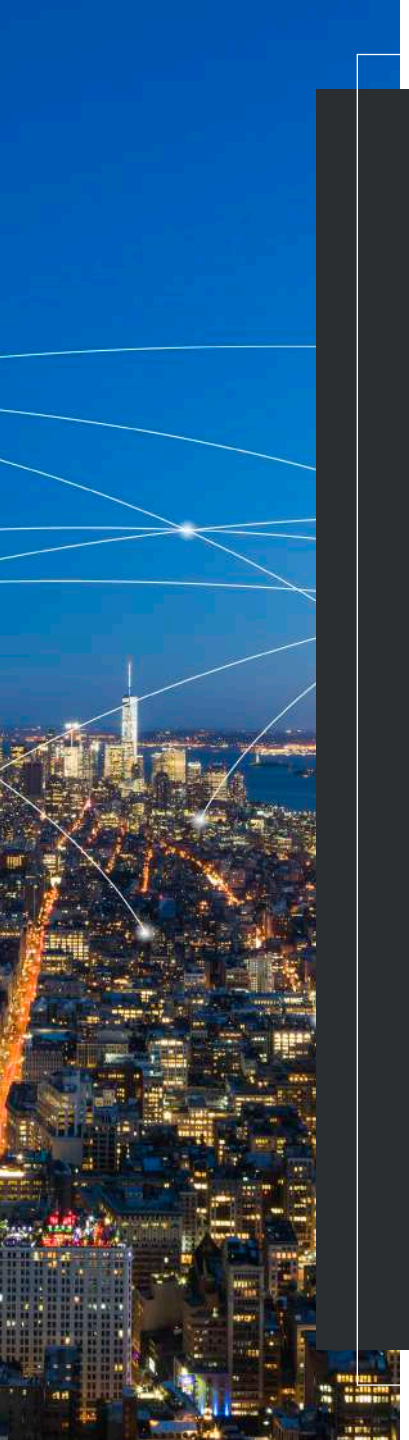
IBM **Global**
Technology Services

Presentación de la solución

IBM Resiliency Orchestration con Recuperación de ciberincidencias

Proteja los datos y las configuraciones de plataforma con un recurso diseñado especialmente para una recuperación rápida, fiable y escalable después de los ciberataques

IBM®



Características principales

- Almacenamiento inalterable aislado para datos y archivos de configuración de plataforma
- Rápida detección de anomalías en configuraciones de sistemas Windows o Linux, incluidos el registro de Windows, las configuraciones de aplicaciones y las configuraciones de dispositivos
- La restauración rápida y organizada de datos y configuraciones de plataforma contribuye a reducir el impacto de las interrupciones ocasionadas por un ciberataque o cualquier otra parada
- La plataforma automatizada de pruebas y verificación permite realizar pruebas frecuentes sin afectar a los sistemas empresariales
- La visibilidad en el proceso y la creación de informes ayuda a cumplir los requisitos de conformidad

Los ciberataques siguen asolando las organizaciones de todos los tamaños. Aunque los equipos de seguridad de TI mejoran la prevención para que no se produzcan ciberataques, estos siguen siendo más una cuestión de “cuándo” se producirá uno (si aún no se ha producido) que de “si” se producirá. Una interrupción del negocio causada por ciberataques que dañen sus datos críticos y las configuraciones de sus sistemas puede ser tan perjudicial para el bienestar financiero y la reputación de una organización como el robo de datos o una parada completa de TI.

Esto puede ser especialmente verdadero cuando los ciberataques involucran al cifrado de los datos, o un programa malintencionado se dirige específicamente a las copias de seguridad de datos. La continua exposición de las redes a las ubicaciones de copia de seguridad y recuperación tras desastre (DR) puede dar al programa malintencionado la oportunidad de corromper o cifrar estos datos, dejando inutilizable tanto los datos primarios como los de copia de seguridad, retrasando significativamente la capacidad para recuperar las operaciones a nivel de producción.

A menudo el daño se produce porque las soluciones de DR existentes no están diseñadas para recuperarse de cibereventos o están plagadas de problemas persistentes relativos a las capacidades de DR: demasiada dependencia de procesos manuales, runbooks desfasados y pruebas inadecuadas. El resultado es que la recuperación lleva demasiado tiempo, los puntos de recuperación de datos son demasiado antiguos o falla la recuperación en sí.

Capacidad creada especialmente para la ciberresiliencia

La Recuperación de ciberincidencias, basada en IBM Resiliency Orchestration, se ha diseñado para recuperar rápidamente datos y configuraciones de plataforma, en el caso de que se produzca una ciberparada. Diseñada especialmente para la ciberrecuperación, la Recuperación de ciberincidencias ofrece:

- Capacidad para realizar pruebas rápidas que no afecten a los entornos de producción
- Detección más rápida de corrupción de datos y respuesta rápida para reducir el tiempo de inactividad
- Recuperación de un punto en el tiempo eficiente que optimiza los objetivos de punto de recuperación (RPO)
- Escalabilidad para gestionar la detección a nivel de localización y la recuperación en pocos minutos
- Visibilidad simplificada y creación de informes para ayudar a cumplir los requisitos normativos

Los bloques de tecnología que forman la capacidad de Recuperación de ciberincidencias proporcionan una plataforma que abarca las capas de computación y datos de entornos tanto de producción como de DR, para poder tener un enfoque ágil en la recuperación de un ciberdesastre. Esta arquitectura incluye:

Almacenamiento inalterable. El uso de tecnología de almacenamiento inalterable para los datos de configuración o el almacenamiento Grabar una vez leer varias (WORM) para los datos de aplicación contribuye a impedir la corrupción y a asegurar la recuperabilidad, al no permitir que se realicen cambios en las copias de seguridad una vez se hayan

guardado. Para los datos de aplicación, este método también permite reducir costes de almacenamiento, al escribir solamente nuevas copias de cambios incrementales en un momento específico.

Protección aislada. El aislamiento de la red separa los entornos de producción y el almacenamiento WORM que contiene los datos protegidos de los que se han hecho copias de seguridad, en un sitio remoto o DR. También se restringe el acceso al almacenamiento WORM solamente en los momentos en que están disponibles los datos para realizar su copia de seguridad. Este método, combinado con el almacenamiento inalterable, ayuda a impedir que los programas malintencionados corrompan los datos protegidos, programas que pueden atravesar redes o que se han diseñado específicamente para apuntar a los datos de copia de seguridad.

Verificación de los datos de configuración. Este componente ayuda a garantizar que la configuración o los datos protegidos están limpios y se puedan recuperar. Este proceso, incorporado en Resiliency Orchestration, detectará automáticamente el momento en que se modifiquen las configuraciones del sistema y no coincidan con las versiones “maestro”. Resiliency Orchestration también se integrará con los scripts de validez de aplicación proporcionados por el cliente, así como las pruebas a nivel de datos.

Automatización y orquestación. Con la automatización del proceso de recuperación a todos los niveles (E2E) para datos, aplicaciones, conmutadores e infraestructura de computación, Resiliency Orchestration permite realizar una restauración rápida del entorno de TI. Resiliency Orchestration sustituye a los procesos manuales tradicionales con flujos de trabajo predeterminados que se han probado y validado, lo que le permite recuperar todo un proceso de negocio, aplicación, base de datos o sistema discreto haciendo clic en un botón. Estos flujos de trabajo organizan los distintos pasos necesarios para recuperar sistemas y datos interconectados, limitando el error humano. Resiliency Orchestration ayuda a acelerar la implementación de soluciones al aprovechar una amplia biblioteca de más de 450 patrones predefinidos, que se pueden combinar para crear flujos de trabajo.

Recuperación de ciberincidencias para la configuración de plataforma

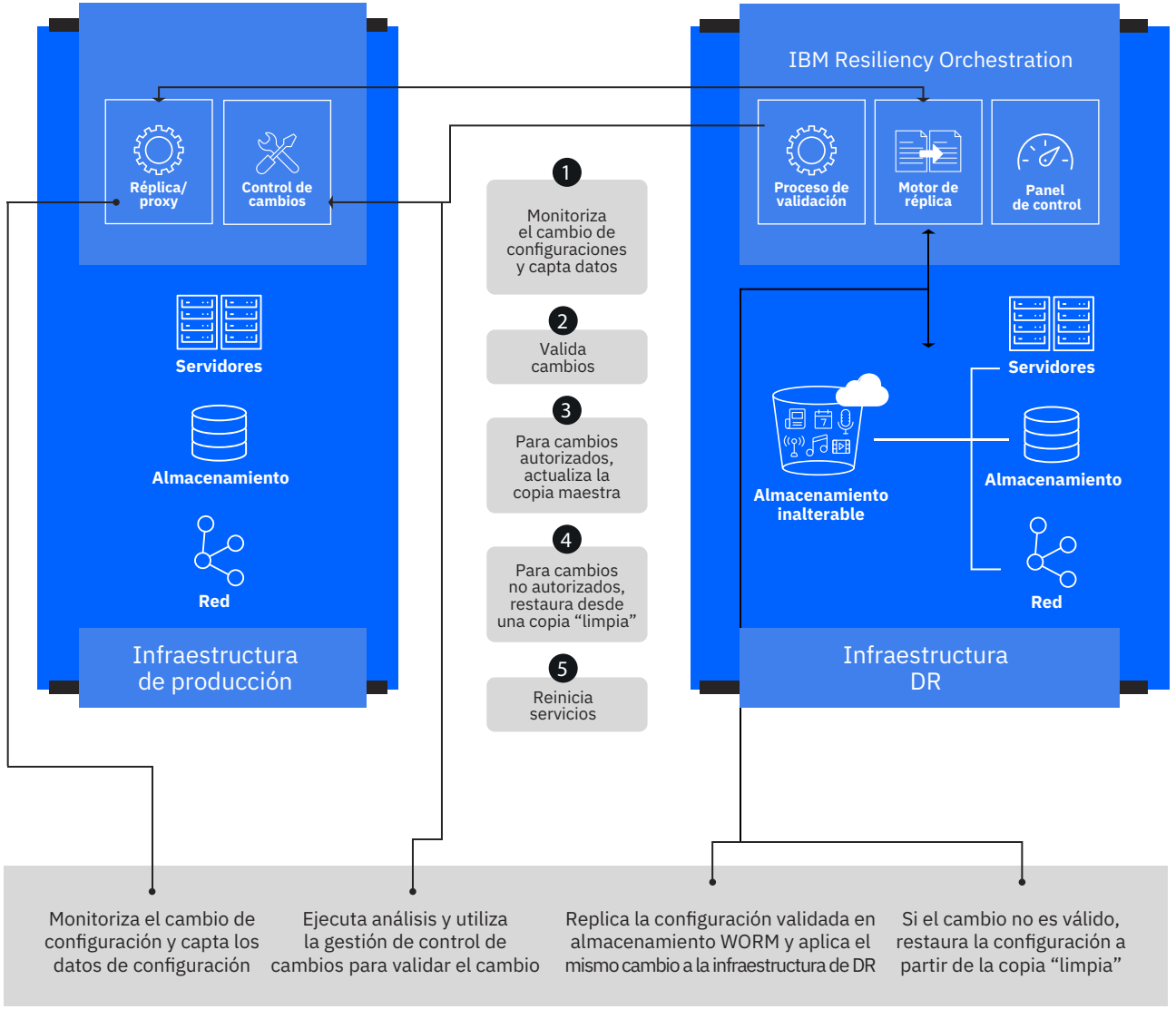
Para realizar operaciones comerciales se requiere en todo momento disponibilidad continua de la infraestructura de TI subyacente a las aplicaciones críticas de negocio: servidores físicos, instancias de VM, sistemas de almacenamiento y dispositivos de red. Los ciberataques pueden tener como resultado la paralización de la actividad de las empresas al corromper los datos de configuración de estas plataformas.

La función de configuración de plataforma de la Recuperación de ciberincidencias (véase la figura 1) permite efectuar una restauración rápida de los servicios, replicando una “copia maestra” de los datos de configuración de servidores y dispositivos de almacenamiento inalterable aislado y protegido, en un almacenamiento de objetos en la nube o centro de datos de IBM. Los dispositivos de producción se examinan para detectar cambios en los datos de configuración. El sistema analiza el cambio para determinar si es válido y muestra alertas cuando detecta un cambio sospechoso en los datos de configuración. Las alertas también pueden proporcionar tiques relevantes del software de gestión del control de cambios.

En el caso de que se realice un cambio válido, los datos de configuración se protegen mediante la replicación de una nueva “copia maestra” en almacenamiento inalterable. Si se identifica un cambio no válido, Resiliency Orchestration restaura rápidamente la última copia limpia de configuraciones del dispositivo en la infraestructura de producción, basándose en políticas preestablecidas y con el oportuno consentimiento de la dirección. Las configuraciones de máquina virtual y dedicada se restauran en una infraestructura de producción limpia.

Recuperación de ciberincidencias para datos

Figura 1: La Recuperación de ciberincidencias para la configuración de plataformas ayuda a proteger datos de configuración y servidores físicos y virtuales, así como dispositivos de almacenamiento y red.



Recuperación de ciberincidencias para datos

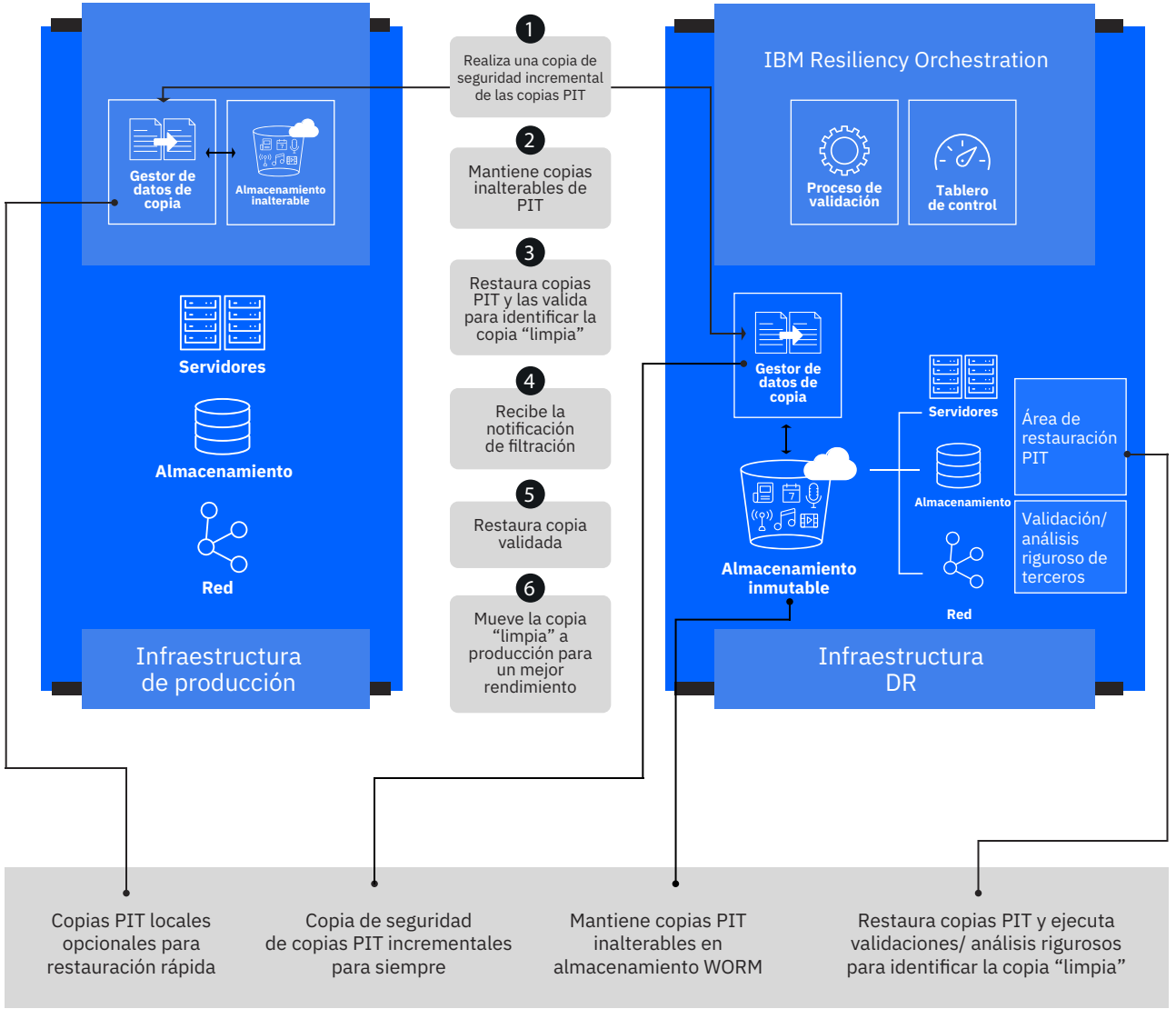
La función de datos de la Recuperación de ciberincidencias permite realizar una recuperación rápida y altamente fiable frente a los ciberataques que dañan los datos en sí. Protege los datos mediante el uso de una protección aislada y almacenamiento inalterable, organizando al mismo tiempo la recuperación rápida en el sitio DR del cliente.

La Recuperación de ciberincidencias se ha diseñado para gestionar grandes volúmenes de datos de aplicación. Emplea tecnología de gestión de datos de copia para crear y mantener copias en un momento específico (PIT, point-in-time) de los datos. Puesto que estas copias se conservan en almacenamiento inalterable como, por ejemplo, en almacenamiento de objetos en la nube o almacenamiento con capacidad de WORM, son copias “para siempre” que no se pueden modificar. Tal como se muestra en la figura 2, el software de gestión de datos de copia replica los datos en un sitio DR o alternativo, creando las copias PIT. Opcionalmente, también pueden realizarse copias PIT y almacenarlas en el sitio de producción para disponer de una capacidad de restauración rápida.

Cuando un gestor de DR recibe la notificación de que se ha descubierto una filtración de datos o una infección de malware de cifrado, se realiza la prueba automatizada de copias PIT en el sitio de DR para verificar la recuperabilidad de los datos. Mediante el proceso de prueba y verificación se identifica la última copia “limpia” y, a continuación, se recupera en la infraestructura de DR mediante el proceso de recuperación rápida del software de gestión de datos de copia. En el sitio de DR también se pueden llevar a cabo pruebas con frecuencia, para ayudar a garantizar la

recuperabilidad de los datos sin afectar a las operaciones de negocio. Resiliency Orchestration permite asegurarse de que las plataformas se puedan recuperar de forma rápida y en paralelo.

Figura 2: La Recuperación de ciberincidencias para datos proporciona copia de seguridad eficiente de grandes volúmenes de datos con pruebas no disruptivas y restauración rápida.



Los paneles de control e informes simplifican la gestión

La Recuperación de ciberincidencias incluye un panel de control (véase la figura 3) que permite monitorizar los cambios de configuración de la plataforma y de datos. También proporciona actualizaciones de recuperaciones críticas en tiempo real a la dirección o al consejo de dirección, que les permiten tomar rápidamente decisiones bien fundadas.

Un panel de control de ciberincidencias proporciona detalles como el número de vulnerabilidades y nivel de gravedad, y permite realizar el seguimiento de las vulnerabilidades abiertas. Un ciberpanel de control de datos proporciona visibilidad de las desviaciones RPO, las desviaciones RTO, el estado de validación de instantáneas y la ciberpreparación actual.

El módulo incorporado de creación de informes ofrece un amplio conjunto de ellos, incluidos los de resiliencia o posición de DR, que se pueden exportar y compartir con los reguladores a efectos de conformidad, junto con gráficas capturadas durante las operaciones normales de negocio.

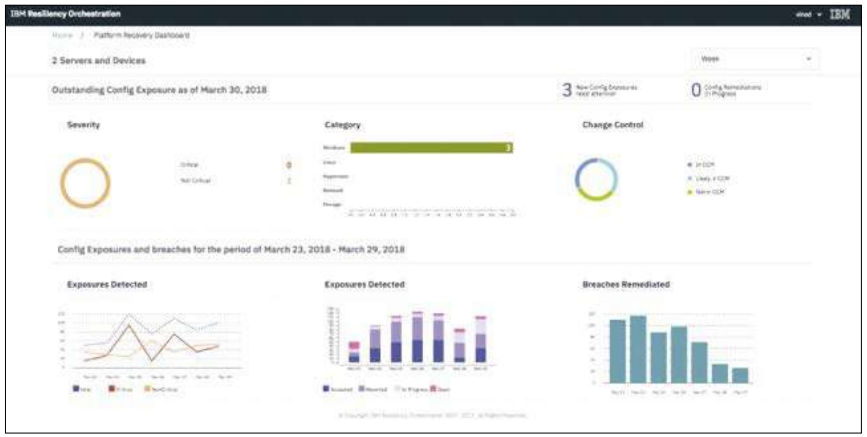


Figura 3: Panel de control central

¿Por qué IBM?

IBM Business Resiliency Services cuenta con casi 60 años de experiencia en ayudar a clientes de todo el mundo a resolver sus necesidades de copia de seguridad y recuperación. En la actualidad, nuestros servicios de gestión de datos y DR protegen a más de 9000 clientes y tenemos más de 3,5 exabytes de datos copiados anualmente y bajo nuestra gestión. Más de 300 IBM Resiliency Centres en más de 60 países de todo el mundo proporcionan protección de datos y DR gestionada y más de 6000 profesionales de IBM en el mundo están dedicados a la resiliencia.

¿Quiere conocer más sobre Cyber Incident Recovery y saber cómo IBM puede ayudar a su empresa?

Hable con un especialista

IBM **Global**
Technology Services

IBM España, S.A
Tel.: +34-91-397-6611 Santa Hortensia, 26-28 28002
Madrid
Spain

La página de inicio de IBM se encuentra en: ibm.com

Este documento es válido en la fecha inicial de publicación y puede estar sujeto a cambios por parte de IBM en cualquier momento. No todas las ofertas están disponibles en todos los países en los que IBM opera.

LA INFORMACIÓN DE ESTE DOCUMENTO SE PROPORCIONA “TAL CUAL” SIN GARANTÍA DE NINGÚN TIPO, NI EXPLÍCITA NI IMPLÍCITA, INCLUYENDO, PERO NO LIMITÁNDOSE, A LAS DE COMERCIALIZACIÓN, ADECUACIÓN A UN PROPÓSITO Y A LAS GARANTÍAS O CONDICIONES DE NO INFRACCIÓN. Los productos de IBM se garantizan con arreglo a los términos y condiciones de los acuerdos bajo los cuales se proporcionan.

El cliente es responsable de asegurar su propio cumplimiento de los requisitos legales vigentes. IBM no proporciona asesoramiento legal ni representa o garantiza que sus servicios o productos aseguren el seguimiento por parte del cliente de cualquier legislación vigente.

Por favor, recicle