Impulsar la resiliencia operativa con soporte y servicios de TI

Aspectos destacados

Apoyo a las infraestructuras

Visibilidad y priorización de los riesgos de TI

Gestión de riesgos con servicios de soporte proactivos

Gestión de riesgos con una estrategia de soporte consolidada en el centro de datos

Pruebas de resiliencia operativa

Con el continuo aumento de los incidentes de ciberseguridad, no es de extrañar que surja nueva legislación sobre resiliencia operativa en el sector financiero. La normativa como la Ley de Resiliencia Operativa Digital (DORA) de la Unión Europea, la SR 20-24, Sound Practices to Strengthen Operational Resilience de Estados Unidos y la Operational Risk and Resilience Guidance de Canadá están aumentando las expectativas puestas en las entidades financieras en términos de gobierno, identificación y gestión de riesgos, resiliencia operativa y gestión de riesgos de terceros. Por supuesto, el objetivo final es garantizar que las organizaciones financieras dispongan de las estrategias adecuadas para permitir una prevención y recuperación proactivas en caso de ciberataque, corrupción de datos, fallo catastrófico del sistema o cualquier otro tipo de incidente. En muchos casos, el incumplimiento o el fallo pueden acarrear graves sanciones económicas para las empresas afectadas.

IBM ofrece una gama de servicios y soluciones que permiten a las entidades financieras garantizar la seguridad y la resiliencia operativa. IBM Consulting ofrece servicios de evaluación de riesgos, gobierno y control de riesgos, y gestión de riesgos de TIC de terceros. Las soluciones de software de IBM reducen el tiempo necesario para automatizar la detección y el gobierno de datos hasta en un 90 %[1], simplificando el cumplimiento y la elaboración de informes. IBM Data Security ayuda a proteger los datos y a automatizar las auditorías de cumplimiento. IBM Security ayuda con la generación de informes y la gestión de incidentes, IBM Security X-Force proporciona servicios de detección y recuperación de incidentes, así como detección y respuesta gestionadas, e IBM Control Desk con Maximo ayuda a las organizaciones a gestionar e informar sobre recursos críticos.

Además de estos servicios y soluciones, IBM cree que el soporte y los servicios de TI pueden ser un elemento importante de los requisitos permanentes en materia de resiliencia operativa. IBM® TLS puede ayudar a sus clientes ofreciéndoles servicios y soluciones de soporte que identifiquen y resuelvan proactivamente los posibles problemas antes de que se produzcan.

Apoyo a las infraestructuras
La resiliencia operativa depende del buen funcionamiento y la seguridad de la infraestructura. Esto significa encontrar un equilibrio permanente entre los costes y los recursos necesarios para implantar nuevas tecnologías, como el cloud híbrido o la contenerización, y la necesidad de mantener contratos de soporte básico (como mínimo) para el hardware y el software en producción. Según IDC, "Las empresas deben priorizar los servicios de soporte de TI en función de la criticidad de las cargas de trabajo y considerarlos como una inversión para preservar el valor empresarial de estos sistemas, confiando en los proveedores para optimizar el rendimiento". El informe también indica que las empresas encuestadas están ahorrando actualmente 290 horas de tiempo de inactividad gracias a los contratos de soporte para servidores, almacenamiento y redes; más explícitamente, están evitando 79 horas de inactividad no planificada gracias a herramientas de soporte predictivo y proactivo. [2] Parece que cuanto más crucial es la carga de trabajo, más se debería de considerar el soporte proactivo.

Para gestionar eficazmente más de 6 millones de incidencias de servicio al año, IBM cuenta con una infraestructura de soporte global que incluye herramientas basadas en IA como la llamada al centro de soporte, el soporte técnico remoto (RTS) y la plataforma de soporte cognitivo (CSP). El soporte remoto de IBM está diseñado para conectarse automáticamente, realizar análisis de diagnóstico y recuperar/resolver la mayoría de los problemas, a menudo en menos de 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 Client Availability Leaders y los Technical & Project Escalation Managers garantizan que las situaciones cruciales se aborden rápidamente, tanto de forma remota como in situ. El enfoque de soporte escalonado de IBM con IBM® Expert Care e IBM® Multivendor Enterprise Care permite a los clientes elegir el mejor nivel de soporte en función de sus necesidades.

Visibilidad y priorización de los riesgos de TI
Una de las preguntas clave que deben hacerse las organizaciones es cómo pueden monitorizar y evaluar proactivamente los riesgos de TI para cuantificar y priorizar los más cruciales. Tener visibilidad de toda la infraestructura de TI puede ser difícil, y los riesgos de TI cambian con frecuencia. Aun así, la visibilidad no es suficiente. Los riesgos deben comprenderse, evaluarse y priorizarse en planes de acción oportunos para gestionar eficazmente los riesgos más cruciales desde el principio.

IBM® Support Insights, incluido en los contratos de mantenimiento y soporte de la garantía de infraestructuras de IBM, ofrece visibilidad de toda la infraestructura de TI y destaca los problemas potenciales y las acciones recomendadas para proveedores específicos. Este servicio basado en el cloud actúa como una vista única que unifica la experiencia de soporte en toda la infraestructura de IBM y de múltiples proveedores, proporcionando analítica, gestión de inventario y recomendaciones de mantenimiento preventivo. La suscripción a IBM® Support Insights Pro ofrece valor añadido al proporcionarle información priorizada sobre vulnerabilidades de seguridad y ciclo de vida, recomendaciones del sistema operativo y niveles de firmware, que en la actualidad se centran en información sobre IBM® Power y CISCO.

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

Las categorías de puntuación de riesgo se basan en datos e información procedentes de diversas fuentes y análisis:

- Seguridad: vulnerabilidades y exposiciones comunes (CVE) para niveles conocidos de sistemas operativos y firmware
- Cobertura: vencimiento del contrato y de la garantía
- Firmware: fin de soporte/fin de vida útil del software y diversidad de sistemas operativos y firmware
- Hardware: fin de soporte/fin de vida útil del hardware (solo infraestructura de IBM) y avisos a proveedores (solo CISCO)

Estas categorías ayudan a comprender los riesgos y proporcionan la información necesaria para identificar y mitigar eficazmente las posibles consecuencias negativas asociadas a los recursos en cuestión. Las alertas incluyen una puntuación de riesgo (alto, medio, bajo) determinada por el tipo, la prioridad y el marco temporal (inmediato o previsto) del riesgo. Esto permite a las organizaciones priorizar rápidamente los esfuerzos de mitigación en función de los niveles de riesgo. Las alertas también van acompañadas de recomendaciones específicas de mitigación que incluyen sugerencias y opciones concretas para resolver el problema en cuestión. Dependiendo de la categoría de riesgo, las recomendaciones pueden incluir información sobre qué parches aplicar, a qué versiones actualizar, consejos sobre opciones de sustitución, etc. No todas las alertas contienen recomendaciones específicas, pero en general proporcionan una orientación sobre buenas prácticas para ayudar a mitigar el riesgo cubierto por la alerta.

Gestión de riesgos con servicios de soporte proactivos

La visibilidad de los riesgos de TI es el punto de partida, pero luego corresponde a los equipos de TI de las organizaciones, ya sobrecargados de trabajo, supervisar las alertas y adoptar oportunamente las medidas paliativas adecuadas. En 2022, XForce identificó 23 964 vulnerabilidades de seguridad.[4] Una vez emitidas las alertas, las organizaciones deben explorarlas, priorizarlas y empezar a tomar medidas paliativas. Al reforzar el personal de TI con el soporte proactivo de los proveedores, las organizaciones pueden dar prioridad a las acciones de mantenimiento cotidianas que a menudo pueden verse retrasadas por problemas inesperados y proyectos estratégicos de TI.

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

- 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 asistencia actual, las aplicaciones cruciales, los escenarios de fallos críticos y el entorno
- Informes que resumen la actividad de servicio en relación con los problemas notificados, con recomendaciones proactivas
- Documentación y mantenimiento de 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 correctamente 24x7

Gestión de riesgos con una estrategia de soporte consolidada en el centro de datos
Según IDC, el aumento de proveedores en el centro de datos tiene un impacto directo en el tiempo de inactividad.[2] Con cada nuevo producto y proveedor llegan riesgos exponenciales de interoperabilidad. Con contratos independientes para cada proveedor, cada vez es más difícil identificar el área que afecta al rendimiento. El tiempo que los equipos de TI de las organizaciones dedican al soporte de los proveedores es también una preocupación importante para muchas empresas, ya que les impide centrarse en actividades más estratégicas. Por último, cualquier persona con acceso físico a su centro de datos representa un riesgo potencial para la seguridad.

Consolidar todo el soporte de proveedores con un proveedor de confianza es una forma de que las organizaciones garanticen la resiliencia operativa de todo el centro de datos. La elección de IBM como proveedor de confianza para consolidar el soporte del centro de datos ha resuelto los problemas mencionados. Los clientes se han beneficiado de la reducción del tiempo medio de resolución, la reducción del tiempo dedicado al soporte de hardware y la gestión de proveedores, la prevención de interrupciones y el ahorro de costes.[5] Lea el siguiente informe de Forrester: The Total Economic Impact of IBM Hybrid IT Support para obtener más información sobre la estrategia de soporte consolidado con IBM.

Pruebas de resiliencia operativa
También es esencial comprobar periódicamente la infraestructura en busca de posibles puntos débiles para garantizar su resiliencia. Las organizaciones deben identificar los únicos puntos de error que pueden causar o prolongar las interrupciones. Deben planificar la revisión de los registros de máquinas, registros y tendencias para aislar los problemas crónicos y desarrollar planes de acción para evitar o minimizar el impacto de las interrupciones imprevistas. IBM puede proporcionar comprobaciones rápidas del estado de los productos en el centro de datos. Además de estas comprobaciones, se pueden realizar evaluaciones más profundas para ajustar el rendimiento óptimo o investigar en profundidad vulnerabilidades de seguridad.

Dada la multiplicidad de productos y proveedores individuales en la mayoría de los centros de datos actuales, no basta con probar la resiliencia a nivel de producto. Tanto si una organización acaba de sufrir un incidente grave como si quiere ser más proactiva a la hora de mantener altos niveles de disponibilidad, una evaluación del entorno en su conjunto puede ayudar a descubrir dependencias y obstáculos a la alta disponibilidad, y sugerir buenas prácticas para mantenerla. El IBM High Availability Center of Competency puede ayudar a llevar a cabo evaluaciones y revisiones posteriores a incidentes, proporcionar buenas prácticas y compartir conocimientos.

Conclusión
La resiliencia operativa depende de una infraestructura eficaz y eficiente. Mantener esta infraestructura actualizada, tener visibilidad de los riesgos potenciales y tomar medidas decisivas para mitigarlos es crucial para el éxito. Las organizaciones necesitan un socio de confianza que comprenda sus necesidades empresariales y adopte un enfoque holístico del soporte y los servicios, centrado en la resiliencia.

Razones para elegir IBM Technology Lifecycle Services
IBM® Technology Lifecycle Services trabaja con las organizaciones para diseñar un enfoque que satisfaga sus necesidades de resiliencia operativa. IBM cuenta con más de 35 años de experiencia en el mantenimiento y soporte de 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, puede estar tranquilo sabiendo que puede disponer de nuestros recursos siempre que lo necesite. Por último, según el estudio IDC Marketscape 2022 Worldwide Support Vendor Assessment, los principales puntos fuertes de IBM como proveedor de soporte mundial son su presencia global y sus capacidades multiproveedor, sus capacidades de soporte proactivo y sus relaciones con los equipos directivos que le permiten comprender las necesidades empresariales de sus clientes[6].

IBM España, S.A.
Santa Hortensia, 26-28
28002 Madrid
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. n.º US50240823. Marzo de 2023
3 Datos internos de IBM
4 X-Force Threat Intelligence Index 2023
5 The Total Economic Impact for IBM Hybrid IT Support. Un estudio Forrester encargado por IBM. Enero de 2023.
6 IDC Marketscape 2022 Worldwide Support Vendor Assessment. IDC. Marzo de 2022