Seguridad de Microsoft

# Protección de datos con Microsoft Purview: un manual práctico

**Comience con un enfoque dinámico para proteger los datos, poniendo énfasis en la integración de personas, procesos y tecnología en línea con los procedimientos recomendados de Microsoft**

**Este recurso está diseñado para los líderes de seguridad que buscan mejorar la seguridad de los datos de su empresa a través de un enfoque holístico basado en los procedimientos recomendados derivados de la amplia experiencia de los expertos de Microsoft y los conocimientos de los clientes.**

En este manual se hace hincapié en los elementos críticos entre las personas, los procesos y la tecnología que le permitirán proteger los activos de datos más valiosos de su organización. Podrá comprender cómo integrar los datos y el contexto del usuario en sus aplicaciones, servicios, dispositivos y herramientas de IA generativa en la nube.

En primer lugar, explorará los procedimientos recomendados de Microsoft para prepararse para proteger sus datos, entre los que se incluyen:

- Identificar sus requisitos de seguridad de los datos
- Formular una estrategia sólida
- Involucrar a las partes interesadas multifuncionales
- Determinar la tolerancia al riesgo de su organización
- Implementar controles de seguridad
- Comprometerse con la mejora continua

En las siguientes secciones del manual se describe el enfoque recomendado para implementar Microsoft Purview, que abarca:

- Evaluar su entorno de datos
- Comprender y preparar sus datos
- Ajustar y revisar sus directivas
- Mejorar los escenarios de seguridad de datos y configurar la Protección adaptativa

# Contenido

# Introducción

Los desafíos de seguridad de datos son únicos para cada organización, conformados por factores como los requisitos reglamentarios, los volúmenes de datos y la complejidad de los diferentes entornos de TI. Ya sea que se embarque en su viaje de seguridad de datos, pasando de una solución anterior o mejorando un programa establecido, desarrollar una estrategia sólida y adaptable es esencial para proteger la información confidencial de manera eficaz.

En este contexto, la seguridad de los datos implica no solo proteger la información, sino también comprender dónde residen los datos, clasificarlos con precisión y comprender las actividades de los usuarios para garantizar un acceso y uso responsables. Se trata de crear un marco que administre y gobierne los datos de manera holística, para que las organizaciones puedan cumplir con confianza los estándares de cumplimiento, mantener la confianza del usuario y mitigar los riesgos.

Obtenga más información sobre la seguridad de los datos y los riesgos a los que sus datos podrían ser vulnerables.

Esta guía representa la experiencia de Microsoft, desarrollada a través de años de trabajo estrecho con los clientes para superar estos desafíos y optimizar sus prácticas de seguridad de datos. Con base en experiencias reales, esta guía le llevará paso a paso a través de la maximización de las capacidades de seguridad de datos de Microsoft Purview, desde las primeras etapas de planificación hasta la mejora continua y la excelencia operativa sostenida.

**Al leer esta guía, aprenderá a hacer lo siguiente:**

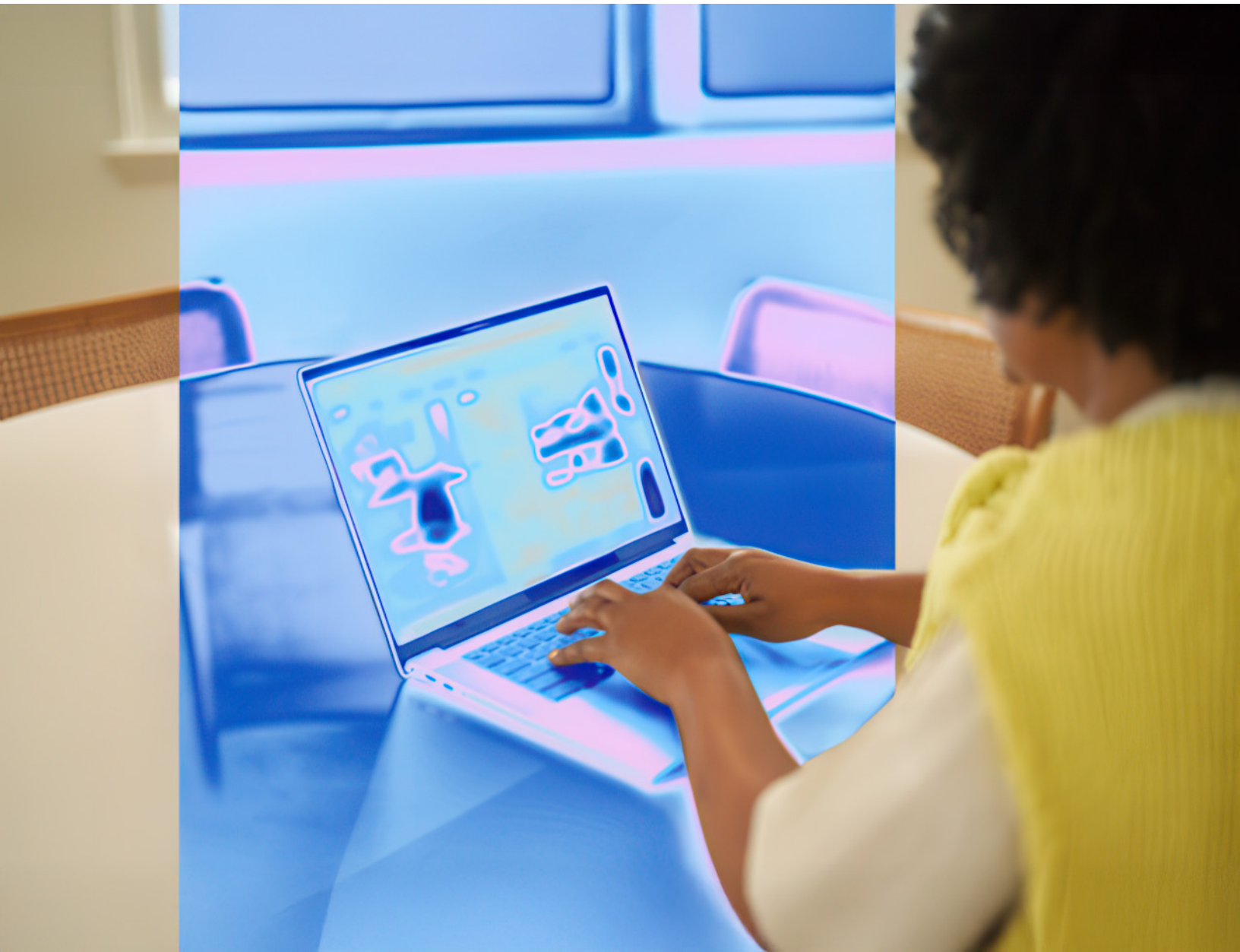
- Comenzar poco a poco y generar impulso con su implementación.
- Diseñar un plan de participación de las partes interesadas multifuncional para optimizar la cooperación.
- Determinar su tolerancia al riesgo.
- Equilibrar los controles de seguridad con la productividad del usuario final.

Esta guía se creó para ayudar a los equipos de seguridad de datos a operacionalizar el programa y las tareas al adoptar Microsoft Purview. Siga leyendo para profundizar en este importante tema, incluidos los seis pasos para preparar a su organización, las cuatro fases de implementación de la seguridad de datos, así como la solución de problemas y la optimización después de la implementación.

# Preparación para proteger sus datos

Casi todos los principios de seguridad de datos se centran en tres objetivos principales: garantizar la disponibilidad de datos para un uso debidamente examinado, descubrir y proteger la confidencialidad de los datos confidenciales, y preservar la integridad de los datos. Sin embargo, la implementación de una seguridad de datos eficaz va más allá de la mera implementación de tecnología; se trata de un esfuerzo combinado que requiere que personas, procesos y tecnología trabajen de manera fluida. Establecer procesos claros, capacitar a sus equipos y alinear la tecnología con los objetivos organizacionales pueden ayudar a crear una postura de seguridad de datos resiliente y adaptable.

Con la implementación de cualquier nueva tecnología, una preparación adecuada puede ayudarlo a evitar obstáculos importantes y conducir a una mayor eficiencia y valor para su organización de cara al futuro. En esta sección, encontrará seis pasos clave que debe seguir antes de implementar Microsoft Purview.



# Defina sus objetivos

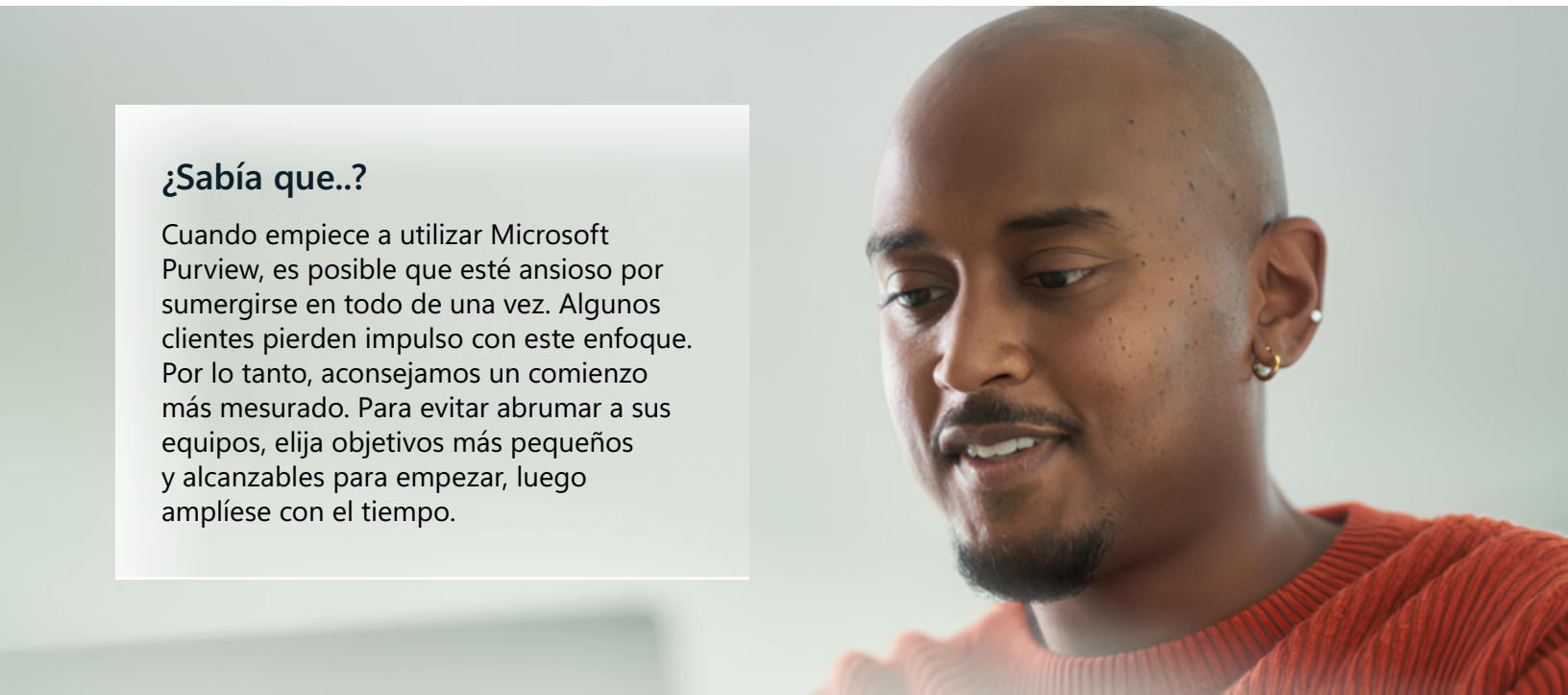
Para iniciar la operacionalización de la seguridad de datos con Microsoft Purview, entender sus objetivos puede ser de utilidad para formar el marco de su viaje de seguridad de datos. ¿Cuáles son los mayores desafíos de datos para su organización? ¿Cuáles son sus principales necesidades empresariales? ¿Cuáles son sus oportunidades más emocionantes? Recomendamos que comience con objetivos que sean prácticos, alcanzables y que prometan un impacto rápido para impulsar una mayor adopción y cobertura de seguridad de datos.

Aquí hay algunas otras consideraciones para guiar la base de sus objetivos de seguridad de datos:

- **Viaje de seguridad preferido:** Diferentes equipos y organizaciones pueden optar por administrar la seguridad de sus datos de distintas maneras con diferentes soluciones o rutas personalizadas para lograr sus objetivos. Este recorrido se adapta a las necesidades específicas, los recursos, la tolerancia al riesgo y los niveles de madurez de cada organización. Como la seguridad de los datos no es una solución universal que sirva para todos, diferentes organizaciones priorizarán e implementarán controles de seguridad de la manera que mejor se alinee con sus necesidades operativas y su panorama de riesgos.
- **Madurez de seguridad de los datos:** Comprender en qué lugar de su viaje de seguridad de datos se encuentra lo ayuda a identificar cuáles deberían ser sus prioridades iniciales, sentando las bases para implementar y poner en funcionamiento una solución de seguridad de datos. ¿Cómo trabajan en conjunto los distintos sectores dentro de su organización para tomar decisiones relacionadas con temas de seguridad de datos? ¿Qué tecnologías y procesos actuales debe tener en cuenta? ¿Qué capacitación potencial necesita mi organización?
- **Participantes de la iniciativa:** Evalúe quién debe participar en la preparación de esta implementación y cómo pueden contribuir mejor a la creación de los objetivos de seguridad de datos de su organización. ¿Qué equipos y departamentos deben ser conscientes, participar o responsabilizarse de los distintos aspectos de la seguridad de los datos? ¿Qué personas debería considerar involucrar o ya están involucradas y son responsables de la seguridad de los datos dentro de su organización? Esto le ayudará a identificar qué partes interesadas influirán en este proceso de operacionalización.
- **Objetivos empresariales:** Defina cada objetivo pensando en cómo lograrlo satisfará sus necesidades empresariales.

## ¿Sabía que..?

Cuando empiece a utilizar Microsoft Purview, es posible que esté ansioso por sumergirse en todo de una vez. Algunos clientes pierden impulso con este enfoque. Por lo tanto, aconsejamos un comienzo más mesurado. Para evitar abrumar a sus equipos, elija objetivos más pequeños y alcanzables para empezar, luego amplíese con el tiempo.



# Determine su enfoque

Comience con los principios de seguridad por defecto para preparar su organización para el éxito con Microsoft Purview. Cuando su estrategia de seguridad de datos se basa en el modelo de seguridad de Confianza cero, sus procesos y directivas admitirán una protección de datos más sólida, una detección y corrección más rápidas y una mejor contención de las vulneraciones de datos.

- Considere sus principales procesos y servicios empresariales que necesitan cobertura y visibilidad de seguridad de datos.
- Comprenda los diferentes requisitos de seguridad de datos de las distintas regiones del mundo en las que opera su organización.
- Determine la manera en que su organización educará a las partes interesadas, el personal y terceros sobre la clasificación de datos, las formas más seguras de interactuar con datos confidenciales, y los controles preventivos y las medidas de protección.

## Planificación de la tecnología

Supervise y proteja sus datos en reposo, los datos en uso y los datos en movimiento en los servicios de Microsoft 365, dispositivos Windows 10, Windows 11 y macOS (las tres versiones más recientes), los recursos compartidos de archivos locales y SharePoint local. Existen implicaciones de planificación para las diferentes ubicaciones, el tipo de datos que desea supervisar y proteger, y las acciones que se deben tomar cuando se produce una coincidencia de directiva.

## Planificación de los procesos empresariales

Las directivas pueden impedir que los usuarios realicen actividades prohibidas, como compartir de forma inapropiada información confidencial por correo electrónico. A medida que planifique sus directivas de seguridad de datos, tiene que identificar los procesos empresariales que afectan a sus elementos confidenciales. Los propietarios de procesos empresariales pueden ayudarle a identificar los comportamientos adecuados del usuario que deben permitirse y los comportamientos inapropiados del usuario contra los que se debe proteger. Debe planificar las directivas e implementarlas en modo de simulación y evaluar su impacto antes de ejecutarlas en modos más restrictivos.

## Planificación de la cultura organizativa

La implementación exitosa de un programa de seguridad de datos depende tanto de que sus usuarios estén capacitados y se aclimaten a las prácticas de prevención de pérdida de datos (DLP) como de directivas bien planificadas y ajustadas. Dado que sus usuarios están muy involucrados, asegúrese de planificar la capacitación para ellos también. Puede utilizar estratégicamente la información sobre directivas para sensibilizar a los usuarios antes de cambiar el estado de la directiva del modo de simulación a modos más restrictivos.

### El desafío del equilibrio

Equilibrar la productividad de los empleados con las necesidades de seguridad de datos es un desafío continuo. Cuando las organizaciones establecen su tolerancia al riesgo o sufren un incidente, es posible que deseen implementar directivas generales o integrales, como cifrar todos sus datos en OneDrive o bloquear todo el intercambio de datos con correos electrónicos externos. Sin embargo, la implementación de directivas basadas únicamente en ciertos patrones de seguridad de datos puede ser perjudicial para los resultados del negocio y provocar la insatisfacción y la ineficiencia de los empleados. Antes de que se establezcan directivas, se deben entender claramente las necesidades de la empresa y, con ese entendimiento, la seguridad puede mantenerse sin sorprender a los líderes empresariales ni interrumpir los flujos de trabajo empresariales establecidos. Este desafío también puede abordarse con soluciones que refuerzan dinámicamente las protecciones basadas en diferentes niveles de comportamiento de riesgo, como la Protección adaptativa en Microsoft Purview, que abordaremos más adelante en esta guía.

# Comprenda su tolerancia al riesgo de datos y los elementos no negociables

Comprender su tolerancia al riesgo, así como sus no negociables en materia de seguridad de datos puede ayudarlo a encontrar la combinación correcta de directivas de seguridad y cobertura para su organización. A continuación, puede ponerse en contacto con las partes interesadas designadas para validar el riesgo y los supuestos no negociables, a fin de asegurarse de que se encuentra en el camino correcto para proteger sus datos y de que también está alineado con otras áreas de la organización.

Otras consideraciones críticas que juegan un papel en este proceso incluyen:

- Determinar qué considera su organización como datos confidenciales. Reconozca que, para la mayoría de las organizaciones, solo una parte de los datos es verdaderamente confidencial; la mayoría de las veces (pero no siempre), los datos confidenciales incluyen información de identificación personal (PII), datos de recursos humanos, datos financieros, proyectos confidenciales o datos relacionados con la investigación y el desarrollo o la propiedad intelectual de su negocio.
- Desarrollar estrategias sobre cómo proteger los datos sin bloquear las iniciativas comerciales. Algunas organizaciones, por ejemplo, consideran que la protección a nivel de servidor y contenedor para sus flujos de trabajo sensibles es la forma más fácil de equilibrar la seguridad y la accesibilidad.
- Decidir qué nivel de riesgo es apropiado o tolerable para su organización. Si bien algunas organizaciones no pueden tolerar mucho riesgo, otras prefieren centrarse en la detección de riesgos específicos para evitar abrumar a los miembros del equipo o crear una fatiga de alerta innecesaria. La tolerancia al riesgo de su organización puede estar en algún punto entre estos dos extremos del espectro.
- Establecer y socializar directivas sobre cuándo se bloquearán las iniciativas empresariales para protegerse contra amenazas a la seguridad de los datos. La transparencia en torno a sus estándares de seguridad de datos puede ayudar a educar y gestionar el compromiso de los equipos.

### ¿Sabía que..?

Muchas organizaciones carecen de una comprensión sólida de dónde residen sus datos confidenciales y qué actividades potencialmente riesgosas pueden estar ocurriendo. Un buen lugar para comenzar es con los datos en Microsoft 365, correo electrónico, SharePoint, Teams y OneDrive. Centre sus esfuerzos en identificar las ubicaciones donde se encuentran su información financiera, propiedad intelectual y registros de recursos humanos.

# Comprometa a un equipo multifuncional

Si bien las necesidades de cada organización difieren, cada empresa necesita incluir un equipo multifuncional para lograr la alineación y generar impulso para la adopción generalizada de medidas de seguridad de datos. Para obtener resultados óptimos, tenga en cuenta los siguientes pasos clave:

**Identifique a las partes interesadas clave:** Conéctese con representantes de cada área de importancia para la seguridad de datos de su organización y para quienes su programa de seguridad de datos podría tener más impacto. A un alto nivel, el equipo podría incluir representantes de riesgo y cumplimiento (privacidad), seguridad, administración del ciclo de vida de los datos, TI, equipos de negocio, jurídico y recursos humanos. Considere incluir un rol de administración de proyectos para cronometrar y programar, hacer seguimiento del progreso de los hitos y la comunicación. A la hora de decidir quién es el mejor representante de cada área de especialización, busque personas que tengan un conocimiento profundo de qué datos deben protegerse. Será importante involucrar a las partes interesadas en el proceso y tener en cuenta las necesidades y preocupaciones de sus equipos al desarrollar la estrategia de seguridad de datos.

**Determine el nivel de interacción:** Establezca qué representantes tienen que estar informados, involucrados, comprometidos profundamente y cuáles tienen que formar parte de los procesos de aprobación y alineación de las directivas. Considere la cadencia del compromiso y con qué eventos importantes tiene sentido alinearse (muchas organizaciones alinean el compromiso con sus requisitos continuos de cumplimiento y presentación de informes).

**Eduque a todos los equipos:** Al acercarse a posibles miembros del equipo, comparta con ellos por qué la organización está adoptando Microsoft Purview. Comparta cómo la implementación afectará a la empresa, a su equipo y el rol que tienen que desempeñar durante la implementación y más allá. Comprender los posibles escenarios de riesgo y vulnerabilidades de los datos, así como la "visión" de seguridad de datos, ayudará a lograr que las partes interesadas acepten su estrategia de seguridad de datos.

Nota: El liderazgo ejecutivo puede ayudar a establecer el tono sobre la importancia de su equipo multifuncional.

**Prevea obstáculos y limitaciones:** Estructure su equipo de partes interesadas para que se ajuste a los retos y objetivos específicos de su organización y asegúrese de que existen planes de contingencia para las transiciones, como cuando una parte interesada se marcha o necesita ceder responsabilidades. Establezca un plan claro y viable con hitos alcanzables para fomentar el compromiso y la alineación en todo su equipo multifuncional desde el principio.

Las posibles preocupaciones y necesidades de las partes interesadas podrían ser:

| Riesgo y cumplimiento | Seguridad | TI | Legal | Recursos Humanos | Gerente de negocios |
|---|---|---|---|---|---|
| *"Tengo que asegurarme de que cumplimos todos los compromisos empresariales y normativos".* | *"Soy responsable de proteger todos nuestros datos más sensibles".* | *"Gobernamos y mantenemos todos los aspectos del entorno de Microsoft 365".* | *"Necesito descubrir todo el contenido relevante de manera oportuna para las solicitudes e investigaciones".* | *"Necesito conocer las repercusiones para nuestros empleados y capacitarlos para que cumplan las nuevas directivas".* | *"Necesito una estrategia de seguridad de datos que proteja nuestros resultados empresariales y nuestra reputación sin afectar a la productividad".* |

## ¿Cuántas personas necesitamos para la implementación?

El tamaño y la estructura de su organización importan bastante a la hora de determinar cuántos miembros del equipo deben encargarse de la implementación y el mantenimiento de Microsoft Purview.

Al dimensionar los equipos de seguridad de datos, las organizaciones deben considerar el alcance y la complejidad de su entorno de datos, así como los requisitos regulatorios y de cumplimiento específicos, que a menudo determinan el nivel de personal especializado necesario. El tamaño del equipo debe estar alineado con la madurez de seguridad de la organización: los equipos establecidos pueden enfocarse en la optimización, mientras que los equipos más nuevos necesitan recursos para construir procesos fundamentales. Además, el perfil de riesgo y el panorama de amenazas son factores esenciales, y las industrias de mayor riesgo requieren roles dedicados para la detección y respuesta proactivas.

Aprovechar la tecnología y la automatización, como Microsoft Purview, puede agilizar las tareas rutinarias, lo que permite que los equipos se concentren en iniciativas estratégicas. La colaboración interdisciplinaria también es crucial, ya que la seguridad de los datos a menudo involucra TI, legal, cumplimiento y operaciones.

Por último, las proyecciones de crecimiento deben informar la estructura del equipo para garantizar la escalabilidad a medida que evolucionan las necesidades de los datos y la organización. Un equipo bien equilibrado considera todos estos aspectos para satisfacer las demandas de seguridad inmediatas mientras se mantiene adaptable a los desafíos futuros.

# Defina cómo se ve el éxito para su organización

No puede medir su éxito con Microsoft Purview sin saber primero cómo se ve el éxito para usted. Las organizaciones deben decidir de antemano métricas claras para evaluar la efectividad de su implementación de Microsoft Purview, lo que facilitará la identificación de oportunidades de mejora en el futuro. Documentar su "por qué" para cada logro deseado puede ayudar a facilitar la transferencia de conocimientos cuando un miembro individual del equipo se va, para que los nuevos miembros del equipo sepan por qué existe cada directiva y por qué se implementó una estrategia. Ejemplos de métricas de éxito incluyen:

**El porcentaje de datos confidenciales clasificados:** La proporción de datos confidenciales que se han identificado y etiquetado del conjunto de datos total.

**Confirmaciones de alerta:** El número de alertas de seguridad que se han revisado y confirmado como incidentes reales.

**La relación entre falsos positivos y detecciones verdaderas:** Una medida de la precisión del sistema de seguridad, que indica cuántas alertas falsas se generan en comparación con amenazas reales.

**El número de incidentes de pérdida de datos detectados:** El recuento de eventos en los que se identificaron datos confidenciales como potencialmente filtrados o a los que se accedió de manera no autorizada.

**El número de incidentes de pérdida de datos evitados:** El recuento de intentos de filtración de datos bloqueados con éxito por las medidas de seguridad.

**La finalización del piloto:** Indica si una ejecución de prueba del programa de seguridad o una medida de seguridad específica se ha finalizado correctamente.

**La creación de directivas de implementación:** El desarrollo de directrices y reglas para la implementación de medidas de seguridad en toda la organización.

**Cargas de trabajo completadas:** El número de tareas o procesos relacionados con el programa de seguridad que se han finalizado.

La conclusión es que, a la hora de determinar sus métricas de éxito, busque lo que le quita el sueño y resuelva primero los mayores riesgos para la organización. Y siempre puede modificar o agregar a sus métricas de éxito a medida que cambian los desafíos de seguridad de datos y el nivel de madurez de su organización.

# Requisitos previos y por dónde empezar

Microsoft Purview es un conjunto integral de soluciones que pueden ayudar a su organización a proteger y administrar datos, dondequiera que residan.

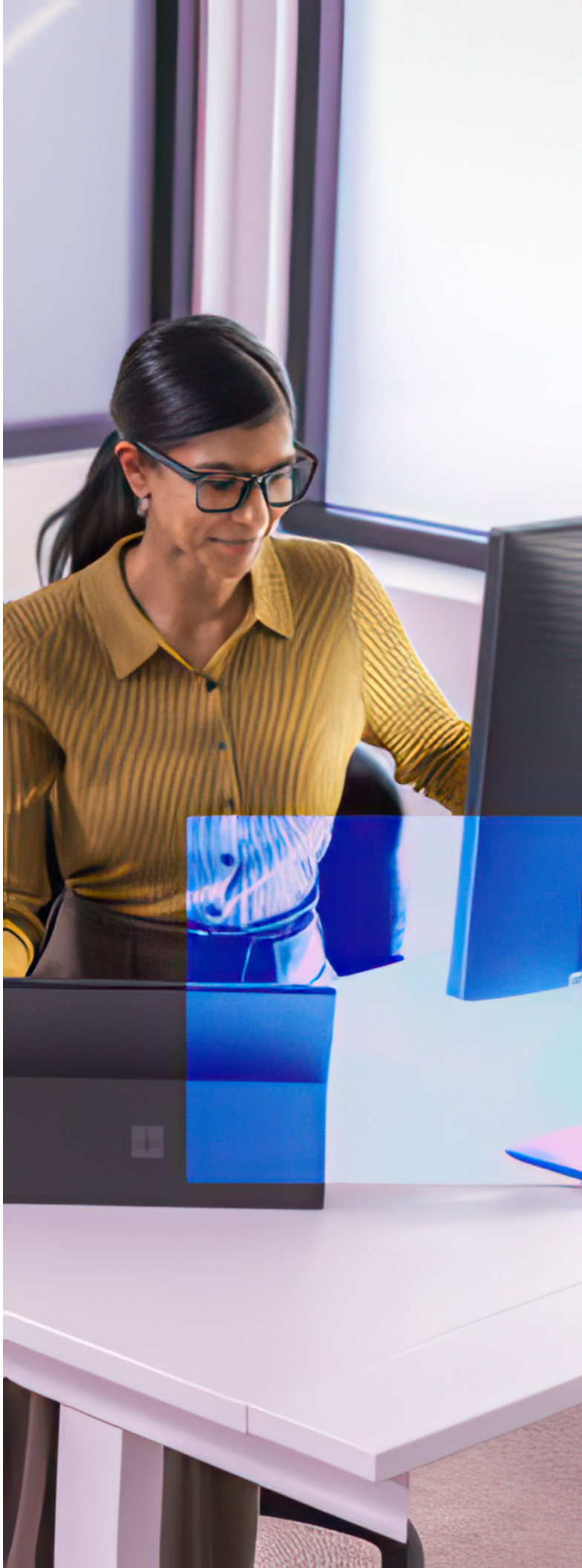
## Requisitos previos comunes

- **Incorporación de dispositivos:** Este es un paso importante para las cargas de trabajo de DLP y la Gestión de riesgos internos, sobre todo para la primera en lo que se refiere a DLP de punto de conexión.
- **Revisión de la extensión del navegador:** Este requisito previo puede ayudarle a obtener visibilidad sobre cómo se comparte la información confidencial y aplicar directivas de DLP de punto de conexión para advertir o impedir que los usuarios compartan en exceso información confidencial.
- Requisitos específicos de los entornos locales.
- Requisitos previos no tácticos, como la capacitación de los usuarios en la forma de etiquetar sus documentos.

## Dónde empezar

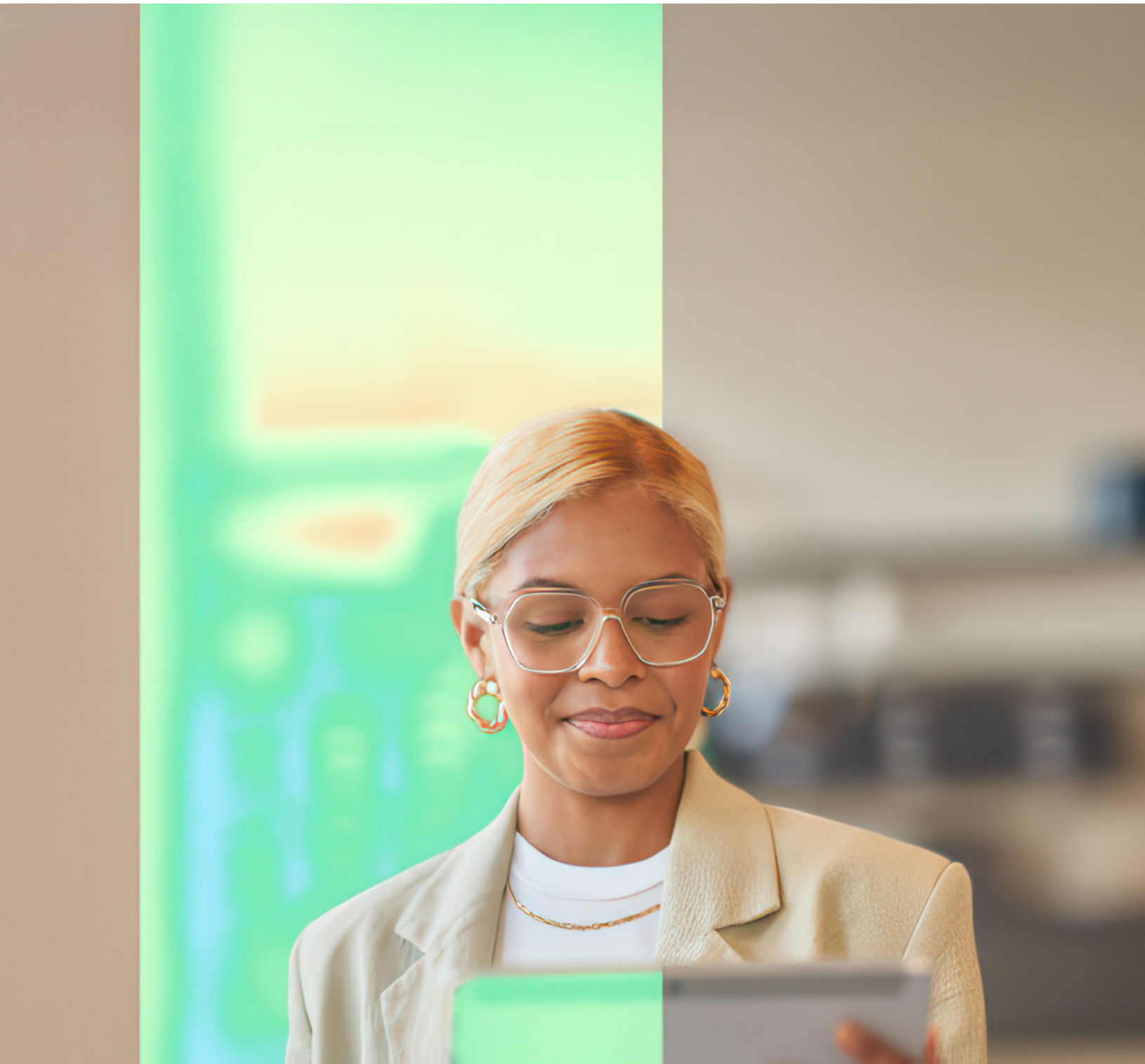
Cada organización elegirá sus propias prioridades, pero estos son algunos ejemplos de por dónde empiezan las organizaciones para ayudarle a determinar por dónde comenzar su propia implementación de Microsoft Purview.

- **Piloto corto:** Elija una carga de trabajo de datos o un tipo de datos que se preste a un piloto a corto plazo, idealmente de cuatro a seis semanas desde el principio hasta el hito clave completado.
- **Por directiva:** Implemente primero una directiva clave, luego analice y ajústela con el tiempo.
- **Por carga de trabajo:** Comience con el correo electrónico o Teams, SharePoint o OneDrive.
- **Conector de RR. HH.:** Elija un tipo de datos de Recursos Humanos para importar según la plantilla de directiva específica que desee implementar.



# Optimización de la implementación de Microsoft Purview

Ha completado la planificación preliminar y está listo para empezar a beneficiarse de las capacidades de Microsoft Purview para proteger sus datos. Pero, ¿qué implica eso? En esta sección, compartiremos un plan de acción de cuatro fases para operacionalizar y comenzar con Microsoft Purview.



# Evaluación

Así como comienza a crear los objetivos para su estrategia de seguridad de datos con Microsoft Purview, debe comenzar a evaluar su entorno en pasos breves y prácticos. También puede comenzar a involucrarse e interactuar con las partes interesadas previamente identificadas para validar los resultados que podrían surgir desde la comprensión inicial de su entorno de datos.

A través de la evaluación, comenzará a trabajar con las tres soluciones principales de seguridad de datos de Microsoft Purview:

**Microsoft Purview Information Protection (IP):** Permite a las organizaciones descubrir, clasificar, etiquetar y proteger la información confidencial, garantizando que la protección siga a los datos dondequiera que residan o se muevan.

**Prevención de pérdida de datos (DLP) de Microsoft Purview:** Ayuda a cumplir con los estándares empresariales y las regulaciones de la industria al identificar, monitorear y asegurar automáticamente la información confidencial en varios entornos de datos.

**Gestión de riesgos internos (IRM) de Microsoft Purview:** Ayuda a reducir los riesgos internos al detectar, investigar y actuar sobre actividades potencialmente riesgosas dentro de la organización, aprovechando las señales de la actividad del usuario, los sistemas de recursos humanos y otras fuentes contextuales.

Entraremos en más detalles sobre cómo trabajará con cada una de las soluciones en la siguiente fase del proceso.

**Etapa de iniciación:** La primera etapa consiste en comenzar a evaluar dónde se encuentra su organización hoy en día con respecto a la seguridad de la información y el cumplimiento con su objetivo de definir una dirección estratégica para su organización. El uso de esta estrategia favorecerá la adopción de una solución al reunir los requisitos de los sistemas de soporte, el impacto en los usuarios finales y el conjunto de habilidades necesarias para cada titular de rol. La fase inicial describe los pasos que debe dar al principio de cualquier implementación, tanto si los requisitos son básicos como avanzados. Incluye los pasos para la educación del producto, la definición de requisitos y la evaluación o prueba.

Como parte de la fase de evaluación de su organización, considere las siguientes tareas e ideas:

- **Analice los datos procesados en el entorno:** Para hacer esto, diríjase al portal de Microsoft Purview, donde puede encontrar detalles en las pestañas del explorador de actividades y del explorador de contenido. Si no encuentra lo que necesita allí, explore el escáner local para obtener más información.
- **Prepare la clasificación de datos:** Identifique tipos de información confidencial, asigne ubicaciones de datos y acceda al explorador de contenido para comprender la clasificación de sus datos.
- **Implemente el escáner de la protección de la información:** Configure un Windows Server con los permisos necesarios, instale el escáner, configure los trabajos de análisis y ejecute análisis en repositorios de datos clave.
- **Revise y proteja los datos:** Analice los resultados del análisis en el explorador de actividades para aplicar las directivas de protección adecuadas, como etiquetas de confidencialidad o DLP, según los hallazgos.

- **Active los análisis en la Gestión de riesgos internos:** Este proceso es transparente y lleva a cabo una evaluación de los posibles riesgos de información privilegiada en su organización sin configurar ninguna directiva de riesgos de información privilegiada. También proporciona orientación en tiempo real sobre la configuración de los ajustes del umbral del indicador.
- **Entreviste a propietarios de procesos empresariales y profesionales de análisis de procesos para recopilar casos de uso de seguridad de datos relevantes:** Anime a los propietarios de empresas y servicios a enumerar la información más importante que debe identificarse y protegerse en sus procesos (por ejemplo, tarjeta de crédito, IBAN, número de contrato, orden de compra, currículum vitae o CV, propuesta de proyecto, planos o propiedad intelectual).
- **Concientice:** Informe a los empleados sobre las capacidades de seguridad de datos de Microsoft Purview mediante el desarrollo de manuales de usuario y permita que los usuarios empresariales y no técnicos se sientan seguros con el uso de la solución.
- **Ajuste el uso de datos y desarrolle expectativas coherentes en torno a una estrategia de etiquetado de confidencialidad:** El etiquetado es una de las principales preocupaciones de muchos clientes, y le recomendamos que sea minucioso en la identificación de sus datos confidenciales. La mayoría de los datos confidenciales están relacionados con la propiedad intelectual de una organización: investigación y desarrollo, finanzas o liderazgo.

Si es cliente de cumplimiento de ME5 o E5, también tiene la valiosa oportunidad de activar la Administración de postura de seguridad de datos (DSPM) de Microsoft Purview.

DSPM ofrece visibilidad de los riesgos de seguridad de los datos y recomienda controles para protegerlos, lo que ofrece información contextual sobre los datos y su uso, así como una evaluación continua de riesgos de su panorama de datos en evolución, y ayuda a mitigar los riesgos de datos y fortalecer su postura de seguridad de la información.

- **Participación en el procesamiento analítico:** Para empezar a trabajar con DSPM (versión preliminar), debe habilitar y participar en:
  - Análisis de la Gestión de riesgos internos.
  - Análisis de DLP.
  - Procesamiento analítico en DSPM (versión preliminar) para el análisis en busca de datos no protegidos en su organización.
- **Evalúe la información y tome medidas:** Una vez completado el procesamiento de análisis automatizado, puede evaluar la información creada por DSPM (versión preliminar) para ayudar a mitigar los riesgos de los datos desprotegidos.
- **Acciones:**
  - Investigue con Seguridad de Copilot: Utilice mensajes integrados y personalizados con Seguridad de Copilot para ayudar a identificar áreas específicas de riesgo.
  - Cree directivas con recomendaciones: Utilice las recomendaciones para crear rápidamente directivas de Gestión de riesgos internos y DLP que ayuden a mitigar los riesgos de seguridad de los datos de los activos de datos no protegidos.
- **Realice un seguimiento de la postura con tendencias e informes analíticos:** Use tendencias e informes analíticos para ver su posición a lo largo del tiempo y para las ubicaciones de los datos en toda su organización.
  - Para las organizaciones que comienzan con Microsoft Purview, DSPM (versión preliminar) simplifica la configuración y la creación de directivas en soluciones de seguridad de datos. Analiza los datos automáticamente, proporcionando información de referencia y recomendaciones para datos no protegidos, lo que ayuda a una configuración rápida en DLP, protección de la información y Gestión de riesgos internos.
  - Para los usuarios existentes de estas soluciones, DSPM (versión preliminar) identifica cualquier brecha en la cobertura actual de la directiva, donde destaca los datos no protegidos que están en riesgo sin la necesidad de una revisión y prueba exhaustivas de la directiva.

# Comprenda y prepare sus datos

En las primeras semanas después de la adopción, tómese el tiempo para preparar sus datos explorando las soluciones de seguridad de datos dentro de Microsoft Purview. Dentro de los primeros 30 días, trate de completar las tareas de preparación de datos críticas:

**Cumplimiento y requisitos normativos:** Revise los requisitos del Reglamento General de Protección de Datos (RGPD) de la Unión Europea, la Ley de Protección de Información Personal y Documentos Electrónicos, la Ley de Transferencia y Responsabilidad de Seguros de Salud (HIPAA) y evalúe estos reglamentos según la región donde opera su organización. Asegúrese de que está reforzando las directivas correctas de retención, acceso y uso de datos.

**Propiedad y clasificación de los datos:** Asigne administradores de datos y clasifique los datos como públicos, internos, confidenciales o restringidos.

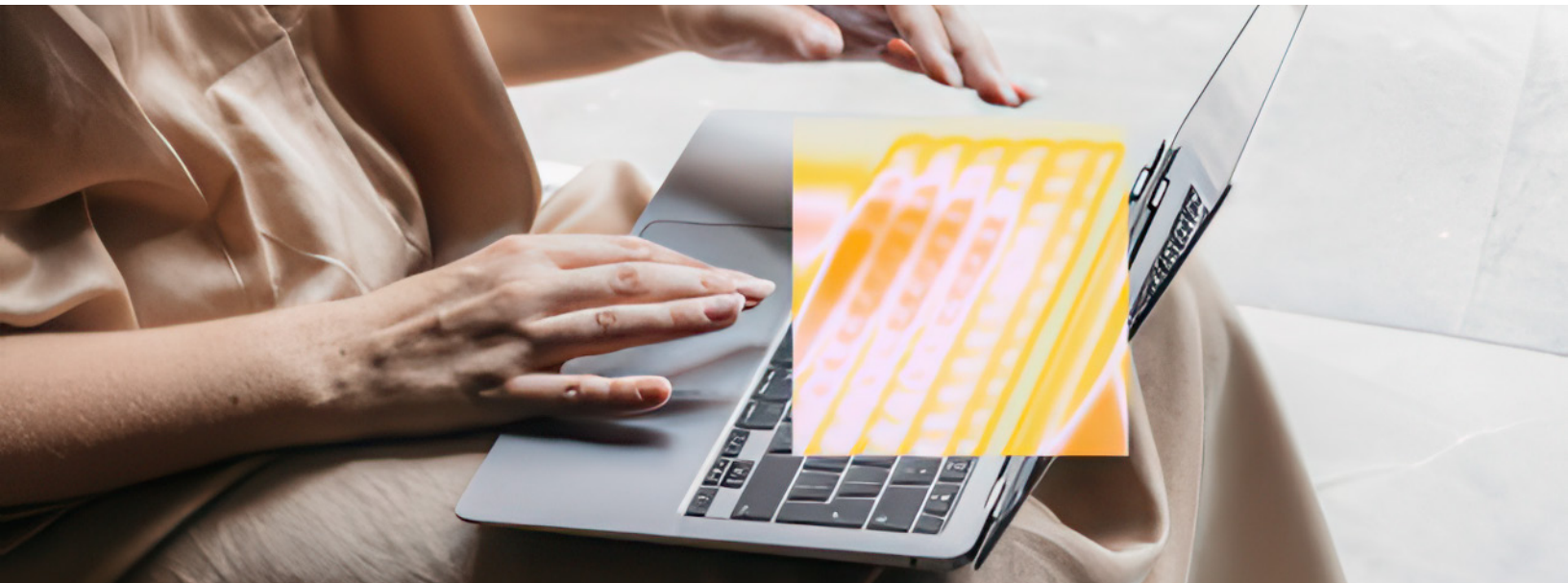
**Defina y administre los datos confidenciales:** Cree un documento que enumere ejemplos de datos confidenciales, como PII y registros financieros, y desarrolle pautas para almacenar, acceder y compartir datos confidenciales de forma segura.

**Administración y respuesta ante incidentes:** Desarrolle o revise su plan de respuesta ante incidentes en el que se describan los pasos a seguir en caso de producirse una filtración de datos.

**Administración de usuarios y control de acceso:** Defina roles (por ejemplo, administrador, gerente, empleado) con permisos de acceso específicos. Utilice Microsoft Entra ID para la creación o eliminación automática de cuentas e implemente la autenticación multifactor (MFA) para todos los empleados.

**Explore los análisis en sus soluciones:** Ya activó los análisis de Gestión de riesgos internos, ahora obtendrá información valiosa que lo guiará por el entorno de seguridad de datos. Activarlo temprano lo ayuda a obtener valor rápidamente. Además, esto le permite identificar las brechas.

**Comience con lo que es importante para usted:** Aunque debería empezar con cualquier solución de seguridad de datos a la que dé prioridad, muchas organizaciones empiezan con la Gestión de riesgos internos porque no tienen que etiquetar nada, los requisitos previos son mínimos y pueden empezar rápidamente sin que ello repercuta en los usuarios finales (la empresa).



## Qué podrá implementar con las soluciones de seguridad de datos de Microsoft Purview

| Protección de la información | Prevención de pérdida de datos | Gestión de riesgos internos |
|---|---|---|
| • Desarrolle su taxonomía de etiquetas, como "confidencial general", "público", "finanzas", "recursos humanos", "altamente confidencial"<br>• Utilice las características integradas para identificar el contenido confidencial y considere implementar el etiquetado automático.<br>• Establezca la gobernanza en todo su patrimonio de datos.<br>• Asegúrese de que todos los datos se clasifiquen correctamente, determinando qué requiere cifrado, a quién está destinado y qué se puede clasificar en general. | • Revise las ubicaciones donde se almacena la información confidencial.<br>• Desarrolle e implemente directivas para educir las filtraciones de datos, los robos de datos y otras actividades de filtración relacionadas con información confidencial.<br>• Cree directivas o categorías personalizadas específicas de su industria, como salud o finanzas. | • Identifique riesgos ocultos con más de 100 modelos e indicadores de machine learning integrados, sin necesidad de agentes de punto de conexión.<br>• Utilice plantillas para desarrollar directivas para las filtraciones de datos, los robos de datos y las vulneraciones de seguridad por parte de usuarios riesgosos.<br>• Acelere la mitigación con investigaciones enriquecidas y Protección adaptativa que aplican los controles de DLP de forma dinámica. |

**Etapa de ejecución:** En la segunda etapa se sientan las bases para una implementación exitosa, escalable y sostenible. En esta fase, usted planifica los detalles de la implementación y desarrolla la solución. También puede ejecutar un piloto o una prueba de concepto con un grupo seleccionado de usuarios o ubicaciones.

## Microsoft Information Protection (MIP)

Las capacidades integradas de MIP pueden ayudar a que su organización descubra, clasifique, proteja y gobierne la información confidencial dondequiera que resida o viaje. Tiene información que reside en todos los servicios de Microsoft 365 y en el entorno local. Identificar qué elementos son confidenciales y obtener visibilidad sobre cómo se usan es fundamental para su práctica de protección de la información. Microsoft Purview incluye:

- Tipos de información confidencial para identificar elementos confidenciales mediante el uso de funciones o expresiones regulares integradas o personalizadas.
- Clasificadores entrenables para identificar elementos confidenciales mediante ejemplos de los datos que le interesan en lugar de identificar elementos individuales.
- Clasificación de datos para proporcionar una identificación gráfica de los elementos de su organización que tienen una etiqueta de confidencialidad, una etiqueta de retención o que se han clasificado, y las acciones que los usuarios están realizando sobre ellos.

Considere comenzar con la clasificación de datos en lugar de etiquetar si se siente abrumado por las etiquetas. Piense en los pasos para hacer operativo Microsoft Purview como una serie de bloques de creación sin orden establecido.

MIP ofrece un marco y capacidades para descubrir, clasificar y proteger datos confidenciales en entornos locales, SharePoint, OneDrive, Exchange, Teams, puntos de conexión y nubes que no son de Microsoft mediante la aplicación de niveles de confidencialidad a los datos. Ayuda a gestionar los riesgos de datos críticos y los requisitos reglamentarios con tres conceptos básicos: conozca sus datos, proteja sus datos y evite la pérdida de datos.

Obtenga más información sobre la Protección de la información y, a continuación, complete los siguientes pasos para comenzar a proteger su primera carga de trabajo:

1. Pasos fundamentales: Comience con las etiquetas recomendadas para proteger el contenido nuevo o actualizado. Las etiquetas de confidencialidad son etiquetas organizativas significativas e intuitivas para los usuarios finales. La estrategia para aplicar etiquetas suele iniciarse con el etiquetado manual, luego el etiquetado automático del lado del cliente con tipos de información confidencial (SIT), seguido del etiquetado automático del lado del servicio (en reposo) con SIT y condiciones contextuales.

a. Comience con las etiquetas predeterminadas (público, general, confidencial, altamente confidencial) y la protección en el nivel de archivos y sitios.
b. Active los requisitos previos de seguridad de datos y el análisis avanzado.
c. Capacite a los usuarios en la administración de excepciones.

2. Pasos administrados: Aborde los archivos con la confidencialidad más alta para proteger el contenido con prioridad. Identifique sus sitios prioritarios a partir de sitios bien conocidos, incluidos sitios de equipos de liderazgo, explorador de contenido con un alto número de documentos confidenciales, informes y Graph API para sitios con grandes cantidades de información confidencial.

   a. Configure manualmente el etiquetado de biblioteca predeterminado de los sitios prioritarios.
   b. Etiquetado automático para credenciales y condiciones contextuales.

3. Pasos optimizados: Amplíe todo el patrimonio de datos de Microsoft 365 para proteger el contenido histórico y aplicar directivas progresivamente en escenarios. El etiquetado automático es ideal para casos en los que se requiere una mayor confidencialidad que la etiqueta predeterminada.

   a. Etiquete automáticamente los archivos confidenciales en los clientes (umbrales bajos).
   b. Simule el etiquetado automático de archivos confidenciales en reposo.
   c. Reduzca los falsos positivos con clasificadores avanzados.
   d. Automatice y mejore la protección de Microsoft 365 para los datos históricos y en uso.

4. Medidas estratégicas: Opere, amplíe y realice acciones retroactivas para protegerse más allá de Microsoft 365.

   a. Realice una revisión operativa de los comportamientos de etiquetado de los usuarios.
   b. Itere con nuevos escenarios de etiquetado.
   c. Configure la cadena de responsabilidad y la administración del ciclo de vida.
   d. Amplíe la protección a Azure SQL y almacenamiento que no es de Microsoft 365.

### ¿Sabía que..?

El mejor enfoque es multifacético. Use una combinación de métodos de etiquetado, incluido el etiquetado automático, el etiquetado manual, el etiquetado obligatorio y el etiquetado predeterminado. Si bien el etiquetado es importante, no tiene que completarlo antes de comenzar una segunda secuencia de trabajo. Fortalezca la seguridad para múltiples flujos de trabajo mientras trabaja en el etiquetado al mismo tiempo, ya que cosas como las etiquetas específicas de cada país y las consideraciones específicas de la industria llevan tiempo.

## Anatomía de una directiva

Al crear una directiva de etiquetas de protección de la información, estos son los factores que deberá tener en cuenta:

- Elija las etiquetas de confidencialidad que desea publicar (entre personales, públicas, generales, confidenciales, altamente confidenciales, relacionadas con proyectos, etc.). Una vez publicadas, las etiquetas que elija estarán disponibles en las aplicaciones de Office de usuarios especificados (Word, Excel, PowerPoint y Outlook), los sitios de SharePoint y Teams y los grupos de Microsoft 365.
- Asigne unidades administrativas. Elija las unidades de administración a las que desea asignar esta directiva. Las unidades de administración se crean con Microsoft Entra ID y restringen la directiva a un conjunto específico de usuarios o grupos. Sus selecciones afectarán las opciones de ubicación disponibles para usted en el siguiente paso.
- Publique para usuarios y grupos. Las etiquetas que seleccione estarán disponibles para los usuarios, los grupos de distribución, los grupos de seguridad habilitados para correo y los grupos de Microsoft 365 que elija aquí.

- Implemente configuraciones específicas de la directiva, como "Los usuarios deben proporcionar una justificación para quitar una etiqueta o reducir su clasificación" o "Requerir a los usuarios que apliquen una etiqueta a sus correos electrónicos y documentos".
- Aplique la configuración predeterminada a los documentos. La etiqueta que elija se aplicará automáticamente a los documentos, reuniones, correos electrónicos, sitios, grupos y otro contenido cuando se creen o modifiquen.
- Use las directivas predeterminadas tal cual, cree nuevas, modifíquelas como prefiera o personalícelas completamente para que se adapten mejor a sus requisitos empresariales individuales.

### ¿Sabía que..?

Protección de la información de Microsoft Purview para aplicaciones y servicios de Microsoft 365, SQL Server, Azure Data Lake Storage y Microsoft Fabric le permite agregar etiquetas de confidencialidad a los datos. Luego, Microsoft 365 Copilot hereda cualquier etiqueta de estos archivos. Incluso puede configurar el etiquetado automático, que aplica etiquetas de confidencialidad a archivos y correos electrónicos en función de la introducción de datos confidenciales. De hecho, Microsoft 365 E5 indexa todo desde el primer momento; el 99 % del etiquetado está automatizado.

## Gestión de riesgos internos (IRM)

IRM le permite minimizar los riesgos de seguridad de los datos mediante la detección, investigación y acción contra actividades internas maliciosas, negligentes o involuntarias. Correlaciona varias señales para identificar posibles riesgos internos, como robo de IP, fuga de datos e infracciones de seguridad. Hasta el 59 % de los empleados admiten que llevan los datos consigo cuando dejan una organización.* La Gestión de riesgos internos utiliza toda la gama de servicios de Microsoft 365, Fabric e indicadores de terceros para ayudarlo a identificar, priorizar y actuar con rapidez sobre actividad potencialmente riesgosa. Mediante el uso de registros en el entorno de Microsoft y en aplicaciones de terceros, la Gestión de riesgos internos le permite definir directivas específicas para identificar indicadores de riesgo. Después de identificar los riesgos, puede tomar medidas para mitigar estos riesgos y, si es necesario, abrir casos de investigación y tomar las medidas legales apropiadas.

Obtenga más información sobre la Gestión de riesgos internos, complete los siguientes pasos para crear su primera directiva de la Gestión de riesgos internos y comience a analizar su entorno de riesgos internos:

1. Habilite los permisos para la Gestión de riesgos internos: Existen seis grupos de roles que se utilizan para configurar las características de la Gestión de riesgos internos. Para que la Gestión de riesgos internos esté disponible como una opción de menú en Microsoft Purview y para seguir con la configuración, tiene que estar asignado a uno de los grupos.
2. Habilite el registro de auditoría de Microsoft 365: Los registros de auditoría de Microsoft 365 son un resumen de todas las actividades dentro de su organización, y las directivas de Gestión de riesgos internos pueden usar estas actividades para generar perspectivas de directivas.
3. Configure los requisitos previos para las directivas: Configure los requisitos previos adecuados para las directivas que planea configurar de modo que sus indicadores de directiva generen alertas de actividad pertinentes.
4. Configure los ajustes de riesgos internos: Esta configuración controla la privacidad, los indicadores, las exclusiones globales, los grupos de detección, las detecciones inteligentes y mucho más, y se configuran mediante el botón de configuración que se encuentra en la parte superior de las páginas de Gestión de riesgos internos.
5. Cree una directiva de Gestión de riesgos internos: Las directivas incluyen usuarios asignados y definen qué tipos de indicadores de riesgo se configuran para las alertas. Antes de que las actividades potencialmente riesgosas puedan activar alertas, se debe configurar una directiva. Utilice el asistente de directivas para crear nuevas directivas de Gestión de riesgos internos.

*Departing workers often steal data from ex-employers: study | CBC News

a. **Recomendaciones de directivas a partir de análisis:** Microsoft Purview Insider Risk Management utiliza análisis para ofrecer recomendaciones de directivas. Estas recomendaciones se basan en el análisis de las actividades de los usuarios y otras señales, lo que ayuda a identificar riesgos potenciales y sugerir directivas adecuadas para mitigarlos.

b. **Directivas rápidas de acciones recomendadas:** A partir de las acciones recomendadas proporcionadas por los análisis, las organizaciones pueden crear directivas rápidamente. Esta característica permite una respuesta rápida a los riesgos identificados mediante la generación de directivas que abordan comportamientos o actividades de riesgo específicos.

Escenarios disponibles:

- La protección de activos críticos detecta actividades que involucran los activos más valiosos de su organización. La pérdida de estos activos podría resultar en responsabilidad legal, pérdida financiera o daño a la reputación.
- Las filtraciones de datos detectan posibles fugas de datos de todos los usuarios de su organización, que pueden ir desde el uso compartido excesivo accidental de información confidencial hasta el robo de datos con intenciones maliciosas.
- El robo de datos por parte de los usuarios que salen detecta un posible robo de datos por parte de los usuarios cerca de la fecha de renuncia o finalización, o en función de la eliminación de su cuenta de Microsoft Entra ID.
- La filtración de correo electrónico detecta cuando los usuarios envían correos electrónicos con activos confidenciales fuera de su organización. Por ejemplo, los usuarios envían activos confidenciales a su dirección de correo electrónico personal.

c. **Directiva creada desde cero:** Las organizaciones también tienen la flexibilidad para crear directivas desde cero. Esto significa que pueden definir directivas personalizadas adaptadas a sus requisitos y escenarios de riesgo únicos, sin depender de las recomendaciones automatizadas.

Estas explicaciones deben darle una idea clara de cómo la Gestión de riesgos internos de Microsoft Purview ayuda en la creación de directivas y administración de riesgos. Si tiene más preguntas o necesita más detalles, ¡no dude en preguntar!

Una vez completados estos pasos, empezará a recibir alertas de indicadores de actividad después de alrededor de 24 horas. Para obtener más información sobre la investigación de las alertas de riesgo interno y el panel de alertas, consulte Actividades de la Gestión de riesgos internos.

### ¿Sabía que..?

Al establecer directivas de riesgos internos, puede definir los tipos de riesgos que se identificarán y detectarán en su organización. Una vez que detecte y clasifique los riesgos, puede remitir los casos a Microsoft eDiscovery (Premium) para una investigación adicional, si es necesario.

## Anatomía de una directiva

Al crear una directiva de Gestión de riesgos internos, estos son los factores que deberá tener en cuenta:

- Las plantillas de directivas pueden especificar las condiciones y los indicadores que definen las actividades de riesgo sobre las que desea recibir alertas, según los principales casos de uso de riesgo interno (guías).
- Elija si la directiva se aplicará a todos los usuarios y grupos o si limitará la cobertura a usuarios, grupos y ámbitos adaptables específicos.
- Priorización de contenido: Puede priorizar el contenido según factores como el lugar donde se almacena, los tipos de archivos y cómo se clasifica (confidencialidad). Las puntuaciones de riesgo aumentan para cualquier actividad que contenga contenido prioritario, lo que a su vez aumenta la posibilidad de generar una alerta de gravedad alta.
- Elija uno o más eventos desencadenantes para determinar cuándo una directiva comenzará a asignar puntuaciones de riesgo a la actividad de un usuario. A continuación, puede establecer

umbrales personalizados o recomendados para cada evento. Al establecer umbrales, puede definir qué actividades deben desencadenar una evaluación más detallada para los posibles riesgos internos y puede reducir el ruido para generar más alertas de alto valor.

- Elija los indicadores que formarán parte de esa directiva y que se utilizarán para generar alertas para la actividad detectada por la plantilla de directiva que seleccionó. Puede elegir indicadores como los de Office, dispositivos, almacenamiento en la nube, Fabric o incluso indicadores personalizados.
- Elija sus opciones de detección avanzadas, como:
  - **Secuencias:** Un grupo de dos o más actividades realizadas una tras otra durante un período de 7 días que podría sugerir un riesgo elevado. Se utilizan indicadores específicos para detectar cada paso de una secuencia, que se organizan en cuatro tipos principales de actividad: descargar, filtrar, ofuscar y eliminar.
  - **Detección de filtración acumulativa:** Detecta cuando el número de actividades de filtración que un usuario realiza durante un tiempo determinado supera la cantidad normal realizada por los usuarios de su organización durante los últimos 30 días.

## Prevención de pérdida de datos (DLP)

DLP le ayuda a identificar e impedir que se compartan, transfieran o utilicen de forma arriesgada o inadecuada datos confidenciales en aplicaciones de la nube, dispositivos, repositorios locales y mucho más. Los datos confidenciales pueden incluir datos financieros, datos de propiedad, números de tarjetas de crédito, registros médicos, números de seguridad social y más.

Muchas organizaciones optan por implementar DLP a fin de cumplir con diversas normativas gubernamentales o de la industria, como RGPD de la Unión Europea, HIPAA o la Ley de privacidad del consumidor de California (CCPA). También implementan DLP para proteger su propiedad intelectual. Sin embargo, el lugar de partida y el destino final en el viaje de DLP varían.

Las organizaciones que conocen su información sensible suelen comenzar su andadura de DLP a nivel de plataforma o carga de trabajo, o con el tipo de información sensible que desean proteger prioritariamente. Para las organizaciones que aún determinan qué incluye su información confidencial y dónde reside, pueden ir directamente a definir directivas y revisar los resultados para refinarlos más adelante. No importa dónde empiece; DLP es lo suficientemente flexible como para adaptarse a varios tipos de recorridos de protección de la información desde el inicio hasta una estrategia de DLP por completo realizada.

Cuando configure DLP por primera vez:

- Comience con el modo de solo auditoría. A continuación, puede revisar las alertas para decidir qué tipos de datos confidenciales o actividades bloquear o advertir. El modo de auditoría garantiza que no interfiera en procesos empresariales importantes en los que sea necesario compartir datos confidenciales dentro o fuera de la organización.
- Use la característica de moderación para correos electrónicos a fin de administrar las excepciones.
- Comprenda que la filtración de datos ocurre a través del punto de conexión, donde los usuarios a menudo copian los datos en una memoria USB o los imprimen y reenvían a una dirección de correo electrónico personal.
- Reconozca qué análisis de DLP y modo de simulación falta. (Idealmente, los clientes crean directivas y las ejecutan en modo de simulación antes de la implementación).

Obtenga más información sobre la Prevención de pérdida de datos de Purview y, a continuación, explore los siguientes pasos para comenzar a identificar, asignar y preparar sus datos para el diseño de directivas de DLP:

1. Identifique las categorías de elementos confidenciales que se protegerán y los procesos empresariales en los que se utilizan; el Administrador de cumplimiento de Microsoft Purview puede ayudarlo a comenzar con una evaluación predeterminada y un conjunto de controles para normativas y estándares clave.

2. Priorice qué datos se deben proteger primero según la confidencialidad de los elementos y el riesgo involucrado.

3. Determine el comportamiento de riesgo que debe limitarse. Comience por definir sus objetivos de control y cómo se aplican a cada carga de trabajo respectiva.

4. Diseñe sus directivas. Redacte una directiva que incorpore sus objetivos. Puede empezar con una carga de trabajo a la vez, o puede considerar varias de ellas. Puede partir de una plantilla predefinida y crear una directiva con solo unos clics, o puede diseñar la suya propia desde cero.

Cuando llegue a la etapa de diseño de una directiva, revise los procedimientos recomendados de diseño de directivas de DLP recomendadas por Microsoft. Tomarse el tiempo para diseñar una directiva antes de implementarla le permite obtener los resultados deseados más rápido que si la crea y ajusta solo mediante ensayo y error, y experimentará menos problemas no deseados. Contar con sus diseños de directivas documentados también lo ayudará con las comunicaciones, las revisiones de directiva, la solución de problemas, entre otros ajustes.

El diseño de una directiva consiste principalmente en definir con claridad las necesidades de su empresa, documentarlas en una declaración de intenciones de directiva y, a continuación, asignar esas necesidades a la configuración de la directiva. Usted utiliza las decisiones que tomó en su fase de planificación para informar algunas de sus decisiones de diseño de directivas. Con las partes interesadas clave identificadas, los siguientes pasos son:

- Defina la intención de la directiva.
- Asigne las necesidades empresariales a la configuración de la directiva.
- Describa las categorías de información confidencial que se van a proteger.
- Defina sus objetivos y estrategia.
- Defina su plan de implementación de directivas.

5. Implemente la directiva en el modo de simulación. Las acciones definidas en una directiva no se aplican mientras la directiva está en modo de simulación. Es correcto aplicar la directiva a todas las cargas de trabajo en modo de simulación para que pueda obtener toda la gama de resultados, pero puede empezar con una carga de trabajo si es necesario.

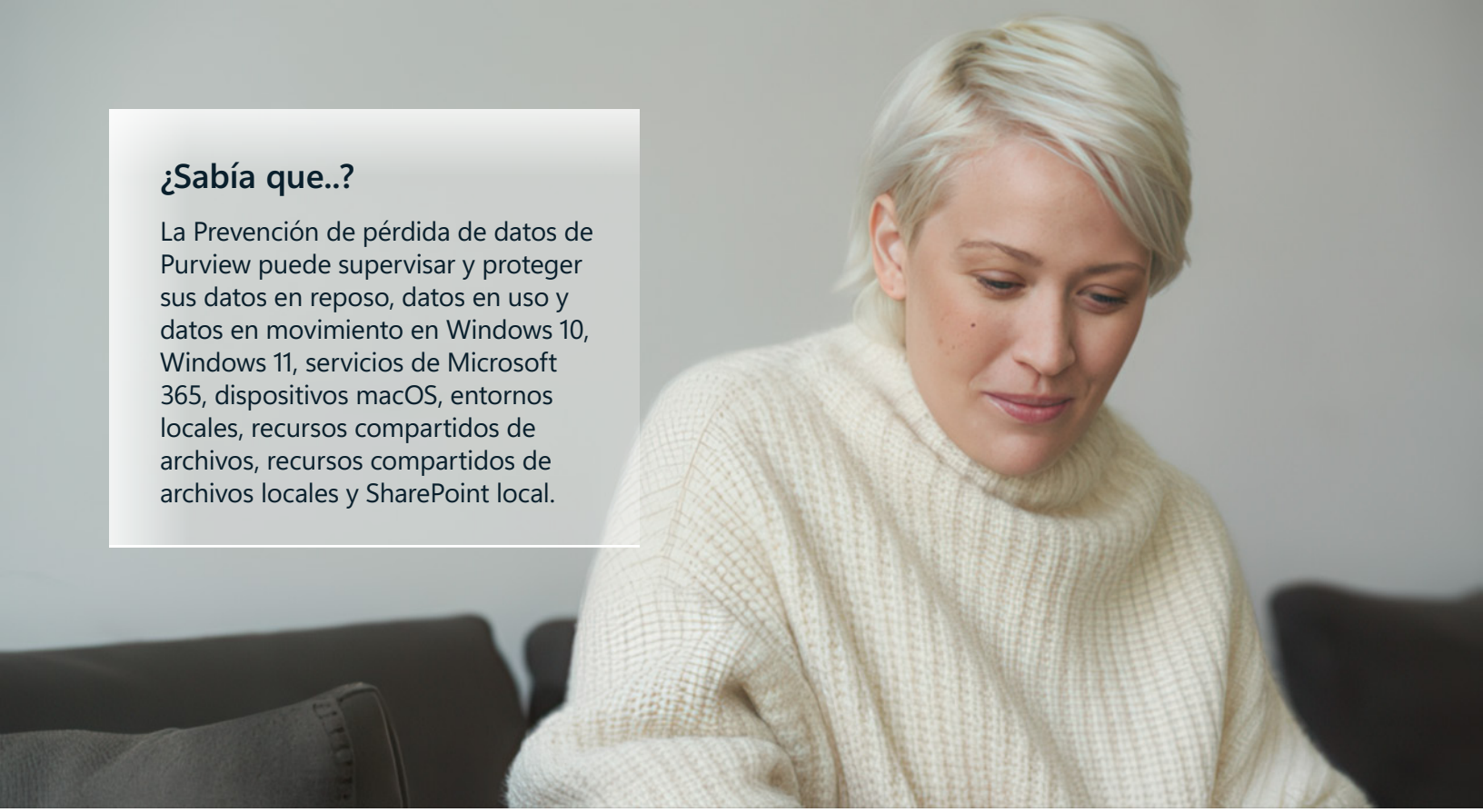
6. Supervise los resultados y ajuste la directiva. Mientras está en modo de simulación, supervise los resultados de la directiva y ajústela para que cumpla con sus objetivos de control. Además, asegúrese de que no tendrá un impacto adverso o accidental en los flujos de trabajo y la productividad de usuarios válidos.

7. Describa el proceso de revisión y corrección de eventos de coincidencia de directivas de DLP. Establezca objetivos de protección y desarrolle un plan de implementación.

8. Habilite el control y ajuste sus directivas.

9. No olvide lo siguiente:
   - Active las directivas de DLP para el contenido etiquetado.
   - Active DLP para el contenido que no está etiquetado.
   - Active la Protección adaptativa y las reglas de comportamiento de fuga de datos.

10. Analice las alertas de DLP generadas. DLP genera una alerta cuando un usuario realiza una acción que cumple los criterios de una directiva de DLP y tiene informes de incidentes configurados para generar alertas. DLP publica la alerta para investigación en el panel de alertas de DLP. Use el panel de alertas DLP para ver las alertas, clasificarlas, establecer el estado de la investigación y realizar un seguimiento de la resolución. Las alertas también se enrutan al portal de Microsoft Defender, donde puede realizar todas las tareas del panel de alertas y mucho más.



### ¿Sabía que..?

La Prevención de pérdida de datos de Purview puede supervisar y proteger sus datos en reposo, datos en uso y datos en movimiento en Windows 10, Windows 11, servicios de Microsoft 365, dispositivos macOS, entornos locales, recursos compartidos de archivos, recursos compartidos de archivos locales y SharePoint local.

## Anatomía de una directiva

Al crear una directiva de DLP, estos son los factores que deberá considerar:

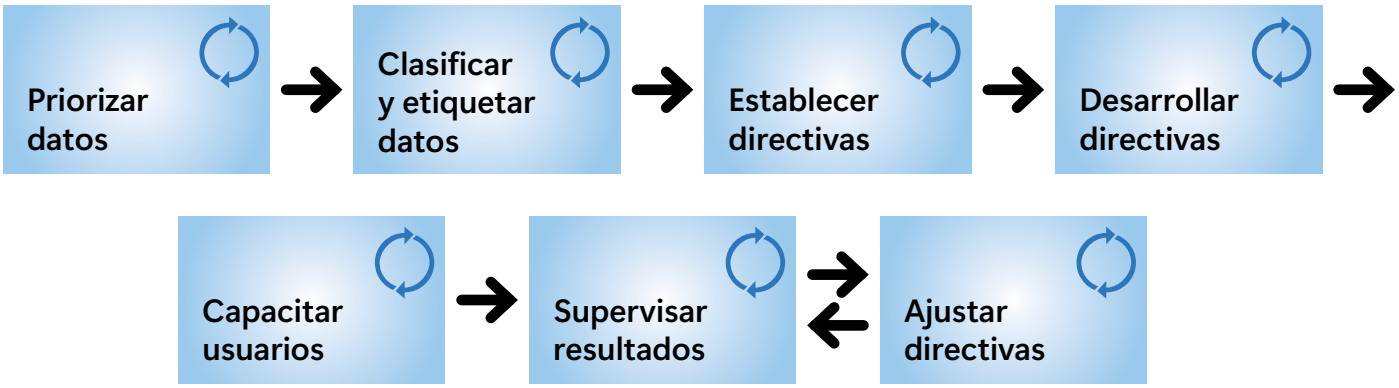
- Comience con una plantilla o cree una directiva personalizada. Elija una normativa de la industria para ver las plantillas de directiva de DLP que puede utilizar para proteger esa información o crear una directiva personalizada desde cero.
- Asigne unidades administrativas. Elija las unidades de administración a las que desea asignar esta directiva. Las unidades de administración se crean con Microsoft Entra ID y restringen la directiva a un conjunto específico de usuarios o grupos.
- Elija dónde desea aplicar la directiva en función de los datos almacenados en las ubicaciones que elija, como correo electrónico, sitios de SharePoint, cuentas de OneDrive, dispositivos, Teams, etc.
- Personalice las reglas avanzadas de DLP, como condiciones específicas, excepciones, acciones que afectan al usuario objetivo, notificaciones, opciones de invalidación, informe de incidentes y si desea permitir controles dinámicos basados en niveles de riesgo interno (obtenga más información sobre los controles automáticos habilitados por la Protección adaptativa en la siguiente fase de esta guía).

### Una historia de la vida real

Una organización experimentó la filtración de una gran cantidad de gigabytes de archivos, incluidos algunos que contenían datos confidenciales, en un solo día. Antes de adoptar Microsoft Purview, no tenía la visibilidad necesaria para detectar un incidente como este. De hecho, no habría sabido cuántos datos confidenciales había en esos archivos. La organización compartió que este incidente reforzó la razón por la que implementó Microsoft Purview en primer lugar: porque la visibilidad ayuda a prevenir incidentes de pérdida de datos.

# Afine y revise sus directivas

Una vez que haya establecido las primeras etapas de implementación y operacionalización de la seguridad de datos con Microsoft Purview en su organización, sus interacciones con estas soluciones pueden ser muy frecuentes o más dispersas. Recuerde que, dependiendo del tamaño y nivel de madurez de su organización, podría tardar meses, o incluso años, implementar cada paso para explorar todas las capacidades de seguridad de datos de Microsoft Purview.




Las organizaciones suelen implementar directivas que abordan primero sus principales preocupaciones. Sin embargo, cierta información confidencial puede generar alertas que se vuelven abrumadoras y hacen demasiado ruido. Por el contrario, es posible que reciba menos alertas de las previstas y le preocupe no haber configurado correctamente las directivas. El ajuste y la revisión de sus directivas son partes críticas de la operacionalización de la seguridad de los datos y actividades clave de la administración continua.

Si desea establecer un marco de tiempo para revisar las directivas, considere la posibilidad de alinearse con un marco de gestión de riesgos, como el desarrollado por el Instituto Nacional de Estándares y Tecnología. Esto implica revisar todas las directivas relacionadas con la seguridad anualmente como parte de su proceso general.

Microsoft Purview le ofrece la posibilidad de ajustar ligeramente las definiciones de las directivas con solo pulsar un botón. Además, debe ajustar continuamente sus directivas a medida que descubre lo que funciona mejor para su organización e identifica nuevos riesgos potenciales. Ya sea que eso signifique hacer ajustes todos los días o todas las semanas, será exclusivo para su organización, industria y requisitos de cumplimiento.

Al implementar nuevas soluciones, configure acciones de cumplimiento. Algunos clientes no se sienten cómodos con el cifrado en los documentos, la aplicación de los controles de protocolo de semáforo o la adopción de otras medidas porque temen un impacto comercial importante. Pero el refuerzo de la ciberseguridad es la razón por la que comenzó su recorrido de seguridad de datos en primer lugar. Y para lograrlo, tiene que definir un camino que vaya de la alerta a la aplicación.

**Etapa de escala:** La última fase consiste en optimizar la solución para Microsoft 365. En esta fase configurará un enfoque escalable automatizado para cada solución.

## Gestión de riesgos internos

Debido a la naturaleza de la información y a la amplitud de las señales, la Gestión de riesgos internos puede ser un buen candidato para afinar el enfoque con el fin de evitar el ruido y las alertas innecesarias.

Obtenga más información sobre el diseño y el ajuste de las directivas de DLP aquí: Ajuste las exclusiones en la Gestión de riesgos internos mediante la creación de grupos de detección y la modificación de variantes de indicadores integrados (versión preliminar) - Microsoft Learn.

Para la Gestión de riesgos internos, tiene la opción de "ajustar para obtener alertas más precisas". Existe una acción recomendada en el producto denominada "explorar los procedimientos recomendados para las alertas de ajuste". Incluye algunos consejos excelentes sobre el ajuste, incluido el uso de las siguientes características: dominios permitidos, tipo de archivo, exclusión de palabras clave y exclusión de SIT. También puede aprovechar la orientación en el producto para el ajuste, como el uso de las plantillas de directivas basadas en escenarios disponibles.

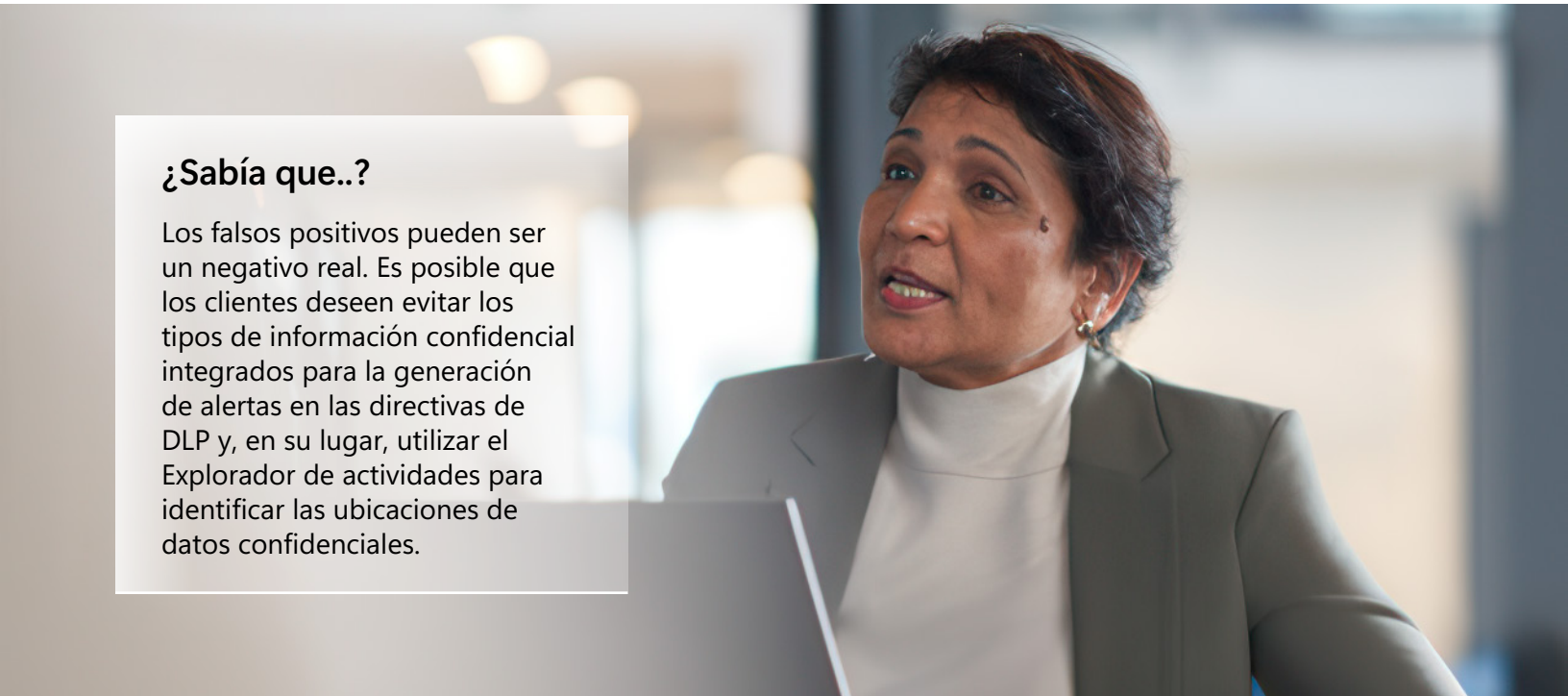
## Prevención de pérdida de datos

Para ajustar las directivas de Prevención de pérdida de datos de Microsoft Purview, comience por implementarlas en modo de simulación para evaluar su impacto sin aplicar restricciones. Este enfoque le permite supervisar los resultados e identificar posibles falsos positivos. Durante esta fase, recopilará comentarios de los usuarios que reciben alertas de directivas y ajustará las directivas en consecuencia para minimizar las interrupciones. Los ajustes clave pueden incluir el perfeccionamiento de las condiciones que desencadenan las acciones de directiva, la modificación del ámbito de las ubicaciones supervisadas y la actualización de la lista de tipos de información confidencial. Una vez que las directivas equilibren con eficacia la protección y la facilidad de uso, actívelas completamente y continúe supervisando su rendimiento, realizando los ajustes adicionales necesarios para adaptarse a la evolución de las necesidades de protección de datos.

Obtenga más información sobre el diseño y el ajuste de las directivas de DLP aquí: Diseño de una directiva de prevención de pérdida de datos: Microsoft Learn.

### Caso de éxito

Una empresa de atención de salud implementó la administración de respuesta ante incidentes en los Estados Unidos y convirtió su programa de pérdida de datos en un programa de amenazas internas. Un pequeño equipo de tres o cuatro personas administró el programa, pero tenía preguntas sobre cómo hacerlo efectivo. Dos de ellos acudieron a Microsoft y trabajaron con nuestros expertos para obtener respuestas a sus preguntas.



### ¿Sabía que..?

Los falsos positivos pueden ser un negativo real. Es posible que los clientes deseen evitar los tipos de información confidencial integrados para la generación de alertas en las directivas de DLP y, en su lugar, utilizar el Explorador de actividades para identificar las ubicaciones de datos confidenciales.

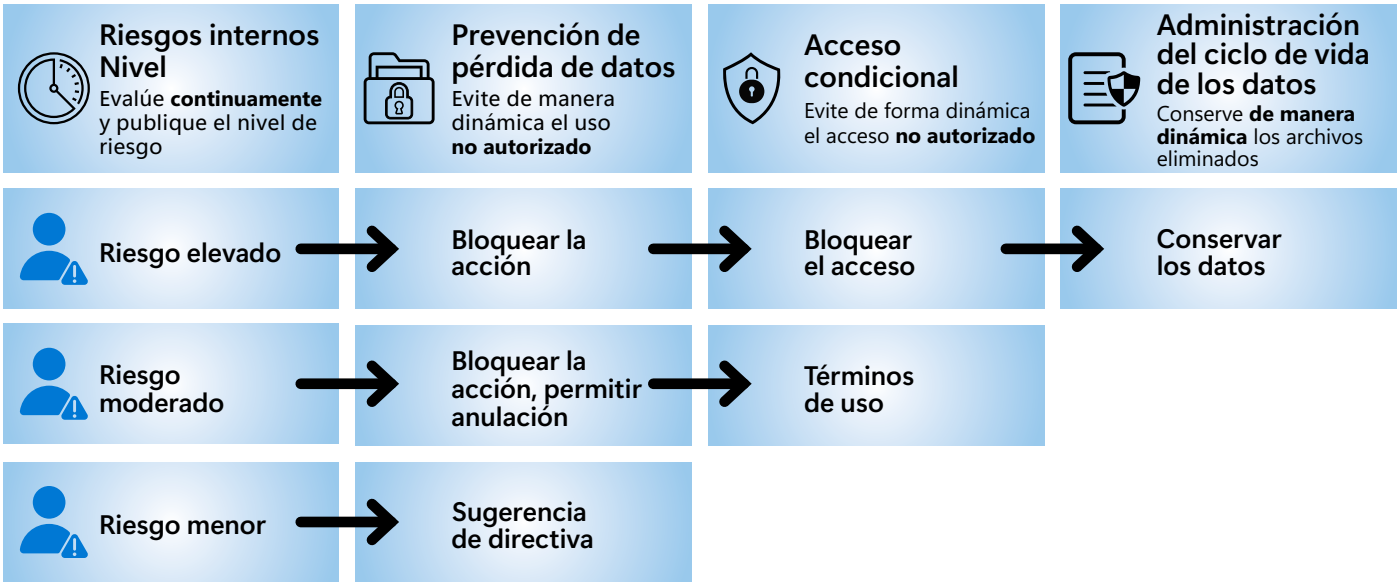
# Mejore los escenarios de seguridad de datos y configure la Protección adaptativa

Es comprensible que las organizaciones implementen habitualmente directivas que abordan sus principales preocupaciones. Las alertas iniciales a menudo provocan ajustes finos si las alertas se vuelven abrumadoras y desea reducir el ruido al centrarse en las directivas que son más críticas. O bien, puede recibir muy pocas alertas y preocuparse de no haber configurado correctamente las directivas. Al revisar las alertas y los eventos que las desencadenan, considere las oportunidades para mejorar aún más la seguridad de sus datos:

- Apoye la protección de datos pertinente y los escenarios basados en la seguridad.
- Complete una evaluación de los escenarios de riesgo interno.
- Implemente la Gestión de riesgos internos y configure y ajuste las directivas de la Gestión de riesgos internos.
- Habilite la evaluación de los conectores de datos de terceros, si son necesarios y aplicables. Por ejemplo, debe evaluarse si el conector de datos de RR. HH. comparte o no usuarios que renunciaron entre RR. HH. y la seguridad de TI.
- Investigue las alertas de DLP y refuerce los controles.
- Investigue las alertas de Gestión de riesgos internos hasta la creación de un caso de eDiscovery.

Una vez que su programa de seguridad de datos esté más maduro y sus directivas estén mejor ajustadas para reflejar los escenarios clave que protegen y permiten a su equipo centrarse en investigar lo importante, su organización puede sentirse lo suficientemente segura como para comenzar a aplicar controles de seguridad de datos más automáticos.

## Protección adaptativa en Microsoft Purview



## Configuración de la protección adaptativa

La Protección adaptativa es una funcionalidad de Microsoft Purview que integra niveles de riesgo interno para aplicar dinámicamente controles sobre usuarios más riesgosos que interactúan con los datos y el acceso en su organización. Cuando los riesgos internos identifican a un usuario que está incurriendo en un comportamiento de riesgo, se le asigna dinámicamente un nivel de riesgo interno. Entonces, la Protección adaptativa se puede adjuntar automáticamente a una directiva de DLP, a un acceso condicional de Microsoft Entra o a la administración del ciclo de vida de los datos para ayudar a proteger a la organización contra el comportamiento de riesgo asociado con ese nivel de riesgo interno. A medida que los niveles de riesgo interno en la Gestión de riesgos internos cambian, las directivas de DLP aplicadas a los usuarios pueden ajustarse.

La Protección adaptativa se puede usar para supervisar los niveles de riesgo sin aplicar ninguna acción de bloqueo inmediatamente, cuando se ejecutan directivas de Microsoft Purview en modo auditoría o en modo de simulación. Considere que cuando cree nuevas directivas, querrá ejecutarlas en modo de auditoría o simulación hasta que vea que se generan las alertas para evitar bloquear la productividad inadvertidamente.

Después de todo, muchas organizaciones nos dicen que adoptaron Microsoft Purview en parte porque no quieren interrumpir la colaboración entre usuarios que trabajan en el mismo archivo o en instancias similares donde la productividad podría verse afectada. Con sus sistemas anteriores, dicen, tenían reglas de caja específicas o un escenario de bloqueo en el que esa colaboración simultánea no era posible.

## Pasos para configurar la Protección adaptativa

La **opción de configuración rápida** es la forma más rápida de empezar a utilizar la Protección adaptativa. Con esta opción, no necesita ninguna directiva preexistente de Gestión de riesgos internos, DLP, Administración del ciclo de vida de datos o Acceso condicional, y no necesita realizar previamente ninguna configuración ni característica. Para empezar, seleccione **Activar la Protección adaptativa** en las tarjetas de Protección adaptativa de la página principal del portal de Microsoft Purview o en la página de introducción a DLP. También puede comenzar con el proceso de configuración rápida yendo a **Gestión de riesgos internos > Protección adaptativa > Panel > Configuración rápida.** La opción de **configuración personalizada** permite personalizar la directiva de Gestión de riesgos internos, los niveles de riesgo interno y las directivas de DLP y Acceso condicional configuradas para la Protección adaptativa.

1. Cree una directiva de Gestión de riesgos internos.
2. Configure los ajustes de nivel de riesgos internos.
3. Cree o edite una directiva de DLP.
4. Cree o edite una directiva de acceso condicional.
5. Active la protección adaptativa.

Al ajustar la Protección adaptativa, su organización puede preocuparse por la magnitud de las interrupciones que podría provocar el bloqueo de los usuarios que utilizan Protección adaptativa. El potencial de interrupción accidental de la productividad puede mitigarse mediante definiciones predecibles para los niveles de riesgo y editando sus directivas de DLP y Acceso condicional para usar acciones menos disruptivas.

Para reducir la probabilidad de interrumpir la productividad, le recomendamos que utilice las siguientes definiciones para sus niveles de riesgo. Estas definiciones son las menos propensas a producir falsos positivos:

- **Elevado:** Alerta confirmada de cualquier gravedad
- **Moderado:** Alerta de gravedad alta o media generada
- **Menor:** Alerta de gravedad alta, media o baja generada

Para reducir la interrupción para el usuario final, puede configurar sus directivas de DLP y Acceso condicional de Protección adaptativa para aplicar acciones sin bloqueo que aún mitigarán el riesgo. Para DLP, puede configurar su directiva para advertir a los usuarios riesgosos o para bloquear con anulación. Para el acceso condicional, puede configurar su directiva para presentar términos de uso a los usuarios riesgosos, requerirles configurar MFA o bloquearlos de ciertos sitios de SharePoint.

Obtenga más información sobre las opciones de configuración rápida y personalizada de Protección adaptativa.

# Solución de problemas y mejora continua

Lanzar Microsoft Purview es solo el comienzo. Le recomendamos revisar y actualizar sus directivas para asegurarse de que se cumplan sus métricas de éxito y aplicar cambios cuando no se cumplan. Mientras sigue ajustando su uso de Microsoft Purview, no deje que la perfección se interponga en el camino del progreso.

## Estrategias de mantenimiento del programa de seguridad de datos

- Afronte una carga de trabajo, entidad o reto cada vez para empezar con hitos alcanzables y generar el impulso a partir de ahí. Repita esta estrategia cada vez que esté determinando lo que sigue en una secuencia de trabajo.
- Supervise la seguridad de los datos durante un mes y establezca nuevas directivas de DLP en función de sus hallazgos. Siempre surgirán sorpresas que no podría haber anticipado. También puede seguir revisando sus directivas para asegurarse de que se alineen con las regulaciones nuevas o cambiantes y los requisitos de cumplimiento.
- Consulte con sus profesionales de gestión de cambios o recursos humanos para revisar la capacitación regularmente y cada vez que se incorporan nuevos empleados. Es imperativo que todos los empleados comprendan claramente la estrategia de seguridad de datos de su organización.
- Planifique la rotación y el cambio de empleados a nuevos roles para así evitar las dependencias de un solo hilo. Espere que los roles cambien con el tiempo y esté preparado para evitar cualquier brecha de conocimiento.
- Reconozca que así como la capacitación es un proceso continuo, también lo es el mantenimiento de la solución. El mantenimiento consiste en la mejora continua a medida que su equipo de TI adapta la capacitación en soluciones, las integraciones, las directivas y la solución de problemas para adaptarse a sus necesidades únicas.
- Optimice el uso de la Protección adaptativa mediante la configuración de los niveles de riesgo para que sean más apropiados para su organización.

## Aprender y tomar impulso

- Extienda sus ambiciones más allá de su solución anterior. Muchas organizaciones suponen que tienen limitaciones por lo que estaban limitadas con su antigua solución.
- Estudie sus análisis para obtener información sobre qué directivas debe crear. En los primeros tres meses, obtendrá información valiosa sobre cómo las líneas de negocio utilizan los datos, sobre todo su patrimonio de datos, y ganará confianza en la supervisión y la identidad.
- Agilice la implementación mediante el cambio a un modelo en el que elabore un plan claro basado en la consecución de resultados manejables (como implementar una directiva para pocos usuarios) y objetivos medibles. Y todos en el equipo deben responsabilizar a todos por alcanzar esos hitos.
- Como ha ajustado el uso de la directiva y recibe menos falsos positivos, puede dedicar menos tiempo a clasificar las alertas y más tiempo a abordar las alertas verdaderas, los ajustes de umbral y los ajustes de las directivas.
- Agregue un proceso para controlar las nuevas características de Microsoft Purview a fin de tener en cuenta cómo las nuevas capacidades pueden afectar y mejorar la seguridad de los datos de su organización.

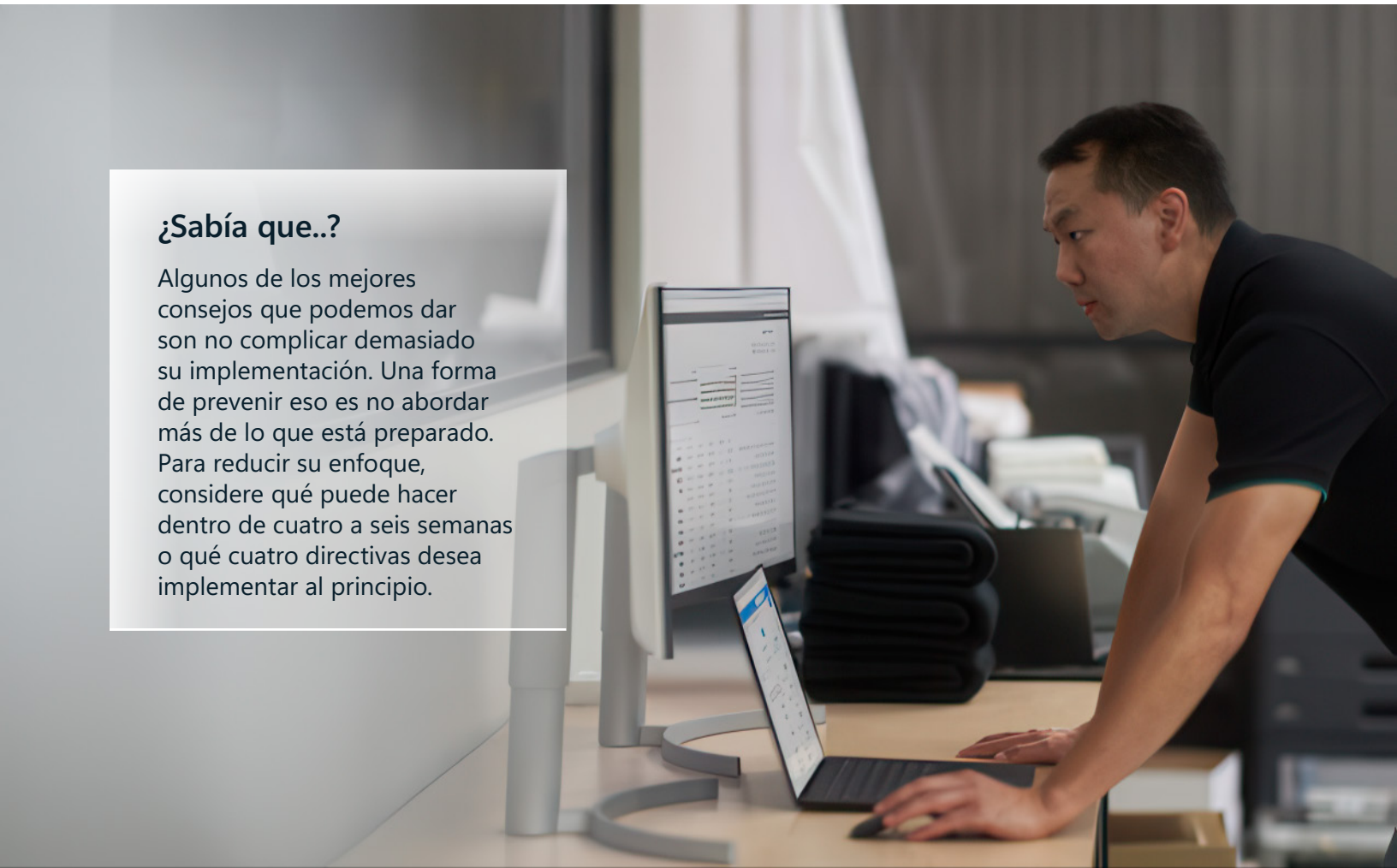
## Comunicaciones y capacitación

- Minimice el impacto en la productividad empresarial.
- Piense en lo "doloroso" que puede ser demasiado bloqueo para el negocio.

- Determine cuánta confianza depositar en los usuarios y su capacidad para etiquetar correcta y coherentemente; utilice el etiquetado automático siempre que sea posible.
- Considere cuándo debe revisar sus directivas.

La implementación de Microsoft Purview para la seguridad de datos implica muchos pasos, pero hay una gama de recursos disponibles para ayudarlo en todo el proceso:

1. **Modelos de implementación:** Estas guías, desarrolladas por el equipo de ingeniería de Microsoft, ofrecen pautas de implementación prescriptivas basadas en experiencias reales de los clientes. Proporcionan información general de alto nivel y pasos detallados adaptados a escenarios empresariales específicos. Microsoft Learn
2. **Guías de configuración:** Hay disponibles guías de configuración completas que le ayudarán a configurar diversas soluciones de Microsoft Purview, como Protección de la información, Administración del ciclo de vida de los datos e eDiscovery. Estas guías ofrecen instrucciones paso a paso para agilizar el proceso de implementación. Microsoft Learn
3. **Procedimientos recomendados de seguridad:** Para ayudar a garantizar una implementación segura, es esencial seguir los procedimientos recomendados. Microsoft proporciona recomendaciones detalladas sobre la configuración segura de Microsoft Purview, incluido el aislamiento de red y los controles de acceso. Microsoft Learn
4. **Lista de comprobación para la preparación:** Antes de la implementación, revisar una lista de comprobación de preparación puede ayudar a identificar los requisitos previos y garantizar que el entorno esté preparado. Esta lista de comprobación abarca la planificación, la preparación de la organización y los pasos fundamentales de la configuración. Microsoft Learn
5. **Soporte técnico de Microsoft y foros de la comunidad:** Para obtener asistencia personalizada, puede ponerse en contacto con el soporte técnico de Microsoft o participar en los foros de la comunidad de Microsoft Purview. Estas plataformas le permiten hacer preguntas, compartir experiencias y aprender de otros usuarios.



## ¿Sabía que..?

Algunos de los mejores consejos que podemos dar son no complicar demasiado su implementación. Una forma de prevenir eso es no abordar más de lo que está preparado. Para reducir su enfoque, considere qué puede hacer dentro de cuatro a seis semanas o qué cuatro directivas desea implementar al principio.

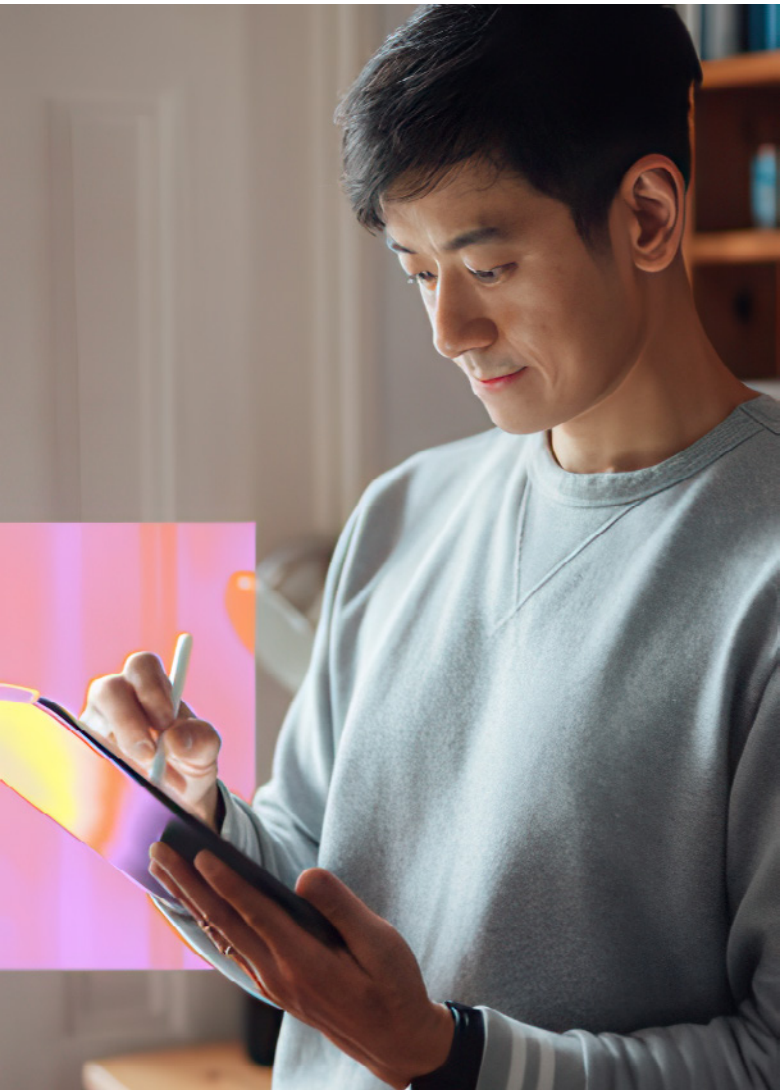
# Continuación de su viaje hacia la seguridad de los datos

Lanzar Microsoft Purview es solo el comienzo. Le recomendamos revisar y actualizar sus directivas para asegurarse de que se cumplan sus métricas de éxito y aplicar cambios cuando no se cumplan. Mientras sigue ajustando su uso de Microsoft Purview, no deje que la perfección se interponga en el camino del progreso.

## Administración de postura de seguridad de Microsoft Purview para IA

La Administración de postura de seguridad de datos de Microsoft Purview para IA (DSPM para IA) está actualmente en versión preliminar y proporciona herramientas gráficas e informes fáciles de usar para obtener con rapidez información sobre el uso de la IA dentro de su organización. Las directivas de un solo clic le ayudan a proteger sus datos y a cumplir los requisitos normativos.

Obtenga más información sobre Microsoft Purview DSPM para IA.



## Microsoft Security Copilot

Microsoft Security Copilot es una plataforma de IA basada en la nube que puede ayudar a los profesionales de seguridad y cumplimiento a proteger los datos de su organización. Con Seguridad de Copilot integrado en Microsoft Purview, los equipos pueden usarlo para identificar, resumir, clasificar y corregir problemas dentro de las soluciones de Microsoft Purview.

Principales escenarios actuales para que los administradores de datos de seguridad aprovechen Seguridad de Copilot integrada en Microsoft Purview:

- Descubra los riesgos ocultos en su entorno de seguridad de datos con información inicial, investigación guiada y análisis de indicaciones abiertas en la Administración de postura de seguridad de datos. Para obtener más información, consulte Uso de Microsoft Security Copilot con la Administración de postura de seguridad de datos (versión preliminar) | Microsoft Learn.
- Obtenga información sobre las directivas. Seguridad de Copilot puede ayudarle a entender qué hacen sus directivas en su organización y dónde están activas. Para obtener más información, consulte Obtener información con Seguridad de Copilot.
- Resuma las alertas en la Gestión de riesgos internos. Para obtener más información sobre esto y cómo obtener acceso a Copilot en la Gestión de riesgos internos, consulte Investigar las actividades de Gestión de riesgos internos.

Para obtener más información sobre lo que puede hacer Seguridad de Copilot y los diferentes escenarios que admite, lea ¿Qué es Microsoft Security Copilot?

## Integración de Microsoft Purview con Microsoft Defender XDR

Para que los investigadores del Centro de operaciones de seguridad (SOC) dispongan de los datos adecuados y de información sobre la intención del usuario para clasificar y priorizar mejor los incidentes, proporcionamos contexto de seguridad de datos en Defender XDR. Los equipos pueden administrar las alertas de DLP de Microsoft Purview y acceder al contexto de usuario de IRM directamente en el portal de Microsoft Defender. Desde el portal de Defender, puede:

- Ver todas sus alertas de DLP e IRM agrupadas en incidentes en la cola de incidentes de Microsoft Defender XDR y buscar registros de cumplimiento junto con la seguridad en Búsqueda avanzada.
- Acciones de corrección de administración in situ en el usuario, el archivo y el dispositivo.
- Los analistas del SOC con los permisos necesarios determinados por el cliente pueden acceder a un resumen de riesgos internos de las actividades de filtración de usuarios que pueden conducir a posibles incidentes de seguridad de datos.

Obtenga más información sobre la integración de Microsoft Purview con Microsoft Defender XDR.

## Investigaciones de seguridad de los datos

Para optimizar y simplificar este proceso, las organizaciones han compartido su necesidad de una solución unificada y especialmente diseñada que les permita identificar y mitigar con rapidez los riesgos de la exposición de datos confidenciales.

Investigaciones de seguridad de datos (DSI) de Microsoft Purview es una nueva solución que permite a los equipos de seguridad de datos identificar datos relacionados con incidentes, investigar esos datos con análisis de contenido profundo con tecnología de IA generativa y mitigar el riesgo dentro de una solución unificada. DSI descubre los riesgos clave de seguridad y datos confidenciales y facilita la colaboración segura entre los equipos de socios para mitigar los riesgos identificados, simplificando las tareas que anteriormente eran complejas y consumían mucho tiempo. Esta solución vincula las investigaciones de seguridad de datos con los incidentes de Defender XDR y los casos de Administración de riesgos internos de Purview.

Con la IA en su núcleo, DSI está diseñado para abordar los incidentes de seguridad de datos más complejos, de gran volumen y urgentes, redefiniendo la forma en que los equipos de seguridad de datos investigan y mitigan el riesgo.

Obtenga más información sobre las Investigaciones de seguridad de datos.

## Gobernanza y cumplimiento de los datos

Microsoft Purview ofrece un conjunto completo de soluciones diseñadas para ayudar a las organizaciones a administrar, proteger y gobernar sus datos en diversos entornos, que abarcan la seguridad de los datos, el cumplimiento normativo y la gobernanza de datos.

Los productos de cumplimiento de Microsoft Purview, como Administrador de cumplimiento y Cumplimiento de comunicaciones, ayudan a las organizaciones a cumplir los estándares normativos y administrar los riesgos. El Administrador de cumplimiento proporciona un panel unificado para evaluar y mejorar el cumplimiento con respecto a estándares como RGPD e HIPAA, ofreciendo plantillas, evaluaciones de riesgos y recomendaciones. El Cumplimiento de comunicaciones garantiza que las comunicaciones internas adhieran a las directivas mediante el uso de IA para detectar el incumplimiento, lo que ayuda a las organizaciones a mantener un ecosistema de comunicación conforme.

El conjunto de Gobierno de datos de Microsoft Purview está estrechamente relacionado con el cumplimiento de la normativa de datos, lo que garantiza que los datos se administren de forma apropiada, sean confiables y utilizables para la toma de decisiones empresariales. Las soluciones de gobernanza de datos como Catálogo de datos de Microsoft Purview y Microsoft Purview Data Insights se centran en la administración de metadatos, el linaje de los datos y la supervisión de la calidad de los datos, lo que ayuda a las organizaciones a organizar y gobernar eficazmente los activos de datos. Estas herramientas permiten a las organizaciones comprender de dónde provienen sus datos, cómo se transforman y garantizar que los usuarios tengan acceso a datos precisos y de alta calidad. El gobierno de datos efectivo no solo mejora el cumplimiento, sino que también mejora la capacidad de detección de datos y facilita una mejor toma de decisiones basada en datos.

La interconexión entre estas áreas es fundamental: los datos seguros se gobiernan con más facilidad y los datos gobernados facilitan el cumplimiento, lo que crea un enfoque unificado para proteger y administrar los datos a lo largo de todo su ciclo de vida.

# Conclusión

La seguridad de los datos es un imperativo en la era de la IA. Elegir Microsoft Purview es un gran paso hacia una mayor seguridad de datos en su organización. Seguir las estrategias de esta guía puede maximizar el valor total de su inversión.

Proteger los datos de su organización no solo consiste en implementar las herramientas adecuadas, sino también en fomentar una cultura de conciencia de seguridad y colaboración. Al aprovechar Microsoft Purview y seguir los procedimientos recomendados descritos en esta guía, puede crear una estrategia de seguridad de datos sólida que proteja sus activos valiosos y respalde sus objetivos empresariales.

Obtenga más información sobre Microsoft Purview, Protección de la información, Prevención de pérdida de datos de Purview y Gestión de riesgos internos. Descubra cómo Microsoft 365 Copilot puede ser su asistente de IA en su misión de fortalecer la seguridad de los datos.

Seguridad de Microsoft