Impulsar la resiliencia operativa con soporte y servicios de TI

Aspectos destacados

Soporte de infraestructura

Visibilidad y priorización de los riesgos de TI

Gestión de riesgos con servicios de soporte proactivo

Gestión de riesgos con una estrategia consolidada de soporte del centro de datos

Pruebas de resiliencia operativa

Con el continuo aumento de los incidentes de ciberseguridad, se espera que surjan legislaciones en torno a la resiliencia operativa en las industrias financieras. Ya sea la ley sobre resiliencia operativa digital (DORA) de la Unión Europea, las directrices normativas como SR 20-24, sobre prácticas sólidas para fortalecer la resiliencia operativa en los EE. UU. o las directrices sobre resiliencia y riesgos operativos de Canadá, estas normas están aumentando las expectativas sobre las instituciones financieras para la gobernanza, la identificación y la gestión de riesgos, así como para la resiliencia operativa y la gestión de riesgos de terceros. Por supuesto, el objetivo final es garantizar que las organizaciones financieras estén preparadas con la estrategia adecuada para prevenir y recuperarse de forma proactiva ante un ataque cibernético, corrupción de datos, falla catastrófica del sistema u otro tipo de incidentes. En muchos casos, el incumplimiento o las fallas pueden dar lugar a sanciones económicas graves para las empresas afectadas.

IBM tiene una gama de servicios y soluciones para permitir que las entidades financieras aborden la seguridad y la resiliencia operativa. IBM® Consulting ofrece servicios de evaluación, gobernanza, controles y gestión de riesgos de TIC de terceros. Las soluciones de software de IBM reducen hasta en un 90 % el tiempo necesario para automatizar el descubrimiento y la gestión de los datos,[1] lo que contribuye al cumplimiento normativo y la elaboración de informes. IBM Data Security ayuda a proteger los datos y automatizar las auditorías de cumplimiento normativo. IBM® Security ayuda con la generación de informes y gestión de incidentes, mientras que IBM® Security X-Force ofrece servicios de detección y recuperación de incidentes, así como detección y respuesta gestionadas; por su parte, IBM® Control Desk with Maximo ayuda a las organizaciones a gestionar e informar sobre activos críticos.

Además de estos servicios y soluciones, IBM cree que el soporte y los servicios de TI pueden ser un elemento importante en los requisitos continuos para la resiliencia operativa. IBM TLS puede ayudar a los clientes con servicios y soluciones de soporte que brindan identificación y corrección proactiva de problemas potenciales antes de que ocurran.

Soporte de infraestructura
La resiliencia operativa depende de que la infraestructura funcione sin problemas y de forma segura. Eso significa equilibrar constantemente el costo y los recursos involucrados en la implementación de nuevas tecnologías como las de nube híbrida o contenerización con la necesidad de mantener al menos contratos de soporte básicos para hardware y software en producción. Según IDC, "las empresas deben priorizar los servicios de soporte de TI según la criticidad de la carga de trabajo; deben considerarlos como una inversión para preservar el valor comercial de estos sistemas al confiar en los proveedores para lograr un rendimiento optimizado". El informe también señala que las empresas encuestadas actualmente ahorran 290 horas de tiempo de inactividad con contratos de soporte de servidores, almacenamiento y redes. En otras palabras, están evitando 79 horas de tiempo de inactividad no previsto gracias a las herramientas de soporte proactivo.[2] Parece que cuanto más crítica es la carga de trabajo, más se debe considerar el soporte proactivo.

Para gestionar de forma eficaz más de 6 millones de tickets de servicio al año, IBM confía en una infraestructura de soporte global que incluye herramientas impulsadas por IA como Call Home, Remote Technical Support (RTS) y Cognitive Support Platform (CSP). El soporte remoto de IBM está diseñado para conectarse automáticamente, realizar análisis de diagnóstico y recuperar/resolver la mayoría de los problemas, por lo general, en una hora. Los equipos de soporte remoto de IBM resuelven el 74 % de los problemas de hardware y software de la infraestructura de IBM.[3] Los líderes de disponibilidad de clientes y gerentes técnicos y de escalamiento de proyectos garantizan el manejo oportuno de situaciones críticas, tanto de forma remota como in situ. El enfoque de soporte por niveles de IBM con IBM Expert Care e IBM Multivendor Enterprise Care permite a los clientes elegir el mejor nivel de soporte según sus necesidades.

Visibilidad y priorización de los riesgos de TI
Una de las preguntas clave que las organizaciones deberían hacerse es cómo pueden supervisar y evaluar proactivamente los riesgos de TI para cuantificar y priorizar los más críticos. La visibilidad en todo el entorno de TI puede ser un desafío y los riesgos de TI cambian con frecuencia. Pero la visibilidad no es suficiente. Es necesario comprender, evaluar y priorizar los riesgos con planes de acción oportunos para gestionar de manera eficaz los riesgos más críticos desde el principio.

IBM Support Insights, que se incluye con los contratos de mantenimiento y soporte de garantía de infraestructura de IBM, proporciona visibilidad de todo el patrimonio de TI junto con alertas de problemas potenciales y acciones recomendadas para ciertos proveedores. Este servicio basado en la nube actúa como un solo panel, que unifica la experiencia de soporte en IBM y en la infraestructura con múltiples proveedores, y proporciona insights basados en analytics, gestión de inventario y recomendaciones de mantenimiento preventivo. La suscripción de IBM Support Insights Pro proporciona valor adicional con vulnerabilidad de seguridad priorizada e insights del ciclo de vida, sistema operativo recomendado y niveles de firmware (actualmente se centra en insights para IBM Power y CISCO).

Support Insights emite alertas para diferentes factores de riesgo que incluyen vulnerabilidades de seguridad, cobertura de soporte, riesgos del sistema operativo/firmware y de hardware. Además de las alertas continuas, la herramienta proporciona puntuaciones de riesgo con una visión general de las amenazas potenciales para el entorno de TI.

Las categorías para clasificar los riesgos se calculan por medio de los datos y los insights obtenidos de una variedad de fuentes y análisis:

- Seguridad: vulnerabilidades y exposiciones comunes (CVE) para niveles conocidos de sistemas operativos y firmware
- Cobertura: eventos relacionados con vencimientos de contratos y garantías
- Firmware: eventos relacionados con la finalización del soporte de software o el fin de la vida útil y diversidad de sistemas operativos y firmware
- Hardware: eventos relacionados con la finalización del soporte de hardware/fin de la vida útil (solo IBM Infrastructure) y avisos del campo del proveedor (solo CISCO)

Esto ayuda a comprender los riesgos y proporciona los insights necesarios para abordar y mitigar de forma eficaz los posibles resultados negativos asociados con el activo en cuestión. Las alertas incluyen una puntuación de riesgo (alto, medio y bajo) que se determina en función del tipo, la prioridad y el plazo del riesgo (inmediato versus proyectado). Esto permite a las organizaciones priorizar rápidamente los esfuerzos de mitigación en función de los niveles de riesgo. Las alertas también vienen con recomendaciones de mitigación específicas que incluyen sugerencias y opciones específicas para remediar el problema en cuestión. Según la categoría de riesgo, las recomendaciones pueden incluir información sobre los parches que se van a aplicar, las versiones a las que se va a actualizar, las opciones de reemplazo de asesoramiento y otros. No todas las alertas tienen recomendaciones específicas, pero generalmente brindan orientación sobre las mejores prácticas para ayudar a mitigar el riesgo de la alerta.

Gestión de riesgos con servicios de soporte proactivo

La visibilidad de los riesgos de TI es el punto de partida, pero luego depende del ya reducido personal de TI de las organizaciones para dar seguimiento a las alertas y realizar las acciones de mitigación apropiadas de manera oportuna. En 2022, XForce identificó 23 964 vulnerabilidades de seguridad.[4] Una vez publicadas las alertas, las organizaciones deben explorarlas y priorizar aquellas que deben atenderse primero, para luego iniciar acciones de mitigación. Complementar el personal de TI con soporte proactivo proporcionado por el proveedor puede permitir a las organizaciones priorizar las acciones de mantenimiento diarias que a menudo pueden retrasarse debido a problemas inesperados y proyectos estratégicos de TI.

IBM trabaja con los clientes para personalizar sus servicios de soporte y ofrecer soluciones tanto reactivas como proactivas. Algunos ejemplos de diferentes servicios de soporte que IBM puede ejecutar en lugar del personal de TI incluyen:

- Punto de contacto único para problemas de gravedad 1 y 2
- Determinación de problemas, identificación del origen del problema y resolución
- Planes de soporte personalizados que incluyan los procesos operativos y de mantenimiento, la estructura de soporte actual, las aplicaciones críticas, los escenarios de interrupción críticos y el entorno
- Informes que resumen la actividad del servicio para los problemas reportados con recomendaciones proactivas
- Documentar y mantener los requisitos de disponibilidad
- Análisis de rendimiento y recomendaciones de mejora
- Ejecución de servicios preventivos

Puede confiar en IBM® Technology Lifecycle Services para mantener sus sistemas críticos funcionando sin problemas en todo momento

Gestión de riesgos con una estrategia consolidada de soporte del centro de datos
Según IDC, la proliferación de proveedores en el centro de datos tiene un impacto directo en la cantidad de tiempo de inactividad experimentado.[2] Con cada nuevo producto y proveedor, los riesgos de interoperabilidad son exponenciales. Con contactos separados para cada proveedor, resulta cada vez más difícil identificar un área única que afecte el rendimiento. La cantidad de tiempo que el personal de TI de las organizaciones dedica al soporte de los proveedores también es una preocupación clave para muchos, ya que resta tiempo a actividades más estratégicas. Finalmente, cada persona que tiene acceso físico a su centro de datos es un riesgo potencial para la seguridad.

Consolidar el soporte de los proveedores con un proveedor confiable es una forma en que las organizaciones pueden abordar la resiliencia operativa en todo el centro de datos. Trabajar con IBM como proveedor confiable para el soporte consolidado de los centros de datos ha demostrado que permite abordar las inquietudes mencionadas anteriormente. De hecho, los clientes han logrado reducir el tiempo medio hasta la resolución de problemas, reducir el tiempo dedicado al soporte de hardware y a la gestión de proveedores, evitar interrupciones del servicio y reducir los costos.[5] Lea el informe de Forrester: The Total Economic Impact of IBM Hybrid IT Support para obtener más detalles sobre una estrategia de soporte consolidado con IBM.

Pruebas de resiliencia operativa
Verificar periódicamente la infraestructura en busca de posibles debilidades también es fundamental para mantener la resiliencia. Las organizaciones necesitan identificar posibles puntos únicos de falla que pueden causar o extender interrupciones. Deben planear la revisión de los registros, bitácoras y tendencias de las máquinas para aislar problemas crónicos y desarrollar planes de acción para evitar o minimizar el impacto de las interrupciones imprevistas. IBM puede proporcionar controles rápidos del estado de los productos en el centro de datos. Además de los controles de estado rápidos, se pueden realizar evaluaciones más profundas para optimizar el rendimiento o profundizar en las vulnerabilidades de seguridad.

Dada la multiplicidad de productos y proveedores individuales en la mayoría de los centros de datos actuales, no basta con realizar pruebas de resiliencia a nivel de producto. Ya sea que una organización acabe de sufrir un incidente importante o quiera ser más proactiva a la hora de mantener altos niveles de disponibilidad, una evaluación del entorno en su conjunto puede ayudar a descubrir dependencias e inhibidores de la alta disponibilidad, y proponer mejores prácticas para mantenerla. El High Availability Center of Competency de IBM puede ayudar con la evaluación, las revisiones posteriores al incidente, así como con las mejores prácticas y el intercambio de conocimientos.

Conclusión
La resiliencia operativa depende de una infraestructura eficiente y eficaz. Mantener esa infraestructura actualizada, lograr visibilidad de los riesgos potenciales y tomar medidas para mitigar dichos riesgos son aspectos críticos para el éxito. Las organizaciones necesitan un socio confiable que comprenda sus necesidades comerciales y adopte un método integral para el soporte y los servicios centrado en la resiliencia operativa.

¿Por qué IBM® Technology Lifecycle Services?
IBM Technology Lifecycle Services trabaja con organizaciones para adaptar un enfoque que satisfaga sus necesidades de resiliencia operativa. IBM tiene más de 35 años de experiencia brindando mantenimiento y soporte para entornos con múltiples proveedores para aproximadamente 22 000 productos de hardware y software de IBM y de terceros. Con una presencia global que se extiende a más de 130 países, usted puede estar tranquilo al saber que los recursos estarán disponibles cuando los necesite. Finalmente, según la evaluación de proveedores de soporte a nivel mundial de IDC Marketscape 2022, las principales fortalezas de IBM como proveedor de soporte global son nuestra presencia global, las capacidades para atender entornos con múltiples proveedores, las capacidades de atención proactiva y nuestras relaciones con altos ejecutivos, que nos permiten comprender las necesidades comerciales de nuestros clientes.[6]

Alfonso Nápoles Gandara 3111
Col. Parque corporativo de Peña Blanca
C.P. 01210
México D.F.
IBM Corporation
New Orchard Road
Armonk, NY 10504

Producido en los Estados Unidos de América,
enero de 2024.

1 “IBM Cloud Pak for Data enhances DataOps services to deliver business agility with cost savings and risk reduction”, Aliye Ozcan, mayo de 2020.
2 IDC Perspective: The Cost of Downtime in Datacenter Environments: Key Drivers and How Support Providers Can Help, Doc # US50240823, marzo de 2023.
3 Datos internos de IBM
4 Índice X-Force Threat Intelligence 2023
5 The Total Economic Impact for IBM Hybrid IT Support, un estudio de Forrester encargado por IBM, enero de 2023.
6 IDC Marketscape 2022 Worldwide Support Vendor Assessment, IDC, marzo de 2022.