Seguridad de los Datos

Un Enfoque Normativo

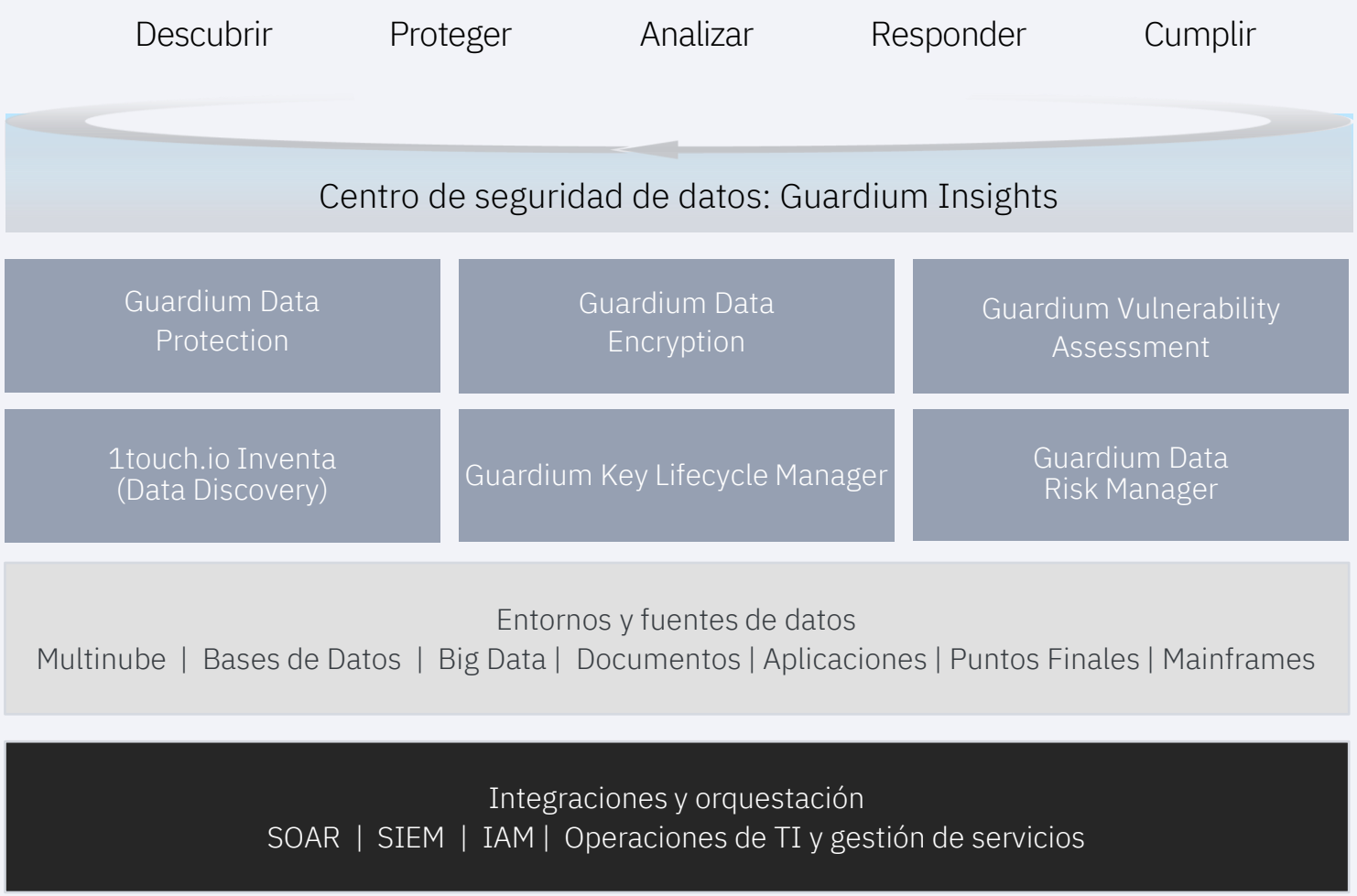
Daniel Arias Vargas

IBM Security Technical Specialist
Colombia

IBM Security

IBM

IBM Security Guardium:
Seguridad de datos moderna



Consultoría, integración de sistemas y servicios de seguridad gestionados

- Estrategia de seguridad de datos
- Descubrimiento de datos
- Gobierno de seguridad de los datos
- DAM Administrado
- Cifrado de datos gestionado

Diseñado para proteger los datos on-prem, en la nube y en cualquier lugar intermedio

- ✓ Soporte sobre la protección de datos multinube híbrida con políticas de seguridad de datos coherentes en todos los entornos, vistas de riesgo holísticas
  - Bases de Datos & Data Warehouses
  - Big Data
  - Archivos
  - Mainframe and z/OS
  - Cloud: AWS, Azure, Google Cloud, IBM Cloud, Oracle Cloud, Database-as-a-Service
- ✓ Amplio soporte de plataforma y escalabilidad masiva para los entornos locales y en la nube más grandes

Requisitos detallados del sistema y plataformas compatibles →

Conexiones flexibles a sus fuentes de datos para la supervisión activa y pasiva

S-TAP: Basado en agentes para la supervisión en tiempo real de las fuentes de datos locales

E-TAP: Solución proxy basada en agentes para el monitoreo en tiempo real de fuentes de datos en la nube

Universal Connectors: Supervisión pasiva sin agentes para orígenes de datos locales y en la nube

Streaming APIs: Supervisión pasiva sin agentes para fuentes de datos en la nube

... Porque una sola talla no sirve para todos!

Es posible que sus necesidades se relacionen al uso de agentes para monitorear fuentes con datos confidenciales en tiempo real, pero deseen adicionalmente, monitorear fuentes que consideren "más seguras" o que no contengan datos confidenciales sin usar agentes, para reducir costos ya que el riesgo es bajo.

Visión estratégica de futuro

IBM está en el camino de proteger los datos en la nube híbrida, Guardium Insights DSPM acelera esta estrategia

PHASE 1

Proteger los datos On-Premises

PHASE 2

Proteja el traslado de datos a la nube

PHASE 3

Proteja los datos originados en varias nubes

Guardium Data Protection

Guardium Insights SaaS

Plataforma de seguridad de datos NextGen

Las capacidades de DSPM amplían la visibilidad a los proveedores de servicios en la nube, las aplicaciones SaaS críticas y las fuentes de datos no estructurados en la nube

- Implementaciones sin agentes SaaS
- Detección automatizada de datos shadow
- Alertas por errores de configuración de datos
- Supervisión de los flujos de datos a través de las nubes
- Soporte para aplicaciones IaaS y SaaS

¿Cómo ayuda DSPM?

Descubrimiento
Detección continua de datos gestionados, no gestionados y shadow

Custodia
Identificar al custodio de los almacenes de datos (aplicación, usuario del servicio)

Clasificación
Etiquetado automatizado de datos sensibles

Mapeo de flujos de datos
Realice el seguimiento del movimiento y el acceso a los datos potenciales y reales

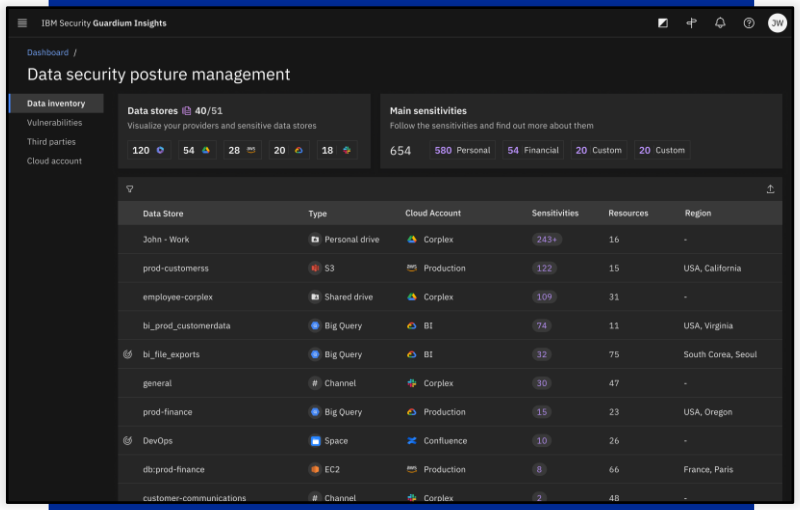
Postura
Detecte y corrija las vulnerabilidades de datos y las violaciones de cumplimiento

- Sin agentes
- Solo lectura
- Impacto Cero en el rendimiento

Plataforma de gestión de la postura de seguridad de los datos

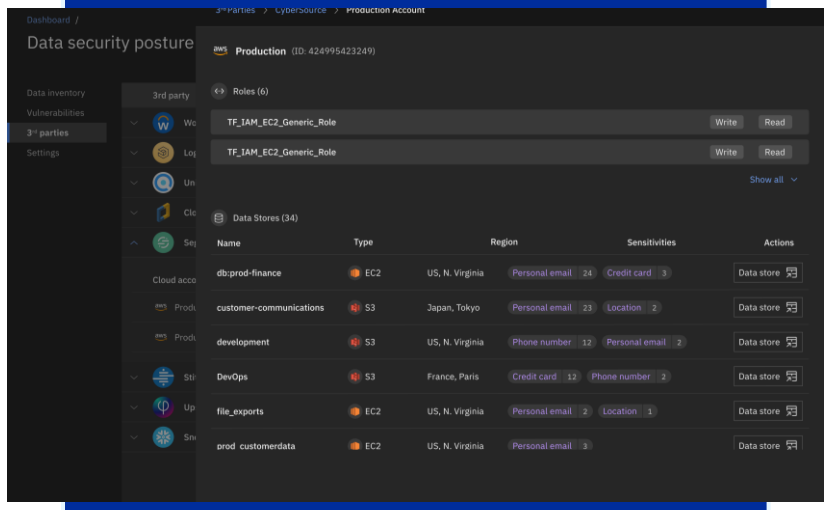
Visibilidad de datos en la nube

- Descubrimiento de datos shadow
- Clasificación de datos confidenciales



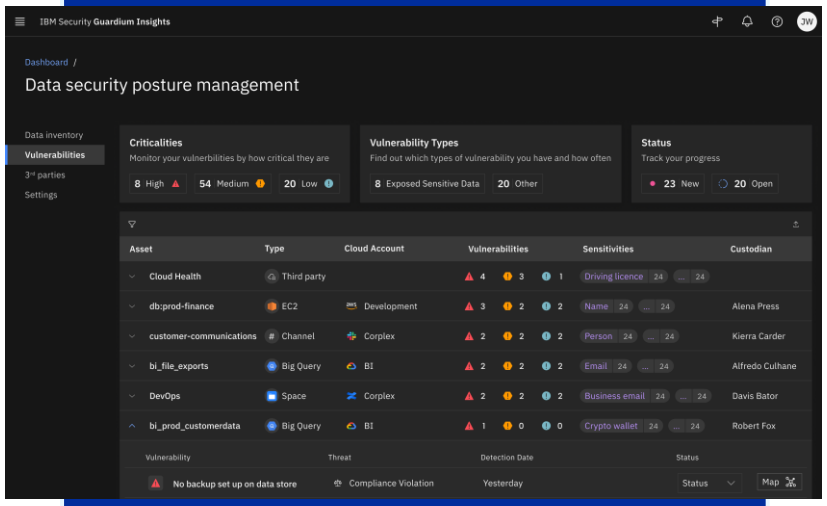
Movimiento de datos en la nube

- Mapeo de flujos de datos
- Gestión de acceso a datos



Protección de datos en la nube

- Data Security Posture Management
- Recomendaciones de corrección



Los mejores del sector ponen a trabajar a Guardium Data Protection

4 de las 5

Principales **bancos** de EE. UU.

4 de las 5

Principales organizaciones de **salud** del mundo

6 de las 10

Principales organizaciones de **seguros** a nivel mundial

7 de las 10

Principales organizaciones mundiales de **telecomunicaciones**

4 de las 5

Principales organizaciones globales de servicios financieros

3 de las 5

Principales minoristas de EE. UU.

3 de las 5

Agencias gubernamentales más grandes de EE. UU.

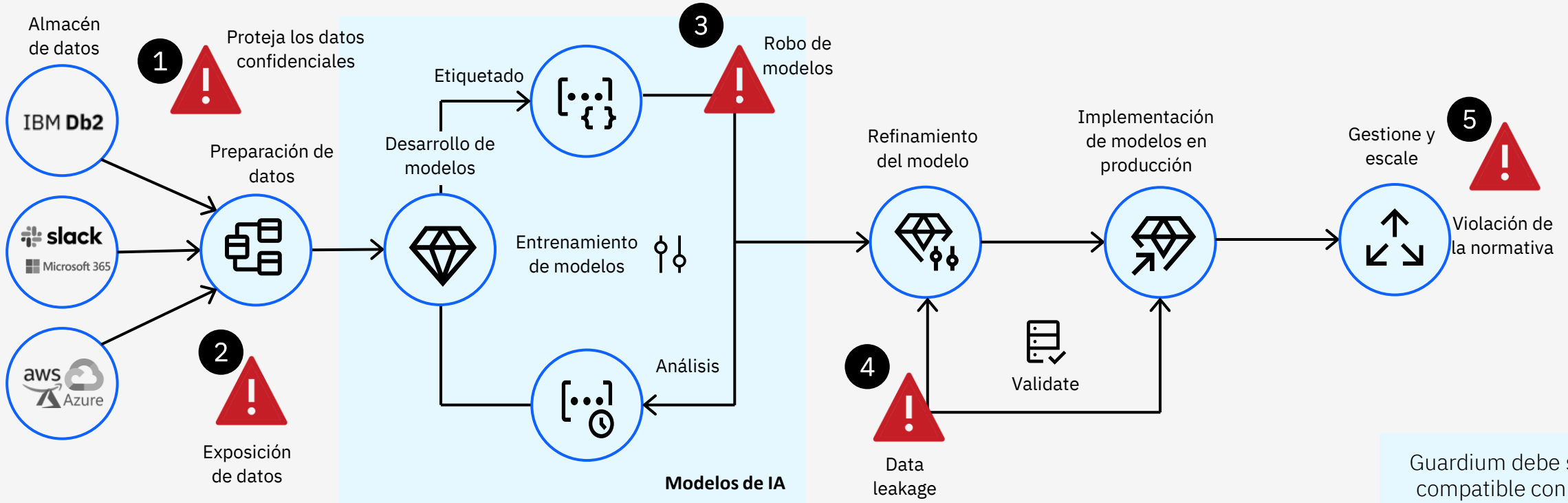
Las Regulaciones

Vista resumida de las principales regulaciones cubiertas por IBM Guardium

DDL = Data Definition Language (También conocidos como cambios de esquema)
DML = Data Manipulation Language (Cambios en el valor de los datos)
DCL = Data Control Language (Se utiliza para el control de acceso y la gestión de permisos para los usuarios de la base de datos)

Audit Requirements	COBIT (SOX)	PCI – DSS	ISO 27002	Leyes de Protección de Datos y Privacidad	NSIT SP 800-53 (FISMA)	GDPR o Leyes de Protección de Datos
1. Acceso a Data Sensible (SELECTs exitosos/fallidos)		✓	✓	✓	✓	
2. Cambios al SCHEMA – DDL (CREATEs, DROPs, ALTER TABLEs, etc...)	✓	✓	✓	✓	✓	
3. Cambios a Datos – DML (DML)	✓	✓	✓			
4. Excepciones de Seguridad (Login fallido, SQL error, etc..)	✓	✓		✓	✓	
5. Cuentas, Roles & Permisos – DCL (GRANTs & REVOKES)	✓	✓	✓	✓	✓	
6. Derecho del interesado a acceder, rectificar, suprimir y portabilidad de sus datos.						✓

Protección del Pipe de la IA con Guardium



1 **Proteja los datos confidenciales**
Evite el uso de información confidencial en el modelo de IA que se encuentra en big data (por ejemplo, Parquet) y cumpla con las regulaciones.

2 **Exposición no intencional**
Supervise las copias de datos confidenciales en aplicaciones y nubes para evitar la exposición a un tercero (por ejemplo, modelos de código abierto no aprobados)

3 **Claves o tokens encontrados en Slack**
Detecte si las claves están expuestas en canales de Slack compartidos, lo que puede dar acceso a los atacantes que tienen como objetivo robar IP

4 **Evite la fuga de datos**
Detectar si se han filtrado datos confidenciales (por ejemplo, PII) durante la validación del modelo (podría deberse a una amenaza interna)

5 **Violación de la transferencia de datos**
Supervise el flujo de datos para garantizar el cumplimiento de las aplicaciones SaaS en varias zonas geográficas (por ejemplo, GDPR)

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity