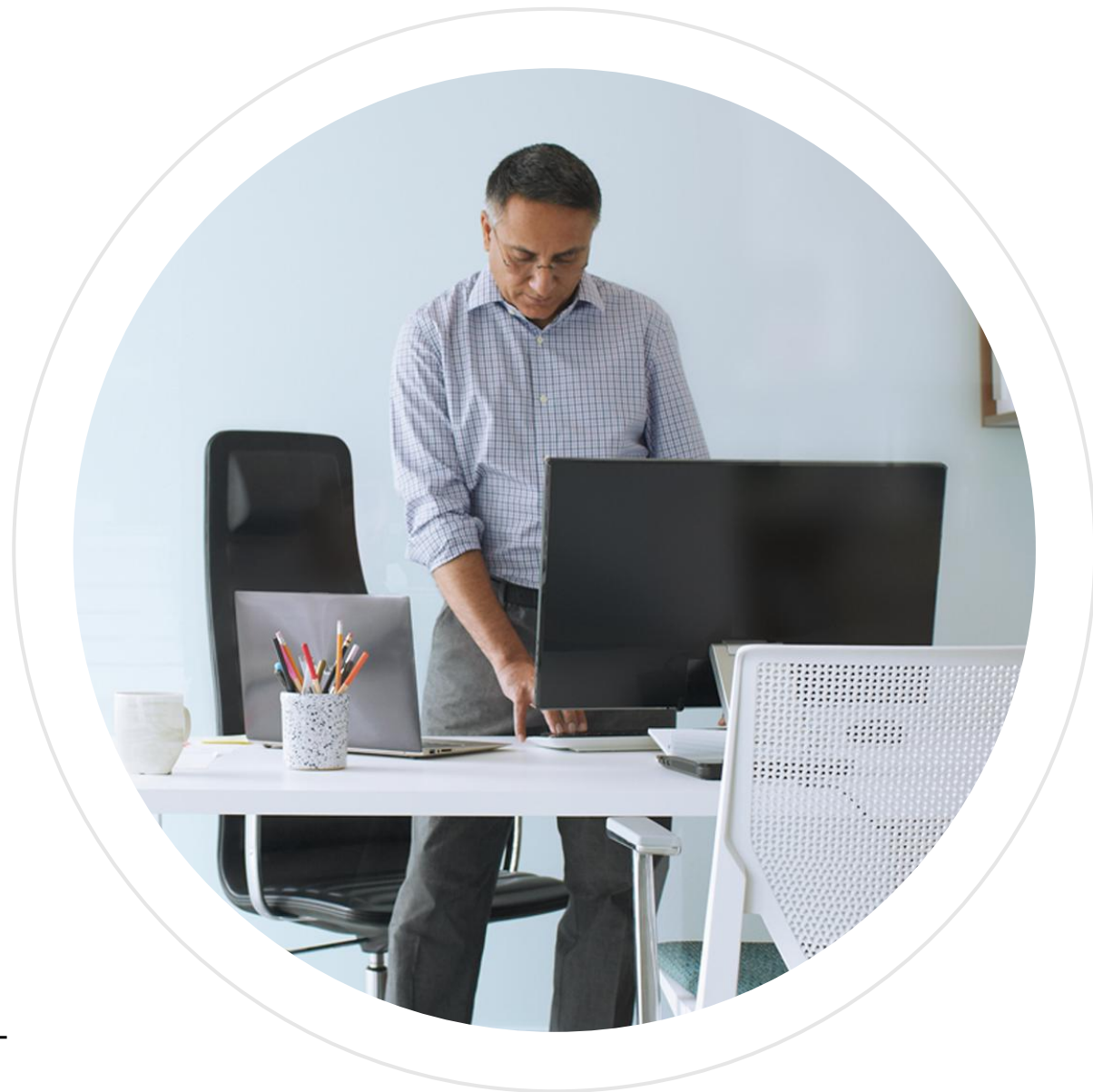


Describir las funcionalidades de las soluciones de cumplimiento de Microsoft

<https://learn.microsoft.com/es-mx/training/paths/describe-capabilities-of-microsoft-compliance-solutions/>



Lecturas

1. Diijase a SC-900: Microsoft Security, Compliance, and Identity Fundamentals
2. Realice la lectura de la ruta de aprendizaje: [Describir las funcionalidades de las soluciones de cumplimiento de Microsoft](#)





Los servicios en la nube de Microsoft se basan en **confianza, seguridad y cumplimiento.**

confianza

Microsoft nos **describe las practicas**
que ellos emplean para proteger
nuestra información.

confianza

Microsoft **nos muestra** cuáles
servicios podemos usar para
proteger nuestra información.

seguridad

Microsoft nos muestra cuáles
servicios podemos usar para
proteger nuestra información.



Microsoft nos muestra herramientas
que nos permite **vigilar si nuestra
organización está cumpliendo ciertas
reglas o estándares.**

cumplimiento



Confianza

Portal de confianza de servicios

Proporciona una variedad de contenido, herramientas y otros recursos sobre:

- Cómo los servicios en la nube de Microsoft protegen los datos.
- Cómo se puede administrar el cumplimiento y la seguridad de los datos en la nube para su organización.

The screenshot shows the Microsoft Service Trust Portal homepage. At the top, there's a navigation bar with the Microsoft logo, 'Service Trust Portal', 'My Library', 'All Documents', a search icon, and a 'Sign in' link. The main header is blue with the text 'Service Trust Portal' and a subtitle: 'Learn how Microsoft cloud services protect your data, and how you can manage cloud data security and compliance for your organization.' To the right of the text is an illustration of a shield, a key, a cloud, and a magnifying glass. Below the header, the page is organized into several sections:

- Certifications, Regulations and Standards:** This section contains a grid of 10 tiles, each representing a different certification or regulation. The tiles are: ISO/IEC (International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)), SOC (System and Organization Controls (SOC) 1, 2, and 3 Reports), GDPR (General Data Protection Regulation), FedRAMP (Federal Risk and Authorization Management Program), PCI (Payment Card Industry (PCI) Data Security Standards (DSS)), CSA STAR (Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR)), IRAP (Australia Information Security Registered Assessors Program (IRAP)), Singapore MTCS (Multi-Tier Cloud Security (MTCS) Singapore Standard), Spain ENS (Spain Esquema Nacional de Seguridad (ENS)), and ENS (Spain Esquema Nacional de Seguridad (ENS)).
- Reports, Whitepapers and Artifacts:** This section contains a grid of 4 tiles: BCP and DR (Business Continuity and Disaster Recovery), Pen Test and Security Assessments (Attestation of Penetration tests and security assessments conducted by third parties), Privacy and Data Protection (Privacy and Data Protection Resources), and FAQ and Whitepapers (Whitepapers and answers to frequently asked questions).
- Industry and Regional Resources:** This section contains a grid of 5 tiles: Financial Services (Resources elaborating regulatory compliance guidance for FSI (by country)), Healthcare and Life Sciences (Capabilities offered by Microsoft for Healthcare Industry), Media and Entertainment (Media and Entertainment Industry Resources), United States Government (Resources exclusively for US Government customers), and Regional Resources (Documents describing compliance of Microsoft's online services with various regional policies and regulations).
- Resources for your Organization:** This section contains a single tile: Resources for your Organization (Documents based on your organization's subscription and permissions).

Seguridad (Privacidad)

Principios de privacidad de Microsoft



Control: ponerle a usted, el cliente, en control de su privacidad con herramientas fáciles de usar y opciones claras.



Transparencia: ser transparentes sobre la recopilación y utilización de datos para que todos puedan tomar decisiones informadas.



Seguridad: protección de los datos confiados a Microsoft mediante una seguridad y un cifrado sólidos.



Fuertes protecciones legales: Respetar las leyes locales de privacidad y luchar por la protección legal de la privacidad como derecho humano fundamental.



Sin segmentación basada en contenido: no usar correo electrónico, chat, archivos u otro contenido personal para orientar la publicidad.



Ventajas para usted: Cuando Microsoft recopila datos, los utiliza para beneficiarle a usted, el cliente, y para mejorar su experiencia.

Microsoft Priva

- Las organizaciones recolectan información de sus clientes.
- El proceso de recolección y manipulación de datos de los clientes esta regido por políticas y normativas (ej. Política de tratamiento de datos personales).
- Por lo tanto, los usuarios conceden derechos a las organizaciones para recolectar y administrar sus datos.
- Pero las organizaciones deben garantizar la privacidad de los datos de sus clientes de acuerdo a la normativa de cada país.
- Microsoft Priva es servicio que ayuda a las organizaciones a garantizar la protección de los datos de sus clientes.

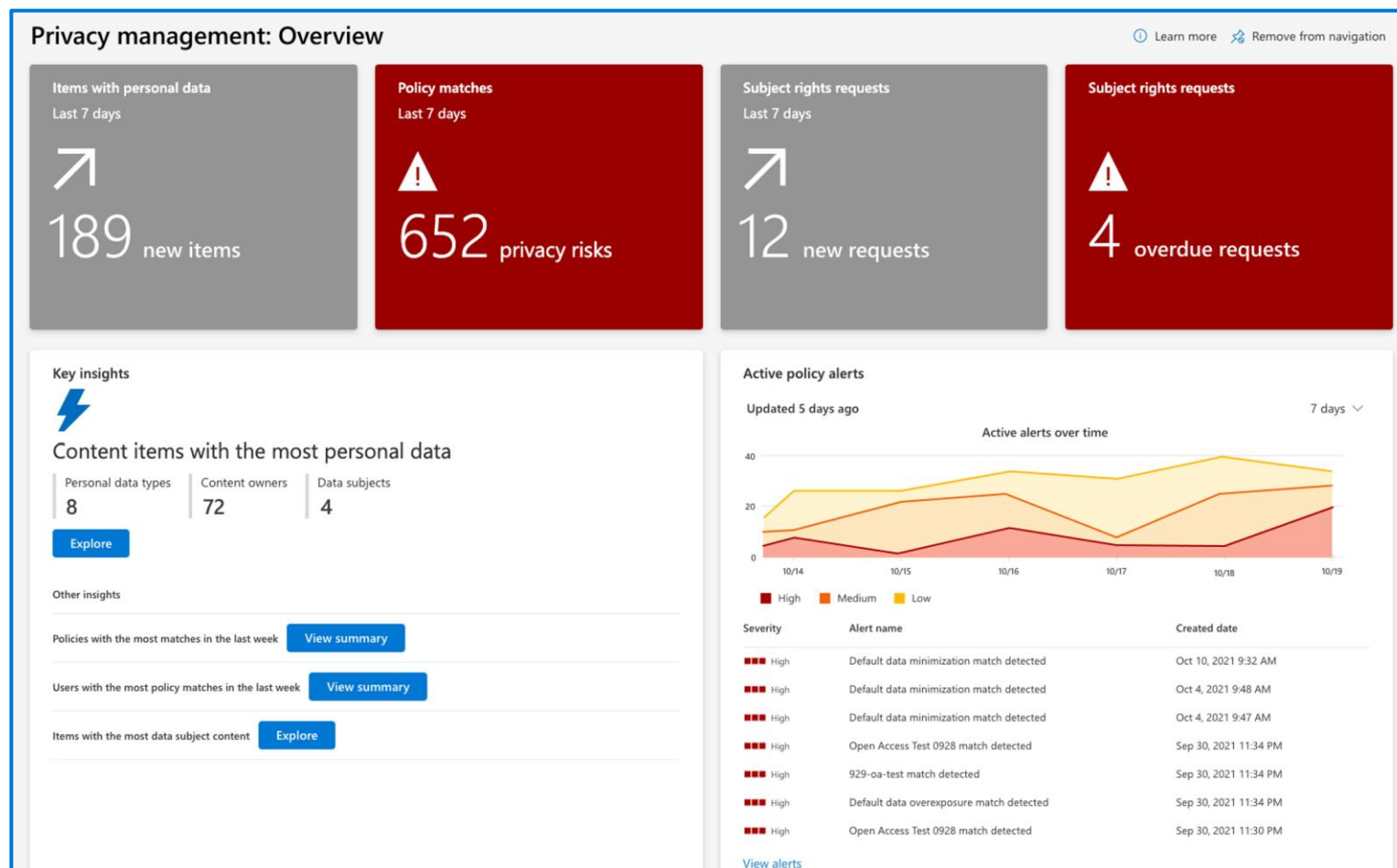
Microsoft Priva

Administración de riesgo de privacidad Priva

- Se conecta con Microsoft Purview para recolectar información de posibles riesgos de privacidad.
- El perfil de datos proporciona una vista de los datos personales que la organización almacena de sus clientes.

Solicitudes de derechos de los interesados Priva

Capacidades de flujo de trabajo, automatización y colaboración para ayudarle a buscar datos de los interesados (ej. clientes), revisar las conclusiones, recopilar los archivos adecuados y generar informes.



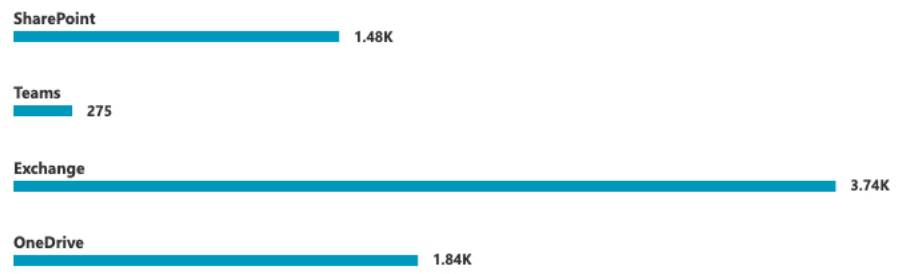
Privacy management: Data profile

Settings

Learn more

Remove from navigation

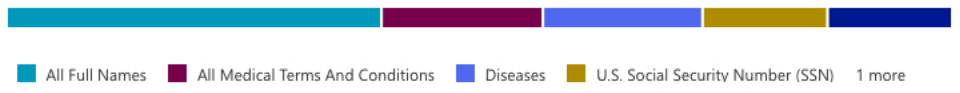
Personal data type instances detected in Microsoft 365 locations



Location	Personal data types	Last updated
SharePoint	64	Oct 13, 2021 5:00 PM
Teams	16	Oct 13, 2021 5:00 PM
Exchange	29	Oct 13, 2021 5:00 PM
OneDrive	48	Oct 13, 2021 5:00 PM

[Explore](#)

Top personal data types across your organization



Personal data type	Count	Location	Last updated
All Full Names	1.36K	ODB, SharePoint, +2 others	Oct 13, 2021 5:00 PM
All Medical Terms And Conditions	583	ODB, SharePoint, +2 others	Oct 13, 2021 5:00 PM
Diseases	577	SharePoint, ODB, +2 others	Oct 13, 2021 5:00 PM

[Explore all personal data types](#)

Personal data type instances by region



[Explore personal data by region](#)

Cumplimiento

Microsoft Purview

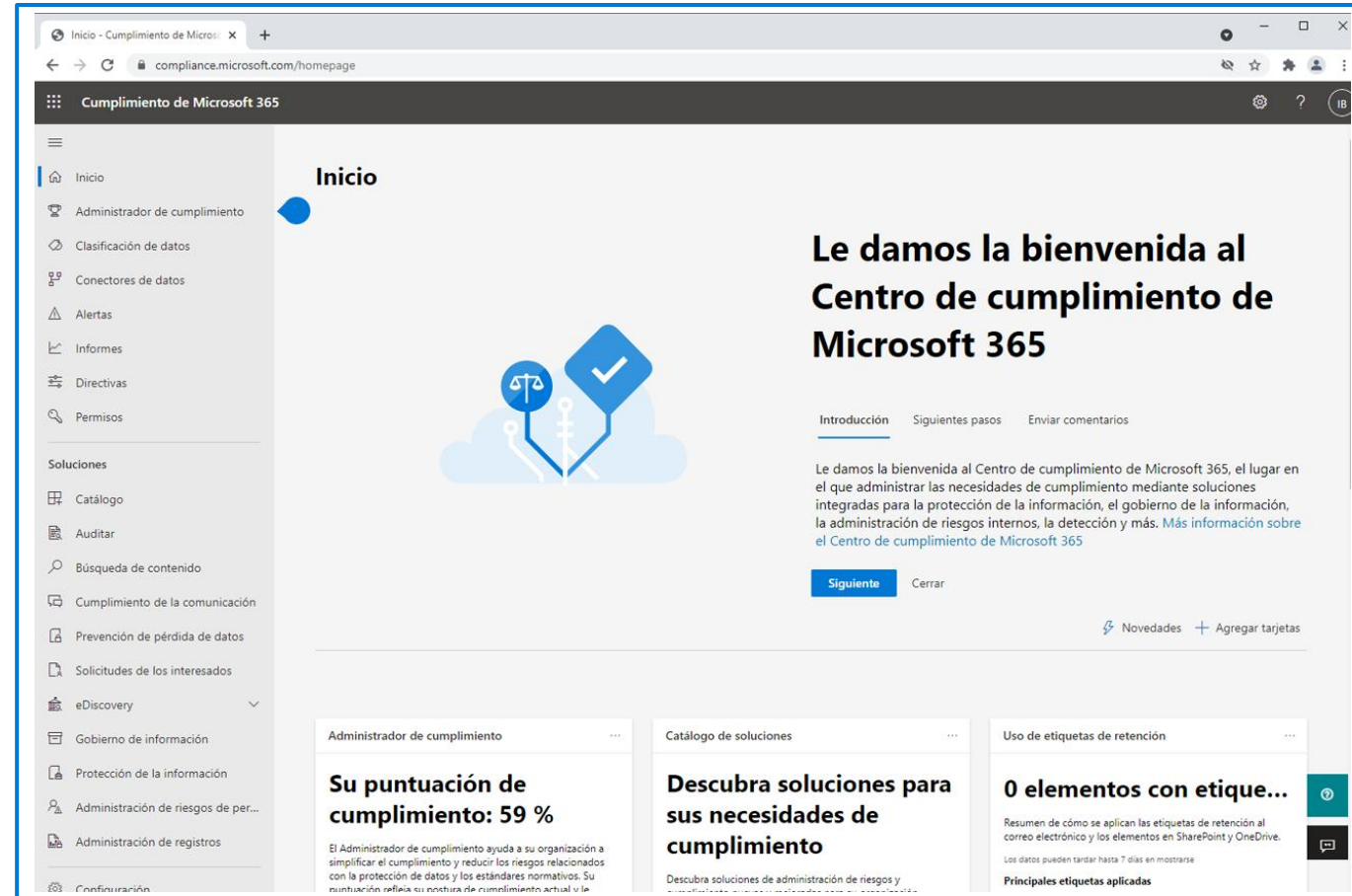


Portal de cumplimiento de Microsoft Purview

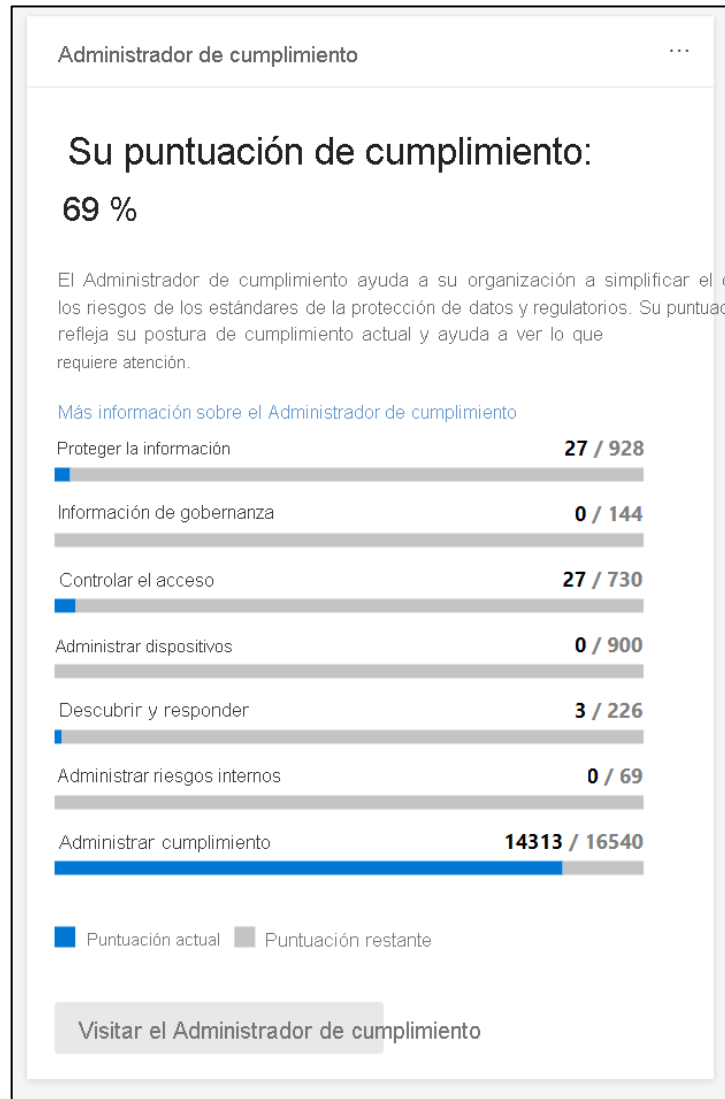
Portal de cumplimiento de Microsoft Purview

Las organizaciones deben mantener actualizados los **estándares legales, normativos** y de **privacidad** relacionados con el cumplimiento para proteger a sus clientes, asociados y a ellas mismas.

- Purview permite validar si la organización esta cumpliendo con los estándares legales, normativos y de privacidad.
- La validación se realiza analizando los datos que la organización tiene de sus clientes, así mismo se analizan los servicios de Azure que usan los clientes.



Portal de cumplimiento de Microsoft Purview



Inicio - Cumplimiento de Micro... x +

compliance.microsoft.com/homepage

Cumplimiento de Microsoft 365

Inicio

Administrador de cumplimiento

Clasificación de datos

Conectores de datos

Alertas

Informes

Directivas

Permisos

Soluciones

Catálogo

Auditar

Búsqueda de contenido

Cumplimiento de la comunicación

Prevención de pérdida de datos

Solicitudes de los interesados

eDiscovery

Gobierno de información

Protección de la información

Administración de riesgos de per...

Administración de registros

Configuración

Inicio

Le damos la bienvenida al Centro de cumplimiento de Microsoft 365

[Introducción](#) [Sigüientes pasos](#) [Enviar comentarios](#)

Le damos la bienvenida al Centro de cumplimiento de Microsoft 365, el lugar en el que administrar las necesidades de cumplimiento mediante soluciones integradas para la protección de la información, el gobierno de la información, la administración de riesgos internos, la detección y más. [Más información sobre el Centro de cumplimiento de Microsoft 365](#)

[Sigüiente](#) [Cerrar](#)

[Novedades](#) [Agregar tarjetas](#)

Administrador de cumplimiento

Su puntuación de cumplimiento: 59 %

El Administrador de cumplimiento ayuda a su organización a simplificar el cumplimiento y reducir los riesgos relacionados con la protección de datos y los estándares normativos. Su puntuación refleja su postura de cumplimiento actual y la

Catálogo de soluciones

Descubra soluciones para sus necesidades de cumplimiento

Descubra soluciones de administración de riesgos y

Uso de etiquetas de retención

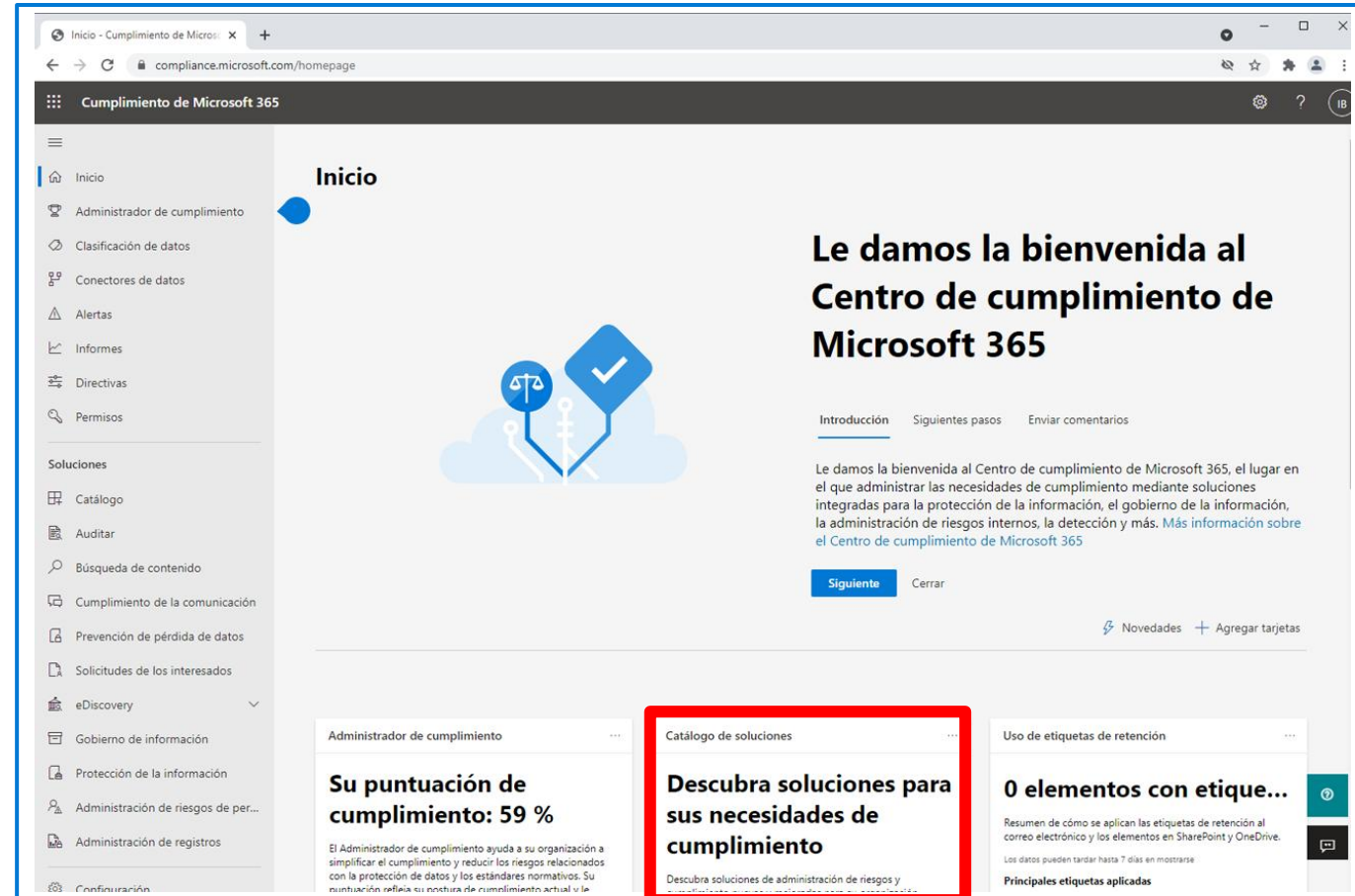
0 elementos con etique...

Resumen de cómo se aplican las etiquetas de retención al correo electrónico y los elementos en SharePoint y OneDrive. Los datos pueden tardar hasta 7 días en mostrarse.

Principales etiquetas aplicadas

<https://www.youtube.com/watch?v=Kteh9cXkHIE>

Portal de cumplimiento de Microsoft Purview



Portal de cumplimiento de Microsoft Purview

Alertas activas

34 alertas activas

Nombre de la alerta	Gravedad
El usuario que comparte una gran ...	<div></div> Medio
El usuario que comparte una gran ...	<div></div> Medio
Elevación de privilegios de adminis...	<div></div> Bajo
El usuario que comparte una gran ...	<div></div> Medio
El usuario que comparte una gran ...	<div></div> Medio
El usuario que comparte una gran ...	<div></div> Medio
El usuario que comparte una gran ...	<div></div> Medio
El usuario que comparte una gran ...	<div></div> Medio

Mostrar más

Inicio - Cumplimiento de Micro...

compliance.microsoft.com/homepage

Cumplimiento de Microsoft 365

Inicio

Administrador de cumplimiento

Clasificación de datos

Conectores de datos

Alertas

Informes

Directivas

Permisos

Soluciones

Catálogo

Auditar

Búsqueda de contenido

Cumplimiento de la comunicación

Prevención de pérdida de datos

Solicitudes de los interesados

eDiscovery

Gobierno de información

Protección de la información

Administración de riesgos de per...

Administración de registros

Configuración

Inicio

Le damos la bienvenida al Centro de cumplimiento de Microsoft 365

Introducción

Siguientes pasos

Enviar comentarios

Le damos la bienvenida al Centro de cumplimiento de Microsoft 365, el lugar en el que administrar las necesidades de cumplimiento mediante soluciones integradas para la protección de la información, el gobierno de la información, la administración de riesgos internos, la detección y más. [Más información sobre el Centro de cumplimiento de Microsoft 365](#)

Siguiente

Cerrar

Novedades

Agregar tarjetas

Administrador de cumplimiento

Su puntuación de cumplimiento: 59 %

El Administrador de cumplimiento ayuda a su organización a simplificar el cumplimiento y reducir los riesgos relacionados con la protección de datos y los estándares normativos. Su puntuación refleja su postura de cumplimiento actual y la...

Catálogo de soluciones

Descubra soluciones para sus necesidades de cumplimiento

Descubra soluciones de administración de riesgos y...

Uso de etiquetas de retención

0 elementos con etique...

Resumen de cómo se aplican las etiquetas de retención al correo electrónico y los elementos en SharePoint y OneDrive. Los datos pueden tardar hasta 7 días en mostrarse

Principales etiquetas aplicadas

© Copyright Microsoft Corporation. Todos los derechos reservados.

Microsoft Purview

Administrador de Cumplimiento



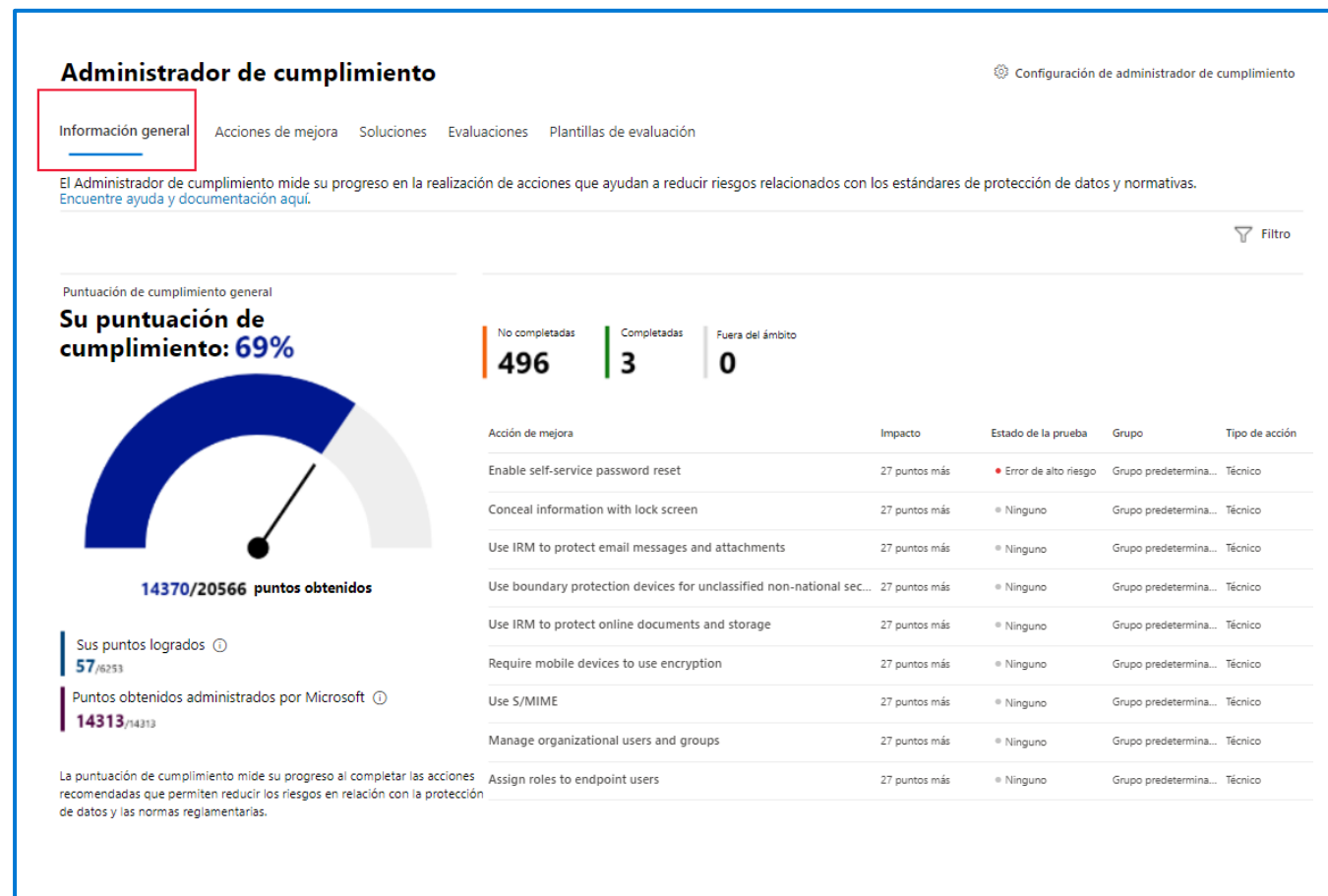
Administrador de cumplimiento

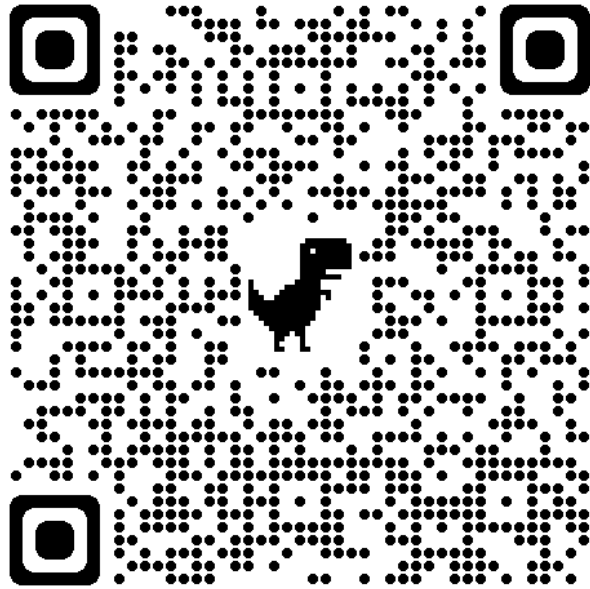
El Administrador de cumplimiento simplifica el cumplimiento y reduce el riesgo mediante lo siguiente:

- Evaluaciones predefinidas basadas en estándares comunes.
- Acciones de mejora detalladas paso a paso.
- Puntuación de cumplimiento, muestra el estado general respecto al cumplimiento.

Elementos clave del Administrador de cumplimiento

- Controles
- Valoraciones
- Plantillas
- Acciones de mejora





Demostración

Administrador de Cumplimiento de Microsoft Purview



Microsoft Purview

Conocimiento, protección y gobernanza de los datos



Conocimiento, protección y gobernanza de los datos



Conozca sus datos: Comprenda sus datos en general e identifique datos importantes en entornos locales, en la nube e híbridos.



Proteja sus datos: Aplique acciones de protección flexibles, como el cifrado, las restricciones de acceso y las marcas visuales.



Evite la pérdida de datos: Detecte comportamientos arriesgados y evite compartir información confidencial por accidente.



Administre sus datos: Guarde, elimine y almacene datos y registros automáticamente de una manera conforme a las normativas.



Funcionalidades de clasificación de datos del portal de cumplimiento



Tipos de información confidencial.



Clasificadores capacitados: clasificadores preparados previamente y clasificadores capacitados personalizados.



Comprender y explorar los datos.



El explorador de contenido: Permite a los administradores obtener visibilidad sobre el contenido que se ha resumido en el panel de información general.



El explorador de actividades: Puede supervisar lo que se está haciendo con el contenido etiquetado en la organización.

Sus conjuntos de clasificaciones principales



- Estados Unidos Datos financieros
- Estados Unidos Datos de información personal identificable (P
- Estados Unidos Ley de seguros de salud (HIPAA)
- Reino Unido Datos financieros
- Reino U

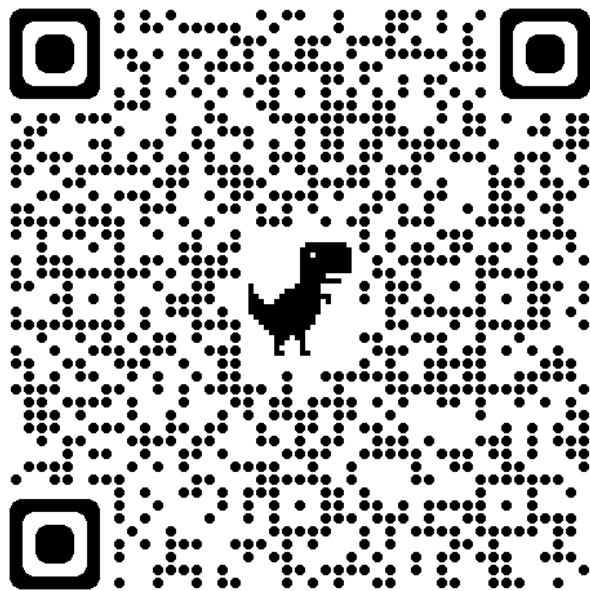
[Explorar datos según reguladores del sector en el explorador de contenido](#)

Tipos de información de alta confidencialidad

Col **Número de pasaporte de Holanda** **405** **que se**



- Número de pasaporte de Holanda
- Número de pas



Demostración

Funcionalidades de clasificación
de datos del portal de
cumplimiento



Microsoft Purview

Etiquetas y directivas de confidencialidad



Etiquetas y directivas de confidencialidad

Etiquetas de confidencialidad

Las etiquetas son:

- Personalizable
- Texto no cifrado
- Persistente

Uso:

- Cifrar correos electrónicos y documentos.
- Marcar el contenido.
- Aplicar la etiqueta automáticamente.
- Proteger el contenido en contenedores: sitios y grupos.
- Extender las etiquetas de confidencialidad a aplicaciones y servicios de terceros.
- Clasificar el contenido sin usar ninguna configuración de protección.

Directivas de etiquetas

Las directivas permiten a los administradores hacer lo siguiente:

- Elegir los usuarios y los grupos que pueden ver las etiquetas.
- Aplicar una etiqueta por defecto a todos los correos electrónicos y documentos nuevos.
- Exigir justificación para cambiar etiquetas.
- Exigir que los usuarios apliquen una etiqueta (etiquetado obligatorio).

Una vez que se aplica una etiqueta de confidencialidad a un correo electrónico o un documento, se aplican al contenido los valores de protección configurados para esa etiqueta.

Microsoft Purview

Prevención de pérdida de datos (DLP)



Prevención de pérdida de datos (DLP)

La DLP protege la información confidencial y evita su divulgación inadvertida.

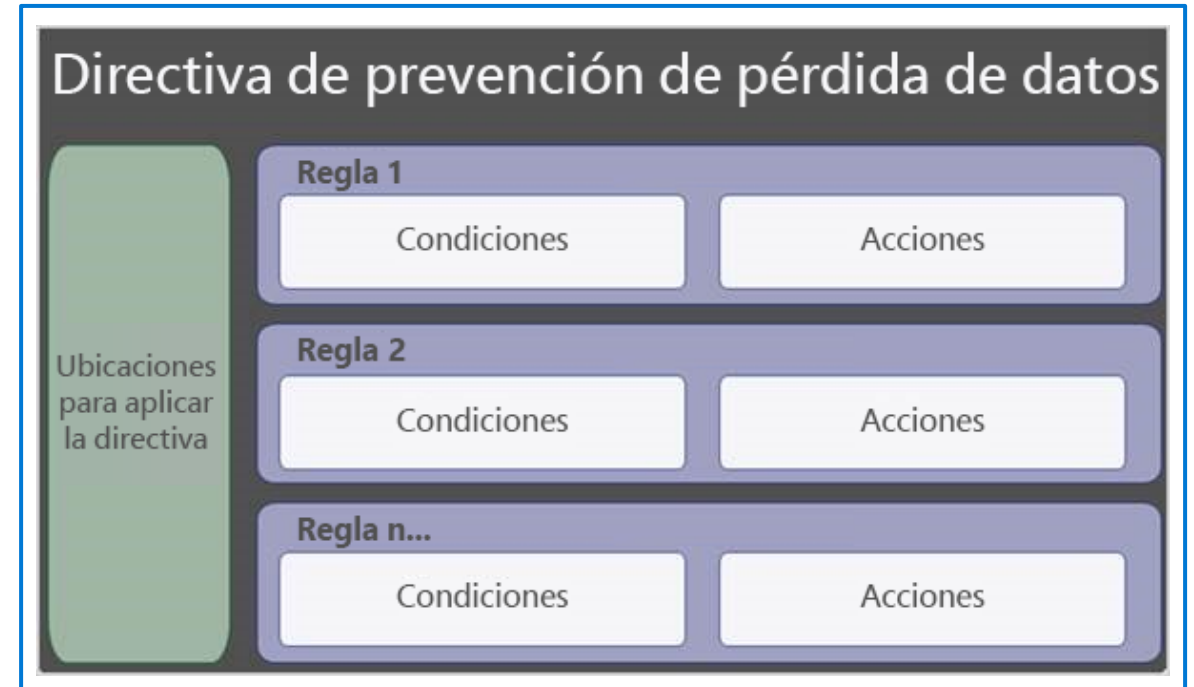
- Las directivas DLP protegen la información mediante la identificación y la protección automática de los datos confidenciales.
- Proteger la información confidencial en Microsoft 365: OneDrive para la Empresa, SharePoint Online, Exchange Online y Microsoft Teams.

Prevención de pérdida de datos en puntos de conexión

- DLP extendida a dispositivos con Windows 10.
- Auditar y administrar las actividades, entre las que se incluyen la creación, copia, impresión y cambio de nombre de elementos.

Prevención de pérdida de datos en Microsoft Teams

- Funcionalidades de DLP extendidas a los chats y mensajes de canal de Microsoft Teams.



Clasificación de datos

Información general Clasificadores que... Tipos de información conf... Explorad... Explorador de actividades

Revise la actividad relacionada con el contenido que alberga información confidencial o tiene etiquetas aplicadas, como qué etiquetas se cambiaron, qué archivos se modificaron, dispositivos... Próximamente se ofrecerá compatibilidad con más ubicaciones. [Más información](#)

Filtro

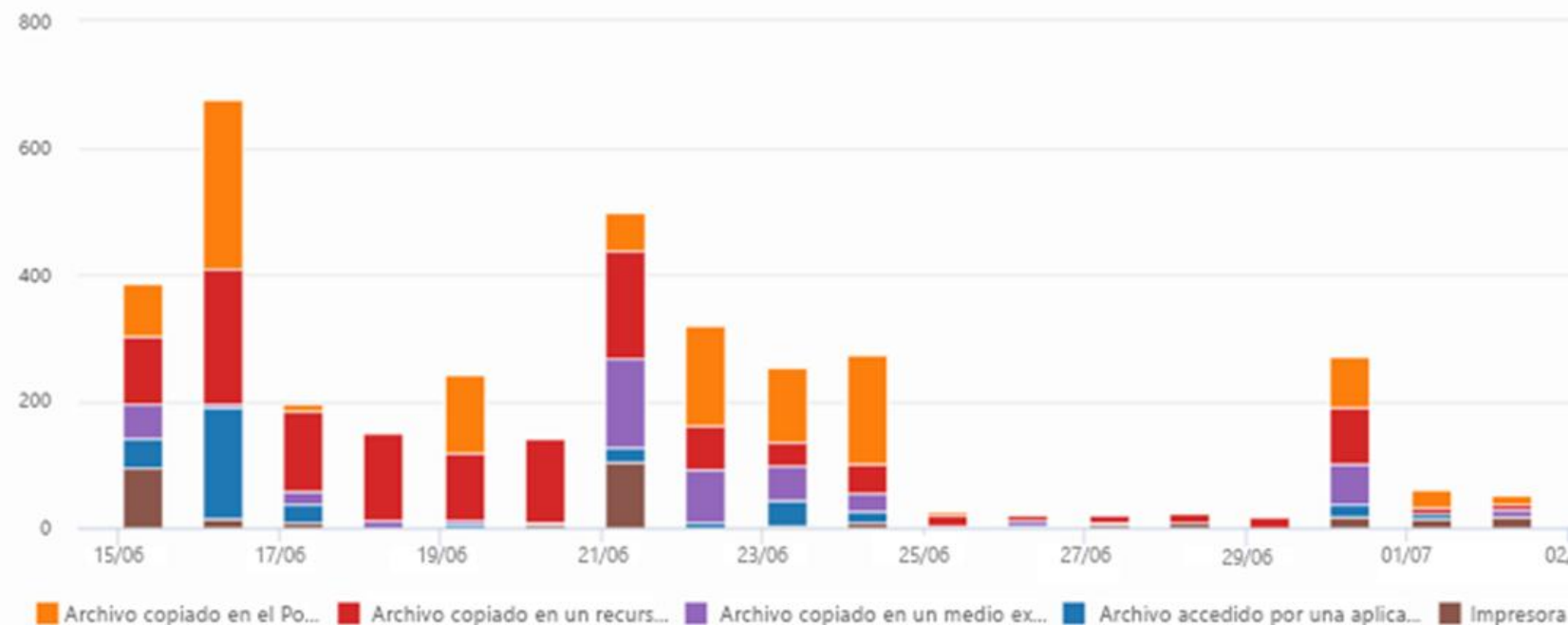
Fecha: 16/6/2020-16/7/2020

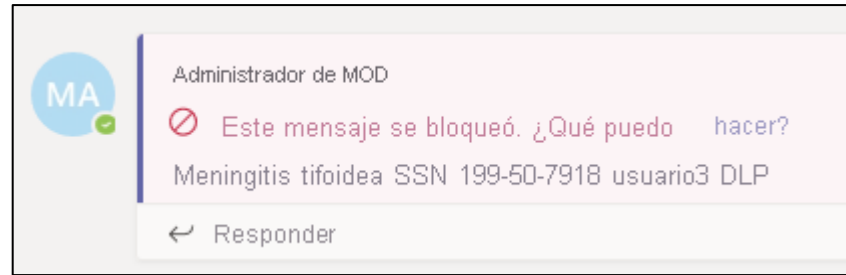
Actividad: FileCopiedToClipboard, FilePrinted, +4

Ubicación: Punto d...

Usuario: Cualq...

↓ Exportar





Su mensaje se ha bloqueado porque contiene datos confidenciales

- U.S. Social Security Number (SSN)
- International Classification of Diseases (ICD-10-CM)
- International Classification of Diseases (ICD-9-CM)

Este elemento está protegido por una directiva de su organización.

Esto es lo que hay que hacer:

Invalide la directiva y envíe el mensaje, o informe a su administrador si cree que el mensaje se bloqueó por error.

☐ Invalidar y enviar.

Escriba la justificación

☐ Notificar esto a mi administrador. No contiene datos confidenciales.

Cancelar

Confirmar

Microsoft Purview

Etiquetas y directivas de retención



Etiquetas y directivas de retención

Las directivas y las etiquetas de retención ayudan a las organizaciones a administrar y controlar la información, ya que **garantizan que el contenido se mantenga únicamente durante el tiempo necesario**. La configuración de retención funciona en SharePoint, OneDrive, Teams, Yammer y Exchange, y garantiza que el contenido se elimine para siempre tras un tiempo exigido.

Las etiquetas de retención tienen estas características:

- Se aplican a los elementos.
- **Solo se puede asignar una etiqueta de retención a la vez a los correos electrónicos y documentos.**
- La configuración de retención de las etiquetas de retención se mueve con el contenido en su inquilino de Microsoft 365.
- Se pueden aplicar manual o automáticamente.
- **Las etiquetas de retención admiten revisión para eliminación del contenido antes de que se elimine para siempre.**

Las directivas de retención tienen estas características:

- Se aplican en sitios o buzones.
- Se pueden aplicar a varias ubicaciones o a ubicaciones o usuarios específicos.
- **Los elementos heredan la configuración de retención de su contenedor.**
- Si se mueve un elemento, la configuración de retención no se mueve a la nueva ubicación.

Microsoft Purview

Administración de registros



Administración de registros

La administración de registros ayuda a una organización a ocuparse de sus obligaciones legales y a cumplir con las regulaciones.

- **Cuando el contenido se etiqueta como un registro, ocurre lo siguiente:**
 - Se aplican restricciones para impedir determinadas actividades.
 - Se registran las actividades.
 - La prueba para la eliminación se mantiene al final del período de retención.
- Para permitir que los elementos se marquen como registros, un administrador configura etiquetas de retención.

Durante el período de retención

☐ Conservar elementos aunque los usuarios los eliminen

☒ Marcar elementos como registro

Los usuarios no podrán editar ni eliminar correos electrónicos, y solo algunos usuarios podrán modificar o quitar la etiqueta. No podrán eliminar archivos de SharePoint ni OneDrive, pero se les bloquean o permiten otras acciones en función de si el estado de registro del elemento está bloqueado o desbloqueado. [Más información](#)

☐ Marcar elementos como registro reglamentario

Al final del período de retención:

☒ Eliminar elementos automáticamente

Los elementos se eliminarán de forma automática del lugar donde están almacenados actualmente.

Microsoft Purview

Administración de registros



Soluciones de riesgo interno en Microsoft Purview



La **administración de riesgo interno** minimiza los riesgos internos al **permitirle detectar, investigar y tomar medidas sobre las actividades malintencionadas e inadvertidas en su organización.**



El **cumplimiento** de comunicaciones minimiza los riesgos de comunicaciones al **ayudarle a detectar, capturar y tomar acciones ante mensajes inapropiados en su organización.** Servicios compatibles: Microsoft Teams, Exchange Online, Yammer y comunicaciones con terceros en una organización.



Las **barreras de información** le **permiten restringir la comunicación y la colaboración entre dos grupos internos para evitar que se produzca un conflicto de intereses** en su organización. Funcionan en Microsoft Teams, OneDrive para la Empresa, SharePoint Online, etc.

Microsoft Purview eDiscovery



eDiscovery en Microsoft Purview

- La exhibición de documentos electrónicos, o eDiscovery, **es el proceso de identificación y entrega de información electrónica que se puede utilizar como prueba en casos legales.**
- Herramientas de eDiscovery: Búsqueda de contenido, eDiscovery (Standard), eDiscovery (Premium)

Búsqueda de contenido	Core eDiscovery	eDiscovery avanzado
<ul style="list-style-type: none">■ Buscar contenido■ Consultas de palabras clave y condiciones de búsqueda■ Exportar resultados de la búsqueda■ Permisos basados en roles 	<ul style="list-style-type: none">■ Buscar y exportar■ Administración de casos■ Suspensión legal 	<ul style="list-style-type: none">■ Administración de custodios■ Notificaciones de suspensión legal■ Indexación avanzada■ Filtros para conjuntos de revisión■ Etiquetado■ Análisis■ Modelos de codificación predictiva■ Y mucho más. 

Auditoría en Microsoft Purview

- Las soluciones de auditoría de Microsoft Purview ayudan a las organizaciones a responder eficazmente a eventos de seguridad, investigaciones forenses, investigaciones internas y obligaciones de cumplimiento.
- Microsoft Purview proporciona dos soluciones de auditoría: Auditoría (Estándar) y Auditoría (Premium).

Auditoría básica



Registre y busque actividades auditadas:

- Habilitado de forma predeterminada
- Miles de eventos auditados
- Retención de registros de auditoría de 90 días
- Se puede acceder a través de la GUI, cmdlet y API

Auditoría avanzada



Capacidades de auditoría avanzada:

- Mayor retención de registros de auditoría
- Directivas de retención de auditorías personalizadas
- Eventos cruciales de gran valor
- Acceso de ancho de banda más amplio a las API



Governanza

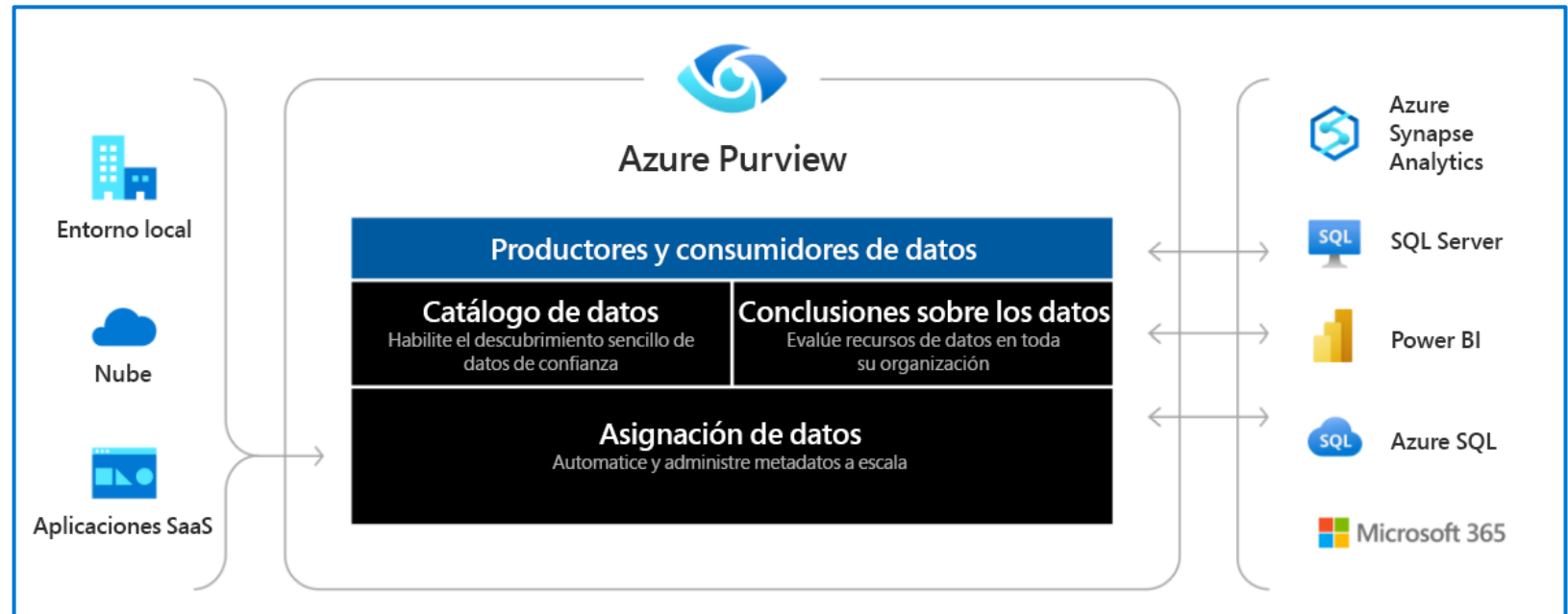
Microsoft Purview



Microsoft Purview

Microsoft Purview es un servicio unificado de gobernanza de datos que ayuda a las organizaciones a administrar y gobernar los datos locales, de varias nubes y de software como servicio (SaaS).

- Mapa de datos: capture metadatos sobre los datos empresariales, a fin de identificar y clasificar los datos confidenciales.
- Catálogo de datos: busque datos pertinentes de forma rápida y fácil.
- Conclusiones de datos de infraestructura: entienda qué datos se examinan activamente, dónde se encuentran los datos confidenciales y cómo se mueven.

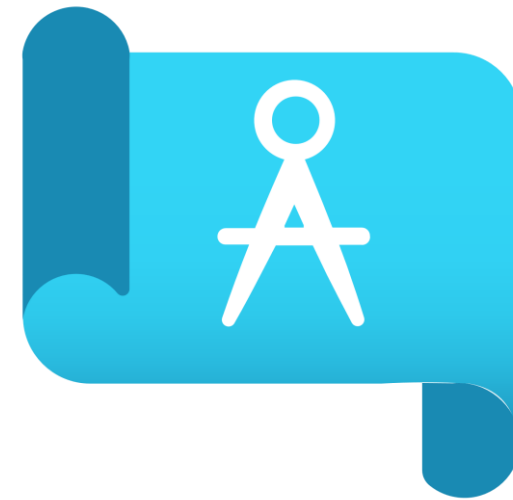


Azure Blue Prints



Azure Blue Prints

Azure Blue Prints (Planos de Azure) Planos de Azure permite **definir un grupo de recursos** de forma declarativa y, posteriormente, permite **automatizar el despliegue** de los recursos en Azure.



Azure Blue Prints

Un plano de Azure se constituye de **cuatro artefactos**:

1. Azure Resource Management (ARM) Template
2. Resource Group
3. Role-based access control (RBAC)
4. Azure policies



Azure Blue Prints

Un plano de Azure se constituye de **cuatro artefactos**:

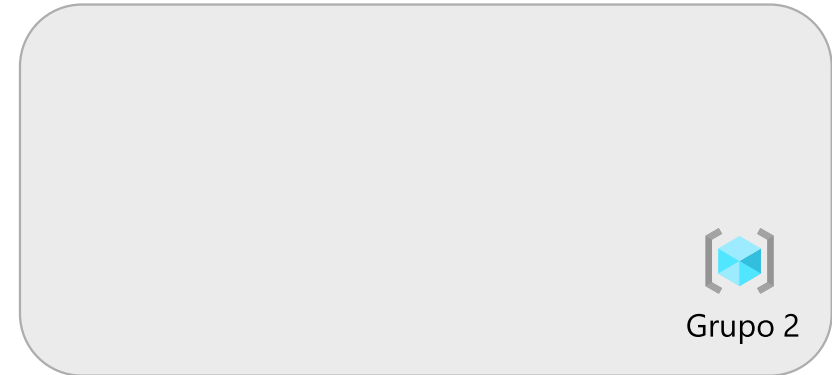
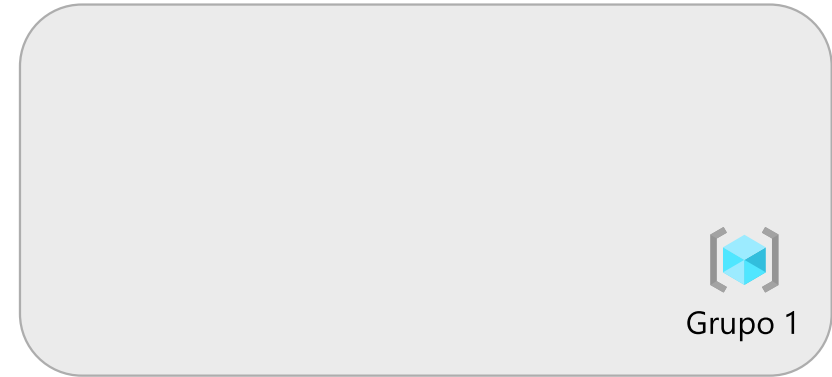
1. Grupos de recursos
2. Plantillas de Azure Resource Manager
3. Asignación de directivas (o políticas)
4. Asignación de roles



Azure Blue Prints

Un plano de Azure se constituye de cuatro artefactos:

1. **Grupos de recursos**
2. Plantillas de Azure Resource Manager
3. Asignación de directivas (o políticas)
4. Asignación de roles



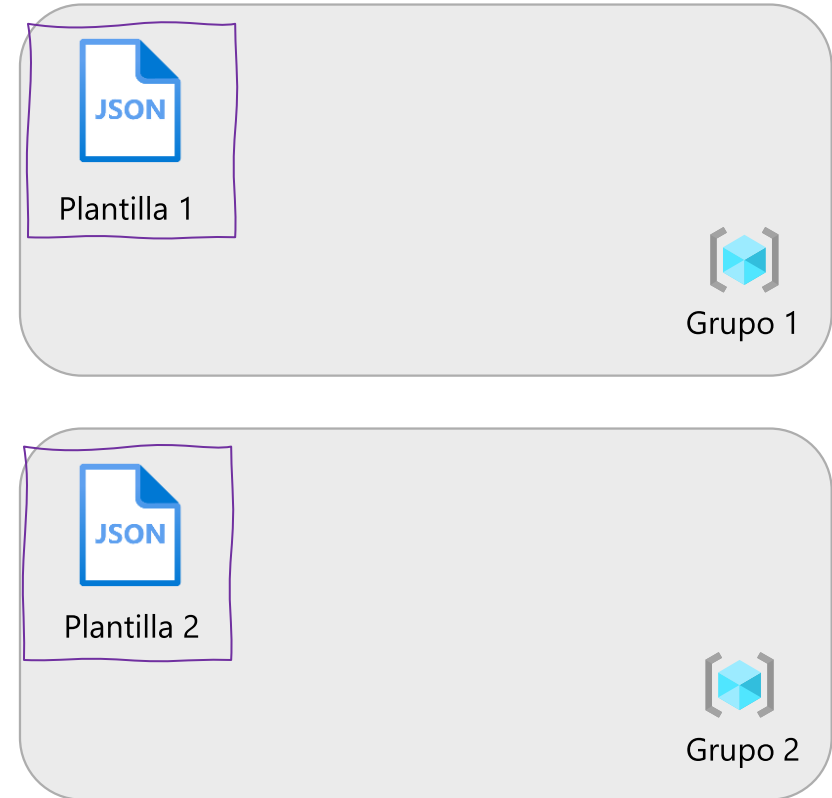
Los grupos de recursos permiten estructurar y organizar los recursos de forma que se facilite su administración.



Azure Blue Prints

Un plano de Azure se constituye de cuatro artefactos:

1. Grupos de recursos
2. **Plantillas de Azure Resource Manager**
3. Asignación de directivas (o políticas)
4. Asignación de roles



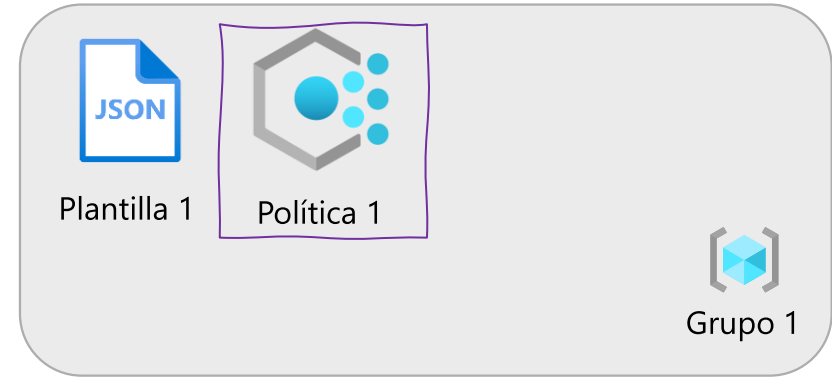
Las plantillas de Azure Resource Manager permiten **definir la infraestructura** que se desea desplegar en la nube de forma declarativa.



Azure Blue Prints

Un plano de Azure se constituye de cuatro artefactos:

1. Grupos de recursos
2. Plantillas de Azure Resource Manager
3. **Asignación de directivas (o políticas)**
4. Asignación de roles



Las directivas o políticas de Azure permiten validar que los recursos cumplen con los requisitos que establece una organización.

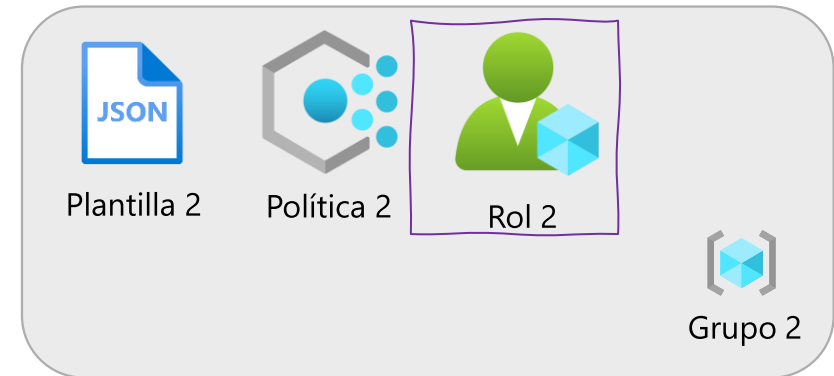
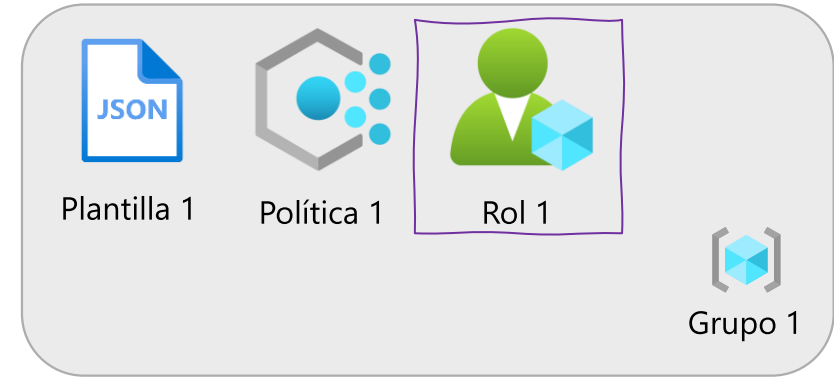
Las directivas se construyen a partir de **propiedades de los recursos** como su ubicación, tipos de recursos, [entre otros](#).



Azure Blue Prints

Un plano de Azure se constituye de cuatro artefactos:

1. Grupos de recursos
2. Plantillas de Azure Resource Manager
3. Asignación de directivas (o políticas)
4. **Asignación de roles**



Los roles de Azure permiten administrar **quién accede a los recursos de Azure, qué puede hacer con esos recursos y a qué áreas (ej. Portal) puede acceder.**

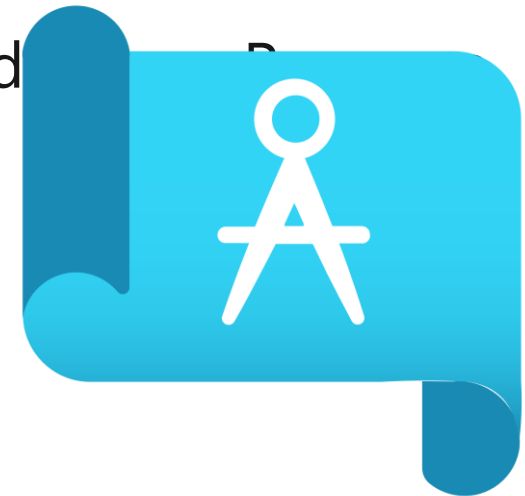


Azure Blue Prints

Azure Blue Prints (Planos de Azure) Planos de Azure permite **definir la infraestructura** de forma declarativa y, posteriormente, permite **automatizar el despliegue** de la infraestructura definida en Azure.

Los planos de azure consta de los siguientes artefactos:

1. Azure Resource Management (ARM) Templates (Plantillas de Azure Resource Manager).
2. Grupos de recursos
3. Role-based access control (RBAC)
4. Azure policies



Planos de Azure

Azure Blueprints

deploy and update cloud environments in a repeatable manner using composable artifacts

