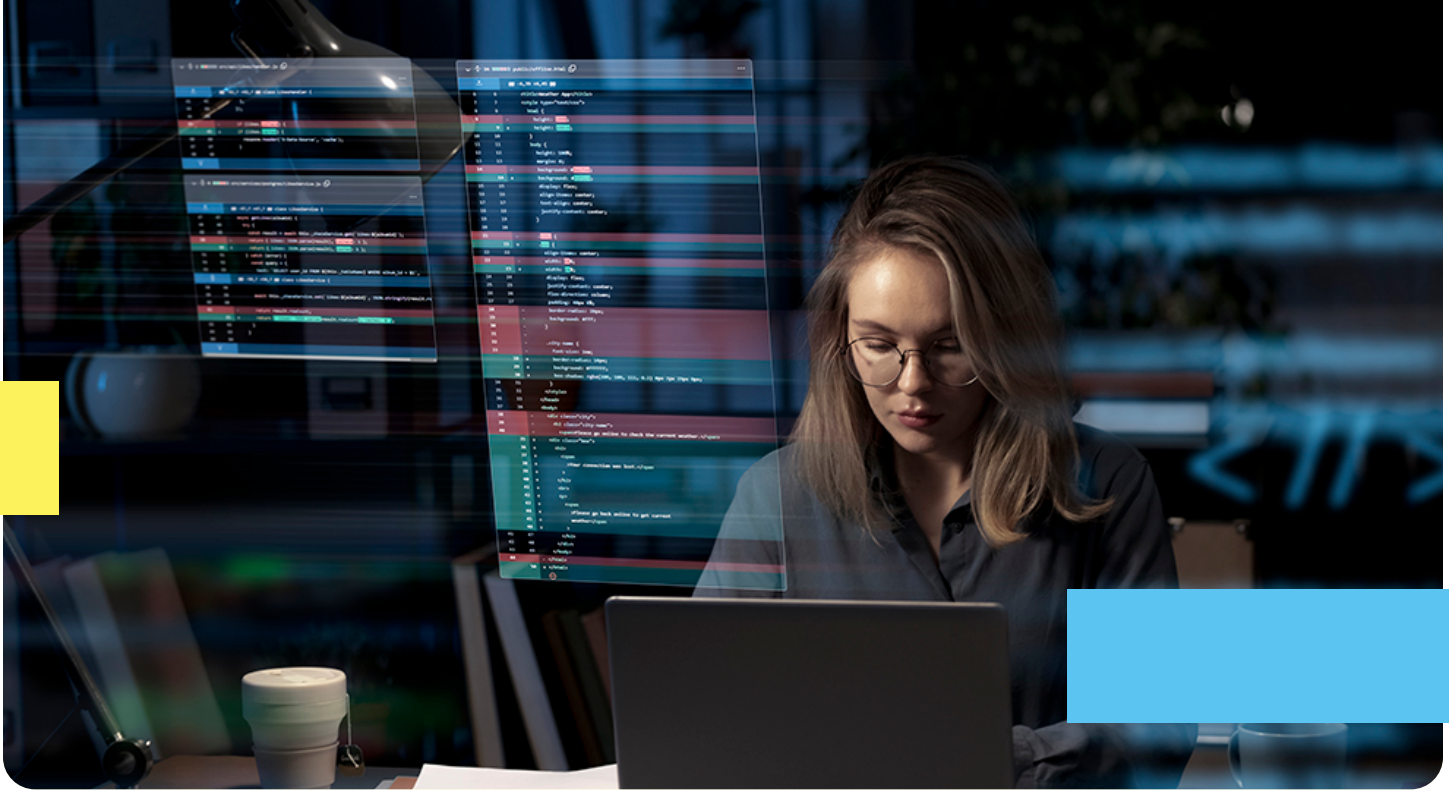
SBRT Computing

Comercializando TI con Valor Único

WHITEPAPER

Alerta de brecha de datos: un checklist de seguridad de la información para aseguradoras mexicanas



La brecha de datos en el sector asegurador mexicano: ¿Crisis o ventaja competitiva?

En la era digital, los datos se han convertido en el principal activo de las aseguradoras mexicanas. Frente al crecimiento exponencial de la información y a la creciente sofisticación de amenazas cibernéticas, el sector asegurador enfrenta retos inéditos para garantizar la protección y gestión segura de datos sensibles, no sólo por mandato regulatorio, sino como requisito para mantener la confianza de los clientes y proteger la reputación organizacional.

Las nuevas regulaciones mexicanas, como la recién actualizada Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP 2025) y la Ley Fintech, establecen lineamientos estrictos para el tratamiento, resguardo y transferencia de información personal en el ámbito financiero y asegurador. Bajo este contexto, plataformas como *IBM Guardium* han emergido como escudos para la seguridad de la información en las compañías de seguros, integrando capacidades para la visibilidad, cumplimiento normativo, automatización y respuesta avanzada ante incidentes.

Este informe explora los retos actuales del sector asegurador en México, así como la brecha que existe entre la teoría de iniciativas impulsadas para la seguridad de la información y lo que la mayoría de organizaciones ejecuta en la práctica, muchas veces sin conseguir la protección real de la información.

A través de un análisis del ciclo de vida de los datos, se identifican los costos multidimensionales que tiene para estas aseguradoras la omisión de puntos ciegos que pueden encontrarse en las plataformas de defensa digital, así como su impacto dentro del marco regulatorio vigente en México, desde los silos de información hasta amenazas emergentes como *“Shadow AI”*.

Como conclusión a este informe, el lector encontrará un checklist estratégico que consta de una serie de preguntas críticas que evalúan la verdadera profundidad y funcionalidad de la estrategia de seguridad de la información de su organización aseguradora en México.

Finalmente, se propone una ruta que permite cambiar el paradigma respecto a la inversión en seguridad de la información: de un gasto obligado a una ventaja competitiva tangible que demuestra gobernanza de seguridad proactiva que asegura la confianza de los clientes, otorga todo su valor a la protección de datos y demuestra la resiliencia de las aseguradoras para adaptarse a la era digital, gracias a plataformas unificadas como *IBM Guardium*.

Capítulo 1

El campo de batalla digital: por qué las aseguradoras mexicanas son un objetivo de alto valor

1.1. Anatomía del riesgo cibernético en México

El volumen de datos en el mundo está creciendo a una velocidad impresionante: se estima que para 2025 se generarán 181 zettabytes. *(Statista, 2024)* En perspectiva, un zettabyte equivale a mil millones de terabytes. Para las aseguradoras en México, esto significa enfrentarse cada día a una avalancha de información que además de ser enorme, es cada vez más difícil de clasificar y proteger.

El verdadero reto no es solo cuánto crecen los datos, sino cómo cambian. Hoy, la mayoría de la información que manejan las aseguradoras ya no está organizada en tablas o bases de datos tradicionales (como nombres, fechas o números de póliza), sino que llega en formatos mucho más variados: correos electrónicos, PDFs de siniestros, fotos de daños, grabaciones de llamadas o documentos legales. A esto se le llama “datos no estructurados”. *(I.B.M. s.f.-c.)*

Este cambio ha dejado obsoletos los modelos de seguridad tradicionales, que estaban diseñados para proteger redes internas cerradas. Ahora, los datos sensibles de las aseguradoras se encuentran repartidos en ecosistemas híbridos que incluyen servidores locales, nubes públicas y decenas de aplicaciones de Software como Servicio (SaaS) *(Forrester, 2020)*. En este contexto, un firewall no puede detectar si alguien sube un informe médico confidencial a una app de inteligencia artificial no autorizada, por ejemplo, dejando expuestos datos privados de los que puede hacerse mal uso.

Por eso, la única forma efectiva de proteger esta información es cambiar el enfoque: en lugar de proteger solo la red, hay que proteger los datos directamente, sin importar dónde estén. Esto implica aplicar controles de acceso y seguridad que viajen con los datos, estén donde estén.

1.2. El costo multidimensional de la inacción en seguridad de la información

En muchas aseguradoras, persiste la idea de “si funciona, no lo cambies”. Pero en el entorno actual, lleno de datos sensibles y amenazas digitales, esa actitud puede salir muy cara. Ser reactivo ya no es una estrategia: es una invitación al desastre.

Una fuga de datos no solo implica pérdidas económicas inmediatas. Puede afectar la reputación, frenar operaciones y debilitar la posición competitiva de una empresa durante años. Según el informe *Cost of a Data Breach Report 2025* de IBM, el costo promedio global de una filtración es de 4.44 millones de dólares. En Estados Unidos, esa cifra sube a 10.22 millones, y los ataques internos maliciosos son los más costosos: 4.92 millones por incidente.

Más allá del dinero, los impactos clave son:

- **Confianza dañada:** En seguros, la confianza lo es todo. Una filtración puede hacer que los clientes se vayan con competidores que perciben como más seguros. La cobertura mediática negativa puede prolongar el daño por años.
- **Operaciones interrumpidas:** Muchas empresas deben pausar sus actividades para contener el incidente y reforzar sus sistemas, perdiendo productividad y compromisos clave.
- **Ventaja competitiva perdida:** Si se filtran modelos actuariales, estrategias de precios o bases de clientes, los competidores pueden aprovechar esa información y ganar terreno en el mercado.

Tabla 1: Anatomía financiera de una fuga de datos (2025)

Métrica	Costo / Impacto	Fuentes
Costo promedio global de una fuga de datos	4.44 Millones USD	(IBM, 2025a; Reddit, 2025)
Costo promedio en los Estados Unidos	10.22 Millones USD	(IBM, 2025a; Reddit, 2025)
Vector de ataque más costoso (Insider malicioso)	4.92 Millones USD	(IBM, 2025a)
Costo adicional por "Shadow AI"	+ 670,000 USD	(IBM, 2025a; Nudge Security, 2025)
Ahorro por uso extensivo de IA en seguridad	- 1.9 Millones USD	(IBM, 2025a)

1.3. El marco regulatorio: más allá del papeleo, un riesgo de negocio crítico

Proteger de forma inadecuada los datos no es solo un error técnico: es una falla de gobernanza que puede poner en riesgo la operación de toda la empresa. Normas como el Reglamento General de Protección de Datos (RGPD) en Europa o la Ley de Privacidad del Consumidor de California (CCPA) marcaron un estándar global que exige que los datos personales y financieros se resguarden con protocolos estrictos, y las multas por incumplimiento pueden llegar a decenas de millones de dólares. *(DCD,2021)*

Para las aseguradoras mexicanas, que operan en un entorno internacional y manejan datos de clientes de distintas regiones, ignorar estos estándares no es opción. Cumplir con la regulación ya no es un trámite más qué cumplir para las auditorías; es parte esencial de la gestión de riesgos.

Una protección débil puede afectar directamente los resultados del negocio, tanto por las sanciones económicas, como por la revocación de licencias para operar en ciertos mercados o quedar fuera de alianzas estratégicas con socios que exigen altos niveles de seguridad.

Capítulo 2

El ciclo de vida del dato: identificando los puntos ciegos en su fortaleza digital

2.1. Complejidades que debilitan la seguridad tradicional

El día a día de una aseguradora moderna está lleno de retos que los modelos de seguridad antiguos no pueden cubrir. Estos son algunos de los más críticos:

- **Silos de datos:** La información clave suele estar dispersa entre departamentos, sistemas viejos y nubes mal integradas o fragmentadas.*(Astera,2024; 9altitudes,2024)* Esta fragmentación impide tener una visión completa del cliente y dificulta aplicar políticas de protección consistentes.

- **Datos no estructurados:** Correos, PDFs, imágenes y otros formatos no organizados han crecido exponencialmente. Las herramientas tradicionales no pueden escanear ni entender el contenido de millones de archivos para detectar información sensible. *(IBM, s.f.-c)*

- **Shadow AI:** Una amenaza emergente y potente. Ocurre cuando empleados, buscando ser más eficientes, usan herramientas de inteligencia artificial generativa sin aprobación del área de TI. Al subir datos de pólizas o siniestros a plataformas públicas, exponen a la empresa a riesgos graves de filtración y violación de privacidad. *(Praxilia, 2024)* Las fugas relacionadas con Shadow AI pueden costar hasta 670,000 dólares adicionales por incidente. *(IBM, 2025a; Nudge Security, 2025)*

2.2. De soluciones aisladas a una estrategia evolutiva: el modelo de madurez en seguridad de datos

Como se ha visto en los puntos anteriores, en el entorno actual, lleno de datos sensibles y amenazas complejas, ya no basta con usar soluciones de seguridad puntuales. Las aseguradoras necesitan una estrategia clara, que les permita pasar de una postura reactiva a una gestión proactiva y resiliente. Para lograrlo, muchas organizaciones adoptan modelos de madurez basados en marcos reconocidos como los de Gartner, NIST y Forrester. *(Gartner, s.f.-a.; NIST, 2014; Forrester, 2020)*

Este modelo se puede dividir en cuatro fases que garanticen la gobernanza de la seguridad de los datos:

Fase 1: Visibilidad total

No se puede proteger lo que no se ve. El primer paso es implementar herramientas que escaneen de forma continua todos los entornos —bases de datos, nubes, archivos y aplicaciones SaaS— para identificar y clasificar automáticamente la información sensible.

Fase 2: Reglas claras y aplicables

Cuando se consigue tener visibilidad, llega el momento de definir políticas de seguridad basadas en las necesidades del negocio y las obligaciones legales. Esto incluye principios como el de menor privilegio, que limita el acceso solo a lo necesario.

Fase 3: Automatización y monitoreo

Las políticas deben aplicarse de forma consistente. Esta fase usa tecnología para hacer cumplir las reglas en tiempo real, monitorear el uso de los datos (DAM) y detectar comportamientos anómalos que puedan indicar una amenaza.

Fase 4: Optimización continua

En el nivel más avanzado, la organización usa la inteligencia recopilada para ajustar su estrategia de riesgo, eliminar datos innecesarios que aumentan la exposición, y habilitar el uso seguro de tecnologías como la inteligencia artificial.

Capítulo 3

El checklist estratégico de seguridad de la información

Para enfrentar los riesgos digitales que rodean a una aseguradora en México, lo más importante es saber qué preguntar. Este checklist no se queda en lo técnico: está diseñado para ayudar a evaluar si la estrategia de seguridad de la información de la organización es realmente sólida, madura y capaz de adaptarse a los desafíos actuales.

3.1. ¿Tu estrategia de cumplimiento protege de verdad o solo sirve para pasar auditorías?

Muchas organizaciones siguen viendo el cumplimiento como un trámite para "marcar casillas" en temporada de auditorías. *(IBM, s.f.-d)* Pero, como se mencionó antes, este enfoque reactivo es débil y arriesgado. Una estrategia realmente útil convierte el cumplimiento en un escudo activo: automatiza políticas, aplica controles de forma constante y se adapta a regulaciones como GDPR, PCI-DSS y SOX sin depender del esfuerzo manual.

Por ejemplo, plataformas como *IBM Guardium Data Protection* permiten aplicar plantillas preconfiguradas para cumplir con estas normas, lo que reduce hasta en un 75% el tiempo de preparación para auditorías. Así, los controles no se activan solo cuando hay revisión externa, sino que funcionan todo el tiempo. *(Forrester, 2020)*

3.2. ¿Tienes una vista completa de tus datos o estás atrapado en silos que nadie controla?

Los silos de información son uno de los mayores riesgos para la seguridad de datos. Cuando cada área o sistema guarda sus propios datos sin conexión con el resto, es imposible tener una visión integral del negocio o aplicar políticas de protección de forma consistente. *(Astera, 2024)*

Una plataforma de seguridad unificada permite romper esos silos. Por ejemplo, *IBM Guardium Discover and Classify* crea un inventario automatizado de todos los datos —estructurados y no estructurados— en entornos locales, nubes públicas y aplicaciones SaaS. Así, la organización puede ver y proteger todo su patrimonio de datos desde una sola consola, sin depender de procesos manuales ni de visibilidad parcial. *(IBM,s.f.-a)*

3.3. Si hay una brecha de datos a las 2 a.m., ¿quién responde y quién comunica?

Esta pregunta revela si la organización tiene un plan de respuesta sólido para el manejo de crisis o si todo recae, de forma riesgosa, en el equipo de TI. *(Ransomware Help, s.f.)* En una aseguradora, la gobernanza de datos debe estar bien definida: ¿quién es dueño de los datos?, ¿quién los custodia?, ¿quién toma decisiones en una crisis?

Una estrategia madura no improvisa; establece roles claros y coordina la respuesta entre áreas clave: legal, comunicación, negocio y tecnología. Así, si ocurre una filtración, hay un protocolo listo para contener el daño, comunicar con transparencia y proteger la reputación de la empresa.

3.4. ¿Tu seguridad está atrapada en el pasado o preparada para los ataques de hoy?

Las defensas estáticas ya no bastan. Los atacantes evolucionan constantemente, y las vulnerabilidades cambian cada día. Para protegerse de verdad, las aseguradoras necesitan una postura proactiva: evaluar sus sistemas de forma continua y corregir debilidades antes de que alguien las aproveche.

Herramientas como *IBM Guardium Vulnerability Assessment* permiten escanear los almacenes de datos en busca de fallas conocidas, configuraciones incorrectas o parches pendientes. Así, los equipos pueden reforzar sus sistemas antes de que se conviertan en una puerta abierta para los hackers. *(IBM, 2024)*

3.5. ¿Detectas amenazas internas en tiempo real o te enteras cuando ya es noticia?

Las amenazas internas y el robo de credenciales son dos de los ataques más costosos y difíciles de detectar. *(IBM, 2025a)* Si la organización no monitorea el uso de sus datos en tiempo real, corre el riesgo de descubrir el problema demasiado tarde —cuando ya ha habido daño reputacional, legal o financiero.

La única defensa efectiva es el monitoreo continuo de la actividad sobre datos sensibles (DAM). Herramientas como *IBM Guardium Data Protection* analizan cada interacción en tiempo real, usando inteligencia artificial para identificar comportamientos sospechosos. Si detecta una anomalía, puede bloquear el acceso o aislar al usuario automáticamente, transformando la seguridad de una reacción tardía a una respuesta inmediata. *(Optima Tech, s.f.)*

Capítulo 4

La próxima frontera: proteger la inteligencia artificial y asegurar la continuidad del negocio

4.1. El dilema de la IA en el sector asegurador: innovación con riesgos

La inteligencia artificial está transformando el sector asegurador: permite personalizar pólizas, automatizar procesos de siniestros y mejorar la atención al cliente. Pero también abre nuevas puertas al riesgo. Uno de los más críticos es la *Shadow AI:* el uso de herramientas de IA sin aprobación ni supervisión. El 97% de los incidentes de seguridad relacionados con IA ocurrieron en sistemas sin controles de acceso adecuados. *(IBM, 2025a; Reddit, 2025)*

Además, muchos modelos de IA operan sin trazabilidad clara de los datos que utilizan. Sin un linaje de datos —es decir, sin saber de dónde vienen, cómo se transforman y quién los usa—, es imposible auditar su funcionamiento o demostrar cumplimiento normativo. Esto convierte a la IA en una caja negra que puede comprometer la confianza y la legalidad de las operaciones. *(erwin, s.f.)*

4.2. Implementación segura de IA (Secure AI Deployment)

Para que la IA sea una herramienta confiable, las aseguradoras necesitan un marco de gobernanza específico. Aquí un checklist práctico basado en *IBM Guardium AI Security*:

Detectar IA no autorizada
Escanear continuamente todos los entornos para identificar modelos de IA que operan sin supervisión (Shadow AI) y registrarlos en un inventario centralizado. (IBM, 2024b)

Evaluar vulnerabilidades
Realizar pruebas automatizadas para detectar configuraciones inseguras o brechas en los modelos de IA antes de que sean explotadas.

Proteger en tiempo real
Implementar un Gateway especializado que revise las instrucciones (prompts) y respuestas de las aplicaciones de IA, bloqueando código malicioso y evitando filtraciones de datos sensibles (PII).

Asegurar cumplimiento y trazabilidad
Alinear los equipos de seguridad y gobernanza en métricas comunes, garantizando que los datos usados por la IA sean auditables y cumplan con las regulaciones aplicables.

4.3. Más allá del “Disaster Recovery”: una nueva visión de seguridad

La resiliencia en el marco del resguardo de información va más allá del clásico “plan de recuperación ante desastres”. Es la capacidad de anticiparse, resistir, adaptarse y recuperarse frente a ataques. En esta etapa avanzada del modelo de madurez, la seguridad de datos se convierte en un motor estratégico.

Las aseguradoras pueden usar la inteligencia de sus plataformas de seguridad para:

- **Reducir riesgos innecesarios**
  Identificar y eliminar datos sensibles que ya no se usan (ROT), reduciendo los puntos vulnerables que podrían ser atacados. *(IBM,s.f.-a)*

- **Predecir amenazas**
  Analizar patrones históricos para anticipar zonas de alto riesgo y asignar recursos para el resguardo informativo de forma más eficiente.

- **Impulsar innovación segura**
  Crear una base de datos confiable, bien gobernada y de alta calidad que permita desplegar iniciativas de IA y análisis avanzado sin comprometer la seguridad.

Conclusión: de obligación técnica a ventaja competitiva

La forma en que las aseguradoras mexicanas gestionan sus datos está en un punto de inflexión. El crecimiento acelerado de la información y el uso de inteligencia artificial han dejado obsoletos los enfoques tradicionales de seguridad. Hoy, los datos —el activo que impulsa la innovación, la personalización y la eficiencia operativa— pueden convertirse en el mayor riesgo si no se protegen adecuadamente.

Superar esta brecha no se logra con controles aislados ni con respuestas reactivas. Requiere un cambio de enfoque: integrar la seguridad directamente en la gobernanza de datos. Esta fusión estratégica permite anticipar amenazas, cumplir con regulaciones, proteger la reputación y habilitar el crecimiento. Es lo que se conoce como *gobernanza de seguridad proactiva*.

El caso de negocio:

IBM Guardium como habilitador estratégico

La eficacia de una plataforma como IBM Guardium no es una promesa, es una realidad comprobada. Según el estudio *Total Economic Impact*™ de Forrester *(2022)*, encargado por IBM, una organización que implementó Guardium logró:

406%

de retorno de inversión (ROI) en un periodo menor de seis meses

- 40%

Reducción del 40% en la probabilidad de sufrir una fuga de datos

1.1 millones

de dólares en ahorros relacionados con cumplimiento normativo

Estos resultados demuestran que invertir en una plataforma unificada de seguridad de datos no solo protege: transforma la operación y genera valor tangible.

Orientación a actuar: liderar con visión

La decisión de implementar una plataforma de seguridad de datos como *IBM Guardium* no es una mejora técnica aislada: es una transformación estratégica. Para las aseguradoras mexicanas, esto significa pasar de gestionar riesgos a capitalizar oportunidades. La gobernanza de seguridad proactiva permite anticipar amenazas, cumplir con regulaciones complejas y habilitar tecnologías como la IA sin comprometer la privacidad ni la reputación.

Según Cybersecurity News, **más del 50% de las aseguradoras ya están utilizando tecnologías como IA, cloud y big data para reforzar su postura de seguridad de la información, automatizar procesos y reducir riesgos operativos**. Además, el *InsurTech Report 2025* de Konfront destaca que los seguros de vida y autos —los más digitalizados en México— han logrado avances significativos en eficiencia y experiencia del cliente gracias a plataformas seguras y bien gobernadas.

La evidencia es clara: las aseguradoras que invierten en seguridad de datos no solo evitan pérdidas, sino que mejoran su capacidad de innovación, reducen costos operativos y fortalecen la confianza del cliente.

En un entorno donde la reputación y la continuidad operativa son clave, una plataforma no es un gasto: es una inversión que habilita y diferencia; protege la gobernanza de seguridad proactiva y es el puente que cierra la brecha para convertir el potencial de los datos en una realidad rentable y segura.

Apéndice: Referencias

9altitudes. (2024, 21 de octubre). El peligro de los silos de datos y cómo abordarlos. 9altitudes.

Astera. (2024). ¿Qué son los silos de datos y cómo impactan en su negocio? Astera.

DCD. (2021, 15 de septiembre). Cómo las fugas de datos pueden afectar la reputación de una empresa. Data Center Dynamics.

EasyDMARC. (2024, 12 de enero). ¿Cuáles son las consecuencias de una violación de datos?

erwin. (s.f.). ¿Qué es el linaje de datos? erwin by Quest.

Forrester. (2020). Zero Trust Requires A Data-Centric Security Approach.

Forrester. (2022). The Total Economic Impact™ Of IBM Security Guardium Data Protection. IBM.

Gartner. (s.f.-a). Roadmap for a Maturing Cybersecurity Program. Consultado el 11 de octubre de 2025.

Gartner. (s.f.-b). The Gartner Enterprise Information Management Maturity Model. Consultado el 11 de octubre de 2025.

IBM. (s.f.-a). Guardium Discover and Classify. Consultado el 11 de octubre de 2025.

IBM. (s.f.-b). Shadow AI: What it is, risks and how to manage it. IBM.

IBM. (s.f.-c). Structured vs. unstructured data: What's the difference? IBM.

IBM. (s.f.-d). Guardium Data Protection. Consultado el 11 de octubre de 2025.

IBM. (2024a). Guardium Vulnerability Assessment.

IBM. (2024b, 14 de mayo). Unlock trustworthy AI with integrated governance and security.

IBM. (2025a). Cost of a Data Breach Report 2025.

IBM. (2025b, 22 de agosto). Cost of a Data Breach Report 2025. Baker Donelson.

NIST. (2014). Framework for Improving Critical Infrastructure Cybersecurity.

Nudge Security. (2025). Shadow AI: The emerging security threat in IBM's 2025 Cost of a Data Breach Report.

OptimaTech. (s.f.). Guardium Data Protection. Consultado el 11 de octubre de 2025.

Praxilia. (2024, 25 de julio). Fugas de Datos por IA en la Sombra y el Auge del Coste por Brecha a $4.88M.

Ransomware Help. (s.f.). Fuga de datos: qué es, consecuencias y cómo protegerte. Consultado el 11 de octubre de 2025.

Reddit. (2025). IBM's 2025 Cost of a Data Breach Report: The AI Edition. r/Information_Security.

Statista. (2024). Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025.

TNI. (2020, 1 de julio). El capitalismo digital es una mina, no una nube. Transnational Institute.