kyndryl

Resiliency Orchestration con Cyber Incident Recovery

Ciberresiliencia desarrollada a medida para una recuperación rápida, fiable y escalable en entornos multinube híbridos

Contenidos

Es posible que necesite un cambio

Cuanto más atraviesen sus datos y aplicaciones una infraestructura cada vez más interconectada de entornos locales, de nube pública y multinube, más formas tienen los ejecutores de ciberataques de interrumpir la continuidad de su empresa. La naturaleza compleja de los entornos multinube híbridos expone sus datos críticos y las configuraciones del sistema a niveles de riesgo más elevados que nunca, tanto es así que la probabilidad de un ciberataque exitoso se ha convertido en una certeza absoluta. Por más atento que esté su equipo de seguridad de TI, un ciberataque terminará provocando una interrupción de la actividad comercial en forma de corte, robo o corrupción de datos, causando daños a la reputación y consecuencias financieras.

En un pasado no muy lejano, se podía contar con las soluciones tradicionales de recuperación de desastres para ayudar a mitigar los daños de la mayoría de los ciberataques convencionales. Pero eso fue mucho antes de que los entornos multinube híbridos fueran una realidad. Mientras que las infraestructuras de TI han crecido en complejidad, los ejecutores de ciberataques también se han vuelto más sofisticados. Hoy en día, el cifrado de datos y los ataques de malware se diseñan para encontrar copias de seguridad de datos de una forma que antes era inimaginable. Por consiguiente, estos ataques están logrando acceder a la ubicación de la copia de seguridad y de la recuperación de desastres, dejando tanto los datos primarios como la copia de seguridad inutilizables, lo cual retrasa significativamente la capacidad de restaurar las operaciones al nivel de producción.

Kyndryl Resiliency Orchestration con Cyber Incident Recovery minimiza el impacto de los ciberataques en la empresa con su recuperación rápida, fiable y escalable en entornos multinube híbridos.

Recuperación cibernética a medida para un mundo multinube híbrido
Kyndryl™ Resiliency Orchestration con Cyber Incident Recovery puede recuperar la configuración de sus datos y su plataforma a gran velocidad en caso de producirse un corte cibernético. Proporciona una automatización inteligente de los flujos de trabajo de protección de datos y recuperación de desastres, y permite pruebas de recuperación, la inmutabilidad de los datos y la detección, supervisión, gestión y reporte de anomalías en entornos multinube híbridos . La solución ofrece una recuperación automatizada, fiable y rápida de las cargas de trabajo físicas y virtuales, incluidos los procesos, las aplicaciones, los sistemas y las bases de datos de la empresa frente a los ciberataques.

Cyber Incident Recovery proporciona:
- Función de pruebas sencilla que no afecta los entornos de producción
- Detección más rápida de la corrupción de datos y respuesta inmediata para reducir el tiempo de inactividad
- Recuperación eficiente a un momento dado (PIT) que optimiza los objetivos del punto de recuperación (RPOs)
- Escalabilidad para manejar grandes detecciones y recuperaciones a nivel de sitio en minutos
- Visibilidad e informes simplificados que ayudan a cumplir con los requisitos reglamentarios

Kyndryl Resiliency Orchestration con Cyber Incident Recovery ofrece una recuperación automatizada, fiable y rápida de las cargas de trabajo físicas y digitales frente a los ciberataques.

Una arquitectura que permite un enfoque ágil de la ciberresiliencia

Los bloques de construcción de tecnología que conforman la función Cyber Incident Recovery proporcionan una plataforma que abarca las capas de computación y datos de los entornos de producción y recuperación de desastres. Esto permite un enfoque ágil de la recuperación en sus cargas de trabajo virtuales y físicas.

Almacenamiento inmutable
El uso de la tecnología de almacenamiento inalterable para los datos de configuración o el almacenamiento de escritura única y lectura múltiple (WORM) para los datos de las aplicaciones ayuda a evitar la corrupción y a garantizar la facilidad de recuperación al no permitir que se realicen cambios en las copias de seguridad una vez guardadas. Para los datos de las aplicaciones, este enfoque también ayuda a reducir sus costos de almacenamiento mediante la escritura de nuevas copias de los cambios incrementales en un momento dado.

Protección por air-gap
El aislamiento de red separa los entornos de producción del almacenamiento WORM que contiene los datos protegidos y respaldados en un sitio remoto o de recuperación de desastres (DR). El acceso al almacenamiento WORM también está restringido solo a los momentos en que los datos están disponibles para la copia de seguridad. Este enfoque, combinado con el almacenamiento inmutable, ayuda a evitar que los datos protegidos se corrompan debido al malware que pueda atravesar las redes o que esté diseñado específicamente para encontrar la copia de seguridad de los datos.

Detección de anomalías
Kyndryl Resiliency Orchestration incluye una función de detección de anomalías que utiliza la identificación heurística basada en reglas, mejorada con inteligencia artificial.Se entrena en diferentes patrones de cambio del malware identificado, capta y compara los patrones de cambio en los datos guardados como copia de seguridad para prever las anomalías de los datos con gran precisión. Esta capacidad de detección de anomalías en el sitio de DR ayudará a identificar las instantáneas de copia de seguridad anómalas y a restaurar a partir de copias limpias.

Verificación de datos de configuración
Este componente utiliza la capacidad incorporada de detección de anomalías basada en la IA para ayudar a garantizar que la configuración o los datos que se protegen estén limpios y sean recuperables.
El proceso, integrado en Resiliency Orchestration, detectará automáticamente cuando sus configuraciones del sistema hayan sido modificadas. Resiliency Orchestration también se integrará con los scripts de validez de la aplicación suministrados por el cliente para proporcionar pruebas a nivel de aplicación y de datos.

Automatización y orquestación
Al automatizar el proceso de recuperación de extremo a extremo de los datos y las aplicaciones, Resiliency Orchestration permite una rápida restauración de su entorno de TI. Resiliency Orchestration sustituye los procesos manuales tradicionales por flujos de trabajo predeterminados que han sido probados y validados, permitiéndole recuperar todo un proceso empresarial, una aplicación, una base de datos o un sistema discreto con solo pulsar un botón. Estos flujos de trabajo orquestan los diversos pasos necesarios para recuperar sistemas y datos interconectados, limitando el error humano. Resiliency Orchestration ayuda a la implementación de una solución rápida aprovechando una amplia biblioteca de más de 800 patrones predefinidos que pueden combinarse para construir flujos de trabajo.

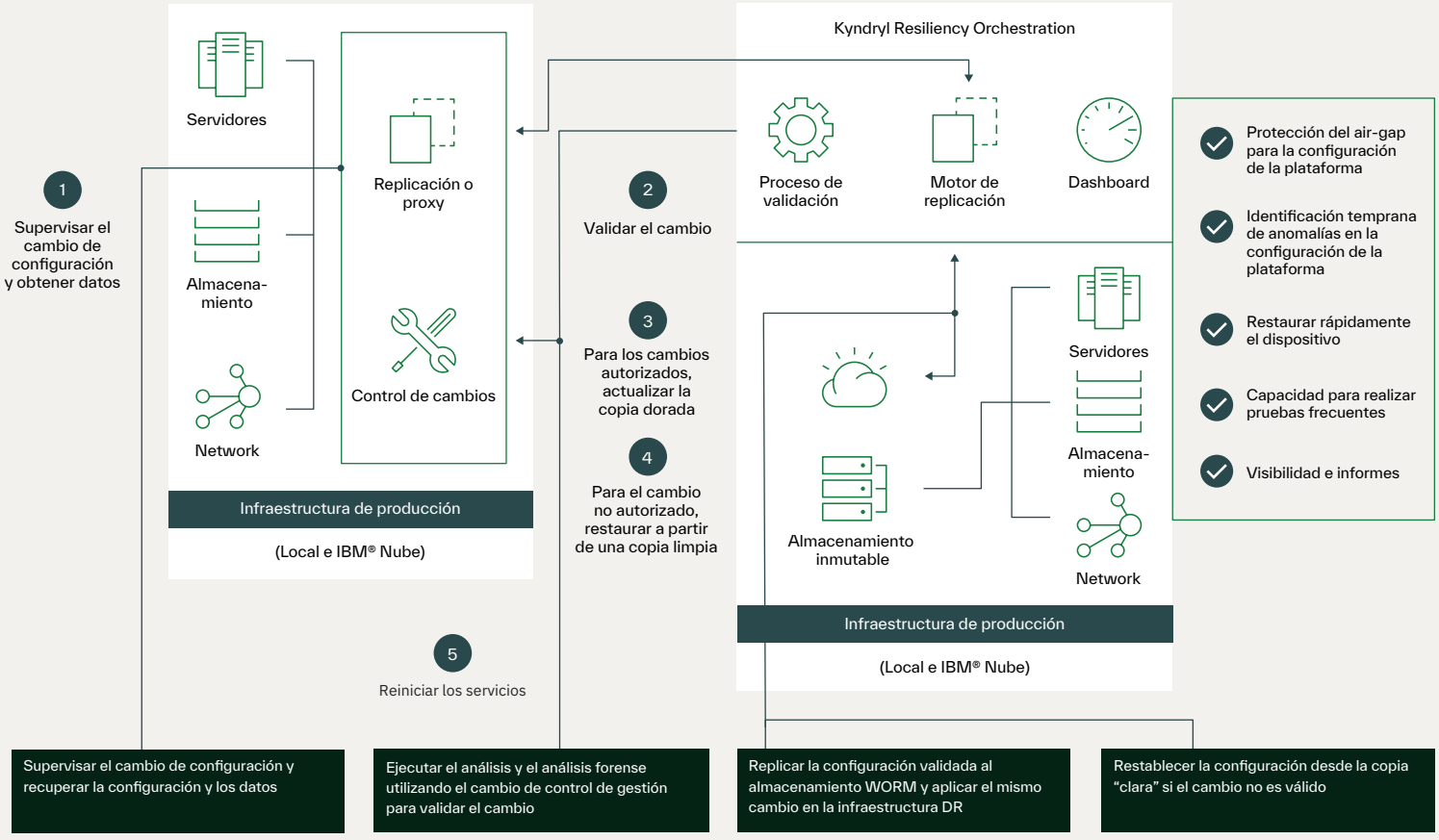
Cyber Incident Recovery para la configuración de la plataforma

El malware generalmente altera las configuraciones antes de corromper los datos mismos, por lo cual es crítico para detectar cualquier cambio de configuración antes de que los datos reales se infecten. La característica de configuración de plataforma de Cyber Incident Recovery protege los datos de configuración de las cargas de trabajo virtuales y físicas, las aplicaciones, los sistemas de almacenamiento y los dispositivos de red en todos los entornos locales, de nube pública, nube híbrida y multinube.

La empresa en marcha con una "copia dorada"
Este componente utiliza las tecnologías incorporadas para identificar cualquier cambio en las configuraciones de los puntos finales de producción y alerta al usuario de cualquier cambio autorizado y no autorizado. Las alertas también pueden proporcionar tickets del software de gestión de control de cambios. Para permitir un rápido restablecimiento de los servicios, Cyber Incident Recovery replica una "copia dorada" de los datos de configuración del servidor y de los dispositivos en un almacenamiento inmutable protegido por air-gap.

Respuesta a los cambios de configuración válidos y no válidos
En el caso de un cambio válido, los datos de configuración se protegen mediante la réplica de una nueva "copia dorada" en un almacenamiento inmutable. Si se identifica un cambio no válido, la última copia limpia de las configuraciones del dispositivo se restablece rápidamente a la Infraestructura de la producción mediante Resiliency Orchestration, basada en políticas preestablecidas y con el correspondiente consentimiento de la gerencia. Las configuraciones de máquinas dedicadas y virtuales se restauran en una Infraestructura de producción limpia. En caso de cambios válidos, se crea una nueva " copia dorada" en un almacenamiento inmutable.

Kyndryl Cyber Recovery as a Service
Cyber Incident Recovery para la configuración de la plataforma



*Air-gap no compatible para el almacenamiento inmutable alojado en la nube

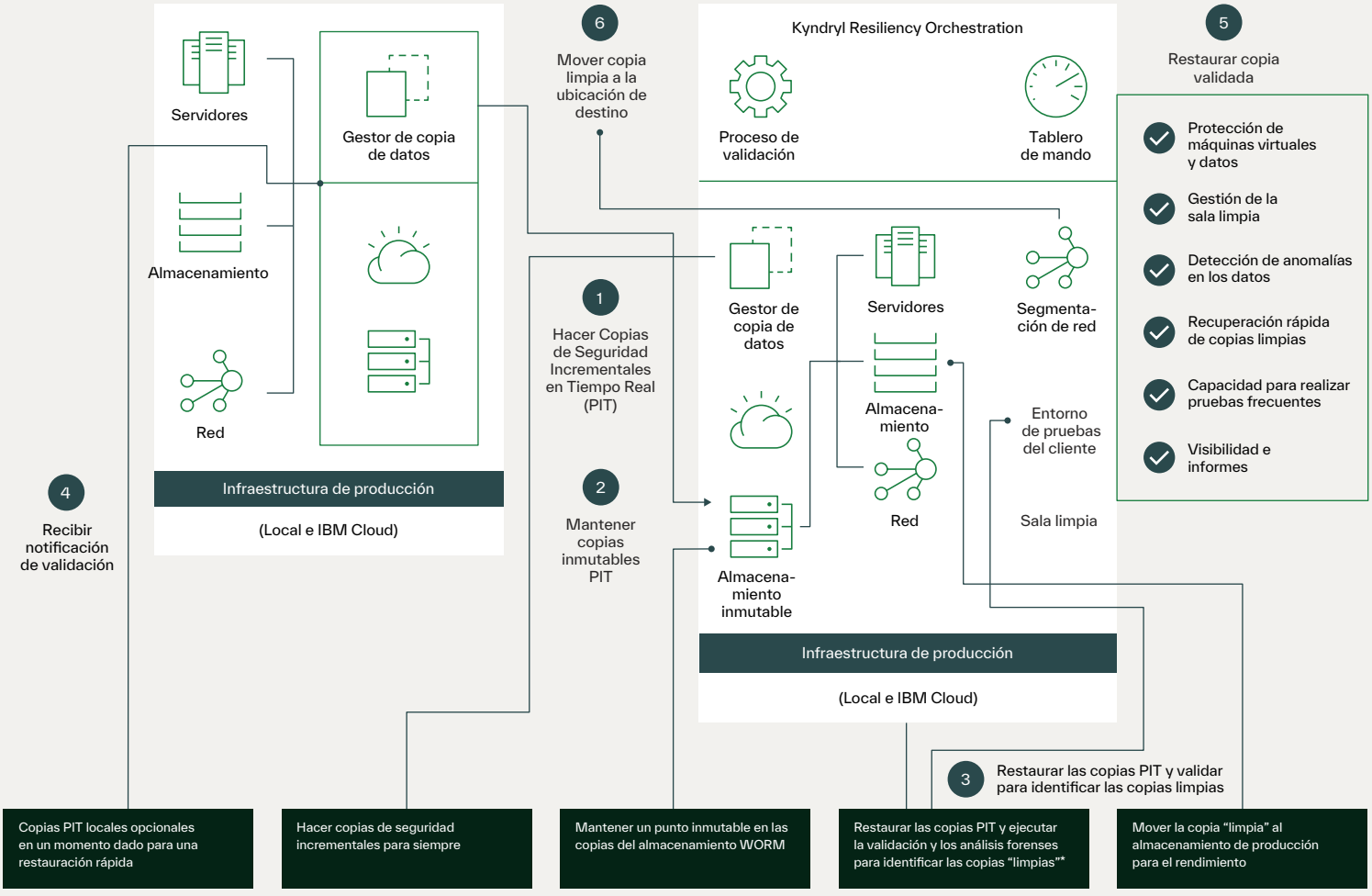
Cyber Incident Recovery para datos

La característica para datos de Cyber Incident Recovery permite una recuperación altamente fiable y rápida frente a los ciberataques que corrompen los datos mismos. Protege los datos mediante el aislamiento físico tipo air-gap y el almacenamiento inmutable, al tiempo que orquesta la recuperación rápida en el sitio de recuperación de desastres.

Protección de grandes volúmenes de datos en todos los entornos
Cyber Incident Recovery está diseñada para manejar grandes volúmenes de datos de aplicaciones, independientemente de dónde se hallen esos datos. Emplea la tecnología Copy Data Management para crear y mantener copias de datos incrementales a un momento dado (PIT). Dado que estas copias se guardan en un almacenamiento inmutable como el almacenamiento de objetos en nube o el almacenamiento con función WORM, son copias "para siempre" que no se pueden cambiar. El software Copy Data Management replica los datos a un sitio de recuperación de desastres o a una ubicación alternativa, creando las copias PIT . Las copias PIT también pueden hacerse y almacenarse en el sitio de producción para la función de restauración rápida.

Respuesta rápida a los ciberataques para mantener la continuidad del negocio
Cuando un gestor de recuperación de desastres recibe una notificación de que se ha descubierto una filtración de datos o una infección cifrada de malware, se realiza una prueba automática de copias PIT en el sitio de recuperación de desastres para verificar la factibilidad de la recuperación de los datos . El software Resiliency Orchestration recupera en la infraestructura de recuperación de desastres la última copia "limpia" identificada por el proceso de prueba y verificación. También pueden llevarse a cabo con frecuencia pruebas en el sitio de recuperación de desastres, lo que ayuda a asegurar la factibilidad de la recuperación de los datos sin afectar las operaciones de la empresa. Resiliency Orchestration ayuda a garantizar que las plataformas puedan recuperarse rápidamente, en paralelo.

Kyndryl Cyber Recovery as a Service
Cyber Incident Recovery for Data



Paneles e informes que simplifican la gestión

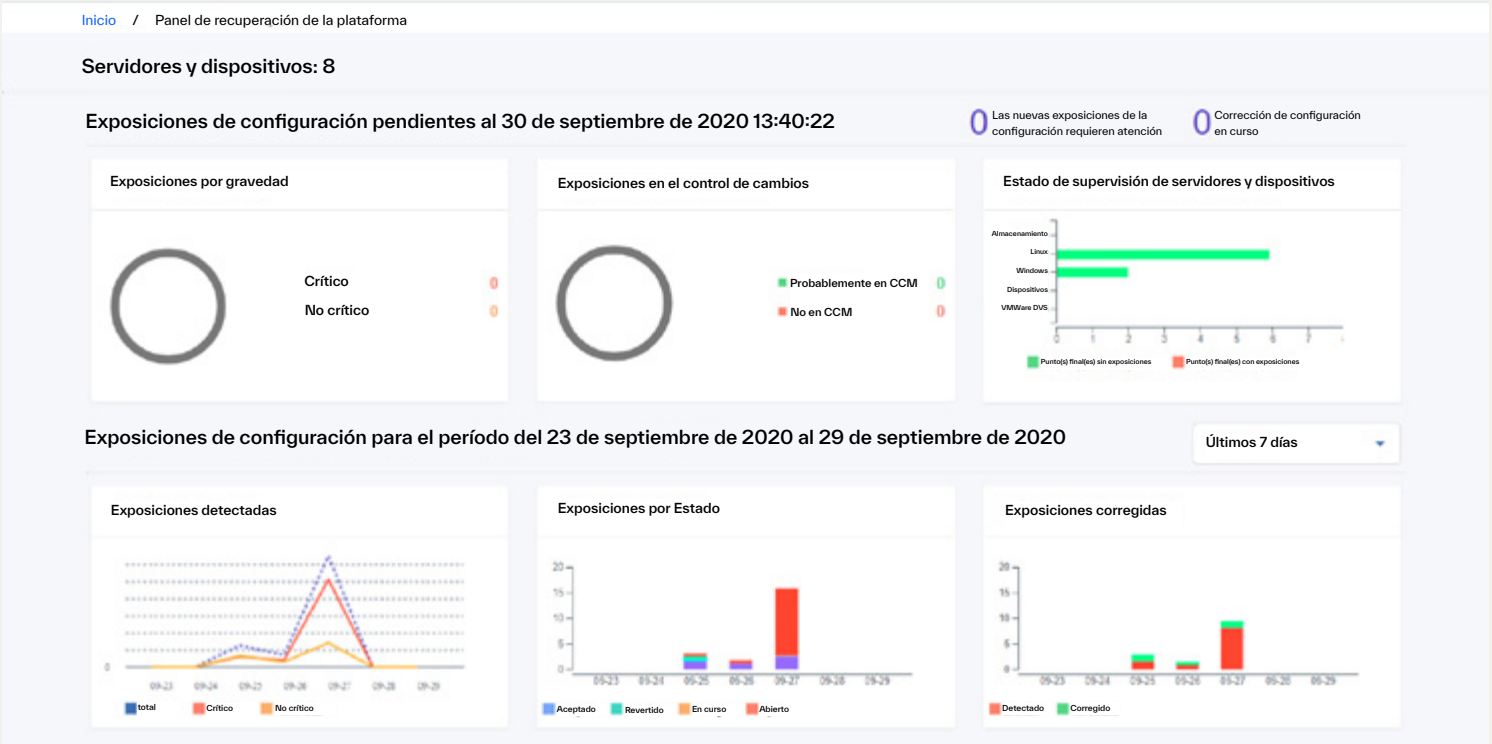
Cyber Incident Recovery incluye un panel que simplifica la gestión de la recuperación cibernética y el seguimiento de los cambios de configuración de la plataforma y de los datos. Proporciona visibilidad en tiempo real de las desviaciones del RPO y el RTO, del estado de validación de las instantáneas y de las actualizaciones críticas de la recuperación cibernética.

Mientras tanto, los altos directivos o la junta directiva pueden recibir actualizaciones de recuperación cibernética crítica en tiempo real para una toma de decisiones más rápida e informada.

Mejor seguimiento de las vulnerabilidades y mayor visibilidad
El panel de Cyber Incident Recovery le indica el número de vulnerabilidades de sus entornos, además del nivel de gravedad de cada una de ellas. Usted puede realizar un seguimiento de las vulnerabilidades abiertas y tomar decisiones informadas en función de la visibilidad de la desviación del RPO cibernético, la desviación del RTO cibernético, el estado de validación de las instantáneas y la preparación cibernética actual.

Sólida función de generación de informes
El módulo de informes incorporado ofrece un amplio conjunto de informes, incluida la postura de ciberresiliencia o de recuperación de desastres, que pueden ser exportados y compartidos con los entes reguladores a los efectos del cumplimiento, junto con los gráficos capturados durante las operaciones normales de la empresa.

Cyber Incident Recovery proporciona visibilidad en tiempo real de las desviaciones del RPO y RTO, el estado de validación de las instantáneas y las actualizaciones críticas



Kyndryl Business Resiliency Services tiene décadas de experiencia ayudando a clientes de todo el mundo con sus necesidades de copias de seguridad y recuperación.

Beneficios de Kyndryl
- Experiencia en todo el ciclo de vida de la resiliencia
- Recuperación automatizada de cargas de trabajo físicas, virtuales y en la nube
- Más de 800 patrones predefinidos para una implementación y escalabilidad más rápida y eficiente
- Elección de nubes, incluidas AWS, Azure e IBM Cloud, para la escalabilidad de la empresa

Confiable
- Más de 9.000 clientes están protegidos con los servicios de recuperación de desastres y gestión de datos de Kyndryl
- Kyndryl cuenta con más de 3,5 exabytes respaldados anualmente y bajo gestión

Alcance global
- Hay más de 300 IBM Resiliency Centers en más de 50 países de todo el mundo
- IBM dedica más de 6.000 profesionales en todo el mundo a la resiliencia

¿Por qué elegir Kyndryl?

Kyndryl cuenta con una vasta experiencia en el diseño, la ejecución y la gestión de la infraestructura tecnológica más moderna, eficiente y confiable de la que el mundo entero depende cada día. Estamos profundamente comprometidos con la promoción de la infraestructura crítica, que impulsa el progreso humano. Construimos sobre nuestra base de excelencia creando sistemas de forma innovadora: incorporando a los socios adecuados, invirtiendo en nuestra empresa y trabajando lado a lado con nuestros clientes para obtener el máximo potencial.

¿Listo para obtener más información?

Para conocer más sobre lo que Kyndryl Resiliency Orchestration con Cyber Incident Recovery puede hacer por usted, póngase en contacto con su representante de Kyndryl o visite www.kyndryl.com

kyndryl

IBM Argentina
Pje. Ing. Enrique Butty 275
C.A.B.A – Argentina

Producido en los Estados Unidos de América
Julio de 2021