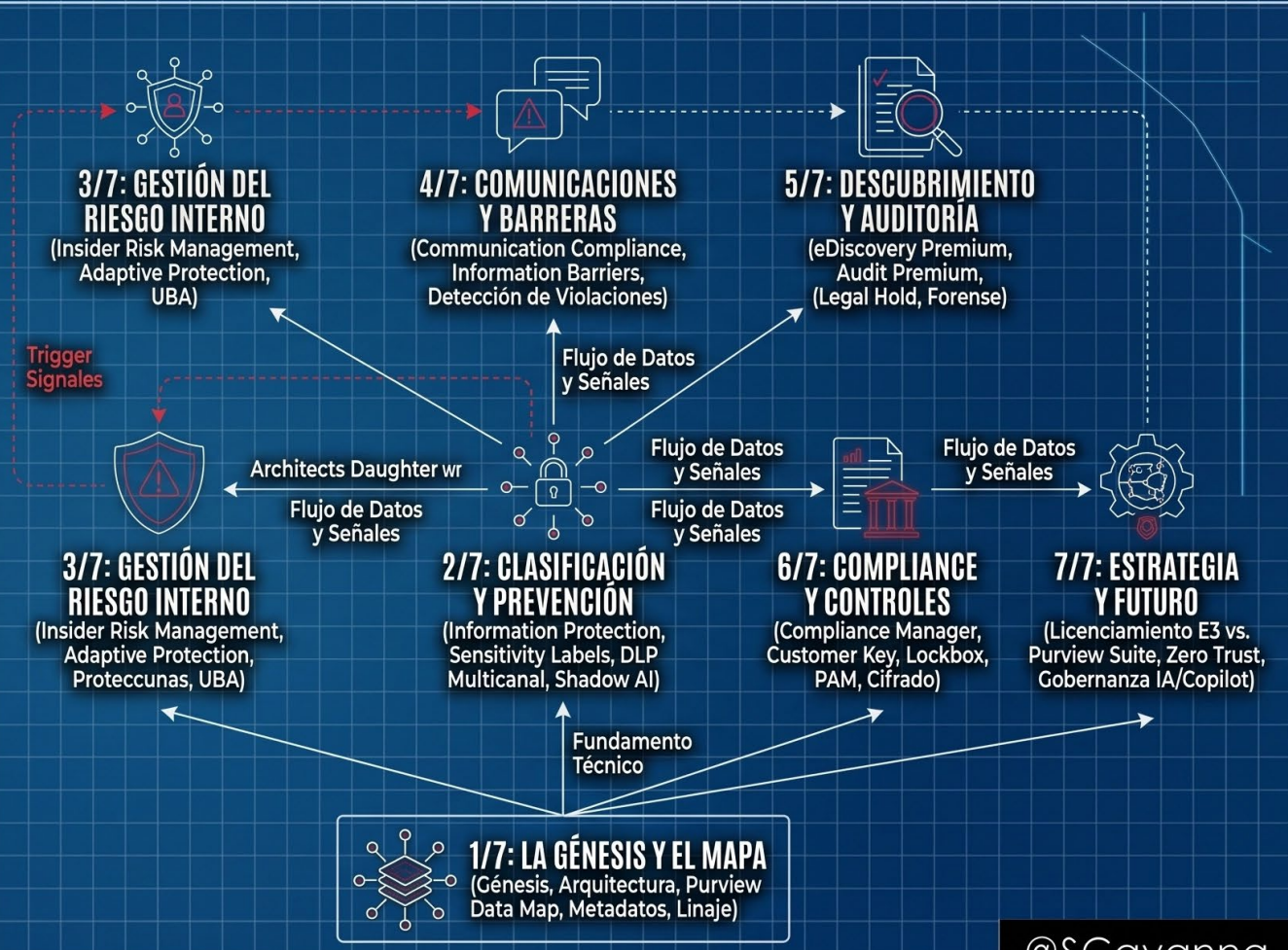
MICROSOFT PURVIEW SUITE: GOBERNANZA, PROTECCIÓN Y CUMPLIMIENTO

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

01/ - Génesis y arquitectura conceptual de Microsoft Purview

Idea Central

El texto explica el origen y la arquitectura conceptual de Microsoft Purview como plataforma unificada de gobierno, seguridad y cumplimiento del dato. Describe cómo se integran los mundos de Azure y Microsoft 365 y qué problemas resuelve esta convergencia.
También explica cómo se organiza la solución en pilares funcionales, modelos de licencia y principios de diseño. Su finalidad es ayudar a alinear a equipos de datos, seguridad, cumplimiento y negocio en una narrativa técnica y operativa, clara y orientada a decisiones.

Temas principales

1. Antes de 2022 coexistían Azure Purview y Microsoft 365 Compliance sin integración real. La protección cubría un contexto: colaboración o infraestructura. La unificación en Microsoft Purview crea un modelo común de metadatos y una identidad de plataforma. Etiquetas y políticas acompañan al dato a través de nubes, aplicaciones y equipos.

2. Purview se organiza en tres pilares. Gobierno de datos gestiona inventario, linaje, calidad y acceso en entornos de información. Seguridad y Riesgo y Cumplimiento ofrecen clasificación, cifrado, DLP, auditoría y eDiscovery en Microsoft 365. Esta división marca licenciamiento y equipos separados, coordinados por un portal y control de acceso unificados.

3. Purview Suite, nombre del paquete avanzado de cumplimiento, representa el máximo nivel de capacidades en Seguridad y en Riesgo y Cumplimiento. Aporta automatización e inteligencia frente al enfoque manual de Microsoft 365 E3. El principio central es que cifrado y etiquetas acompañan siempre al dato, también fuera del perímetro seguro.

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.

02/ - Purview Data Map: corazón técnico de la gobernanza

Idea Central

Purview Data Map es el núcleo técnico de la gobernanza de datos en Microsoft Purview. Conecta fuentes multicloud y on-premises, escanea y cataloga metadatos técnicos y semánticos, y construye linaje detallado. Sobre ese inventario habilita catálogo unificado y políticas de acceso centralizadas. También ofrece uso compartido seguro y una taxonomía común de sensibilidad que integra gobierno y seguridad. Su modelo de capacidad escala con el tamaño del patrimonio de datos y alimenta clasificación, DLP, Compliance Manager e investigaciones eDiscovery clave.

Temas principales

1. Purview Data Map escanea fuentes de datos en Azure, otras nubes y entornos locales. Usa conectores nativos y ejecuciones completas o incrementales para minimizar impacto. De cada activo captura metadatos técnicos. En paralelo aplica clasificadores de datos sensibles. El resultado es un inventario técnico y semántico centralizado. Base de gobernanza.

2. Sobre ese inventario, el Data Map construye linaje automático para procesos en servicios analíticos de Azure y Fabric. Registra orígenes, transformaciones y destinos. Facilita auditorías de privacidad y análisis de impacto ante brechas. El Unified Catalog traduce nombres técnicos a lenguaje de negocio y facilita búsqueda guiada por dominio claramente.

3. Data Policy centraliza permisos sobre servicios de datos en Azure y reduce configuraciones inconsistentes. El modelo de Capacity Units alinea costo con tamaño del patrimonio gobernado. Data Estate Insights ofrece métricas ejecutivas. Data Sharing habilita colaboración sin duplicar datos. Las sensitivity labels unifican gobierno, seguridad y capacidades DLP y eDiscovery.

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

03/ - Information Protection: clasificación y etiquetado

Idea Central

El texto describe cómo Microsoft Purview Information Protection clasifica y protege información sensible en Microsoft 365 y Azure. Explica los motores de detección, los clasificadores entrenables y las sensitivity labels. Detalla el etiquetado automático a gran escala y su despliegue por fases. También aborda la integración con aplicaciones no Microsoft y la convivencia con soluciones DLP de terceros. Describe la conexión con otros como Data Map, Information Barriers y el cifrado con claves de cliente. Resalta taxonomías y políticas.

Temas principales

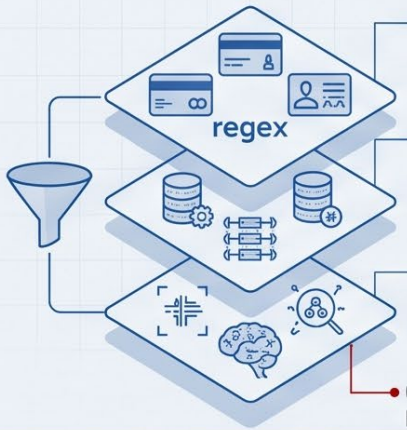
1. Los motores de detección combinan tipos de información sensible basados en patrones, coincidencias exactas con datos corporativos y entidades nombradas en texto libre. Sobre esta base se añaden clasificadores entrenables que aprenden categorías, como contratos o historiales clínicos. Así se identifica contenido y se prepara el terreno para etiquetado automático.
2. Las sensitivity labels agrupan marcas visuales, cifrado y configuración de contenedores como equipos y sitios. El cifrado controla quién abre, qué puede hacer y durante cuánto tiempo. Purview Suite amplía su alcance a bibliotecas, Teams y reuniones, añade marcas de agua dinámicas y permite aplicar estas protecciones de forma coherente.

3. La implantación comienza definiendo la taxonomía de etiquetas, sigue con etiquetado manual asistido y activa auto labeling en simulación y enforcement progresivo. El modelo contempla compatibilidad con PDF y usuarios externos y convivencia con DLP de terceros. Las etiquetas sostienen políticas de DLP, Information Barriers, Customer Key y Data Map.

BLOQUE 3/11: INFORMATION PROTECTION – CLASIFICACIÓN Y ETIQUETADO

Flujo Secuencial de Madurez: De la Detección de Contenido a la Protección Cifrada y el Alcance Extendido.

1. MOTOR DE DETECCIÓN (SIT, EDM, NAMED ENTITIES)



SENSITIVE INFO TYPES (SIT)
300+ Patrones Predefinidos (Validación, Funciones, Confianza Alta/Media/Baja).

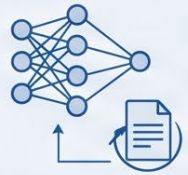
EXACT DATA MATCH (EDM)
Detección sobre Datos Reales Hashed (Sin acceso al dato en claro). Reduce Falsos Positivos.

NAMED ENTITIES
Detección Semántica AI (Personas, Org., Lugares, Términos Médicos) en Texto Libre.

Capas de detección superpuestas para máxima precisión.

2. CLASIFICADORES ENTRENABLES (TRAINABLE CLASSIFIERS) [SUITE EXCLUSIVO]

Crítico para automatizar contenido propietario no estructurado.



Modelos de Machine Learning para Categorías Propias de la Organización.

ENTRENAMIENTO:
50-500 Ejemplos Positivos/Negativos. Retroalimentación Iterativa.

3. ESTRUCTURA DE SENSITIVITY LABELS (LA INSTRUCCIÓN TÉCNICA)

MARCAS VISUALES
Encabezado, Pie, Marca de Agua (Estática/Dinámica). Trazabilidad Visual.

CIFRADO (AES-256 / AZURE RMS)
Quién accede, con qué permisos (Ver, Editar, Imprimir), por cuánto tiempo. La clave viaja con el archivo.

CONFIGURACIONES DE CONTENEDOR
Privacidad de Team/Site, Acceso Externo, Dispositivos No Gestionados.

Se aplica al ABRIR, no al crear. Genera trazabilidad de acceso individual.

4. AUTO-LABELING A ESCALA (LA DIFERENCIA OPERACIONAL)

CLIENT-SIDE (EN TIEMPO REAL) [CRÍTICO]
Aplicación en creación/edición por usuario (basado en contenido).

SERVICE-SIDE (EN REPOSO/TRÁNSITO) [CRÍTICO]
Políticas de escaneo en segundo plano. Aplica retroactivamente a inventario histórico (60-80% del total).

Sin esto, el etiquetado de millones de documentos heredados es imposible.

5. ALCANCE EXTENDIDO DEL ETIQUETADO [PURVIEW SUITE EXCLUSIVO]

CONTENEDORES (TEAMS, M365 GROUPS, SITES)
Configura privacidad y acceso automáticamente.

LIBRERÍAS SHAREPOINT POR DEFECTO

REUNIONES ONLINE (TEAMS PREMIUM)
Etiqueta define permisos de grabación y acceso externo.

Extensión de la protección más allá del archivo individual.

NOTAS DE SOPORTE Y COEXISTENCIA

INTEGRACIÓN PDF/EXTERNA:
Plugin AIP para Acrobat. Portal de mensajes para usuarios sin Azure AD.

COEXISTENCIA DLP TERCEROS:
Sensitivity Labels como metadatos inspeccionables vía SDK/Graph API.

ESTRATEGIA DE IMPLEMENTACIÓN POR FASES (MÉTODO RECOMENDADO)

1. **DEFINIR TAXONOMÍA** (4-6 Niveles, Sublabels)
2. **ETIQUETADO MANUAL + TIPS** (Educación)
3. **AUTO-LABELING EN SIMULACIÓN** (Evaluación de Impacto, SIN enforcement)
4. **DESPLIEGUE PROGRESIVO** (Exchange -> SP/OD -> Endpoint)

⚠ Fase crítica: evita ruido operacional y pérdida de confianza.

CONEXIONES EXTERNAS

- Prerequisito para DLP (Bloque 4/11)
- Conecta con Information Barriers (Bloque 6/11)
- Base para Customer Key (Bloque 8/11)
- Comparte taxonomía con Data Map (Bloque 2/11)

[@SCavanna]

04/ - Data Loss Prevention: control de todas las superficies

Idea Central

Este bloque describe cómo Microsoft Purview controla la pérdida de datos en todas las superficies clave. Explica el rol del agente en los dispositivos, los servicios de colaboración en la nube y aplicaciones SaaS de terceros. Presenta el uso de protección adaptativa basada en riesgo y su integración con Insider Risk. Además, detalla recomendaciones de enccomendabidos de despliegue gradual y uso de justificaciones de negocio. También presenta capacidades para proteger datos frente a herramientas de inteligencia artificial generativa en entornos complejos.

Temas principales

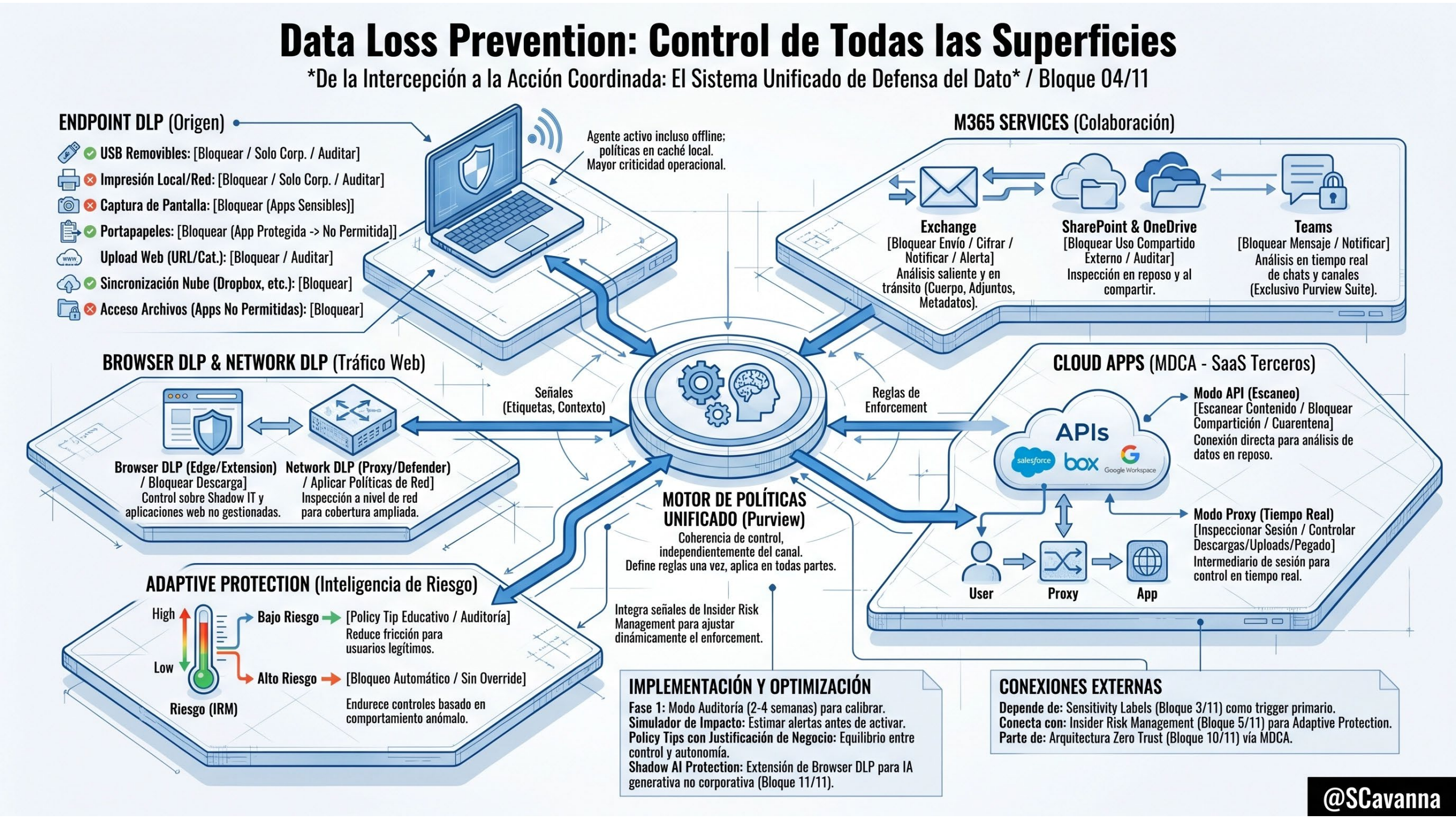
1. El texto explica cómo Purview protege datos en el origen, con control en dispositivos Windows y macOS. El agente de endpoint limita USB, impresión, capturas y portapapeles. Además, DLP en Exchange, SharePoint, OneDrive y Teams vigila correos, archivos y chats, bloqueando compartición externa inadecuada y aplicando cifrado cuando es necesario.

2. Luego describe el control en el navegador y la red. Browser DLP protege el uso de aplicaciones web personales y evita subir o pegar datos sensibles. Network DLP inspecciona tráfico mediante proxy. Defender for Cloud Apps amplía estas políticas a SaaS de terceros, usando integraciones API y proxy de sesión.

3. Finalmente expone la protección adaptativa, que combina análisis de riesgo interno con DLP. Así, el bloqueo se endurece para usuarios de alto riesgo y se relaja para el resto. También recomienda empezar en auditoría, usar simulador, exigir justificación escrita y extender controles a herramientas de inteligencia artificial no corporativas externas.

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



05/ - Insider Risk Management y Adaptive Protection

Idea Central

Insider Risk Management (IRM) y Adaptive Protection describen cómo Microsoft 365 detecta y mitiga riesgos internos basados comportamiento. El documento explica la arquitectura de señales, los escenarios de riesgo y la puntuación dinámica por usuario. Además detalla la integración con DLP y herramientas forenses. Su finalidad es reducir filtraciones, automatizar respuestas y cumplir requisitos legales y de privacidad, especialmente en entornos corporativos complejos y regulados. También muestra cómo coordinar señales de identidad, dispositivos, red y recursos humanos para cerrar el ciclo operativo.

Temas principales

1. IRM construye su modelo de riesgo correlando señales de Microsoft 365, identidad y sistemas de recursos humanos. Observa descargas inusuales, copias a USB, accesos atípicos y cambios de permisos. Los eventos de RRHH, como renuncias o planes disciplinarios, actúan como disparadores. Así detecta tempranamente exfiltración ligada al offboarding de empleados.

2. El modelo define cinco escenarios de riesgo. Incluyen robo de datos de usuarios salientes, filtración de información, uso de datos en inteligencia artificial, violaciones de políticas y exposición de código. Cada escenario tiene plantillas con señales y umbrales. La puntuación dinámica de usuario reduce falsos postitivos usando líneas de referencia.

3. Adaptive Protection cierra el ciclo operativo al traducir la puntuación de riesgo en controles DLP suaves o restrictivos. Forensic Evidence aporta evidencia visual bajo aprobación estricta y plazos limitados. La pseudonimización, las revisiones legales y la integración con Sentinel y eDiscovery alinean alinean monitoreo, privacidad y respuesta coordinada en el SOC.

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

06/ - Communication Compliance e Information Barriers

Idea Central

Communication Compliance e Information Barriers son capacidades de Microsoft Purview para supervisar comunicaciones y bloquear interacciones indebidas. El bloque describe qué canales se cubren y cómo funciona el motor de detección y el flujo de revisión. También explica la aplicación de las barreras de información, sus restricciones arquitectónicas y requisitos legales en Latinoamérica. Finalmente conecta estas capacidades con Insider Risk, eDiscovery e Information Protection para para construir esquemas de cumplimiento regulatorio y protección de datos en sectores financieros, legales y gubernamentales.

Temas principales

1. Communication Compliance supervisa comunicaciones en Teams, Exchange, Viva Engage, Skype empresarial y canales externos financieros. Analiza contenido con clasificadores predefinidos y personalizados que detectan acoso, lenguaje inapropiado, amenazas, conflicto de interés y violaciones de conducta. Las políticas combinan clasificadores, palabras clave y metadatos para generar alertas a revisores internos designados.

2. El flujo de revisión sigue etapas claras: alerta pendiente, en revisión, resuelta o escalada a áreas legales, recursos humanos o cumplimiento. Se respeta la segregación de funciones y se registra cada acción en auditoría. En Argentina y Latinoamérica, el monitoreo exige base legal, política de uso aceptable y comunicación clara.

3. Information Barriers define segmentos y políticas que bloquean comunicación y colaboración entre grupos incompatibles en Teams, SharePoint y Exchange. Las políticas son estáticas; cambiarlas requiere análisis regulatorio estricto. Estas barreras sostienen murallas chinas, evitan conflictos de interés, protegen información sensible y se integran con Insider Risk, eDiscovery e Information Protection.

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).

07/ - eDiscovery Premium y Audit Premium

Idea Central

El texto describe las capacidades avanzadas de eDiscovery Premium y Audit Premium dentro de Microsoft Purview y Microsoft 365. Su foco es la preservación de evidencia digital, la revisión asistida por aprendizaje automático y la exportación con cadena de custodia verificable. Además explica cómo Audit Premium amplía la retención y profundidad de registros forenses y cómo estos datos se integran con plataformas SIEM. documento relaciona estas capacidades con requerimientos regulatorios y de litigación, y con soluciones de riesgo interno y cumpllimiento comunicacional.

Temas principales

1. eDiscovery Premium gestiona custodios y aplica Legal Hold sobre correo, sitios y archivos sin depender del usuario. Crea conjuntos de revisión donde reconstruye hilos de conversación, agrupa casi duplicados y usa modelos de relevancia. Así reduce volumen, prioriza evidencias clave y supera ampliamente las capacidades básicas de eDiscovery Standard actual.

2. Audit Premium extiende la retención de registros a un año, con opción de diez años para sectores regulados. Registra eventos granulares como acceso a mensajes individuales, búsquedas de contenido y descargas de archivos. El evento MailItemsAccessed responde a brechas como SolarWinds y permite saber qué información vio un atacante claramente.

3. La API de auditoría de alta capacidad permite enviar grandes volúmenes de registros a plataformas SIEM como Microsoft Sentinel. Así, Audit Premium se convierte en la fuente forense del plano de productividad. Estos registros alimentan investigaciones de riesgo interno, casos de cumplimiento comunicacional y el modelo de seguridad Zero Trust.

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.

08/ - Compliance Manager y controles de cifrado y acceso

Idea Central

Este bloque describe cómo Microsoft Purview y M365 conectan controles técnicos con requerimientos normativos. Explica el rol de Compliance Manager, Customer Key, Access Management y Advanced Message Encryption. El objetivo es mostrar cómo estos componentes aportan evidencia de cumplimiento, soberanía criptográfica y control granular del acceso privilegiado y del intercambio seguro de información. También explica su integración profunda con Secure Score y con bloques previos de la arquitectura, como clasificación, DLP, IRM, análisis forense y Zero Trust.

Temas principales

1. Compliance Manager actúa como puente entre Purview y los marcos normativos. Organiza evaluaciones, mapea controles a acciones y distingue controles de Microsoft y del cliente. El Compliance Score mide implementación técnica, no certificación. Además, integra acciones con Secure Score y refleja avances de clasificación, DLP, IRM y forense previos

2. Customer Key permite que la organización use sus propias claves en Azure Key Vault para cifrar datos en M365. Otorga soberanía criptográfica y capacidad de revocación total, incluso frente a Microsoft. Exige procesos maduros de gestión, copias de seguridad, pruebas de recuperación y una fase previa con claves gestionadas.

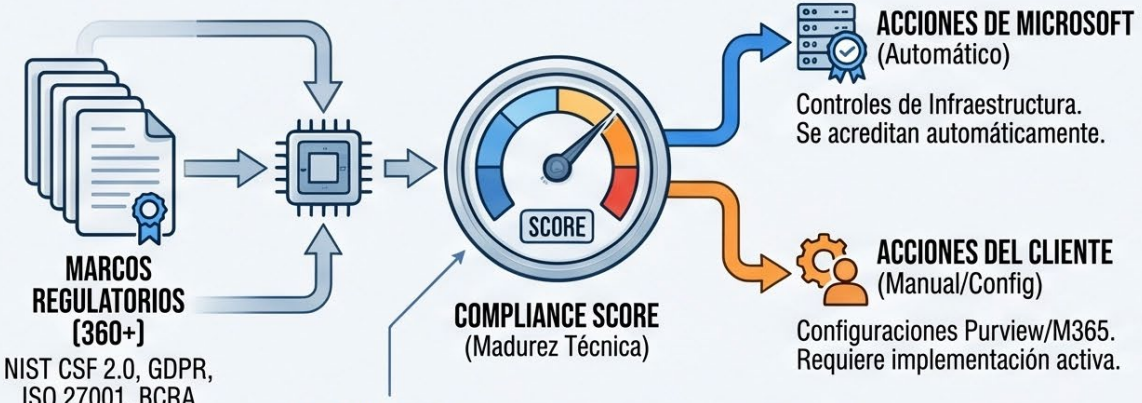
3. Customer Lockbox obliga a aprobar cada acceso de soporte a datos del tenant y deja trazabilidad detallada. Privileged Access Management elimina acceso permanente a tareas sensibles y se alinea con Zero Trust. Advanced Message Encryption protege correos externos, permite revocar o caducar mensajes y aplica identidad visual propia corporativa.

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.

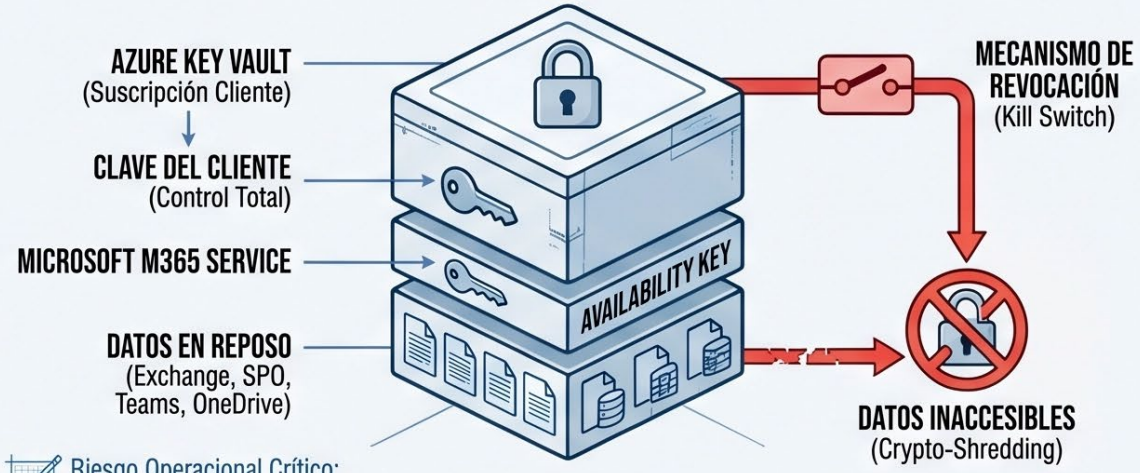
CORE INSIGHT: Traducción de controles técnicos en evidencia auditable. Garantía de soberanía sobre datos y mínimo privilegio, incluso frente al proveedor (Microsoft).

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")



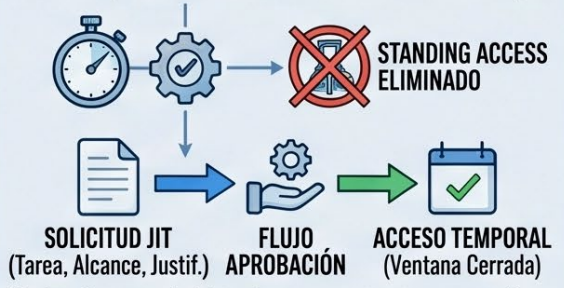
Riesgo Operacional Crítico: La pérdida de acceso al Key Vault = pérdida permanente de datos. Requiere madurez en gestión de claves.

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.

09/ - Licenciamiento: E3 frente a Purview Suite, mapa de valor

Idea Central

El bloque explica cómo decidir entre mantener licencias Microsoft 365 E3 o invertir en Purview Suite y complementos. Compara protección de información manual frente a automatizada, alcance de DLP en distintos canales y capacidades avanzadas de cumplimiento. El objetivo es traducir diferencias técnicas en reducción de riesgo residual y en criterios claros para inversión. Además, vincula estas decisiones con arquitecturas Zero Trust y con la gobernanza de proyectos de inteligencia artificial. Sirve como mapa de valor para conversaciones con ejecutivos.

Temas principales

1. Purview Suite automatiza la clasificación de datos y mejora la cobertura de DLP frente al enfoque manual de E3. El autoetiquetado y los clasificadores reducen el volumen de contenido sin clasificar. La ampliación de DLP a Teams, dispositivos, navegador, red y servicios en la nube cierra brechas de exfiltración silenciosa.

2. Purview Suite incluye funciones sin equivalente en E3, como gestión de riesgo interno e inspección de comunicaciones. También ofrece eDiscovery avanzado, auditoría detallada, barreras de información y controles sobre claves y accesos privilegiados. Reemplazar este conjunto con múltiples herramientas externas suele aumentar costos, integración y puntos de falla operativos adicionales.

3. Los add-ons de Purview permiten licenciar solo capacidades críticas, como clasificación avanzada, ciclo de vida, eDiscovery y auditoría mejorada. El punto de equilibrio llega con más de quinientos usuarios, regulaciones exigentes y riesgo interno relevante. Con el CFO, la discusión compra compara costo esperado de incidentes frente al costo de licencias.

Licenciamiento: E3 vs. Purview Suite — Mapa de Valor

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

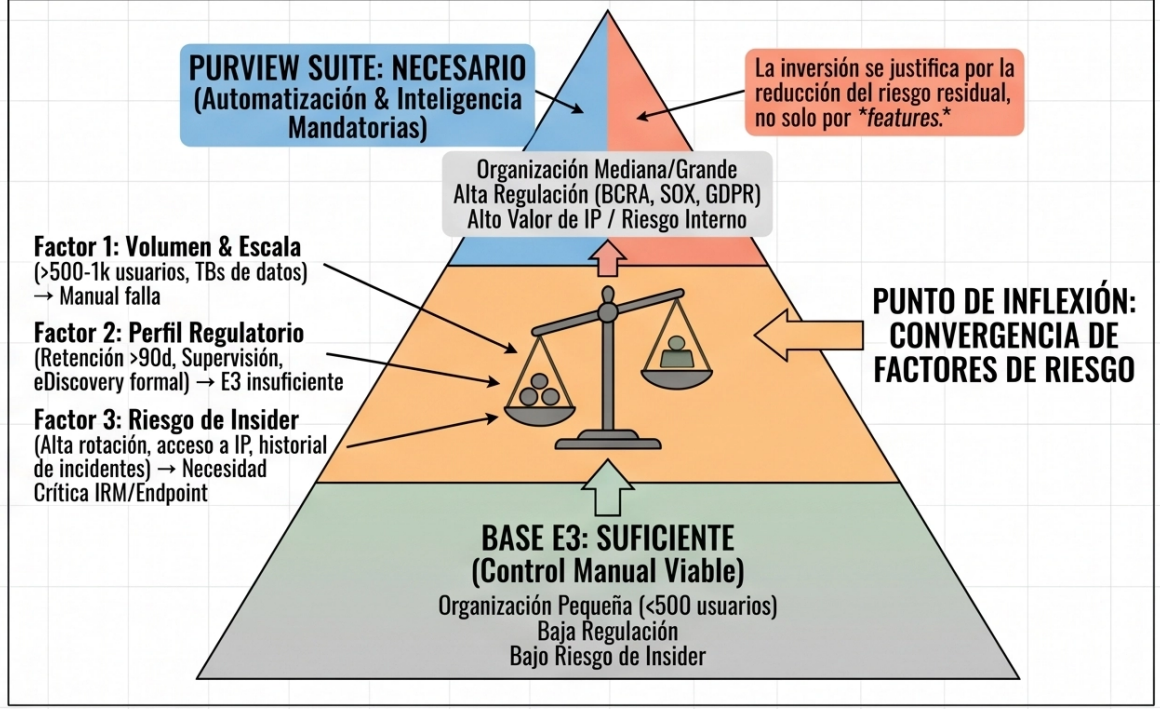
COMPARATIVA FUNCIONAL: DELTA DE CAPACIDADES (Manual vs. Inteligente)

	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

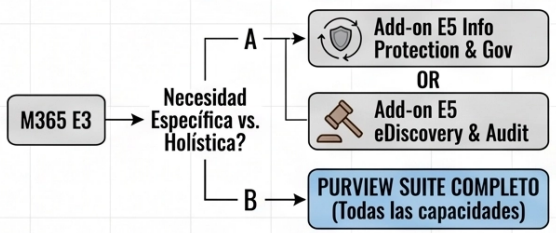
↳ Intentar cubrir esto con terceros suele ser más costoso y complejo que el upgrade.

threshold

JERARQUÍA DE DECISIÓN: EL UMBRAL DE COMPLEJIDAD

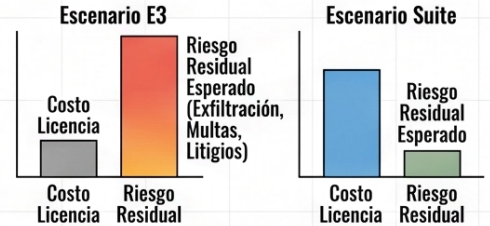


MODELO DE ADD-ONS: INVERSIÓN GRANULAR



↳ 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

10/ - Purview en una arquitectura Zero Trust

Idea Central

Microsoft Purview se presenta como el el plano de control del dato dentro de una arquitectura Zero Trust. El texto explica cómo Purview se integra con Entra ID, Intune, Defender y Sentinel. Aplica cifrado, etiquetado, DLP, DLP, gestión de riesgo interno y auditoría avanzada. Su finalidad es mostrar que la seguridad del dato debe ser independiente, dinámica y verificable, incluso ante identidades comprometidas, dispositivos inseguros, redes hostiles y nuevos agentes de IA generativa como Copilot.

Temas principales

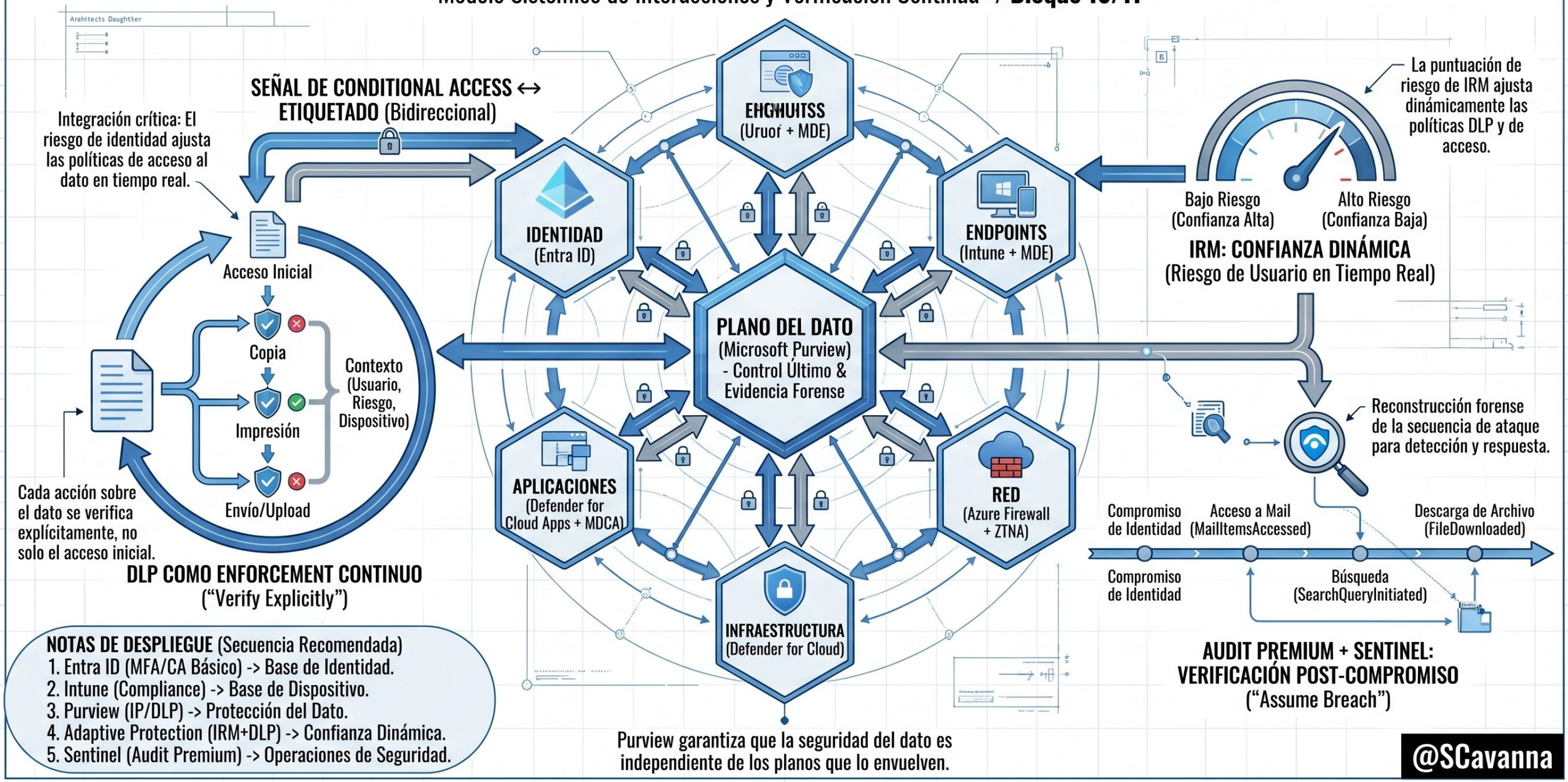
1. el texto sitúa a purview como pilar de datos en el modelo zero trust de microsoft, junto a identidad, dispositivos, aplicaciones, red e infraestructura. explica cómo las sensitivity labels cifran y clasifican archivos, y se usan como señal en conditional access. destaca que identidad e información deben desplegarse y madurar primero.

2. en cuanto al control del uso del dato, describe purview dlp como aplicación del principio verify explicitly. cada acción sobre información sensible se evalúa con contexto de usuario, dispositivo gestionado por intune y destino. además, adaptive protection ajusta las reglas según el riesgo calculado por insider risk management, por eso se activa después de dlp.

3. por otro lado, audit premium materializa el principio assume breach. registra durante un año acciones detalladas sobre correos y archivos, y las envía a sentinel para correlación con señales de identidad, dispositivo, red y aplicación. finalmente, se destaca que agentes de ia como copilot heredan permisos y controles de purview.

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**



11/ - Gobernanza para IA y Copilot, el nuevo perímetro del dato

Idea Central

El documento explica cómo cambia el perímetro del dato al introducir Copilot para Microsoft 365 y otras IA generativas en la empresa. Describe riesgos de exposición derivados de permisos heredados y de Shadow AI, y presenta capacidades de Microsoft Purview, como DSPM for AI, etiquetado automático y DLP. Su finalidad es guiar un despliegue de Copilot basado en gobernanza, madurez de protección de información y cumplimiento regulatorio, más que solo en objetivos de productividad.

Temas principales

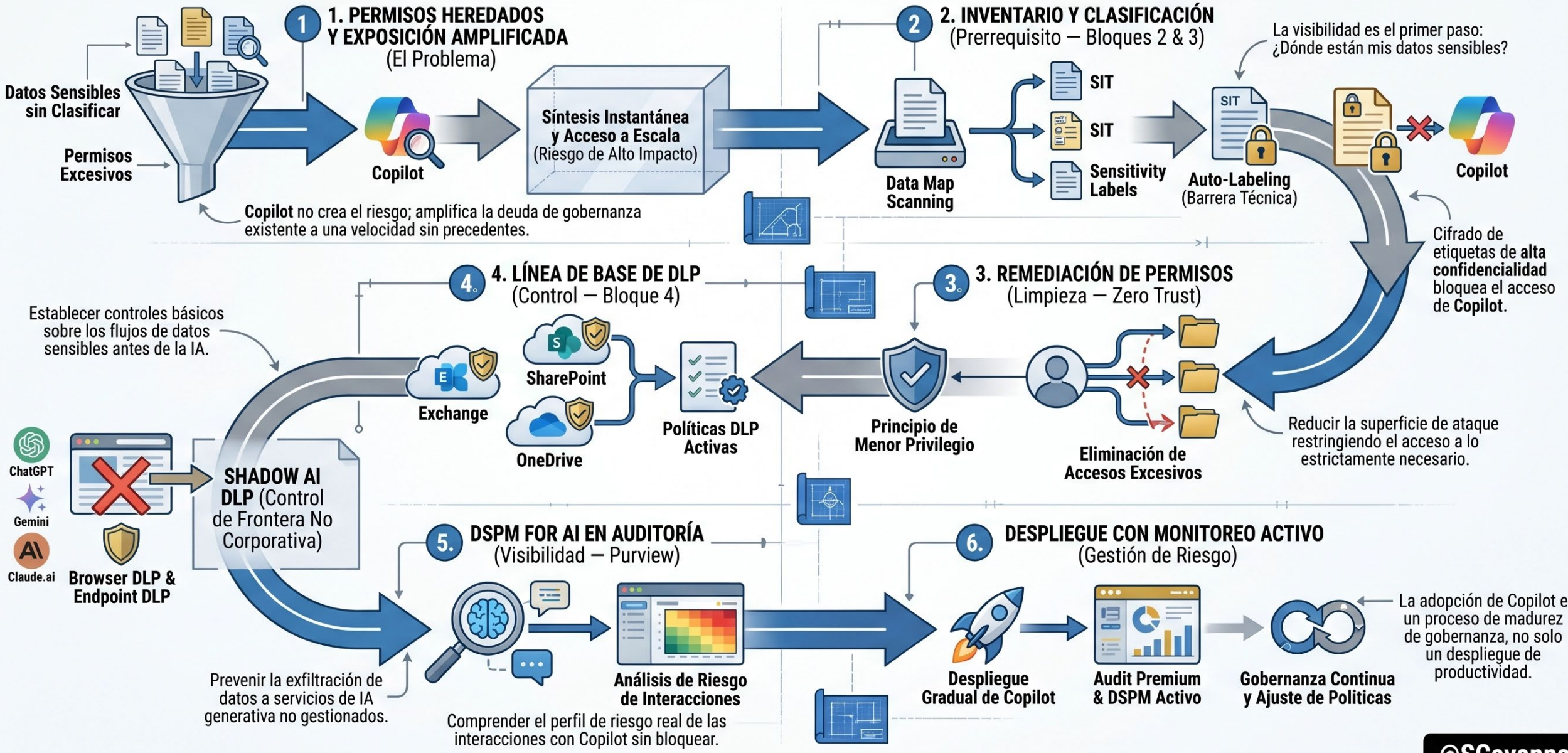
1. Explica que Copilot no amplía permisos, pero convierte todo acceso teórico en acceso real, rápido y sintetizado. Destaca la deuda histórica de permisos en SharePoint, OneDrive, Exchange y Teams. Propone reducir esa superficie mediante etiquetas de sensibilidad con cifrado, clasificación automática y un programa estructurado de remediación de permisos.

2. Detalla DSPM for AI en Purview como radar del riesgo de datos en las respuestas de Copilot y otras IA internas. Identifica tipos de información sensibles, usuarios y sitios más expuestos y prompts inseguros. Opera primero en auditoría. Se diferencia de los paneles de uso de Copilot y se orienta a equipos de seguridad.

3. Presenta Shadow AI DLP, basado en Browser DLP y Endpoint DLP, para bloquear exfiltración hacia servicios públicos de IA. Expone un roadmap en cinco etapas apoyado en Data Map, clasificación automática y DLP. Relaciona este viaje de madurez con arquitecturas de Zero Trust, requisitos regulatorios y revisión continua de capacidades.

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**



Notas

Microsoft Security | MCSA CSU

Microsoft Customer Success Unit - Mexico, Centro & Sud America - Cybersecurity & Data protection.

Seguridad de redes y sistemas informáticos · 85 seguidores · 501-1 mil empleados

https://www.linkedin.com/company/microsoft-mcsa-csu-security/