Cifrado, DLP y Monitoreo de Datos ¿Cuál necesitamos Realmente?

Entendiendo de forma holística las tecnologías para proteger nuestros datos

Joel Alvarado
Regional Data Security Pre Sales Engineer

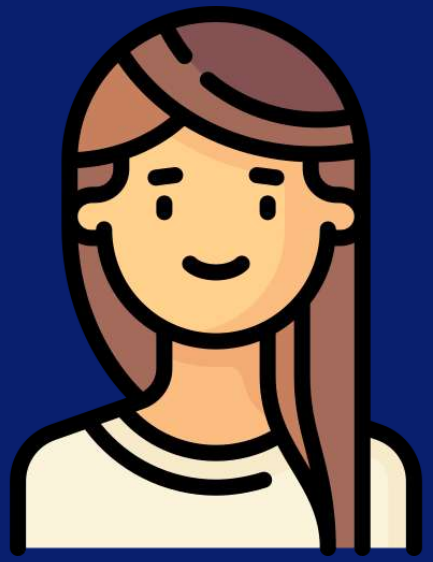
Agenda

- Historia: 3 capas del engaño
- Desafíos de Data Security
- Panorama actual de fuga
- Qué hace cada tecnología?
- Casos de uso reales
- Desafíos de cada tecnología
- Recomendaciones y Conclusiones

3 Capas del Engaño

Viernes
5:30 PM

3 Capas del Engaño

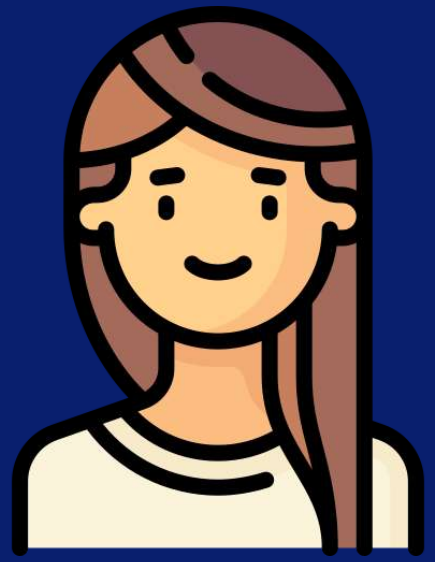


Ana

3 Capas del Engaño

6:15 PM

3 Capas del Engaño



Ana

3 Capas del Engaño

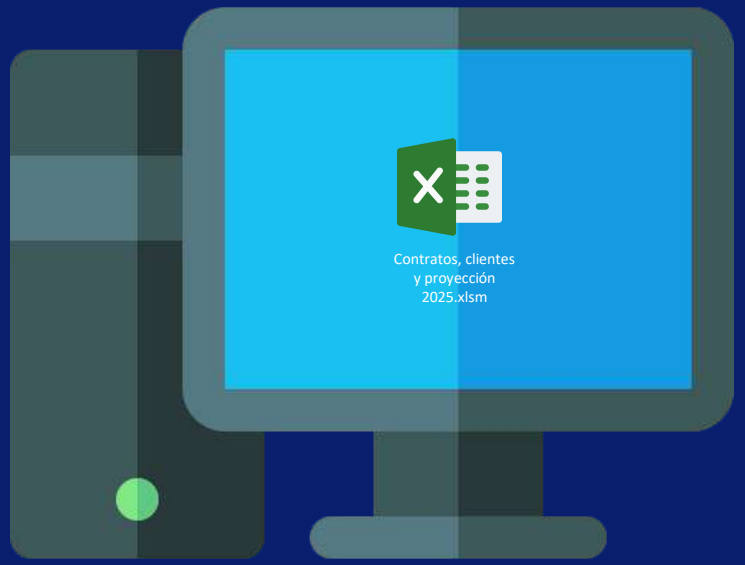
Al día Siguiente

IBM

GBM

3 Capas del Engaño

Rafael



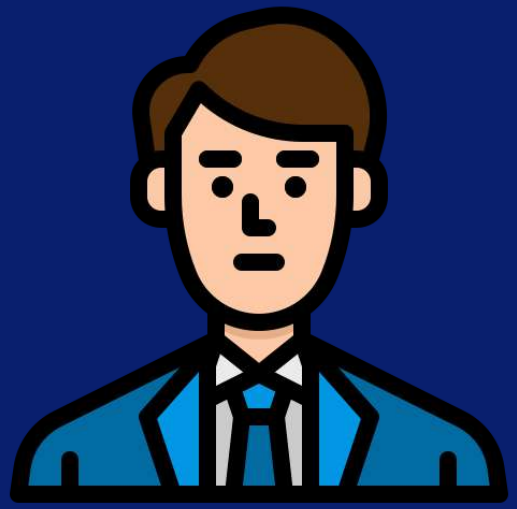
3 Capas del Engaño

Varios Días Después

IBM

GBM

3 Capas del Engaño



Competencia

Contratos, clientes y proyección 2025.xlsm

Cotización Ganadora

3 Capas del Engaño

Ana

Y ¿Qué Faltó?

- Cifrado
- DLP
- Monitoreo de Actividad

Data Security Challenges

Top Three

Explosión de Datos en la Nube

63% de las organizaciones han expuestos datos sensibles en la nube

Exfiltración, Secuestro y Robo de Datos

No. 1 en los listados de tipos de ataques que afectan a las empresas de la región.

Complejidad en el Cumplimiento

1000 horas dedicadas al año por las organizaciones para facilitar las auditorías

Panorama Actual de Fuga de Datos

Filtraciones de datos: Más communes de lo que crees

Fuga de Datos

83% de las organizaciones han expuestos datos sensibles en la nube.

*IBM Cost of a Data Breach Report 2024

Usuarios Internos

35% en promedio los casos de fuga, involucran archivos descargados por usuarios internos.

*Fortra Data Trends LATAM 2023

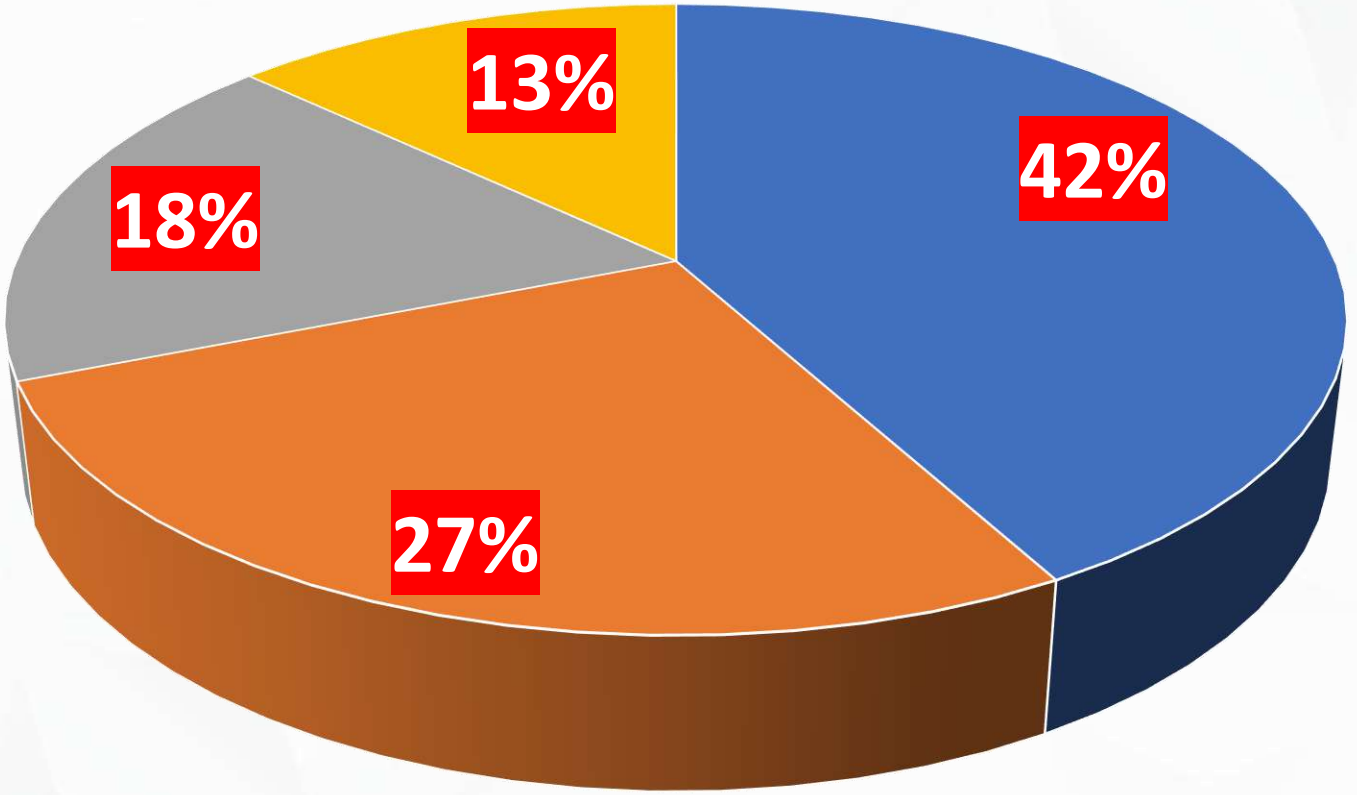
Falta de Reacción

+60% de los incidentes no se detectan durante semanas, incluso meses.

*Verizon DBIR 2024

¿Cómo se filtran los datos?

Las fugas no siempre son ataques externos



¿Qué Hace Cada Tecnología?

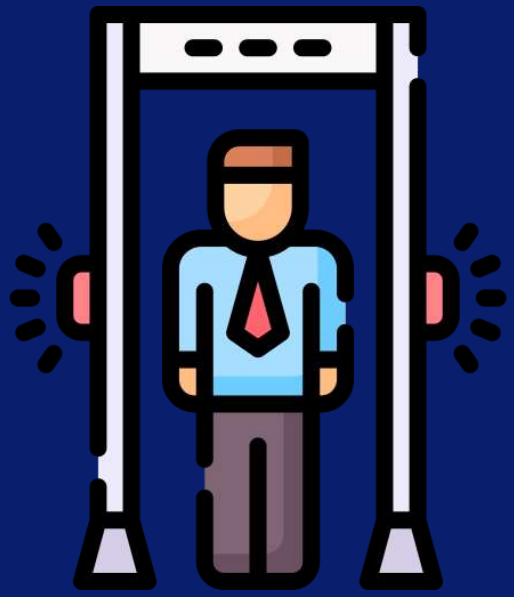
Cifrado

🔐 ¿Qué es?	Convierte la información en un formato ilegible sin la clave adecuada.
🧠 Analogia visual	Como guardar dinero en una caja fuerte: si alguien la roba, no puede usarlo.
🛡️ ¿Qué protege?	Datos *en reposo* (discos, bases de datos, archivos) y *en tránsito* (redes).
💥 ¿Qué previene?	Que los datos sean útiles en caso de robo, fuga o pérdida de dispositivos.

Data Loss Prevention

🚨 ¿Qué es?	Previene que información sensible salga de la organización de forma no autorizada.
🧠 Analogia visual	Como el control de seguridad en un aeropuerto: revisa qué puede salir y qué no.
🛡️ ¿Qué protege?	Archivos, correos, transferencias, dispositivos externos, impresión, nube.
💥 ¿Qué previene?	Fugas accidentales o intencionales por empleados o terceros.

¿Qué Hace Cada Tecnología?



¿Qué Hace Cada Tecnología?

Monitoreo de Actividad

👀 ¿Qué es?	Registra, analiza y alerta sobre el comportamiento de los usuarios hacia los datos.
🧠 Analogia visual	Como cámaras de vigilancia: no impiden el acceso, pero detectan y alertan comportamientos sospechosos.
🛡️ ¿Qué protege?	Bases de datos, accesos críticos, usuarios privilegiados.
💥 ¿Qué previene?	Abusos de privilegios, accesos indebidos, movimientos laterales.

Casos Reales

- **Caso 1:** Empleado filtra archivo excel por correo personal

Casos Reales

Usuario Interno

Correo Personal

Casos Reales

- **Caso 2:** Atacante externo accede a la base de datos

Casos Reales

Atacante
Externo

select * from nomina

name	salary
Pedro S.	XXXXXXXXX
Pablo J.	XXXXXXXXX
Lucas A.	XXXXXXXXX

Base de Datos

Casos Reales

- **Caso 3:** Usuario interno accede fuera de horario desde otro país.

Casos Reales

Usuario Interno
Estados Unidos
Domingo 7:00pm

Base de Datos

C:\Datos Confidenciales

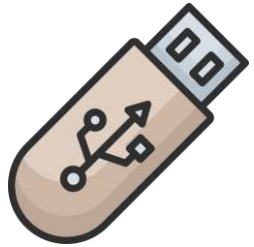
Casos Reales

- **Caso 4:** Data filtrada por impresión o USB.

Casos Reales

Usuario Interno

Impresión



Memoria
Externa

Casos Reales

- **Caso 1:** Empleado filtra archivo excel por correo personal
- **Caso 2:** Atacante externo accede a la base de datos.
- **Caso 3:** Usuario interno accede fuera de horario desde otro país.
- **Caso 4:** Data filtrada por impresión o USB.

DLP

Cifrado

Monitoreo

DLP + MONITOREO

Desafíos del Cifrado, DLP y Monitoreo

Cifrado

- Mala gestión de claves.
- Impacto en el rendimiento.
- Falta de integración.
- Poca automatización.

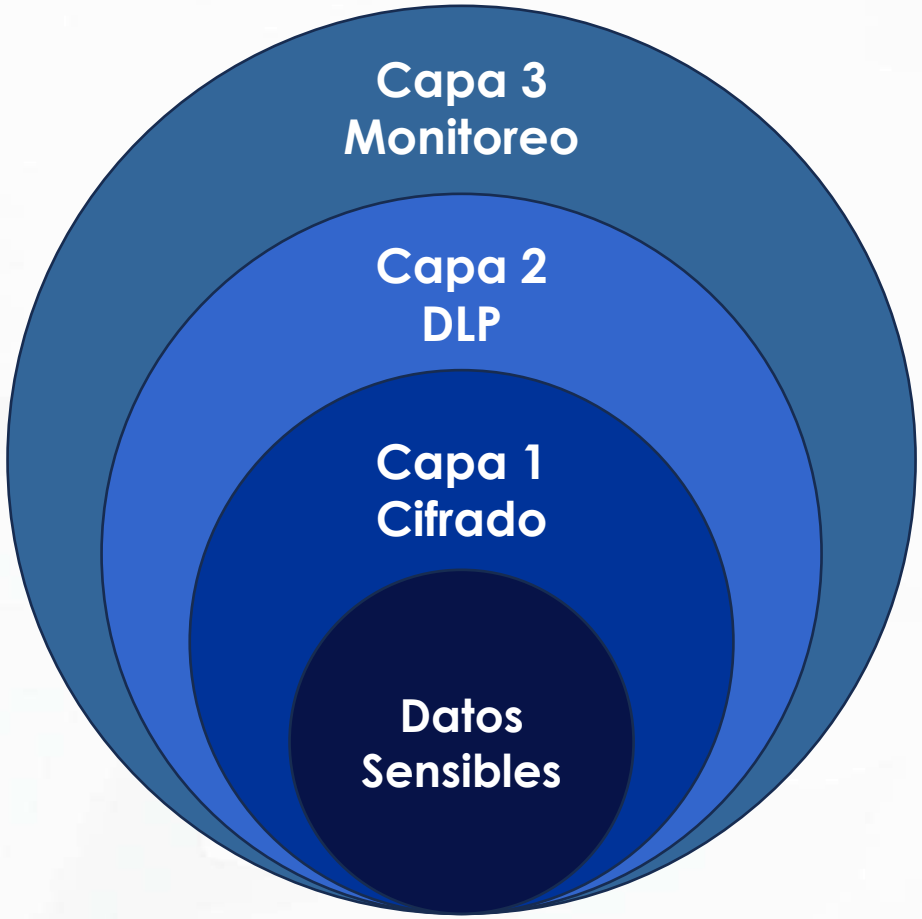
Data Loss Prevention

- Falta de clasificación de datos.
- Reglas demasiado restrictivas.
- Despliegue inconsistente.
- Productividad afectada.

Monitoreo

- Exceso de datos sin análisis.
- Falta de visibilidad de administradores.
- Alertas sin respuesta.
- Temas de privacidad.

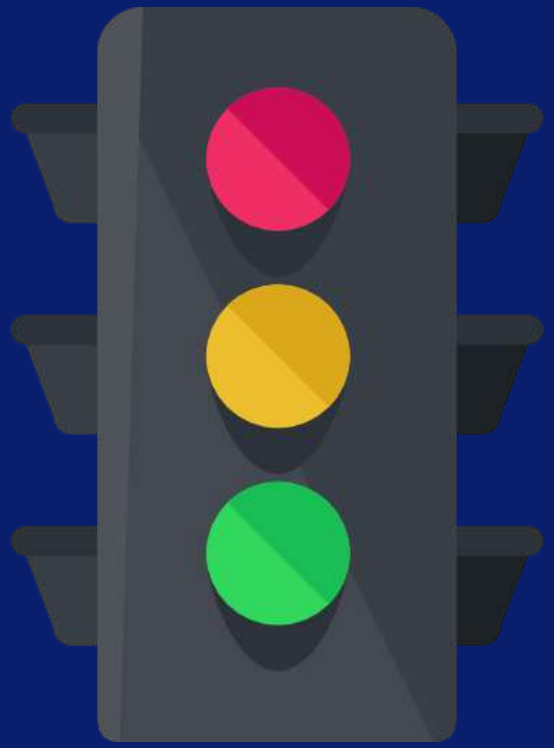
Combinando las 3 capas: Protección Integral



"Ninguna capa es suficiente por sí sola.

Cuando las tres se combinan, proteges tu información desde el corazón hasta el perímetro."

Conclusión y Recomendaciones



- **Rojo:** Protegemos el perímetro, pero no los datos.
- **Amarillo:** Usamos 1 o 2 capas, pero sin integración ni visibilidad.
- **Verde:** Tenemos cifrado, DLP y monitoreo coordinados.

¿En qué nivel está tu organización hoy?
Y más importante… ¿en cuál debería estar?

¿PREGUNTAS?

MUCHAS **GRACIAS**

www.gbm.net
mercadeo@gbm.net | GBMCorp