Data Sec | E 01

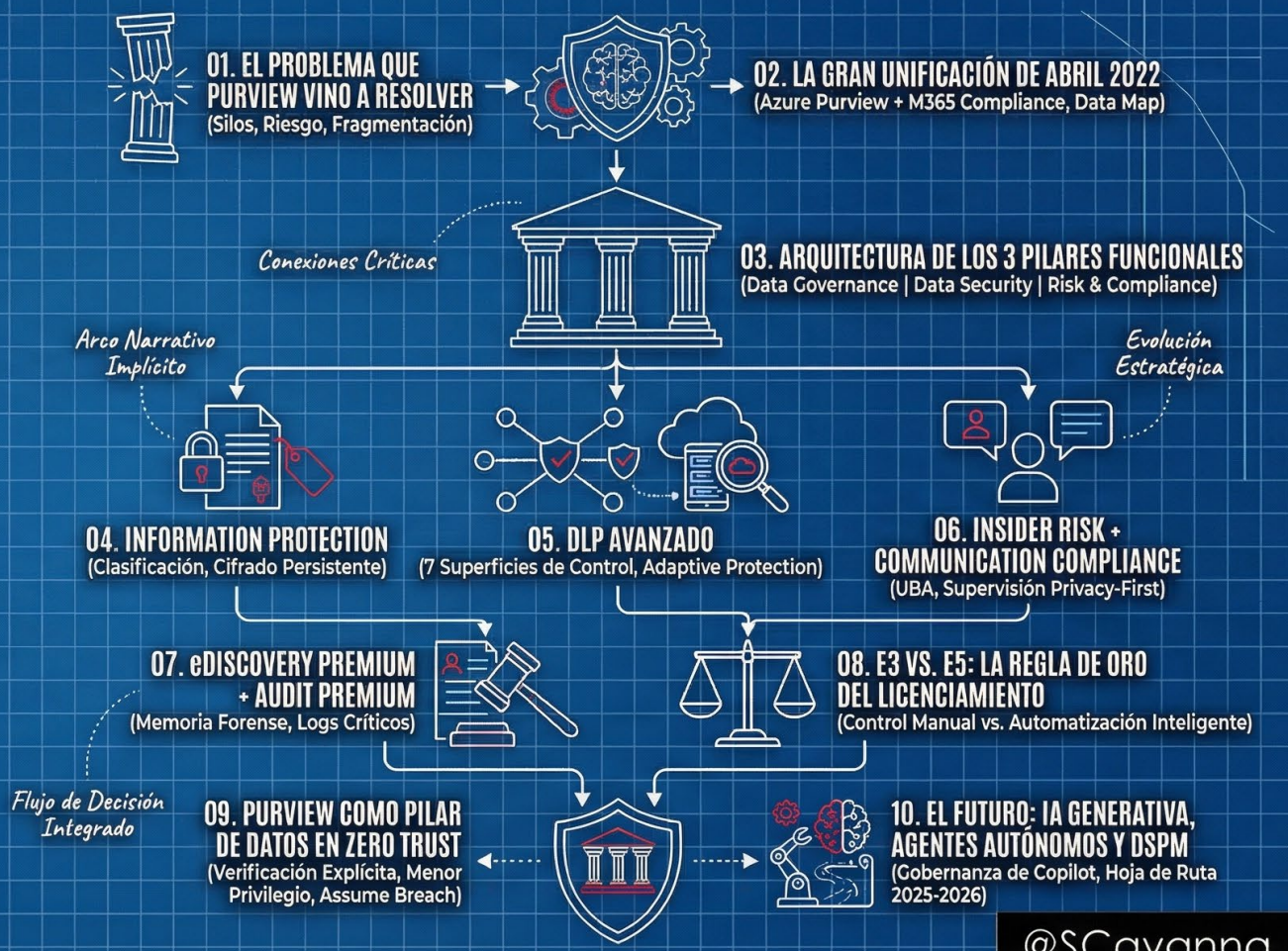
MS_Purview_M365E5-SecOps_e01v01

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

MICROSOFT PURVIEW EN M365 E5 / E5 COMPLIANCE: SERIE INFOGRÁFICA DE 10 ARTEFACTOS

(Índice y Arco Narrativo Sistémico)

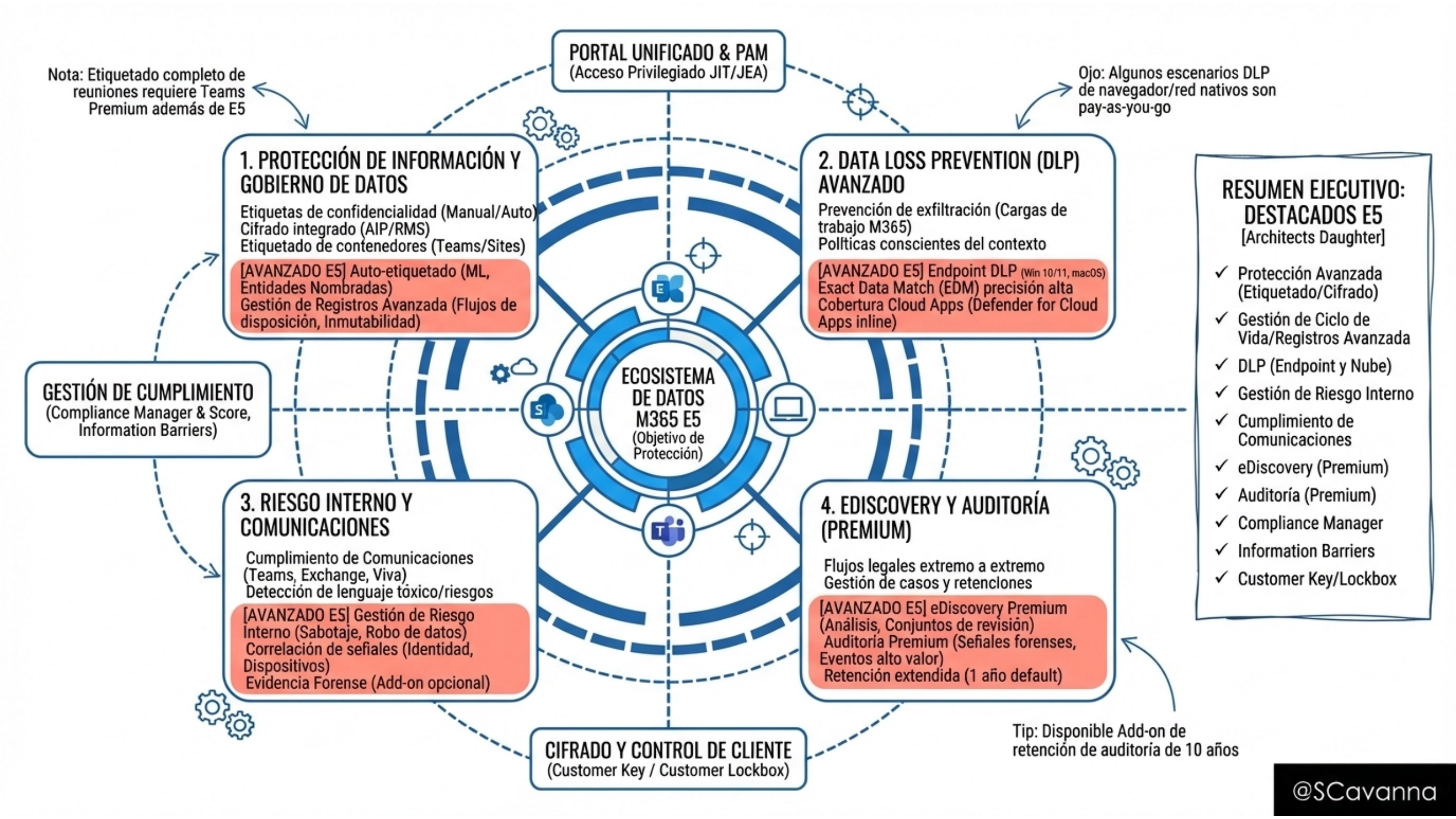
Una exploración profunda del ecosistema de gobernanza, seguridad y cumplimiento de datos. Desde la resolución de fallos estructurales hasta la arquitectura unificada, capacidades avanzadas, defensa contra amenazas internas, gestión forense y el futuro con IA y Zero Trust. Un plano estratégico para la excelencia operativa.



SERIES OVERVIEW: 10-PART FRAMEWORK

Blueprint Sistémico-Editorial

@SCavanna


PORTAL UNIFICADO & PAM
(Acceso Privilegiado JIT/JEA)
Nota: Etiquetado completo de reuniones requiere Teams Premium además de E5
Ojo: Algunos escenarios DLP de navegador/red nativos son pay-as-you-go
1. PROTECCIÓN DE INFORMACIÓN Y GOBIERNO DE DATOS
Etiquetas de confidencialidad (Manual/Auto)
Cifrado integrado (AIP/RMS)
Etiquetado de contenedores (Teams/Sites)
[AVANZADO E5] Auto-etiquetado (ML, Entidades Nombradas)
Gestión de Registros Avanzada (Flujos de disposición, Inmutabilidad)
2. DATA LOSS PREVENTION (DLP) AVANZADO
Prevención de exfiltración (Cargas de trabajo M365)
Políticas conscientes del contexto
[AVANZADO E5] Endpoint DLP (Win 10/11, macOS)
Exact Data Match (EDM) precisión alta
Cobertura Cloud Apps (Defender for Cloud Apps inline)
GESTIÓN DE CUMPLIMIENTO
(Compliance Manager & Score, Information Barriers)
ECOSISTEMA DE DATOS M365 E5
(Objetivo de Protección)
3. RIESGO INTERNO Y COMUNICACIONES
Cumplimiento de Comunicaciones (Teams, Exchange, Viva)
Detección de lenguaje tóxico/riesgos
[AVANZADO E5] Gestión de Riesgo Interno (Sabotaje, Robo de datos)
Correlación de señales (Identidad, Dispositivos)
Evidencia Forense (Add-on opcional)
4. EDISCOVERY Y AUDITORÍA (PREMIUM)
Flujos legales extremo a extremo
Gestión de casos y retenciones
[AVANZADO E5] eDiscovery Premium (Análisis, Conjuntos de revisión)
Auditoría Premium (Señales forenses, Eventos alto valor)
Retención extendida (1 año default)
CIFRADO Y CONTROL DE CLIENTE
(Customer Key / Customer Lockbox)
Tip: Disponible Add-on de retención de auditoría de 10 años
RESUMEN EJECUTIVO: DESTACADOS E5
[Architects Daughter]
✓ Protección Avanzada (Etiquetado/Cifrado)
✓ Gestión de Ciclo de Vida/Registros Avanzada
✓ DLP (Endpoint y Nube)
✓ Gestión de Riesgo Interno
✓ Cumplimiento de Comunicaciones
✓ eDiscovery (Premium)
✓ Auditoría (Premium)
✓ Compliance Manager
✓ Information Barriers
✓ Customer Key/Lockbox
@SCavanna

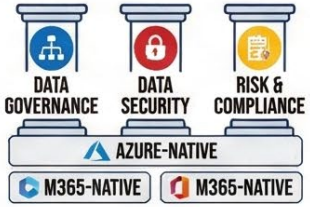
MICROSOFT PURVIEW EN M365 E5 / E5 COMPLIANCE: ÍNDICE DE LA SERIE INFOGRÁFICA [1/1]

01. EL PROBLEMA QUE PURVIEW VINO A RESOLVER

Los 4 fallos estructurales del mundo pre-Purview. La génesis como imperativo estratégico.

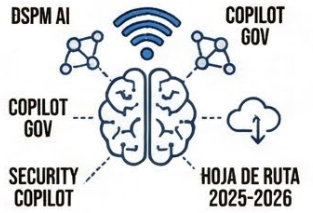
02. LA GRAN UNIFICACIÓN DE ABRIL 2022

Fusión en una marca única. Purview Data Map como corazón técnico compartido.



03. ARQUITECTURA DE LOS 3 PILARES FUNCIONALES

Estructura, componentes y distinción crítica nativa.



10. EL FUTURO: IA GENERATIVA, AGENTES AUTÓNOMOS Y DSPM

Gobernanza de IA, Security Copilot y el roadmap futuro.

Protección que viaja con el archivo

04. INFORMATION PROTECTION: DEL DATO AL CIFRADO PERSISTENTE

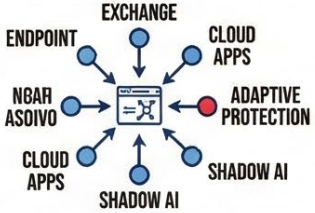
Motor de clasificación y etiquetado. Cifrado persistente.

09. PURVIEW COMO PILAR DE DATOS EN ZERO TRUST

3 principios ZT implementados. Flujo de decisión integrado.

MICROSOFT PURVIEW CORE HUB

ANCLA DEL SISTEMA: Plataforma Unificada de Datos y Cumplimiento



05. DLP AVANZADO: EL BRAZO EJECUTOR DE LAS POLÍTICAS

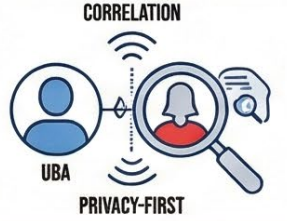
7 superficies de control. Adaptive Protection y Shadow AI como caso límite.

08. E3 VS. E5: LA REGLA DE ORO DEL LICENCIAMIENTO

Comparativa estructurada: control manual vs. inteligencia automatizada.

07. EDISCOVERY PREMIUM + AUDIT PREMIUM: LA MEMORIA FORENSE

El flujo legal forense y logs críticos. Distinción E3 vs. E5.



06. INSIDER RISK + COMMUNICATION COMPLIANCE: LA AMENAZA DESDE ADENTRO

Análisis de comportamiento, correlación de señales y supervisión privacy-first.

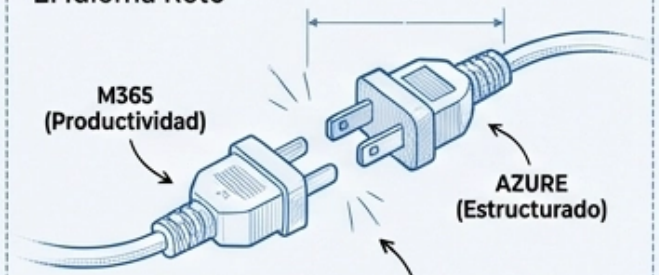
EL PROBLEMA QUE PURVIEW VINO A RESOLVER

Del Caos Informacional al Imperativo Estratégico

Bloque 01/10 / Antes de Purview: El Colapso Silencioso de la Gobernanza de Datos / Cómo los silos, la visibilidad limitada y la fragmentación convirtieron el cumplimiento normativo en una apuesta de alto riesgo

1. SILOS DE POLÍTICAS

El Idioma Roto

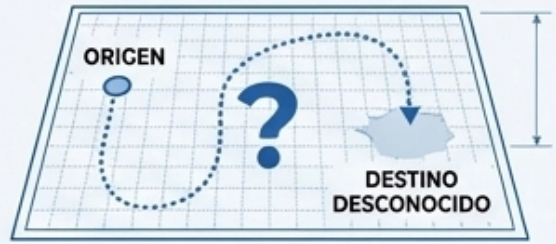


[PROBLEMA CRÍTICO] Dos universos desconectados. Sefiales de sensibilidad no transferibles automáticamente.

Mismo dato, dos idiomas de seguridad, comunicación limitada.

2. VISIBILIDAD LIMITADA

El Dato Sin Pasaporte



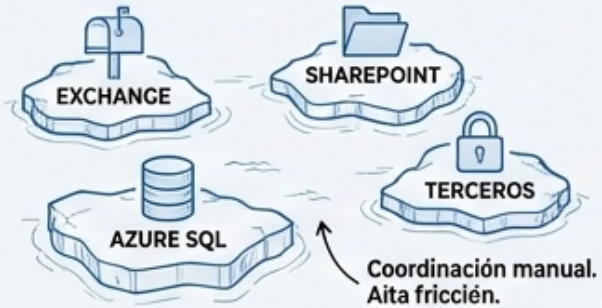
[IMRACTO DIRECTO] Rastro imposible de extremo a extremo. Impacto sn seguridad, cumplimiento y operaciones.

Sabíamos de dónde venia. Nunca supimos adónde fue.

3. FRAGMENTACIÓN DE GOBERNANZA

El Archipiélago de Consolas

[BARRERA OPERATIVA] Múltiples consolas incompatibles con lógicas y roles aislados.

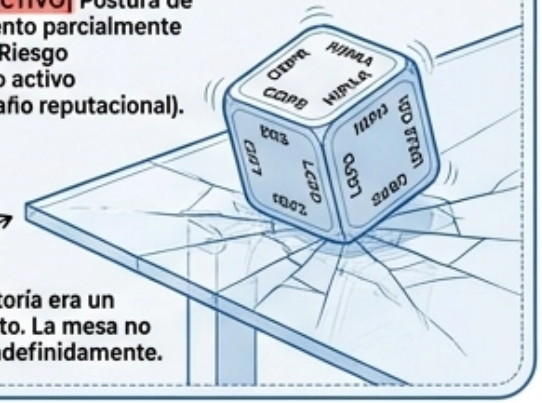


Coordinación manual. Aita fricción. Riesgo de brecha.

4. RIESGO DE INCUMPLIMIENTO NORMATIVO

La Auditoría como Ruleta Rusa

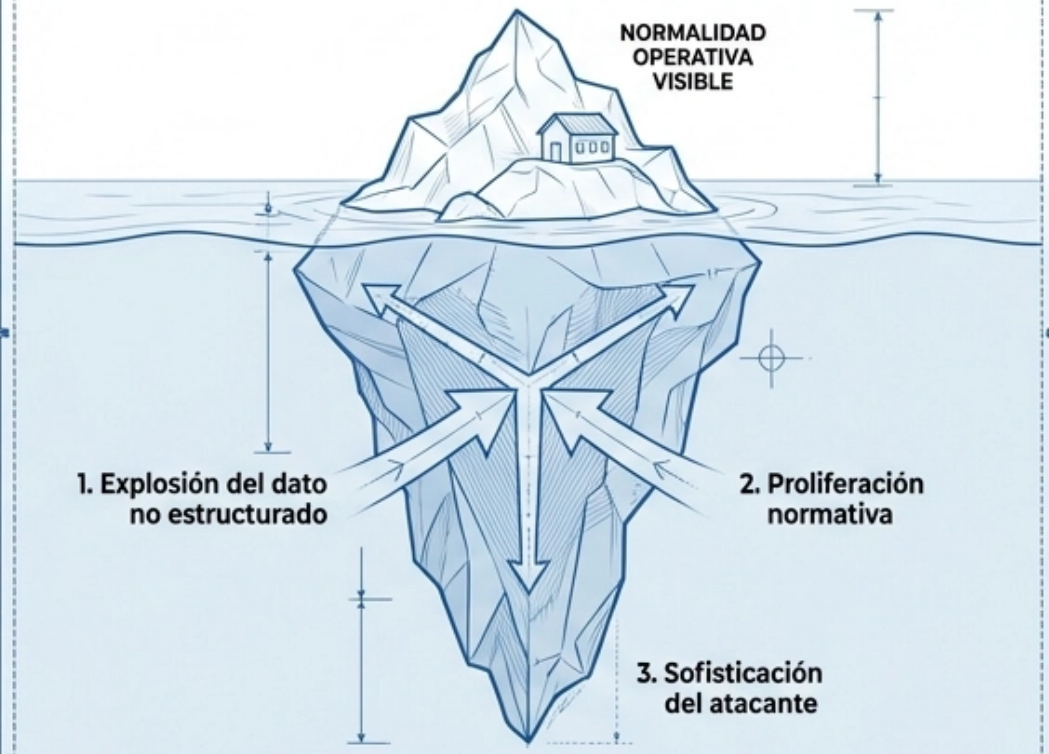
[RIESGO ACTIVO] Postura de cumplimiento parcialmente conocida. Riesgo regulatorio activo (multas, daño reputacional).



Cada auditoría era un lanzamiento. La mesa no aguanta indefinidamente.

CORE INSIGHT: EL COLAPSO SILENCIOSO

La gestión de los activos digitales dejó de ser una función técnica para convertirse en un imperativo estratégico de resiliencia organizacional — y la mayoría de las organizaciones llegó tarde a ese cambio.



⚠ **Lo que no se ve, también se audita.**

En abril de 2022, Microsoft decidió que estos cuatro problemas no podían seguir siendo gestionados por separado. → [Bloque 02]

@SCavanna

ABRIL 2022: EL MOMENTO EN QUE MICROSOFT CONSOLIDÓ LA GOBERNANZA DE DATOS

Del Dos Mundos Divergentes a un Sistema Nervioso Central / Microsoft Purview en M365 E5 / E5 Compliance.

Bloque 02/10

ANTES DE ABRIL 2022
(Silos Funcionales)

DESPUÉS DE ABRIL 2022
(Sistema Nervioso Central)

CONSOLIDACIÓN ESTRATÉGICA

MUNDO 1: DATOS ESTRUCTURADOS (Azure-Native)

Ingeniería / Arquitectura (Pay-as-you-go)

- Azure Purview (anterior)
- Escaneo Multicloud/On-prem
- Linaje Automático
- Catálogo Unificado
- Data Estate Insights

Antes: Sofisticado pero sordo al contexto de usuario. Silo técnico.

Architects Daughter

Metadatos Técnicos y Linaje

PURVIEW DATA MAP

El Corazón Técnico Compartido

Clasificación y Sensibilidad

MUNDO 2: DATOS NO ESTRUCTURADOS (M365-Native)

Seguridad / Compliance (Licencia por Usuario)

- M365 Compliance (anterior)
- Etiquetas de Sensibilidad
- Políticas DLP
- eDiscovery y Auditoría
- Insider Risk

Architects Daughter

Antes: Rico en contexto de usuario pero ciego a la infraestructura. Silo de productividad.

LA NUEVA ARQUITECTURA DEL CONTROL: TRES PILARES FUNCIONALES

DATA GOVERNANCE
¿Qué datos tenemos? Visibilidad y Descubrimiento.

DATA SECURITY
¿Cómo los protegemos? Protección Activa.

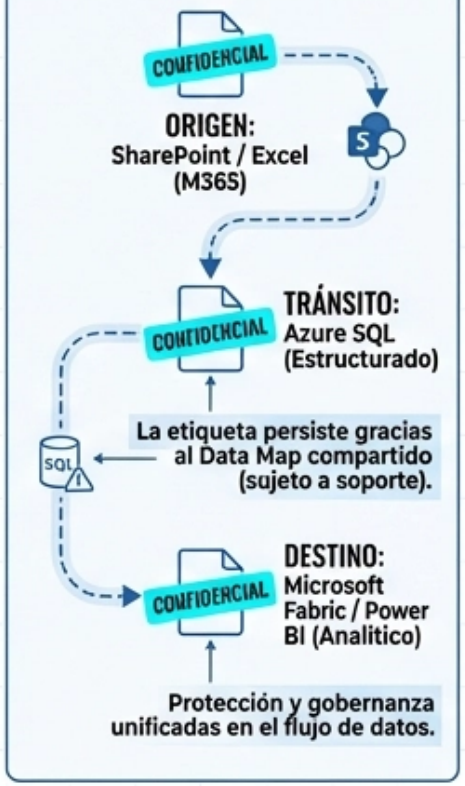
RISK & COMPLIANCE
¿Cumplimos? Auditoría y Normativa.

BASE COMÚN: PURVIEW DATA MAP

INSIGHTS DE PROFUNDIDAD:

1. El nombre "Purview" denota alcance y autoridad de visibilidad.
2. La convergencia con Microsoft Fabric (2022) extiende la gobernanza a la analítica y la IA.
3. Modelo de Licenciamiento Dual: Azure-native (consumo) vs. M365-native (usuario), unificados en el portal.

EL CASO DE USO QUE LO CAMBIA TODO: LA ETIQUETA QUE VIAJA

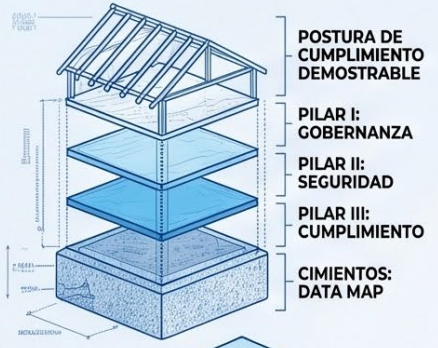


Nota Técnica: La persistencia de etiquetas y metadatos entre entornos depends de la compatibilidad de conectores, configuraciones específicas y el soporte de la plataforma de destino. No es universal ni automática en todos los escenarios.

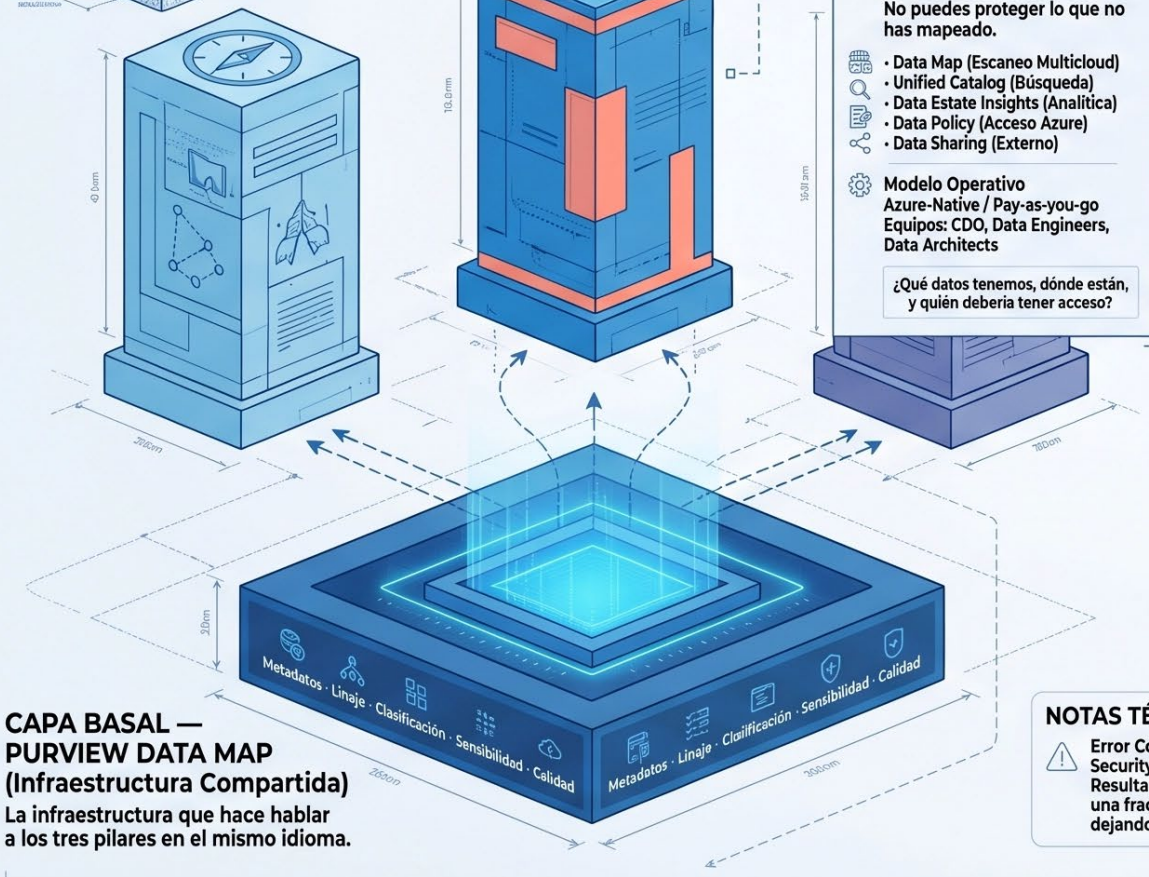
LA ARQUITECTURA PURVIEW: TRES PILARES, UN PATRIMONIO DE DATOS

Data Governance, Data Security y Risk & Compliance — cómo se distribuyen las responsabilidades, los componentes y los modelos de consumo sobre un corazón técnico compartido

Bloque 03/10 / Microsoft Purview en M365 E5 / E5 Compliance.



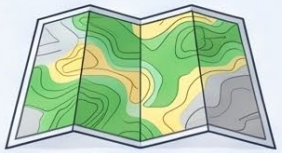
No se construye el techo antes que los cimientos. Purview es un sistema de capas interdependientes.



CAPA BASAL — PURVIEW DATA MAP (Infraestructura Compartida)

La infraestructura que hace hablar a los tres pilares en el mismo idioma.

PILAR I: DATA GOVERNANCE ("El Sistema de Descubrimiento")



No puedes proteger lo que no has mapeado.

- Data Map (Escaneo Multicloud)
- Unified Catalog (Búsqueda)
- Data Estate Insights (Analítica)
- Data Policy (Acceso Azure)
- Data Sharing (Externo)

Modelo Operativo
Azure-Native / Pay-as-you-go
Equipos: CDO, Data Engineers, Data Architects

¿Qué datos tenemos, dónde están, y quién deberia tener acceso?

PILAR II: DATA SECURITY ("El Sistema de Protección Activa")

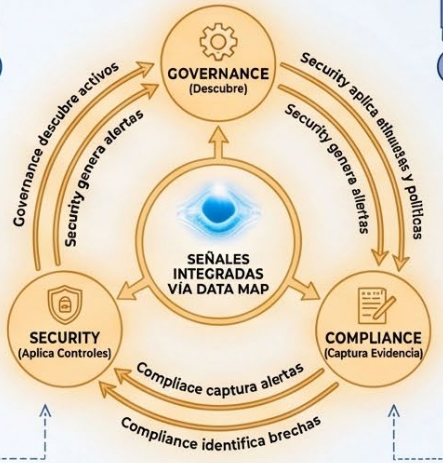
Cada capa detiene una categoría diferente de riesgo.

- Information Protection (Etiquetas)
- DLP (Control de Flujo)
- Insider Risk Management (UBA)
- Communication Compliance (Supervisión)
- Adaptive Protection (Dinámico)

Modelo Operativo
M365-Native / Por Usuario (E3/E5)
Equipos: CISO, Security Teams, DLP Analysts

¿Cómo aseguramos que los datos sensibles sean accedidos solo por autorizados?

FLUJO DE VALOR ENTRE PILARES (Ciclo Virtuoso)



Cada pilar produce señales que los otros consumen. El sistema aprende mientras opera.

PILAR III: RISK & COMPLIANCE ("El Sistema de Demostración")

El cumplimiento sin evidencia es solo una declaración de intenciones.

- Compliance Manager (Postura)
- eDiscovery Premium (Legal)
- Audit Premium (Forense)
- Records Management (Ciclo de Vida)
- Information Barriers (Muros)

Modelo Operativo
M365-Native / Por Usuario (E3/E5)
Equipos: CCO, Legal Counsel, Internal Auditors

¿Podemos demostrar ante un regulador que cumplimos con evidencia?

LA DISTINCIÓN OPERATIVA CRÍTICA: AZURE-NATIVE VS. M365-NATIVE

	AZURE-NATIVE (Pilar I & Infraestructura)	M365-NATIVE (Pilar II & III)
Componentes Principales	Data Map, Catalog, Insights	Info Protection, DLP, eDiscovery
Modelo de Costo	Pay-as-you-go (consumo)	Suscripción Mensual por Usuario (E3/E5)
Equipo Operador	Data Engineering / Cloud Architecture	Security & Compliance Teams
Dominio de Datos	Estructurado/Semiestructurado (SQL, Storage)	No Estructurado (M365: Teams, SharePoint)
Portal de Administración	Azure Portal + purview.microsoft.com	purview.microsoft.com (Principal)
Portal de Administración		Mismo portal. Dos modelos de operación. Una visión unificada del patrimonio.

NOTAS TÉCNICAS Y ESTRATÉGICAS (Insights de Profundidad)

Error Común: Implementar Data Security sin Data Governance previo. Resultado: Políticas aplicadas sobre una fracción visible del patrimonio, dejando el resto sin cobertura.

Cultura Organizacional: El portal unificado fuerza la conversación entre equipos (Seguridad, Cumplimiento, Datos) que históricamente operaban en silos.

Modelo de Madurez: Nivel 1 (Fundamentos activados), Nivel 2 (Intercambio de señales), Nivel 3 (Optimización adaptativa con Adaptive Protection).

Argumento Financiero: El costo total de operación integrada de los tres pilares es inferior a la suma de múltiples soluciones puntuales de terceros con costos de integración.

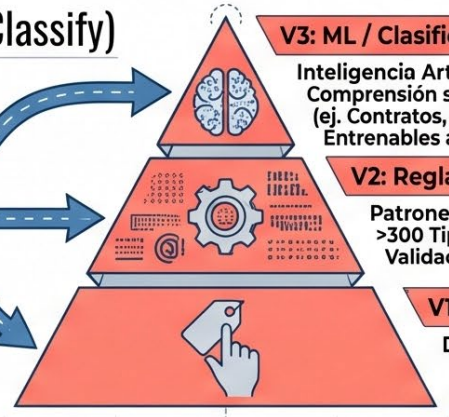
INFORMATION PROTECTION: LA PROTECCIÓN QUE VIAJA CON EL DATO

Bloque 04/10 / Cómo las etiquetas de sensibilidad, los clasificadores inteligentes y el cifrado persistente transforman documentos ordinarios en activos gobernados — independientemente de dónde vayan (en entornos compatibles con el ecosistema Microsoft y mientras existan claves válidas) learn.microsoft.com/microsoft-365/compliance/sensitivity-labels

1. DESCUBRIR (Discover)

Identificación de datos en reposo y en tránsito.

2. CLASIFICAR (Classify)



V3: ML / Clasificadores Entrenables (E5 only)

Inteligencia Artificial
Comprensión semántica y estructural (ej. Contratos, Nóminas).
Entrenables a medida.

V2: Reglas / SITs (E3/E5)

Patrones Explícitos
>300 Tipos de Info Sensible (ej. DNI, CUIT, Tarjetas).
Validación contextual.

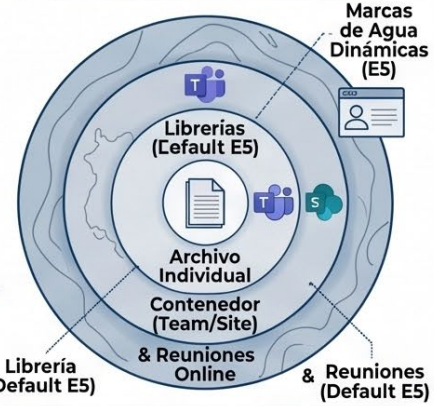
V1: Manual (E3/E5)

Del Instinto Humano
Criterio consciente, alto volumen, riesgo de fatiga.

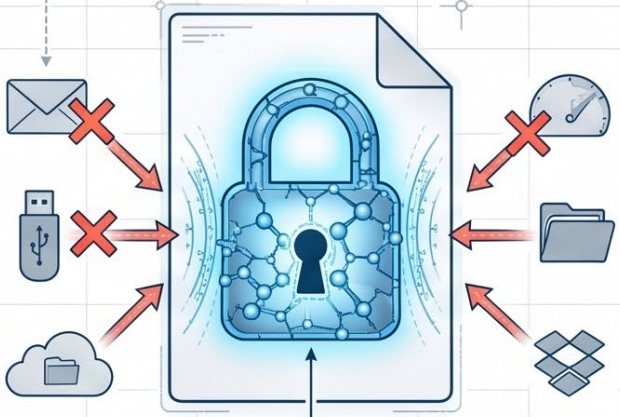
Architects Daughter

Tres vectores. Una cobertura progresivamente más inteligente.

3. ETIQUETAR (Label)



El Alcance del Etiquetado:
La Geometría de la Cobertura.
No es solo una acción, es una arquitectura de múltiples capas.

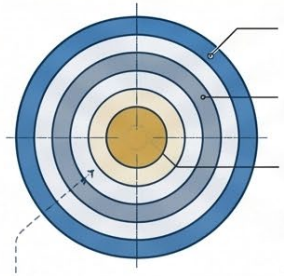


EL CORE: UN CONTRATO TÉCNICO VINCULANTE.
Una etiqueta de sensibilidad no es una nota adhesiva. Es un contrato técnico que define quién puede ver, qué puede hacer y qué ocurre si intenta llevárselo — y viaja con el archivo mientras las claves y políticas estén vigentes y en aplicaciones compatibles. La protección no depende del servidor ni de la red. Acompaña al dato.

5. GOBERNAR (Govern)

Cumplimiento, Auditoría y Control de Ciclo de Vida.

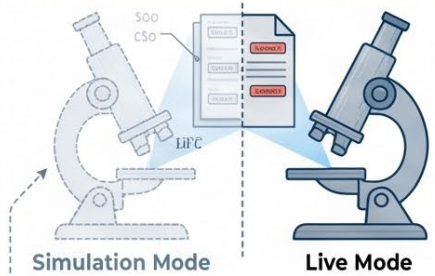
PRECISIÓN QUIRÚRGICA: EDM y Named Entities



- **SITs Genéricos** (Alta cobertura)
- **Named Entities** (Contexto semántico)
- **Exact Data Match (EDM)** Datos exactos de la organización (hash). Reduce drásticamente falsos positivos.

Cuanto más cerca del centro, más precisa la detección y menos fricción operativa.

IMPLEMENTAR SIN DISRUMPIR: Auto-Labeling y Simulation Mode

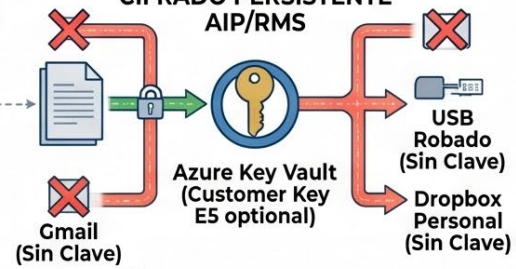


Architects Daughter

La simulación es la diferencia entre implementar y disrumpir. Calibra el threshold de confianza.

4. PROTEGER (Protect)

CIFRADO PERSISTENTE AIP/RMS



La Última Línea de Defensa.
AES-256 + RMS.
El cifrado viaja con el dato, condicionado por apps y claves válidas.

Nota 1: La taxonomía estratégica ideal comienza con 4-6 etiquetas claras, no complejas.
Nota 2: El cliente de Purview Information Protection extiende el etiquetado a PDFs y archivos no-Office.
Nota 3: Soporte nativo en Office Mobile (iOS/Android) y Web Apps para trabajo hibrido.
Nota 4 (E3 vs E5): E5 no es incremental, es transformacional. Protege todo el contenido sensible (ML, Default) vs. solo lo que el usuario recuerda (Manual).

CONEXIONES CLAVE: → Bloque 05 (DLP insumo primario), → Bloque 06 (Señal IRM), → Bloque 07 (Filtro eDiscovery), → Bloque 08 (Customer Key E5), → Bloque 09 (Factor Zero Trust), → Bloque 10 (Señal DSPM IA).

@SCavanna
in Century Gothic

DLP AVANZADO: EL BRAZO EJECUTOR DE LAS POLÍTICAS

Siete Superficies de Control, Una Arquitectura de Contención / **Bloque 05/10** / Cómo el Data Loss Prevention moderno trasciende el correo electrónico para convertirse en un sistema de contención multicapa que cubre endpoints, aplicaciones cloud y comportamiento de usuarios en tiempo real

purview.microsoft.com

MOTOR DE POLÍTICAS CENTRALIZADO:
Una Regla para Gobernarlas a Todas

CONDICIONES (Activadores)
- Etiquetas de Sensibilidad (Bloque 04)
- Tipos de Info Sensible (SITs)
- Destinatarios Externos
- Contexto de Acción

ACCIONES (Respuesta)
- Bloquear
- Bloquear con Override
- Cifrar
- Notificar Usuario
- Generar Alerta de Seguridad

NOTIFICACIONES (Auditoría)
- Registro de Auditoría Unificado (UAL)
- Notificaciones al Usuario (Tips)
- Integración con eDiscovery

Nota: Las etiquetas de Information Protection (Bloque 04) son el insumo primario para activar estas políticas.

Nota: Las etiquetas de Information Protection Protecion (Bloque 04) son el insumo primario para activar estas políticas.

SIETE SUPERFICIES DE CONTROL, UNA ARQUITECTURA DE CONTENCIÓN.
No importa por dónde intente salir. Hay una capa esperando.

7. CLOUD APPS
(Defender for Cloud Apps, E5)
Aplicaciones SaaS de terceros, App Discovery y Control Inline.
Visibilidad y control en tiempo real sobre sesiones.

6. NETWORK DLP
(E5 / Add-on)
Protección a nivel de red. Control de tráfico sin agente en endpoint.
Inspección inline de tráfico.

5. BROWSER DLP
(Edge for Business, E5)
Navegador corporativo. Upload, paste en web, descarga a apps no autorizadas.
Interceptar operaciones en sitios no gestionados.

4. ENDPOINT DLP
(E5 Exclusivo)
Dispositivos Windows/macOS. USB, Impresión, Captura de Pantalla, Bluetooth.
Auditar, notificar, bloquear con override, bloquear absoluto.

3. MICROSOFT TEAMS
(E5 Exclusivo)
Chats internos y externos. Análisis en tiempo real de mensajes y archivos.
Bloquear mensaje antes del envío, notificar.

2. SHAREPOINT Y ONEDRIVE (E3 + E5)
Archivos en reposo y compartidos. Escaneo de contenido y enlaces.
Bloquear uso compartido externo, notificar propietario.

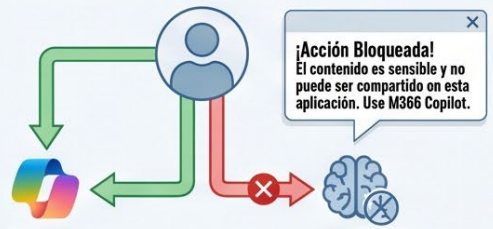
1. EXCHANGE ONLINE (E3 + E5)
Correos salientes. Análisis de contenido y adjuntos en tiempo real.
Bloquear, notificar, cifrar.

ADAPTIVE PROTECTION: EL DLP QUE APRENDE DEL COMPORTAMIENTO

AJUSTE DINÁMICO DE POLÍTICAS DLP
El nivel de riesgo del usuario (IRM) ajusta automáticamente los privilegios y umbrales de DLP en tiempo real.

Nota: Adaptive Protection es el punto de convergencia técnica entre DLP e Insider Risk (Bloque 06).

SHADOW AI COMO CASO LÍMITE: EL NUEVO PERÍMETRO DE EXFILTRACIÓN



M365 COPILOT (IA Gobernada)
Datos bajo control de Purview. Uso seguro y conforme.

IA EXTERNA (Shadow AI)
ChatGPT, Claude, Gemini, etc. Browser DLP intercepta 'Paste' de contenido sensible.

Nota: DLP no bloquea la IA. Canaliza su uso hacia las herramientas que respetan tus políticas (Bloque 10).

Nota 1: La implementación de DLP tiene un riesgo: la fricción excesiva. Iniciar en modo auditoría y ajustar umbrales iterativamente.

Nota 2: DLP es una herramienta de educación. Los mensajes de notificación son oportunidades de microformación.

Nota 3: Las alertas y eventos DLP son evidencia clave en investigaciones de eDiscovery (Bloque 07).

Nota 4: Relevancia sectorial LATAM: DLP permite reglas específicas por sector sobre arquitectura oficial.

CONEXIONES CLAVE:
→ Bloque 06 (DLP + IRM)
→ Bloque 07 (Evidencia eDiscovery)
→ Bloque 10 (Shadow AI y Copilot)
→ Bloque 06 (DLP + IRM)
→ Bloque 07 (Evidencia eDiscovery)
→ Bloque 09 (Endpoint DLP y Zero Trust)
← Bloque 10 (Shadow AI y Copilot)
← Bloque 04 (Insumo Etiquetas)
← Bloque 03 (Arquitectura Pilar II)
→ Bloque 08 (Licenciamiento E3 vs E5)

INSIDER RISK + COMMUNICATION COMPLIANCE: LA AMENAZA DESDE ADENTRO

Cuando el Mayor Riesgo de Seguridad Tiene Credenciales Válidas / Bloque 06/10

Cómo el análisis de comportamiento de usuarios, la correlación de señales multicanal y la supervisión inteligente de comunicaciones detectan amenazas internas que los controles perimetrales son estructuralmente incapaces de ver. Microsoft Purview en M365 E5 / E5 Compliance.

ESCENARIOS DE RIESGO

EXFILTRACIÓN DE DATOS
Descarga masiva + Copia a USB/Nube Personal.
Foco: Robo de IP antes de salida.
ALTA / CRÍTICA

SABOTAJE DE DATOS
Eliminación/Modificación maliciosa de activos.
Foco: Daño deliberado por conflicto.
ALTA / CRÍTICA

RIESGO DE OFFBOARDING
Actividad inusual tras renuncia.
Foco: Fuga de información durante la transición.
ALTA / CRÍTICA

FILTRACIÓN ACCIDENTAL
Compartir por error, mala configuración de permisos.
Foco: Error humano no malicioso.
MEDIA / BAJA

EL CORE: LA VISIÓN ASIMÉTRICA

Un atacante externo tiene que vulnerar tu perímetro. Un insider malicioso ya está adentro — con credenciales válidas, acceso legítimo y conocimiento de dónde están los datos más valiosos.

La única defensa efectiva no es controlar el acceso: es entender el comportamiento.

Las credenciales abren la puerta. El comportamiento revela la intención.

SHAREPOINT / ONEDRIVE (Archivos)
Descargas masivas, accesos inusuales a sitios sensibles, etiquetas de confidencialidad.

MICROSOFT TEAMS (Colaboración)
Mensajes con palabras clave, compartición externa de archivos, canales privados.

INTUNE / DEFENDER (Dispositivos & Endpoint)
Uso de USB no autorizado, impresión de documentos sensibles, instalaciones de software, alertas de endpoint.

USUARIO BAJO ANÁLISIS (Pseudonimizado)

SCORE DE RIESGO (Correlación Multicanal)
ELEVADO (Naranja)
BAJO (Verde) — CRÍTICO (Rojo)

EXCHANGE ONLINE (Correo)
Envíos externos de volumen, adjuntos sospechosos, patrones de comunicación anómalos.

ENTRA ID (Identidad & Acceso)
Intentos fallidos, accesos fuera de horario/ubicación, cambios de perfil de riesgo.

RRHH (Eventos & Contexto)
Renuncia presentada, advertencias disciplinarias, cambios de rol, fechas críticas.

ESCENARIOS DE RIESGO

COMMUNICATION COMPLIANCE: SUPERVISIÓN INTELIGENTE

TEAMS · EXCHANGE · BLOOMBERG · REUTERS · VIVA ENGAGE

CLASIFICADOR NLP & ML (Filtro Inteligente)

- **COMUNICACIÓN NORMAL** (Archivado)
- **ALERTA POTENCIAL** (Riesgo Detectado) → **COLA DE REVISIÓN SUPERVISADA** (Decisión Humana)

La máquina filtra. El humano decide. El proceso queda auditado. Detecta acoso, discriminación, conflictos de interés, y riesgos regulatorios.

DISEÑO PRIVACY-FIRST

PRIVACIDAD
Pseudonimización
Segregación de Roles
Trazabilidad

SEGURIDAD
Correlación de Señales
Alertas
Evidencia

IRM no monitoriza personas. Detecta patrones. La identidad solo se revela cuando el patrón justifica una investigación formal. Equilibrio entre protección y derechos.

CICLO DE INVESTIGACIÓN Y EVIDENCIA

DETECCIÓN & TRIAGE (Anónimo)
Alertas pseudonimizadas basadas en patrones. Evaluación inicial de riesgo.

INVESTIGACIÓN FORMAL (Desanonimización)
Aprobación de roles segregados para revelar identidad. Recopilación de logs y contexto.

EXPORTACIÓN A eDISCOVERY PREMIUM (Evidencia Legal)
Transferencia de evidencia estructurada para revisión legal y cumplimiento.

RESOLUCIÓN DOCUMENTADA (Acción)
Cierre del caso con acciones correctivas, legales o de RRHH, auditado en el sistema.

CONEXIONES CLAVE

← Bloque 05 (Adaptive Protection): IRM provee el score de riesgo dinámico.
→ Bloque 07 (eDiscovery): Escalado de investigaciones y evidencia.
→ Bloque 09 (Zero Trust): IRM como evaluación de comportamiento "assume breach".
→ Bloque 10 (DSPM IA): Extensión de la lógica a agentes de IA.

← Bloque 03 (Data Security): IRM como pilar de análisis de comportamiento.
← Bloque 04 (Information Protection): Etiquetas de sensibilidad como señal clave.
→ Bloque 08 (Audit Premium): Registro de todas las actividades de IRM y CC.

eDiscovery Premium + Audit Premium: La Memoria Forense

Cuando la Organización Necesita Recordar Todo con Precisión Quirúrgica **/ Bloque 07/10**

Cómo el flujo legal end-to-end de eDiscovery Premium y los logs de alto valor de Audit Premium convierten los registros digitales de la organización en evidencia verificable, admisible y preservada con cadena de custodia documentada # Microsoft Purview en M365 E5 / E5 Compliance.

FLUJO LEGAL END-TO-END: LAS SEIS ESTACIONES DE LA CADENA DE CUSTODIA (eDISCOVERY PREMIUM)

1. IDENTIFICAR (Custodios y Fuentes)

Custodios gestionados con estado, historial y fuentes de datos vinculadas (Exchange, OneDrive, SharePoint, Teams).

Basado en actividad histórica de Audit.

2. PRESERVAR (Legal Hold)

Hold Custodial (específico) y Non-Custodial (organizacional).
Preservación indefinida inmune a políticas de retención.

Notificaciones de hold documentadas con acuse de recibo.

3. RECOLECTAR (Collections Inteligentes)

Consultas sofisticadas (palabras clave, fechas, metadatos).
Estimación previa a la colección para reducir volumen.

Solo recolecta lo relevante, ahorrando almacenamiento y tiempo.

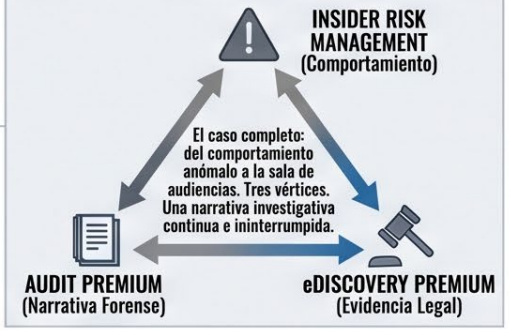
DISTINCIÓN CRÍTICA: HOLD vs. RETENCIÓN

BIFURCACIÓN FORENSE: EL VALOR DE MailItemsAccessed

Asume lo peor.
Incertidumbre costosa.

Certeza forense.
Defensa basada en datos.

EL TRIÁNGULO DE EVIDENCIA INTEGRADA



6. EXPORTAR (Cadena de Custodia Documentada)

Exportación final con metadatos completos y registro ininterrumpido de cada acción desde la preservación.

Evidencia lista para ser presentada en tribunal con su historia intacta.

5. ANALIZAR (Inteligencia Artificial)

Threading de conversaciones, Near-deduplication, Análisis temático, Relevance scoring (Predictive Coding).

La IA transforma la lectura manual en priorización inteligente.

4. REVISAR (Review Sets Controlados)

Espacio de trabajo legal seguro en Azure (frontera de cumplimiento).
Etiquetado, notas y acceso externo controlado.

La evidencia permanece inmutable durante la revisión.

AUDIT PREMIUM: EL RÍO CONTINUO DE EVIDENCIA — INFRAESTRUCTURA FORENSE (E5)

RETENCIÓN EXTENDIDA

Lo que E3 olvida a los 90 días, E5 recuerda durante un año.

EVENTOS CRÍTICOS DE ALTO VALOR

MailItemsAccessed
El testigo que estaba en la escena.
Registro preciso de acceso a mensajes.

Send · SearchQueryInitiated · FileDownloaded

Eventos forenses que Audit Standard no captura.

API ALTO ANCHO DE BANDA

Respuesta a Incidentes Ágil
Consultas masivas para investigaciones en tiempo real.

E3 vs. E5: La Regla de Oro del Licenciamiento

La Decisión que Define el Nivel de Inteligencia, Automatización y Resiliencia de la Organización / **Bloque 08/10**

Cómo la decisión de licenciamiento no es una elección de precio sino una elección de capacidad operativa — y qué add-ons permiten una migración modular para organizaciones que no pueden o no quieren moverse a E5 de forma completa. # Microsoft Purview en M365 E5 / E5 Compliance.

MATRIZ DE COMPARATIVA DETALLADA — CAPACIDAD POR CAPACIDAD

ÁREA FUNCIONAL PURVIEW	M365 E3 (Control Manual/Básico)	M365 E5 (Automatización/Avanzado)
Information Protection (Etiquetado)	Manual por usuario (Office, Web, Móvil). Cifrado básico.	Auto-labeling con ML entrenable. Etiquetado por defecto en SharePoint. Marcas de agua dinámicas.
Data Loss Prevention (DLP)	Exchange, SharePoint, OneDrive. Políticas estáticas.	Teams, Endpoint (Win/Mac), Browser (Edge), Cloud Apps (MDCA). Adaptive Protection dinámico.
Auditoría (Logs)	Audit Standard (90 días). Eventos básicos.	Audit Premium (1 año por defecto). Eventos críticos (MailItemsAccessed), API de alto ancho de banda.
eDiscovery (Legal)	Standard. Búsqueda y exportación básicas.	Premium. Custodios, Análisis IA, Legal Hold, Review Sets, Cadena de Custodia Documentada.
Insider Risk Management	No incluido	Completo. Correlación multicanal, escenarios de riesgo, integración RRHH, Adaptive Protection.
Communication Compliance	No incluido	Teams, Exchange, Viva Engage. Clasificadores NLP, detección de acoso, riesgos regulatorios.
Records Management	Retención básica y eliminación automática.	Advanced Records Management. Regulatory Records, declaración auto por ML, Proof of Disposal.
Clasificadores Entrenables (ML)	Limitado a SITs predefinidos	Clasificadores de ML para auto-labeling, Comm. Compliance, Records, IRM.
Adaptive Protection (Riesgo Dinámico)	No disponible	Integración IRM y DLP para restricciones dinámicas basadas en nivel de riesgo del usuario.

E3 = CONTROL MANUAL
(Escala Humana, Gestión Reactiva)

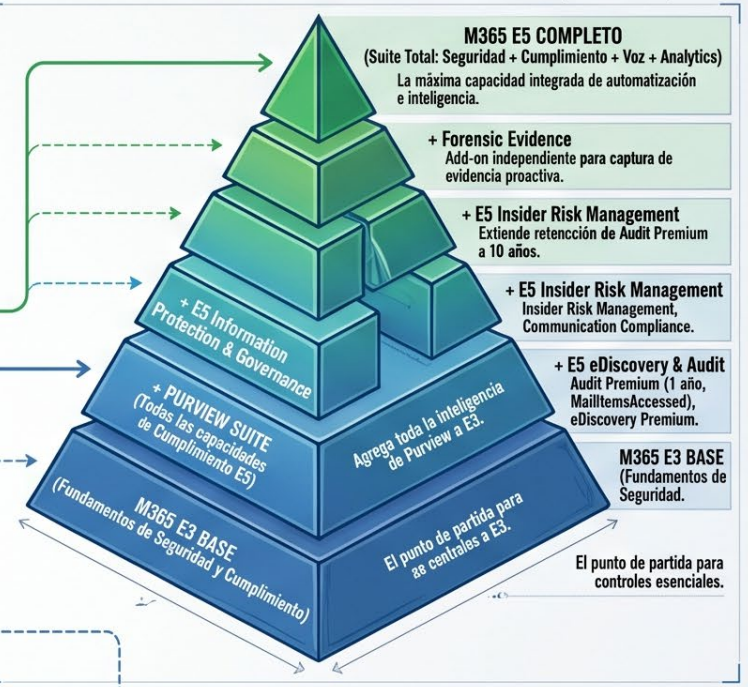
Requiere intervención y disciplina humana constante. Adecuado para entornos de menor complejidad y regulación moderada.

E5 = INTELIGENCIA AUTOMATIZADA
(Escala Máquina, Protección Proactiva)

Habilita automatización, aprendizaje automática

NO ES UNA ELECCIÓN DE PRECIO.
ES UNA ELECCIÓN DE ESCALA Y COMPLEJIDAD.

LOS ADD-ONS MODULARES — LA MIGRACIÓN INTELIGENTE (PIRÁMIDE)



EL ARGUMENTO FINANCIERO — ROI CONSULTIVO

Respuesta a Incidentes (Velocidad)
Reducción drástica de tiempo medio para detectar (MTTD) y responder (MTTR) con automatización E5. Menor impacto financiero de brechas.

Costos eDiscovery Externo (Legal)
eDiscovery Premium reduce volumen de datos enviados a revisión externa costosa mediante análisis in-place y filtrado inteligente.

Multas Regulatorias (Riesgo)
Prevención proactiva y demostración de diligencia debida con controles avanzados (DLP, IRM, Records) mitiga riesgo de sanciones mayores.

Shadow IT / Shadow AI (Visibilidad)
Descubrimiento y control de aplicaciones no sancionadas y uso de IA generativa con MDCA y DLP integrado en E5.

*Las estimaciones de ROI son consultivas y dependen del contexto específico de la organización. Microsoft no publica calculadoras oficiales.

LA REGLA DE ORO APLICADA — ÁRBOL DE DECISIÓN

¿Cuál es el perfil de tu organización?

- Baja Escala / Regulación Moderada / Foco en Costo Inicial? → **M365 E3 + Add-ons Específicos**
  Cubre necesidades puntuales sin costo total de E5.
- Alta Escala / Regulación Estricta / Foco en Automatización y Reducción de Riesgo? → **M365 E5 Completo**
  Inversión estratégica para eficiencia operativa y seguridad robusta.
- Organización Híbrida / Usuarios con Perfiles de Riesgo Diferenciados? → **Segmentación de Licencias (E5 para usuarios de alto riesgo/VIP, E3 para resto)**
  Optimiza la inversión asignando capacidades avanzadas donde más se necesitan.

SOBERANÍA DE DATOS — ARGUMENTO E5 (CUSTOMER KEY + LOCKBOX)

CUSTOMER KEY
(Tú controlas las llaves)
El cliente genera y almacena claves maestras en Azure Key Vault. Al revocar acceso, los datos se vuelven inaccesibles incluso para Microsoft.

CUSTOMER LOCKBOX
(Tú apruebas el acceso)
Acceso de soporte de Microsoft a contenido del cliente solo tras aprobación explícita y temporal del cliente, con registro auditado completo.

Argumentos críticos para sectores altamente regulados y con requisitos estrictos de soberanía de datos.

@SCavanna

PURVIEW COMO PILAR DE DATOS EN ZERO TRUST

Cuando la Confianza Deja de Ser un Estado Permanente y se Convierte en una Verificación Continua / Bloque 09/10

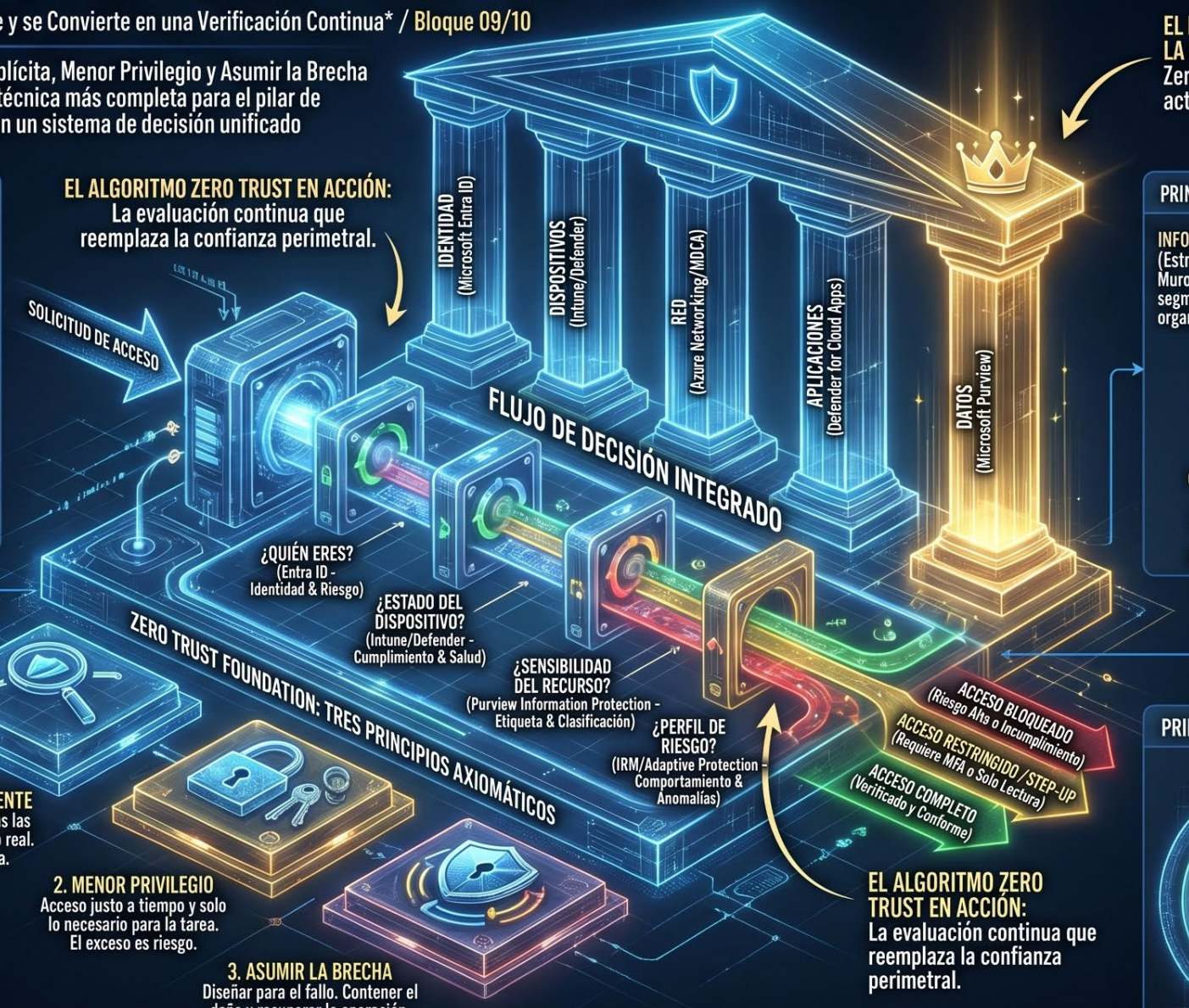
Cómo los tres principios de Zero Trust — Verificación Explícita, Menor Privilegio y Asumir la Brecha — encuentran en Microsoft Purview su implementación técnica más completa para el pilar de datos, integrando identidad, dispositivo y sensibilidad en un sistema de decisión unificado

EL PILAR QUE APORTA LA SEÑAL FALTANTE: LA SENSIBILIDAD DEL DATO. Sin Purview, el sistema Zero Trust tiene visión de túnel, verificando solo al actor y al contenedor, no al contenido.

PRINCIPIO 1: VERIFICACIÓN EXPLÍCITA – LA SEÑAL DE SENSIBILIDAD

La misma identidad y dispositivo generan decisiones diferentes según la etiqueta de sensibilidad del dato. El contexto es clave.

EL ALGORITMO ZERO TRUST EN ACCIÓN: La evaluación continua que reemplaza la confianza perimetral.



ZERO TRUST FOUNDATION: TRES PRINCIPIOS axiomáticos on aperaol. No hay confianza perotonátical.

1. VERIFICAR EXPLÍCITAMENTE
Toda decisión basada en todas las señales disponibles en tiempo real. No hay confianza heredada.

2. MENOR PRIVILEGIO
Acceso justo a tiempo y solo lo necesario para la tarea. El exceso es riesgo.

3. ASUMIR LA BRECHA
Diseñar para el fallo. Contener el daño y recuperar la operación.

EL ALGORITMO ZERO TRUST EN ACCIÓN: La evaluación continua que reemplaza la confianza perimetral.

PRINCIPIO 2: MENOR PRIVILEGIO – TRES DIMENSIONES TÉCNICAS

INFORMATION BARRIERS (Estructural) Muros éticos entre segmentos organizacionales.

CUSTOMER LOCKBOX (Proveedor) Acceso temporal de Microsoft requiere aprobación explícita.

CUSTOMER LOCKBOX (Proveedor) Acceso temporol de Microsoft requiere aprobación explícita.

PRIVILEGED ACCESS MANAGEMENT (Administrativo) Acceso Just-in-Time (JIT) y Just-Enough-Access (JEA) para tareas críticas.

PRINCIPIO 3: ASUMIR LA BRECHA – CONTENCIÓN EN CAPAS

Diseño resiliente: Cada capa está diseñada para detener el daño si la anterior falla.

NOTAS DEL ARQUITECTO:
Zero Trust es un viaje de madurez continua, no un destino.
El desafío común es el "oversharing" heredado en SharePoint; Purview Data Estate Insights es clave para la remediación.
Purview implementa directamente los tenets del NIST SP 800-207 para datos. Una implementación correcta de ZT aplica fricción proporcional al riesgo, no bloqueos indiscriminados.

ZERO TRUST CON PURVIEW: La arquitectura que transforma la seguridad de datos de una defensa perimetral estática a un sistema dinámico de verificación continua, asegurando que cada acceso sea explícitamente validado, mínimamente privilegiado y resilientemente contenido.
#MicrosoftPurview #M365E5 #ZeroTrustSecurity

@SCavanna

El Futuro: IA Generativa, Agentes Autónomos y DSPM

Cuando la Gobernanza de Datos Debe Extenderse a Actores que No Tienen Nombre de Usuario / Bloque 10/10**

Cómo Data Security Posture Management para IA, la gobernanza de agentes autónomos, la integración con Security Copilot y la convergencia con Microsoft Fabric redefinen el perímetro de la gobernanza de datos para un mundo donde los modelos de IA son actores de primera clase en el ecosistema de información organizacional # Microsoft Purview en M365 E5 / E5 Compliance.

EL NUEVO ACTOR DEL ECOSISTEMA DE DATOS: LA IA COMO USUARIO

Los mismos datos. Un nuevo tipo de actor. Las mismas políticas deben extenderse — o el perímetro tiene un agujero del tamaño de un modelo de lenguaje.
Purview redefine la gobernanza para un mundo donde la IA no duerme.

DSPM PARA IA: Ver lo que los Modelos Están Haciendo con tus Datos

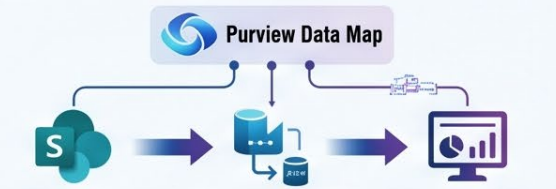
GOBERNANZA DE AGENTES AUTÓNOMOS: Políticas para Actores que No Duermen

Los agentes heredan las políticas. No las inventan.
Las respetan como cualquier otro actor.

SECURITY COPILOT + PURVIEW: La Investigación Forense en Lenguaje Natural

Tiempo Humano: Horas/Días **VS** **Tiempo Copilot:** Minutos (Reducción significativa de fricción técnica)

MICROSOFT FABRIC + PURVIEW: La Gobernanza que Sigue al Dato Analítico



La gobernanza no se detiene. Fabric + Purview aseguran que el dato lleve su historia de sensibilidad.

HOJA DE RUTA 2025-2026: EL MAPA DEL TERRITORIO EN TIEMPO REAL

Q1 2025	Q2 2025	Q3 2025	Q4 2025	Q1 2025	Q2 2026	Q3 2026	Q4 2026
	GA - Disponible: **DSPM Básico** (Visibilidad Copilot), **Security Copilot** (Integración Purview), **Fabric + Purview** (Linaje/Clasificación)		Preview: **Gobernanza de Agentes** (Herencia de políticas), **DSPM Avanzado** (Alertas Oversharing), **Prompt Scanning**		Roadmap: **Clasificación Multimodal** (Imagen/Audio/Video), **Gobernanza Completa de Agentes**, **Expansión Fabric**		**Meta-trend:** Gobernanza continua, automatizada y agnóstica del actor.

CIERRE DEL ARCO NARRATIVO: LA EVOLUCIÓN DEL SISTEMA NERVIOSO CENTRAL

Bloque 01: Silos, Visibilidad Limitada, Fragmentación, Riesgo Normativo. **Bloque 10:** Los mismos problemas reaparecen en el dominio de la IA. La misma plataforma, Purview, extendida para resolverlos de nuevo. El viaje de la gobernanza de datos no termina. Evoluciona.