Data Sec

E02

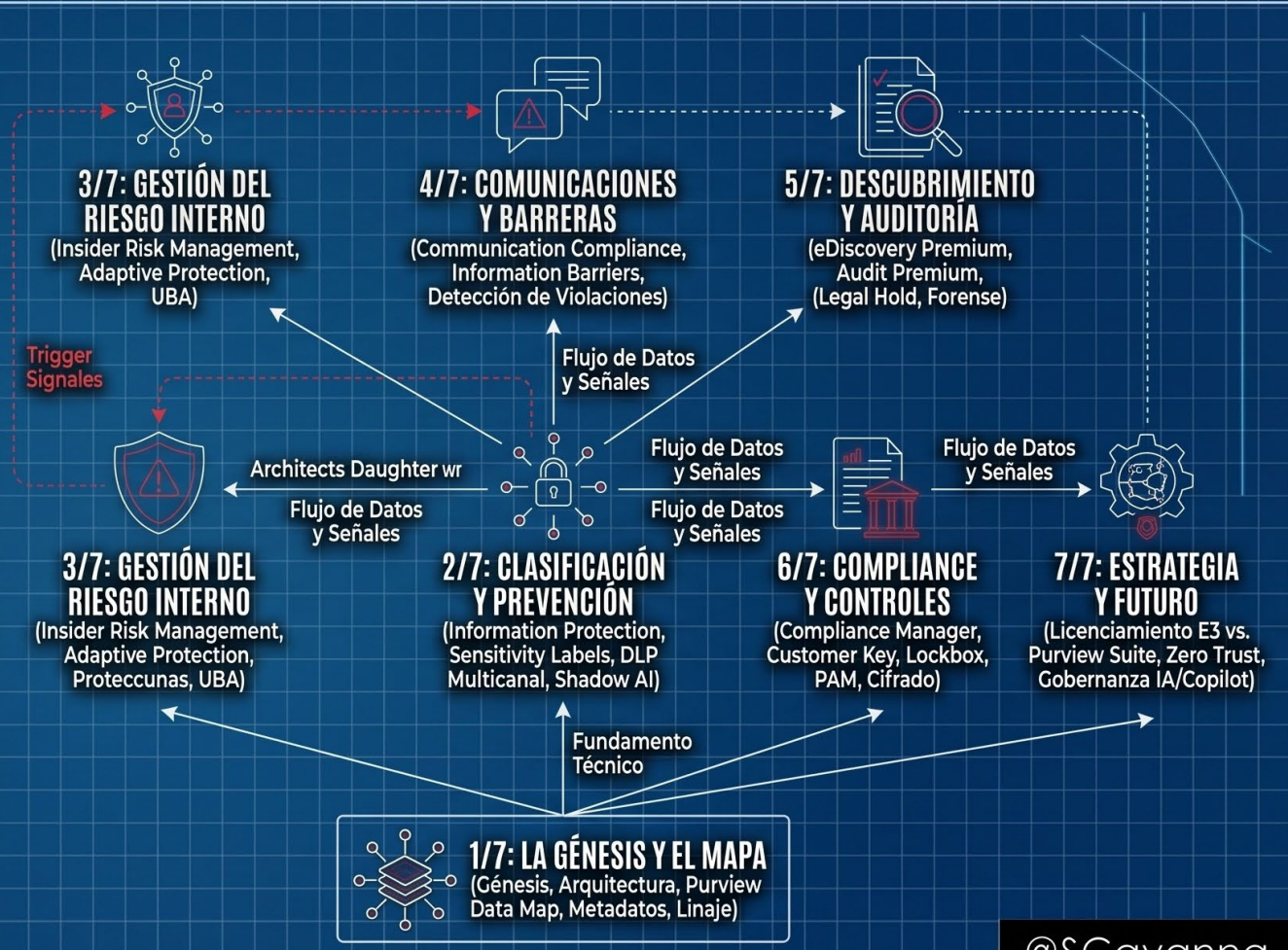
MS_Purview_M365E5-SecOps_e02v01

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: GOBERNANZA, PROTECCIÓN Y CUMPLIMIENTO

El Núcleo Invariable: Unificación de seguridad del dato, independiente del canal y auditablemente demostrable.

RESUMEN EJECUTIVO Y MAPA ARQUITECTÓNICO DE LA SERIE (1/11 - 11/11)

INFORMATION PROTECTION
(Clasificación y Etiquetado)
[Bloque 3/11]

Labels · Sensitivity · ML Classifiers

Prerrequisito Técnico: Sin etiqueta, no hay política de prevención ejecutable.

DATA LOSS PREVENTION
(Control de Todas las Superficies)
[Bloque 4/11]

Exchange · Endpoint · Cloud Apps · Browser · Network

GOBERNANZA PARA IA Y COPILOT
(Nuevo Perímetro del Dato 2025-2026)
[Bloque 11/11]

DSPM · Shadow AI DLP · Copilot Governance

Vector de riesgo emergente que requiere gobernanza Purview.

COMMUNICATION COMPLIANCE & INFORMATION BARRIERS
(Análisis de Comunicaciones Reguladas)
[Bloque 6/11]

Chat Analisis · Detección de Violación · Separación Tecnnica

INSIDER RISK MANAGEMENT & ADAPTIVE PROTECTION
(Señales de Riesgo y Respuesta Dinámica)
[Bloque 5/11]

UBA signals · Risk Scenarios

Genera Señales de Riesgo

ADAPTIVE PROTECTION

Restringe DLP dinámicamente basado en riesgo de usuario.

NÚCLEO TÉCNICO CENTRAL
(Corazón de la Gobernanza)

PURVIEW DATA MAP
(Infraestructura Común de Metadatos, Linaje y Clasificación)

Alimenta clasificación y gobernanza para toda la suite. El "cerebro" del sistema.

AUDIT PREMIUM
(Registro Histórico y Forense)

eDISCOVERY PREMIUM & AUDIT PREMIUM
(Cobertura Forense Completa)
[Bloque 7/11]

Legal Hold · Custodio de Evidencia · API High-bandwidth API

eDiscovery Premium depende de Audit Premium para cobertura completa.

Genera Acciones Mapeadas y Conecta con Controles Técnicos

LICENCIAMIENTO: E3 vs. PURVIEW SUITE
(Mapa de Valor y Alcance) [Bloque 9/11]

VS. Delta de Capacidades

Justifica inversión, acota alcance de controles. Regla de Oro.

COMPLIANCE MANAGER & CONTROLES DE ACCESO
(Evaluación Normativa y Cifrado) [Bloque 8/11]

NIST · ISO · GDPR assessments · Customer Key · Lockbox · PAM

Customer Key: Capa de control sobre datos de Information Protection.

PURVIEW EN UNA ARQUITECTURA ZERO TRUST
(Plano de Datos del Modelo) [Bloque 10/11]

Marco arquitectónico que legitima y contextualiza toda la suite como control de datos.

MAPA DE RUTA DE LA SERIE: ARQUITECTURA Y ESTRATEGIA EN 11 BLOQUES

1. Génesis y Arquitectura (Sistémico)
2. Purview Data Map (Técnico)
3. Information Protection (Secuencial)
4. Data Loss Prevention (Técnico)
5. Insider Risk & Adaptive Protection (Sistémico)
6. Communication Compliance (Analítico)
7. eDiscovery & Audit (Secuencial)
8. Compliance Manager & Controles (Editorial)
9. Licenciamiento E3 vs. Purview (Analítico)
10. Purview en Zero Trust (Sistémico)
11. Gobernanza para IA/Copilot (Secuencial)

@SCavanna

Génesis y Arquitectura Conceptual de Microsoft Purview

Del Silo a la Unificación: El Sistema Operativo Visual para la Gobernanza del Dato / Bloque 01/11

EL PROBLEMA ESTRUCTURAL PREVIO (ANTES DE ABRIL 2022)

AZURE PURVIEW
(Datos Estructurados/Infraestructura)

Gobierno de inventario y activos sin contexto de productividad.

Azure SQL · AWS S3 · GCP · On-Premises · Power BI

Gobierno de inventario y activos sin contexto de productividad.

M365 COMPLIANCE
(Datos No Estructurados/Colaboración)

Exchange · SharePoint · OneDrive · Teams

Protección de documentos sin contexto de infreestructura.

BRECHA DE GOBERNANZA
Silos de política, visibilidad incompleta y riesgo acumulado.

CONSOLIDACIÓN ESTRATÉGICA

LA UNIFICACIÓN (ABRIL 2022): UN NÚCLEO COMPARTIDO DE METADATOS

PORTAL UNIFICADO
(purview.microsoft.com)

MODELO DE METADATOS COMPARTIDO
(Sensibilidad Universal)

IDENTIDAD DE PLATAFORMA ÚNICA
(Comunicación con Reguladores)

No fue rebranding, fue una decisión arquitectónica: construir una capa de coherencia semántica.

DATA GOVERNANCE
(Azure-native)

Inventario, descubrimiento y política de acceso centralizada (Pay-as-you-go).

Data Map · Linaje · Calidad · Catálogo

DATA SECURITY
(M365-native)

Information Protection · DLP · Insider Risk · Communication Compliance

Clasificación, cifrado y protección (Licenciamiento por usuario).

RISK & COMPLIANCE
(M365-native)

eDiscovery · Audit · Records Management · Compliance Manager

Evaluaciones normativas y gestión de riesgos (Licenciamiento por usuario).

PURVIEW SUITE: EL NIVEL DE LICENCIAMIENTO MÁXIMO (DESDE OCT 2025)

M365 E3
(Control Manual)

Gestión básica.

PURVIEW SUITE
(Control Automatizado e Inteligente)

- Automatización ML
- Endpoint DLP
- Insider Risk
- eDiscovery Premium
- Audit Premium
- Information Barriers
- Customer Key
- Customer Lockbox
- PAM

Escala el control con inteligencia y automatización para grandes organizaciones.

PRINCIPIO DE DISEÑO: PERSISTENCIA DEL CONTROL

ETIQUETA DE SENSIBILIDAD
(Cifrado AIP/RMS)

La protección viaja con el dato, no con el contenedor. El acceso depende de la identidad y contexto, no de la ubicación.

El Purview Data Map: Corazón Técnico de la Gobernanza

Despiece del Sistema Nervioso Central del Dato / Bloque 02/11

5 DATA POLICY (GOBERNANZA DE ACCESO CENTRALIZADA)

POLÍTICA CENTRALIZADA EN PURVIEW

ROL DATA READER TIENE ACCESO A "DATOS OPERACIONALES" EN "COLECCIÓN FINANZAS"

PROPAGACIÓN AUTOMÁTICA DE CONTROL
(Servicios Subyacentes)

Azure SQL · Azure Storage · Azure Data Lake

Reduce el riesgo de configuraciones de permisos inconsistentes o residuales.

4 UNIFIED CATALOG (DESCUBRIMIENTO SEMÁNTICO)

BÚSQUEDA SEMÁNTICA

GLOSARIO DE TÉRMINOS DE NEGOCIO
(Ej. "tbl_cust_pii_ar" -> "Datos personales de clientes - Argentina")

ANOTACIONES DE EXPERTOS
(Calidad/Uso Apropiado)

COLECCIONES ORGANIZADAS
(Por Dominio/Unidad)

Democratiza el acceso: un DPO puede encontrar datos sin conocer la arquitectura técnica.

3 LINAJE DEL DATO (CONSTRUCCIÓN AUTOMÁTICA DE FLUJO)

Responde ¿qué datos fueron accedidos, cómo llegaron ahí y qué sistemas downstream están afectados?

ORIGEN
(Fuente Generadora)
(e.g. Data Factory)

Registro de operaciones y pipelines.

TRANSFORMACIÓN
(Procesamiento)
(e.g. Databricks Pipeline)

DESTINO
(Synapse Analytics Table)

DEPENDENCIA
(Activos Downstream)
(Power BI Report)

VISTA DE SENSIBILIDAD INFERIDA (INVENTARIO SEMÁNTICO)
El inventario técnico se enriquece con etiquetas de sensibilidad detectadas.

CLASIFICACIÓN AUTOMÁTICA (DURANTE EL ESCANEO)

Ej. Tarjeta de Crédito, SSN, DNI/CUIT, Pasaporte, Salud, Coordenadas, Credenciales.

200+ CLASIFICADORES DEL SISTEMA
(Tipos de Datos Sensibles)

MULTICLOUD SCANNING & CONECTORES HETEROGÉNEOS

Azure SQL Database · Azure SQL Managed Instance · Azure Data Lake Storage Gen1 · Azure Data Lake Storage Gen2 · Azure Blob Storage · Azure Synapse Analytics · Azure Cosmos DB · Azure Database for PostgreSQL/MySQL · Azure Files

AZURE-NATIVE
(On-premises & Cloud)

Escaneo completo e incremental de metadatos técnicos (nombre, ubicación, tipo, esquema, propietario, fecha mod).

Amazon S3 · Google Cloud Storage · SQL Server (On-prem) · SAP ECC/S4HANA · Oracle Database · Teradata · Power BI

MULTICLOUD & ON-PREMISES
(Self-hosted Integration Runtime)

MULTICLOUD SCANNING & CONECTORES HETEROGÉNEOS

@SCavanna

Information Protection: El Roadmap de la Clasificación y el Etiquetado

De la Detección a la Protección Cifrada: El Viaje del Dato Sensible / **Bloque 08/10**

1. 1. DETECCIÓN Y DESCUBRIMIENTO (Fundamentos)

SIT: Patrones Genéricos (300+)
- Tarjetas, DNI, Financiero

EDM: Datos Exactos (Organización)
- Coincidencia Hash sin acceso a datos

NAMED ENTITIES: Contexto Semántico (IA)
- Personas, Lugares, Términos Médicos

Motor de Análisis de Contenido

Motores de detección superpuestos para minimizar falsos positivos.

2. 2. DEFINICIÓN DE TAXONOMÍA (Estrategia)

Estructura jerárquica clara (4-6 niveles) para usuarios y sistemas.

3. . ETIQUETADO MANUAL Y ASISTIDO (Educación)

Policy Tips educan al usuario en el flujo de trabajo.

4. AUTO-LABELING Y CLASIFICACIÓN INTELIGENTE (Escala - Purview Suite)

Trainable Classifiers
- Machine Learning

Client-Side: Al crear/editar (Interactivo) vs **Service-Side:** En reposo/tránsito (Masivo, Retroactivo)

Clasificación automática de terabytes de datos heredados sin intervención humana.

5. 5. PROTECCIÓN Y CIFRADO (Seguridad)

Cifrado AES-256 (AIP/RMS)

QUIÉN: Identidad (Azure AD)

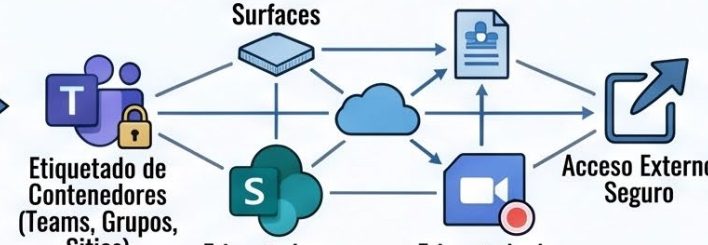
QUÉ: Permisos de Uso (Ver, Editar, Imprimir)

CUÁNDO: Expiración, Acceso Offline

Confidencial – Accedido por [Usuario] el [Fecha/Hora]

La protección viaja con el archivo, independientemente de su ubicación.

6. 6. ALCANCE EXTENDIDO Y GOBERNANZA (Ecosistema - Purview Suite)

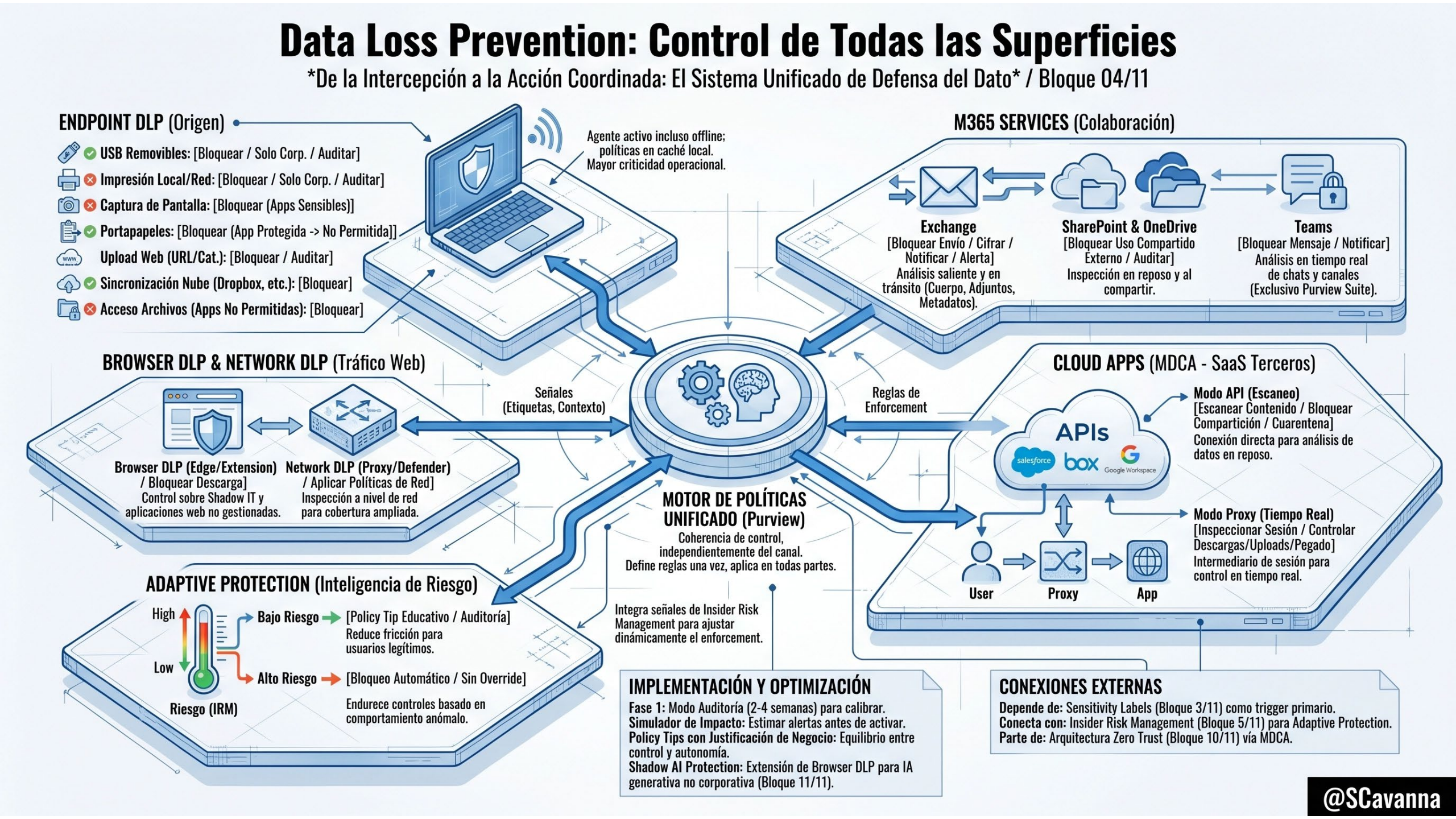


Gobierno Unificado y Trazabilidad

La clasificación se convierte en el sistema nervioso central de la seguridad del dato.

Data Loss Prevention: Control de Todas las Superficies

De la Intercepción a la Acción Coordinada: El Sistema Unificado de Defensa del Dato / Bloque 04/11



Insider Risk Management: El Motor de Correlación de Riesgo Interno y Protección Adaptativa

Detección de Patrones Anómalos, Puntuación Dinámica y Respuesta Automatizada / **Bloque 05/11**

1. ARQUITECTURA DE SEÑALES MULTIFUENTE (Inputs)

SEÑALES M365 (Actividad)

- **SharePoint + Descargas Masivas** (vs. Línea Base)
- **OneDrive + Copias a USB** (Endpoint DLP)
- **Exchange + Impresión Anómala**
- **Endpoint DLP + Movimiento a Carpetas Personales**

→ Monitorización de volumen y comportamiento anómalo en tiempo real.

SEÑALES DE IDENTIDAD (Azure AD/Entra ID)

- **Cambios de Permisos Críticos**
- **Accesos Inusuales** (Geo/Dispositivo)
- **Cambios de Contraseña**
- **Fallos MFA Repetidos**

SEÑALES DE RRHH (Contexto)

- **Notificación de Renuncia**
- **Despido con Causa**
- **Plan de Mejora (PIP)**
- **Cambio de Rol Significativo**

→ Conector HR crítico para identificar el riesgo de salida (ventana de mayor exposición).

Risk Correlation Engine

MOTOR DE CORRELACIÓN DE RIESGO
(Machine Learning + Reglas)

2. PUNTUACIÓN DE RIESGO Y ESCENARIOS (Análisis)

SENARIES DE RIESGO
(Template Ensago)

ESCENARIOS DE RIESGO (Templates Preconfigurados)

- **Robo de Datos por Salida** (Exfiltración pre/post offboarding)
- **Fritreción de Datos** (Compartición inaproppiarda)
- **Filtración de Datos** (Compartición inapropiada)
- **Violaciones de Políticas** (Acceso/Bypass)
- **Uso de Datos Sensibles en IA** (Carga a herramientas no corporativas)
- **Riesgos de Código** (Credenciales en commits)

Risk Score Dial

PUNTUACIÓN DINÁMICA
(Continua, No Binaria)

Baseline Activity — Anomalía

Línea Base Individual vs. Anomalía + Boosters de Puntuación (Ej: Renuncia)

Nivel de Riesgo como Variable Dinámica

3. ADAPTIVE PROTECTION: CIERRE DEL LOOP OPERACIONAL (Respuesta)

- **RIESGO ELEVADO** (Bloqueo Automático sin Override)
- **RIESGO MODERADO** (Alerta + Justificación Requerida)
- **RIESGO MENOR** (Policy Tip Educativo)

DLP ajusta controles automáticamente basado en el nivel de riesgo del usuario, reduciendo fricción.

4. PRIVACIDAD, EVIDENCIA FORENSE Y GOBERNANZA (Control)

Pseudonimización por Defecto

User Ctitre Mule Data → Hashs Hashs Hashs Hashs

→ Analistas ven indicadores, no identidades (Privacidad por Diseño).

FORENSIC EVIDENCE
(Captura Visual Dirigida)

SOC (Solicita) → **LEGAL** (Aprueba) → **ACTIVACIÓN** (Grabación de pantalla acotada)

→ Herramienta de investigación, no vigilancia masiva.

INTEGRACIÓN Y REQUISITOS

- **Microsoft Sentinel** (Incidentes Unificados)
- **Communication Compliance** (Señales de Comunicación)
- **eDiscovery Premium** (Preservación Legal)

→ Implementación requiere evaluación legal local (Ley 25.326, LCT 20.744 en Arg.) y comunicación transparente a empleados.

@SCavanna

Communication Compliance e Information Barriers: Dos Enfoques Complementarios al Riesgo en Comunicaciones

Monitoreo de Contenido (Semántico) vs. Restricción Estructural (Relacional)* / **Bloque 06/11

COMMUNICATION COMPLIANCE (Análisis Semántico)

1. Alcance de Canales de Monitoreo

Microsoft Teams
Exchange Online
Viva Engage
Skype Empresarial

Conectores de Terceros: Bloomberg, ICE Chat, Refinitiv

Análisis de Contenido

*Cobertura esencial para MiFID II, FINRA y normativas financieras.

2. Motor de Detección y Clasificación

Clasificadores Predefinidos
- Angry non/threats
- Contenido inappropriate
- Conflict ed interést
- Código de conduct

Clasificadores Personalizados
- Industry jargon
- Productos específicos
- Termins proprietarios

Condiciones de Política
- Keywords
- Recipientes específicos
- Tipos de atachments

Alertas Generadas

*Detecta patrones de lenguaje y contexto.

3. Flujo de Revisión y Escalación (Segregación de Funciones)

Pendiente assigned to primary reviewer

Pendiente

En Revisión Analysis by reviewer

Resuelta no violation, caso tocsed

Escalada to Legal, RRHH, Compliance Officer

eDiscovery Premium (Investigación Formal)

*Pseudo-anonimización hasta la escalación para proteger privacidad.

INFORMATION BARRIERS (Separación Relacional)

1. Separación Técnica Estructural

Segmento A (Ej: Trading)

Segmento B (Ej: Research)

Error: No se puede añadir usuario. Política de Information Barriers activa.

POLÍTICA DE BARRERA (Bloqueo Técnico)

*Restricciones topológicas: quién puede comunicarse con quién.

2. Definición de Políticas e Impacto

Segmentos (Atributos Azure AD) departament, UPN, título

Políticas de Barrera (Bloquear/Permitir)

Añadir a Conversación
Búsqueda de Usuario
Compartir Archivo/Sitio

*La separación es absoluta y no contextual.

3. Casos de Uso Regulatorios

Servicios Financieros
Muralla China (MiFID II, FINRA, CNV): Trading vs. Research

Servicios Legales
Conflicto de Interés: Equipos en partes opuestas

Sectores Regulados
Información Clasificada: Diferentes niveles de clearance

CONEXIONES EXTERNAS Y SINERGIAS

Insider Risk Management (Bloque 5/11)
Datos communication compliance pars·si Information Barriers

Alert a dects violationes

Breachos las políticas

eDiscovery Premium (Bloque 7/11)
Casos investigaciones y supporta investigaciones.

Information Protection (Bloque 3/11)
- Etiqueta de Contenedor
- IB Policy

*Capas de control adicionales sobre acceso y colaboración.

*Nota LATAM: Requiere evaluación legal y política de uso aceptable clara (Argentina: Ley 25.326, LCT, jurisprudencia CSJN).

eDiscovery Premium y Audit Premium: El Roadmap de la Investigación Forense y Legal

Infraestructura de Preservación, Análisis y Cadena de Custodia en Microsoft Purview / **Bloque 07/11**

1. PRESERVACIÓN Y GESTIÓN DE CUSTODIOS (Legal Hold)

Legal Hold automático sobre custodios designados (incl. elementos eliminados).

Notificación formal y seguimiento de acuse de recibo registrado.

Base de la investigación: congela la evidencia antes de cualquier alteración.

2. RECOLECCIÓN Y PROCESAMIENTO (Review Sets)

Conversation Threading (Hilos de Email/Teams)

Near-Duplicate Detection (Agrupación de Similares)

Predictive Coding (ML Relevance Scoring)

Reducción masiva del volumen de revisión asistida por IA. Priorización estadística de documentos relevantes.

3. ANÁLISIS Y REVISIÓN ASISTIDA (Eficiencia Legal)

El modelo ML aprende de las decisiones del revisor para predecir la relevancia en el resto del set.

Acelera la revisión manual y reduce costos en litigios de alto volumen.

4. EXPORTACIÓN Y CADENA DE CUSTODIA (Defensibilidad)

#SHA-256

Manifest de Exportación (Lista de Ítems, Hashes, Metadatos, Timestamp, Custodio)

Nativos (PST, Office)

Procesados (PDF, Texto)

Registro inmutable de quién exportó qué y cuándo. Verificable ante terceros.

5. AUDIT PREMIUM: RETENCIÓN Y PROFUNDIDAD (Capa Forense)

Standard (E3)	90 Días de Retención
Premium (Purview Suite)	1 Año de Retención (Por Defecto) + Eventos de Alta Fidelidad
Add-on (Regulado)	10 Años de Retención (Extendida)

Eventos Críticos: MailItemsAccessed (Acceso granular a mensajes), SearchQueryInitiated, FileDownloaded.

Fundamental para investigar incidentes detectados tardíamente (BEC, Exfiltración).

6. INTEGRACIÓN SIEM Y API DE ALTO ANCHO DE BANDA (Ecosistema de Seguridad)

API de Gestión de Actividad (50k solicitudes/hora)

Ingesta de logs de alta velocidad para correlación en tiempo casi real. Audit Premium como fuente de verdad forense.

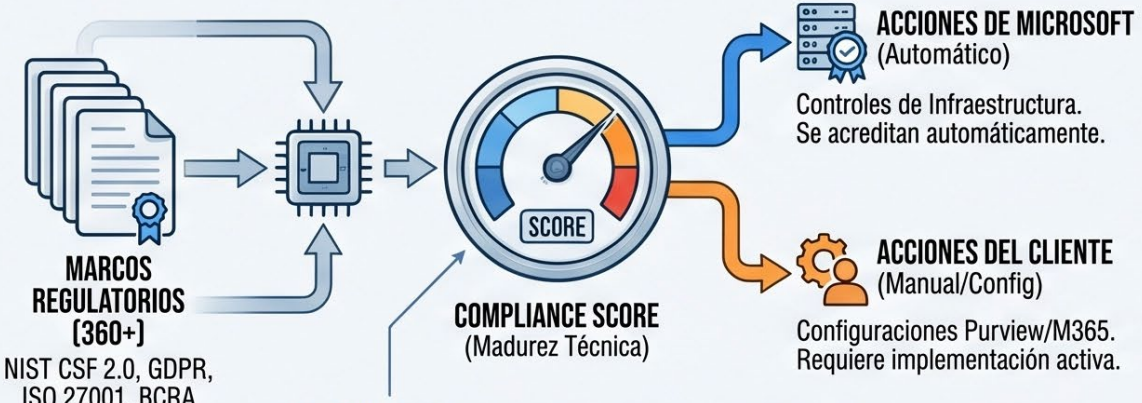
La infraestructura legal y técnica para investigaciones internas, regulatorias y litigios complejos.

BLOQUE 8/11 — COMPLIANCE MANAGER Y CONTROLES DE CIFRADO Y ACCESO PRIVILEGIADO

El Plano de Control y Soberanía de Microsoft Purview: De la Evidencia Normativa al "Kill Switch" Criptográfico.

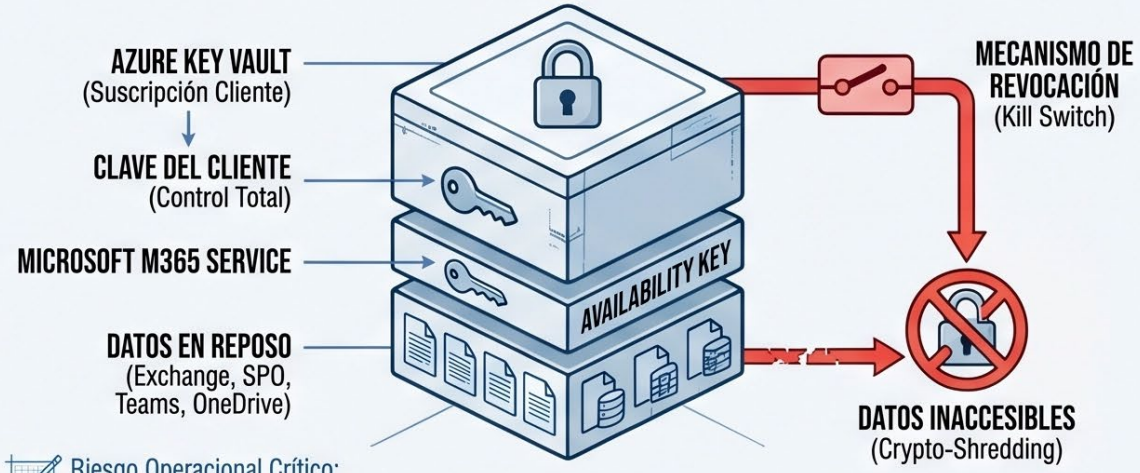
CORE INSIGHT: Traducción de controles técnicos en evidencia auditable. Garantía de soberanía sobre datos y mínimo privilegio, incluso frente al proveedor (Microsoft).

COMPLIANCE MANAGER: EL PUENTE NORMATIVO (Acción vs. Evidencia)



Nota: El Score es un indicador de madurez técnica, no un certificado legal. Integra con Secure Score.

CUSTOMER KEY: SOBERANÍA CRIPTOGRÁFICA (El "Kill Switch")



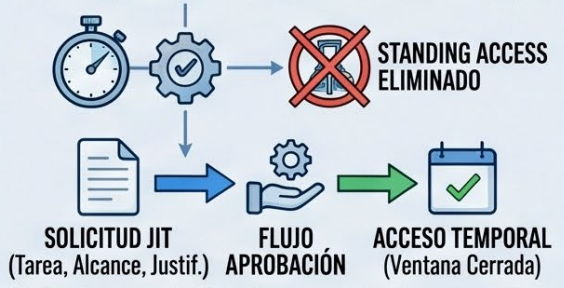
Riesgo Operacional Crítico: La pérdida de acceso al Key Vault = pérdida permanente de datos. Requiere madurez en gestión de claves.

CUSTOMER LOCKBOX: CONTROL DE ACCESO DE SOPORTE (Aprobación Bilateral)

Proceso inmutable registrado en Audit Premium.

PAM & ADVANCED ENCRYPTION (Acceso JIT y Control Externo)

PAM (PRIVILEGED ACCESS MANAGEMENT)



Elimina el acceso administrativo permanente a tareas específicas.

ADVANCED MESSAGE ENCRYPTION

Control sobre datos sensibles fuera del perímetro del tenant.

Licenciamiento: E3 vs. Purview Suite — Mapa de Valor

Manual vs. Automatizado: El Umbral de la Escalabilidad y el Riesgo / **Bloque 09/11**

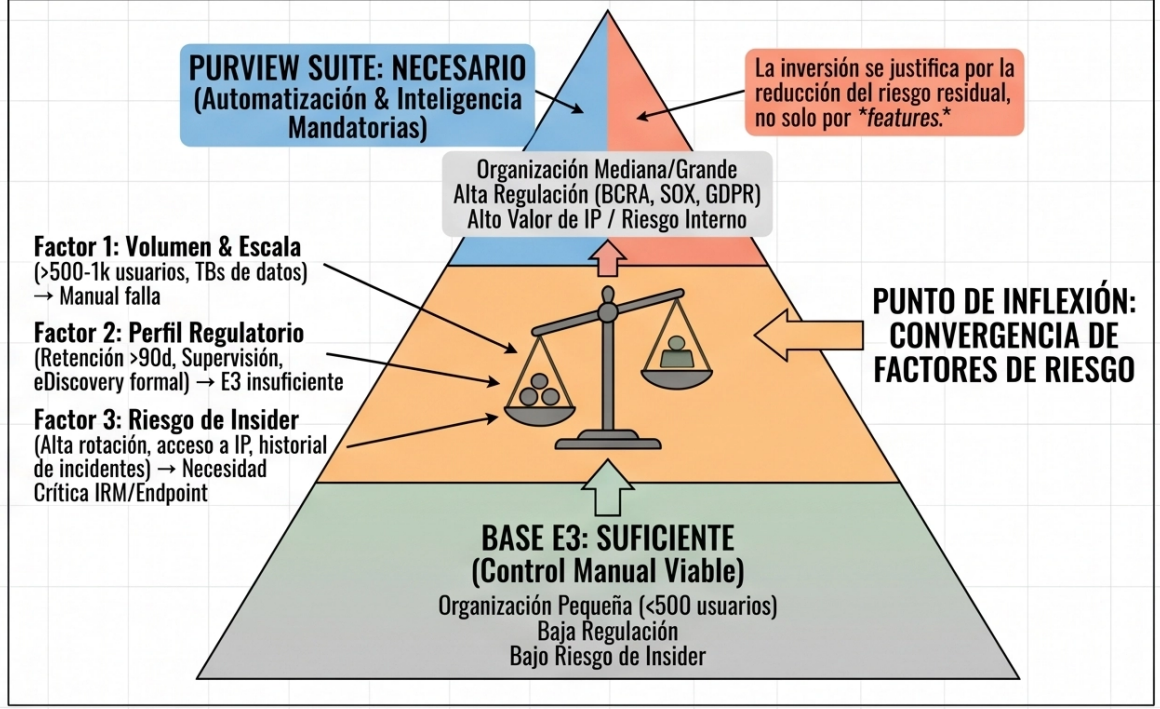
COMPARATIVA FUNCIONAL: DELTA DE CAPACIDADES (Manual vs. Inteligente)

	M365 E3 (Control Manual / Base)	DELTA	PURVIEW SUITE (Automatización / Escala)
1. INFORMATION PROTECTION (Clasificación & Etiquetado)	Etiquetado Manual en Apps Office Cifrado Básico RMS/AIP Marcas Visuales Estáticas Cobertura Típica: ~20-30% (Dependencia del Usuario)	La brecha no es de *features*, es de *cobertura* real sobre el dato.	Auto-Labeling (ML/Clasificadores Entrenables) Etiquetado por Defecto en Librerías Marcas Dinámicas & Variables Objetivo Cobertura: >80% (Escala Sin Intervención)
2. DATA LOSS PREVENTION (DLP - Superficies)	Exchange, SharePoint, OneDrive **3 Canales Core** (Reposo/Tránsito)		Exchange, SharePoint, OneDrive, Teams, Endpoint Endpoint, Browser, Cloud Apps Sin Endpoint DLP, la exfiltración física (USB) queda fuera de control técnico. **7 Superficies** (Incluyendo Endpoint Crítico & Shadow IT)
3. CAPACIDADES EXCLUSIVAS SUITE (Sin Equivalente E3)	NO DISPONIBLE Tin third-party solution stachles		Insider Risk Management Communication Compliance eDiscovery Premium (Custodios, Review Sets) Audit Premium (+90 días, Alta Fidelidad) Information Barriers Customer Key / Lockbox Privileged Access Management

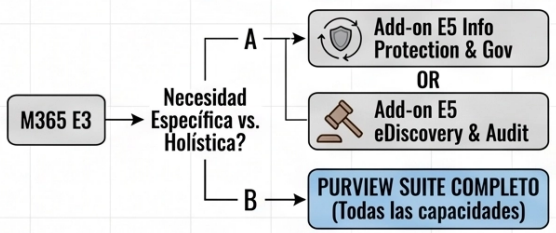
↳ Intentar cubrir esto con terceros suele ser más costoso y complejo que el upgrade.

threshold

JERARQUÍA DE DECISIÓN: EL UMBRAL DE COMPLEJIDAD

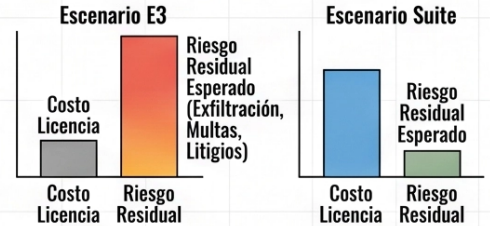


MODELO DE ADD-ONS: INVERSIÓN GRANULAR



↳ Evaluar si la suma de add-ons supera el costo/complejidad de la Suite completa.

PROPUESTA DE VALOR: RIESGO RESIDUAL vs. COSTO

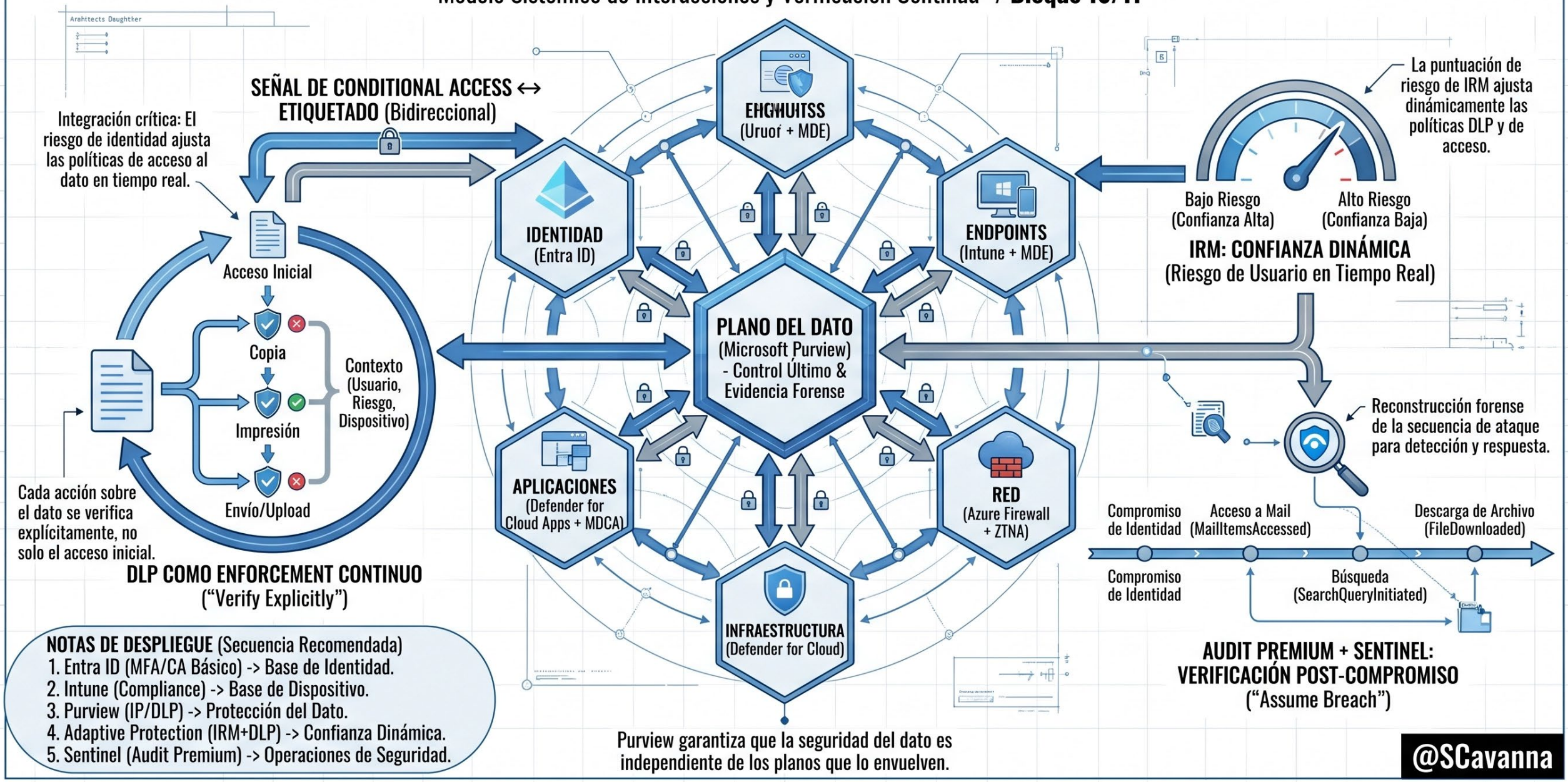


↳ Enmarcar la inversión ante el directorio en términos de costo de riesgo evitado, no de "más herramientas".

@SCavanna

Purview en una Arquitectura Zero Trust: El Plano de Control del Dato como Última Línea de Defensa

Modelo Sistémico de Interacciones y Verificación Continua / **Bloque 10/11**



Gobernanza para IA y Copilot: el Nuevo Perímetro del Dato

De la Exposición Amplificada al Control Estratégico: El Roadmap de la Adopción Segura de IA / **Bloque 11/11**