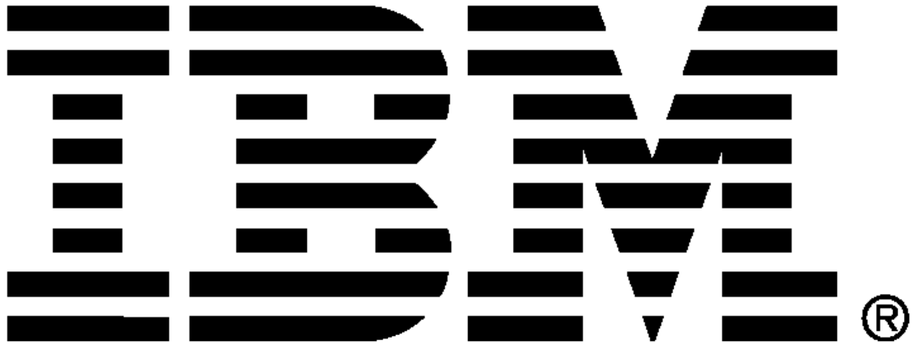
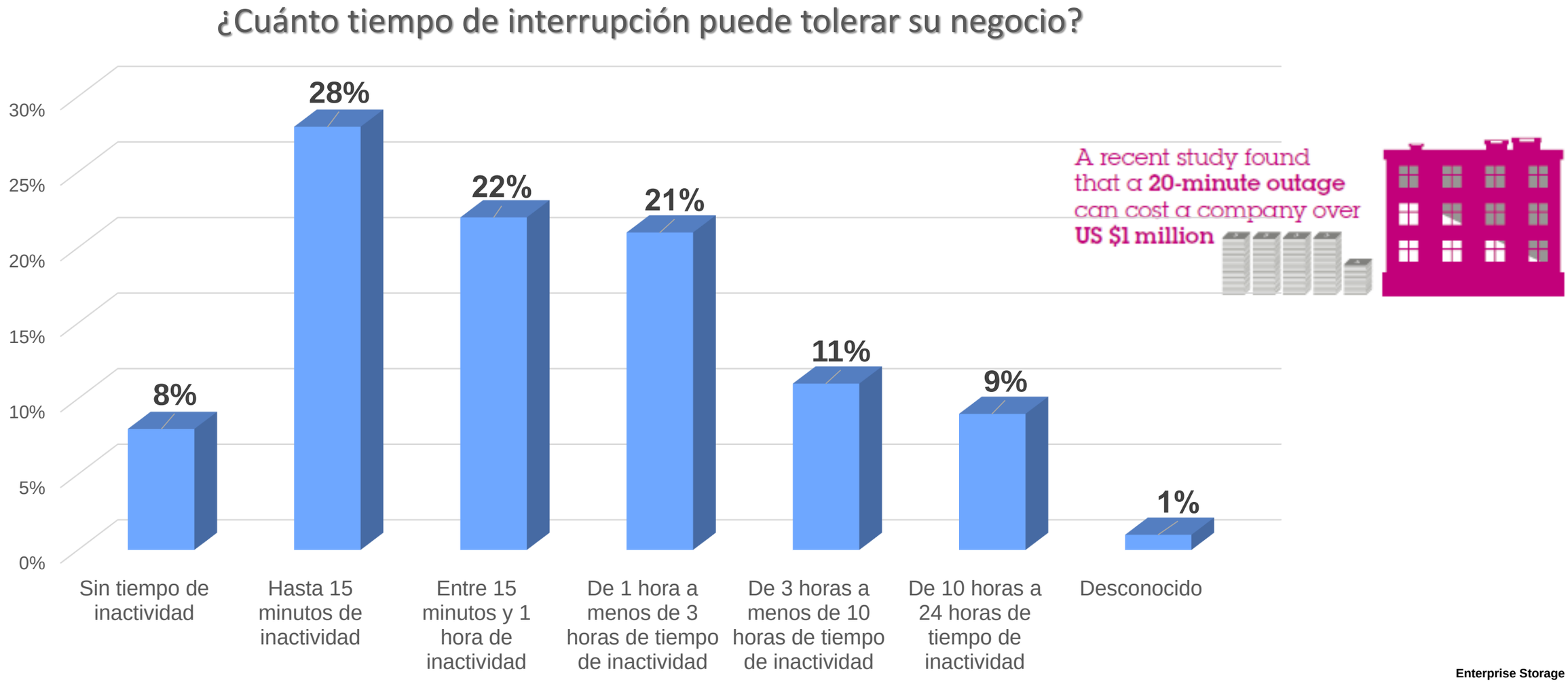
Recuperación ante desastres y Ciber Resiliencia



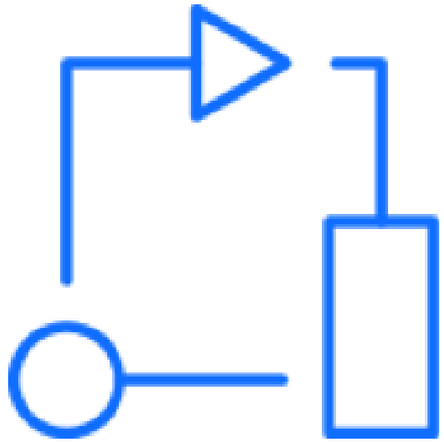
Global, continuo, intensivo en datos, accesible y social….

Son cualidades del negocio digital que generan muchas más causas de disrupción en el negocio



El desafío de recuperar aplicaciones rápidamente

Los entornos dinámicos frustran las actividades de recuperación de aplicaciones de aplicaciones, los *runbooks* obsoletos son comunes.



La recuperación es demasiado larga y tiene fallas frecuentes debido a operaciones manuales pesadas. Se vuelve más desafiante en los ciber ataques.

Las pruebas cargan de trabajo a las organizaciones.

Las regulaciones imponen nuevos requisitos:

- Sheltered Harbor necesita un sitio de terceros
- Norma 4511 de FINRA, Regla 17a-4 de la SEC, HIPAA, Directiva de Protección de Datos, GDPR, Apéndice FFIEC J

Las operaciones manuales son el obstáculo más frecuente !

¿Qué es la orquestación del Disaster Recovery?

Mientras que los servicios tradicionales se ejecutaban únicamente a partir de centros de datos centrales diseñados para arquitecturas cliente / servidor o mainframes, en la actualidad se están utlizando entornos mixtos con servicios tradicionales y cloud híbridas.

IBM Cloud Resiliency Orchestration (CRO) permite automatización completa de operaciones, testeo, monitorización única y reporte de resultados para entornos híbridos complejos. Es escalable y construido sobre estándares de la Industria. Está soportado 24x7. Contempla la práctica totalidad de plataformas y aplicaciones de mercado

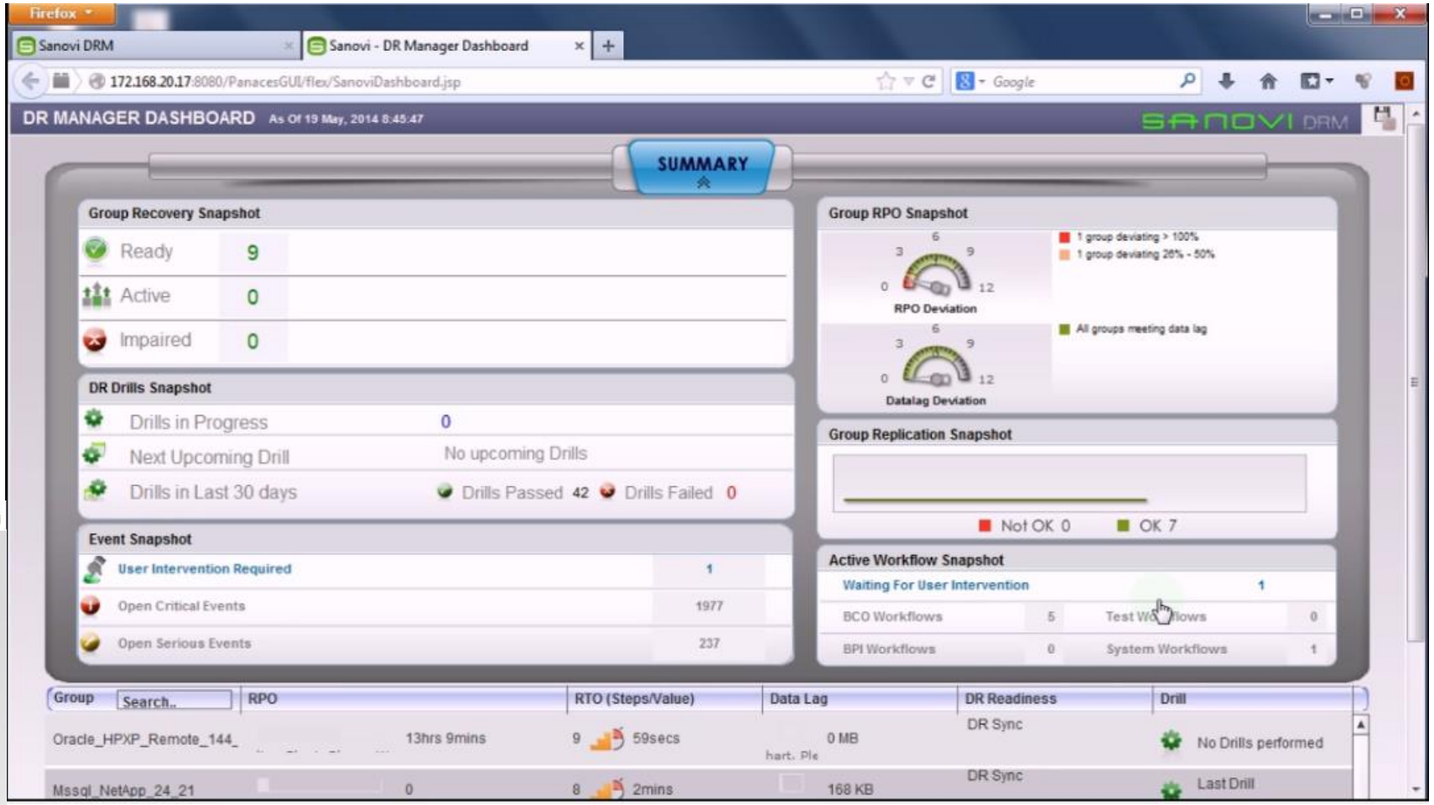
Se ha diseñado para posibilitar implantaciones más rápidas y menos costosas y permitir una gestión más segura, facilitar los test, identificar las inconsistencias entre DC principal y DR y ejecutar una rápida recuperación en contingencia. Además permite la lectura de parámetros generales, difíciles de medir en otras circunstancias

YouTube **CLOUD RESILIENCY ORCHESTRATOR HOW IT WORKS?**

Platforms	Applications	Replication
+ Linux flavors	+ WebSphere	+ NetApp SnapMirror
+ Windows	+ WebLogic	+ EMC SRDF, RecoverPoint
+ AIX, HP UX	+ IIS	+ HP Continuous Access
+ Z OS	+ SAP	+ IBM Global Mirror, SVC
+ Solaris	+ MQ Server	+ Hitachi TrueCopy/UR
+ Oracle Exadata	+ Oracle	+ Database Native Replications
+ FlexPod	+ SQL Server	+ Oracle Dataguard, SQL Log Shipping, Mirroring etc.
+ VMware	+ IBM DB2	
+ AWS	+ PostgreSQL	
	+ MySQL	
	+ MS Exchange	

Cloud Resiliency Orchestrator: Cuadros de mandos de gestión

CRO proporciona cuadros de mandos tanto en alcances de CIO como de responsable o técnico de sistemas.



Los **cuadros de mandos** pueden reflejar desde el estado de la capacidad de contingencia, como la evolución de una entrada en contingencia, e identificar los tiempos de ejecución y resultantes para cada actividad que se haya definido en los workflows.

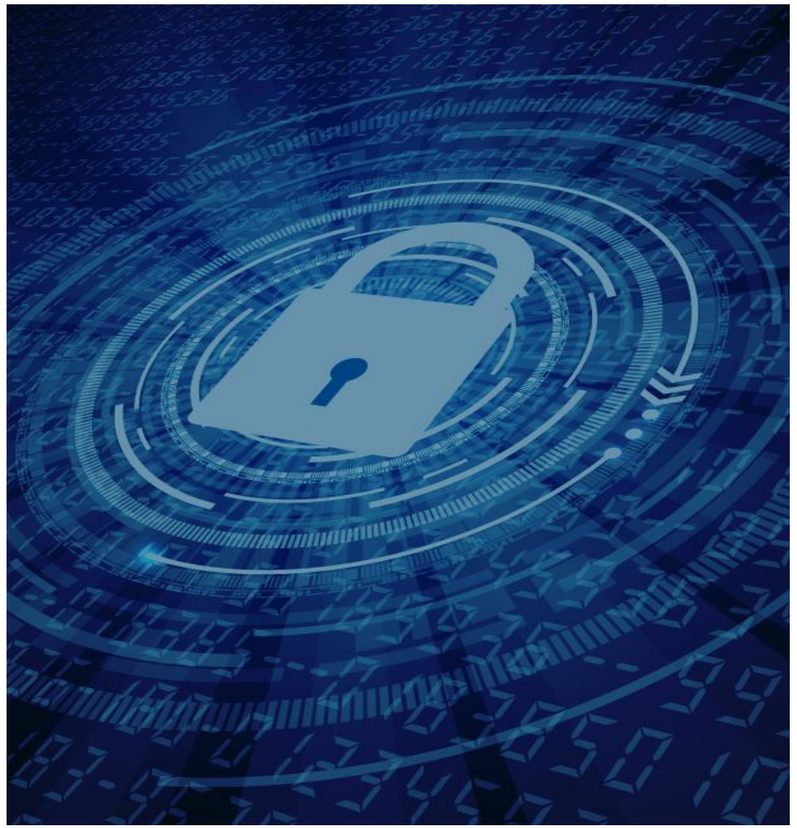
Cloud Resiliency Orchestrator: Menu Principal

Cyber Resilience - Introduction

Prepare for **WHEN**, not **IF**

Ciber Resiliencia

La ciber Resiliencia es la capacidad de una organización para continuar sus operaciones con la menor cantidad de interrupciones frente a los ataques cibernéticos. Es un enfoque de extremo a extremo que reúne tres áreas críticas: la seguridad de la información, la continuidad del negocio y la capacidad de recuperación de las redes de las empresas; para garantizar que las organizaciones sigan funcionando durante los ciberataques.



Ciber Seguridad

La seguridad informática está diseñada para proteger sistemas, redes y datos de delitos cibernéticos. La ciber seguridad efectiva reduce el riesgo de un ciberataque y protege a las organizaciones de la explotación deliberada de sus activos.

Continuidad de negocio

La continuidad del negocio proporciona la capacidad de reanudar las operaciones cuando un evento causa una interrupción del servicio. Los planes para la continuidad del negocio abordan catástrofes naturales, accidentes y ataques físicos deliberados; pero ahora, también deben apoyar la reanudación de las operaciones después de ciber-ataques

¿Por qué la ciber-resiliencia es necesaria?

Los ciberataques evolucionan y van en aumento

TOP 5 de causas de las ciber-rupturas

61% Phishing e ingeniería social

45% Malware

37% Spear-phishing attack

24% Negación de servicio

21% Software desactualizado

Las organizaciones no están preparadas

68% No tiene la capacidad de mantenerse resistente a raíz de un ciberataque

66% Sufrir de una planificación y preparación insuficientes

75% Tener planes de respuesta a ciber incidentes de seguridad ad-hoc, inexistentes o inconsistentes

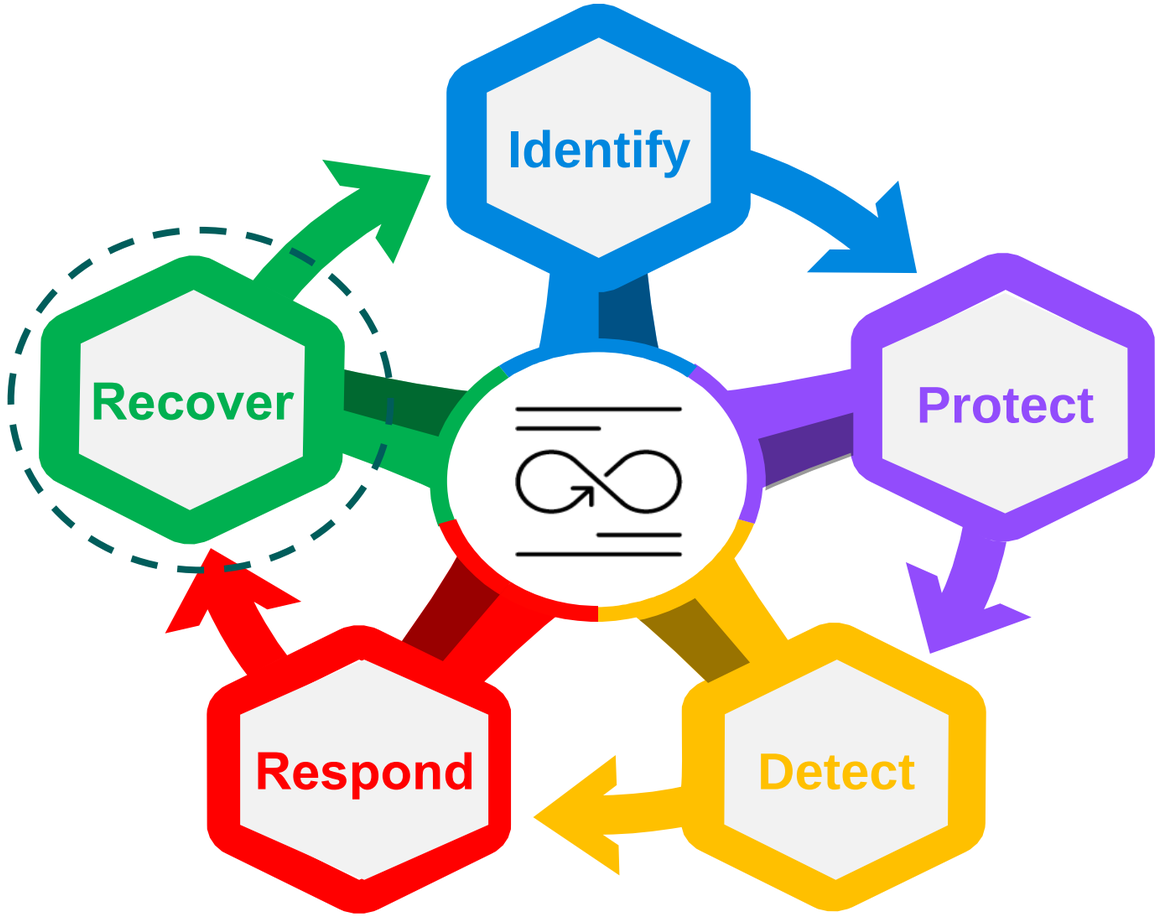
191 días Promedio de tiempo que los hackers ocupan los entornos de TI antes del descubrimiento

* Integration planned

IBM aborda la ciber resiliencia a través de una metodología completa

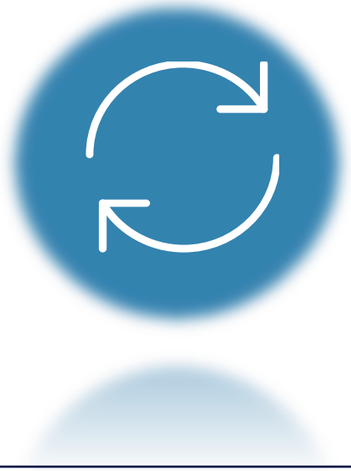
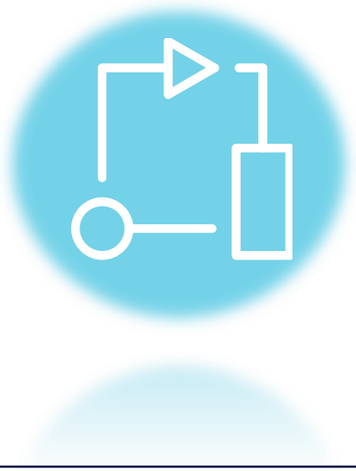
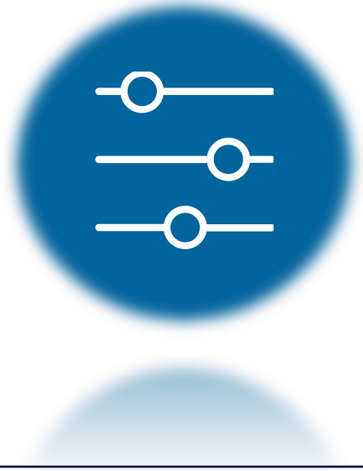
Basado en el NIST Cyber Security Framework (NIST CSF), el ciclo de vida de ciber-resiliencia de IBM permite a las organizaciones mejorar su robustez cibernética en cinco fases:

- ✓ **Identificar** definiendo una hoja de ruta y un plan de acción para construir o mejorar el plan de ciber-resiliencia de la organización.
- ✓ **Proteger** a la organización de ataques descubriendo vulnerabilidades antes de que sean explotadas.
- ✓ **Detectar** amenazas desconocidas con análisis avanzados.
- ✓ **Responder** efectivamente a los brotes cibernéticos.
- ✓ **Recuperar** el acceso a datos y aplicaciones críticas.



IBM aborda la ciber resiliencia con prácticas de última tecnología

Para lograr operaciones comerciales continuas, las organizaciones necesitan soluciones de recuperación de desastres y recuperación de incidentes cibernéticos que pasen de métodos manuales a modelos de automatización y orquestación.

Completa automatización del ciclo de vida de DR	Resiliencia definida por software	Flujos de trabajo inteligentes	Dashboard único
			

Overview: Recuperación de ciber incidentes para datos y configuración de plataformas

IBM Cloud Resiliency Orchestrator (CRO), se ha mejorado para utilizar backup/datos replicados con Air Gap para proteger contra cortes cibernéticos.

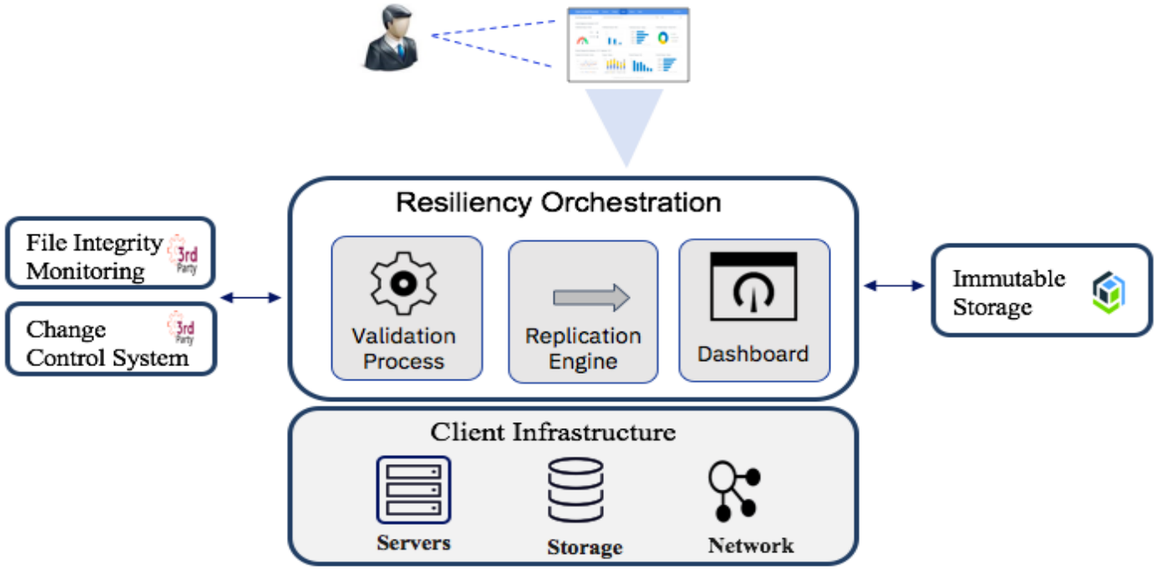
Características principales

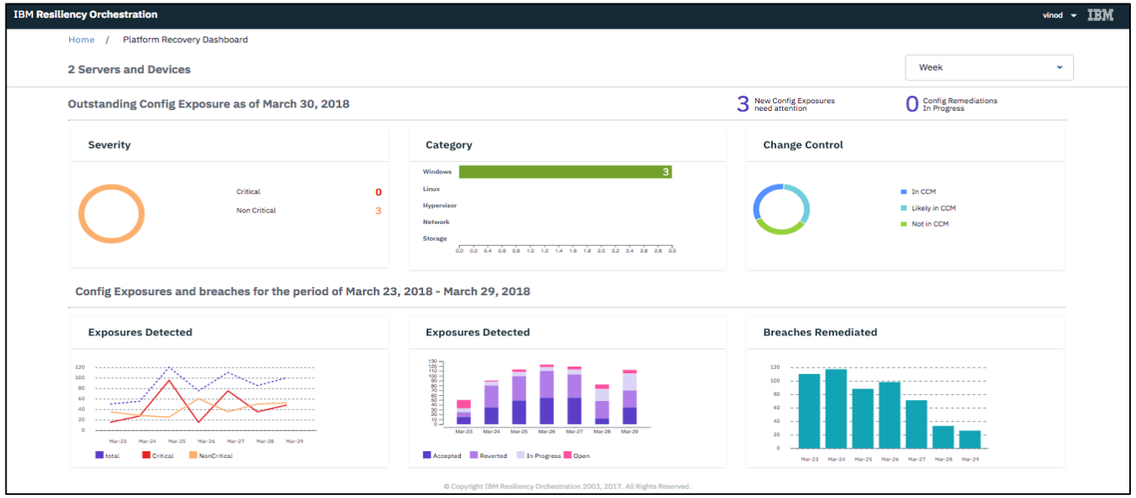
- El acceso vía Air-Gap reduce el riesgo de corrupción del backup.
- La recuperación rápida reduce el tiempo de inactividad y garantiza el RPO mínimo
- Recuperación eficiente en un punto en el tiempo con tecnologías de gestión de datos de copia.
- Almacenamiento inmutable para evitar la corrupción de la copia de seguridad.

Recuperación de la **configuración de plataformas** ante ciber-incidentes

Características principales

- Protección de configuraciones de dispositivos mediante Air-gap, copia de máquinas virtuales y sistemas bare metal a Inmutable Storage con IBM Resiliency Orchestration replication
- La identificación temprana de anomalías en la configuración de la plataforma permite responder de inmediato y orquestar la recuperación con la inteligencia incorporada de Resiliency Orchestration (CRO)
- Restauración rápida de las configuraciones del dispositivo en la infraestructura de producción por CRO
- Restauración rápida de las configuraciones de máquina virtual y bare metal server en infraestructura de producción limpia
- Funcionalidad de pruebas inmediatas, para probar la solución con frecuencia sin afectar la producción
- Proporcionar visibilidad e informes en el proceso para garantizar el grado de cumplimiento y conformidad normativa

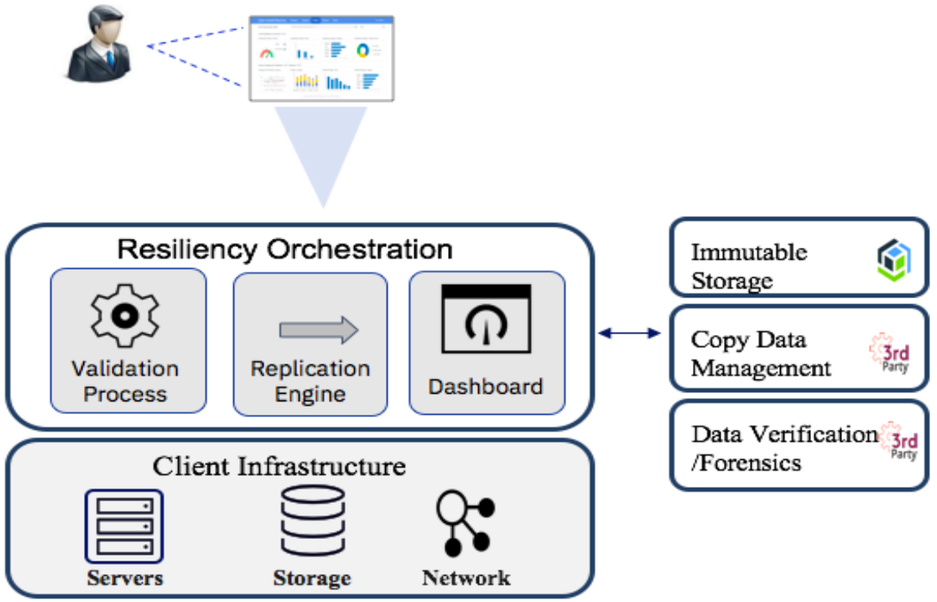


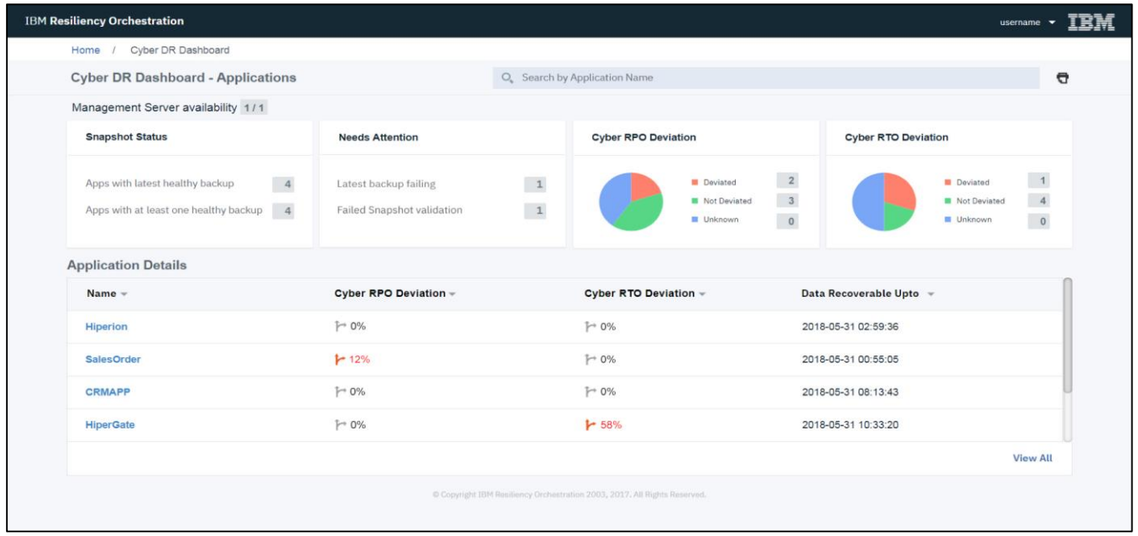


Recuperación de **datos** frente a ciber-incidentes

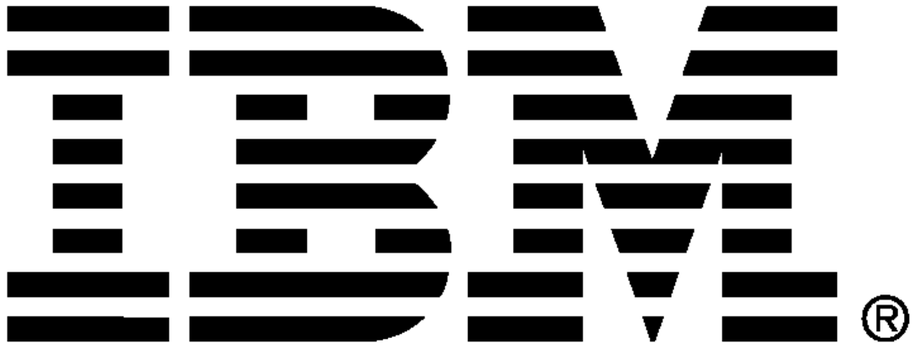
Características principales

- Protección de máquinas virtuales y datos mediante herramientas de Copy Data Management y almacenamiento inmutables
- La detección de anomalías en los datos mediante la integración de múltiples herramientas propias o de terceros, reduce significativamente los daños causados
- Rápida recuperación de copias limpias en la infraestructura de recuperación de desastres
- Además se pueden restaurar copias limpias en infraestructura de producción opcionalmente
- Proporcionar visibilidad e informes en el proceso para garantizar el cumplimiento y la preparación
- Proporcionar visibilidad e informes en el proceso para garantizar el grado de cumplimiento y conformidad normativa





Recuperación ante desastres y Ciber Resiliencia



Links

Business Resiliency Services

DRaaS

Cloud Resiliency Orchestration