Estrategia de Ciberseguridad en los Negocios

Angie Paola Alemán Cardona
Security & Automation Digital Sales Acceleration, MX & SSA

Luisa Maria Lamadrid
Partner Technical Specialist - Security

Kamel Herfaoui Gomez Oliveros
Digital Technical Specialist – Security, LA, SSC

IBM **Security**

IBM

Agenda

1. Slido - Poll
2. Introducción
3. Estrategia de seguridad <IBM>
4. Seguridad de los datos
5. Gestión de identidades
6. Resumen
7. Preguntas

Slido – Poll

slido

Please download and install the Slido app on all computers you use

Join at slido.com
#2919952

ⓘ Start presenting to display the joining instructions on this slide.

slido

Please download and install the Slido app on all computers you use

¿Cuántos días le podría tomar a una empresa identificar una brecha de ciberseguridad relacionada a una explotación de datos?

ⓘ Start presenting to display the poll results on this slide.

slido

Please download and install the Slido app on all computers you use

¿Cuánto le podría costar a una empresa Hispanoamericana un ciberataque de explotación de datos?

ⓘ Start presenting to display the poll results on this slide.

slido

Please download and install the Slido app on all computers you use

¿Cuánto tiempo le puede tomar a un ciberdelincuente generar un mensaje de phishing usando AI?

ⓘ Start presenting to display the poll results on this slide.

slido

Please download and install the Slido app on all computers you use

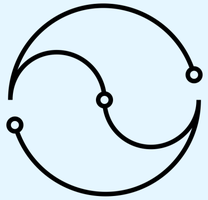
¿La IA Generativa proporcionará una ventaja cibernética general a los atacantes o defensores?

ⓘ Start presenting to display the poll results on this slide.

Estrategia de seguridad <IBM>

Hybrid Cloud

Artificial Intelligence



Hybrid Cloud

La complejidad en la gestión impacta los beneficios netos

Reto: Cumplir con normativas de protección de datos

Problemas de compatibilidad al integrar aplicaciones SaaS con aplicaciones legacy

Aumento de la superficie de ataque, aumenta la exposición a amenazas

Inteligencia artificial

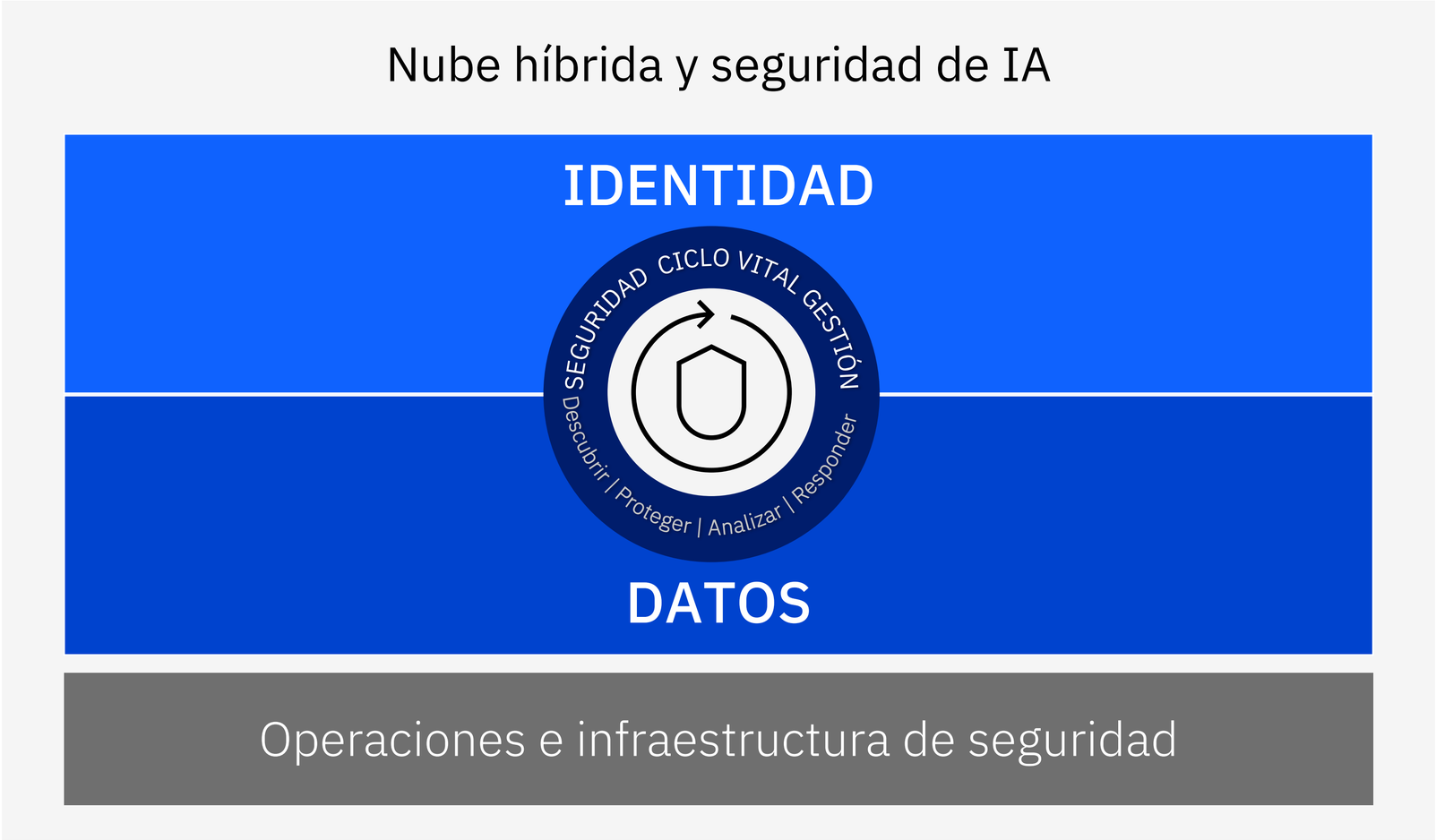
Requiere centralizar grandes cantidades de datos sensibles

Los ciber atacantes pueden explotar las debilidades de los modelos AI para saltar la “baranda”

La tasa de adopción está superando los esfuerzos para hacerlo de manera responsable

Los datos de entrenamiento pueden exponerse involuntariamente a los usuarios

Nube híbrida segura e IA



Costo promedio de una brecha de Seguridad 2023 en Hispanoamérica

*Montos expresados en USD

$3.7M

Incremento del costo para Hispanoamérica año 2023

+31%

¿Porque? – Panorama, ¿Qué esta pasando?

Costo promedio de una brecha de Seguridad 2023

USD 3.69M

Costo promedio de una brecha de seguridad en 2023 en Hispanoamérica

↑+31%

Incremento anual en comparación con 2022 USD $2.8M en la región, Globalmente creció 2.3%

X-Force threat intelligence report 2024

33%

De los casos observados en Latinoamérica estaban relacionados con fugas de datos.

↑14%

Incremento del uso de ataques usando credenciales válidas para 2024.

X-Force threat intelligence report 2024

↓ 15,5%

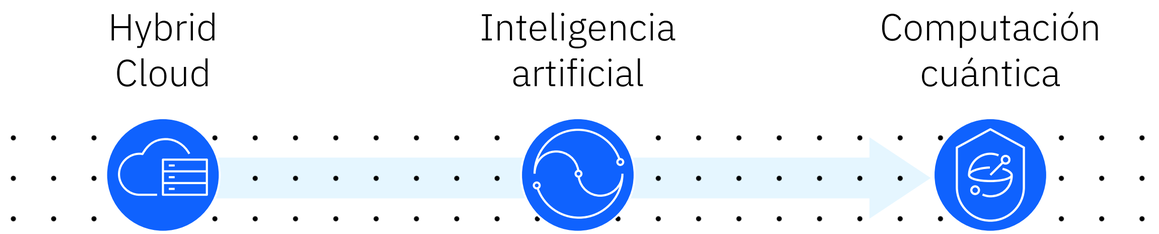
Reducción de los ataques de tipo Ramsoware

Organizaciones ahora con la capacidad de identificar el incidente en tipo real y detenerlo.

La rápida adopción de tecnología está dejando datos sin protección

Los métodos tradicionales de protección de datos deben evolucionar para proteger los datos en la nube, en la IA y en la era cuántica

Las innovaciones tecnológicas impulsan una superficie de amenazas ampliada



Cambio de enfoque de soluciones puntuales a plataformas de seguridad de datos, para simplificar el proceso

Retos de cumplimiento

1000 horas de preparación para auditorías con la regulación actúa.

Nuevas regulaciones que aborden el uso de la IA y, los riesgos de la tecnología cuántica

Exposición de datos

La adopción de la IA generativa y en la nube ha creado una pérdida de visibilidad de dónde se almacenan los datos, quién tiene acceso y cómo se protegen

Las estrategias actuales de cifrado se verá expuesto a la estrategia "Cosechar ahora, descifrar después"

Riesgos de la IA

La IA generativa crea una nueva superficie de amenazas, que debe tener un ciclo de vida de seguridad y gobernanza para protegerse contra los riesgos

Postura de seguridad

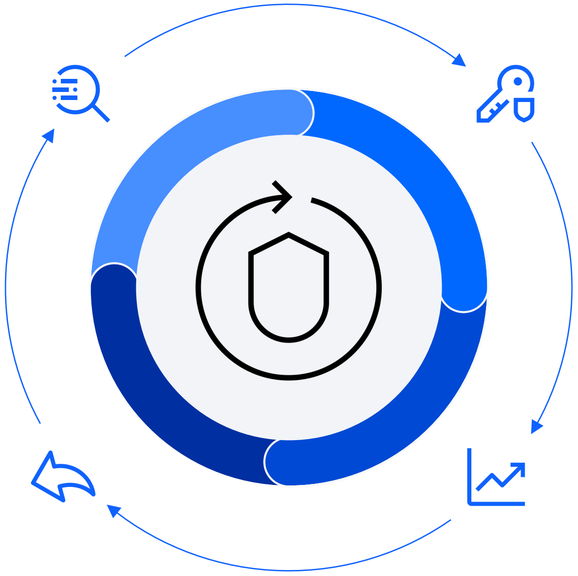
Las organizaciones requieren poder contar con la capacidad de visibilidad, poder priorizar tareas, y como gestionar las brechas de seguridad.

Las soluciones basadas en Silos agravan el problema.

Optimice la protección de datos habilitándolo para innovar

Descubrir

– Descubrimiento y clasificación de datos
– Modelo e inventario criptográfico
– Descubra vulnerabilidades críticas



Proteger

– Proteja los datos con cifrado y gestión de claves
– Defina y aplique políticas de cumplimiento de forma centralizada
– Supervise continuamente la exposición de datos

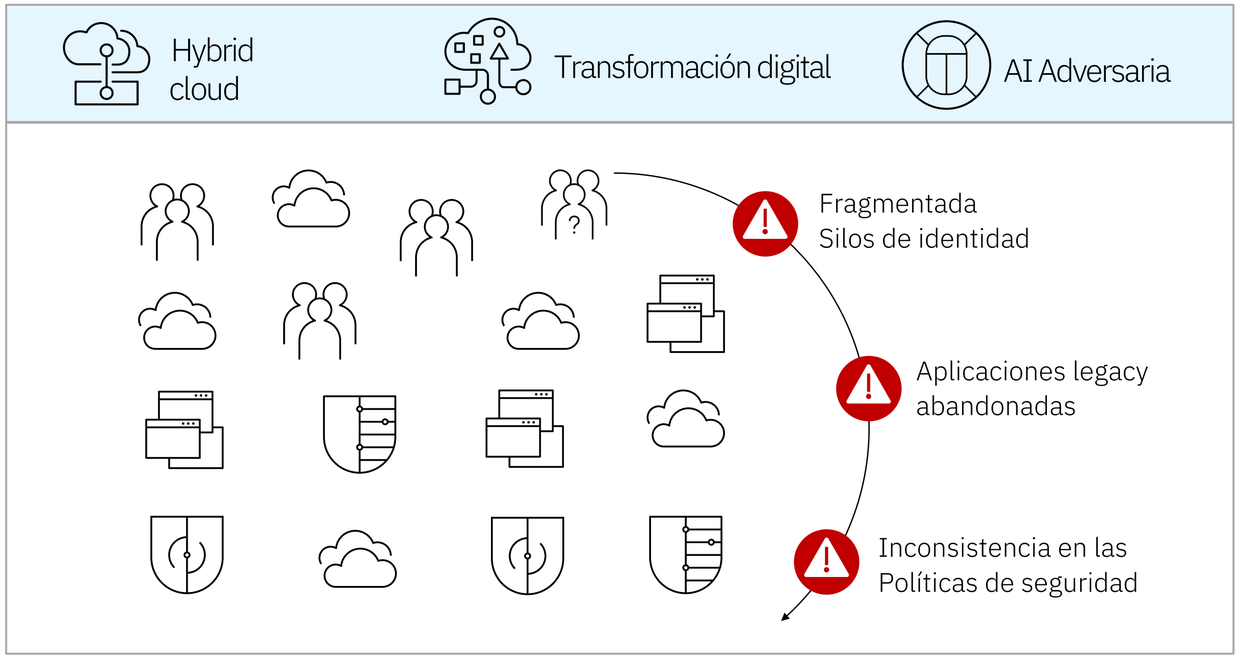
Responder

– Corrija los riesgos priorizados
– Enriquezca las investigaciones de SOC
– Integración con sistemas de flujo de trabajo empresariales (por ejemplo, ServiceNow)

Analizar

– Priorizar riesgos y vulnerabilidades
– Mapear el movimiento y el flujo de datos
– Genere informes y automatice el flujo de trabajo de cumplimiento para auditorías

La modernización de TI deja a las organizaciones con aplicaciones legadas y SaaS.



Experiencia de usuario inconsistente

Las soluciones actuales de gestión de identidades no consideran la experiencia de usuario en el proceso

Elevado riesgo de identidades huérfanas

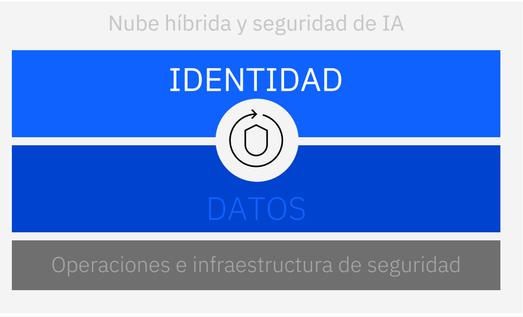
Desconexión de los accesos y las identidades generar una falta de visión completa del comportamiento.

Gestión presupuestal

Restricciones de presupuesto y capacidades de los equipos de seguridad que lleva dejar de lado la protección de aplicaciones legadas.

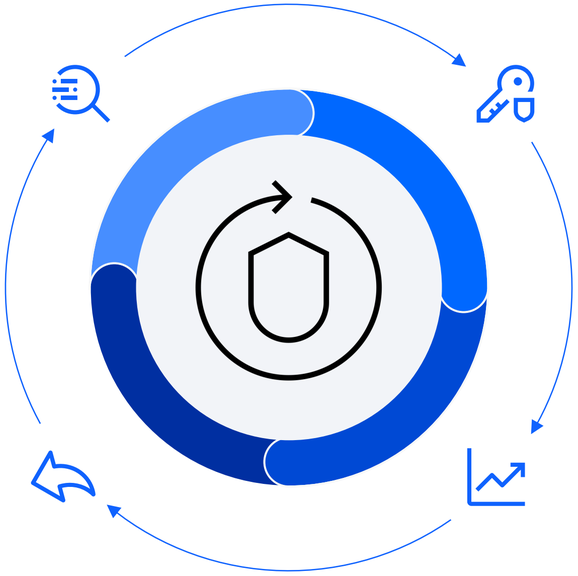
Se necesita una estrategia de identidad simplificada e integrada

Optimice la gestión de identidades híbridas



Descubrir

– Detección de puntos ciegos de identidad
– Proporcionar administración de la postura de identidad
– Identifique la expansión y la complejidad de la identidad



Proteger

– Aprovisionamiento / desaprovisionamiento de usuarios y derechos
– Creación de directivas de acceso y derechos
– Aplicación de la autenticación avanzada
– Integre y automatice flujos de trabajo orquestados

Responder

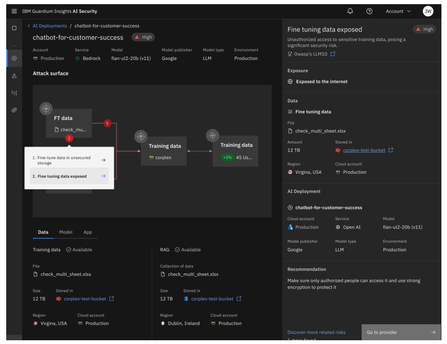
– Informes de cumplimiento
– Proporcione acceso continuo con la gestión de sesiones
– Proporcionar corrección automatizada para las amenazas a la identidad

Analizar

- Perfilar usuarios riesgosos y fraudulentos
- Detecte amenazas a la identidad y comportamientos anómalos
- Proporcionar una gobernanza inteligente

Nueva innovación en seguridad

Seguridad de IA



El uso explosivo de la IA conduce a un uso desconocido, nuevos riesgos

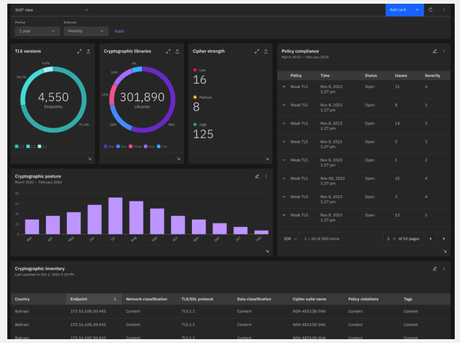
El nuevo producto Guardium protegerá el uso de la IA en la nube con visibilidad de modelos, datos confidenciales y riesgos

Descubra y proteja los datos confidenciales de entrenamiento de la IA y realice un seguimiento de su linaje

Proteja los modelos de IA de la exfiltración, las amenazas internas y el acceso de terceros

Corrija las vulnerabilidades de IA y el contenido de código abierto no aprobado

Caja fuerte cuántica



Los ataques cuánticos pronto romperán el cifrado,

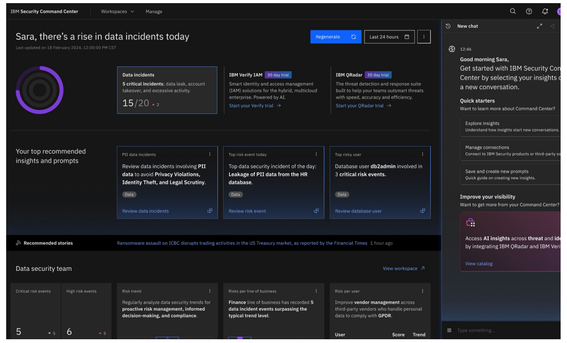
El nuevo producto Guardium ayudará a los clientes a comprender los riesgos cuánticos, las prioridades y comenzar la corrección

Identifique las bibliotecas, los almacenes de datos y las aplicaciones criptográficas en riesgo

Visualice y contextualice el riesgo a través de cuadros de mando e informes

Determine planes de corrección y automatice sugerencias

GenAI en Seguridad



Los profesionales de la seguridad se enfrentan diariamente a tareas repetitivas, complejas y tediosas, a menudo sin respuestas

Nueva IA para casos de uso cibernético en datos, identidad y otros equipos para aumentar la productividad y el conocimiento

Resuma los eventos de seguridad complejos y el riesgo de los datos en información clave, Genere contenido para adelantarse a las infracciones y amenazas de cumplimiento

El enfoque único de IBM para la ciberseguridad

Simplifique la complejidad de la protección
NUBE HÍBRIDA

Expansión de datos en entornos híbridos

Detecte, proteja y controle los datos confidenciales, independientemente de su ubicación

Complejidad de la gestión de nubes

Simplifique la gestión de identidades en todos los entornos con un enfoque de estructura de identidades

Confíe en la adopción segura de
INTELIGENCIA ARTIFICIAL

La IA superficie de ataque desprotegida

Asegúrese de que solo los empleados y consumidores de confianza tengan acceso

La adopción de GenAI sin enfoque de confianza

Proteja los datos de entrenamiento y la integridad de los modelos de lenguaje de gran tamaño

Thank you