# **Protección de Datos:** Estrategia Integral de Ciberseguridad

Jueves, 16 de abril 2026

# Seguridad Centrada en el Dato

**4.4 millones de dólares es el costo promedio mundial de una filtración de datos**, ha disminuido un **9 %** con respecto al año pasado, debido a una identificación y contención más rápida con la gobernanza del dato.

https://www.ibm.com/reports/data-breach

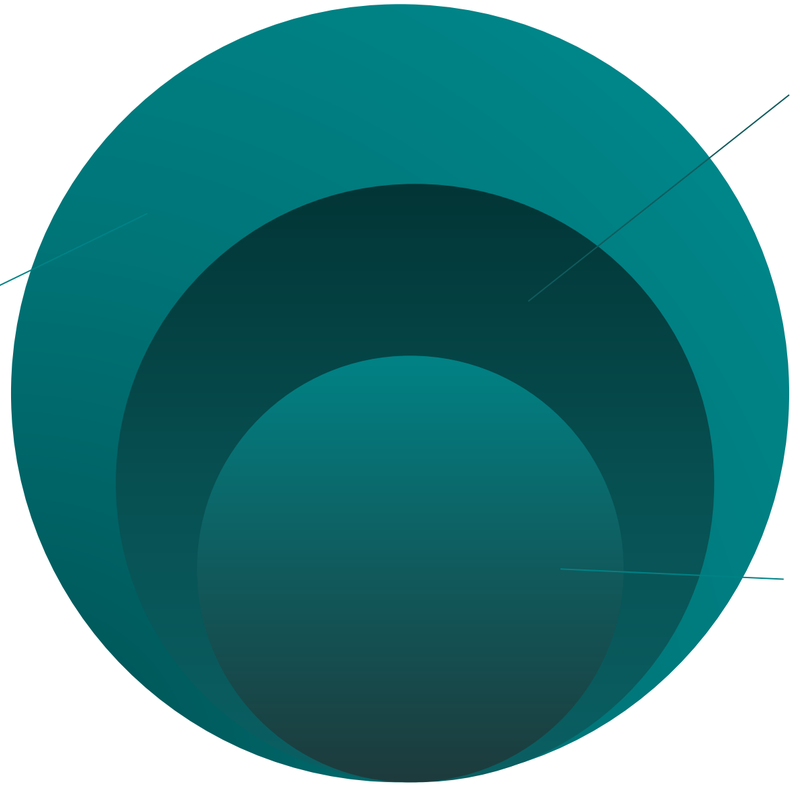

En 2025, el **30 % de las filtraciones involucraron datos en múltiples entornos** (nube y local). Las filtraciones en entornos multinube promediaron 5,05 millones de dólares (frente a 4,01 millones de dólares en entornos locales). La **mala configuración y los fallos de gobernanza del dato** siguen siendo factores recurrentes que generan vulnerabilidades, especialmente en entornos híbridos y multi-entorno.

https://www.ibm.com/reports/data-breach

**97% de organizaciones que reportaron un incidente de seguridad relacionado con la IA** y que carecían de controles de acceso adecuados para la IA.

https://deepstrike.io/blog/data-breach-statistics-2025

# Paradigma de la Seguridad Centrada en el Dato



**Protección de red**
Perímetro y control de tráfico.

**Protección del servidor**
Seguridad en contenedores y endpoints.

**Protección del archivo**
Seguridad integrada al contenido.

## Cambio de Enfoque

Dejar de proteger solo el servidor y la red para proteger directamente el contenido, sin importar dónde se encuentre.

La tecnología de Arexdata/DLP permite que el archivo viaje con su propia seguridad integrada, independiente de la infraestructura

# Pilar 1: Cumplimiento Normativo basado en ISO/IEC 27001 + CIS Control

**Objetivo:** Establecer un marco de control sólido, auditable y alineado a mejores prácticas internacionales.

# Estrategia

- Mapear controles de:
  - ISO 27001 (enfoque de gestión)
  - CIS Controls (enfoque técnico y operativo)
  - Definir niveles de madurez (Inicial → Optimizado)

## 3 Líneas de acción

**1.-Gobierno y liderazgo**

•Políticas y normativas formales

**2.- Gestión de riesgos**

• Identificación de activos críticos
•Evaluación de riesgos (impacto vs probabilidad)
•Plan de tratamiento

**3.- Controles prioritarios (Quick Wins CIS)**

•Inventario de activos (CIS 1)
•Gestión de vulnerabilidades (CIS 7)
•Control de accesos (CIS 6)
•Monitoreo continuo (CIS 8)

# Pilar 2: Trazabilidad del Dato (AREXDATA)

**Objetivo:** : Tener visibilidad total del ciclo de vida del dato: origen, uso, transformación y destino

# Estrategia

•Implementar data lineage + data tracking
•Clasificar la información (crítica, sensible, pública)
•Identificar riesgos asociados al movimiento del dato

### 1. Líneas de acción

- Identificación automática
- Descubrimiento de datos de repositorios
- Mapeo de flujos de información

### 2. Clasificación y etiquetado

- Datos personales
- Datos financieros
- Datos estratégicos

### 3. Monitoreo de uso

1. Quién accede
2. Desde dónde
3. Qué hace con el dato

### 4. Análisis de riesgo del dato

- Exposición
- Transferencias no autorizadas
- Shadow IT

# Pilar 3: Data Loss Prevention (DLP)

**Objetivo:** Prevenir la fuga, filtración o uso indebido de información sensible.

# Estrategia

Implementar Data Loss Prevention (DLP) integrado con clasificación y trazabilidad.

Cubrir los tres frentes:

- Endpoint
- Red
- Nube

# Gracias.

Roberto Cano

**Gerente de Operaciones**

rcano@buromc.com