The **Secure Journey**

Navengando el océano de datos: amenazas y defensas invisibles

En el fondo del océano digital descansan cofres repletos de tesoros. Son los datos de su empresa: **clientes, finanzas, operaciones, propiedad intelectual.** Protegerlos es vital, porque cada vez que un cofre se abre sin control, el impacto puede ser devastado.

Perder datos no es solo perder información: es perder **confianza, continuidad y futuro**.

+US4.88 millones

Costo promedio de una filtración de datos, según IBM

Amenazas en el océano

Corrientes invisibles
(Amenazas internas)

- **Errores humanos y configuraciones incorrectas:** Un permiso mal asignado o una base de datos expuesta pueden convertirse en una puerta abierta.
- **Accesos indebidos de empleados o terceros:** Muchas brechas nacen dentro de la propia organización, ya sea por descuido o mala intención.
- **Falta de visibilidad sobre los datos sensibles:** Cuando no se sabe dónde están, quién los usa o cómo se mueven, es imposible protegerlos.

82% de las brechas de datos en el mundo nacen de errores humanos o configuraciones equivocadas, según Verizon.

Depredadores
(Riesgos externos)

- **Ciberataques avanzados y persistentes:** buscan explotar vulnerabilidades y permanecer ocultos el mayor tiempo posible.
- **Exposición en entornos híbridos y multicloud:** cada nube y cada aplicación abre nuevas rutas de ataque si no están bien controladas.
- **Nuevas amenazas impulsadas por inteligencia artificial:** desde deepfakes hasta accesos automatizados, los atacantes aprovechan IA para escalar ataques.
- **Falta de controles de acceso y monitoreo continuo:** sin defensas activas, incluso la innovación puede convertirse en un riesgo.

97% de las organizaciones no tiene controles adecuados en accesos de IA, según **IBM**.

El guardián invisible

En medio de las corrientes internas y los depredadores externos, existen un guardián invisible que protegen lo más valioso de la organización: **sus datos**.

IBM Guardium

El sonar submarino

- Descubre y clasifica los datos sensibles, incluso en cloud y SaaS.
- Monitorea actividad y anomalías en tiempo real, detectando accesos indebidos antes de que escalen.
- Automatiza auditorías y reportes, simplificando el cumplimiento regulatorio.
- Incorpora controles avanzados para entornos de IA y criptografía post-cuántica.

Esta solución permite reducir significativamente el costo y el impacto de una brecha, asegurando que los cofres digitales estén siempre bajo vigilancia.

Con **IBM Guardium**, de la mano de GBM, su océano de datos no queda a la deriva: tiene un guardián invisible que vigila cada corriente, enfrenta a cada depredador y garantiza la confianza para navegar con seguridad hacia el futuro.

Fuentes:

IBM – Cost of a Data Breach Report 2024–2025
https://www.ibm.com/reports/data-breach

IBM Guardium – Capacidades técnicas (DSPM, DDR, cumplimiento, IA, Quantum Safe):
https://www.ibm.com/mx-es/products/guardium
https://www.ibm.com/mx-es/products/guardium-data-security-center

IBM® GBM CYBERSECURITY CENTER | GBM®