SPEAKER

Elías Badenes

Solution Architect @ Prodware | Dynamics 365 CE, Azure, Data & AI Solutions

@ebadenes

@errante

¡Gracias a nuestros sponsors!

PLATINO

DQS / INNOVATION ATTITUDE

BETWEEN GROUP

MINSAIT

NTT DATA

TD SYNNEX

U-tad CENTRO UNIVERSITARIO DE TECNOLOGÍA Y ARTE DIGITAL

V-Valley

ORO

CrossPoint

axazure by avvale

algoritmia powered by Alba

prodware

bravent

devoteam

RICOH imagine. change.

encamina PIENSA EN COLORES

KPMG

inetum

COSMOCONSULT

TOKIOTA

PLATA

ayesa

BIZZ SUMMIT TV & CATERING

EQM ENTERPRISE QUALITY MANAGEMENT

COLABORAN

Cienciaterapia

logitech

Microsoft

El Expediente Warren

La Maldición de la Power Platform

#BizzSummit2025

El Expediente Warren

La Maldición de la Power Platform

#BizzSummit2025

Agenda

- **Prologo**: La seductora cabaña en el bosque
- **La Mansión y sus pasadizos**: Superficie de riesgo en Dataverse
- **Los Círculos de Sal**: Controles de gobernanza clave
- **Pasadizos secretos**: Movimientos de datos
- **Rituales de cambio**: ALM y pipelines
- **Sombras que dejan huella**: Auditoría, Purview y CoE
- **Cuando tiembla la tierra**: Copias, DR y límites de plataforma
- **El exorcismo final**: Checklist accionable

La seductora cabaña en el bosque

- Power Platform es increíble ¿**verdad**?
  - Democratiza la creación
  - Acelera la innovación
- Dataverse
  - Metadatos ricos
  - Logica de negocio y validaciones integradas
  - Integracion perfecta con el resto de Aplicaciones y Fabric
  - Seguridad y gestión simplificada
- **Coherencia**, **orden** y todo perfecto, **robusto** y **seguro** por diseño

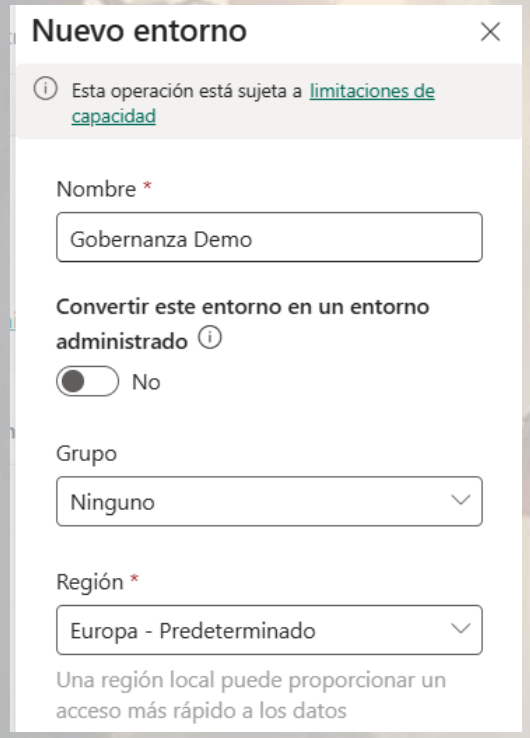
La seductora cabaña en el bosque

- Aparece una app fantasma
  - App "Simple e inocente"
  - Comparte datos PII (Personally Identifiable Information) a un EndPoint externo
  - Conector HTTP sin filtrar
  - Se ejecuta desde IP Publica

La seductora cabaña en el bosque

- ¿¡¿ **Cómo empiezo** ?!?
- Activar entornos administrados (https://r.ebadenes.com/managed-env)
  - Limites de compartición
  - Solution checker
  - Insights de uso
  - IP Firewall
  - IP Cookie Binding
  - Default environment routing

La seductora cabaña en el bosque



Todos los usuarios licencia de Power Apps, Power Automate o Dynamics 365 con derechos de **uso premium** (https://r.ebadenes.com/managed-licensing)

La Mansión y sus pasadizos

Superficie de riesgo en Dataverse

#BizzSummit2025

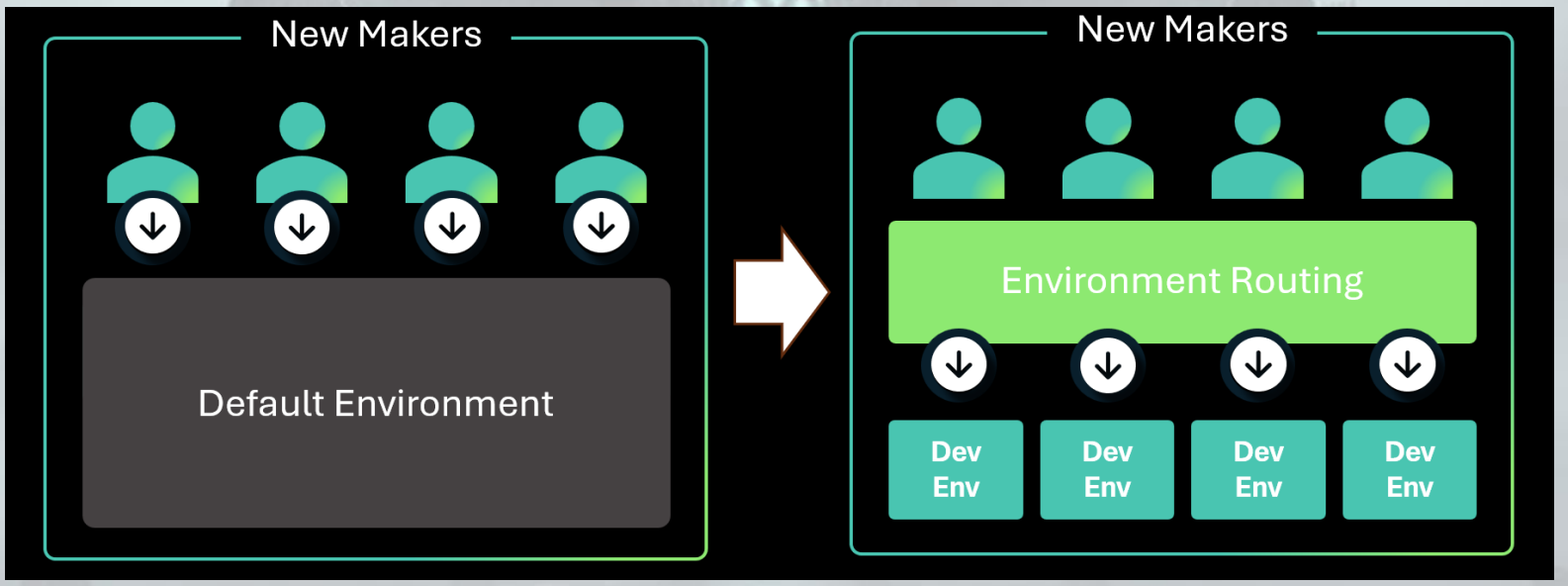
Bizzsummit

La Mansión y sus pasadizos

- ¿Que hay que gobernar?
  - Entornos (Dev / Test / Prod / Default / Personales)
  - Conectores
  - Identidades
  - Endpoints (TDS / SQL y OData),
  - Movimiento de datos (Fabric / Synapse Link / ADF)
  - Seguridad filas / columnas
  - Auditoria
  - Capacidad y limites

La Mansión y sus pasadizos

- Empezar con estrategia de entornos
- Usar Default Environment Routing (https://r.ebadenes.com/env-strategy)



Los Círculos de Sal

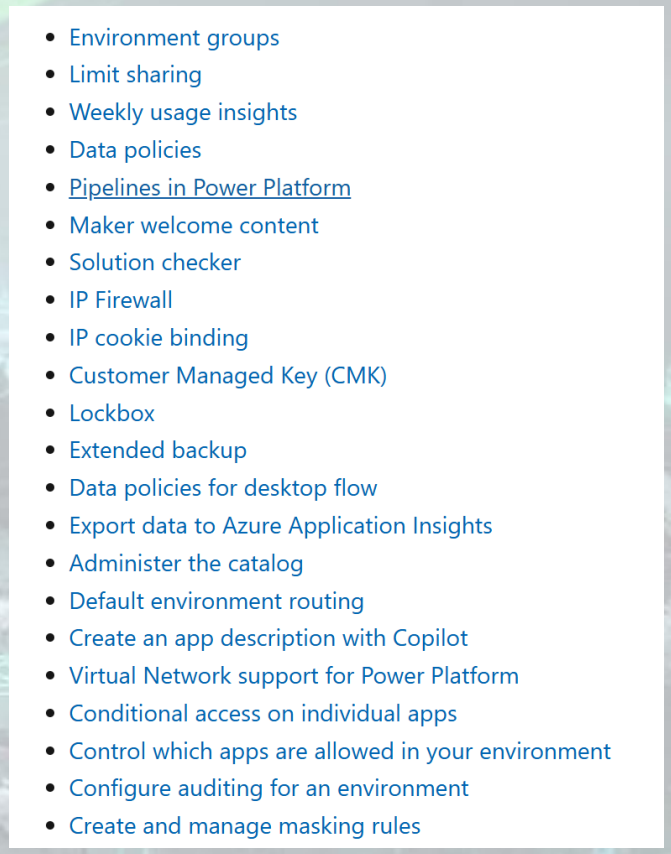
Controles de gobernanza clave

#BizzSummit2025

Bizzsummit

Los Círculos de Sal

- Que activas al administrar un entorno (https://r.ebadenes.com/managed-env)
  - Limit sharing
  - Usage insights semanal
  - Data policies
  - Maker welcome content
  - Solution Checker enforcement
  - IP Firewall, IP cookie binding
  - Lockbox
  - Extended backup
  - Control de apps permitidas
  - etc.



Los Círculos de Sal: Managed Environment

- IP Firewall (https://r.ebadenes.com/ip-firewall)
  - IP's permitidas
  - Bloquea exfiltraciones redes no confiables
  - Consejo: Empieza en **modo auditoria** y luego aplica bloqueos
- IP Cookie binding (https://r.ebadenes.com/ip-binding)
  - Encadena sesión a IP (robo de cookies)

Los Círculos de Sal: DLP y Aislamiento

- DLP Policies (https://r.ebadenes.com/data-policy)
  - Clasifica conectores y define politicas por entorno
- Tenant isolation (https://r.ebadenes.com/tenant-Access)
  - Restringe conexiones entrantes/salientes entre tenants con conectores basados en Entra ID
- App access control
  - Lista blanca/negra de apps que pueden ejecutarse en tu entorno

Los Círculos de Sal: Modelo seguridad DV

- RBAC + Unidades de negocio + Roles + Teams (owner vs access teams) + Jerarquía (por manager o por posición)
- Teams vinculados a grupos de Microsoft Entra
- Seguridad a nivel de columna + reglas de enmascarado (preview) (https://r.ebadenes.com/privacy-mask)
- Control de TDS por usuario o rol
- CMK (Customer-Managed Key): Cifra datos en reposo con tu clave (en Key-Vault)

#BizzSummit2025

Bizzsummit

Pasadizos secretos

- Fabric Link: “atajos” desde Dataverse a OneLake (sin ETL, sin copia)
- Azure Synapse Link para Dataverse: exporta casi en tiempo real a ADLS Gen2
- **Consejo**: Combina con DLP, endpoint filtering y tenant isolation para que “el túnel” no se convierta en “portal a otra dimensión”

Rituales de cambio

ALM y pipelines

#BizzSummit2025

Bizzsummit

Rituales de cambio

- Solutions (managed/unmanaged) y capas
- Pipelines en Power Platform
- Build Tools (Azure DevOps) y Actions (GitHub)
- Buenas prácticas ALM

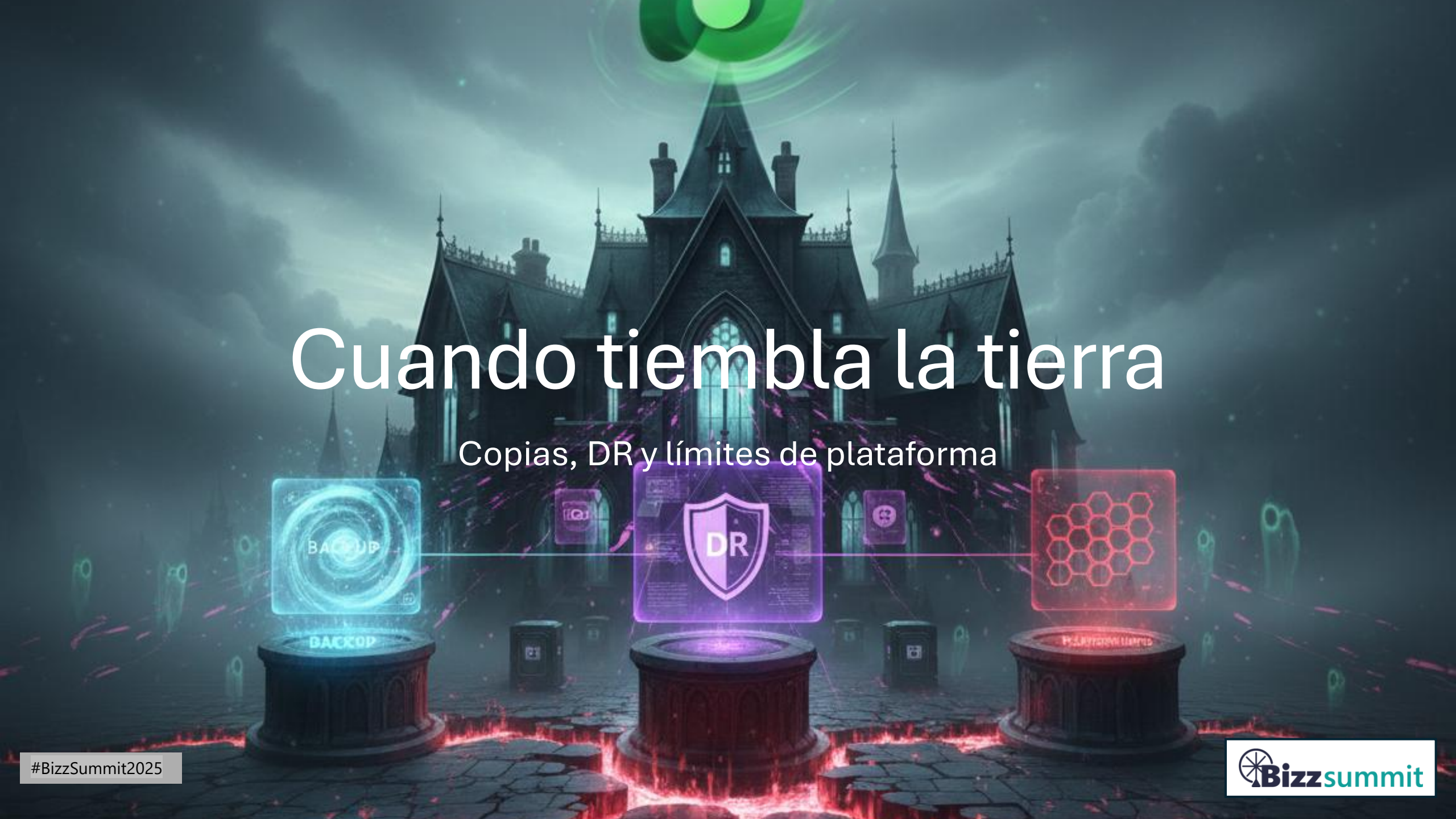

Sombras que dejan huella
Auditoría, Purview y CoE
#BizzSummit2025
Bizzsummit

Sombras que dejan huella

- Auditoría en Dataverse: cambios, accesos, operaciones
- Microsoft Purview + Dataverse
- CoE Starter Kit: inventario, analítica y automatización de cumplimiento

Cuando tiembla la tierra

Copias, DR y límites de plataforma



Bizzsummit

Cuando tiembla la tierra

- Capacidad: Vigila consumos y activa “extensión temporal” si es necesario
- Límites de solicitudes (throttling)
- Backup/Restore & BCDR

El exorcismo final

Checklist accionable

El exorcismo final: Los 12 mandamientos

1. **Habilita Managed Environments** en los entornos críticos
   Habilita controles avanzados (uso, seguridad, límites de compartición, etc.)
2. **En** Default: **Environment Routing** + “maker welcome content” con normas
   Evita que el Default se convierta en el “área gris”
3. **DLP**: políticas **por entorno/grupo**, **endpoint filtering** y **tenant isolation**
   Define qué conectores se pueden, denegar/permitir endpoints y tenants
4. **Activa IP Firewall** (primero en modo auditoría), y **cookie binding**
   Detiene exfiltración desde ubicaciones no confiables y el robo de sesión
5. **TDS deshabilitado** (o limitado por usuario/rol)
   Evita extracciones masivas no controladas por SQL
6. **Modelo** de seguridad con **BU + roles + teams** (Entra groups) +**hierarchy** solo donde aplique
   Separación de deberes, control de columnas, y ofuscación selectiva

El exorcismo final: Los 12 mandamientos

7. **Column security** + **masking rules** para PII
   Separación de deberes, control de columnas, y ofuscación selectiva
8. **Purview**: registra Dataverse, clasifica y aplica **sensitivity labels**
   Clasificación y búsqueda unificada
9. **CMK** si tu sector/cliente lo exige
   Control total y exclusivo sobre cifrado de datos
10. **ALM**: solutions, pipelines, Solution Checker enforced, referencia de conexiones
    Despliegues repetibles y controles automáticos de calidad
11. **Auditoría** + **CoE** para telemetría continua
    Evidencias de acceso y cambios y automatización de gobernanza
12. **Backups y DR** probados (no solo configurados)
    Resiliencia y respirar ante desastres

El exorcismo final: Consejos finales

Configurar en 3 fases:

1. Cortafuegos y exfiltración (1 – 5)
2. Seguridad y datos sensibles (6 – 9)
3. Operación continua (10 – 12)

¡Gracias a nuestros sponsors!