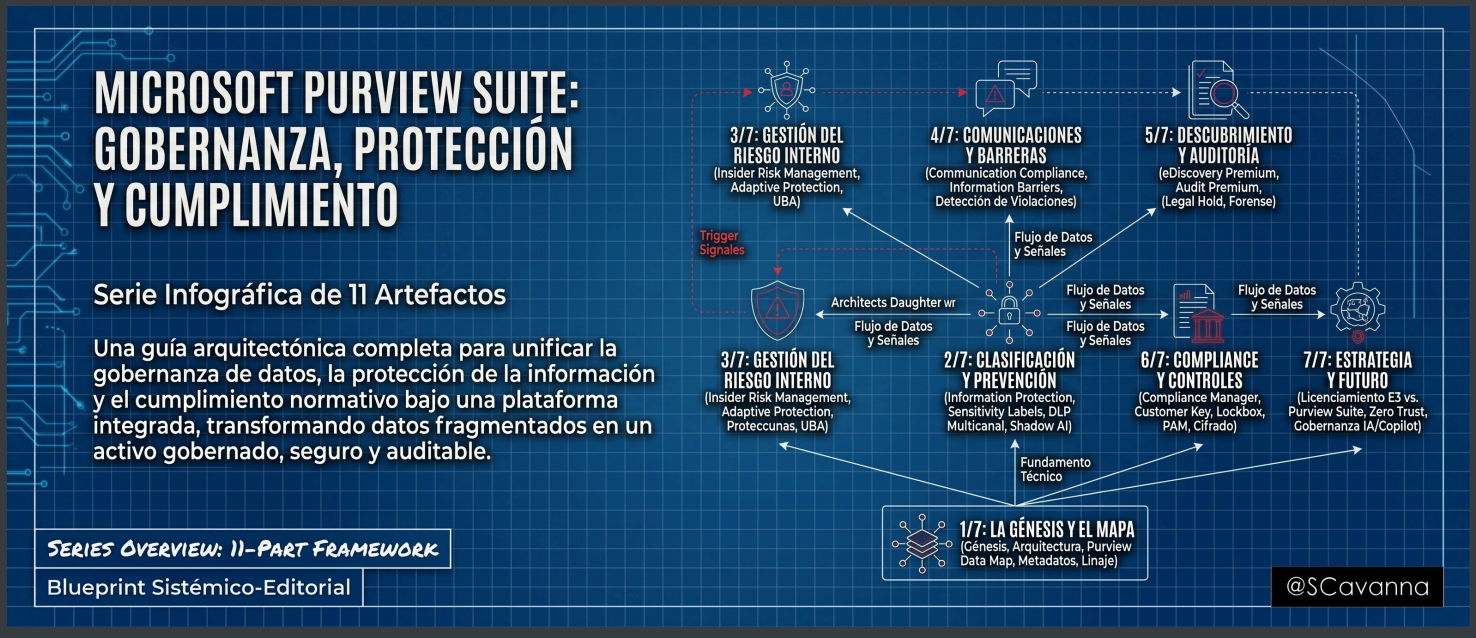
# MS Purview Suite - M365E5 Data Security: Compilado_Ampliado

**Serie de infografias que resumen y sintetizan las capacidades de Data Security ofrecidas por Microsoft Purview Suite / Microsoft Purview en M365E5**

e02v01 - 26 Abril 2026 / https://www.linkedin.com/company/microsoft-mcsa-csu-security/

Santiago Cavanna >> https://www.linkedin.com/in/scavanna/




**Entidades clave**

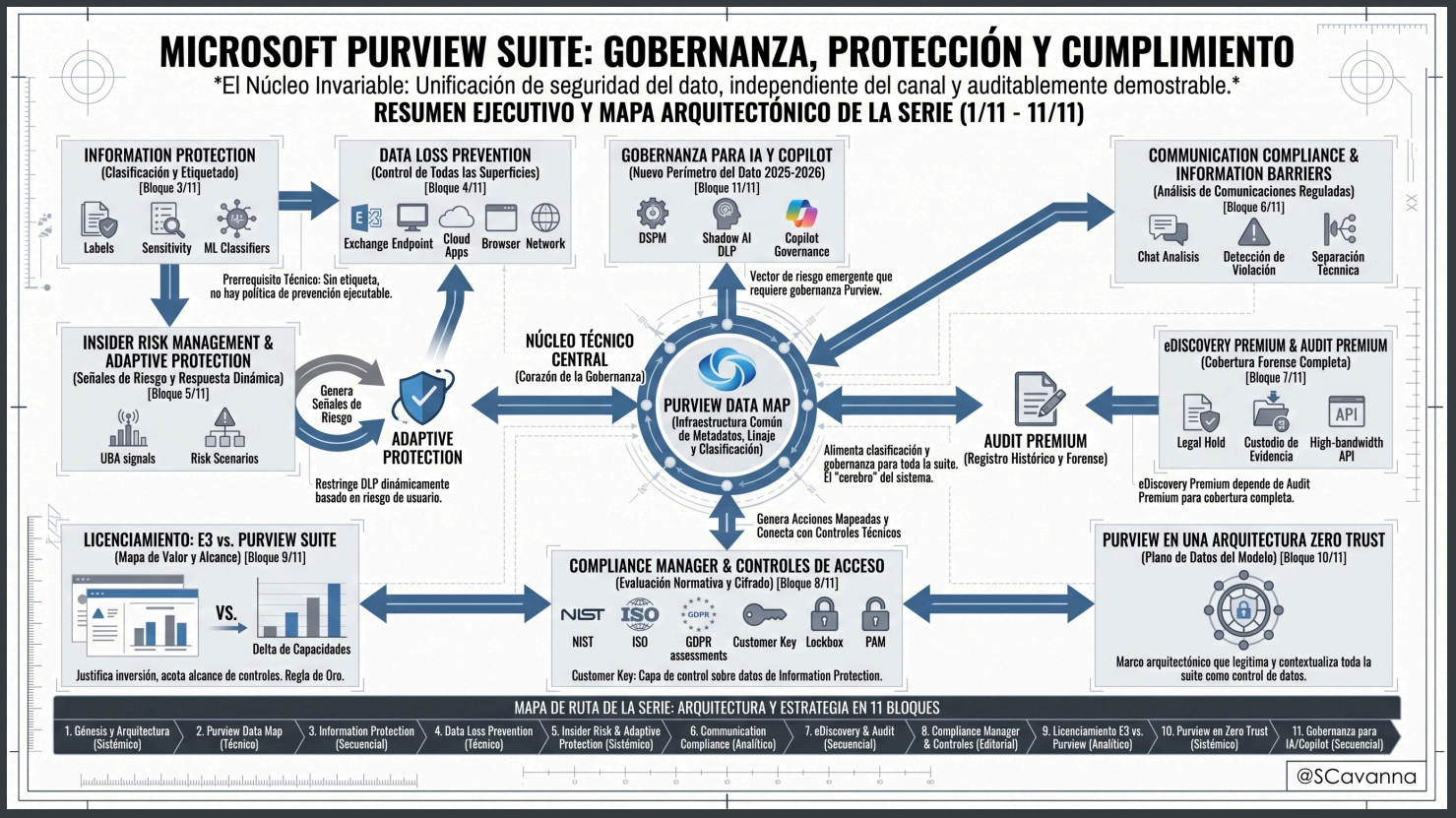
- Microsoft Purview (plataforma unificada)
- Purview Suite / M365 E5
- Purview Data Map
- Information Protection
- Sensitivity Labels
- DLP (todas las superficies)

- Insider Risk Management
- Adaptive Protection
- Communication Compliance
- eDiscovery Premium
- Audit Premium
- Compliance Manager
- Customer Key / Customer Lockbox
- Privileged Access Management (PAM)
- Records Management
- Zero Trust Architecture
- Copilot / AI Governance
- DSPM (Data Security Posture Management)

**Mapa de relaciones**

- Purview Data Map → infraestructura común que alimenta clasificación, linaje y gobernanza de todos los demás módulos.
- Information Protection → prerequisito técnico de DLP (sin etiqueta no hay política de prevención ejecutable).
- Insider Risk Management → genera señales de riesgo → alimenta Adaptive Protection → restringe DLP de forma dinámica.
- Compliance Manager → evalúa el estado normativo → genera acciones mapeadas → conecta con controles técnicos de toda la suite.
- eDiscovery Premium → depende de Audit Premium para ofrecer cobertura forense completa.
- Customer Key → añade una capa de control sobre los datos que maneja Information Protection.
- Zero Trust → marco arquitectónico que legitima y contextualiza toda la suite como control de datos.
- Copilot y otros servicios de IA → vector de riesgo emergente que requiere gobernanza con Purview (DSPM, Shadow AI DLP).

---




## 1.3 Índice de bloques

| # | Título sugerido | Arquetipo tentativo | Descripción en una línea |
|---|---|---|---|
| 1/11 | Génesis y arquitectura conceptual de Microsoft Purview | Sistémico / relacional | Unificación de 2022, tres pilares funcionales y fundamento estratégico de la plataforma |
| 2/11 | Purview Data Map: corazón técnico de la gobernanza | Técnico / despiece | Infraestructura de metadatos, linaje, clasificación multicloud y modelo de capacidad |
| 3/11 | Information Protection: clasificación y etiquetado | Secuencial / narrativo | Sensitivity Labels, SIT, EDM, clasificadores de ML y alcance del etiquetado automático |
| 4/11 | Data Loss Prevention: control de todas las superficies | Técnico / despiece | DLP por canal (Exchange, endpoint, Cloud Apps, navegador, red), EDM y protección ante Shadow AI |
| 5/11 | Insider Risk Management y Adaptive Protection | Sistémico / relacional | UBA multiseñal, escenarios de riesgo e integración dinámica entre IRM y DLP |

| # | Título sugerido | Arquetipo tentativo | Descripción en una línea |
|---|---|---|---|
| 6/11 | Communication Compliance e Information Barriers | Analítico / jerárquico | Análisis de comunicaciones reguladas, detección de violaciones y separación técnica |
| 7/11 | eDiscovery Premium y Audit Premium | Secuencial / narrativo | Legal hold, custodia de evidencia, retención forense y API de alto ancho de banda |
| 8/11 | Compliance Manager y controles de cifrado y acceso | Editorial / modular | Evaluaciones normativas (NIST, ISO, GDPR), Customer Key, Customer Lockbox y PAM |
| 9/11 | Licenciamiento: E3 frente a Purview Suite, mapa de valor | Analítico / jerárquico | Diferencias de capacidad por nivel, complementos, reglas de decisión y criterios de actualización |
| 10/11 | Purview en una arquitectura Zero Trust | Sistémico / relacional | Cómo los controles de Purview operan como plano de datos dentro del modelo Zero Trust |
| 11/11 | Gobernanza para IA y Copilot, el nuevo perímetro del dato | Secuencial / narrativo | DSPM, Shadow AI DLP, gobierno de datos para Copilot y vectores de riesgo emergentes 2025–2026 |

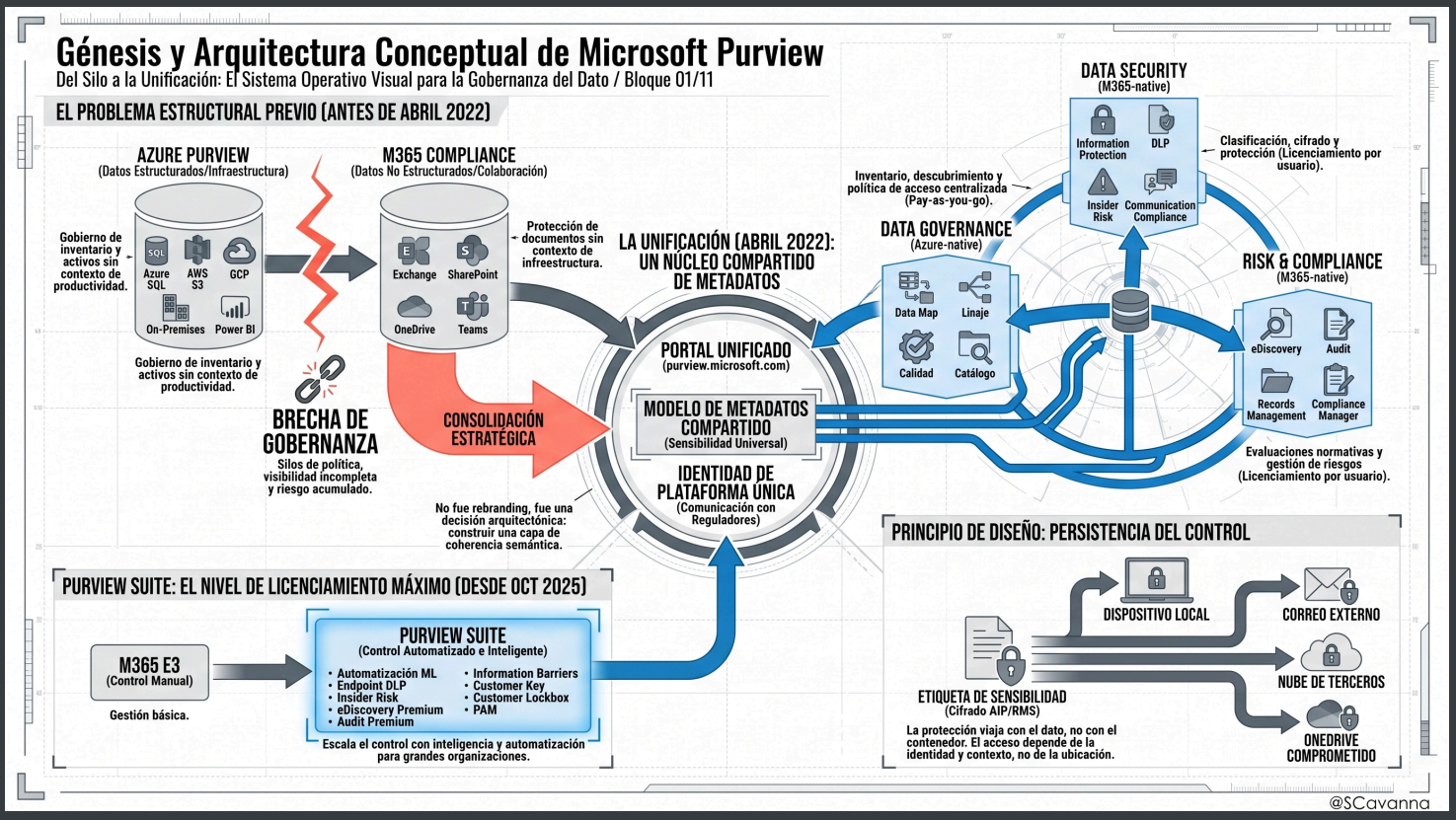
# 01/ - Génesis y arquitectura conceptual de Microsoft Purview

## 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

## Conceptos clave

| Concepto | Explicación / Data |
| --- | --- |
| **El problema estructural previo** | Antes de abril de 2022 coexistían dos plataformas sin integración técnica real: Azure Purview, lanzado en 2021, gestionaba el inventario y la gobernanza de activos de datos estructurados y semiestructurados en Azure, AWS, GCP y fuentes on-premises. Microsoft 365 Compliance, por su parte, gestionaba la protección de datos no estructurados en el ecosistema de productividad de Exchange, SharePoint, OneDrive y Teams. Una etiqueta de sensibilidad aplicada a un documento en SharePoint no era reconocida ni respetada cuando ese mismo documento o sus datos derivados llegaban a Azure SQL, a un pipeline de Azure Data Factory o a una herramienta analítica como Power BI conectada a Synapse. La ausencia de puente entre ambas plataformas hacía que la gobernanza del dato fuera, en el mejor caso, parcial: se protegía |

| Concepto | Explicación / Data |
| --- | --- |
| | el dato en su contexto de colaboración o en su contexto de infraestructura, pero rara vez en ambos de forma coordinada. |
| **La unificación de abril de 2022** | Microsoft consolidó Azure Purview y Microsoft 365 Compliance bajo la marca Microsoft Purview, con tres cambios técnicos y operativos fundamentales: (1) un portal de administración unificado, purview.microsoft.com, que centraliza la gestión de todos los componentes; (2) un modelo de metadatos compartido que permite que una sensitivity label asignada en Microsoft 365 sea reconocida en el Data Map de Azure y viceversa; (3) una única identidad de plataforma para el gobierno del dato que simplifica la comunicación con reguladores, auditores y juntas directivas. La unificación no eliminó las diferencias arquitectónicas entre componentes Azure-native y M365-native, que mantienen modelos de licenciamiento y administración distintos, pero creó una capa de coherencia semántica que antes no existía. |
| **Los tres pilares funcionales** | La familia Purview se organiza en tres grandes áreas operativas que comparten el Purview Data Map como infraestructura común de metadatos: **Data Governance** (inventario del patrimonio de datos, linaje, descubrimiento, calidad y política de acceso centralizada, con componentes predominantemente Azure-native y modelo pay-as-you-go); **Data Security** (clasificación, etiquetado, protección cifrada, DLP, Insider Risk Management, Communication Compliance, con componentes M365-native licenciados por usuario); **Risk & Compliance** (evaluaciones normativas, eDiscovery, Auditoría, Information Barriers y Records Management, también M365-native). La distinción entre pilares no es solo funcional, también define qué equipo administra cada componente, bajo qué modelo de licenciamiento y con qué consola. En organizaciones donde el equipo de Data y Analytics y el equipo de Seguridad y Compliance operan de forma separada, esta distinción es crítica para diseñar el modelo operativo. |

| Concepto | Explicación / Data |
| --- | --- |
| **Purview Suite como nivel de licenciamiento máximo** | A partir del 1 de octubre de 2025, el paquete de licencias avanzado previamente denominado Microsoft 365 E5 Compliance pasa a llamarse Microsoft Purview Suite. El cambio es de nomenclatura y posicionamiento, sin modificación de capacidades, SKUs ni precios. Purview Suite representa el nivel máximo de capacidades de los pilares de Data Security y Risk & Compliance: incluye automatización con machine learning, Endpoint DLP, Insider Risk Management, Communication Compliance, eDiscovery Premium, Audit Premium con un año de retención, Information Barriers, Customer Key, Customer Lockbox y Privileged Access Management. La diferencia con Microsoft 365 E3 no es solo el número de herramientas, sino el modo de operación: E3 provee control principalmente manual, mientras que Purview Suite aporta inteligencia y automatización para escalar ese control en organizaciones con miles de usuarios y millones de documentos. |
| **Persistencia del control como principio de diseño** | El principio arquitectónico central de Purview es que la protección viaja con el dato, no con el contenedor. Un documento cifrado mediante una sensitivity label de "Altamente confidencial" mantiene sus restricciones de acceso si se descarga a un dispositivo local, si se adjunta a un correo y se envía a un destinatario externo, si se sube a un repositorio de terceros o si se sincroniza en el OneDrive de un usuario comprometido. El cifrado AIP o RMS asociado a la etiqueta implementa este principio: la clave de descifrado solo se entrega si la identidad del solicitante, su dispositivo y su contexto de acceso cumplen las condiciones definidas en la política. Esta persistencia diferencia a Purview de soluciones de seguridad perimetral o basadas en contenedores, en las que la protección desaparece cuando el dato abandona el perímetro controlado. |

## Notas de soporte

### Convergencia entre equipos de datos y seguridad

La unificación bajo Purview en 2022 refleja una tendencia de la industria: los equipos de seguridad y los equipos de datos convergen en torno al mismo problema, gobernar quién accede a qué información, con qué propósito y bajo qué condiciones.
Los equipos de datos priorizan inventario, linaje y descubrimiento.
Los equipos de seguridad priorizan clasificación, control y auditoría.

Purview busca resolver ambas necesidades con una plataforma unificada, evitando que las organizaciones mantengan dos stacks paralelos sin integración.

### Diferencias operativas entre componentes Azure-native y M365-native

La distinción entre componentes Azure-native y M365-native tiene implicaciones directas en el modelo administrativo:

- Los componentes Azure-native, como Data Map, Unified Catalog, Data Policy y Data Sharing, se configuran y administran desde una cuenta de Microsoft Purview en el portal de Azure, bajo un modelo pay-as-you-go medido en unidades de capacidad.
- Los componentes M365-native, como Information Protection, DLP, Insider Risk y eDiscovery, se administran desde el portal de Purview en purview.microsoft.com, con licenciamiento por usuario.

En organizaciones donde los equipos de Cloud e Infraestructura y los equipos de Security y Compliance son distintos, esta separación de planos de administración define responsabilidades, permisos y presupuestos de forma diferenciada.

### Portal unificado y modelo RBAC

El portal unificado purview.microsoft.com consolidó en 2023 funcionalidades que antes estaban distribuidas entre compliance.microsoft.com y el portal de Azure Purview.

La migración al portal unificado no fue solo estética: introdujo un modelo de control de acceso basado en roles unificado que permite asignar permisos granulares sobre componentes específicos de Purview sin conceder acceso administrativo global.

Esto resulta relevante para organizaciones que necesitan que los equipos de Legal, Recursos Humanos, Data Governance y Seguridad trabajen en la misma plataforma con alcances de acceso diferenciados.

### Cambio de nombre a Purview Suite

El cambio de nombre de Microsoft 365 E5 Compliance a Purview Suite fue anunciado por Microsoft en septiembre de 2025 y entró en vigor el 1 de octubre de 2025.

Para organizaciones con contratos Enterprise Agreement o Microsoft Customer Agreement vigentes, el cambio de nombre no requiere acciones contractuales adicionales.

---

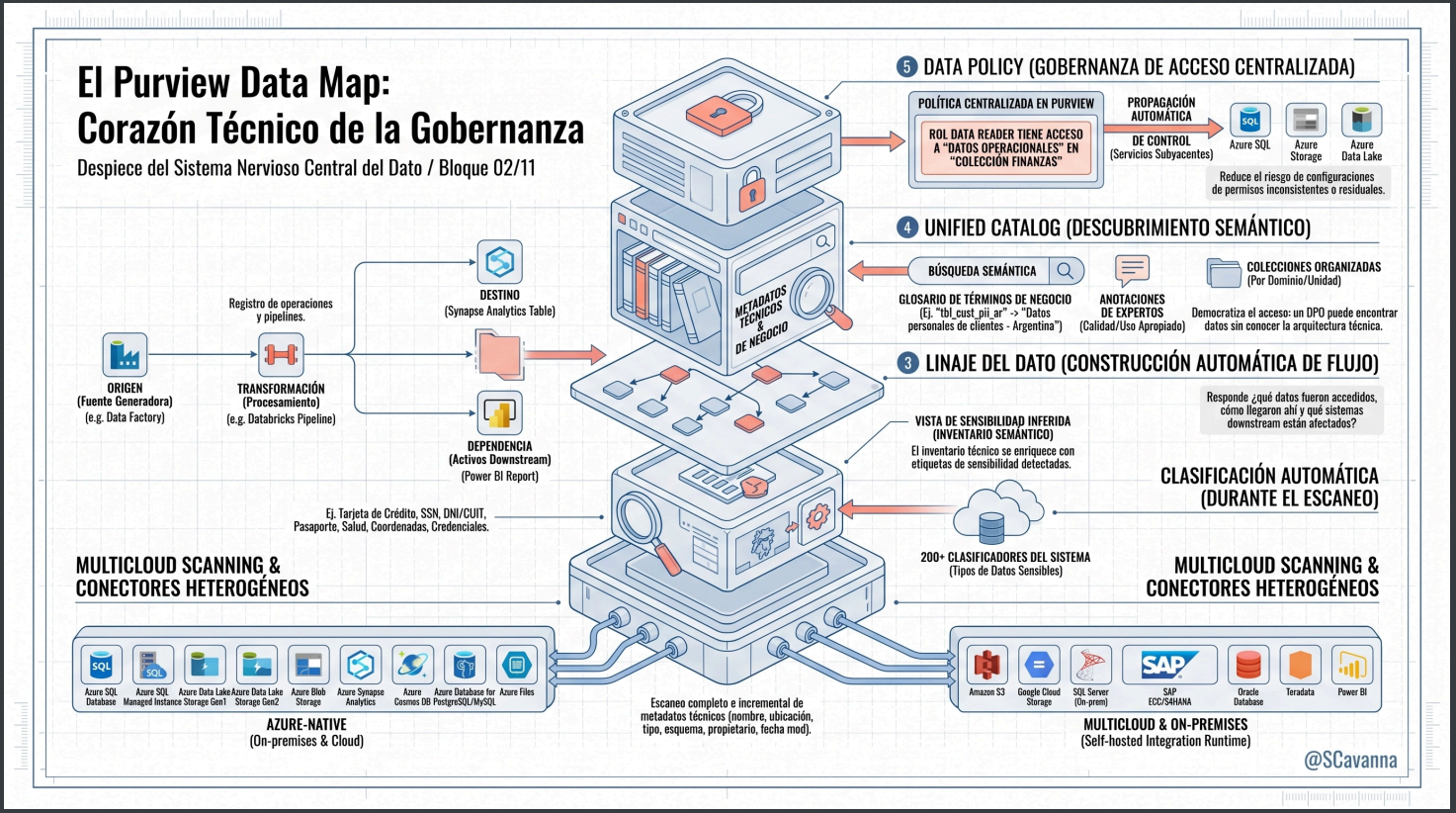
# 02/ - Purview Data Map: corazón técnico de la gobernanza

## 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.




# Bloque 2/11: El Purview Data Map, corazón técnico de la gobernanza

## Nivel 2: Conceptos clave

| Concepto | Explicación / Data |
|---|---|
| **Escaneo multicloud y multiconector** | El Data Map conecta con fuentes de datos heterogéneas mediante conectores nativos. En Azure incluye Azure SQL Database, Azure SQL Managed Instance, Azure Data Lake Storage Gen1 y Gen2, Azure Blob Storage, Azure Synapse Analytics, Azure Cosmos DB, Azure Database for PostgreSQL/MySQL y Azure Files. Fuera de Azure incluye Amazon S3, Google Cloud Storage, SQL Server on-premises, SAP ECC y SAP S/4HANA, Oracle Database, Teradata, Power BI, y otros a través del runtime de integración autohospedado (Self-hosted Integration Runtime). Cada escaneo puede ser completo o incremental, y programarse en ventanas de tiempo definidas para minimizar impacto en producción. El resultado es un conjunto estructurado de metadatos técnicos: nombre del activo, ubicación, tipo de |

| Concepto | Explicación / Data |
| --- | --- |
| | dato, esquema (para datos estructurados), propietario técnico inferido y última fecha de modificación. Este inventario es la base sobre la cual operan las demás capacidades de Purview. |
| **Clasificación automática durante el escaneo** | De forma simultánea a la captura de metadatos técnicos, el Data Map aplica clasificadores predefinidos sobre el contenido de los activos escaneados. Microsoft provee más de 200 clasificadores del sistema que cubren tipos de datos sensibles en múltiples jurisdicciones: números de tarjeta de crédito, números de seguridad social (USA), DNI/CUIT/CUIL (Argentina), números de pasaporte, datos de salud, coordenadas geográficas, credenciales de autenticación, entre otros. El resultado es un inventario también semántico: cada activo queda etiquetado con los tipos de información sensible detectados en su contenido, generando una vista de sensibilidad inferida sin intervención manual. Estos metadatos de sensibilidad son consumibles por las políticas de Information Protection y DLP, unificando el pilar de Data Governance (Azure-native) con el de Data Security (M365-native). |
| **Linaje del dato (Data Lineage)** | El Data Map construye automáticamente el grafo de linaje para activos procesados a través de Azure Data Factory, Azure Synapse Analytics, Azure Databricks y Microsoft Fabric. El linaje registra el origen del dato (fuentes que lo generaron), las transformaciones aplicadas (pipelines y operaciones), los destinos donde se escribe (tablas o sistemas consumidores) y las dependencias entre activos (reportes o modelos que dependen de qué tablas). Para seguridad y cumplimiento, el linaje permite responder preguntas típicas de auditoría de privacidad (dónde están los datos personales de ciertos colectivos, qué sistemas los procesan, quién los consume) y análisis de impacto de brecha (qué datos fueron accedidos, cómo llegaron allí, qué sistemas downstream están afectados). La documentación del linaje es un insumo directo para los registros de actividades de tratamiento requeridos por el GDPR (Art. 30) y normas equivalentes. |

| Concepto | Explicación / Data |
| --- | --- |
| **Unified Catalog: descubrimiento semántico** | Sobre el Data Map opera el Unified Catalog, una capa de descubrimiento que transforma el inventario técnico en un recurso navegable para usuarios de negocio y técnicos. El catálogo ofrece búsqueda semántica sobre metadatos técnicos y de negocio, un glosario de términos de negocio configurable (por ejemplo, mapear el término técnico "tbl_cust_pii_ar" al término de negocio "Datos personales de clientes - Argentina"), anotaciones de expertos de dominio sobre calidad y uso apropiado de cada activo, y colecciones organizadas por dominio de negocio o unidad organizacional. El catálogo democratiza el acceso al inventario: un Data Privacy Officer puede encontrar todos los activos que contienen datos personales de ciudadanos argentinos sin conocer la arquitectura técnica subyacente ni tener acceso directo a los sistemas de producción. |
| **Data Policy: gobernanza de acceso centralizada** | Data Policy permite definir y aplicar políticas de acceso sobre fuentes de datos en Azure (Azure SQL, Azure Storage, Azure Data Lake) directamente desde el portal de Purview, sin gestionar permisos servicio por servicio. En el modelo tradicional, un administrador debía entrar a cada base de datos o cuenta de almacenamiento para otorgar o revocar permisos. Con Data Policy se define una política centralizada en Purview (por ejemplo, "el rol Data Reader tiene acceso a todos los activos clasificados como Datos Operacionales en la colección Finanzas") y la plataforma propaga y aplica ese control en los servicios subyacentes de forma automática. Esto reduce de manera significativa el riesgo de configuraciones de permisos inconsistentes o residuales, una de las causas más frecuentes de sobreexposición de datos en entornos cloud. |

## Nivel 3: Notas de soporte

El modelo de escala del Data Map se basa en Capacity Units (CU). Cada CU proporciona capacidad de operación para el mapa y añade almacenamiento de metadatos. El modelo de pago por uso implica que el costo escala con el tamaño del patrimonio de datos gestionado, no con el número de usuarios. En organizaciones grandes, con datos distribuidos en múltiples regiones y cuentas de nube, el diseño de la arquitectura del Data Map (número de cuentas Purview, organización en colecciones, estrategia de escaneo incremental frente a completo) impacta directamente en el costo operacional y en la calidad y latencia del inventario.

Data Estate Insights es el componente analítico que opera sobre el Data Map y ofrece una vista ejecutiva del estado del patrimonio de datos: porcentaje de activos clasificados frente a sin clasificar, distribución de tipos de información sensible por fuente, tendencias de crecimiento del patrimonio y brechas de cobertura de escaneo. Es el insumo principal para los informes de postura de gobernanza de datos que un CISO o CDO presenta a la junta directiva o a reguladores.

Data Sharing es una capacidad del Data Map que permite compartir activos de datos con socios externos o con otras unidades de negocio internas sin duplicar el almacenamiento físico. El receptor accede a los datos en el origen (por ejemplo, Azure Data Lake) con permisos controlados y auditados, mientras que la organización propietaria mantiene el control completo para revocar el acceso en cualquier momento. Esto es clave en ecosistemas de datos colaborativos (consorcios, joint ventures, intercambio entre filiales) donde privacidad y soberanía del dato son requisitos críticos.

La integración entre el Data Map y los componentes M365-native de Purview se articula mediante sensitivity labels. Las etiquetas definidas en el portal de Purview (purview.microsoft.com) se aplican tanto a documentos en M365 como a activos catalogados en el Data Map, creando una taxonomía de sensibilidad unificada que atraviesa ambos entornos. Esta taxonomía común es el puente técnico central que persiguió la unificación de Purview iniciada en 2022.

### Conexiones externas

El Data Map es el prerrequisito técnico que habilita la clasificación automática descrita en el Bloque 3/11 (Information Protection). Los metadatos de sensibilidad generados durante el escaneo son consumidos por las políticas DLP del Bloque 4/11. Las evaluaciones normativas de Compliance Manager (Bloque 8/11) utilizan los insights del Data Map para evaluar el estado de clasificación y protección del patrimonio de datos. El linaje del dato generado por el Data Map es el insumo forense clave para las investigaciones de eDiscovery Premium del Bloque 7/11.

---

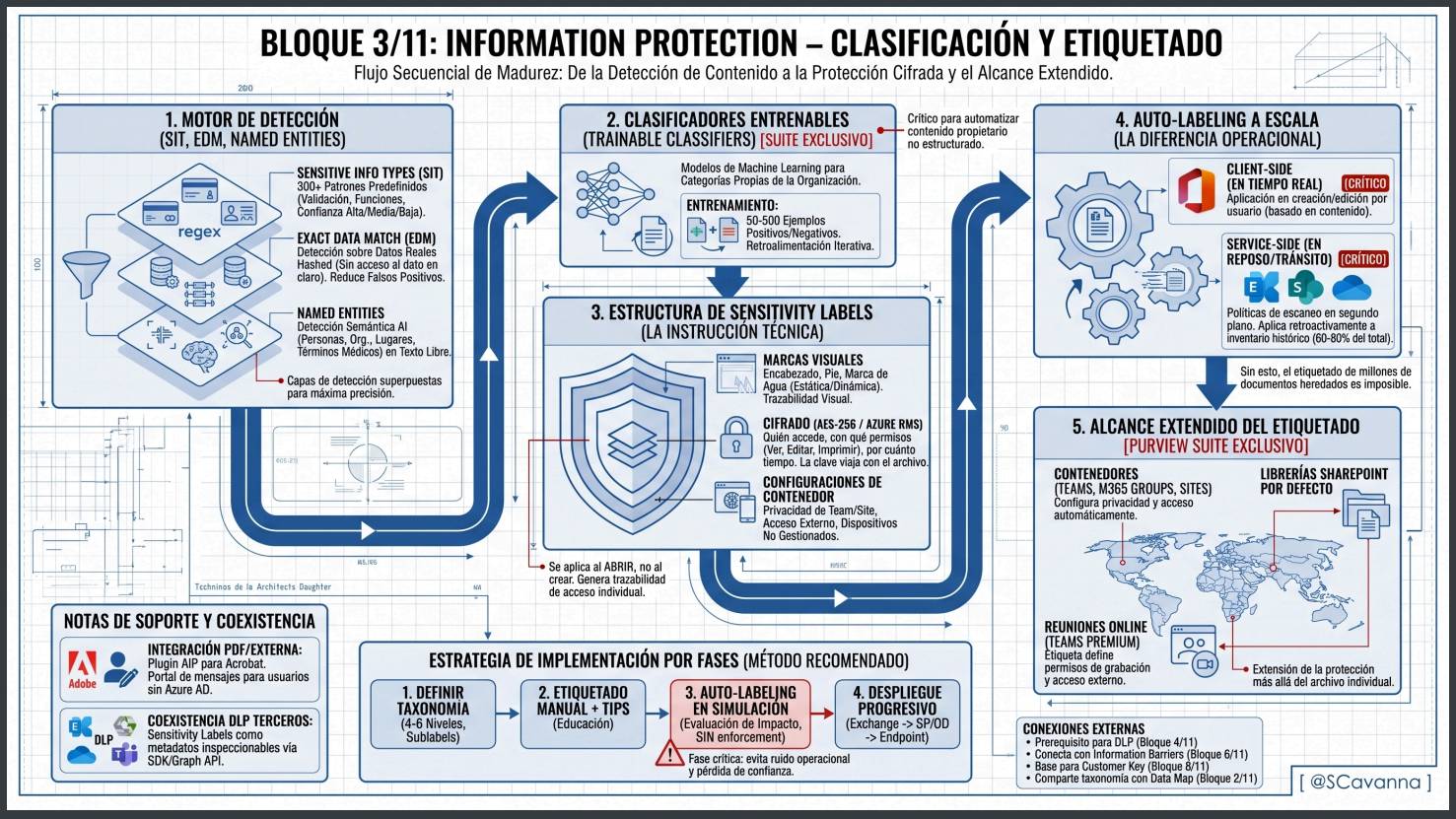
# 03/ - Information Protection: clasificación y etiquetado

## 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 controles 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

## Nivel 2: Conceptos clave

| Concepto | Explicación / Data |
|---|---|
| **Motor de detección: SIT, EDM y Named Entities** | El motor de detección de contenido sensible combina tres mecanismos. Los **Sensitive Information Types (SIT)** predefinidos son más de 300 patrones basados en expresiones regulares y funciones de validación que cubren, entre otros, números de tarjeta de crédito, identificadores nacionales de múltiples países, credenciales de autenticación, datos de salud, información financiera regulada y secretos de servicios cloud. Cada SIT tiene niveles de confianza configurables (alta, media, baja) y puede combinarse en condiciones compuestas para reducir falsos positivos. El **Exact Data Match (EDM)** se centra en datos reales de la organización: en lugar de detectar cualquier número con formato de DNI, detecta solo los DNIs presentes en una base de datos corporativa, usando coincidencia sobre valores hash salteados para que |

| Concepto | Explicación / Data |
| --- | --- |
| | Microsoft no reciba los datos en claro. Esto permite políticas de alto valor, por ejemplo sobre padrones de millones de clientes, con falsos positivos mínimos. Las **Named Entities** son clasificadores que identifican nombres de personas, organizaciones, ubicaciones y términos médicos en texto libre, incluso cuando no siguen un patrón estructurado, aportando una capa semántica que complementa a SIT y EDM. |
| **Clasificadores entrenables (Trainable Classifiers)** | Los clasificadores entrenables son modelos de machine learning que aprenden categorías de contenido específicas de la organización a partir de ejemplos. Microsoft proporciona modelos preconstruidos para casos habituales como currículums, estados financieros, código fuente, contenido de recursos humanos, acoso laboral y discriminación. Además, cada organización puede definir clasificadores personalizados para categorías propias, por ejemplo contratos de distribución, informes de due diligence, comunicaciones de trading o historiales clínicos en formato no estructurado. El entrenamiento inicial requiere en torno a 50 a 500 documentos positivos (que pertenecen a la categoría) y un conjunto de negativos, seguido de ciclos de retroalimentación para refinar precisión y cobertura. Estos clasificadores están disponibles solo en Purview Suite, lo que resulta clave porque sin ellos la clasificación automática del contenido propietario no estructurado, que suele concentrar el mayor valor informacional, resulta prácticamente inalcanzable. |
| **Sensitivity labels: estructura y capacidades** | Una sensitivity label es un objeto de configuración que agrupa tres tipos de controles. Primero, **marcas visuales**: encabezados, pies de página y marcas de agua, estáticas o dinámicas, que pueden incorporar datos del usuario y marcas temporales. Segundo, **cifrado**: si está activado, define quién puede descifrar el archivo, qué permisos tiene (solo lectura, edición, reenvío, impresión) y durante cuánto tiempo, incluyendo expiración o revocación de acceso. Tercero, **configuración de contenedores**: privacidad de Teams y Sites, reglas de acceso externo y restricciones para dispositivos no gestionados. Las marcas de agua dinámicas, disponibles en Purview Suite, insertan automáticamente el nombre del usuario y la fecha de acceso en el momento de apertura del documento, creando trazabilidad visual independientemente del flujo previo del archivo. El cifrado se basa en Azure Information Protection y Azure Rights Management: el contenido se cifra con AES 256 y la clave de descifrado solo se concede si la identidad, el dispositivo y el contexto de acceso cumplen la política definida. |

| Concepto | Explicación / Data |
| --- | --- |
| **Auto labeling: la diferencia de escala** | El etiquetado automático es lo que permite pasar de una clasificación manual limitada a un esquema operativo para decenas de miles o millones de documentos. Existen dos modalidades. El **auto labeling del lado del cliente** aplica etiquetas en las aplicaciones de Office cuando el usuario crea o modifica un documento, según el contenido detectado. El **auto labeling del lado del servicio** se configura en el portal de Purview y escanea contenido en reposo en SharePoint y OneDrive, y en tránsito en Exchange, aplicando etiquetas sin intervención del usuario. Combinado con clasificadores entrenables, el motor del lado del servicio puede etiquetar retroactivamente grandes repositorios heredados donde la mayoría de los documentos carece de clasificación previa, un porcentaje que suele situarse entre el 60 y el 80 por ciento del inventario. Sin este enfoque automatizado, etiquetar repositorios de millones de documentos resulta inviable en términos operativos. |
| **Alcance extendido del etiquetado (Purview Suite exclusivo)** | Purview Suite amplía el alcance de las sensitivity labels más allá del archivo individual. El **etiquetado de contenedores** aplica una etiqueta a un Team, un Microsoft 365 Group o un sitio de SharePoint, de forma que la configuración de privacidad, el acceso externo y las restricciones a dispositivos no gestionados se derivan automáticamente de esa etiqueta. El **etiquetado por defecto de bibliotecas de SharePoint** garantiza que todos los documentos cargados en determinadas bibliotecas reciban una etiqueta preconfigurada, cerrando la brecha de contenido nuevo sin clasificar. El **etiquetado de reuniones de Teams**, integrado con Teams Premium, permite clasificar reuniones con una sensitivity label que controla qué grabaciones se permiten, qué restricciones se aplican a participantes externos y si se habilita o no la transcripción automática. Las **marcas de agua dinámicas** en documentos etiquetados aportan trazabilidad de acceso por usuario en el momento de apertura. |

---

# Nivel 3: Notas de soporte

### Fases recomendadas de implementación

En organizaciones sin una cultura previa de clasificación, la adopción de Information Protection requiere un enfoque por etapas:

1. **Definir la taxonomía de etiquetas**

Normalmente se recomienda entre 4 y 6 niveles, desde Público hasta Altamente confidencial o Restringido, con subetiquetas para ámbitos específicos como Legal o Recursos Humanos. Es clave mapear esta taxonomía a los requisitos normativos y contractuales de la organización.

2. **Desplegar etiquetado manual con ayudas de política**
   Se habilitan las etiquetas para que el usuario seleccione manualmente y se configuran consejos de política (policy tips) que orientan al usuario cuando selecciona una etiqueta inadecuada o cuando se detecta contenido sensible sin etiquetar. Esta fase se centra en educación del usuario y ajuste fino de la taxonomía.
3. **Activar auto labeling en modo simulación**
   Antes del enforcement, las políticas de auto labeling se ejecutan en modo simulación. Esto permite observar qué documentos se etiquetarían, revisar estadísticas de impacto e identificar patrones de falsos positivos o falsos negativos sin modificar todavía el contenido.
4. **Pasar a auto labeling en enforcement progresivo**
   Una vez calibradas las políticas, se activa el enforcement de forma gradual, por tipo de carga de trabajo: primero sobre Exchange (correo en tránsito), después sobre SharePoint y OneDrive (contenido en reposo) y finalmente sobre dispositivos endpoint. Esta progresión limita el riesgo de interrupciones operativas y facilita la corrección rápida de configuraciones inadecuadas.

La fase de simulación es especialmente crítica para evitar que una política excesivamente amplia etiquete como confidenciales grandes volúmenes de contenido público, lo que generaría ruido operativo, ralentización de procesos y pérdida de confianza en el esquema de clasificación.

## Integración con aplicaciones no Microsoft

La aplicación del cifrado basado en sensitivity labels a archivos y flujos de trabajo fuera del ecosistema Microsoft exige revisar compatibilidades:

- **Archivos PDF**
  El cifrado aplicado mediante AIP está soportado en Adobe Acrobat y Adobe Reader cuando se instala el complemento de Azure Information Protection. Sin este complemento, el usuario puede encontrar archivos ilegibles aunque tenga derechos de acceso teóricos.
- **Destinatarios externos sin Azure AD**
  Cuando el destinatario no pertenece a un tenant de Azure AD, el acceso a contenido cifrado se gestiona mediante el portal de mensajes cifrados de Microsoft. El usuario recibe un correo con un enlace seguro y se autentica mediante un código de verificación enviado a su propio correo o mediante un proveedor de identidad compatible. Es necesario incorporar estos flujos en los procedimientos de colaboración con terceros para evitar fricción.

### Coexistencia con soluciones DLP de terceros

Muchas organizaciones operan en escenarios de transición donde Purview Information Protection convive con sistemas DLP de fabricantes como Symantec, Forcepoint o Digital Guardian:

- Las **sensitivity labels** se exponen como metadatos accesibles por soluciones de terceros a través del cliente AIP, sus SDK y las API de Microsoft Graph.
- Esto permite que las plataformas DLP externas utilicen el nivel de sensibilidad como un atributo más en sus políticas de inspección y respuesta, por ejemplo para bloquear la exfiltración de documentos etiquetados como Confidencial o para aplicar reglas diferenciadas según la etiqueta.
- Un diseño consistente debe definir qué motor actúa como autoridad principal para la clasificación y cómo se sincronizan las decisiones de política entre Purview y las demás soluciones de seguridad de contenido.

### Conexiones con otros controles

Las sensitivity labels no solo protegen el contenido de forma aislada, sino que actúan como base para otros bloques de control:

- Son un **prerrequisito técnico para las políticas DLP** desarrolladas en el Bloque 4 ya que muchas reglas se apoyan en el nivel de sensibilidad del contenido.
- El **etiquetado de contenedores** se relaciona directamente con **Information Barriers** descrito en el Bloque 6, ya que la combinación de ambas capacidades permite segmentar equipos y repositorios en función de políticas de separación organizativa o de asesoramiento.
- El **cifrado administrado con Customer Key**, tratado en el Bloque 8, se añade como capa sobre el cifrado gestionado por las sensitivity labels, aportando control adicional sobre las claves raíz.
- El **Data Map** del Bloque 2 aprovecha la misma taxonomía de etiquetas para clasificar activos en la infraestructura de Azure, alineando la visión de riesgo entre datos en Microsoft 365 y cargas de trabajo en la nube.

---

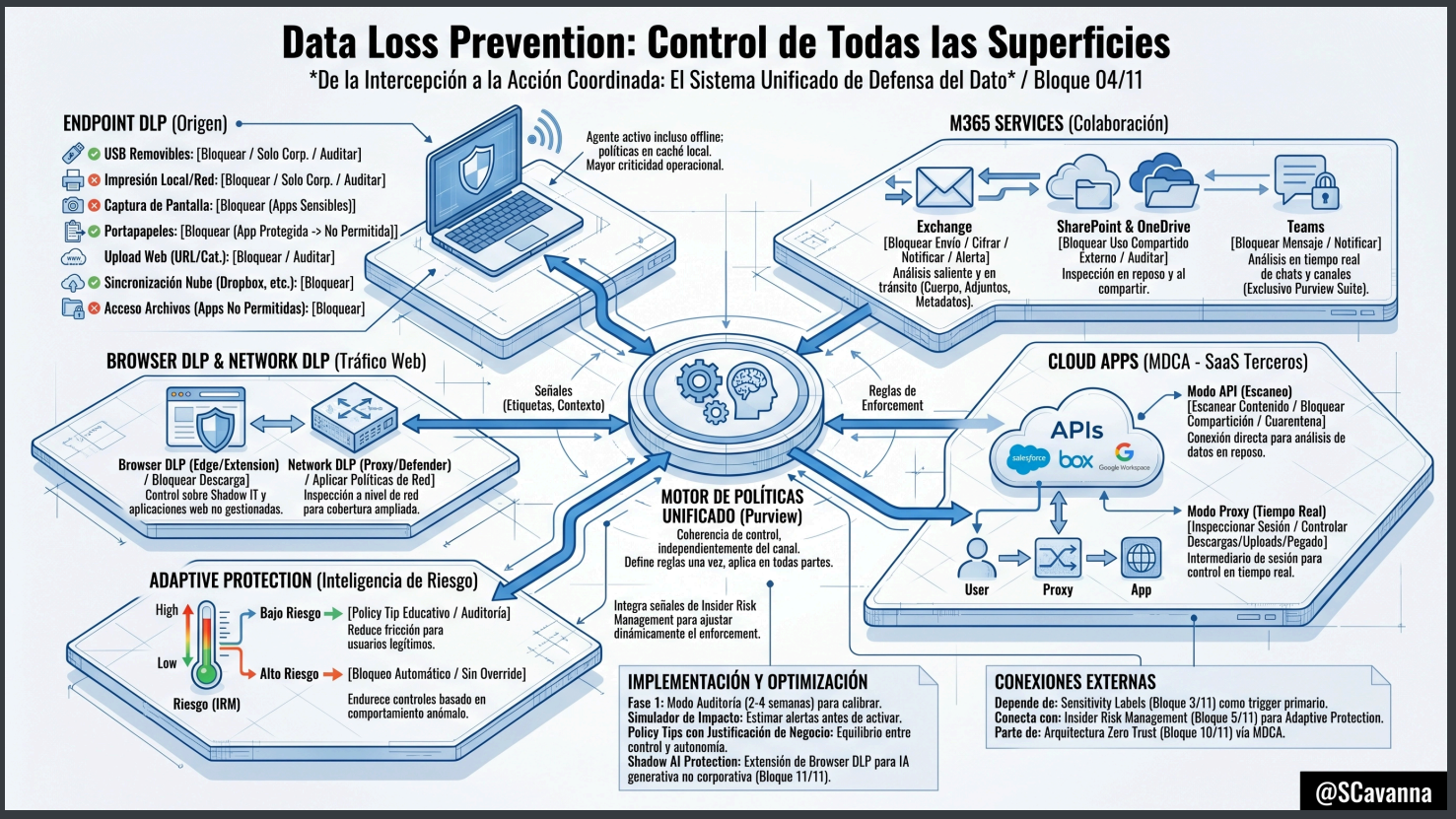
# 04/ - Data Loss Prevention: control de todas las superficies

## 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 las aplicaciones SaaS de terceros. Presenta el uso de protección adaptativa basada en riesgo y su integración con Insider Risk. Además, detalla recomendaciones 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

## Nivel 2 Conceptos Clave

| Concepto | Explicación / Data |
|---|---|
| **Endpoint DLP: el control en el origen** | Endpoint DLP extiende la aplicación de políticas DLP al dispositivo del usuario, la superficie de mayor criticidad porque la exfiltración puede ocurrir sin pasar por servicios de Microsoft. En Windows 10/11 y macOS intercepta y puede bloquear o auditar: copia a dispositivos USB extraíbles (con opción de permitir solo USB corporativos aprobados por política), impresión en impresoras locales o de red (con opción de limitar a impresoras corporativas), capturas de pantalla sobre aplicaciones que muestran contenido etiquetado como sensible, copia al portapapeles entre una aplicación protegida y una no permitida, subida de archivos a sitios web (controlado por URL o categoría de sitio), sincronización con servicios de almacenamiento en nube no corporativos (Dropbox, Box, Google Drive) y acceso a archivos sensibles desde aplicaciones no permitidas (por |

| Concepto | Explicación / Data |
| --- | --- |
| | ejemplo WinRAR o aplicaciones de comunicaciones no corporativas). El dispositivo debe estar gestionado por Microsoft Intune o unido a un dominio Active Directory para que el agente de endpoint esté activo. Las políticas se almacenan en caché local y se aplican incluso sin conexión a la red corporativa. Esta funcionalidad es exclusiva de Purview Suite. |
| **DLP en Exchange, SharePoint, OneDrive y Teams** | En los servicios de colaboración de Microsoft 365, DLP opera en varios niveles. En **Exchange**, analiza correos salientes y en tránsito antes de la entrega y puede bloquear el envío, aplicar cifrado forzado, notificar al remitente mediante un policy tip y generar alertas para revisión administrativa. El análisis abarca cuerpo del mensaje, archivos adjuntos (Office, PDF, imágenes con OCR) y metadatos. En **SharePoint y OneDrive**, DLP inspecciona archivos en reposo durante la subida y de forma periódica sobre contenido existente, además de evaluar los archivos en el momento de ser compartidos. Puede bloquear la compartición de documentos sensibles con destinatarios externos o usuarios no autorizados. En **Teams**, DLP analiza en tiempo real mensajes de chat y de canal y puede bloquear o notificar antes de la entrega cuando detecta contenido sensible. La cobertura de Teams está disponible únicamente en Purview Suite. |
| **Browser DLP y Network DLP** | **Browser DLP**, implementado mediante la extensión Microsoft Purview para Microsoft Edge (Chromium), extiende DLP al navegador. Detecta y puede bloquear la carga de archivos sensibles a sitios no autorizados, el pegado de contenido sensible (incluido texto copiado desde documentos etiquetados) en campos de texto de aplicaciones web y la descarga de contenido sensible a ubicaciones no permitidas. Opera especialmente sobre aplicaciones web no gestionadas como corporativas (Shadow IT) en navegadores gestionados, cubriendo el uso de aplicaciones SaaS personales desde dispositivos corporativos. **Network DLP** actúa en la capa de red. En lugar de controlar directamente la acción del usuario, intercepta tráfico mediante integración con un proxy corporativo o con Microsoft Defender for Endpoint Network Protection. Esto permite aplicar políticas DLP sobre tráfico HTTPS inspeccionado y proteger aplicaciones que no pueden ser controladas directamente por Endpoint DLP o Browser DLP. |

| Concepto | Explicación / Data |
| --- | --- |
| **DLP en Cloud Apps (MDCA): control de SaaS de terceros** | Purview Suite incorpora Microsoft Defender for Cloud Apps (MDCA), que extiende las políticas DLP a aplicaciones SaaS de terceros mediante dos modos complementarios. En **modo API**, MDCA se conecta a las APIs de administración de servicios como Salesforce, ServiceNow, Box, Dropbox, GitHub o Google Workspace para escanear el contenido almacenado y aplicar acciones de remediación sobre datos sensibles (bloqueo de compartición, cuarentena de archivos, notificaciones a administración). En **modo proxy (Conditional Access App Control)**, MDCA se coloca como intermediario de sesión entre el usuario y la aplicación web para inspeccionar y controlar en tiempo real las acciones del usuario dentro de la aplicación: descargas, pegado de contenido y subidas de archivos. Este enfoque es clave en organizaciones con ecosistemas SaaS heterogéneos donde los datos sensibles fluyen continuamente entre M365 y herramientas de terceros. |
| **Adaptive Protection: DLP inteligente basado en riesgo** | Adaptive Protection integra Insider Risk Management (IRM) con DLP para transformar políticas estáticas en controles dinámicos basados en el nivel de riesgo de cada usuario. En un modelo estático, todos los usuarios que intentan copiar a USB un documento etiquetado como Confidencial reciben el mismo tratamiento. Con Adaptive Protection, el tratamiento depende del perfil de riesgo calculado por IRM. Un usuario sin señales de riesgo puede recibir solo un policy tip educativo, mientras que un usuario con riesgo elevado (por ejemplo, en proceso de offboarding o con descargas anómalas) recibe bloqueo automático sin opción de override. Esto reduce fricción para usuarios legítimos de bajo riesgo y endurece los controles sobre los usuarios más críticos, optimizando seguridad y experiencia de usuario. |

## Nivel 3 Notas de Soporte

El diseño de políticas DLP efectivas exige una secuencia de implementación cuidadosa para evitar dos extremos: políticas demasiado permisivas que no detectan exfiltración real y políticas demasiado restrictivas que generan falsos positivos masivos y bloquean operaciones legítimas. La práctica recomendada es iniciar en modo solo auditoría durante 2 a 4 semanas para calibrar el volumen de alertas y ajustar umbrales de detección antes de activar el bloqueo. El portal de Purview incluye un simulador de impacto de política que estima el número de alertas que produciría una política específica sobre el contenido existente antes de habilitarla.

La funcionalidad de política con contexto (Policy Tips con justificación de negocio) permite configurar reglas DLP que, en lugar de bloquear de forma directa, solicitan al usuario una justificación escrita antes de permitir la acción. Esa justificación queda registrada en el log de auditoría y puede revisarse posteriormente. Este enfoque es útil para organizaciones que deben equilibrar control de datos y autonomía operacional de usuarios que necesitan compartir datos sensibles de forma legítima, como equipos de M&A, equipos legales o auditoría interna.

Shadow AI Protection es una extensión emergente de Browser DLP orientada al uso de herramientas de IA generativa. Detecta y puede bloquear la carga o el pegado de contenido sensible (documentos etiquetados, texto copiado de documentos protegidos) en ventanas de chat de herramientas de IA generativa no corporativas como ChatGPT, Claude.ai, Gemini o Copilot.ai personal, cuando se accede desde el navegador gestionado. Esta capacidad se conecta de forma directa con el Bloque 11/11 sobre gobernanza para IA.

**Conexiones externas:** DLP depende del Bloque 3/11, ya que las sensitivity labels son el disparador principal de la mayoría de las políticas DLP de mayor precisión. Adaptive Protection enlaza este bloque con el Bloque 5/11 sobre Insider Risk Management, cerrando el ciclo entre detección de riesgo y aplicación de políticas. La cobertura de Cloud Apps mediante MDCA es parte integral de la arquitectura Zero Trust descrita en el Bloque 10/11.

---

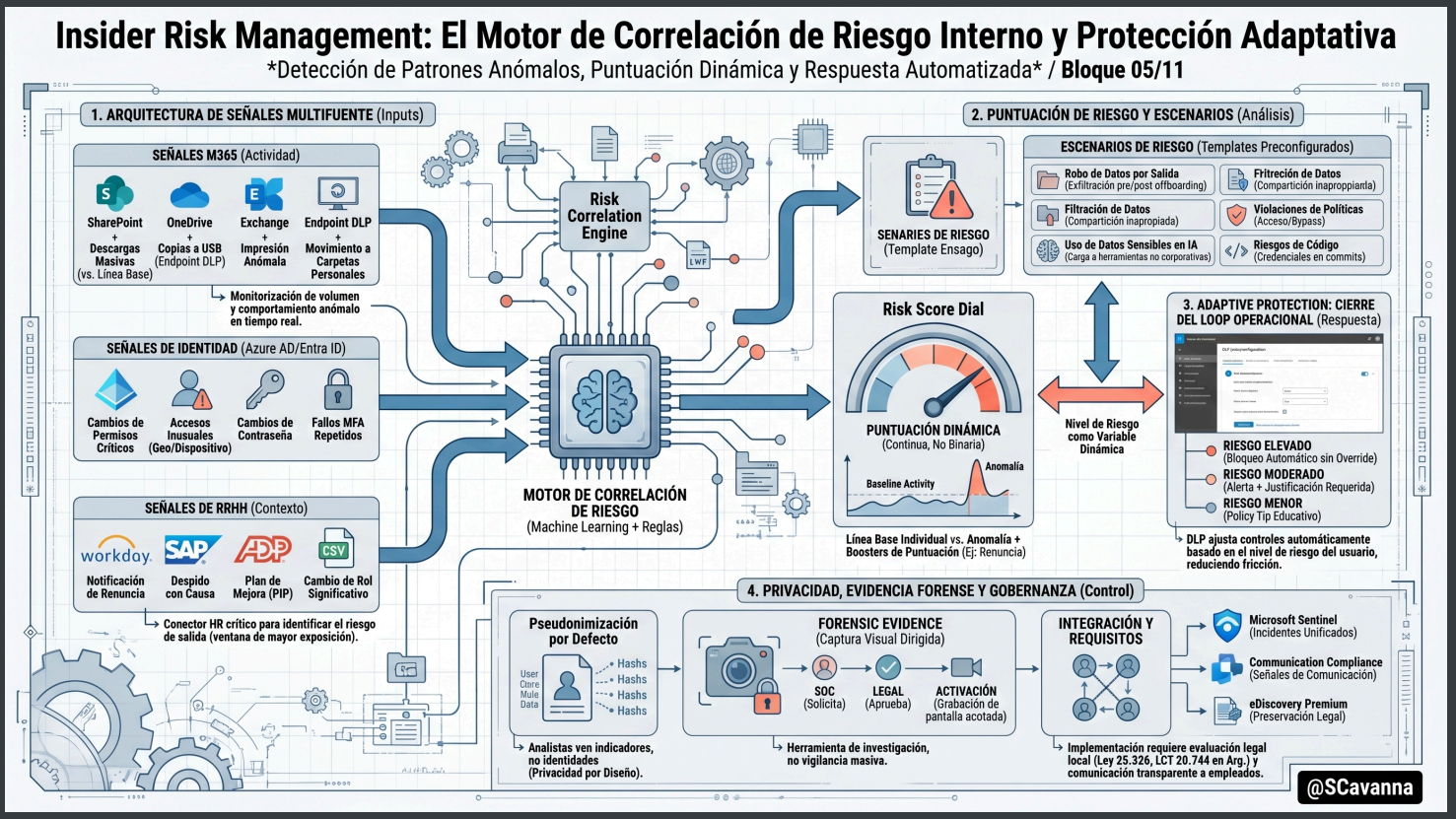
# 05/ - Insider Risk Management y Adaptive Protection

## Idea Central

Insider Risk Management (IRM) y Adaptive Protection describen cómo Microsoft 365 detecta y mitiga riesgos internos basados en 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 positivos 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 monitoreo, privacidad y respuesta coordinada en el SOC.



# Bloque 5/11 Insider Risk Management y Adaptive Protection

## Nivel 2: Conceptos Clave

| Concepto | Explicación / Data |
| --- | --- |
| **Arquitectura de señales multifuente** | IRM construye su modelo de riesgo correlacionando señales de múltiples orígenes simultáneamente. Las señales de actividad en M365 incluyen volumen de descarga de archivos de SharePoint y OneDrive comparado con la línea de base del usuario, copias a USB mediante Endpoint DLP, actividad de impresión, intentos de acceso a contenido fuera del alcance habitual, renombrado masivo de archivos como señal de preparación para exfiltración o sabotaje y movimiento de archivos a carpetas personales de OneDrive. Las señales de Azure AD o Entra ID incluyen cambios de permisos, adición de cuentas externas como delegados, acceso desde ubicaciones geográficas inusuales, cambios de contraseña inusuales y eventos de MFA fallidos. Las señales de RRHH se ingieren mediante conectores con sistemas como Workday, SAP SuccessFactors o ADP, o mediante importación de archivos CSV. Incluyen notificaciones de proceso de terminación (renuncia voluntaria, despido con causa, finalización de contrato), participación en planes de mejora de rendimiento (PIP), cambios de rol significativos y licencias disciplinarias. La correlación de estas señales permite que IRM identifique el escenario de riesgo más frecuente y de mayor impacto: el empleado que ha notificado su renuncia y que en los días siguientes incrementa significativamente su actividad de descarga y copia de archivos. |

| Concepto | Explicación / Data |
| --- | --- |
| **Escenarios de riesgo y templates de detección** | IRM organiza los riesgos del usuario interno en cinco escenarios principales, cada uno con un template de política preconfigurado y ajustable. Robo de datos por usuarios que se van, centrado en la exfiltración pre o post offboarding, suele ser el escenario de mayor frecuencia. Filtración de datos abarca la compartición inapropiada de información sensible por canales no autorizados, con o sin intención maliciosa. Uso de datos sensibles en IA se cubre mediante integración con DSPM for AI para detectar carga de contenido sensible a herramientas de IA no corporativas. Violaciones de políticas de seguridad incluye acceso a categorías de contenido inapropiadas e intentos de bypass de controles de seguridad. Riesgos de código en desarrollo, para organizaciones con equipos de software, detecta commits que incluyen credenciales, claves API o código de seguridad sensible. Cada template define señales ponderadas, umbrales de activación configurables y recomendaciones de acción para cada nivel de alerta. |
| **Puntuación de riesgo dinámica y línea de base individual** | La puntuación de riesgo en IRM es un valor continuo que se calcula de forma individual para cada usuario y se actualiza en tiempo real a medida que llegan nuevas señales. IRM construye una línea de base de comportamiento individual: un usuario que habitualmente descarga 200 archivos por día no genera alerta cuando descarga 300 en un día específico; un usuario cuya línea de base es 20 descargas diarias que descarga 300 en un día sí genera una señal significativa. Esta individualización reduce falsos positivos que afectarían a usuarios con roles de alta actividad legítima como analistas de datos, gestores de documentación o equipos de M&A en períodos de due diligence. Los boosters de puntuación son factores que elevan el riesgo independientemente del volumen, por ejemplo la recepción de una notificación de terminación en el sistema de RRHH, que eleva de inmediato el nivel de vigilancia desde el momento en que IRM recibe la señal. |

| Concepto | Explicación / Data |
| --- | --- |
| **Adaptive Protection: cierre del loop operacional** | Adaptive Protection es la integración bidireccional entre IRM y DLP que transforma la puntuación de riesgo de IRM en una variable de configuración de las políticas DLP. IRM clasifica a los usuarios en tres niveles de riesgo dinámicos: Elevated Risk, Moderate Risk y Minor Risk. DLP define acciones diferenciadas por nivel. Un usuario en Minor Risk que intenta copiar a USB un documento Confidencial recibe un policy tip; un usuario en Elevated Risk que realiza la misma acción recibe un bloqueo automático sin posibilidad de override. Esta diferenciación reduce la fricción para la mayoría de los usuarios que operan dentro de límites normales y endurece de forma automática los controles sobre quienes presentan señales de riesgo, sin requerir intervención manual constante del SOC. La configuración de Adaptive Protection requiere que IRM y DLP estén activos y que las políticas DLP tengan habilitadas condiciones basadas en el riesgo del usuario. |
| **Forensic Evidence y controles de privacidad** | Forensic Evidence es un complemento de licencia para IRM que habilita la captura de actividad visual, mediante grabación de pantalla en segmentos cortos, para usuarios investigados formalmente en un caso IRM. Su activación requiere un flujo de aprobación multirol, típicamente SOC, Legal y RRHH, y se limita a dispositivos específicos durante períodos acotados. No es una capacidad de grabación masiva ni continua, sino una herramienta de investigación forense que complementa los logs de actividad cuando la evidencia textual es insuficiente para demostrar intención. En términos de privacidad, IRM implementa pseudonimización por defecto: los analistas del SOC ven indicadores de riesgo y patrones de comportamiento asociados a identificadores anonimizados. La desanonimización, es decir ver el nombre real del usuario, requiere aprobación explícita por parte de un rol con autorización específica, generalmente en Legal o RRHH, y esa acción queda registrada en el log de auditoría. Este diseño equilibra la detección efectiva del riesgo con los requerimientos de protección de datos bajo GDPR y legislaciones locales equivalentes. |

## Nivel 3: Notas de Soporte

La implementación de IRM en organizaciones de Latinoamérica requiere una evaluación legal previa sobre la legislación laboral y de privacidad aplicable en cada jurisdicción. En Argentina, la Ley 25.326 de Protección de Datos Personales y la jurisprudencia sobre monitoreo de comunicaciones laborales, complementada por la Ley de Contrato de Trabajo 20.744, establecen condiciones específicas sobre

el alcance del monitoreo en el contexto laboral y los requisitos de notificación a los empleados. La recomendación es que la activación de IRM esté precedida por una actualización de las políticas de uso aceptable y una comunicación explícita a los empleados sobre el alcance del monitoreo, avalada por el equipo legal. La pseudonimización por defecto de IRM es un control técnico de privacidad relevante, pero no reemplaza el cumplimiento del marco legal aplicable.

Los conectores de RRHH son críticos para la efectividad de IRM en escenarios de offboarding. Sin la señal de terminación proveniente del sistema de RRHH, IRM no puede elevar automáticamente la puntuación de riesgo de un usuario que ha notificado su renuncia. La configuración del conector requiere que el sistema de RRHH exporte un archivo en formato específico, que incluya nombre del usuario, fecha de terminación efectiva y tipo de terminación, con la frecuencia definida. En organizaciones donde el proceso de offboarding puede tardar semanas desde la notificación hasta el último día efectivo, este lapso es precisamente la ventana de riesgo más alta que IRM está diseñado para cubrir.

Las alertas de IRM se integran de forma nativa con Microsoft Sentinel. Los incidentes de IRM se convierten en incidentes de Sentinel que pueden correlacionarse con señales de identidad de Entra ID Protection, endpoint de Microsoft Defender for Endpoint y red de Defender for Cloud para construir una visión unificada del riesgo en el SOC. Esta integración permite que los playbooks de Sentinel automaticen respuestas iniciales a casos de IRM, por ejemplo suspensión automática de acceso a SharePoint para usuarios en Elevated Risk que superan un umbral de actividad definido.

### Conexiones externas

Adaptive Protection es el vínculo técnico directo con el Bloque 4/11 dedicado a DLP. Las señales de comunicaciones anómalas que alimentan IRM provienen del motor de Communication Compliance del Bloque 6/11. Los casos de IRM que escalan a investigación formal utilizan la infraestructura de eDiscovery Premium del Bloque 7/11 para preservar, recolectar y revisar la evidencia de forma técnicamente defendible. La integración con Sentinel conecta este bloque con la arquitectura Zero Trust del Bloque 10/11.

---

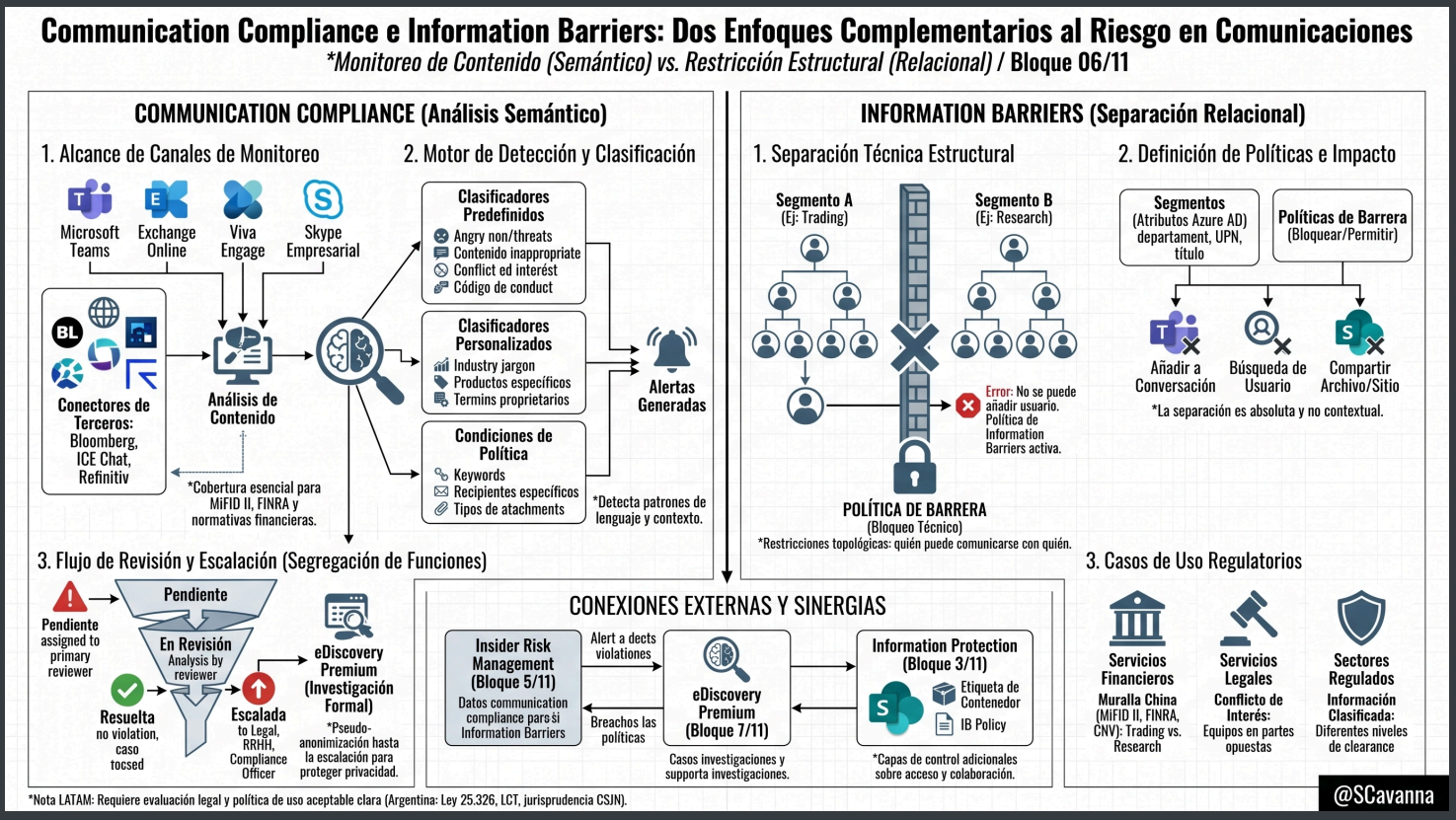
# 06/ - Communication Compliance e Information Barriers

## 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 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.




# Bloque 6/11: Communication Compliance e Information Barriers

## Nivel 2: Conceptos Clave

| Concepto | Explicación / Data |
|---|---|
| **Alcance de canales de Communication Compliance** | Communication Compliance monitorea y analiza comunicaciones en los siguientes canales: **Microsoft Teams** (chats directos, mensajes de canal, canales privados y mensajes de reuniones transcriptos), **Exchange Online** (correo corporativo enviado y recibido, incluyendo adjuntos), **Viva Engage** (mensajes en comunidades y mensajes directos), **Skype Empresarial Online** (para organizaciones que aún no migraron completamente a Teams) y fuentes externas mediante **conectores de terceros** como Bloomberg Messaging, ICE Chat, Refinitiv Eikon y otras plataformas del sector financiero. Esta cobertura de fuentes externas es crítica para instituciones financieras reguladas que deben cumplir con **MiFID II** en Europa, **FINRA** en Estados Unidos y normativas equivalentes, que exigen supervisar todas las comunicaciones relacionadas con trading y asesoramiento financiero, sin importar el canal técnico utilizado. |

| Concepto | Explicación / Data |
| --- | --- |
| **Motor de detección y clasificación de contenido** | El análisis de Communication Compliance combina tres mecanismos. Los **clasificadores entrenables predefinidos** detectan acoso laboral y discriminación (lenguaje basado en características protegidas como género, raza, religión u orientación sexual), lenguaje explícito y contenido sexualmente inapropiado, amenazas verbales o físicas, conflicto de interés (términos financieros en contextos sospechosos con terceros) y violaciones al código de conducta corporativo. Las organizaciones pueden crear **clasificadores personalizados** ajustados a su terminología: comunicaciones reguladas de su sector, nombres de productos propietarios, patrones de lenguaje asociados a conductas específicas de la industria. Las **condiciones de política** permiten combinar clasificadores con palabras clave, grupos o destinatarios específicos, tipos de adjuntos y otros metadatos, para construir políticas de supervisión de alta precisión. El sistema genera alertas que se envían a revisores designados, quienes solo acceden a las comunicaciones marcadas como potencial violación, con segregación estricta de funciones para evitar que un mismo individuo sea sujeto supervisado y revisor. |
| **Flujo de revisión y escalación** | El flujo de trabajo de revisión en Communication Compliance se alinea con requerimientos formales de segregación de funciones. Una alerta pasa por estados definidos: **Pendiente** (alerta generada y asignada a un revisor primario), **En revisión** (el revisor analiza el contenido y el contexto), **Resuelta** (se concluye que no existe violación real y se cierra el caso sin acción) o **Escalada** (se identifica una posible violación que requiere intervención de áreas como Legal, Recursos Humanos o el Compliance Officer). En la escalación, el caso puede etiquetarse, documentarse con notas internas y vincularse a una investigación formal en **eDiscovery Premium**. La pseudoanonimización del sujeto supervisado puede mantenerse durante las fases iniciales de revisión y levantarse solo al momento de la escalación, para proteger la privacidad hasta que la evidencia justifique la identificación. Toda la cadena de revisión queda registrada de forma inmutable en los logs de auditoría, incluyendo quién revisó, cuándo, qué acciones tomó y su justificación. |

| Concepto | Explicación / Data |
| --- | --- |
| **Information Barriers: separación técnica estructural** | **Information Barriers (IB)** aplica políticas que restringen técnicamente la comunicación y colaboración entre segmentos definidos de la organización, de modo que ciertas interacciones sean imposibles en lugar de solo monitoreadas. La implementación se basa en la definición de **segmentos** (grupos de usuarios construidos a partir de atributos de Azure AD como departamento, UPN, título, ubicación u otros atributos de directorio) y **políticas de barrera** que especifican si la comunicación entre segmentos concretos está permitida o bloqueada. Cuando una política de IB está activa, si el usuario A intenta agregar al usuario B a una conversación de Teams y pertenecen a segmentos que no pueden comunicarse, el sistema bloquea la acción y muestra un mensaje de error. Lo mismo aplica para la **búsqueda de usuarios** en Teams y en el directorio (usuarios bloqueados no aparecen en resultados), para la **compartición de archivos en SharePoint** (sitios etiquetados que respetan IB no permiten acceso de segmentos bloqueados) y para **Exchange** (control de listas de distribución y permisos de delegado). |
| **Casos de uso regulatorios de Information Barriers** | Los casos de uso regulatorios más frecuentes de IB se concentran en tres sectores. En **servicios financieros**, se utiliza para separar la mesa de trading de los equipos de research de equity o de banca de inversión y así cumplir con los requisitos de “murallas chinas” de **MiFID II** en Europa, **FINRA Rules 2241/2242** en Estados Unidos y normativas equivalentes de otros reguladores como la **CNV** en Argentina. Esta separación busca impedir que los traders accedan a información material no pública del equipo de research que podría derivar en insider trading. En **servicios legales**, IB se aplica para separar equipos que representan a partes con potencial conflicto de interés en un mismo caso o transacción. En **sectores regulados con información clasificada** (defensa, organismos gubernamentales), se utiliza para separar equipos con distintos niveles de clearance o que gestionan proyectos sujetos a contratos que exigen segregación estricta de información. |

## Nivel 3: Notas de Soporte

### Implementación de Communication Compliance en jurisdicciones latinoamericanas

La implementación de Communication Compliance en jurisdicciones latinoamericanas requiere una evaluación legal cuidadosa sobre el alcance del monitoreo de comunicaciones laborales. En **Argentina**, la combinación de la Ley 25.326 de Protección de Datos Personales, las disposiciones de la **Ley de Contrato de Trabajo 20.744** sobre privacidad del trabajador y la jurisprudencia de la **Corte Suprema de Justicia de la Nación** sobre monitoreo de comunicaciones en el ámbito laboral establece que el monitoreo de comunicaciones corporativas suele considerarse lícito cuando se cumplen ciertas condiciones. Entre ellas se incluyen: la existencia de una **política de uso aceptable** clara, comunicada explícitamente a los empleados; la limitación del monitoreo a las comunicaciones realizadas a través de herramientas corporativas; y el uso de los resultados con fines de supervisión de cumplimiento normativo y no como mecanismo de vigilancia generalizada. La práctica recomendada es que la activación de Communication Compliance vaya precedida por la actualización formal de la política de uso aceptable y por una comunicación transparente a los empleados sobre alcance, base legal y propósito del monitoreo.

### Limitaciones arquitectónicas de Information Barriers

Information Barriers presenta una limitación arquitectónica relevante: sus políticas son **estáticas por diseño**, no dinámicas. Una vez definidos los segmentos y las políticas, la separación que imponen es absoluta y no se ajusta automáticamente al contexto de cada interacción. Si surge una situación excepcional en la que dos usuarios de segmentos bloqueados necesitan colaborar legítimamente en un proyecto específico, la solución requiere crear un nuevo segmento, redefinir la pertenencia de usuarios o modificar temporalmente la política. Estas acciones tienen implicaciones de cumplimiento que deben ser analizadas, aprobadas y documentadas, ya que relajan una separación que usualmente está asociada a obligaciones regulatorias. Esta rigidez es precisamente el atributo que hace a IB adecuado para cumplimiento formal: ofrece a reguladores y auditores la certeza de que la separación entre segmentos es técnicamente absoluta mientras la política permanezca configurada y vigente.

### Conexiones con otros componentes de Microsoft Purview

Las violaciones detectadas por Communication Compliance pueden alimentar casos en **Insider Risk Management** como señales adicionales de riesgo asociadas a un usuario o grupo, integrando comportamiento comunicacional en el modelo de riesgo interno. Las investigaciones formales que se derivan tanto de Communication Compliance como de Insider Risk Management se apoyan en la infraestructura de **eDiscovery Premium**, que proporciona capacidades avanzadas de búsqueda,

retención, análisis y exportación de evidencias. Por su parte, la separación de contenedores implementada por Information Barriers se integra con el **etiquetado de contenedores** de **Information Protection**: un sitio de SharePoint con etiqueta de contenedor y políticas de IB activas acumula múltiples capas de control sobre quién puede acceder, qué puede hacer con el contenido y con quién puede colaborar dentro de ese contenedor. Esta combinación refuerza la defensa en profundidad sobre la información sensible y las comunicaciones vinculadas.

---

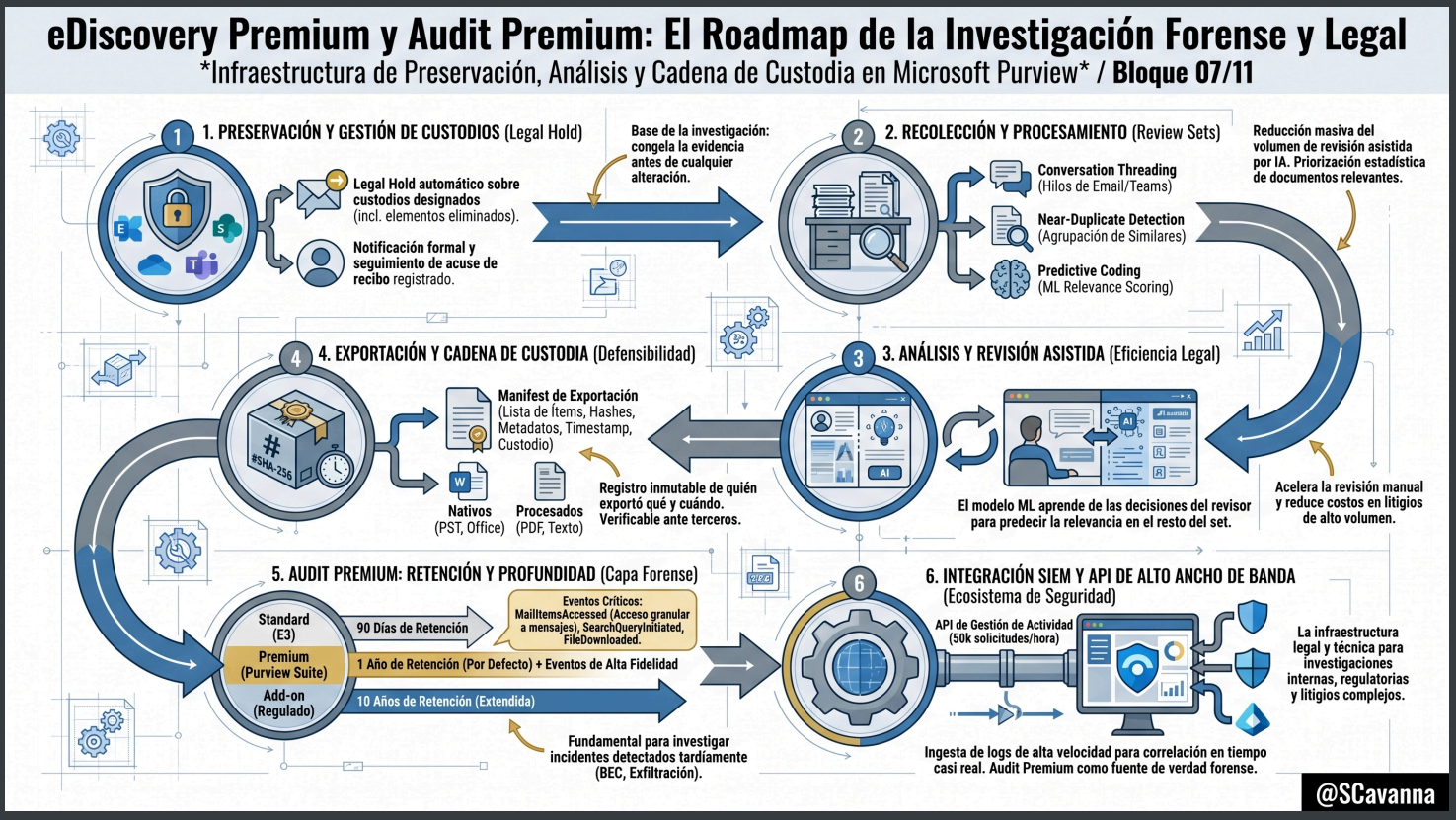
# 07/ - eDiscovery Premium y Audit Premium

## 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. El documento relaciona estas capacidades con requerimientos regulatorios y de litigación, y con soluciones de riesgo interno y cumplimiento 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

## Nivel 2 Conceptos Clave

| Concepto | Explicación / Data |
|---|---|
| **Legal Hold y gestión de custodios** | El proceso de eDiscovery en cualquier investigación formal o litigación comienza con la preservación de la evidencia antes de que pueda ser alterada o eliminada por los sujetos de la investigación. eDiscovery Premium implementa este requerimiento mediante el Legal Hold sobre custodios: se designan formalmente los usuarios (custodios) cuyo contenido debe ser preservado, y el sistema coloca automáticamente un hold sobre todo su contenido en Exchange Online (buzón primario y de archivo), SharePoint Online, OneDrive for Business y Microsoft Teams, incluido el contenido que el usuario haya eliminado durante el período del hold, que se mantiene en las carpetas de recoverable items, inaccesibles para el usuario pero preservadas para la investigación. La notificación al custodio es un proceso formal integrado en eDiscovery Premium: el sistema puede enviar automáticamente notificaciones legales (litigation hold notices) a los custodios, gestionar el seguimiento de quiénes han acusado recibo, enviar recordatorios |

| Concepto | Explicación / Data |
| --- | --- |
| | automáticos y registrar toda la comunicación relacionada con el hold en el expediente del caso. Este flujo de notificación es relevante para organizaciones sujetas a obligaciones de litigation hold bajo sistemas judiciales anglosajones (USA, UK), pero también tiene valor probatorio en procesos regulatorios en jurisdicciones latinoamericanas. |
| **Review Sets y análisis asistido por ML** | Una vez recolectado el contenido bajo hold, eDiscovery Premium lo procesa en Review Sets, conjuntos de trabajo donde el equipo legal y técnico aplica múltiples técnicas de reducción y organización del volumen de evidencia. El conversation threading reconstruye automáticamente los hilos completos de conversaciones de correo electrónico y Teams, presentando los mensajes en contexto conversacional en lugar de como elementos individuales. El near-duplicate detection agrupa documentos con contenido altamente similar, por ejemplo múltiples versiones de un contrato con cambios menores, permitiendo que el revisor marque todos los de un grupo con una sola acción. El email threading identifica la cadena de correos más completa de cada hilo y la presenta como representativa, reduciendo la revisión de mensajes redundantes. El relevance scoring (Predictive Coding) es un modelo de aprendizaje automático que aprende del comportamiento de revisión del usuario, es decir, qué documentos marca como relevantes frente a irrelevantes, y predice la relevancia de los documentos no revisados. Esto permite priorizar la revisión hacia el contenido con mayor probabilidad de ser relevante y aplicar reducciones de volumen estadísticamente defendibles en contextos de litigación con altos estándares probatorios. |
| **Exportación y cadena de custodia** | La exportación de evidencia desde eDiscovery Premium genera automáticamente un manifest de exportación que incluye la lista completa de los ítems exportados, el hash SHA-256 de cada ítem, metadatos de fecha de creación, modificación o recepción, información del custodio asociado y el timestamp de la exportación. Este manifest permite verificar en cualquier momento posterior que el contenido exportado no ha sido alterado desde el momento de la exportación, cumpliendo el requerimiento de integridad de la cadena de custodia. El registro de quién exportó qué y cuándo es inmutable en el log de Audit Premium. La exportación soporta formatos nativos, como PST para correo y archivos de Office originales, y formatos procesados, como PDF o texto plano, con la opción de incluir o excluir metadatos según los requerimientos del destinatario, ya sea un tribunal, un árbitro o un regulador. |

| Concepto | Explicación / Data |
| --- | --- |
| **Audit Premium: retención, profundidad y eventos críticos** | Audit Premium, incluido en Purview Suite, extiende las capacidades de Audit Standard (E3) en dos dimensiones críticas: retención y profundidad de eventos. En retención, Audit Standard mantiene los logs de actividad durante 90 días, mientras que Audit Premium los mantiene durante 1 año por defecto, con un complemento disponible de 10 años para sectores regulados que requieren retención extendida, como financiero, salud o gobierno. La diferencia de retención es operacionalmente crítica porque la mayoría de las investigaciones de compromiso de cuentas o incidentes de exfiltración se inician días o semanas después del evento, y con 90 días de retención la evidencia puede haber expirado. En profundidad de eventos, Audit Premium incluye eventos de alta fidelidad forense que no están disponibles en Audit Standard, el más crítico de los cuales es MailItemsAccessed. Este evento registra exactamente qué mensajes de correo fueron accedidos, cuándo, por quién y desde qué protocolo (MAPI, REST API, OWA), permitiendo determinar qué información leyó un atacante durante un compromiso de cuenta de correo, como BEC o ATO. También incluye SearchQueryInitiated, que registra qué búsquedas realizó un usuario en Exchange y SharePoint, FileDownloaded en SharePoint y OneDrive con metadatos completos, y otros eventos de alta granularidad. |
| **API de Audit de alto ancho de banda e integración SIEM** | Purview Suite incluye acceso a la Management Activity API de Office 365 con una capacidad de throughput significativamente superior a la disponible en Audit Standard, hasta 50.000 solicitudes por hora por publisher frente al límite más restrictivo de Standard. Este throughput extendido es necesario para organizaciones que integran los logs de Audit con plataformas SIEM externas, como Microsoft Sentinel, Splunk, IBM QRadar o Elastic, para correlación en tiempo casi real. La integración con Sentinel es la más directa: los logs de Audit Premium se ingieren automáticamente en el workspace de Sentinel habilitado para M365, donde pueden ser correlacionados con señales de Defender for Endpoint, Entra ID Protection y otras fuentes del stack de seguridad. Esto convierte a Audit Premium en la fuente de verdad forense del plano de productividad M365 dentro de la arquitectura SIEM. |

## Nivel 3 Notas de Soporte

La comparativa entre eDiscovery Standard, incluido en E3, y eDiscovery Premium, disponible en Purview Suite, es sustancial en cualquier contexto que requiera investigación formal. eDiscovery Standard permite crear casos básicos, realizar búsquedas de contenido en Microsoft 365 y exportar los resultados en formatos básicos. No incluye gestión formal de custodios, Legal Hold con notificación, review sets, análisis de relevancia mediante aprendizaje automático ni exportación con cadena de custodia verificable con hash. Para organizaciones sujetas a procesos de litigación en jurisdicciones con alta actividad de discovery, particularmente cualquier litigación que involucre contraparte o regulador estadounidense bajo las Federal Rules of Civil Procedure, la ausencia de las capacidades de eDiscovery Premium puede resultar en costos significativos de plataformas de eDiscovery de terceros, como Relativity, Nuix o Disco, para cubrir las funcionalidades faltantes.

El evento MailItemsAccessed de Audit Premium fue introducido específicamente como respuesta a los hallazgos del breach de SolarWinds y otros incidentes de BEC de alto perfil en los que los investigadores no podían determinar qué información había accedido el atacante durante el período de compromiso porque los logs existentes no registraban accesos a nivel de mensaje individual. Microsoft lo describió como una de las mejoras forenses más significativas del producto desde el lanzamiento del log de auditoría de Microsoft 365.

El complemento de 10 años de retención de Audit es relevante en Argentina para organizaciones que deben cumplir con las disposiciones del Banco Central de la República Argentina sobre conservación de documentación, como la Comunicación A 7724 y las regulaciones de registros de operaciones bancarias, para subsidiarias de multinacionales sujetas a SOX, Sarbanes Oxley Act, Sección 802 sobre conservación de registros durante 5 a 7 años, y para organizaciones sujetas a la Ley 11.683 de Procedimiento Tributario y sus requerimientos de conservación de documentación fiscal.

**Conexiones externas:** Audit Premium es la fuente de evidencia forense que alimenta las investigaciones de Insider Risk Management iniciadas en el Bloque 5/11. Los casos de Communication Compliance que escalan a investigación formal, tratados en el Bloque 6/11, utilizan eDiscovery Premium para preservar y revisar la evidencia de las comunicaciones bajo las condiciones de cadena de custodia requeridas. Los logs de Audit Premium integrados con Sentinel constituyen la capa forense del modelo Zero Trust descrito en el Bloque 10/11.

---

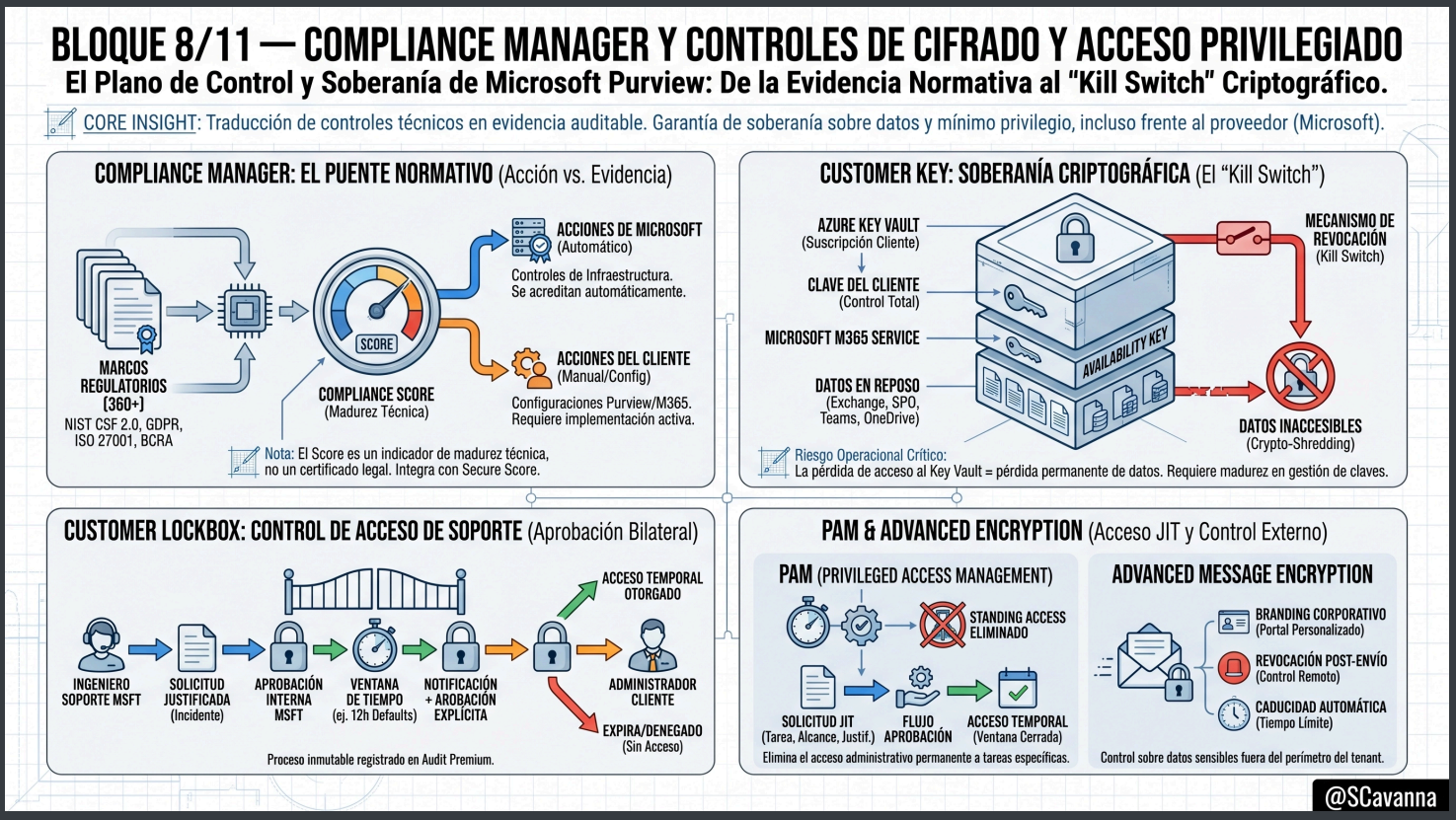
# 08/ - Compliance Manager y controles de cifrado y acceso

## Idea Central

Este bloque describe cómo Microsoft Purview y M365 conectan controles técnicos con requerimientos normativos. Explica el rol de Compliance Manager, Customer Key, Customer Lockbox, Privileged 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

## Nivel 2: Conceptos clave

| Concepto | Explicación / Data |
|---|---|
| **Compliance Manager: de controles técnicos a evidencia normativa** | Compliance Manager es la interfaz entre la implementación técnica de Purview y los marcos normativos que la organización debe demostrar cumplir. Opera sobre un modelo de **evaluaciones**: cada evaluación corresponde a un marco regulatorio o de referencia y contiene un conjunto de controles mapeados a acciones concretas. Microsoft provee evaluaciones preconstruidas para más de 360 marcos y regulaciones, incluyendo NIST CSF 2.0, ISO/IEC 27001:2022, GDPR, HIPAA, SOC 2 Type II, PCI-DSS v4.0 y marcos regionales como la normativa del BCRA para servicios financieros en Argentina, LGPD de Brasil y la Ley Federal de Protección de Datos Personales de México. Cada evaluación distingue entre dos tipos de acciones: **acciones de Microsoft** (controles implementados en la infraestructura del servicio que Microsoft demuestra |

| Concepto | Explicación / Data |
| --- | --- |
| | cumplir a través de sus certificaciones y auditorías externas, y que se acreditan automáticamente en el Compliance Score) y **acciones del cliente** (controles que la organización debe implementar activamente, muchos de los cuales son configuraciones de Purview y del stack M365). El **Compliance Score** (0-100) resume el estado de implementación de las acciones del cliente y es un indicador de madurez de implementación técnica, no un certificado de cumplimiento normativo. Esta distinción debe comunicarse con precisión a juntas directivas y auditores para evitar interpretaciones incorrectas del score. |
| **Customer Key: soberanía criptográfica** | Customer Key es la capacidad de Microsoft Purview que permite a la organización proveer sus propias claves de cifrado para proteger los datos en reposo en los servicios de M365, en reemplazo de las claves de servicio gestionadas por Microsoft. Las claves se almacenan en **Azure Key Vault**, bajo una suscripción de Azure propiedad y control total de la organización. Customer Key aplica sobre Exchange Online (buzones), SharePoint Online y OneDrive (archivos), Microsoft Teams (mensajes y archivos de Teams) y el servicio de etiquetado de información (etiquetas de confidencialidad con cifrado RMS). El mecanismo técnico es un modelo de cifrado jerárquico donde la clave del cliente, almacenada en Key Vault, cifra la clave de disponibilidad del servicio, que a su vez cifra la clave de cifrado de datos. La consecuencia operacional más significativa de Customer Key es la **revocación**: si la organización revoca el acceso de Microsoft a las claves en Key Vault (eliminando las claves o revocando los permisos de acceso del servicio M365), los datos protegidos con Customer Key se vuelven técnicamente inaccesibles incluso para Microsoft. Este mecanismo tiene implicaciones directas en escenarios de terminación de contrato con Microsoft, fusiones y adquisiciones, respuesta a órdenes judiciales de jurisdicciones extranjeras o situaciones donde la organización necesita garantizar que puede revocar el acceso de Microsoft a sus datos de forma irrevocable. |

| Concepto | Explicación / Data |
| --- | --- |
| **Customer Lockbox: control del acceso de soporte** | Customer Lockbox aborda el riesgo del acceso potencial de ingenieros de soporte de Microsoft a los datos del tenant durante la resolución de un incidente de servicio. Sin Customer Lockbox, Microsoft puede acceder a los datos del tenant bajo los términos del acuerdo de servicio cuando es necesario para resolver un problema técnico, con controles internos pero sin aprobación explícita del cliente. Con Customer Lockbox activado, cuando el soporte de Microsoft necesita acceder a datos del tenant para resolver un incidente, el proceso requiere: (1) el ingeniero de soporte de Microsoft genera una solicitud de acceso justificada, (2) la solicitud es aprobada internamente en Microsoft por un nivel de gestión apropiado, (3) se envía una notificación al administrador global designado del cliente con los detalles del acceso solicitado (qué datos, durante cuánto tiempo y con qué propósito), (4) el administrador del cliente dispone de un período de tiempo configurado (12 horas por defecto) para aprobar o rechazar la solicitud y (5) si no hay respuesta en el período configurado, la solicitud expira sin que el acceso sea otorgado. Todo el proceso, incluida la solicitud, la aprobación interna de Microsoft, la notificación al cliente, la decisión del cliente y el resultado, queda registrado en el log de Audit Premium de forma inmutable. |

| Concepto | Explicación / Data |
| --- | --- |
| **Privileged Access Management (PAM)** | PAM en M365 complementa a Entra ID Privileged Identity Management (PIM) para el plano de administración específico de M365. Mientras PIM gestiona la elevación de roles de Azure AD (por ejemplo, Global Administrator, Exchange Administrator) mediante activación temporal con justificación, PAM opera a un nivel de granularidad inferior y gestiona el acceso a **tareas administrativas específicas** dentro de M365, independientemente del rol que el usuario tenga asignado. El principio técnico es eliminar el **standing access**, es decir, la capacidad de un administrador de ejecutar tareas privilegiadas en cualquier momento sin una solicitud adicional. Con PAM configurado, incluso un Exchange Administrator no puede ejecutar tareas como acceder al buzón de un usuario específico o exportar datos de eDiscovery sin enviar una solicitud JIT (Just in Time) que especifica la tarea exacta a realizar, el alcance (usuario, recurso o colección involucrada), la justificación de negocio y la duración del acceso solicitado. La solicitud se aprueba mediante un flujo configurado, que puede requerir aprobación de un segundo administrador, de Legal o de Compliance, o ser automática bajo ciertas condiciones. El acceso se otorga por el tiempo solicitado y expira automáticamente. Toda la cadena, desde la solicitud y la justificación hasta la aprobación, el acceso otorgado, las acciones realizadas y la expiración, queda registrada en Audit Premium. |
| **Advanced Message Encryption** | Advanced Message Encryption extiende las capacidades básicas de Message Encryption de M365, usadas para cifrar correos dirigidos a destinatarios externos, con tres capacidades adicionales: **branding corporativo** en el portal de mensajes cifrados que el destinatario externo usa para leer el mensaje (logo, colores y texto personalizado en lugar del portal genérico de Microsoft), **revocación de mensajes ya enviados** (el remitente o el administrador puede revocar el acceso a un mensaje cifrado después de enviado, de modo que el destinatario ya no pueda abrir el portal de lectura) y **caducidad del mensaje** (el acceso al mensaje se revoca automáticamente después de la fecha configurada). Estas capacidades son relevantes cuando los correos contienen información sensible con vigencia temporal, como propuestas comerciales, términos de negociación o información de due diligence, o cuando la organización necesita mantener control sobre el contenido después de que ha salido del perímetro del tenant. |

# Nivel 3: Notas de soporte

## Customer Key y gestión de claves

Customer Key es una decisión arquitectónica con consecuencias operacionales de largo alcance que no debe tomarse sin evaluar la madurez del proceso de gestión de claves de la organización. Los riesgos operacionales específicos incluyen la pérdida accidental de claves en Key Vault, que resultaría en pérdida permanente de acceso a todos los datos protegidos, la revocación involuntaria de permisos de acceso del servicio M365 a Key Vault, con el mismo resultado, y la complejidad de los procesos de recuperación ante desastres cuando el cifrado está bajo control del cliente.

Microsoft recomienda tener dos Key Vaults independientes en regiones de Azure distintas como medida de resiliencia, con políticas de copia de seguridad y procesos de recuperación probados periódicamente. Para organizaciones que no tienen un proceso maduro de gestión de claves criptográficas, la recomendación estándar es implementar primero **Microsoft Managed Keys** (configuración por defecto) o **Customer Managed Keys (CMK)**, donde Microsoft gestiona las claves en Key Vault bajo los permisos de la organización pero sin la opción de revocación de Customer Key, y migrar a Customer Key en una segunda fase cuando el proceso de gestión de claves esté establecido.

## Compliance Manager e integración con Secure Score

Compliance Manager incluye una funcionalidad de **integración con Microsoft Secure Score**. Las acciones de mejora de Secure Score que son relevantes para el cumplimiento normativo aparecen como acciones recomendadas en las evaluaciones de Compliance Manager, lo que crea un puente entre la postura de seguridad técnica (Secure Score) y el cumplimiento regulatorio (Compliance Score). Esta integración es especialmente útil para CISOs que necesitan justificar inversiones en controles técnicos de seguridad en términos de reducción del riesgo normativo.

## Conexiones con otros bloques de la arquitectura

El Compliance Score de Compliance Manager refleja el estado de implementación de controles distribuidos en bloques anteriores: la clasificación de información del Bloque 3/11, el enforcement de DLP del Bloque 4/11, la supervisión de IRM del Bloque 5/11 y los controles forenses del Bloque 7/11 contribuyen todos al score.

Customer Key interactúa directamente con la infraestructura de cifrado de Information Protection descrita en el Bloque 3/11. PAM se integra como control de acceso privilegiado dentro del modelo de Zero Trust desarrollado en el Bloque 10/11, reforzando el principio de mínimo privilegio en la administración del entorno M365.

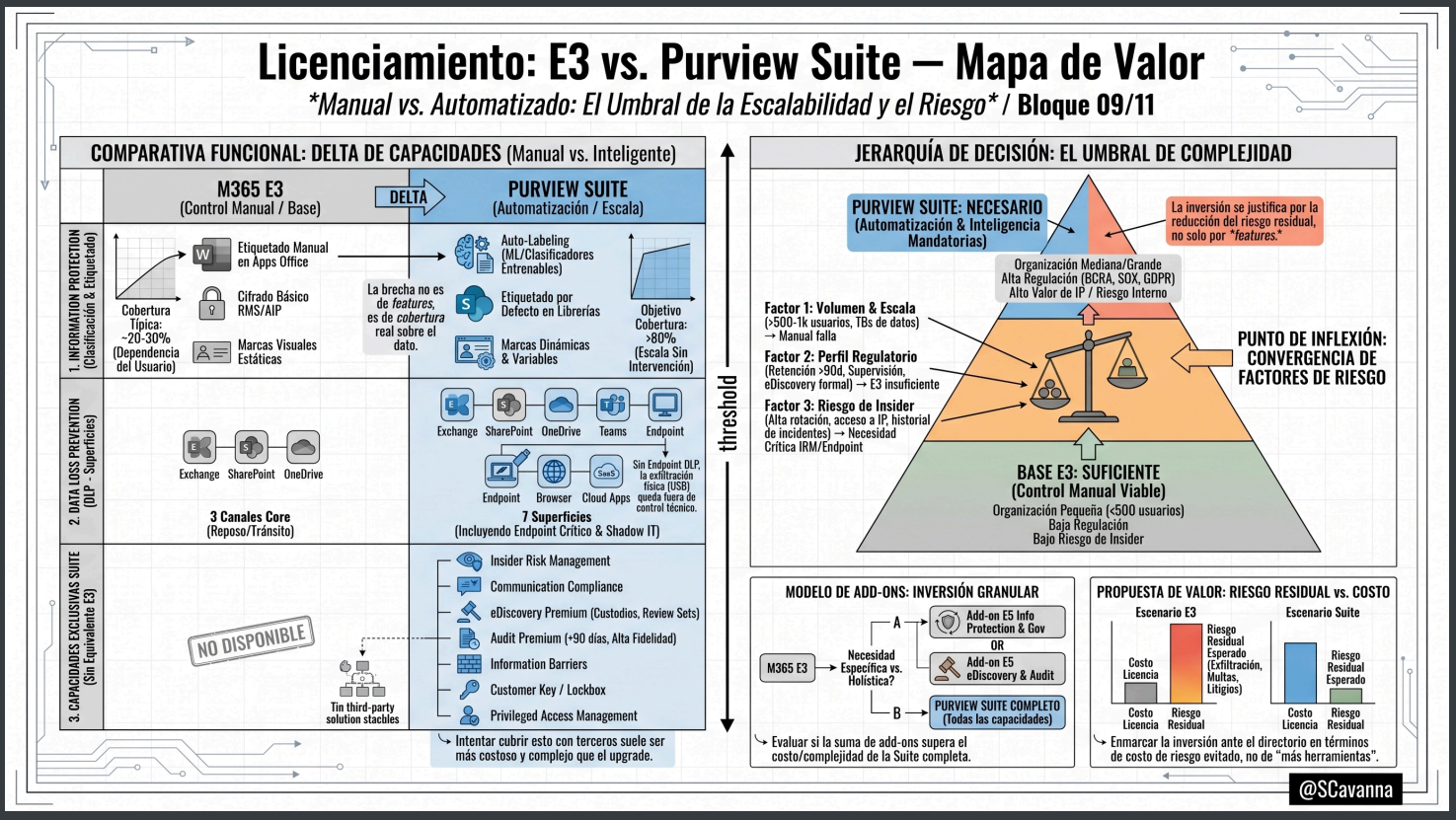
# 09/ - Licenciamiento: E3 frente a Purview Suite, mapa de valor

## 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 compara costo esperado de incidentes frente al costo de licencias.




# Bloque 9/11 - Licenciamiento: E3 vs. Purview Suite - Mapa de Valor

## Nivel 2 - Conceptos clave

| Concepto | Explicación / Data |
|---|---|
| **Delta de Information Protection: manual vs. automatizado** | E3 incluye sensitivity labels con etiquetado manual en aplicaciones Office (Word, Excel, PowerPoint, Outlook), cifrado básico con RMS/AIP y marcas visuales estáticas. No incluye auto-labeling con clasificadores entrenables (ML), etiquetado por defecto en librerías de SharePoint, marcas de agua dinámicas, etiquetado de reuniones de Teams ni etiquetado de contenedores avanzado. En organizaciones de varios miles de usuarios y millones de documentos, el etiquetado manual es estadísticamente ineficaz: en despliegues E3 la cobertura de etiquetado sobre el patrimonio documental rara vez supera el 20-30 % en los primeros 12-18 meses, incluso con campañas de concientización activas. Sin auto-labeling, el 70-80 % del contenido permanece sin clasificar, lo que deja al sistema DLP con cobertura |

| Concepto | Explicación / Data |
| --- | --- |
| | parcial sobre el dato real. Purview Suite cierra esta brecha con auto-labeling en modo servicio sobre el inventario existente y en modo cliente sobre el contenido nuevo. |
| **Delta de DLP: tres canales vs. siete superficies** | E3 incluye DLP sobre Exchange, SharePoint y OneDrive, que cubren el mayor volumen de datos en reposo y en tránsito por correo. No incluye DLP en Teams (mensajes de chat y canal), Endpoint DLP (canales físicos como USB, impresión, cargas desde aplicaciones locales), Browser DLP (control de Shadow IT y cargas a servicios no corporativos desde el navegador), Network DLP ni DLP en aplicaciones cloud de terceros (Salesforce, Box, Dropbox y otros SaaS). La ausencia de Endpoint DLP en E3 es la brecha operacional más crítica: un empleado con acceso legítimo a documentos confidenciales puede descargarlos desde SharePoint, copiarlos a un USB y llevárselos sin que exista un control preventivo, solo evidencias en logs. Purview Suite extiende DLP a las siete superficies con una capa de políticas centralizadas. |
| **Capacidades sin equivalente en E3** | Hay capacidades de Purview Suite que no tienen equivalente parcial en E3 y que obligan a evaluar add-ons o terceros si se quieren cubrir desde E3: **Insider Risk Management** (no existe en E3), **Communication Compliance** (no existe en E3), **eDiscovery Premium** (E3 solo incluye eDiscovery Standard, con búsqueda y exportación básica, sin gestión de custodios, Legal Hold con notificación, review sets con ML ni exportación con hash), **Audit Premium** (E3 ofrece Audit Standard con 90 días de retención y sin eventos de alta fidelidad como MailItemsAccessed), **Information Barriers**, **Customer Key**, **Customer Lockbox** y **Privileged Access Management**. Cuando se intenta cubrir estas capacidades con soluciones de terceros, el costo y la complejidad de integración rara vez resultan inferiores al costo del upgrade a Purview Suite. |

| Concepto | Explicación / Data |
| --- | --- |
| **Modelo de add-ons para usuarios E3: granularidad de inversión** | Para organizaciones que no migran a M365 E5 completo, existen add-ons de Purview que permiten licenciar solo las capacidades que el perfil de riesgo y la regulación requieren. Los principales son: **Microsoft Purview Suite** (todas las capacidades de cumplimiento avanzadas, antes E5 Compliance), **E5 Information Protection & Governance** (subset con auto-labeling, Records Management avanzado y Data Lifecycle Management, adecuado cuando la prioridad es clasificación y ciclo de vida) y **E5 eDiscovery & Audit** (subset con eDiscovery Premium y Audit Premium, enfocado en capacidades forenses y de investigación legal). La elección entre add-ons específicos y Purview Suite completo debe basarse en los riesgos regulatorios y operacionales actuales. Si ya se necesitan o se anticipan requerimientos de Insider Risk Management y Communication Compliance, el costo marginal de Purview Suite completo frente a add-ons individuales rara vez justifica una estrategia fragmentada. |
| **Regla de oro del licenciamiento: umbral de complejidad** | El criterio para justificar el upgrade a Purview Suite no es solo el tamaño ni el sector, sino la combinación de tres factores de complejidad que hacen insuficiente el control manual de E3. **Factor 1 - Volumen de datos y usuarios**: por encima de 500-1.000 usuarios activos con producción significativa de documentos, el etiquetado manual y la gestión manual de políticas DLP llevan a niveles de cobertura incompatibles con estándares regulatorios exigentes. **Factor 2 - Perfil regulatorio**: organizaciones sujetas a regulaciones que exigen retención de evidencia superior a 90 días (por ejemplo BCRA, SOX, FINRA), supervisión de comunicaciones (MiFID II, regulaciones de valores) o demostración de cadena de custodia formal en investigaciones requieren Purview Suite o los add-ons específicos. **Factor 3 - Exposición a riesgo de insider**: organizaciones con alta rotación de personal con acceso a información sensible o con historial de incidentes de exfiltración interna encuentran en Insider Risk Management y Endpoint DLP una reducción del riesgo residual que por sí sola puede justificar la inversión. |

## Nivel 3 - Notas de soporte

La presentación del valor de Purview Suite ante una junta directiva o un CFO debe enmarcar la inversión en términos de riesgo residual diferencial, no solo como un conjunto de funcionalidades adicionales. La metodología recomendada es estimar el costo esperado del riesgo bajo E3 (probabilidad de incidente multiplicada por el impacto en cada categoría de riesgo: exfiltración de

datos de clientes, incumplimiento regulatorio con multa, litigios sin capacidad de eDiscovery formal) y compararlo con el costo del upgrade a Purview Suite. En sectores financieros regulados, el riesgo regulatorio asociado al incumplimiento de obligaciones de conservación y seguridad de la información puede superar ampliamente el costo anual de Purview Suite para una institución de tamaño mediano.

Los precios de licenciamiento de Microsoft cambian periódicamente y varían por región y por programa de canal (CSP, EA, MCA-E). La referencia definitiva de precios y condiciones es el Microsoft Product Terms actualizado mensualmente y los acuerdos de precio vigentes con el partner o distribuidor. Ninguna cifra de precio debe comunicarse como definitiva sin verificación contra estas fuentes oficiales.

#### Conexiones externas

Este bloque conecta las capacidades técnicas descritas en los Bloques 1-8 con una decisión de inversión estratégica. Las capacidades avanzadas de Purview Suite habilitadas aquí son las que permiten la arquitectura Zero Trust descrita en el Bloque 10/11 y la gobernanza para IA desarrollada en el Bloque 11/11.

---

# 10/ - Purview en una arquitectura Zero Trust

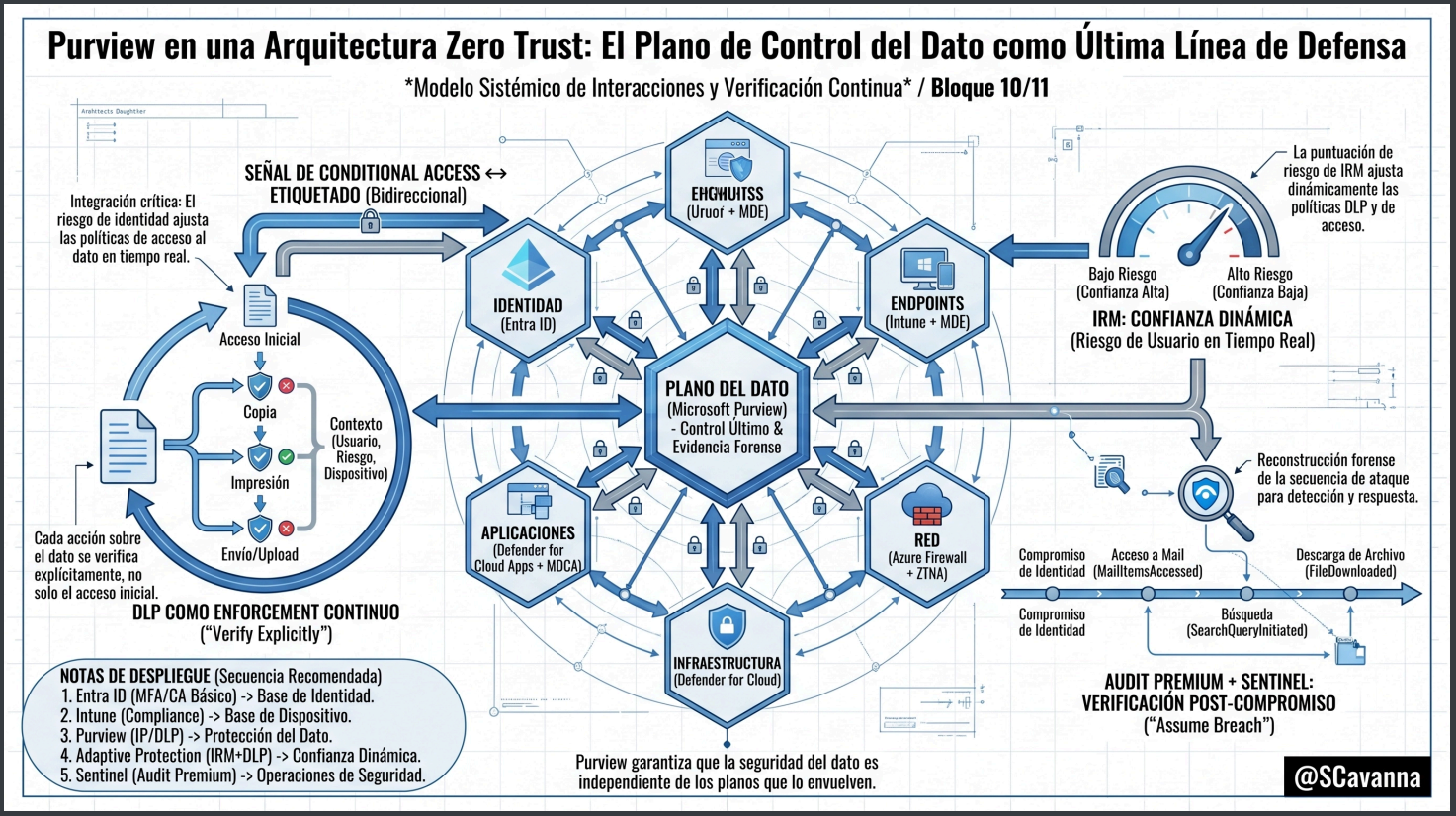
## Idea Central

Microsoft Purview se presenta como 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, 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

## Nivel 2 - Conceptos clave

| Concepto | Explicación |
| --- | --- |
| **Los cinco planos de Zero Trust y el posicionamiento de Purview** | El modelo Zero Trust de Microsoft, documentado en el Zero Trust Guidance Center, define seis pilares: Identidad (Entra ID), Endpoints (MDE + Intune), Aplicaciones (Defender for Cloud Apps + MDCA), Red (Azure Firewall + Defender for Cloud + ZTNA), Infraestructura (Defender for Cloud) y Datos |

| Concepto | Explicación |
| --- | --- |
| | (Microsoft Purview). La posición del dato como último plano de control refleja el principio de defensa en profundidad: incluso si la identidad se compromete, el dispositivo se compromete o la red es interceptada, un archivo cifrado con una sensitivity label de alta confidencialidad y protegido con Customer Key sigue siendo técnicamente inaccesible sin las credenciales correctas y los permisos definidos en la política. Purview es el plano de control que garantiza que la seguridad del dato sea independiente de la seguridad de los planos que lo rodean. |
| **Sensitivity Labels como señal de Conditional Access** | La integración entre Purview Information Protection y Conditional Access de Entra ID crea un bucle de control bidireccional entre los planos de identidad y dato. En la dirección Purview → Entra ID, las sensitivity labels aplicadas a documentos se consumen como condición de contexto en políticas de Conditional Access, de modo que el acceso a documentos con labels de alta confidencialidad puede requerir MFA, dispositivo gestionado o ubicación de red específica, aunque el acceso general al tenant no exija esos requisitos. En la dirección Entra ID → Purview, el estado de cumplimiento del dispositivo evaluado por Intune y el nivel de riesgo de la identidad calculado por Entra ID Protection pueden condicionar qué acciones de etiquetado y cifrado están disponibles para el usuario en ese contexto. Esta bidireccionalidad convierte a la combinación Purview + Entra ID en el núcleo integrado del plano de datos y el plano de identidad en una arquitectura Zero Trust coherente. |
| **DLP como enforcement del principio "verify explicitly" en el dato** | El principio "verify explicitly" de Zero Trust establece que cada solicitud de acceso o acción debe autenticarse y autorizarse utilizando todo el contexto disponible. En el plano del dato, Purview DLP implementa este principio: cada acción que un usuario intenta realizar sobre un dato sensible, no solo el acceso, sino también copiar, imprimir, enviar o subir, se intercepta, se analiza contra la política y se permite o bloquea según la combinación de sensibilidad del dato, identidad del usuario, nivel de riesgo del usuario (via Adaptive Protection), estado del dispositivo y destino de la acción. DLP deja de ser un control perimetral centrado en la frontera del tenant y pasa a ser un control de acción continua, con verificación en cada punto de manipulación del dato, que es la diferencia fundamental entre seguridad perimetral y modelo Zero Trust. |

| Concepto | Explicación |
| --- | --- |
| **IRM como señal de confianza dinámica en el modelo Zero Trust** | Zero Trust asume que la confianza es un valor dinámico para cada identidad, no un estado binario fijado en el onboarding. Insider Risk Management es el mecanismo de Purview que materializa este principio en el plano del dato: la puntuación de riesgo de IRM es una medida continua y actualizable del nivel de confianza que se puede depositar en las acciones de un usuario sobre datos sensibles. A través de Adaptive Protection, esta puntuación de riesgo se convierte en una variable de entrada para las políticas DLP, reduciendo la confianza efectiva y endureciendo las políticas cuando el riesgo del usuario aumenta. Esta señal también puede alimentar políticas de Conditional Access en Entra ID, por ejemplo exigiendo reautenticación o MFA adicional a usuarios en estado de riesgo elevado. IRM se convierte así en el motor de ajuste dinámico de confianza del modelo Zero Trust en el plano del usuario. |
| **Audit Premium como plano de verificación del modelo Zero Trust** | El principio "assume breach" exige que la arquitectura permita detectar compromisos, limitar el radio de explosión y reconstruir lo ocurrido. Audit Premium implementa este principio en el plano del dato de M365: la retención de un año de logs de actividad con eventos de alta fidelidad (como MailItemsAccessed, SearchQueryInitiated, FileDownloaded con metadatos completos) proporciona la base forense para reconstruir la secuencia de acciones ejecutadas por un atacante tras comprometer una identidad. La integración de Audit Premium con Microsoft Sentinel como SIEM central permite correlacionar en tiempo casi real las señales de identidad (Entra ID Protection), endpoint (MDE), red (Defender for Cloud), aplicación (MDCA) y dato (Audit). Esto habilita detecciones sobre patrones de comportamiento post-compromiso en el plano del dato tan pronto como hay señales suficientes para generar una alerta. |

# Nivel 3 - Notas de soporte

### Secuencia recomendada de despliegue de Purview en Zero Trust

La implementación de Purview dentro de una arquitectura Zero Trust requiere respetar las dependencias técnicas entre planos. Una secuencia práctica recomendada es:

1. **Identidad primero**
   Completar el despliegue básico de Entra ID con MFA y Conditional Access antes de activar las

integraciones de sensitivity labels con Conditional Access. Si las políticas de Zero Trust en identidad no están maduras, estas integraciones pueden introducir fricciones excesivas para el usuario.

2. **Gestión de dispositivos antes de Endpoint DLP**
   Desplegar Intune con compliance policies para dispositivos antes de activar Endpoint DLP. El agente de Endpoint DLP requiere dispositivos gestionados para operar de forma fiable y para poder aplicar decisiones basadas en el estado de cumplimiento del endpoint.
3. **Information Protection y DLP antes de Adaptive Protection**
   Activar primero Information Protection y las políticas DLP básicas. Solo después habilitar Adaptive Protection, ya que IRM necesita que DLP esté activo para poder ajustar las políticas de manera dinámica según el riesgo detectado.
4. **Audit Premium y Sentinel cuando ya existan señales**
   Integrar Audit Premium con Microsoft Sentinel una vez que los demás componentes estén generando telemetría suficiente. De este modo, el SIEM puede correlacionar los logs de Audit con señales de identidad, endpoint, red y aplicaciones, y producir detecciones significativas en el plano del dato.

### Referencia arquitectónica oficial

La referencia arquitectónica oficial de Microsoft para Zero Trust es el Zero Trust Guidance Center, que incluye:

- El Zero Trust Adoption Framework con fases de despliegue recomendadas.
- Diagramas de integración entre pilares de identidad, endpoint, aplicación, red, infraestructura y datos.
- Guías de configuración específicas por producto.

Dentro de este framework se posiciona explícitamente a Microsoft Purview como el pilar de datos y se documenta cómo contribuye a los principios de "verify explicitly", "use least privileged access" y "assume breach".

### Extensión hacia el plano de riesgo de IA generativa

Este bloque sintetiza los controles técnicos tratados en los planos de identidad, dispositivo, red, aplicación y dato, reencuadrándolos en el modelo Zero Trust con Purview como plano de control del dato.

En una evolución posterior, el plano de riesgo se amplía con la introducción de la IA generativa: por ejemplo, Copilot actúa como un nuevo agente que hereda los permisos del usuario y los controles de Purview, pero añade vectores de exposición que el modelo Zero Trust original no contemplaba. La arquitectura debe considerar a estos agentes de IA como identidades operativas adicionales, sujetas a las mismas dependencias e integraciones entre Purview, Entra ID, DLP, IRM y Audit Premium.

---

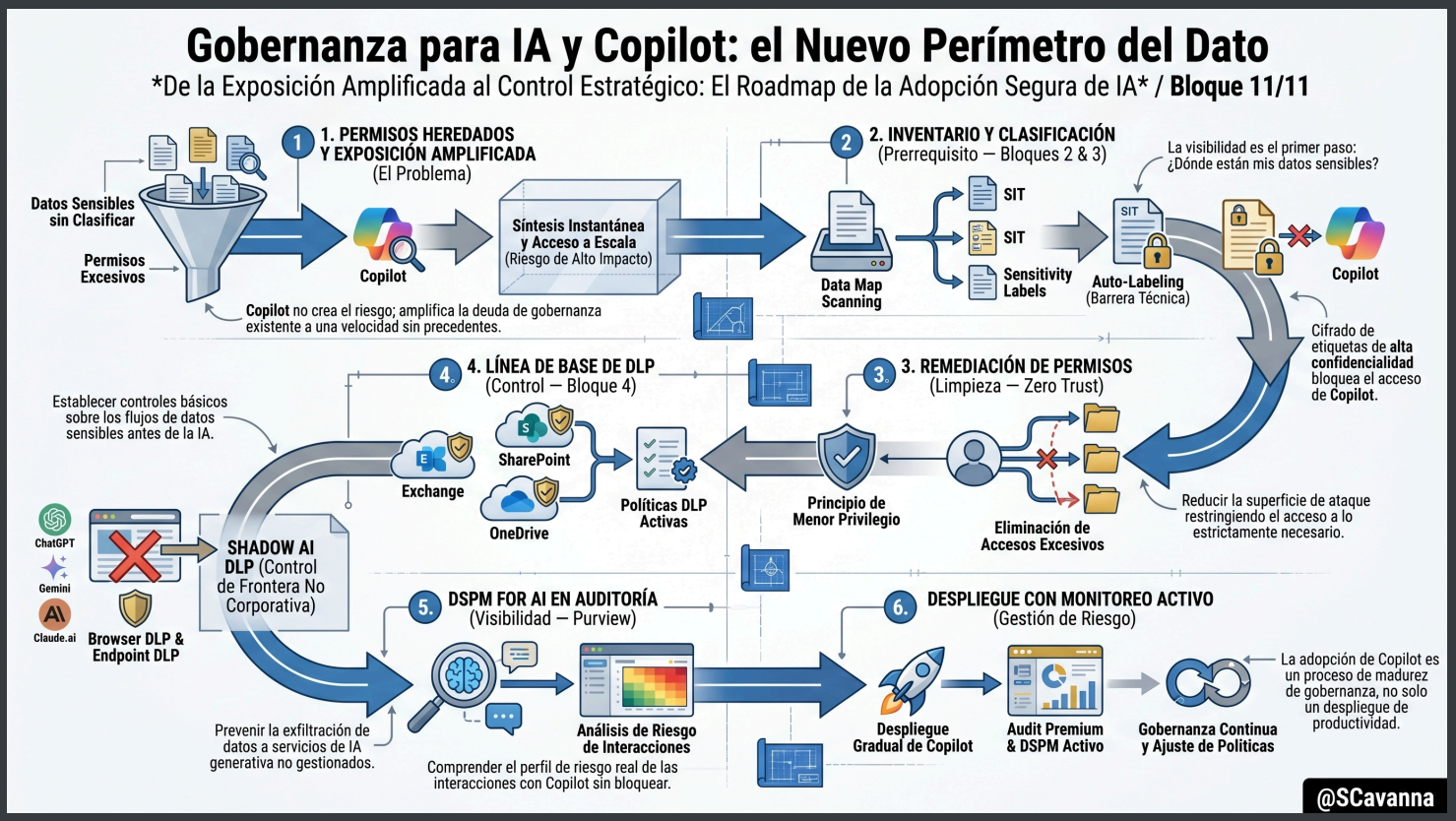
# **11/ -** Gobernanza para IA y Copilot, el nuevo perímetro del dato

## 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

## Conceptos clave

| Concepto | Explicación |
|---|---|
| **El mecanismo de exposición: permisos heredados por Copilot** | Copilot para M365 respeta los permisos del usuario que lo invoca: solo accede y sintetiza contenido al que ese usuario ya tiene permisos en Exchange, SharePoint, OneDrive y Teams, sin acceso privilegiado ni escalamiento de permisos. El riesgo proviene de años de deuda en la configuración de permisos, que hace que muchos usuarios tengan acceso efectivo a mucho más contenido del que usan en la práctica. Antes, encontrar un documento exigía saber que existía o buscarlo de forma explícita; Copilot elimina esa fricción. Una consulta en lenguaje natural puede sintetizar información de decenas de documentos dispersos a los que el usuario tenía acceso teórico pero que nunca habría |

| Concepto | Explicación |
| --- | --- |
| | localizado manualmente. Copilot no rompe el control de acceso, pero convierte todo el acceso posible en acceso fácilmente explotable y de alto impacto. |
| **DSPM for AI: visibilidad del riesgo de datos en IA** | Data Security Posture Management for AI (DSPM for AI) en Microsoft Purview ofrece visibilidad sobre el uso de datos sensibles en interacciones con Copilot y otras herramientas de IA corporativas. Identifica qué tipos de información sensible aparecen en las respuestas de Copilot y qué clasificadores de tipos de información (SIT) se activan, quiénes son los usuarios que generan más respuestas con datos altamente confidenciales, qué prompts de usuario incluyen información sensible que no debería introducirse en estas interfaces y qué sitios de SharePoint aportan el mayor volumen de contenido sensible citado. Funciona inicialmente en modo de auditoría, sin bloquear el uso, para que el equipo de seguridad entienda el perfil de riesgo real antes de aplicar restricciones. La funcionalidad básica de auditoría está disponible en el portal de Purview sin requerir licenciamiento adicional sobre Purview Suite. |
| **Shadow AI DLP: control de la frontera de IA no corporativa** | El riesgo de Shadow AI complementa el de Copilot. Mientras Copilot amplifica la exposición de datos internos dentro del entorno corporativo, las herramientas de IA generativa no corporativas (ChatGPT, Gemini, Claude.ai personal, Mistral, Perplexity y servicios similares accedidos desde el navegador) pueden usarse para exfiltrar datos sensibles hacia servicios externos. Shadow AI DLP extiende Browser DLP y Endpoint DLP de Purview para este escenario: detecta y puede bloquear la carga de archivos etiquetados con sensitivity labels de alta confidencialidad a sitios de IA generativa, el pegado de texto procedente de documentos protegidos en campos de chat de estas herramientas y la descarga a dispositivos de respuestas de IA que contengan información que active tipos de información sensibles. La lista de sitios de IA generativa controlados se actualiza de forma continua mediante la inteligencia de amenazas de Microsoft Defender for Cloud Apps. Esta capacidad requiere tener activos Endpoint DLP y Browser DLP, ambos incluidos exclusivamente en Purview Suite. |

| Concepto | Explicación |
| --- | --- |
| **Sensitivity Labels como barrera técnica en el pipeline de Copilot** | Las sensitivity labels son el mecanismo técnico más directo para limitar la exposición de datos sensibles en Copilot. Copilot respeta el cifrado asociado a las etiquetas: si un documento etiquetado como Altamente Confidencial está cifrado y la política de acceso no incluye al usuario que realiza la consulta, Copilot no puede abrirlo ni citarlo, igual que el propio usuario no puede abrirlo. Por eso, el programa de etiquetado automático de Purview Suite, basado en clasificadores entrenables, es el principal control preventivo para reducir la superficie de exposición. Cada documento que recibe una etiqueta de alta confidencialidad con cifrado aplicado queda fuera del alcance de Copilot para usuarios sin permisos explícitos. El nivel de madurez de Information Protection se traduce directamente en el nivel de riesgo del despliegue de Copilot: una organización con un 80 % de cobertura de etiquetado automático sobre su contenido sensible tiene un riesgo sustancialmente menor que otra que solo etiqueta manualmente un 20 %. |
| **Roadmap de madurez de datos como prerequisito de Copilot** | La preparación para desplegar Copilot a escala debe seguir una secuencia de cinco etapas técnicas con dependencias claras:<br><br>**Etapa 1: Inventario y clasificación.** Activar el escaneo del Data Map y el auto-labeling de Information Protection para conocer el porcentaje de contenido clasificado y el perfil de sensibilidad del patrimonio documental.<br>**Etapa 2: Remediación de permisos.** Usar los insights del Data Map y de Information Protection para identificar y corregir el sobre-acceso, en especial contenido Confidencial o Altamente Confidencial accesible por Toda la organización o por grupos demasiado amplios.<br>**Etapa 3: Línea de base de DLP.** Implementar políticas de DLP sobre Exchange, SharePoint y OneDrive antes de activar Copilot para disponer de una línea base de los flujos de datos sensibles.<br>**Etapa 4: DSPM for AI en auditoría.** Activar DSPM for AI en modo de auditoría durante 30 a 60 días antes del despliegue masivo de Copilot para entender el perfil de riesgo de las primeras interacciones.<br>**Etapa 5: Despliegue con monitoreo activo.** Desplegar Copilot en grupos de usuarios controlados con Audit Premium y DSPM for AI activos, y escalar gradualmente según se verifique que el perfil de riesgo resultante es aceptable.<br><br>Esta secuencia convierte el despliegue de Copilot en un proceso de gestión de riesgo, no solo en un proyecto de productividad. |

# Notas de soporte

## Implicaciones regulatorias y contractuales

La relación entre la madurez de implementación de Purview y el riesgo de Copilot tiene implicaciones contractuales y regulatorias. En jurisdicciones con obligaciones de protección de datos activas (como GDPR, la Ley 25.326 en Argentina o la LGPD en Brasil), el procesamiento de datos personales mediante herramientas de IA generativa puede requerir una evaluación de impacto de privacidad adicional (DPIA o EIPD) si el nuevo alcance de procesamiento habilitado por Copilot es materialmente diferente del propósito original para el que se recopilaron los datos.

La posición oficial de Microsoft es que Copilot para M365 procesa los datos dentro del tenant del cliente y no los utiliza para entrenar los modelos de Microsoft. No obstante, cada organización debe verificar, contextualizar y documentar esta postura en función de sus propias bases legales de tratamiento, políticas de privacidad y obligaciones de transparencia y responsabilidad.

## Visibilidad y responsabilidades operativas

Es fundamental distinguir DSPM for AI de las capacidades de seguridad integradas en Copilot, como Microsoft 365 Copilot usage reports o el Copilot Dashboard en Viva Insights. Las herramientas nativas de Copilot ofrecen métricas de uso y productividad; DSPM for AI, en cambio, ofrece visibilidad sobre el perfil de riesgo de datos asociado a ese uso.

Son capacidades complementarias con objetivos distintos que suelen corresponder a equipos diferentes: IT y adopción orientados a habilitar y medir el uso, y seguridad y cumplimiento orientados a gestionar el riesgo y la conformidad regulatoria.

## Evolución de capacidades

La funcionalidad de DSPM for AI y de Shadow AI DLP evoluciona en ciclos de actualización acelerados a lo largo de 2025 y 2026. La referencia técnica actualizada se mantiene en la documentación oficial de Microsoft Purview para capacidades de IA, que se actualiza con cada ciclo de lanzamiento del producto.

La descripción incluida aquí refleja el estado de la plataforma a comienzos de 2026 y debe revisarse periódicamente contra la documentación oficial para alinear la arquitectura de seguridad y cumplimiento con las capacidades disponibles.

## Dependencias con otros controles de protección de datos

Los controles de Data Map, Information Protection, DLP y la arquitectura Zero Trust son prerequisitos concretos y secuenciados para reducir el riesgo de datos en despliegues de IA generativa corporativa. El nivel de madurez alcanzado en cada uno de estos dominios determina directamente el perfil de riesgo del despliegue de Copilot: no existe un atajo que permita saltarse la gobernanza del dato para acelerar la obtención de beneficios de productividad con IA.