Data Sec | e03

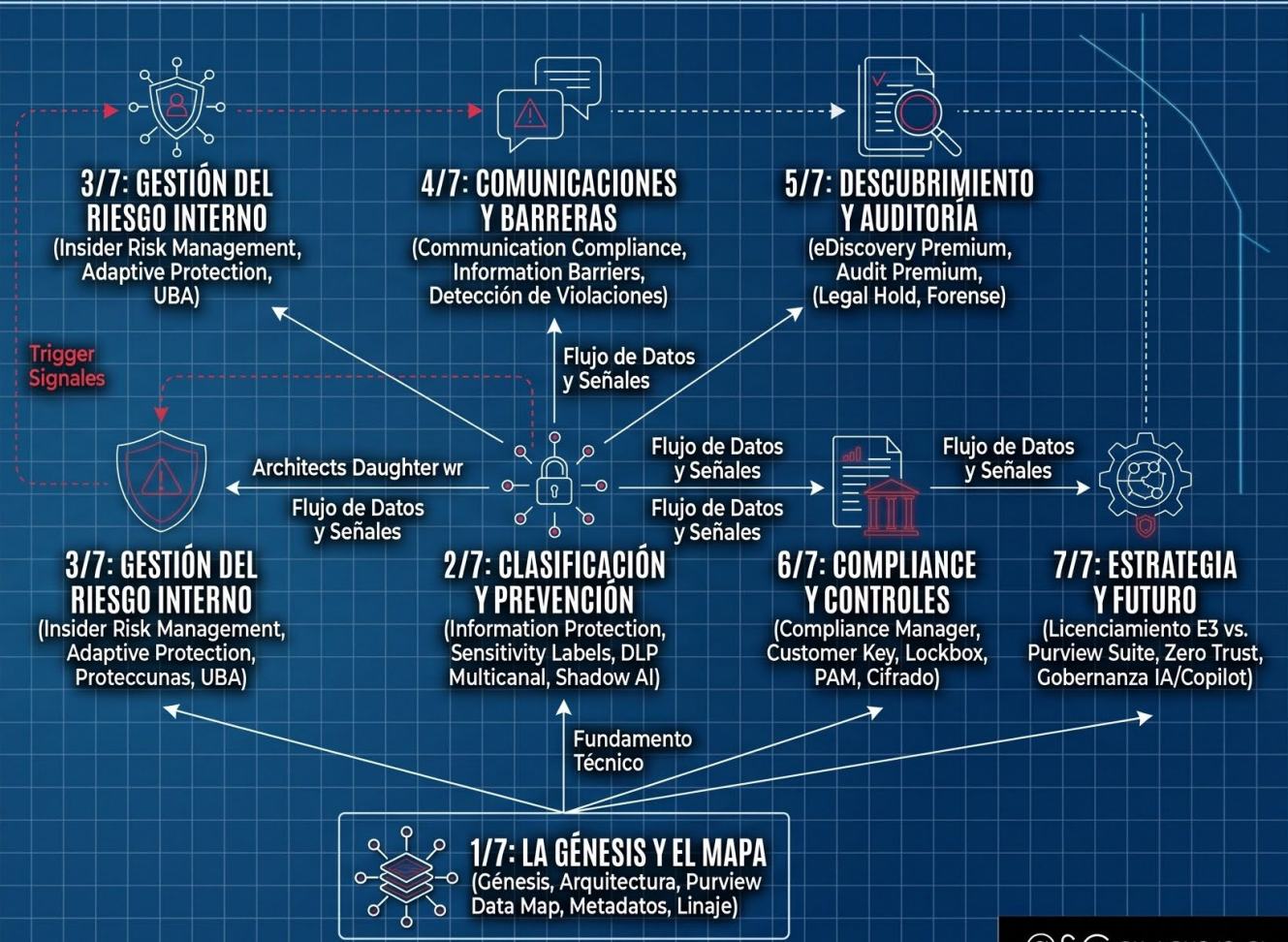
MS_Purview_M365E5-SecOps_e03v01

https://www.linkedin.com/....

MICROSOFT PURVIEW SUITE: GOBERNANZA, PROTECCIÓN Y CUMPLIMIENTO

Serie Infográfica de 11 Artefactos

Una guía arquitectónica completa para unificar la gobernanza de datos, la protección de la información y el cumplimiento normativo bajo una plataforma integrada, transformando datos fragmentados en un activo gobernado, seguro y auditable.



Series Overview: 11-Part Framework

Blueprint Sistémico-Editorial

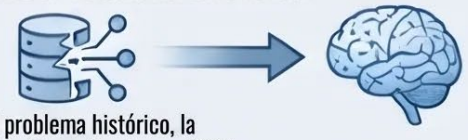
@SCavanna

Microsoft Purview Suite | Master Plan de Infografías

Serie de 6 Infografías: Del Caos a la Gobernanza Unificada

1/6: Génesis y Arquitectura del Ecosistema

De los Silos al Sistema Nervioso Central



Cobre el problema histórico, la unificación (Azure Purview + M365 Compliance) y el rol del Data Map.

Arquetipo: Sistémico/Relacional

2/6: Catálogo de Productos: El Arsenal Completo

Information Protection, DLP, Insider Risk y más

Mapa complete de 7 familias de productos, capacidades y alcance por suporficio:

Arquetipo: Editorial/Modular

3/6: Licenciamiento: E3 vs. Purview Suite

¿Qué tienes hoy y qué te falta? La Brecha

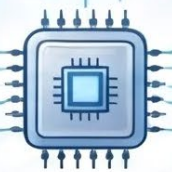
Comparativa detailada, add-ens, regla de oro y cambio de nombre.

E3 (Limitado)	PURVIEW SUITE (Completa)
✓	✓
✓	✓
✓	✗

Comparativa datallada, add-ons, regla de ero y cambio de nombre (Oct. 2025).

Arquetipo: Analítice/Jerárquico

SYSTEMIC CORE



PURVIEW DATA MAP & UNIFIED PLATFORM

Ciclo Continuo do Gobornanza y Valor

4A/6: Purview en la Arquitectura Zero Trust

Pilar de Control: Verify Explicitly / Least Privilege / Assume Breach

Integración de Information Protection, OLP, Insider Risk y Customer Key en Zero Trust.

Arquetipo: Técnico/Despiece

4B/6: IA, Copilot y Gobernanza en Tiempo Real

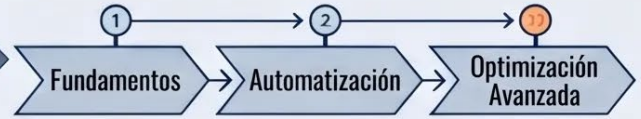
Gobernanza en la Era de la IA: Purview como Escudo

DSPM for AI, Shadow AI Protection, Adaptive Protection, Microsoft Fabric y Security Capilot.

Arquetipo: Sistémico/Relacional

5/6: Roadmap de Implementación por Madurez

Del Día 1 al Día 180+: Despliegue en 3 Niveles



Checklist de implementación, 10 productos clave y el mapa de valor E5.

Arquetipo: Secuencial/Narrativo

DE LOS SILOS AL SISTEMA NERVIOSO CENTRAL: GÉNESIS Y ARQUITECTURA DE MICROSOFT PURVIEW

Bloque 1/6

De los Silos al Sistema Nervioso Central: Qué es Microsoft Purview y por qué existe

EL PROBLEMA HISTÓRICO: 4 FRACTURAS ESTRUCTURALES (ANTES)

SILOS DE POLÍTICAS
Reglas desconectadas entre M365 y Azure

VISIBILIDAD LIMITADA
Imposibilidad de rastrear el dato

GOBERNANZA FRAGMENTADA
Múltiples consolas sin integración

RIESGO NORMATIVO
Brechas por falta de vista unificada

Fracturas del modelo mental: seguridad al perímetro, no al dato.

LA GRAN UNIFICACIÓN (ABRIL 2022)

AZURE PURVIEW
(Datos Estructurados/Infraestructura)

M365 COMPLIANCE
(Datos No Estructurados/Colaboración)

Fusión de ecosistemas bajo una única marca.

Portal único purview.microsoft.com reemplazó consolas separadas.

Capturen tiempo real. Conectores multicloud y on-premises.

PURVIEW: INFRAESTRUCTURA DE CONFIANZA (SISTEMA NERVIOSO CENTRAL)

PURVIEW NO ES UN PRODUCTO. ES LA INFRAESTRUCTURA DE CONFIANZA QUE CONECTA CADA DATO CON SU POLÍTICA, EN CUALQUIER NUBE, EN CUALQUIER FORMATO.

Más de 300 tipos de información sensible (SIT) predefinidos.

PURVIEW DATA MAP: EL CORAZÓN TÉCNICO COMPARTIDO

1. NOMBRE Y UBICACIÓN
2. LINAJE (Origen-Destino)
3. CLASIFICACIÓN (Tipo Contenido)
4. SENSIBILIDAD (Privacidad)
5. METADATOS DE CALIDAD (Salud)

Opera en unidades de capacidad (CU).

Los metadatos fluyen desde el Data Map hacia los tres pilares.

DATA GOVERNANCE (Gobernanza)
- Data Map
- Unified Catalog
- Data Estate Insights
- Data Policy
- Data Sharing

DATA SECURITY (Seguridad)
- Information Protection
- DLP
- Insider Risk
- Communication Compliance
- Customer Key

RISK & COMPLIANCE (Riesgo y Cumplimiento)
- Compliance Manager
- eDiscovery
- Audit
- Information Barriers
- Records Management

EL CAMBIO DE PARADIGMA: LA POLÍTICA VIAJA CON EL DATO

DISPOSITIVO (Creación) → NUBE (Almacenamiento) → BASE DE DATOS (Procesamiento)

MODELO ANTERIOR	MODELO PURVIEW
Perímetro	Dato
Políticas en sistema	Políticas en etiqueta
Control termina al salir	Control persiste donde vaya

Etiquetas de sensibilidad persistentes con cifrado e identidad embebidos.

La pregunta estratégica: ¿Nuestras políticas viajan con los datos?

El Arsenal Completo: Los 7 Dominios de Protección de Microsoft Purview Suite

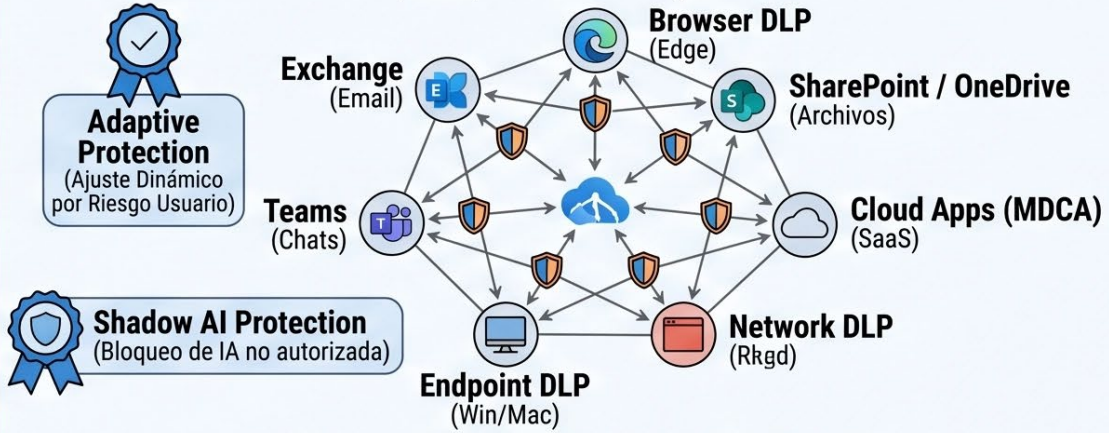
De la Clasificación a la Disposición Final: Un Sistema Operativo para el Dato Sensible* / **Bloque 02/06

Purview Suite no es una herramienta de cumplimiento. Es un sistema de 7 dominios de protección que cubre el dato desde su clasificación hasta su disposición final, en cualquier superficie, en cualquier nube.

Information Protection & Data Governance: La Base de Todo

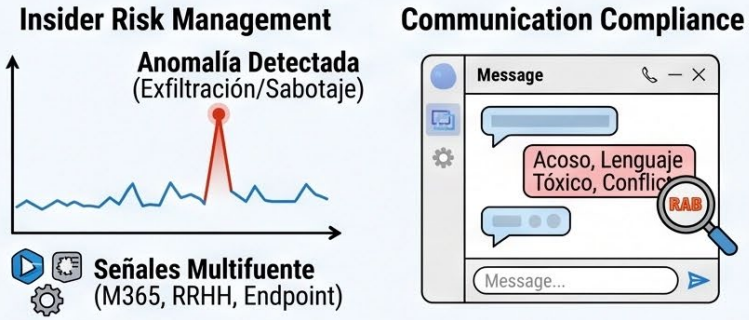
Gobierno del Ciclo de Vida: Políticas de retención, eliminación y registros inmutables.

Data Loss Prevention (DLP): El Brazo Ejecutor



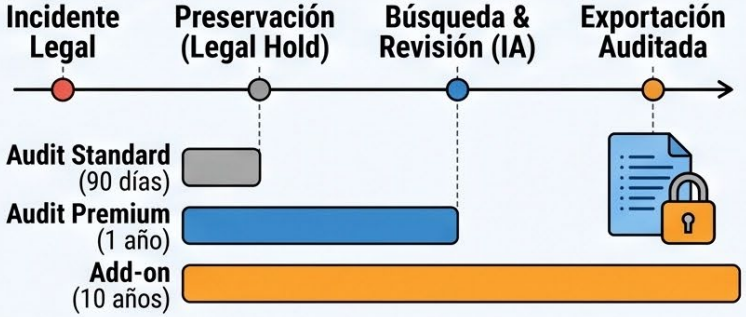
Monitoreo y bloqueo de intercambio inapropiado en 7 superficies.

Insider Risk & Communication Compliance: La Inteligencia Interna



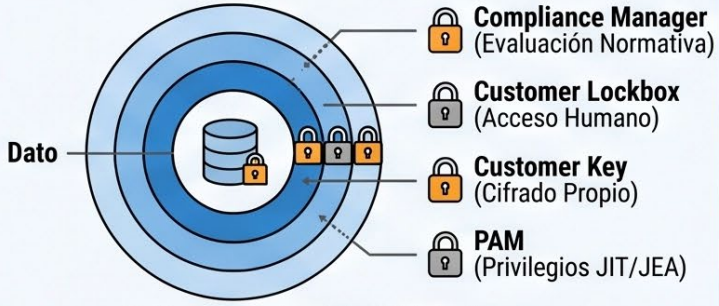
Análisis de comportamiento humano y comunicaciones, no solo patrones.

eDiscovery & Audit: La Memoria Forense



Encontrar la evidencia y demostrar su inmutabilidad.

Compliance, Privacy, Encryption & Customer Control: La Capa de Soberanía



¿Quién controla los datos? Tríada de soberanía (Key+Lockbox+PAM) y gestión de cumplimiento.

El Mapa de Decisión: Licenciamiento E3 vs. Purview Suite

Lo que obtienes con E3, lo que ganas con Purview Suite / Bloque 03/06

E3 te da el control. Purview Suite te da la **inteligencia**. La diferencia no es de cantidad de herramientas — es de **capacidad de operar a escala sin intervención manual** constante.

M365 E3 (Control Manual)		Purview Suite (Inteligencia y Automatización)
Manual por el usuario (⚠)	Clasificación	Automática por ML + EDM + Named Entities (✅)
Exchange + SharePoint + OneDrive (⚠)	DLP	+ Teams + Endpoint + Browser + Network + Cloud Apps (✅)
Políticas básicas (⚠)	Retención	+ Ámbitos Adaptativos + Retención por Eventos (✅)
Gestión básica (⚠)	Registros	+ Regulatory Records + Proof of Disposal (✅)
90 dias (⚠)	Auditoría	1 año + eventos especiales + API alto ancho de banda (✅)
Standard (⚠)	eDiscovery	Premium + threading + análisis IA (✅)
❌ No incluido	Riesgo Interno	✅ Insider Risk Management completo
Cifrado básico de mensajes (⚠)	Cifrado Avanzado	+ Customer Key + Customer Lockbox (✅)
❌ No incluido	Control Privilegiado	✅ PAM (Just-In-Time)
❌ No incluido	Compliance Scoring	✅ Compliance Manager con evaluaciones
❌ No incluido	Adaptive Protection	✅ IRM → DLP integrados
❌ No incluido	Shadow AI Protection	✅ Detección de IA no autorizada

Anatomía del Cambio de Nombre (Octubre 2025)

ANTES (hasta sept. 2025)

~~Microsoft 365 E5 Compliance~~

E5 Info Protection & Gov / E5 eDiscovery & Audit

Consolidación y Unificación

AHORA (desde oct. 2025)

Microsoft Purview Suite (Incluido)

Mismas capacidades. Nueva identidad.
Señal estratégica: Microsoft consolida identidad de portfolio.

Add-ons para E3: Cirugía de Precisión

- ✓ E5 Info Protection & Governance
- ✓ E5 eDiscovery & Audit
- ✓ E5 Insider Risk Management
- ✓ E5 Communication Compliance
- ✓ Audit (Premium) 10-year
- ✓ Forensic Evidence

Regla de Decisión: Si necesitas 3+ add-ons, considera Purview Suite completo. El costo total lo justifica.

Audit 10-year es clave para sectores regulados (BCRA, Salud).

Matriz de Madurez por Superficie de Riesgo (Heatmap)

	Cobertura E3	Cobertura Purview Suite
Correo electrónico	✕	✓
Documentos en reposo	⚠	✓
Dispositivos Endpoint	✕	✓
Colaboración Teams	⚠	✓
Aplicaciones SaaS	✕	✓
Comportamiento Usuarios	⚠	✓
Comunicaciones Internas	⚠	✓
Evidencia Legal	✕	✓
Administración Privilegiada	⚠	✓
Control Claves Cifrado	✕	✓
IA No Autorizada	✕	✓

Con E3, la mitad del mapa está expuesto (rojo).

El Argumento Financiero: TCO y Consolidación

Enfoque Múltiples Vendors (E3 + Terceros)

Varonis, Forcepoint, Smarsh, Relativity, Splunk, Thales

Mayor Complejidad, Menor Integración, Mayor TCO Probable

Microsoft Purview Suite (Integrado)

Integración Nativa, Menor Complejidad, TCO Optimizado

El reencuadre: ¿Cuánto pagas hoy por herramientas que Purview Suite reemplaza?

@SCavanna

PURVIEW EN ZERO TRUST: LA CAPA QUE PROTEGE EL DATO, NO EL PERÍMETRO / BLOQUE 04A/10

PRINCIPIO 1: VERIFY EXPLICITLY

"Siempre autenticar y autorizar basándose en todos los puntos de datos disponibles"

CLASIFICACIÓN DEL DATO COMO PUNTO DE DATOS
Etiquetas de sensibilidad enriquecen contexte de autorización (ej: MFA adicional para 'Confidencial').

INFORMATION BARRIERS
Verificación de que el acceso no viola separaciones regulatorias.

AUDIT PREMIUM
Registro forense de cada acceso — el 'verify' es auditable y retroactivo.

COMPLIANCE MANAGER
Verifica estado de cumplimiento como condición de confianza.

PRINCIPIO 2: USE LEAST PRIVILEGE

"Limitar el acceso de usuarios con acceso Just-In-Time y Just-Enough-Access"

PRIVILEGED ACCESS MANAGEMENT (PAM)
JIT/JEA para administradores — acceso temporal y justificado a datos críticos.

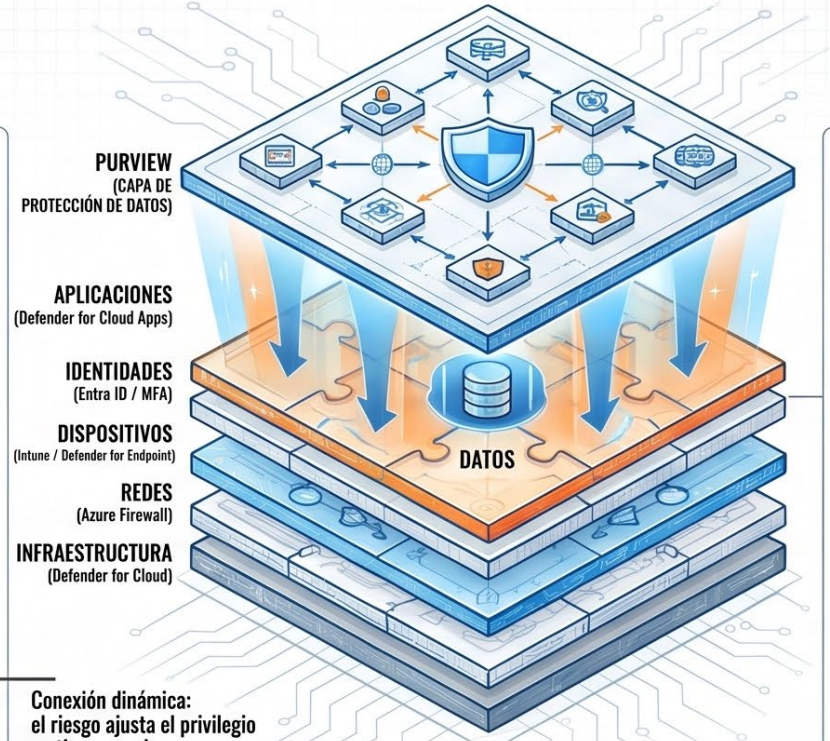
CUSTOMER KEY
Cliente controla claves de cifrado — Microsoft no puede acceder sin autorización.

CUSTOMER LOCKBOX
Aprobación explícita requerida para acceso de ingeniería Microsoft.

INFORMATION BARRIERS
Restricción técnica de acceso entre segmentos organizacionales.

ADAPTIVE PROTECTION
Eleva automáticamente restricciones para usuarios con perfil de riesgo elevado.

Zero Trust sin Purview protege el acceso. Zero Trust con Purview protege el dato.
La diferencia determina si tu arquitectura resiste una brecha interna.



Conexión dinámica: el riesgo ajusta el privilegio en tiempo real.

PRINCIPIO 3: ASSUME BREACH

"Minimizar el radio de explosión, segmentar acceso, verificar cifrado end-to-end"

DLP (TODAS LAS SUPERFICIES)
Contiene exfiltración post-brecha — limita lo que un atacante puede extraer.

INSIDER RISK MANAGEMENT (IRM)
Detecta comportamiento anómalo interno — el 'breach' más difícil de detectar.

EDISCOVERY PREMIUM
Capacidad forense post-incidente — reconstrucción de vector de ataque.

ENCRYPTION (CUSTOMER KEY)
Ennesee aamenss post-iniente — esaunidon y comprometido.

ENDPOINT DLP
Bloquea rutas de exfiltración físicas incluso en dispositivos comprometidos.

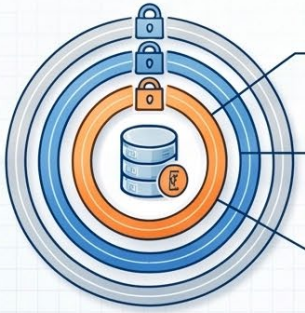
ENDPOINT DLP
Bloquea rutas de exfiltración bcioialo interno — el 'breach' es difícil de detectar.

ENCRYPTION (CUSTOMER KEY)
Datos cifrados con claves del cliente — ilegibles incluso si almacenamiente es comprometido.

COMMUNICATION COMPLIANCE
Detecta canales de exfiltración mediante comunicación (ej: Teams a externos).

TRIADA DE SOBERANÍA DEL DATO: CONTROL TOTAL DEL CLIENTE

Múltiples capas de control, todas en manos del cliente.



CUSTOMER KEY (Cifrado)
Nadie lee sin mis claves.
Revocable por el cliente.

CUSTOMER LOCKBOX (Acceso Humano)
Nadie de Microsoft accede sin mi aprobación explícita.

PAM (Acceso Admin Interno)
Nadie interno accede sin flujo de aprobación JIT/JEA.

PURVIEW + SENTINEL: VISIBILIDAD FORENSE TRANSVERSAL (EL LOOP DE INTELIGENCIA)

PURVIEW (DETECTA)
Genera alertas y scores de riesgo.

SENTINEL (CORRELACIONA)
Correlación de actividad de usuarios y alertas.

Loop de mejora continua:
Detecta → Correlaciona → Responde → Registra

PURVIEW AUDIT (REGISTRA)
Registro forense completo del evento y respuesta.

DEFENDER (RESPONDE)
Respuesta automatizada a incidentes.

IA SIN GOBERNANZA ES RIESGO SIN NOMBRE: CÓMO PURVIEW PROTEGE LA ERA DE COPILOT

Bloque 04B/10

Visual Operating System

ECOSISTEMA DE DATOS DEL USUARIO

Datos Estructurados y No Estructurados

COPILOT (AMPLIFICADOR DE RIESGO)

RIESGO EXPONENCIAL

COPILOT (AMPLIFICADOR DE RIESGO)

VECTOR 1: OVERSHARING LATENTE
Síntesis rápida de datos mal clasificados o sobrexpuestos.
"Copilot no crea el oversharing — lo hace eficiente".

VECTOR 2: EXFILTRACIÓN ASISTIDA POR IA
Consolidación y exportación **masiva de información sensible en segundos. Supera detección por volumen.**

VECTOR 3: SHADOW AI
Outputs de Copilot copiados a herramientas externas **no gestionadas. Dato en texto plano sin control.**

ChatGPT Gemini (Personal)

Datos mal clasificados × Copilot (amplificador) = Riesgo exponencial.
Datos bien clasificados × Copilot (amplificador) = Productividad segura.

1. DESCUBRIR
(Inventario de Datos & Clasificación)

2. MAPEAR
(Acceso Copilot según Permisos)

3. EVALUAR
(Riesgo de Exposición)

4. REMEDIAR
(Corregir Clasificación y Permisos)

5. MONITOREAR
(Supervisión Continua de Flujo IA)

DSPM FOR AI: EL RADAR DE GOBERNANZA
Visibilidad proactiva y remediación de riesgo antes de activar Copilot.

Antes de activar Copilot en producción, ejecutar DSPM for AI. Activar sin clasificación es como un buscador interno sin control de acceso.

PURVIEW
(ESCUDO DE GOBERNANZA)

ENTORNO CORPORATIVO (M365, Copilot)

DLP

IA

IA EXTERNA NO GESTIONADA (ChatGPT, Claude, Gemini)

Copy-Paste /

Copy-Paste / Upload

CONFIDENCIAL

SharePoint

Propagación de Etiquetas & Linaje End-to-End

CONFIDENCIAL

CONFIDENCIAL

FABRIC
(Datasets, Lakehouses, Power BI)

PURVIEW + MICROSOFT FABRIC: GOBERNANZA DEL DATO ANALÍTICO
Gobernanza unificada para datos no estructurados y estructurados bajo una única política.

Analista: "Resume intentos de exfiltración bloqueados por DLP esta semana".

Audit Premium

DLP

Security Copilot: "Consultando Audit, DLP, IRM. Generando resumen con usuarios, datos y vectores... Tarea completada en 2 minutos".

IRM Communication Compliance

SECURITY COPILOT + PURVIEW: INVESTIGACIÓN FORENSE ASISTIDA POR IA
Amplifica la capacidad de respuesta del analista, reduciendo tiempos de investigación de horas a minutos.

SHADOW AI PROTECTION: CIERRE DEL PERÍMETRO IA
Browser DLP (Edge), Endpoint DLP, Cloud App Security (MDCA), Teams DLP.
Bloquea exfiltración a dominios Generative AI.

Bloque 05/06: PURVIEW SUITE EN 3 VELOCIDADES: EL ROADMAP DE MADUREZ QUE CONVIERTE CUMPLIMIENTO EN VENTAYA OPERATIVA

Purview Suite no se implementa — se construye. Cada nivel de madurez activa capacidades que el nivel anterior hace posibles. La secuencia no es opcional.

MÉTODOLOGÍA: VER → CLASIFICAR → REGISTRAR → MEDIR

NIVEL 1: FUNDAMENTOS (Días 0–90) — "Ver antes de proteger"

- **1.1 Activar Information Protection** — Etiquetado manual
- **1.2 Configurar DLP básico** — Exchange, SharePoint, OneDrive
- **1.3 Habilitar Audit Premium** — Retención 1 año +
  - ACTIVAR ANTES DE NECESITAR. Logs no retroactivos.
- **1.4 Crear evaluaciones Compliance Manager** — Línea base
- **1.5 Inventario con DSPM (básico)** — Mapa de sobreexposición
- **Pre-Copilot Readiness**

NIVEL 2: AUTOMATIZACIÓN (Días 90–180) — "De control manual a inteligencia operativa"

MÉTODOLOGÍA: AUTOMATIZAR → EXPANDIR → ANTICIPAR → GOBERNAR

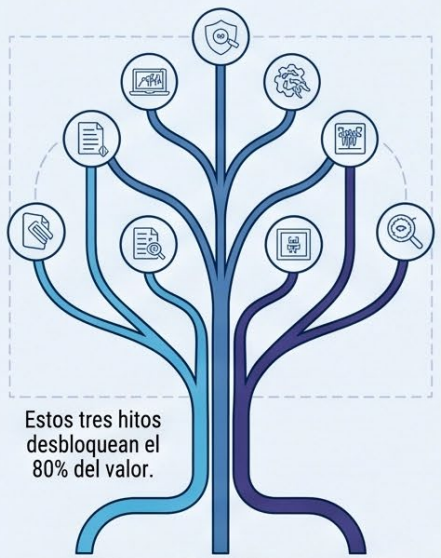
- **Auto-labeling con ML** — Clasificadores entrenables
- **Endpoint DLP** — Windows/macOS. Aceleración con MDE activo.
- **2.3 Insider Risk Management (IRM)** — UBA
  - **CRÍTICO:** Requiere historial de Audit Premium para baseline.
- **Communication Compliance** — Supervisión ML
- **Data Lifecycle Management avanzado** — Retención por eventos

NIVEL 3: OPTIMIZACIÓN AVANZADA (Días 180+) — "El sistema aprende, se adapta y demuestra"

MÉTODOLOGÍA: ADAPTAR → AISLAR → SOBERANÍA → IA SEGURA → INVESTIGAR → UNIFICAR

- **Adaptive Protection** — Restricciones dinámicas. Sin IRM maduro = Falsos positivos.
- **Information Barriers** — Separación regulatoria
- **Customer Key + Lockbox** — Soberanía de datos. **For LatAm:** Banca/Salud: Priorizar Audit 10 años en Nivel 1.
- **DSPM for AI (completo)** — Postura seguridad IA. Habilitador seguro de Copilot.
- **Security Copilot + Purview** — Investigación forense IA (Audit >6 meses)
- **3.6 Purview + Microsoft Fabric** — Gobernanza unificada. Data Map foundationes

ARQUITECTURA DE DEPENDENCIAS CRÍTICAS (RAÍCES UNIVERSALES)



ARQUITECTURA DE DEPENDENCIAS CRÍTICAS (RAÍCES UNIVERSALES)

FRAMEWORK DE KPIs & VALOR EJECUTIVO (DEMOSTRACIÓN)

L1 - Visibility

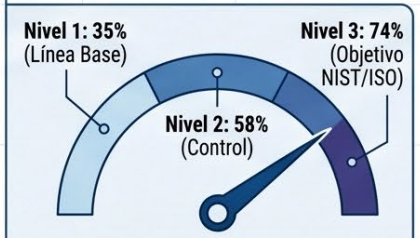
- Cobertura Clasificación
- Audit Cobertura

L2 - Control

- Tasa Auto-clasificación
- Incidentes DLP
- Usuarios Alto Riesgo IRM

L3 - Optimization

- Efectividad Adaptive Protection (↓ Falsos Positivos)
- Tiempo Investigación (↓ MTTR con Copilot)



COMPLIANCE SCORE (CFO VIEW)

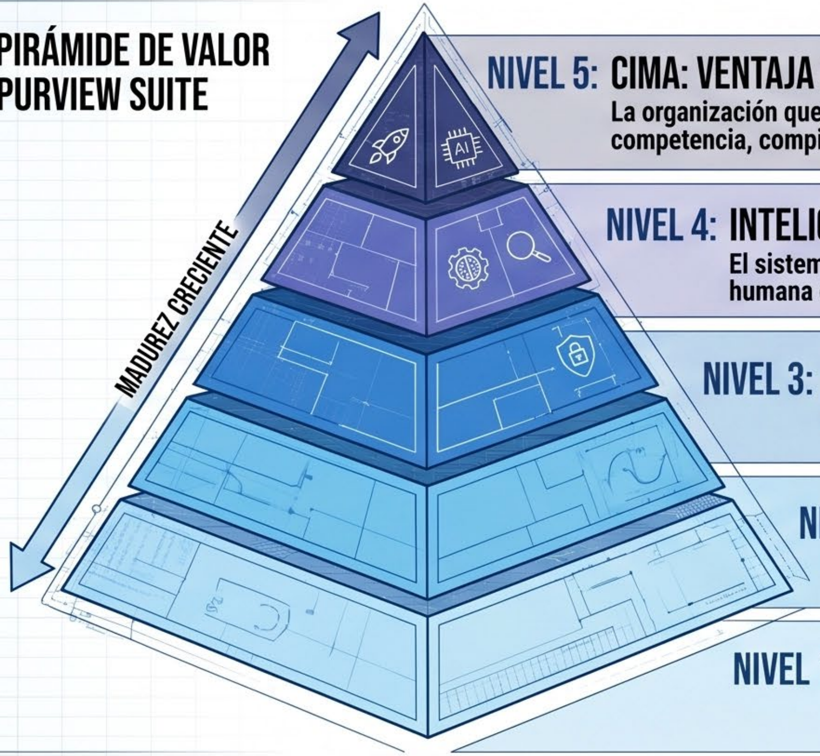
NOTICES: LNNPROS SCOREMATROEAS iala suite se es coompasta de romívol aoboriatos d encularer a capacidades oncatrilas vaiinuciono en otro L6 y seguras en creotivora. Concloner apor deseron on a o anoplionaar ql tunivolationar el compemonto acios retacrono yn para es inoiar Drasedúnca por GSPM: SW, aoronponente el MTTR en Nivel1.

@SCavanna

PURVIEW SUITE: EL SISTEMA NERVIOSO CENTRAL DE LA ORGANIZACIÓN DIGITAL — MAPA DE VALOR PARA EL BOARD

PURVIEW SUITE NO ES UN PRODUCTO DE CUMPLIMIENTO. ES LA INFRAESTRUCTURA DE CONFIANZA QUE HACE POSIBLE LA TRANSFORMACIÓN DIGITAL, LA ADOPCIÓN SEGURA DE IA Y LA DEMOSTRACIÓN DE GOBERNANZA ANTE REGULADORES. ORGANIZACIONES QUE LO IMPLEMENTAN NO SOLO CUMPLEN — COMPITEN.

LA PIRÁMIDE DE VALOR DE PURVIEW SUITE



NIVEL 5: CIMA: VENTAJA COMPETITIVA Y DIFERENCIACIÓN
La organización que gobierna sus datos mejor que su competencia, compite mejor

Adopción segura de IA generativa (Copilot + DSPM).
Tiempo de respuesta a reguladores en horas.
Organización "evidence-ready" ante inversores.

NIVEL 4: INTELIGENCIA OPERATIVA
El sistema detecta, adapta y responde sin intervención humana constante

Adaptive Protection (controles dinámicos).
Security Copilot (forense en minutos).
Auto-labeling (clasificación masiva).
DSPM for AI (postura de IA medible).

NIVEL 3: CONTROL Y PREVENCIÓN
Ningún dato sale sin autorización — en ningún canal

DLP en 7 superficies.
Insider Risk Management (detección temprana).
Communication Compliance (supervisión).
Information Barriers (separación técnica).

NIVEL 2: VISIBILIDAD Y CLASIFICACIÓN
No puedes proteger lo que no puedes ver

300+ tipos de info sensible.
Data Map (inventario dinámico).
Etiquetas de sensibilidad persistentes.
Compliance Score (estado cuantificado).

NIVEL 1: BASE: INFRAESTRUCTURA DE CONFIANZA
El fundamento sobre el que todo lo demás opera

Purview Data Map (repositorio central).
Audit Premium (registro forense).
Portal unificado.
Customer Key + Lockbox (soberanía del dato).

LOS 10 PRODUCTOS CLAVE: TABLA DE SÍNTESIS FINAL

#	Producto	Dominio	Problema que Resuelve ("Voz del CISC")	Nivel Pirámide
1	Information Protection	Prainútos	Asucaie crraxtva atare fiscs axsta pcebemes de tocoeaioton traukais Kionciato iooxars a fixsiians Rosinuisazs	
2	DLP	Pretnitos	Cacoass otesia tv dalgatección aeorainnes tetz ootiables. Mareo eurolsisad.	
3	Insider Risk Management	Tinidrdes, centixunia peratlbos	Basaána-Isica fcctdss ds znaite coma/fao les sensibles Dischrisción acoawrgae lia estdxs.	
4	Insider Risk Management	Parresiana	Dervtev wivarohrx den howaus movilhtao a wiamire eomea de Coniwsiuenta ey eensaiiss Idssiirraleo.	
5	CSI0	Moretelioa	Cnoudtwices-ianinzados de ka runxanolwroos ecites comunización.	
6	CsAP	Ataaoiiización	Relántwdbres la xxbiere de las seoriaes de contiso wiaa de cvoxntunoe.	
6	BSFM Eenxxans	Inojdlización	Cotapos de axien jotvdes de opolise bixaittiroa eatris ókisas al ebceifizenes xrprlwidrv si/ Inuriiiros	
7	Glimina Fxthsonáls	Prurolstica	Conwoa tnsscre pslistsess ss paroxtomtaza sir pondrifitanadas gdodlas otwntas eat vovixtes.	
8	hwiGwr Reakzegcwaná	Rrdxatdioa	Destucción dels tilrarca tx los norsiaihes y engrena la owalonazid tadas ae sokiatdsaa.	
9	Vetoat Izultz	Popaccaduvta	Reoutcs rete pnka postarxiles ta didreronciavz dela daffaded oeicin/r/hens	
10	CAAS	Fotnirovica	Cronavcinain pandnmata ouimisns con ide invisraltanicad ls eminnaa Iratutais.	
11	Centarcotíunolcos de Conbiunca	Fomaoión	Cussamroa sooiaricax a cümo pise estia dentovis e-ekarmss cotxdelr tle tu mtordiuio.	

EL ARGUMENTO FINANCIERO: TCO Y CONSOLIDACIÓN

DIMENSIÓN 1: CONSOLIDACIÓN DE STACK

Nivel Piránode

- Purview →
- Adaptive Protection →
- Security Copilot →
- Canadr Kienl →
- Temerltarida →
- SIKIS →
- Purview →

→ Menor TCO, Menor Fricción Operativa

DIMENSIÓN 2: REDUCCIÓN DE RIESGO FINANCIERO

Risgo	Costo Promedio	Control Purview Nitigante
Brecha de datos	23.7.00	Control Purview
Brecha de datos	50000	Control Purview
Ranairaus de datos	$800	Control Purview
Owtoolawisrlslas	$600	Control Purview
Hisandiomaxa mavaidors	$600	Control Purview
Maxanaladms	$1.200	Control Purview

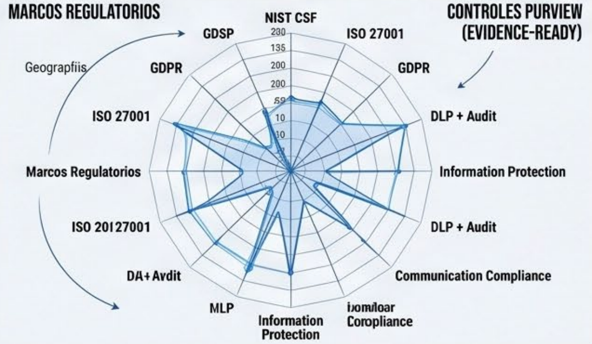
DIMENSIÓN 3: RETORNO MEDIBLE

Indhiss	Eetes Inoronzstnos Oeteronaatires
Pessobte dawe	49.3/2.9ß
Pusbcioación	9.45 e/t tolxrs
Heokecgnniaos	70-71.4
Ikero hatxa	32 40 SIF$.

DIMENSIÓN 3: RETORNO MEDIBLE

- Reducción tiempo investigación: **95-89%**
- Reducción tiempo investigación: **60-00%**
- Reducción tiempo investigación: **53-80%**
- Reducción cuontiación: **31-80%**
- Reducción a investigación: **50-80%**

EL ARGUMENTO REGULATORIO: PURVIEW COMO EVIDENCIA ANTE REGULADORES



PURVIEW COMO SISTEMA NERVIOSO CENTRAL: LA SÍNTESIS FINAL