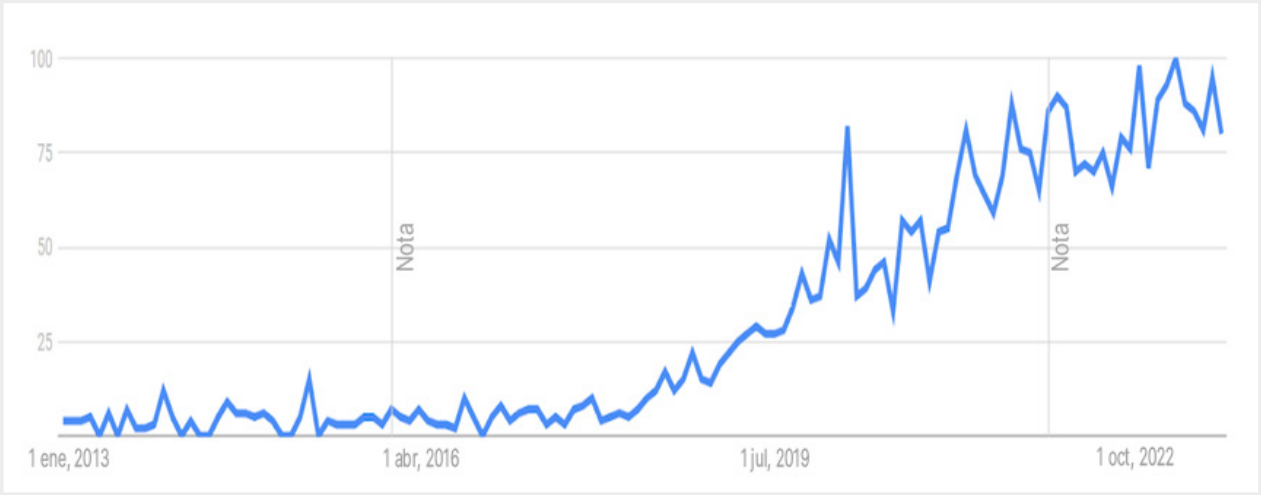

FIGURE 1 Fuente: Google Trends: Cuando el río suena, agua lleva: las búsquedas en Internet de la expresión "resiliencia operativa" aumentaron espectacularmente a principios de 2018.

En resumen, aunque la cuestión de la resiliencia operativa empezó a cobrar importancia para los reguladores de todo el mundo a mediados de la década de 2010, la manera de afrontarla es muy distinta de una región geográfica a otra y el ritmo de implementación también varía mucho. En concreto, la UE y el Reino Unido son líderes tanto por lo que se refiere al calendario de implementación como al nivel de obligatoriedad de las regulaciones, mientras que los Estados Unidos están siguiendo un enfoque más colaborativo e inconexo y en Asia Pacífico unos regímenes son estrictos y otros menos.

La UE y el Reino Unido

- La Unión Europea ha adoptado las regulaciones más exhaustivas y prescriptivas de la resiliencia operativa. El anteproyecto de Reglamento sobre la resiliencia operativa digital (DORA, por sus siglas en inglés) se publicó en septiembre de 2020 y está previsto que la normativa entre en vigor el 17 de enero de 2025. DORA se desarrolló a partir de los 12 principios para la resiliencia operativa (POR, por sus siglas en inglés), que se publicaron en 2021 y que se basaban en los Principios de Supervisión Bancaria del Comité de Basilea para la buena gestión del riesgo operativo (los PSMOR, por sus siglas en inglés), publicados originalmente en 2011 y revisados en 2014 y 2021.[2] DORA es un marco integral que unifica procesos y estándares en el sector financiero. Garantiza que todos los operadores del sistema financiero, incluidas las empresas de tecnofinanzas y los terceros prestatarios de servicios, están sujetos a un conjunto común de normas para mitigar los riesgos de las TIC en sus operaciones.

Los aspectos clave de DORA incluyen el establecimiento y el mantenimiento constante de unas políticas de seguridad, unos principios y marcos de gestión del riesgo, la sensibilización sólida y activa de los usuarios y unas auditorías y pruebas regulares de los procesos y los sistemas de seguridad. Por otro lado, aunque el reglamento DORA no establece multas y sanciones por escrito, los estados miembros de la UE pueden imponer condenas y sanciones penales, que pueden incluir multas de hasta un 2 % de la cifra de negocio global de una empresa.

Para más información sobre DORA, lea nuestro blog: Cómo se benefician los bancos del nuevo Reglamento sobre la resiliencia operativa digital

- El Reino Unido también se ha mostrado activo a la hora de desarrollar y adoptar directrices relativas a la resiliencia operativa y, de hecho, impuso una multa de casi 50 millones de libras en diciembre de 2022 por un incidente relacionado con la resiliencia operativa en un banco británico.[3] En respuesta a la mayor sensibilización respecto de las vulnerabilidades cibernéticas, la Autoridad de Conducta Financiera (FCA) del Reino Unido junto con el Banco de Inglaterra (BoE) y la Autoridad de Regulación Prudencial (PRA) promulgaron su propia normativa de resiliencia operativa en marzo de 2021. Esta norma hace hincapié en la necesidad de que las empresas financieras mejoren su resiliencia frente a las disrupciones operativas y les exige que establezcan planes para responder a los riesgos graves, pero probables. La normativa entró en vigor en abril de 2022 y las empresas disponen de un periodo de transición de tres años, hasta 2025, para garantizar su conformidad permanente con las directrices de su plan.

  La esencia de la reglamentación es exigir a las empresas que definan y defiendan unos servicios empresariales críticos y que determinen los niveles de disrupción que pueden soportar para poder seguir prestando sus funciones vitales. Para ello, la regulación exige que las empresas realicen pruebas de escenarios y mapeos y pone el énfasis en la estrategia de comunicación y la capacidad interna para autoevaluar el rendimiento, sobre todo por lo que se refiere a la identificación de los puntos débiles o las vulnerabilidades.

  En resumen, para la FCA, el BoE y la PRA, los principios fundamentales son prevenir, adaptarse, responder, recuperarse y aprender de las disrupciones operativas.

La perspectiva de los Estados Unidos

- A diferencia de la UE y el Reino Unido, el desarrollo de la resiliencia operativa en los EE. UU. se ha basado en una colaboración de asesoramiento ascendente e interinstitucional en lugar de en una regulación descendente. La Agencia de Seguridad Cibernética y de la Infraestructura (CISA) ha desempeñado un papel fundamental en este esfuerzo. Se creó en 2018 y forma parte del Departamento de Seguridad Interior de los EE. UU. Las responsabilidades de la CISA incluyen la evaluación del riesgo, la reducción de las vulnerabilidades, la detección de las amenazas, la respuesta a los incidentes y los esfuerzos de recuperación junto con otras agencias federales, las administraciones estatales y locales y el sector privado. La actividad de la CISA se centra en la colaboración voluntaria y en proporcionar recursos, como herramientas de gestión del riesgo, de evaluación de las amenazas o formación, para fortalecer las infraestructuras estadounidenses y ayudar a las instituciones a mejorar su ciberseguridad.
- En los Estados Unidos, parte de la responsabilidad corresponde también al Consejo Federal de Examen de las Instituciones Financieras (FFIEC), pero este tiene un mandato mucho más amplio y menos específico. El FFIEC es un organismo interinstitucional compuesto por los responsables de las cinco agencias bancarias federales: el Consejo de Gobernadores del Sistema de la Reserva Federal, la Corporación Federal de Seguros de Depósitos, la Administración Nacional de Cooperativas de Crédito, la Oficina de Control de la Moneda y la Oficina de Protección Financiera del Consumidor. En general, su papel es de coordinación y asesoramiento y no de regulación propiamente dicha. La Comisión de Valores y Bolsa (SEC) y la Comisión de Negociación de Futuros de Productos Básicos (CFTC) también revisan las prácticas de resiliencia operativa de las empresas, además de su capacidad para prevenir las interrupciones de los servicios críticos y de proteger los datos, registros y activos de los inversores.

Más recientemente, la Casa Blanca publicó una Estrategia Nacional de Seguridad en la primavera de 2023. Esta también tiene un mandato general, que va más allá de los mercados financieros para incluir áreas como las infraestructuras energéticas y los sistemas sanitarios, y, al igual que la mayoría de los esfuerzos que se realizan en los Estados Unidos, se basa más en la colaboración que en la regulación.

Los enfoques en Asia Pacífico

- En la región de Asia Pacífico, Singapur y Hong Kong han sido los más directos y activos a la hora de establecer unas prácticas de resiliencia operativa, mientras que otros centros financieros, como Australia, Japón y Malasia, abordan los requisitos de ciberseguridad y otros, pero con un enfoque más limitado o conservador.
- La Autoridad Monetaria de Singapur (MAS) introdujo sus primeras directrices de gestión de la continuidad operativa (BCM, por sus siglas en inglés) en 2003 y desde entonces no ha parado de ampliar y perfeccionar su estrategia. En junio de 2022 se completaron unas directrices revisadas, que están mucho más cerca de los parámetros más estrictos y exhaustivos de la resiliencia operativa, y las instituciones financieras están trabajando actualmente para llegar a cumplirlas. En junio de 2023 se exigió un plan que se ajustara a los requisitos regulatorios, así como un régimen de auditorías, y en junio de 2024 debe haberse completado la primera auditoría.

  Para cumplir, una entidad financiera debe adoptar una visión completa, de inicio a fin, de las dependencias de los servicios empresariales críticos, que tenga en cuenta el conjunto completo de procesos implicados. Algunos conceptos de la continuidad operativa son obligatorios, como los objetivos de tiempo de recuperación del servicio (SRTO), pero la regulación también reconoce la complejidad creada por las relaciones con terceros y el hecho de que algunos aspectos de los servicios deben priorizarse a otros durante un proceso de recuperación largo y por etapas.
- En Hong Kong, la Autoridad Monetaria de Hong Kong (HKMA) publicó una circular sobre la resiliencia operativa, el Manual de Política de Supervisión OR-2, en mayo de 2022, que se alineaba con los estándares del Banco de Pagos Internacionales (BPI) promulgados en 2021. La primera fase de la nueva regulación, que finalizó en mayo de 2023, incluía la exigencia de que se completara un marco de resiliencia operativa y un calendario para el pleno cumplimiento. La segunda fase se prolonga hasta mayo de 2026, cuando las instituciones financieras deberán contar con unos planes de resiliencia operativa plenamente funcionales.

  El OR-2 impone a las instituciones financieras la obligación de "realizar pruebas de escenarios de acontecimientos graves, pero probables, establecer unas políticas de gestión del riesgo más completas y unos marcos específicos de las operaciones empresariales críticas identificadas e implementar unos programas sólidos de gestión de los incidentes –cuyos requisitos van mucho más allá de los planes de continuidad operativa y los marcos de gestión del riesgo operativo existentes–. Se exige a las instituciones financieras que muestren, mediante planes e informes de pruebas, que han definido e implementado de manera eficaz unos escenarios que evalúan adecuadamente las operaciones críticas".[4]

> "Las disrupciones operativas pueden causar un perjuicio muy grande a los consumidores y constituyen un riesgo para la integridad del mercado, amenazan la viabilidad de las empresas y provocan inestabilidad en el sistema financiero".
>
> **FCA—AUTORIDAD REGULADORA DEL REINO UNIDO**[5]

Los puntos clave de los enfoques globales de la resiliencia operativa

En vista de la complejidad y las divergencias entre los enfoques de la resiliencia operativa adoptados por los distintos reguladores, una empresa de servicios financieros debería elegir el camino más fácil y fijarse solo en las regulaciones directamente aplicables a su región o geografía concreta. Sin embargo, este sería un enfoque corto de miras, porque las regulaciones pueden ir más allá de su propio territorio y afectar a otros. El Reglamento DORA, por ejemplo, es aplicable a todas las compañías de servicios financieros que operan en la Unión Europea y ello incluye a todas las empresas que les suministran servicios tecnológicos y de comunicaciones. Esta lista incluye a los procesadores de pagos, los proveedores de dinero electrónico, los proveedores de servicios de información contable, las sociedades de gestión, las aseguradoras, los proveedores de servicios de datos (incluidos los servicios de nube y de centro de datos) y los servicios de hardware. Es decir, es algo que afecta de manera profunda a una gran cantidad de empresas, de un modo nunca visto. Y, en poco tiempo, no habrá manera de escapar de las regulaciones y exigencias en materia de resiliencia operativa.

Teniendo esto en cuenta, es muy útil fijarse en los aspectos comunes que definen los distintos enfoques globales de la resiliencia operativa. En concreto, hay un énfasis en un enfoque común que incluye el establecimiento de unos estándares de ciberseguridad de obligado cumplimiento, unas pruebas obligatorias, una especial atención a la notificación de los incidentes y un mandato amplio de garantizar la resiliencia en los sectores críticos, y no solo en los servicios financieros.

Un análisis más detallado de estos aspectos

La ciberseguridad en primer plano

No todos los problemas de resiliencia operativa tienen su origen en las TIC o en el ámbito cibernético, pero, en última instancia, todos afectan a la espina dorsal tecnológica de la empresa moderna. Por este motivo, la ciberseguridad es fundamental en estos esfuerzos con un fuerte énfasis en la concienciación y la preparación para los episodios de ransomware. La aparición del ransomware como servicio como una industria en sí misma y el crecimiento continuado del ransomware patrocinado por los estados muestran la evolución y el crecimiento constantes de esta amenaza. Además, los incidentes cibernéticos tienden a tener un alcance más amplio y persistente que las interrupciones operativas tradicionales. También se puede necesitar mucho más tiempo para resolverlos y recuperarse de ellos y, por lo general, tienen un nivel más alto y son mucho más costosos.

La importancia de las infraestructuras y los servicios críticos

Un enfoque de "la vieja escuela" de la continuidad operativa seguía un modelo que podría denominarse de "muros altos y foso profundo", que no diferenciaba entre los elementos operativos centrales y los incidentales. Este enfoque ya no es eficaz (¡si es que alguna vez lo fue!), lo que hace necesario adoptar una estrategia que ponga el énfasis en el mantenimiento de un máximo posible de funciones empresariales en caso de disrupción. El plan debe ser exhaustivo y flexible. Por ejemplo, ahora es fundamental distinguir entre los elementos críticos y los menos críticos de una empresa, para que los planes de emergencia de la empresa permitan "mantener el funcionamiento", aunque sea con una capacidad reducida.

La gestión del riesgo — El alcance

Tal como se ha dicho anteriormente, la gestión del riesgo fue, en otro tiempo, un simple indicador financiero, pero esos días hace mucho que pasaron. El alcance de la gestión del riesgo ha aumentado sensiblemente con la inclusión de la resiliencia operativa como uno de los factores, lo que exige unos enfoques nuevos e innovadores a nivel de la empresa. El hecho de agregar los factores de resiliencia a las mediciones del riesgo financiero cambia radicalmente la orientación de los análisis y aumenta de forma muy importante la cantidad de esfuerzo necesario.

La gestión del riesgo — El coste

El coste de la gestión del riesgo solía medirse únicamente en términos de exposición al mercado, como Valor en Riesgo (VeR) o Pérdida Esperada (PE). En este tipo de régimen, las mejores herramientas de gestión del riesgo son las menos costosas. En el nuevo mundo de las regulaciones de la resiliencia operativa, la gestión del riesgo es mucho más compleja y polifacética, lo que hace que las antiguas mediciones del riesgo sean obsoletas. De cara al futuro, la complejidad del cumplimiento significa que el coste tiene que medirse con la mirada puesta en el coste por rendimiento, en lugar de centrarse solo en los costes iniciales. Y las herramientas también tienen que hacer más: buscar solo la solución más barata que ofrezca el mínimo indispensable ya no bastará.

Directrices y normas

De forma lenta, pero segura, las directrices y las normas que definen la resiliencia operativa van apareciendo. Aunque todavía hay que unificarlas y optimizarlas, es de esperar que con el tiempo estas normas se amplíen y se codifiquen. Además, las empresas se pueden ver afectadas cada vez más por las regulaciones de fuera de su propio territorio. El reglamento DORA es el marco regulatorio más desarrollado, prescriptivo y probablemente de mayor impacto, por lo que para la mayoría de empresas de servicios y proveedores tecnológicos es una buena idea acogerse a él.

Observabilidad

El principio de “ojos que no ven, corazón que no siente” no es una buena estrategia de gestión del riesgo. Sin embargo, las soluciones de supervisión tradicionales, acumuladas con los años y en numerosos silos, generan puntos ciegos, cuellos de botella en el rendimiento y un aumento del tiempo medio de reparación (MTTR, por sus siglas en inglés); además, no cumplen los estrictos requisitos de los reguladores. Como parte de un plan de resiliencia completo, las instituciones financieras deben adoptar un enfoque de observabilidad proactivo que les permita supervisar de manera constante las canalizaciones de datos y utilizar los flujos de trabajo automatizados para detectar anomalías, activar alertas y mejorar la mitigación. Como se suele decir, más vale prevenir que curar.

Notificación de incidentes

En reconocimiento implícito de la rápida evolución de las ciberamenazas y de la relativa inmadurez de los regímenes de resiliencia operativa, los reguladores dan una especial importancia a la notificación inmediata y completa de los incidentes, tanto a los propios reguladores como a la comunidad en su conjunto. Hay que olvidarse del reflejo tradicional de desconectar y callar durante y después de un incidente. En el futuro, la colaboración y la transparencia en materia de resiliencia operativa será la manera de funcionar estándar.

Gestión del riesgo de terceros

La continuidad operativa tradicional tendía a tratar a las empresas como si fueran una isla, pero las prácticas empresariales modernas han hecho que ese concepto haya quedado irremediablemente desfasado. Los nuevos enfoques de la resiliencia operativa aceptan el hecho de que la planificación debe extenderse hacia fuera desde la empresa, para incluir a los terceros, que son tanto una fuente de riesgo como un elemento vital para el funcionamiento del ecosistema financiero.

Complejidad

Por si no ha quedado ya bastante claro, hay que destacar que la expansión de la gestión del riesgo en los servicios financieros para incluir la resiliencia operativa aumenta drásticamente la complejidad de la tarea. Se trata de una labor que exige nuevos conocimientos y recursos, en la que participan más partes de la empresa y que está más entrelazada debido a las diversas interdependencias, incluidas las que involucran a terceros. Además, la aparición de categorías de activos digitales, como las criptomonedas y las finanzas descentralizadas (DeFi), y de las disrupciones causadas por el cambio climático o los mandatos ASG aún complican más las cosas.

> "La mejora de la resiliencia operativa puede reportar unos beneficios enormes, que van mucho más allá del mero cumplimiento normativo".
>
> **GUY WARREN, DIRECTOR GENERAL DE ITRS**[6]

En resumen, la resiliencia operativa es una disciplina relativamente nueva, pero se está convirtiendo rápidamente en una de las áreas más importantes a las que las compañías de servicios financieros deben prestar atención. Aunque aún estamos en las primeras etapas de definición de la resiliencia operativa como disciplina de gestión del riesgo, es importante reconocer que todos los esfuerzos deben ser dinámicos y que no deben tratarse como un acontecimiento aislado. Un plan de resiliencia operativa nunca se "completa": debe ponerse a prueba y mantenerse de forma activa y constante. Y, a medida que las normas y los requisitos se van codificando y van evolucionando junto con el negocio y la tecnología, el resultado es claro: en el futuro, un enfoque completo, potente y práctico de la resiliencia operativa beneficiará a todas las instituciones financieras.

Técnicas para lograr la resiliencia operativa

Si se compara con los enfoques tradicionales de la ciberseguridad o la continuidad operativa, la resiliencia operativa es mucho más amplia y complicada. La resiliencia operativa admite que es muy probable que se produzca un incidente, así que abandona el enfoque puramente defensivo y preventivo y adopta una estrategia que también incorpora un plan operativo que establece qué hay que hacer en caso de incidente. Las organizaciones deben prepararse interna y externamente y ello incluye un sólido programa de formación de los empleados, protocolos de comunicación y un equipo de gestión de la amenaza, tanto para ayudar a prevenir los incidentes como para garantizar que se han implementado unos procesos por si se produce un incidente o para cuando se produzca

Los Datos son el Centro

Como hemos visto, el panorama completo de ámbitos que preocupan a la resiliencia operativa es increíblemente amplio, pero hay un hecho incontestable: los datos siempre son el meollo de la cuestión. Los datos son el motor que impulsa a la empresa moderna y los datos son también el máximo objetivo de los responsables del ransomware y de los otros ciberdelincuentes. Proteja sus datos y ya habrá avanzado mucho en la protección de su empresa.

Un elemento clave de esta protección de los datos es una arquitectura de resiliencia por niveles eficaz, que incluya una recuperación con varias capas, que utilice instantáneas de seguridad para lograr los tiempos de recuperación más bajos posible, basándose en las necesidades y los objetivos de tiempo de recuperación (RTO) de la organización. Si bien la capacidad para recuperar los datos es esencial, una recuperación que tarde minutos, horas, días o más tiempo puede no satisfacer las necesidades de la empresa, de los clientes o de los reguladores. De hecho, los reguladores y las instituciones financieras pueden designar ciertas cargas de trabajo como de "Nivel 1", lo que hace que tengan que recuperarse con el mínimo tiempo de inactividad posible y perdiendo muy pocos datos. En el supuesto de que se produzca un acontecimiento negativo, ya sea un desastre natural, un ciberataque o incluso un accidente administrativo, la velocidad y la recuperación casi al instante son cruciales.

Los snapshots son un elemento esencial del plan, pero es importante tener en cuenta que no todas ellas se crean de la misma manera. Aunque los snapshots "inmutables" no pueden modificarse, con los privilegios adecuados, es posible borrarlos. Una arquitectura realmente resiliente exige unas instantáneas que no puedan modificarse ni borrarse, ni por accidente ni por parte de un actor malintencionado (que puede ser interno o externo a la organización), proporcionando de este modo un punto de recuperación garantizado. Para lograr esta "superinmutabilidad", los snapshots tienen que estar fuera de banda y haber sido autenticados de forma multifactorial.

Los niveles de una arquitectura de resiliencia

Una arquitectura de resiliencia por niveles se implementa en varios niveles o capas, cada uno de los cuales satisface una finalidad única e importante. La suma de estos niveles proporciona velocidad y durabilidad a una estrategia de recuperación.

Nivel 0

Este nivel incluye (sin limitarse a ello) la infraestructura de misión crítica, como Active Directory, DNS y los servicios de tiempo. Sin estos servicios, nada o casi nada funcionará en el entorno.

Nivel 1

En esta capa de resiliencia se alojan los datos primarios y las aplicaciones que tienen una importancia crítica para el funcionamiento de la empresa, incluidas las bases de datos y los servicios de aplicación más importantes, junto con sus dependencias definidas. Cuando se produce un incidente, una organización debe empezar la recuperación en el punto más cercano al incidente, así que estos serán el objetivo principal de la recuperación. Si no están disponibles, su organización no podrá prestar los servicios empresariales a los clientes. El Nivel 1 debería contener de tres a siete días de snapshots realmente inmutables.

Nivel 2

El Nivel 2 es la capa de respuesta a un incidente, que las organizaciones pueden utilizar para analizar lo ocurrido, responder al incidente y proceder a una recuperación más general. Esta capa es como un archivo de réplica en el que almacenar las instantáneas descargadas del Nivel 1. El archivo debería poder almacenar snapshots a medio y largo plazo, al menos de tres a doce meses, o más, si es posible, para que los equipos de respuesta a los incidentes puedan obtener de forma inmediata (y fácil) una visión a más largo plazo de cualquier incidente concreto.

NOTE: *Si bien el Nivel 2 está pensado para almacenar datos a más largo plazo o para satisfacer las necesidades de conformidad normativa de los datos, si se produce una disrupción importante, también puede ejecutar las cargas de trabajo con un rendimiento ligeramente menor, para que la empresa se mantenga en funcionamiento.*

Nivel 3

Normalmente, este tercer nivel se utiliza como capa de copia de seguridad, proporciona retención a largo plazo para los datos de cumplimiento normativo o históricos o para restaurar los datos para las aplicaciones menos críticas que no necesitan protegerse mediante snapshots. Las organizaciones también pueden utilizar este nivel para la copia de seguridad en una situación extrema.

Nivel 4

El Nivel 4 proporciona una capa opcional (pero muy recomendable) de defensa, compuesta por un búnker de datos de un solo sentido, en caso de desastres a gran escala. En esta capa, las organizaciones pueden replicar sus datos para que se encuentren en un sitio completamente distinto. Los búnkeres de datos están diseñados para ser muy seguros, con el fin de ofrecer una capa adicional de durabilidad, y pueden proporcionar un almacenamiento crucial para los años de datos exigidos por los reguladores. Además, si se produce un incidente, este nivel también permite que las organizaciones activen la computación de manera dinámica y bajo demanda, para ponerse en marcha rápidamente sin necesidad de mover los datos a través de largas distancias.

Recuadro lateral: Resiliencia operativa, ciberresiliencia y continuidad operativa

La continuidad operativa y **la resiliencia operativa** son dos enfoques críticos, pero distintos, de la gestión del riesgo. Si bien las dos se encargan de abordar las disrupciones para que la empresa vuelva a un funcionamiento normal, tienen unos puntos de partida esencialmente opuestos y se centran en aspectos diferentes de la respuesta de una organización a las disrupciones.

Por otro lado, la continuidad operativa (BC, por sus siglas en inglés, y también conocida como continuidad del negocio) y la resiliencia operativa (OR, por sus siglas en inglés) son distintas, pero se complementan y están interconectadas. La continuidad operativa es un componente de la resiliencia operativa y esta última incorpora más aspectos, como una gestión global del riesgo, **la ciberresiliencia**, la gestión de terceros y la de las crisis. Ambas son esenciales para una organización que quiera seguir prestando sus servicios en unas condiciones adversas.

La continuidad operativa o del negocio es la más conocida de las dos y se centra principalmente en la recuperación y la restauración de las funciones críticas de la empresa después de una disrupción. Un plan de continuidad operativa es reactivo por naturaleza, ya que se pone en marcha cuando se produce un incidente, y su objetivo principal es minimizar el tiempo de inactividad y acelerar la vuelta a un funcionamiento normal. Por lo general, la continuidad operativa utiliza un enfoque de coste/beneficio para determinar el alcance y la escala de las actividades.

La resiliencia operativa, por su parte, es un concepto más amplio y proactivo, que no solo incluye la capacidad para recuperarse de las disrupciones, sino también la de evitarlas o prevenirlas desde el principio siempre que sea posible. A diferencia del enfoque de coste/beneficio de la continuidad operativa, la resiliencia operativa parte de una mentalidad de “cisne negro”, que asume que lo peor es probable que ocurra. La resiliencia operativa incluye la capacidad de resistir y adaptarse rápidamente a las disrupciones, preservando la continuidad de la prestación de los servicios esenciales, pero va más allá de la recuperación para incluir la identificación de las posibles vulnerabilidades, la mitigación de los riesgos y la adaptación a los cambios del entorno operativo.

Desde el punto de vista de esta conversación, la ciberresiliencia es el área concreta que más debe preocuparnos. La ciberresiliencia se refiere a la capacidad de la institución para seguir prestando sus servicios en caso de que se produzcan ciberataques. A diferencia de la ciberseguridad, que está diseñada para proteger los sistemas, las redes y los datos frente a los ciberdelitos, la ciberresiliencia se concibe para garantizar que los sistemas y las redes no fallen por completo en el supuesto de que la seguridad se vea comprometida. Ante el aumento de los ataques y su creciente sofisticación, la ciberresiliencia es la respuesta lógica al hecho de que actualmente ya no se trata de si se va a producir un ataque, sino de cuándo vamos a sufrirlo.

Las soluciones de Pure facilitan la resiliencia operativa

Pure Storage es ideal para satisfacer las necesidades de los datos de resiliencia operativa de las empresas de servicios financieros. La velocidad y la flexibilidad están maximizadas gracias a una configuración all-flash, la recuperación en caso de disrupción está optimizada y la seguridad máxima de los datos está incorporada. Pure Storage admite la resiliencia operativa por diseño.

FlashBlade® y FlashArray™

Las soluciones de datos all-flash de alto rendimiento de Pure Storage son ideales para un mundo que exige más en cuanto a resiliencia operativa. La mejora de la velocidad, la simplicidad y el rendimiento hacen que la empresa sea más ágil por diseño y más capaz de cumplir los estrictos acuerdos de nivel de servicio de protección y disponibilidad de los datos, que son críticos para un funcionamiento eficiente de la empresa. Al proporcionar una cartera de soluciones de almacenamiento muy consistente, basada en una arquitectura común (estas soluciones comparten el software Purity, un flash adaptado y las herramientas de gestión), es posible optimizar el uso para satisfacer los requisitos de las cargas de trabajo y disfrutar de las suscripciones Evergreen™, que permiten que los clientes se mantengan al día de las nuevas amenazas y retos de manera no disruptiva.

SafeMode

Pure también ofrece unas sólidas funcionalidades integradas de protección de los datos con SafeMode, que proporciona snapshots siempre disponibles de sus datos. Basado en el "principio de los cuatro ojos", según el cual solo dos personas independientes y predefinidas pueden aprobar cualquier cambio, SafeMode protege los datos y los metadatos al crear unas copias instantáneas (snapshots) inmutables y seguras, que no pueden borrarse, modificarse ni cifrarse, ni siquiera con credenciales de administrador. Es eficiente, totalmente funcional, flexible y automatizable, lo que lo convierte en una herramienta indispensable para desarrollar la resiliencia operativa.

Rapid Restore (restauración rápida)

La resiliencia operativa exige volver a funcionar lo más rápidamente posible. Rapid Restore, incluido en FlashBlade, proporciona una capacidad de recuperación a una escala de petabytes para cumplir los requisitos más exigentes. Y lo que es más importante, aumenta enormemente la velocidad de restauración de los datos, sin necesidad de cambiar el software de copia de seguridad. Los sistemas tradicionales son notoriamente lentos y están muy poco preparados para las operaciones de restauración y recuperación. Al mismo tiempo, la arquitectura all-flash de FlashArray proporciona unas copias de seguridad y una restauración rápidas, para superar las limitaciones de las arquitecturas tradicionales de protección de los datos.

Tenemos una historia de resiliencia

La arquitectura de múltiples capas, segura y escalable con Pure Storage, los partners de protección de datos y otros controles y funciones SIEM (gestión de información y eventos de seguridad)

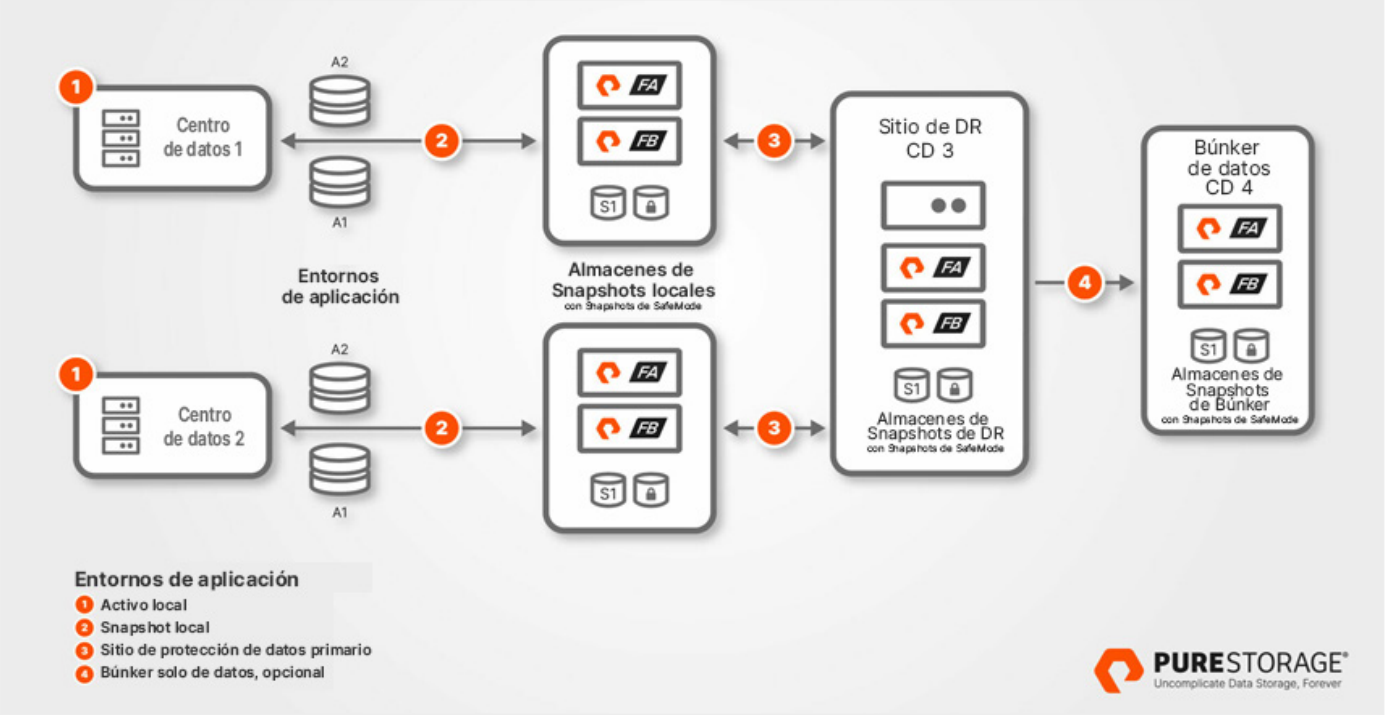

FIGURE 2 El funcionamiento de una arquitectura de copia de seguridad por niveles

Otras características y funcionalidades

- La evaluación del sistema y el soporte predictivo son fáciles con Pure1®. Esta herramienta basada en la nube proporciona análisis de pila completa, una puntuación de la resiliencia de datos y la potencia de Pure1 Meta®, que se basa en la IA, para evaluar la vulnerabilidad de su entorno y permitirle corregir sus puntos débiles. Con una interfaz única para gestionar todas sus cabinas de almacenamiento, Pure1 le ofrece información crucial sobre su pila tecnológica, incluida una vista de la topología que le permite simplificar la localización y resolución de los problemas de las VM.
- La solución Purity ActiveCluster hace que sea fácil y asequible alcanzar los máximos niveles de disponibilidad. Con ActiveCluster, pueden lograrse unos objetivos de punto de recuperación (RPO) y unos objetivos de tiempo de recuperación (RTO) de cero entre FlashArrays con una verdadera replicación sincrónica activa/activa para una conmutación por error transparente.
- Pure Cloud Block Store™ ofrece un almacenamiento de bloques nativo de la nube, para una movilidad perfecta de los datos entre los entornos locales y de la nube, y al mismo tiempo protege los datos en la nube y proporciona unos RTO y RPO rápidos. Su cifrado constante y la ciberseguridad nativa de la nube proporcionan una solución que protege los datos y permite cumplir las exigencias normativas y del sector, preservando la integridad de los datos y ofreciendo un tiempo de actividad continuo.
- Pure Protect //DRaaS es una solución tras desastres como servicio, que reduce la complejidad, el coste, el tiempo de recuperación y la disrupción operativa después de un desastre o de una disrupción informática. Ahora las empresas tienen unos entornos limpios con múltiples puntos de restauración en los que recuperar las copias limpias de sus datos locales de vSphere, en AWS EC2 nativo, sin importar la infraestructura de almacenamiento subyacente de que se trate y garantizando que los centros de datos permanecen aislados para su estudio.
- Un acuerdo de nivel de servicio de ransomware para una oferta como servicio que es única en el sector y una Garantía de Cero Pérdidas de Datos en toda la cartera Evergreen, que proporciona la tranquilidad de saber que los datos de los clientes no se perderán debido a problemas con el software o el hardware de Pure Storage.

> "Con miles de millones de dólares en juego y sus reputaciones en riesgo si los sistemas caen, nuestros clientes necesitan unos servicios de datos fiables y seguros. Eso es exactamente lo que Pure Storage nos permite ofrecer y gracias a ello estamos en una posición desde la que podemos construir unas relaciones muy sólidas con nuestros clientes a largo plazo".
>
> **JESSE BONSERIO,** DIRECTOR SÉNIOR DE INGENIERÍA DE ABACUS GROUP[7]

Las soluciones de medios flash son ideales para la resiliencia operativa porque cambian totalmente nuestra manera de abordar la agilidad de los datos en los distintos silos. El rendimiento y la fiabilidad del flash permiten una nueva forma de trabajar, que las entidades financieras pueden utilizar para mejorar la resiliencia operativa de un modo que hará que también estén preparadas para los retos del futuro —todo ello con un coste competitivo, incluso para los datos fríos (a los que se accede muy poco)—.

Conclusión: la maximización de la resiliencia operativa en los servicios financieros

La gestión del riesgo en los servicios financieros evoluciona constantemente y está bastante claro que en el futuro la resiliencia operativa será una parte muy importante de cualquier régimen de gestión del riesgo. Los reguladores de todo el mundo han tomado buena nota de que los mercados nunca han estado tan interconectados y de que la tecnología es un talón de Aquiles [8] de todo el sistema. Con la aparición de enfoques integrales como DORA, los reguladores han indicado que están cambiando su forma de ver y gestionar el riesgo. Las empresas de servicios financieros deben estar muy atentas y seguir su ejemplo.

De la misma manera que la resiliencia operativa se basa en la noción de que no se trata de "si, sino de cuándo" se producirá un incidente, las empresas financieras también tienen que ser conscientes de que no se trata de "si, sino de cuándo" los reguladores les exigirán unos mayores requisitos para la resiliencia operativa. Y, al mismo tiempo, los costes del incumplimiento —ya sea por multas, por otros costes o por las pérdidas de negocio causadas por el daño reputacional— también seguirán aumentando.

Los retos son grandes y el camino que hay por delante es complicado y cambiante; esto hace que sea difícil saber qué estrategia aplicar, pero la cuestión no puede ignorarse. El mejor momento para empezar es ahora mismo, aunque al principio solo sea para dar unos pequeños pasos. Al final del día, muchas cosas cambiarán y todo, de las personas a los procesos, se verá afectado. Ha llegado el momento de ponerse en marcha.

Recursos adicionales

Siguientes pasos

- Descubra qué es una arquitectura de resiliencia y cómo crear una.
- Aprenda de qué modo las soluciones de Pure aceleran los servicios financieros.
- Hable con un experto para que le ayude a fortalecer su resiliencia operativa.

Información complementaria

- Protección de datos
- Continuidad operativa
- Mitigación del ransomware

Acerca de la autora

Diane Saucier es la Directora de Servicios Financieros de Pure Storage y dirige el marketing para los servicios financieros, las tecnofinanzas y la tecnología regulatoria. Diane ha desempeñado funciones clave en instituciones financieras mundiales y proveedores tecnológicos y ha desarrollado soluciones de estrategia y negociación de producto, riesgo y cumplimiento normativo para múltiples clases de activos. Es fundadora y consejera de la organización Women in Listed Derivatives (WILD) y miembro del consejo asesor del Programa Fintech de la Universidad del Sur de Florida y de John J. Lothian & Company, Inc. Diane es licenciada en economía y ciencias políticas por la Northwestern University y posee una patente de un sistema flexible de operaciones electrónicas en bolsa.

1A medida que se intensifican los riesgos, los directores generales pueden ver la resiliencia operativa como una ventaja competitiva
2Revisiones del BCBS de los Principios para la buena gestión del riesgo operativo | PwC UK
3Los reguladores financieros del Reino Unido imponen unas multas de casi 50 millones de libras por los fallos de resiliencia operativa de un banco – Tech & Sourcing @ Morgan Lewis
4Afrontar el reto de los requisitos sobre resiliencia operativa de la HKMA
5PS21/3 Aumento de la resiliencia operativa | FCA
6La resiliencia operativa: una cuestión global
7El Grupo Abacus genera confianza en el sector financiero | Pure Storage
8https://www.britishmuseum.org/blog/who-was-achilles

PS2526-01-es 02/24