# Utilizar la clasificación de datos

## NetApp Data Classification

NetApp
February 11, 2026

This PDF was generated from https://docs.netapp.com/es-es/data-services-data-classification/task-controlling-governance-data.html on February 11, 2026. Always check docs.netapp.com for the latest.

# Tabla de contenidos

# Utilizar la clasificación de datos

## Vea los detalles de gobernanza sobre los datos almacenados en su organización con NetApp Data Classification

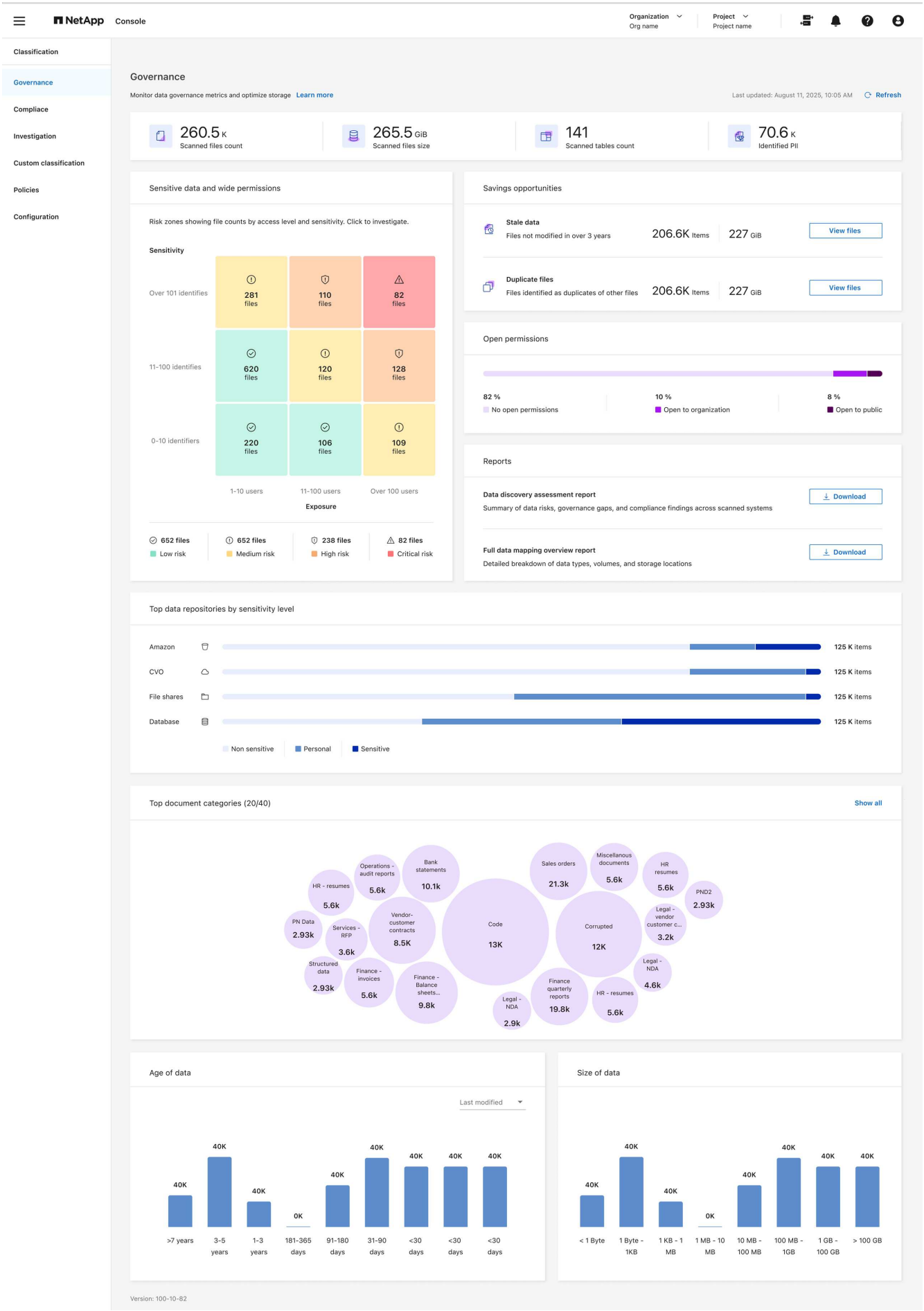
Obtenga control de los costos relacionados con los datos en los recursos de almacenamiento de su organización. La NetApp Data Classification identifica la cantidad de datos obsoletos, archivos duplicados y archivos muy grandes en sus sistemas para que pueda decidir si desea eliminar o agrupar algunos archivos en un almacenamiento de objetos menos costoso.

Aquí es donde debes comenzar tu investigación. Desde el panel de Gobernanza, puede seleccionar un área para realizar una investigación más profunda.

Además, si planea migrar datos desde ubicaciones locales a la nube, puede ver el tamaño de los datos y si alguno de ellos contiene información confidencial antes de moverlos.

### Revisar el panel de gobernanza

El panel de gobernanza proporciona información para que pueda aumentar la eficiencia y controlar los costos relacionados con los datos almacenados en sus recursos de almacenamiento.


NetApp Console
Organization
Org name
Project
Project name
Classification
Governance
Compliace
Investigation
Custom classification
Policies
Configuration
Governance
Monitor data governance metrics and optimize storage Learn more
Last updated: August 11, 2025, 10:05 AM
Refresh
260.5 K
Scanned files count
265.5 GiB
Scanned files size
141
Scanned tables count
70.6 K
Identified PII
Sensitive data and wide permissions
Risk zones showing file counts by access level and sensitivity. Click to investigate.
Sensitivity
Over 101 identifies
11-100 identifies
0-10 identifiers
281 files
110 files
82 files
620 files
120 files
128 files
220 files
106 files
109 files
1-10 users
11-100 users
Over 100 users
Exposure
652 files
Low risk
652 files
Medium risk
238 files
High risk
82 files
Critical risk
Savings opportunities
Stale data
Files not modified in over 3 years
206.6K Items
227 GiB
View files
Duplicate files
Files identified as duplicates of other files
206.6K Items
227 GiB
View files
Open permissions
82 %
No open permissions
10 %
Open to organization
8 %
Open to public
Reports
Data discovery assessment report
Summary of data risks, governance gaps, and compliance findings across scanned systems
Download
Full data mapping overview report
Detailed breakdown of data types, volumes, and storage locations
Download
Top data repositories by sensitivity level
Amazon
CVO
File shares
Database
125 K items
Non sensitive
Personal
Sensitive
Top document categories (20/40)
Show all
Operations - audit reports 5.6k
Bank statements 10.1k
Sales orders 21.3k
Miscellanous documents 5.6k
HR resumes 5.6k
PND2 2.93k
HR - resumes 5.6k
PN Data 2.93k
Services - RFP 3.6k
Vendor-customer contracts 8.5K
Code 13K
Corrupted 12K
Legal - vendor customer c... 3.2k
Structured data 2.93k
Finance - invoices 5.6k
Finance - Balance sheets... 9.8k
Legal - NDA 2.9k
Finance quarterly reports 19.8k
HR - resumes 5.6k
Legal - NDA 4.6k
Age of data
Last modified
40K
>7 years
40K
3-5 years
40K
1-3 years
0K
181-365 days
40K
91-180 days
40K
31-90 days
40K
<30 days
40K
<30 days
40K
<30 days
Size of data
40K
< 1 Byte
40K
1 Byte - 1KB
40K
1 KB - 1 MB
0K
1 MB - 10 MB
40K
10 MB - 100 MB
40K
100 MB - 1GB
40K
1 GB - 100 GB
40K
> 100 GB
Version: 100-10-82

**Pasos**

1. Desde el menú de la NetApp Console , seleccione **Gobernanza > Clasificación**.
2. Seleccione **Gobernanza**.

   Aparece el panel de gobernanza.

### Revisar oportunidades de ahorro

El componente *Oportunidades de ahorro* muestra datos que puede eliminar o almacenar en un almacenamiento de objetos menos costoso. Los datos en *Saving Opportunities* se actualizan cada 2 horas. También puede actualizar los datos manualmente.

**Pasos**

1. En el menú Clasificación de datos, seleccione **Gobernanza**.
2. Dentro de cada mosaico de Oportunidades de ahorro del panel de Gobernanza, seleccione **Optimizar almacenamiento** para ver los resultados filtrados en la página de Investigación. Para descubrir qué datos debe eliminar o transferir a un almacenamiento menos costoso, investigue las *Oportunidades de ahorro*.
   - **Datos obsoletos**: de forma predeterminada, los datos se consideran obsoletos si se modificaron por última vez hace más de 3 años. Puede [personalizar la definición de datos obsoletos](task-stale-data.html).
   - **Archivos duplicados**: archivos que están duplicados en otras ubicaciones en las fuentes de datos que está escaneando. "Vea qué tipos de archivos duplicados se muestran" .

Si alguna de sus fuentes de datos implementa niveles de datos, los datos antiguos que ya residen en el almacenamiento de objetos se pueden identificar en la categoría *Datos obsoletos*.

## Crear el informe de evaluación de descubrimiento de datos

El informe de evaluación de descubrimiento de datos proporciona un análisis de alto nivel del entorno escaneado para mostrar áreas de preocupación y posibles pasos de remediación. Los resultados se basan tanto en el mapeo como en la clasificación de sus datos. El objetivo de este informe es crear conciencia sobre tres aspectos importantes de su conjunto de datos:

| Característica | Descripción |
|---|---|
| Preocupaciones sobre la gobernanza de datos | Una imagen detallada de todos los datos que posee y las áreas en las que puede reducir la cantidad de datos para ahorrar costos. |
| Exposiciones de seguridad de datos | Áreas donde sus datos son accesibles a ataques internos o externos debido a amplios permisos de acceso. |
| Brechas de cumplimiento de datos | Dónde se encuentra su información personal o información personal confidencial, tanto por motivos de seguridad como para las DSAR (solicitudes de acceso de interesados). |

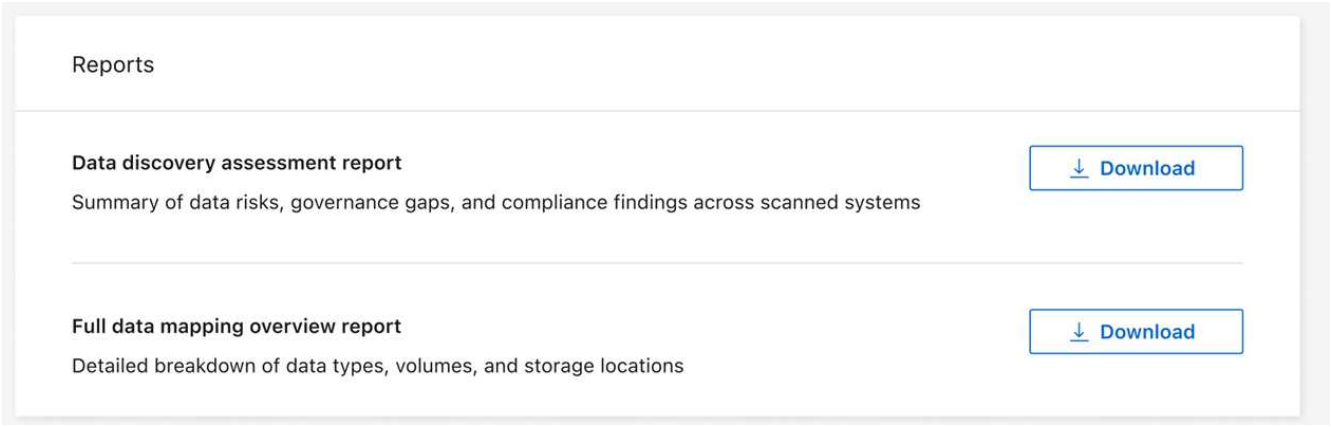
Con el informe podrás realizar las siguientes acciones:

- Reduzca los costos de almacenamiento modificando su política de retención o moviendo o eliminando ciertos datos (datos obsoletos o duplicados).
- Proteja sus datos que tienen permisos amplios revisando las políticas de administración de grupos globales.

- Proteja sus datos que contienen información personal o confidencial moviendo PII a almacenes de datos más seguros.

**Pasos**

1. En Clasificación de datos, seleccione **Gobernanza**.
2. En el mosaico de informes, seleccione **Informe de evaluación de descubrimiento de datos**.




**Resultado**

La clasificación de datos genera un informe en PDF que puedes revisar y compartir.

## Crear el informe de descripción general del mapeo de datos

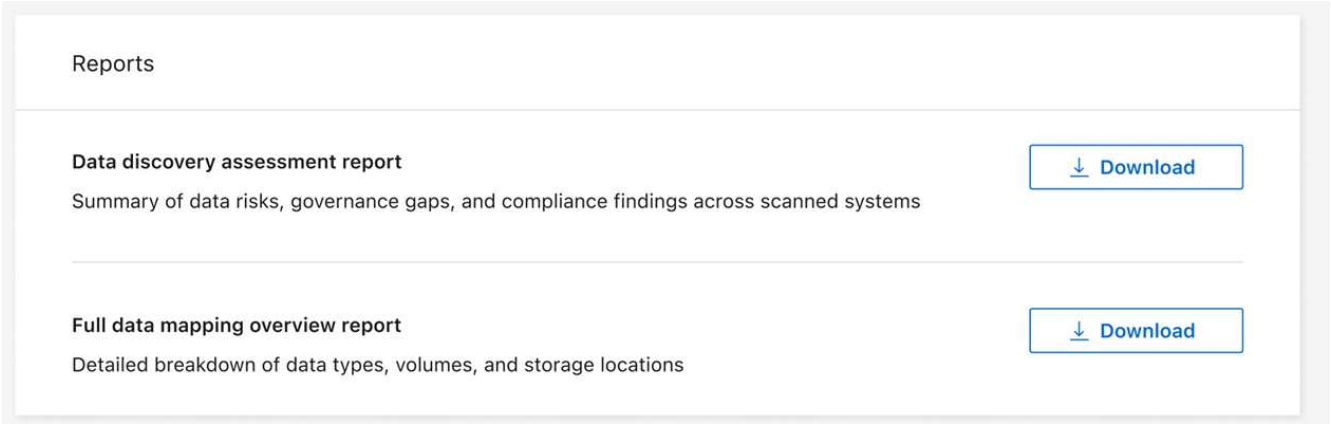
El informe de descripción general de mapeo de datos proporciona una descripción general de los datos almacenados en sus fuentes de datos corporativas para ayudarlo con las decisiones sobre procesos de migración, respaldo, seguridad y cumplimiento. El informe resume todos los sistemas y fuentes de datos. También proporciona un análisis para cada sistema.

El informe incluye la siguiente información:

| Categoría | Descripción |
|---|---|
| Capacidad de uso | Para todos los sistemas: enumera la cantidad de archivos y la capacidad utilizada para cada sistema. Para sistemas individuales: enumera los archivos que utilizan la mayor capacidad. |
| La era de los datos | Proporciona tres cuadros y gráficos que indican cuándo se crearon los archivos, cuándo se modificaron por última vez o cuándo se accedió por última vez. Enumera la cantidad de archivos y su capacidad utilizada, en función de determinados rangos de fechas. |
| Tamaño de los datos | Enumera la cantidad de archivos que existen dentro de ciertos rangos de tamaño en sus sistemas. |

**Pasos**

1. En Clasificación de datos, seleccione **Gobernanza**.
2. En el mosaico de informes, seleccione **Informe de descripción general de mapeo de datos completo**.




**Resultado**

La clasificación de datos genera un informe en PDF que puede revisar y enviar a otros grupos según sea necesario.

Si el informe tiene más de 1 MB, el archivo PDF se conserva en la instancia de Clasificación de datos y verá un mensaje emergente sobre la ubicación exacta. Cuando Data Classification está instalado en una máquina Linux en sus instalaciones o en una máquina Linux implementada en la nube, puede navegar directamente al archivo PDF. Cuando se implementa la clasificación de datos en la nube, es necesario autorizar con SSH la instancia de clasificación de datos para descargar el archivo PDF.

### Revise los principales repositorios de datos enumerados por sensibilidad de datos

El área *Principales repositorios de datos por nivel de sensibilidad* del informe Descripción general de mapeo de datos enumera los cuatro principales repositorios de datos (sistemas y fuentes de datos) que contienen los elementos más sensibles. El gráfico de barras de cada sistema se divide en:

- Datos no sensibles
- Datos personales
- Datos personales sensibles

Estos datos se actualizan cada dos horas y se pueden actualizar manualmente.

**Pasos**

1. Para ver el número total de elementos en cada categoría, coloque el cursor sobre cada sección de la barra.
2. Para filtrar los resultados que aparecerán en la página de Investigación, seleccione cada área en la barra e investigue más.

### Revisar datos confidenciales y permisos amplios

El área *Datos confidenciales y permisos amplios* del panel de Gobernanza muestra los recuentos de archivos que contienen datos confidenciales y tienen permisos amplios. La tabla muestra los siguientes tipos de permisos:

- Desde los permisos más restrictivos hasta las restricciones más permisivas en el eje horizontal.
- Desde los datos menos sensibles hasta los más sensibles en el eje vertical.

**Pasos**

1. Para ver el número total de archivos en cada categoría, coloque el cursor sobre cada cuadro.
2. Para filtrar los resultados que aparecerán en la página de Investigación, seleccione una casilla e investigue más.

### Revisar los datos enumerados por tipos de permisos abiertos

El área *Permisos abiertos* del informe Descripción general de asignación de datos muestra el porcentaje de cada tipo de permisos que existen para todos los archivos que se están escaneando. El gráfico muestra los siguientes tipos de permisos:

- Sin permisos abiertos
- Abierto a la Organización
- Abierto al público
- Acceso desconocido

**Pasos**

1. Para ver el número total de archivos en cada categoría, coloque el cursor sobre cada cuadro.
2. Para filtrar los resultados que aparecerán en la página de Investigación, seleccione una casilla e investigue más.

### Revisar la edad y el tamaño de los datos

Puede investigar los elementos en los gráficos *Edad* y *Tamaño* del informe Descripción general de mapeo de datos para ver si hay datos que debería eliminar o colocar en un nivel de almacenamiento de objetos menos costoso.

**Pasos**

1. En el gráfico Era de los Datos, para ver detalles sobre la edad de los datos, coloque el cursor sobre un punto del gráfico.
2. Para filtrar por rango de edad o tamaño, seleccione esa edad o tamaño.
    - **Gráfico de antigüedad de los datos**: clasifica los datos según el momento en que se crearon, la última vez que se accedió a ellos o la última vez que se modificaron.
    - **Gráfico de tamaño de datos**: clasifica los datos según su tamaño.

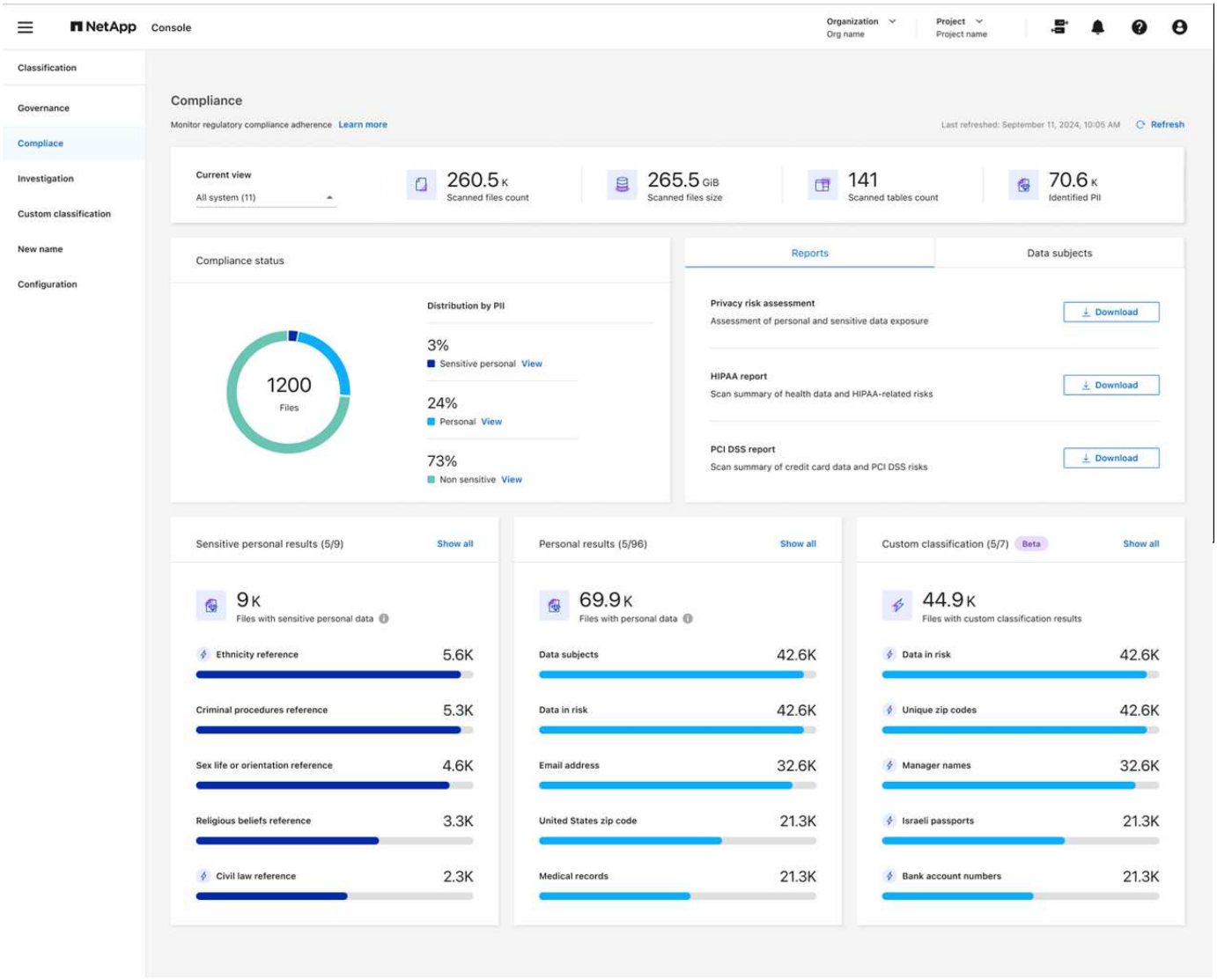
Si alguna de sus fuentes de datos implementa niveles de datos, los datos antiguos que ya residen en el almacenamiento de objetos podrían identificarse en el gráfico *Antigüedad de los datos*.

# Vea los detalles de cumplimiento sobre los datos privados almacenados en su organización con NetApp Data Classification

Obtenga control de sus datos privados al ver detalles sobre los datos personales (PII) y los datos personales confidenciales (SPII) de su organización. También puede obtener visibilidad al revisar las categorías y los tipos de archivos que NetApp Data Classification encontró en sus datos.

Los detalles de cumplimiento a nivel de archivo solo están disponibles si realiza un análisis de clasificación completo. Los escaneos de solo mapeo no brindan detalles a nivel de archivo.

De forma predeterminada, el panel de Clasificación de datos muestra datos de cumplimiento de todos los sistemas y bases de datos. Para ver los datos de sólo algunos de los sistemas, selecciónelos.




Puede filtrar los resultados desde la página Investigación de datos y descargar un informe de los resultados como un archivo CSV. Ver"Filtrado de datos en la página Investigación de datos" Para más detalles.

## Ver archivos que contienen datos personales

La clasificación de datos identifica automáticamente palabras, cadenas y patrones específicos (Regex) dentro de los datos. "Por ejemplo, números de tarjetas de crédito, números de seguro social, números de cuentas bancarias, contraseñas y más."La clasificación de datos identifica este tipo de información en archivos individuales, en archivos dentro de directorios (recursos compartidos y carpetas) y en tablas de bases de datos.

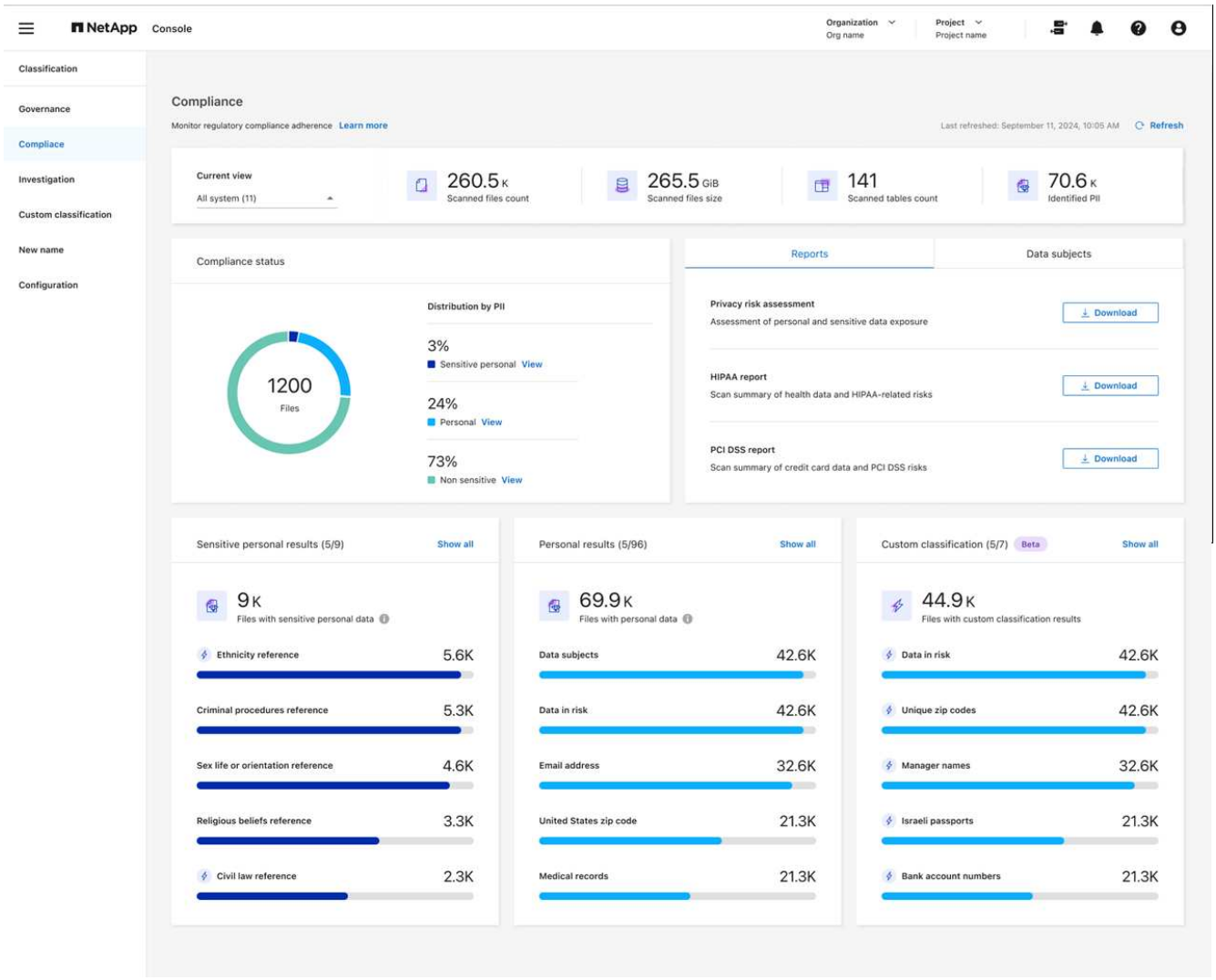
También puede crear términos de búsqueda personalizados para identificar datos personales específicos de su organización. Para obtener más información, consulte "Crear una clasificación personalizada" .

Para algunos tipos de datos personales, la clasificación de datos utiliza *validación de proximidad* para validar

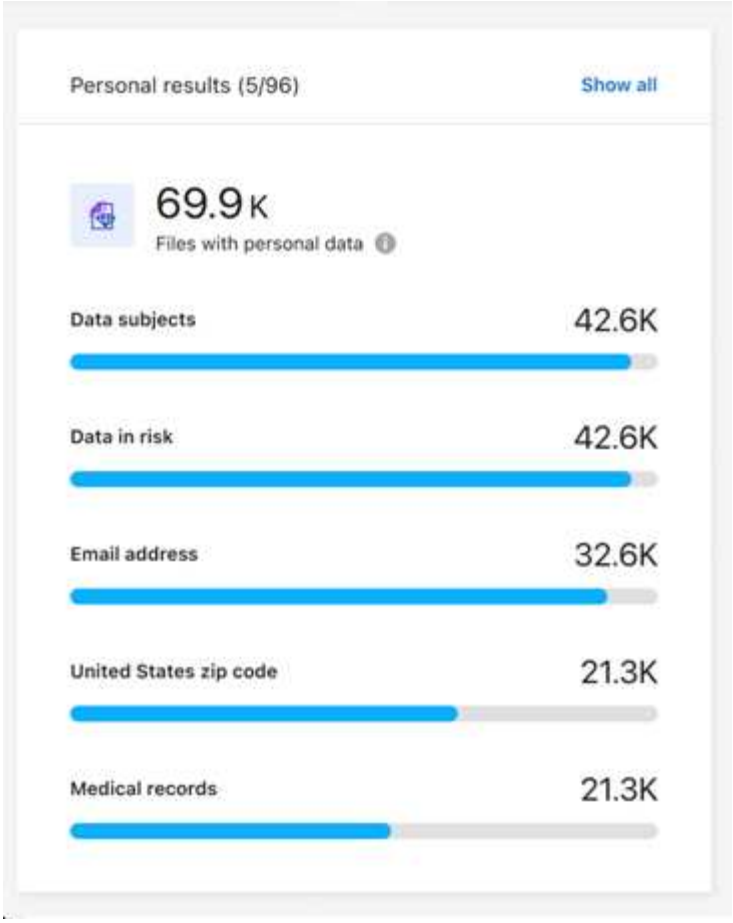
sus hallazgos. La validación se realiza mediante la búsqueda de una o más palabras clave predefinidas en proximidad a los datos personales encontrados. Por ejemplo, la clasificación de datos identifica un número de seguro social (SSN) de EE. UU. como un SSN si ve una palabra de proximidad junto a él, por ejemplo, *SSN* o *seguridad social*. "La tabla de datos personales" muestra cuándo la clasificación de datos utiliza la validación de proximidad.

**Pasos**

1. Desde el menú Clasificación de datos, seleccione la pestaña **Cumplimiento**.
2. Para investigar los detalles de todos los datos personales, seleccione el ícono junto al porcentaje de datos personales.

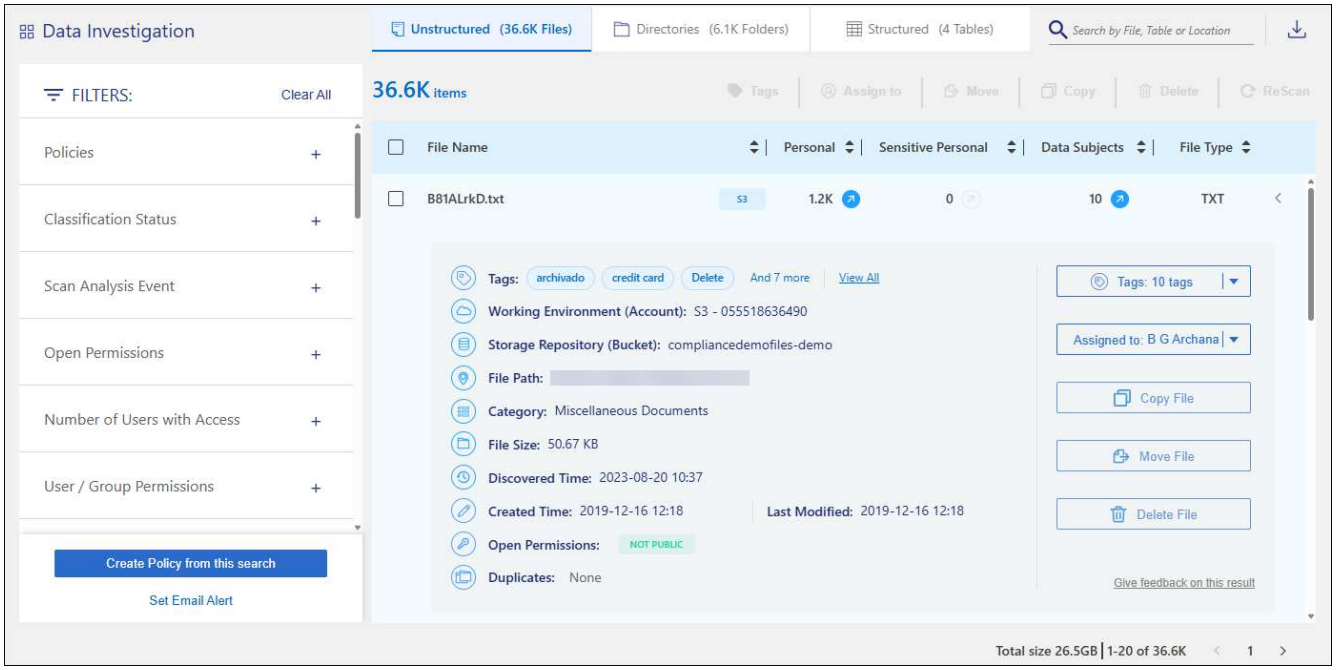


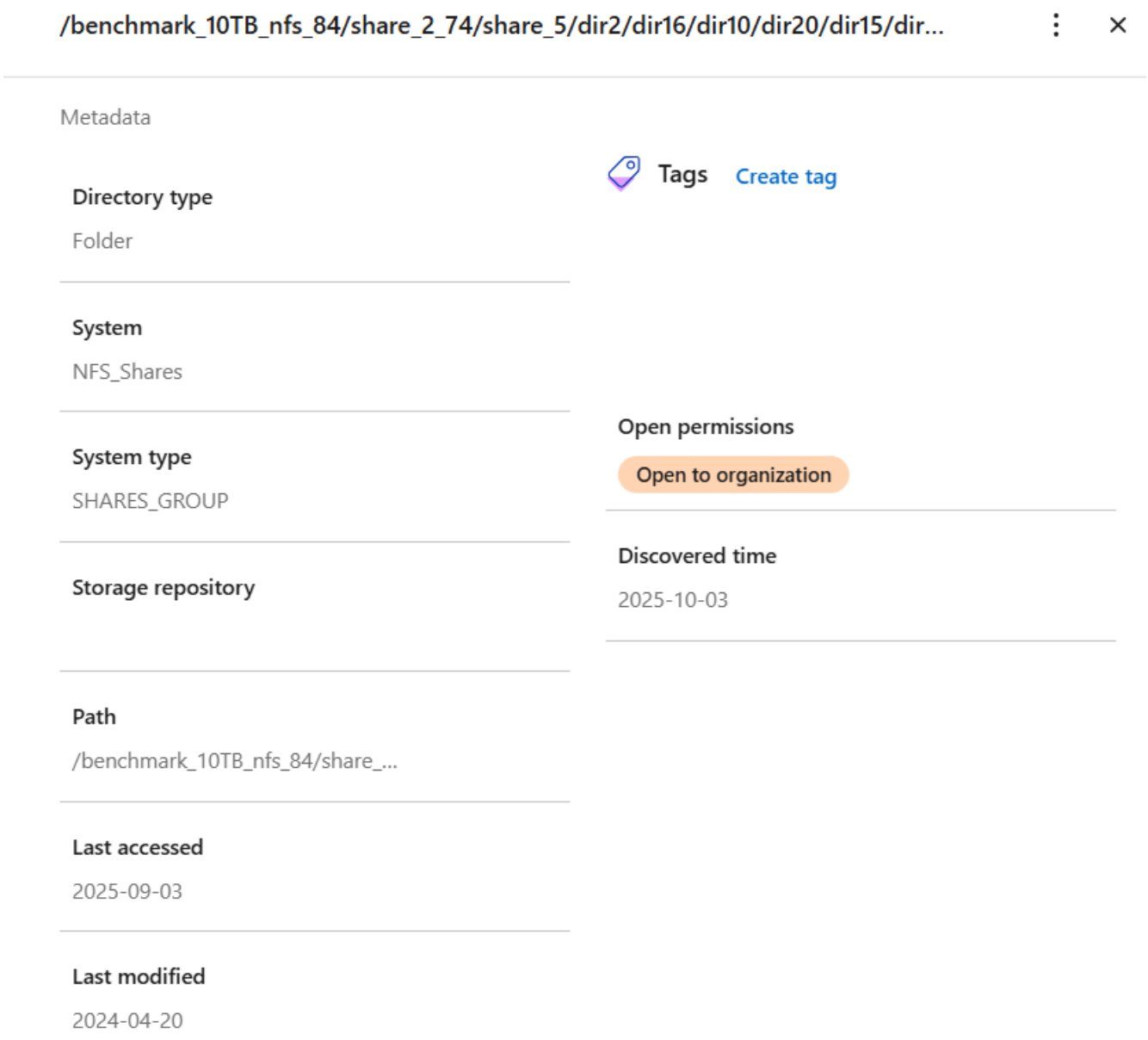

3. Para investigar los detalles de un tipo específico de datos personales, seleccione **Ver todo** y luego seleccione el ícono de flecha **Investigar resultados** para un tipo específico de datos personales, por ejemplo, direcciones de correo electrónico.




4. Investigue los datos buscando, ordenando, expandiendo detalles de un archivo específico, seleccionando la flecha **Investigar resultados** para ver información enmascarada o descargando la lista de archivos.

   Las siguientes imágenes muestran datos personales encontrados en un directorio (archivos compartidos y carpetas). En la pestaña **Estructurado**, puede ver los datos personales que se encuentran en las bases de datos. En la pestaña **No estructurado**, puede ver datos a nivel de archivo.






## Ver archivos que contienen datos personales confidenciales

La clasificación de datos identifica automáticamente tipos especiales de información personal confidencial, según lo definen las regulaciones de privacidad, como "artículos 9 y 10 del RGPD" . Por ejemplo, información sobre la salud de una persona, su origen étnico o su orientación sexual. "Ver la lista completa" . La clasificación de datos identifica este tipo de información en archivos individuales, en archivos dentro de directorios (recursos compartidos y carpetas) y en tablas de bases de datos.

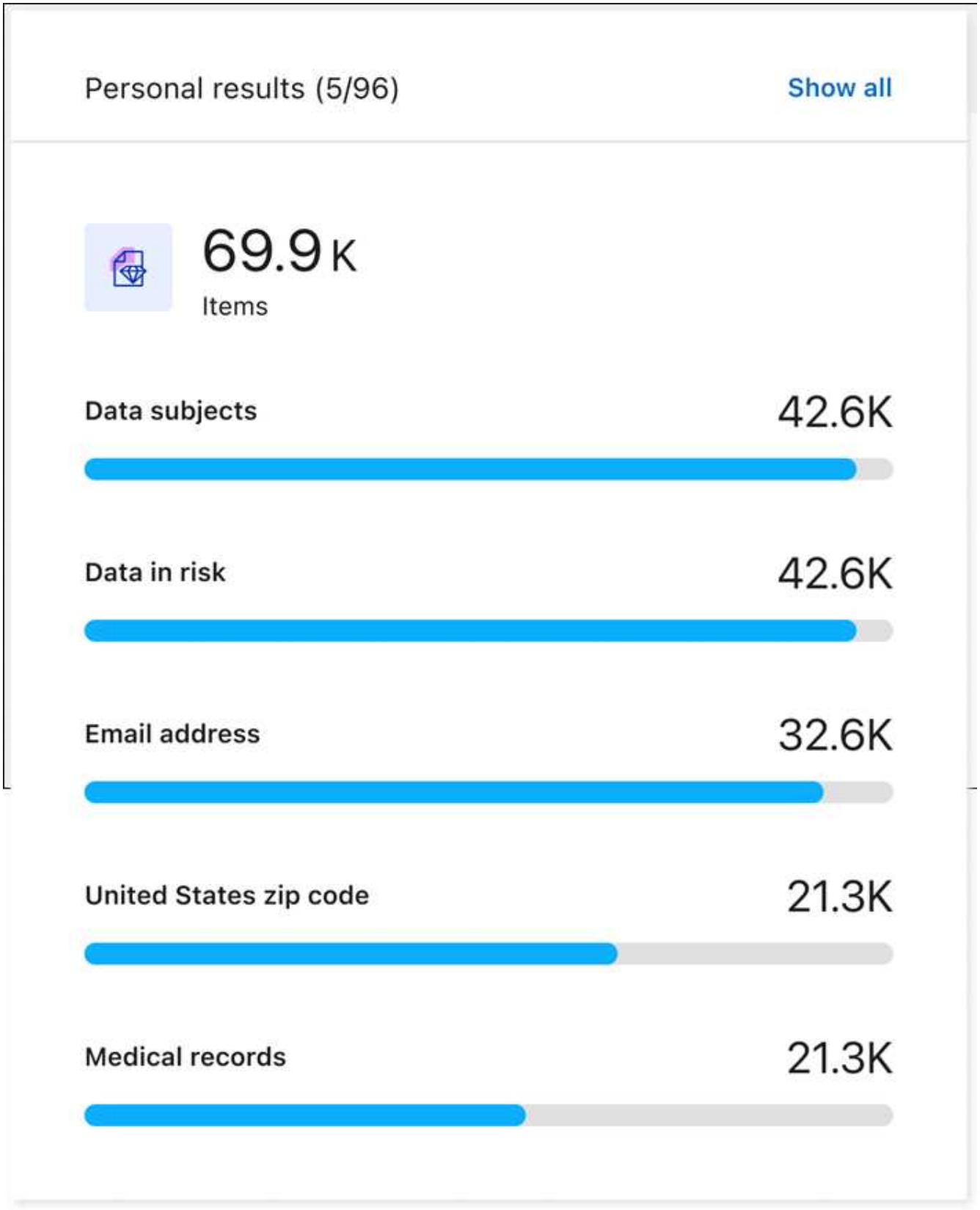
La clasificación de datos utiliza IA, procesamiento del lenguaje natural (PLN), aprendizaje automático (ML) y computación cognitiva (CC) para comprender el significado del contenido que escanea con el fin de extraer entidades y categorizarlo en consecuencia.

Por ejemplo, una categoría de datos sensibles del RGPD es el origen étnico. Gracias a sus capacidades de PNL, Data Classification puede distinguir la diferencia entre una frase que dice "George es mexicano" (lo que indica datos confidenciales según lo especificado en el artículo 9 del RGPD) y "George está comiendo comida mexicana".

Al escanear datos personales confidenciales solo se admite el idioma inglés. Más adelante se añadirá soporte para más idiomas.

**Pasos**

1. En el menú Clasificación de datos, seleccione **Cumplimiento**.
2. Para investigar los detalles de todos los datos personales confidenciales, busque la tarjeta **Resultados personales confidenciales** y luego seleccione **Mostrar todo**.




.

3. Para investigar los detalles de un tipo específico de datos personales confidenciales, seleccione **Ver todo** y luego seleccione el ícono de flecha **Investigar resultados** para un tipo específico de datos personales confidenciales.
4. Investigue los datos buscando, ordenando, expandiendo detalles de un archivo específico, haciendo clic

en **Investigar resultados** para ver información enmascarada o descargando la lista de archivos.

# Categorías de datos privados en la NetApp Data Classification

Hay muchos tipos de datos privados que NetApp Data Classification puede identificar en sus volúmenes y bases de datos.

La clasificación de datos identifica dos tipos de datos personales:

- **Información de identificación personal (PII)**
- **Información personal sensible (SPII)**

Si necesita clasificación de datos para identificar otros tipos de datos privados, como números de identificación nacional adicionales o identificadores de atención médica, comuníquese con su gerente de cuenta.

## Tipos de datos personales

Los datos personales, o *información de identificación personal* (PII), que se encuentran en los archivos pueden ser datos personales generales o identificadores nacionales. La tercera columna de la tabla a continuación identifica si la clasificación de datos utiliza"validación de proximidad" para validar sus hallazgos para el identificador.

En la tabla se identifican los idiomas en los que se pueden reconocer estos elementos.

| Tipo | Identificador | ¿Validación de proximidad? | Inglés | Alemán | Español | Francés | japonés |
|---|---|---|---|---|---|---|---|
| General | Número de Tarjeta de Crédito | Sí | ✓ | ✓ | ✓ | | ✓ |
| | Titulares de los datos | No | ✓ | ✓ | ✓ | | |
| | Dirección de correo electrónico | No | ✓ | ✓ | ✓ | | ✓ |
| | Número IBAN (Número de cuenta bancaria internacional) | No | ✓ | ✓ | ✓ | | ✓ |
| | Dirección IP | No | ✓ | ✓ | ✓ | | ✓ |
| | Password | Sí | ✓ | ✓ | ✓ | | ✓ |

| Tipo | Identificador | ¿Validación de proximidad? | Inglés | Alemán | Español | Francés | japonés |
|---|---|---|---|---|---|---|---|
| Identificadores nacionales | | | | | | | |

| Tipo | Identificador | ¿Validación de proximidad? | Inglés | Alemán | Español | Francés | japonés |
|---|---|---|---|---|---|---|---|

| Tipo | Identificador | ¿Validación de proximidad? | Inglés | Alemán | Español | Francés | japonés |
|---|---|---|---|---|---|---|---|

| Tipo | Identificador | ¿Validación de proximidad? | Inglés | Alemán | Español | Francés | japonés |
|---|---|---|---|---|---|---|---|

| Tipo | Identificador | ¿Validación de proximidad? | Inglés | Alemán | Español | Francés | japonés |
|---|---|---|---|---|---|---|---|
| | Identificación del Reino Unido (NINO) | Sí | ✓ | ✓ | ✓ | | |
| | Licencia de conducir de California, EE. UU. | Sí | ✓ | ✓ | ✓ | | |
| | Licencia de conducir de Indiana, EE. UU. | Sí | ✓ | ✓ | ✓ | | |
| | Licencia de conducir de Nueva York, EE. UU. | Sí | ✓ | ✓ | ✓ | | |
| | Licencia de conducir de Texas, EE. UU. | Sí | ✓ | ✓ | ✓ | | |
| | Número de Seguro Social de EE. UU. (SSN) | Sí | ✓ | ✓ | ✓ | | |

## Tipos de datos personales sensibles

La clasificación de datos puede encontrar la siguiente información personal confidencial (SPII) en los archivos.

Los siguientes SPII actualmente solo se pueden reconocer en inglés:

- **Referencia de Procedimientos Penales**: Datos relativos a condenas y delitos penales de una persona física.
- **Referencia étnica**: Datos relativos al origen racial o étnico de una persona física.
- **Referencia de Salud**: Datos relativos a la salud de una persona física.
- **Códigos médicos CIE-9-CM**: Códigos utilizados en la industria médica y de la salud.
- **Códigos médicos CIE-10-CM**: Códigos utilizados en la industria médica y de la salud.
- **Referencia de creencias filosóficas**: Datos relativos a las creencias filosóficas de una persona física.
- **Referencia de opiniones políticas**: Datos relativos a las opiniones políticas de una persona física.
- **Referencia de creencias religiosas**: Datos relativos a las creencias religiosas de una persona física.
- **Referencia sobre la vida sexual o la orientación sexual**: Datos relativos a la vida sexual o la orientación sexual de una persona física.

## Tipos de categorías

La clasificación de datos categoriza sus datos de la siguiente manera.

La mayoría de estas categorías se pueden reconocer en inglés, alemán y español.

| Categoría | Tipo | Inglés | Alemán | Español |
|---|---|---|---|---|
| Finanzas | Balances generales | ✓ | ✓ | ✓ |
| | Órdenes de compra | ✓ | ✓ | ✓ |
| | Facturas | ✓ | ✓ | ✓ |
| | Informes trimestrales | ✓ | ✓ | ✓ |

| Categoría | Tipo | Inglés | Alemán | Español |
|---|---|---|---|---|
| HORA | Verificación de antecedentes | ✓ | | ✓ |
| | Planes de compensación | ✓ | ✓ | ✓ |
| | Contratos de empleados | ✓ | | ✓ |
| | Reseñas de empleados | ✓ | | ✓ |
| | Salud | ✓ | | ✓ |
| | Currículums | ✓ | ✓ | ✓ |
| Legal | Acuerdos de confidencialidad | ✓ | ✓ | ✓ |
| | Contratos entre proveedor y cliente | ✓ | ✓ | ✓ |
| Marketing | Campañas | ✓ | ✓ | ✓ |
| | Conferencias | ✓ | ✓ | ✓ |
| Operaciones | Informes de auditoría | ✓ | ✓ | ✓ |
| Ventas | Órdenes de venta | ✓ | ✓ | |
| Servicios | Solicitud de información | ✓ | | ✓ |
| | Solicitud de propuestas | ✓ | | ✓ |
| | SEMBRAR | ✓ | ✓ | ✓ |
| | Formación | ✓ | ✓ | ✓ |
| Soporte | Quejas y tickets | ✓ | ✓ | ✓ |

Los siguientes metadatos también están categorizados e identificados en los mismos idiomas admitidos:

- Datos de la aplicación
- Archivos de archivo
- Audio
- Migas de pan de datos de aplicaciones empresariales de clasificación de datos
- Archivos CAD
- Código
- Corrupto
- Archivos de base de datos e índice
- Archivos de diseño
- Datos de la aplicación de correo electrónico
- Cifrados (archivos con una puntuación de entropía alta)
- Ejecutables
- Datos de aplicaciones financieras
- Datos de la aplicación de salud

- Imágenes
- Registros
- Documentos varios
- Presentaciones varias
- Hojas de cálculo varias
- Misceláneo "Desconocido"
- Archivos protegidos con contraseña
- Datos estructurados
- Vídeos
- Archivos de cero bytes

## Tipos de archivos

La clasificación de datos escanea todos los archivos en busca de información sobre categorías y metadatos y muestra todos los tipos de archivos en la sección de tipos de archivos del panel. Cuando la clasificación de datos detecta información de identificación personal (PII) o cuando realiza una búsqueda DSAR, solo se admiten los siguientes formatos de archivo:

`.CSV, .DCM, .DOC, .DOCX, .JSON, .PDF, .PPTX, .RTF, .TXT, .XLS, .XLSX, Docs, Sheets, and Slides`

## Exactitud de la información encontrada

NetApp no puede garantizar el 100 % de precisión de los datos personales y los datos personales confidenciales que identifica la clasificación de datos. Siempre debes validar la información revisando los datos.

Según nuestras pruebas, la siguiente tabla muestra la precisión de la información que encuentra la clasificación de datos. Lo desglosamos por *precisión* y *recuperación*:

**Precisión**
: La probabilidad de que lo que encuentra la Clasificación de Datos haya sido identificado correctamente. Por ejemplo, una tasa de precisión del 90% para datos personales significa que 9 de cada 10 archivos identificados como que contienen información personal, en realidad contienen información personal. 1 de cada 10 archivos sería un falso positivo.

**Recordar**
: La probabilidad de que la clasificación de datos encuentre lo que debería. Por ejemplo, una tasa de recuperación del 70% para datos personales significa que la clasificación de datos puede identificar 7 de cada 10 archivos que realmente contienen información personal en su organización. La clasificación de datos perdería el 30% de los datos y no aparecerán en el panel de control.

Estamos mejorando constantemente la precisión de nuestros resultados. Estas mejoras estarán disponibles automáticamente en futuras versiones de Clasificación de datos.

| Tipo | Precisión | Recordar |
|---|---|---|
| Datos personales - General | 90%-95% | 60%-80% |

| Tipo | Precisión | Recordar |
|---|---|---|
| Datos personales - Identificadores de país | 30%-60% | 40%-60% |
| Datos personales sensibles | 80%-95% | 20%-30% |
| Categorías | 90%-97% | 60%-80% |

# Cree una clasificación personalizada en NetApp Data Classification

La NetApp Data Classification le permite crear categorías personalizadas o identificadores personales para identificar datos específicos según los requisitos normativos y de cumplimiento de su organización.

La clasificación de datos admite dos tipos de clasificadores personalizados: categorías e identificadores personales. Las categorías personalizadas se crean en función de un conjunto de archivos que usted carga, desde los cuales Data Classification crea un modelo de IA para identificar datos similares en su organización (por ejemplo, una empresa de investigación de salud podría crear una categoría de análisis clínico). Los identificadores personales personalizados se crean utilizando listas de palabras clave o una expresión regular (regex) para identificar información específica de su organización que pueda representar un riesgo de cumplimiento.

Todas las clasificaciones personalizadas están disponibles en el panel de clasificación personalizada.

## Crear un identificador personal personalizado

La clasificación de datos le permite crear un identificador personal personalizado utilizando palabras clave contextuales o una expresión regular para identificar datos exclusivos de su organización.

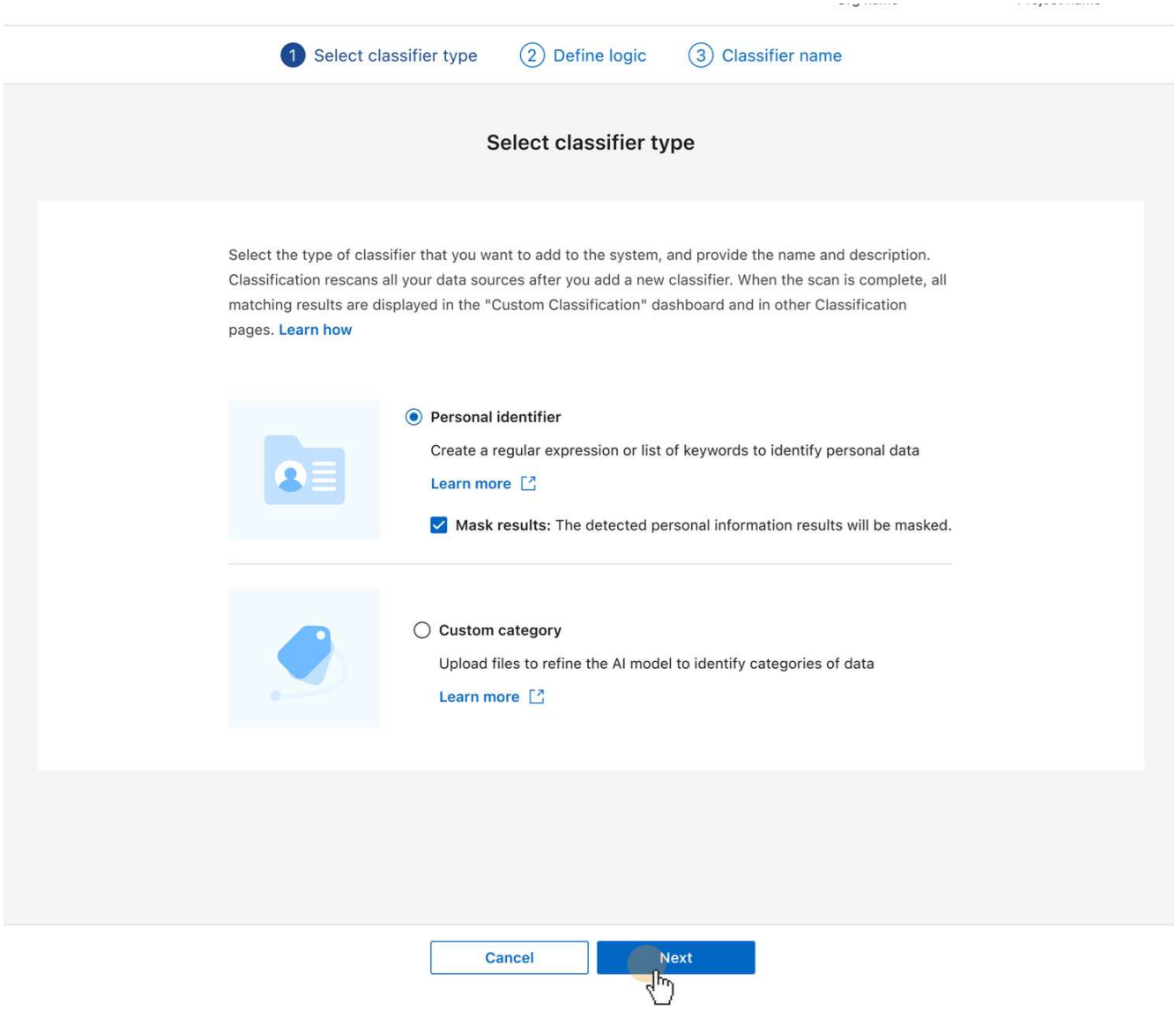
#### Requisitos para palabras clave

Si está creando su identificador personal con una lista de palabras clave, la lista debe cumplir los siguientes requisitos:

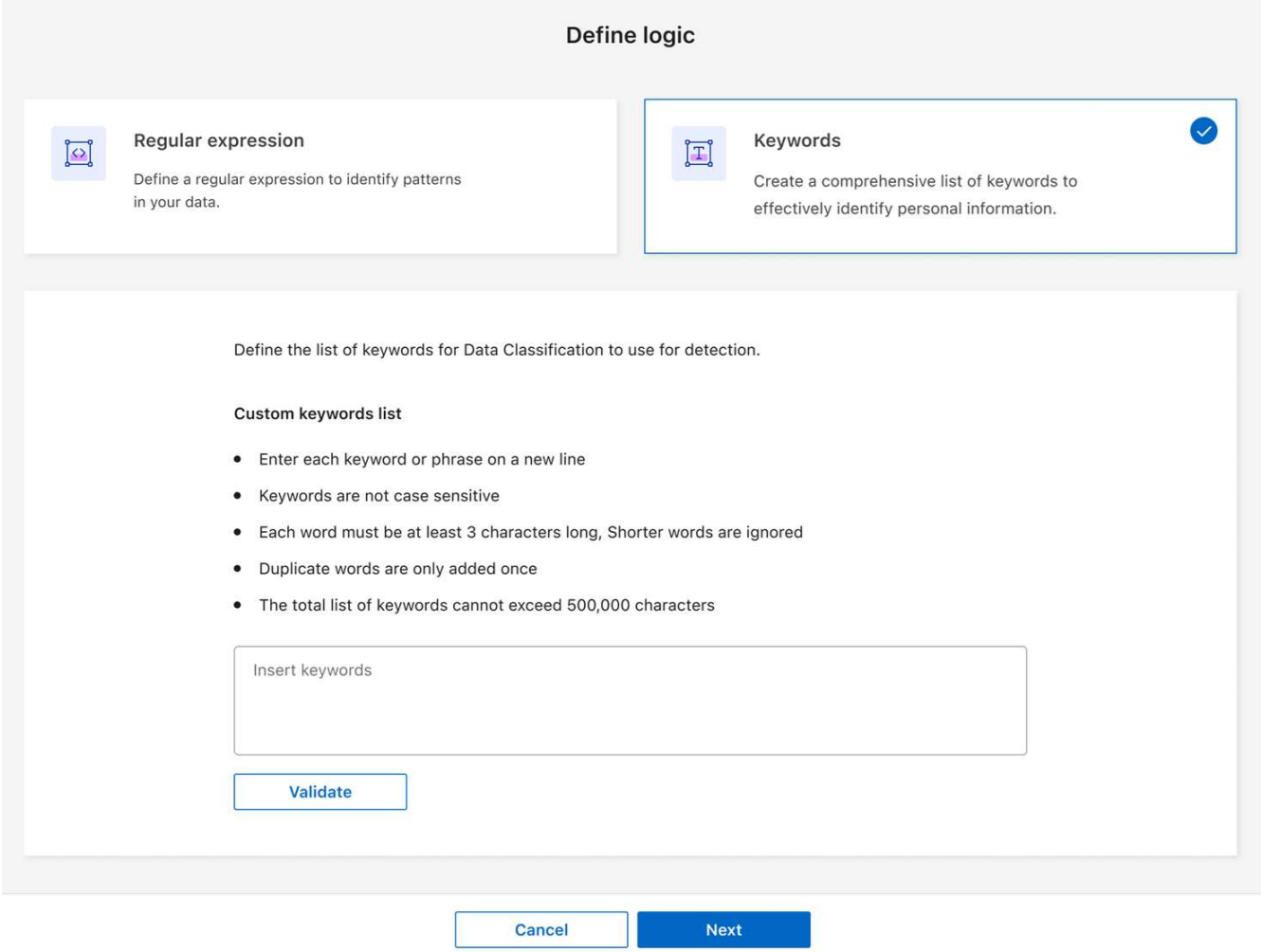
- Las entradas de palabras clave no distinguen entre mayúsculas y minúsculas.
- Las palabras clave deben tener al menos tres caracteres. Cualquier palabra con menos de tres caracteres será ignorada.
- Las palabras duplicadas solo se agregan una vez.
- La lista total de palabras clave no puede superar los 500.000 caracteres. La lista debe incluir al menos una palabra clave.

#### Pasos

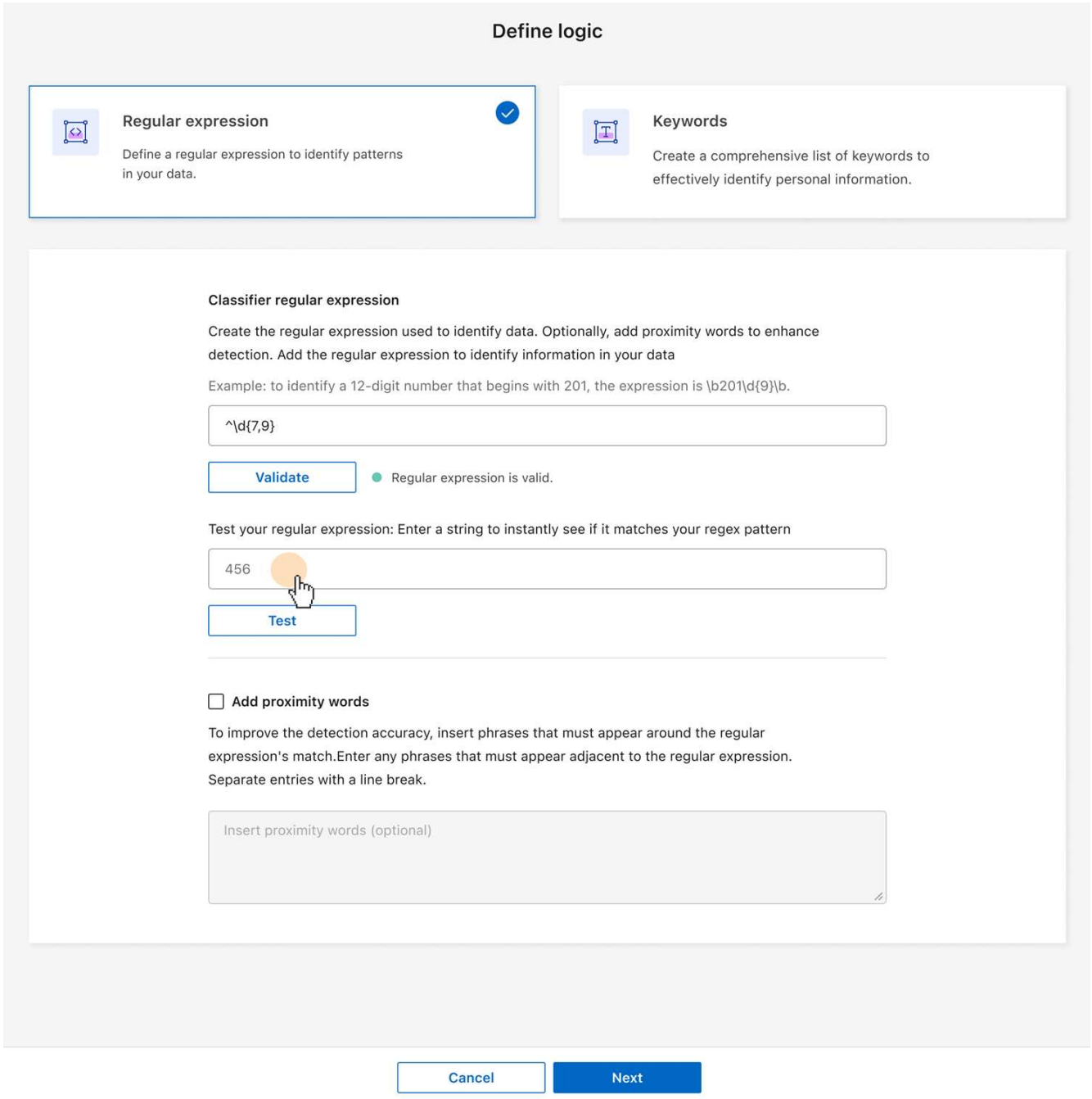
1. Seleccione la pestaña **Clasificación personalizada**.
2. Seleccione **+ Nuevo clasificador** para crear el clasificador personalizado.
3. Seleccione **Identificador personal**. Opcionalmente, seleccione **Ocultar resultados** para enmascarar los datos personales detectados.
4. Seleccione **Siguiente**.




5. Para agregar el clasificador con palabras clave, seleccione **Palabras clave**. Introduzca una lista de palabras clave, con cada entrada en una línea separada. Asegúrese de que las palabras clave cumplan con los requisitos.




Para agregar el clasificador como una expresión regular, seleccione **Expresión regular** y luego agregue un patrón para detectar la información específica de sus datos. Seleccione **Validar** para confirmar la sintaxis de su entrada.




a. Opcionalmente, ingrese una cadena de muestra que debe coincidir con su patrón de expresión regular y luego seleccione **Probar** para comprobarlo.

b. Opcionalmente, agregue palabras de proximidad. Si agrega palabras de proximidad, la clasificación de datos solo marca el patrón de expresión regular si las palabras de proximidad están adyacentes a la cadena coincidente.

6. Seleccione **Siguiente**.
7. Ingrese un **Nombre de clasificador** y una **Descripción** para identificar la categoría personalizada en su panel.
8. Seleccione **Guardar** para crear el identificador personal personalizado.

Después de crear un identificador personal personalizado, sus resultados se capturan en el próximo escaneo programado. Para capturar resultados antes, realice un análisis a pedido. Para ver los resultados, consulte

Generar informes de cumplimiento.

## Crear una categoría personalizada

Con categorías personalizadas, puede categorizar datos específicos de su organización. Las categorías personalizadas se crean en función de los archivos de texto que usted carga, desde los cuales Data Classification crea un modelo de IA para identificar información similar en otros archivos.

**Requisitos de datos de entrenamiento**

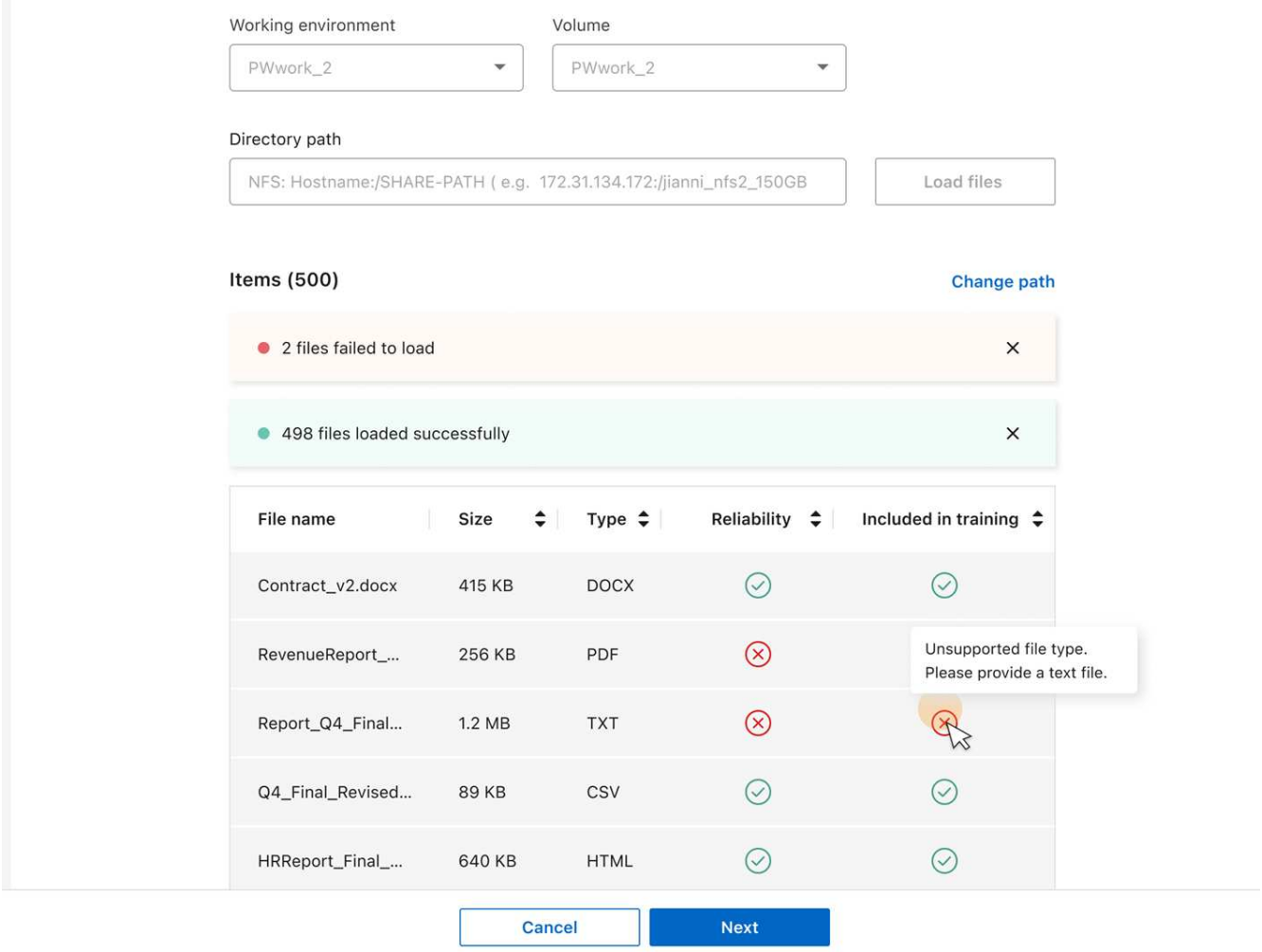
- El conjunto de datos de entrenamiento debe contener un mínimo de 25 archivos. El número máximo de archivos es 1000.
- Todos los archivos deben estar ubicados directamente en la ruta de archivo que usted proporcione.
- Todos los archivos deben tener más de 100 bytes.
- Los datos de entrenamiento de clasificación de datos deben ser uno de los siguientes tipos de archivos: CSV, DOCX, DOC, GZ, JSON, PDF, PPTX, TXT, RTT, XLS o XLSX. Puede cargar una combinación de todos los tipos de archivos admitidos.

**Pasos**

1. En NetApp Data Classification, seleccione **Clasificación personalizada**.
2. Seleccione **+ Nuevo clasificador**.
3. Seleccione **Categoría personalizada** como su tipo de clasificador y luego **Siguiente**.
4. Define la lógica de tu categoría personalizada con una colección de archivos basados en texto. Proporcione la dirección IP de la **Dirección de trabajo** y luego seleccione el **Volumen** en el menú desplegable.

   Ingrese la **Ruta del directorio** para el directorio que contiene los datos de entrenamiento.

5. Seleccione **Cargar archivos** para Clasificación de datos para realizar una verificación de los archivos. Puede revisar el resumen de los archivos, que enumera el nombre del archivo, el tamaño, el tipo y las notas si el archivo se consideró aceptable para la capacitación.




Clasificación de datos muestra el tiempo estimado de finalización del entrenamiento de datos. .. Para cambiar la ruta del archivo o volver a subir archivos, selecciona **Change path**, luego ingresa los datos y carga los archivos de nuevo.

6. Cuando esté satisfecho con los archivos cargados, seleccione **Siguiente**.
7. Ingrese un **Nombre de clasificador** y una **Descripción** para identificar la categoría personalizada en su panel.
8. Seleccione **Guardar** para crear la categoría personalizada.

**Resultado**

Después de crear una categoría personalizada, sus resultados se capturan en el próximo análisis programado. Para capturar resultados antes, inicie el escaneo manualmente.

## Editar un clasificador personalizado

Puede modificar la lógica de un identificador personal después de crearlo. No puede cambiar el tipo de identificador personal ni el tipo de lógica; por ejemplo, no puede cambiar una categoría personalizada a un identificador personal personalizado. Tampoco puedes cambiar un identificador personalizado basado en palabras clave a un identificador personalizado basado en expresiones regulares.

**Pasos**

1. En NetApp Data Classification, seleccione **Clasificación personalizada**.

2. Identifique el clasificador que desea eliminar y luego seleccione el menú de acciones … al final de su fila.
3. Seleccione **Editar lógica**.
4. Si está modificando palabras clave, agregue, elimine o edite las palabras clave adecuadas. Si está modificando una expresión regular, ingrese la nueva expresión regular y valídela. Opcionalmente, agregue palabras clave de proximidad.
5. Seleccione **Guardar** para aplicar los cambios.

### Eliminar un clasificador personalizado

1. En NetApp Data Classification, seleccione **Clasificación personalizada**.
2. Identifique el clasificador que desea eliminar y luego seleccione el menú de acciones … al final de su fila.
3. Seleccione **Eliminar clasificador**.

### Próximos pasos

- Generar informes de cumplimiento

# Investigue los datos almacenados en su organización con NetApp Data Classification

El panel de investigación de datos muestra información a nivel de archivo y directorio sobre sus datos, lo que le permite ordenar y filtrar los resultados. La página Investigación de datos presenta información sobre metadatos y permisos de archivos y directorios, además de identificar archivos duplicados. Con información a nivel de archivo, directorio y base de datos, puede tomar medidas para mejorar el cumplimiento de su organización y ahorrar espacio de almacenamiento. La página Investigación de datos también admite mover, copiar y eliminar archivos.

Para obtener información de la página Investigación, debe realizar un análisis de clasificación completo de sus fuentes de datos. Las fuentes de datos que han tenido un escaneo de solo mapeo no muestran detalles a nivel de archivo.

### Estructura de la investigación de datos

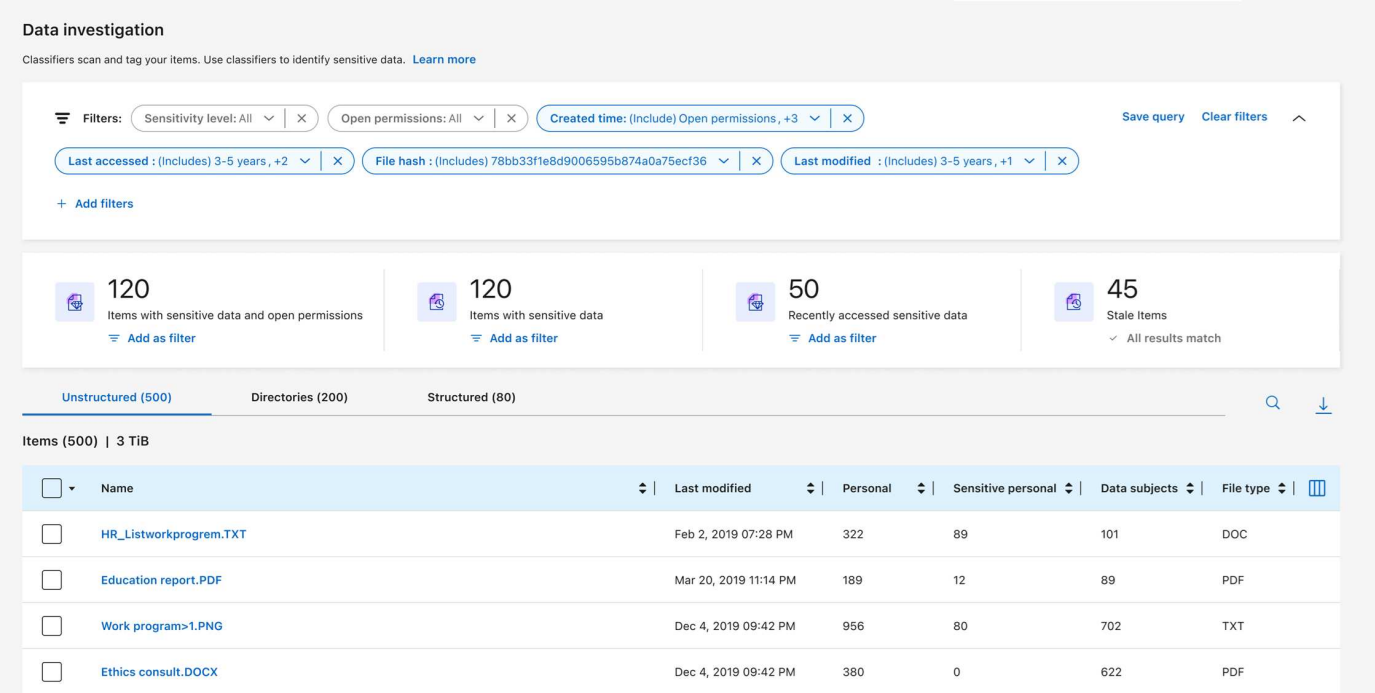
La página Investigación de datos clasifica los datos en tres pestañas:

- **Datos no estructurados**: datos de archivo
- **Directorios**: carpetas y recursos compartidos de archivos
- **Estructurado**: base de datos

### Filtros de datos

La página de Investigación de datos proporciona numerosos filtros para ordenar sus datos para que pueda encontrar lo que necesita. Puedes utilizar varios filtros en conjunto.

Para agregar un filtro, seleccione el botón **Agregar filtro**.




### Sensibilidad y contenido del filtro

Utilice los siguientes filtros para ver cuánta información confidencial contienen sus datos.

| Filtrar | Detalles |
|---|---|
| Categoría | Seleccione el"tipos de categorías" . |
| Nivel de sensibilidad | Seleccione el nivel de sensibilidad: Personal, Personal sensible o No sensible. |
| Número de identificadores | Seleccione el rango de identificadores sensibles detectados por archivo. Incluye datos personales y datos personales sensibles. Al filtrar en directorios, la clasificación de datos totaliza las coincidencias de todos los archivos en cada carpeta (y subcarpetas). NOTA: La versión de diciembre de 2023 (versión 1.26.6) eliminó la opción para calcular la cantidad de datos de información personal identificable (PII) por directorios. |
| Datos personales | Seleccione el"tipos de datos personales" . |
| Datos personales sensibles | Seleccione el"tipos de datos personales sensibles" . |
| Titular de los datos | Introduzca el nombre completo o un identificador conocido del interesado. "Obtenga más información sobre los interesados aquí" . |

### Filtrar propietario de usuario y permisos de usuario

Utilice los siguientes filtros para ver los propietarios de archivos y los permisos para acceder a sus datos.

| Filtrar | Detalles |
|---|---|
| Permisos abiertos | Seleccione el tipo de permisos dentro de los datos y dentro de las carpetas/recursos compartidos. |

| Filtrar | Detalles |
| --- | --- |
| Permisos de usuario/grupo | Seleccione uno o varios nombres de usuario y/o nombres de grupo, o ingrese un nombre parcial. |
| Propietario del archivo | Introduzca el nombre del propietario del archivo. |
| Número de usuarios con acceso | Seleccione uno o varios rangos de categorías para mostrar qué archivos y carpetas están abiertos para una determinada cantidad de usuarios. |

**Filtrar cronológicamente**

Utilice los siguientes filtros para ver datos según criterios de tiempo.

| Filtrar | Detalles |
| --- | --- |
| Tiempo creado | Seleccione un rango de tiempo cuando se creó el archivo. También puede especificar un rango de tiempo personalizado para refinar aún más los resultados de la búsqueda. |
| Tiempo descubierto | Seleccione un rango de tiempo cuando la Clasificación de datos descubrió el archivo. También puede especificar un rango de tiempo personalizado para refinar aún más los resultados de la búsqueda. |
| Última modificación | Seleccione un rango de tiempo cuando el archivo fue modificado por última vez. También puede especificar un rango de tiempo personalizado para refinar aún más los resultados de la búsqueda. |
| Último acceso | Seleccione un rango de tiempo cuando se accedió por última vez al archivo o directorio*. También puede especificar un rango de tiempo personalizado para refinar aún más los resultados de la búsqueda. Para los tipos de archivos que Data Classification escanea, esta es la última vez que Data Classification escaneó el archivo. |

* La hora del último acceso a un directorio solo está disponible para recursos compartidos NFS o CIFS.

**Filtrar metadatos**

Utilice los siguientes filtros para ver datos según ubicación, tamaño y directorio o tipo de archivo.

| Filtrar | Detalles |
| --- | --- |
| Ruta del archivo | Ingrese hasta 20 rutas parciales o completas que desee incluir o excluir de la consulta. Si ingresa rutas de inclusión y rutas de exclusión, la Clasificación de datos busca primero todos los archivos en las rutas incluidas, luego elimina los archivos de las rutas excluidas y luego muestra los resultados. Tenga en cuenta que el uso de "*" en este filtro no tiene ningún efecto y que no puede excluir carpetas específicas del análisis: se analizarán todos los directorios y archivos bajo un recurso compartido configurado. |
| Tipo de directorio | Seleccione el tipo de directorio; "Compartir" o "Carpeta". |
| Tipo de archivo | Seleccione el"tipos de archivos" . |
| Tamaño del archivo | Seleccione el rango de tamaño del archivo. |

| Filtrar | Detalles |
| --- | --- |
| Hash de archivo | Ingrese el hash del archivo para encontrar un archivo específico, incluso si el nombre es diferente. |

### Tipo de almacenamiento de filtro

Utilice los siguientes filtros para ver los datos por tipo de almacenamiento.

| Filtrar | Detalles |
| --- | --- |
| Tipo de sistema | Seleccione el tipo de sistema. |
| Nombre del entorno del sistema | Seleccione sistemas específicos. |
| Repositorio de almacenamiento | Seleccione el repositorio de almacenamiento, por ejemplo, un volumen o un esquema. |

### Consulta de filtro

Utilice el siguiente filtro para ver los datos por consultas guardadas.

| Filtrar | Detalles |
| --- | --- |
| Consulta guardada | Seleccione una consulta guardada o varias. Ir a la"pestaña de consultas guardadas" para ver la lista de consultas guardadas existentes y crear otras nuevas. |
| Etiquetas | Seleccionar"la etiqueta o etiquetas" que están asignados a sus archivos. |

### Estado del análisis del filtro

Utilice el siguiente filtro para ver los datos según el estado del escaneo de clasificación de datos.

| Filtrar | Detalles |
| --- | --- |
| Estado del análisis | Seleccione una opción para mostrar la lista de archivos que están pendientes de primer escaneo, cuyo escaneo se completó, pendientes de reescaneo o cuyo escaneo no se pudo realizar. |
| Evento de análisis de escaneo | Seleccione si desea ver los archivos que no se clasificaron porque la Clasificación de datos no pudo revertir la hora del último acceso, o los archivos que se clasificaron aunque la Clasificación de datos no pudo revertir la hora del último acceso. |

"Ver detalles sobre la marca de tiempo de "último acceso""para obtener más información sobre los elementos que aparecen en la página Investigación al filtrar mediante el Evento de análisis de escaneo.

### Filtrar datos por duplicados

Utilice el siguiente filtro para ver los archivos que están duplicados en su almacenamiento.

| Filtrar | Detalles |
| --- | --- |
| Duplicados | Seleccione si el archivo está duplicado en los repositorios. |

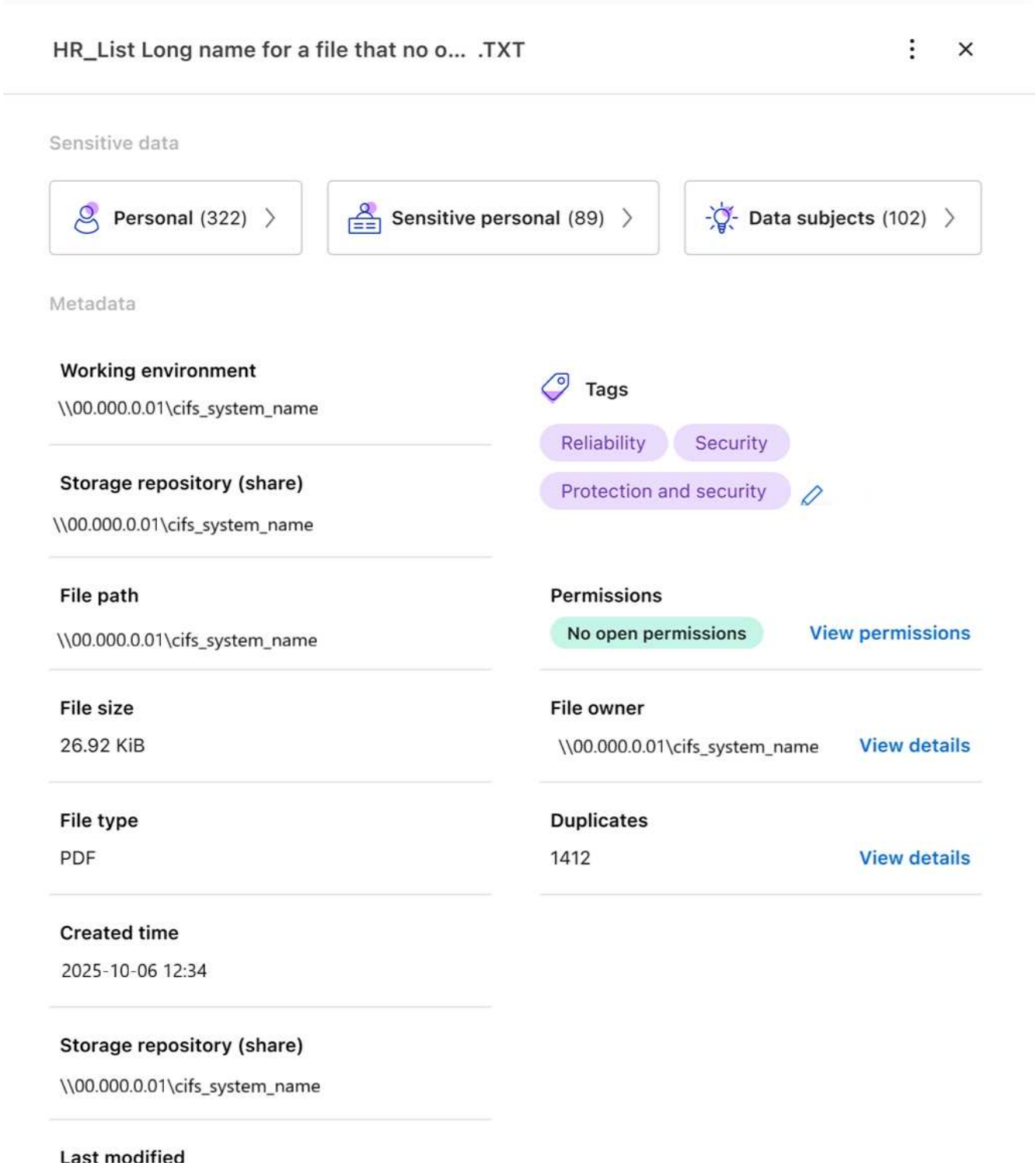
## Ver metadatos del archivo

Además de mostrarle el sistema y el volumen donde reside el archivo, los metadatos muestran mucha más información, incluidos los permisos del archivo, el propietario del archivo y si hay duplicados de este archivo. Esta información es útil si estás planeando"crear consultas guardadas" porque podrás ver toda la información que puedes utilizar para filtrar tus datos.

La disponibilidad de la información depende de la fuente de datos. Por ejemplo, el nombre del volumen y los permisos no se comparten para los archivos de base de datos.

**Pasos**

1. En el menú Clasificación de datos, seleccione **Investigación**.
2. En la lista Investigación de datos a la derecha, seleccione el símbolo de cursor hacia abajo a la derecha para cualquier archivo individual para ver los metadatos del archivo.




3. Opcionalmente, puede crear o agregar una etiqueta al archivo con el botón **Crear etiqueta**. Seleccione una etiqueta existente del menú desplegable o agregue una nueva etiqueta con el botón **+ Agregar**. Las etiquetas se pueden utilizar para filtrar datos.

## Ver permisos de usuario para archivos y directorios

Para ver una lista de todos los usuarios o grupos que tienen acceso a un archivo o directorio y los tipos de permisos que tienen, seleccione **Ver todos los permisos**. Esta opción solo está disponible para datos en recursos compartidos CIFS.

Si utiliza identificadores de seguridad (SID) en lugar de nombres de usuarios y grupos, debe integrar su Active Directory en la clasificación de datos. Para obtener más información, consulte "Agregar Active Directory a la clasificación de datos" .

**Pasos**

1. En el menú Clasificación de datos, seleccione **Investigación**.
2. En la lista Investigación de datos a la derecha, seleccione el símbolo de cursor hacia abajo a la derecha para cualquier archivo individual para ver los metadatos del archivo.
3. Para ver una lista de todos los usuarios o grupos que tienen acceso a un archivo o directorio y los tipos de permisos que tienen, en el campo Permisos abiertos, seleccione **Ver todos los permisos**.

   La clasificación de datos muestra hasta 100 usuarios en la lista.

4. Seleccione el cursor hacia abajo Botón para que cualquier grupo vea la lista de usuarios que forman parte del grupo.

   Puedes expandir un nivel del grupo para ver los usuarios que forman parte del grupo.

5. Seleccione el nombre de un usuario o grupo para actualizar la página de Investigación para que pueda ver todos los archivos y directorios a los que el usuario o grupo tiene acceso.

## Compruebe si hay archivos duplicados en sus sistemas de almacenamiento

Puede comprobar si se están almacenando archivos duplicados en sus sistemas de almacenamiento. Esto es útil si desea identificar áreas donde puede ahorrar espacio de almacenamiento. También es bueno asegurarse de que ciertos archivos que tienen permisos específicos o información confidencial no se dupliquen innecesariamente en sus sistemas de almacenamiento.

La clasificación de datos compara todos los archivos (excluidas las bases de datos) en busca de duplicados si son:

- 1 MB o lager
- O contienen información personal o información personal sensible.

La clasificación de datos utiliza tecnología hash para determinar archivos duplicados. Si dos archivos tienen el mismo código hash que otros, son duplicados exactos aunque sus nombres sean diferentes.

**Pasos**

1. En el menú Clasificación de datos, seleccione **Investigación**.
2. En el panel Filtro, seleccione "Tamaño de archivo" junto con "Duplicados" ("Tiene duplicados") para ver qué archivos de un determinado rango de tamaño están duplicados en su entorno.
3. Opcionalmente, descargue la lista de archivos duplicados y envíela a su administrador de almacenamiento para que pueda decidir qué archivos, si hay alguno, se pueden eliminar.
4. Opcionalmente, puede eliminar, etiquetar o mover los archivos duplicados. Seleccione los archivos en los que desea realizar una acción y luego seleccione la acción adecuada.

### Ver si un archivo específico está duplicado

Puede ver si un solo archivo tiene duplicados.

**Pasos**

1. En el menú Clasificación de datos, seleccione **Investigación**.
2. En la lista Investigación de datos, seleccione ⌄ a la derecha para cualquier archivo individual para ver los metadatos del archivo.

   Si existen duplicados para un archivo, esta información aparece junto al campo *Duplicados*.

3. Para ver la lista de archivos duplicados y dónde se encuentran, seleccione **Ver detalles**.
4. En la página siguiente, seleccione **Ver duplicados** para ver los archivos en la página de Investigación.
5. Opcionalmente, puede eliminar, etiquetar o mover los archivos duplicados. Seleccione los archivos en los que desea realizar una acción y luego seleccione la acción adecuada.

> Puede utilizar el valor de "hash de archivo" proporcionado en esta página e ingresarlo directamente en la página de Investigación para buscar un archivo duplicado específico en cualquier momento, o puede usarlo en una consulta guardada.

## Descargue su informe

Puede descargar sus resultados filtrados en formato CSV o JSON.

Se pueden descargar hasta tres archivos de informe si la clasificación de datos escanea archivos (datos no estructurados), directorios (carpetas y recursos compartidos de archivos) y bases de datos (datos estructurados).

Los archivos se dividen en archivos con un número fijo de filas o registros:

- JSON: 100.000 registros por informe que tarda unos 5 minutos en generarse
- CSV: 200.000 registros por informe que tarda aproximadamente 4 minutos en generarse

> Puede descargar una versión del archivo CSV para verlo en este navegador. Esta versión está limitada a 10.000 registros.

**Qué incluye el informe descargable**

El **Informe de datos de archivos no estructurados** incluye la siguiente información sobre sus archivos:

- Nombre del archivo
- Tipo de ubicación
- Nombre del sistema
- Repositorio de almacenamiento (por ejemplo, un volumen, un depósito, recursos compartidos)
- Tipo de repositorio
- Ruta del archivo
- Tipo de archivo
- Tamaño del archivo (en MB)
- Hora de creación
- Última modificación
- Último acceso

- Propietario del archivo
  - Los datos del propietario del archivo incluyen el nombre de la cuenta, el nombre de la cuenta SAM y la dirección de correo electrónico cuando se configura Active Directory.
- Categoría
- Información personal
- Información personal sensible
- Permisos abiertos
- Error de análisis de escaneo
- Fecha de detección de eliminación

  La fecha de detección de eliminación identifica la fecha en la que se eliminó o movió el archivo. Esto le permite identificar cuándo se han movido archivos confidenciales. Los archivos eliminados no contribuyen al recuento de números de archivos que aparece en el panel o en la página Investigación. Los archivos solo aparecen en los informes CSV.

El **Informe de datos de directorios no estructurados** incluye la siguiente información sobre sus carpetas y recursos compartidos de archivos:

- Tipo de sistema
- Nombre del sistema
- Nombre del directorio
- Repositorio de almacenamiento (por ejemplo, una carpeta o recursos compartidos de archivos)
- Propietario del directorio
- Hora de creación
- Tiempo descubierto
- Última modificación
- Último acceso
- Permisos abiertos
- Tipo de directorio

El **Informe de datos estructurados** incluye la siguiente información sobre las tablas de su base de datos:

- Nombre de la tabla de la base de datos
- Tipo de ubicación
- Nombre del sistema
- Repositorio de almacenamiento (por ejemplo, un esquema)
- Recuento de columnas
- Recuento de filas
- Información personal
- Información personal sensible

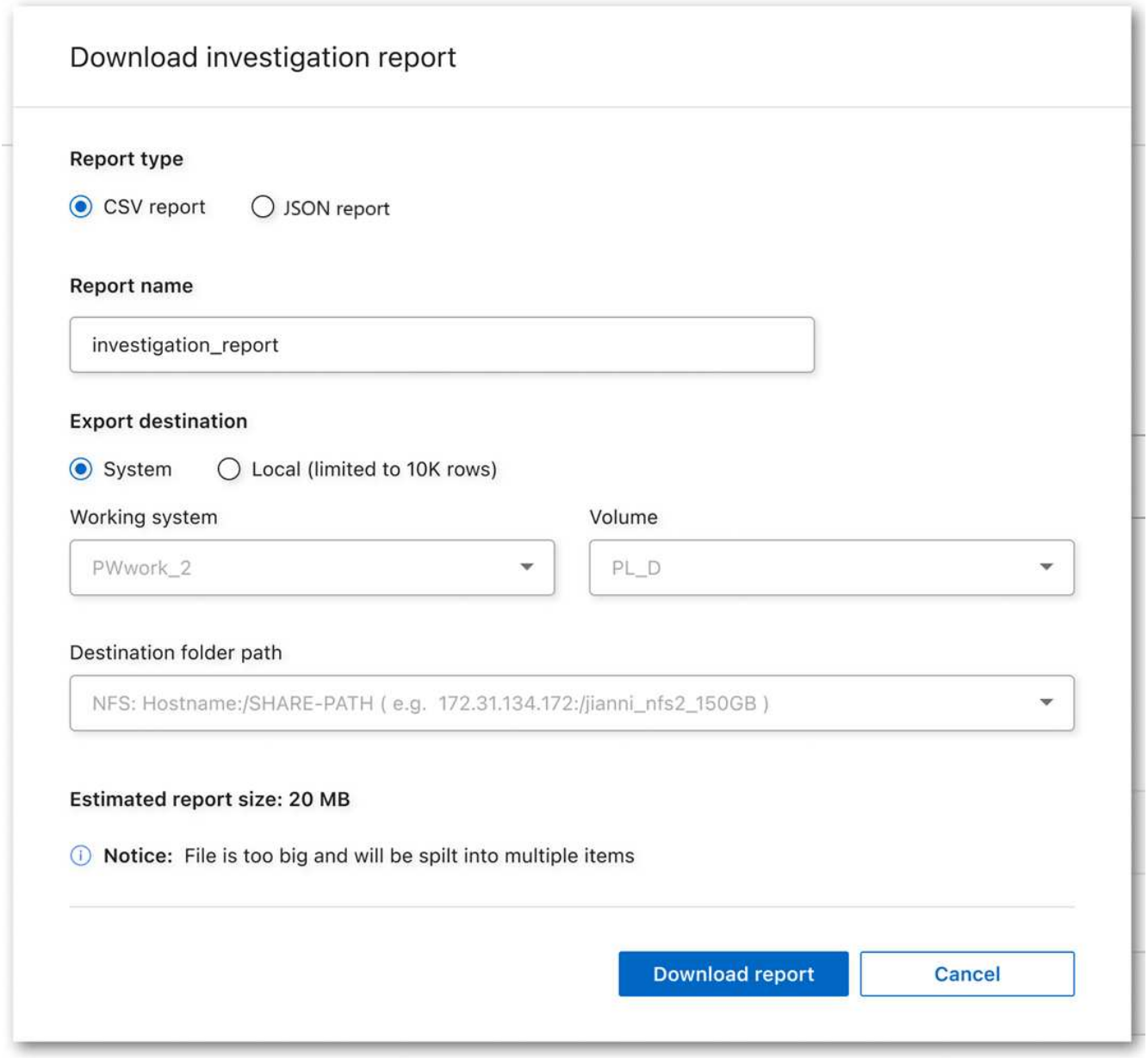
**Pasos para generar el informe**

1. Desde la página Investigación de datos, seleccione el Botón en la parte superior derecha de la página.

2. Elija el tipo de informe: CSV o JSON.
3. Introduzca un **nombre de informe**.
4. Para descargar el informe completo, seleccione **Sistema** y luego elija **Sistema** y **Volumen** en los respectivos menús desplegables. Proporcione una **Ruta de carpeta de destino**.

   Para descargar el informe en el navegador, seleccione **Local** . Tenga en cuenta que esta opción limita el informe a las primeras 10 000 filas y está limitada al formato **CSV**. No es necesario completar ningún otro campo si selecciona **Local**.

5. Seleccione **Descargar informe**.



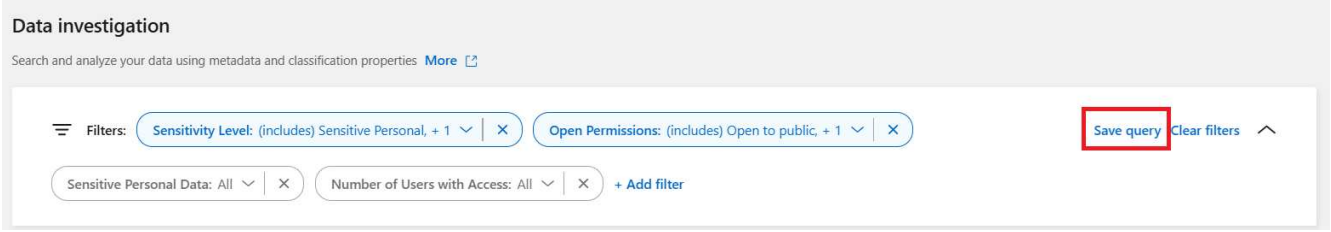

**Resultado**

Un cuadro de diálogo muestra un mensaje que indica que se están descargando los informes.

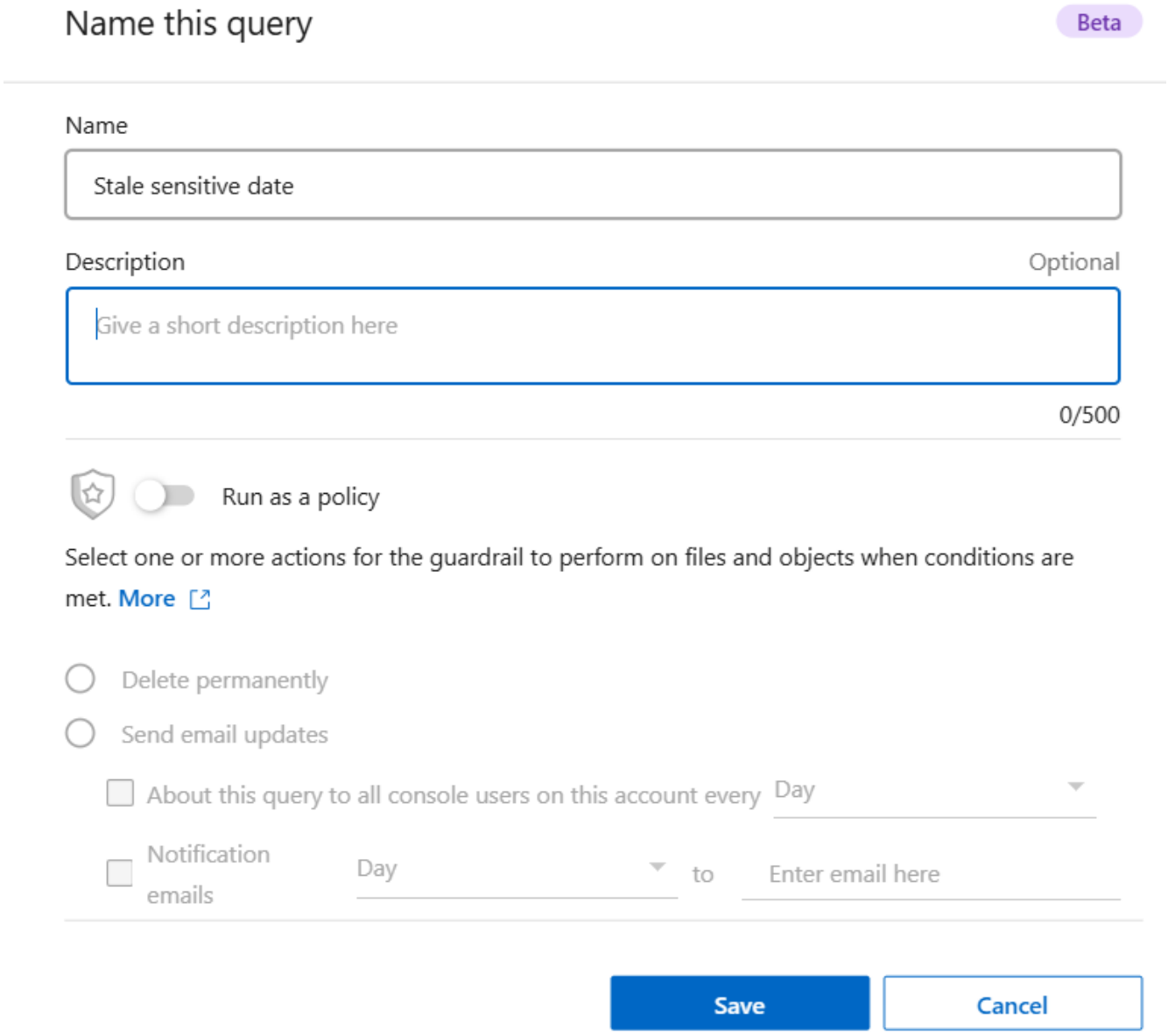
## Crear una consulta guardada basada en filtros seleccionados

### Pasos

1. En la pestaña Investigación, defina una búsqueda seleccionando los filtros que desea utilizar. Ver"Filtrado de datos en la página de Investigación" Para más detalles.
2. Una vez que tenga todas las características del filtro configuradas a su gusto, seleccione **Guardar consulta**.




3. Nombra la consulta guardada y agrega una descripción. El nombre debe ser único.
4. Opcionalmente, puede guardar la consulta como política:
   a. Para guardar la consulta como una política, cambie el interruptor **Ejecutar como política**.
   b. Elija **Eliminar permanentemente** o **Enviar actualizaciones por correo electrónico**. Si elige actualizaciones por correo electrónico, puede enviar por correo electrónico los resultados de la consulta a *todos* los usuarios de la consola con frecuencia diaria, semanal o mensual. Alternativamente, puede enviar la notificación a una dirección de correo electrónico específica con las mismas frecuencias.
5. Seleccione **Guardar**.




Una vez que haya creado la búsqueda o política, podrá verla en la pestaña **Consultas guardadas**.

Los resultados pueden tardar hasta 15 minutos en aparecer en la página Consultas guardadas.

# Administre consultas guardadas con NetApp Data Classification

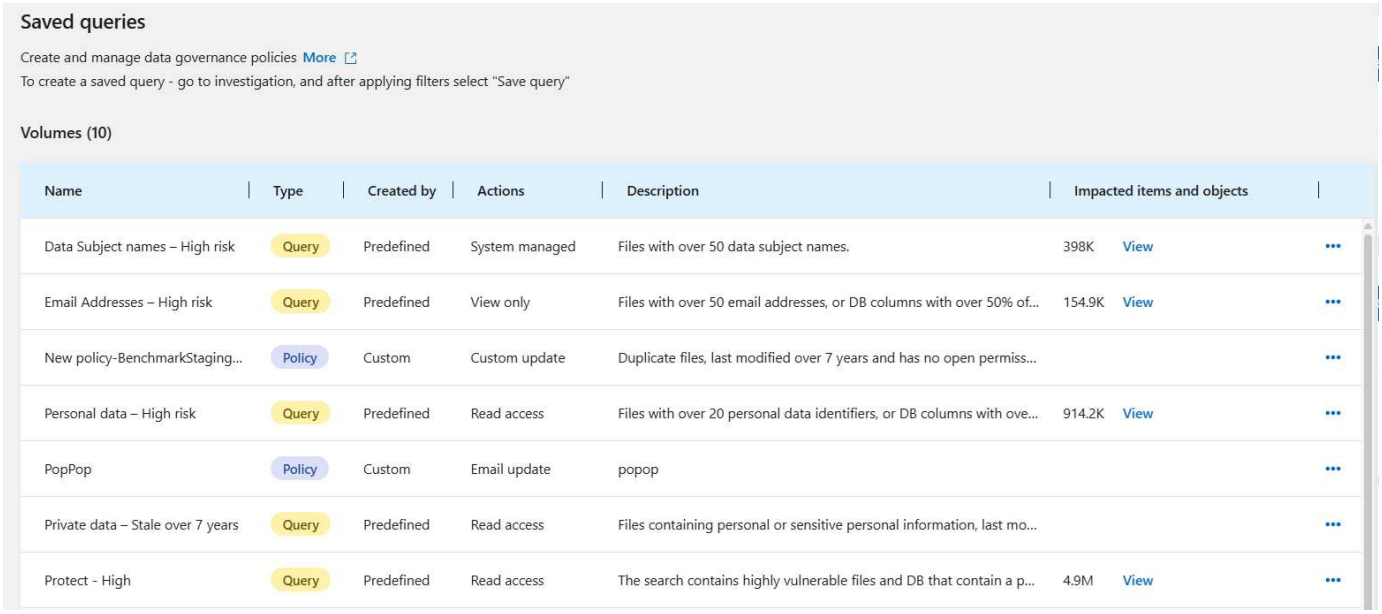
La clasificación de datos de NetaApp permite guardar sus consultas de búsqueda. Con una consulta guardada, puede crear filtros personalizados para ordenar las consultas frecuentes de su página de investigación de datos. La clasificación de datos también incluye consultas guardadas predefinidas basadas en solicitudes comunes.

La pestaña **Consultas guardadas** en el panel de Cumplimiento enumera todas las consultas guardadas

predefinidas y personalizadas disponibles en esta instancia de Clasificación de datos.

Las consultas guardadas también se pueden guardar como **políticas**. Mientras que las consultas filtran datos, las políticas le permiten actuar sobre los datos. Con una política: puede eliminar datos descubiertos o enviar actualizaciones por correo electrónico sobre los datos descubiertos.

Las consultas guardadas también aparecen en la lista de filtros en la página Investigación.




## Ver los resultados de las consultas guardadas en la página de Investigación

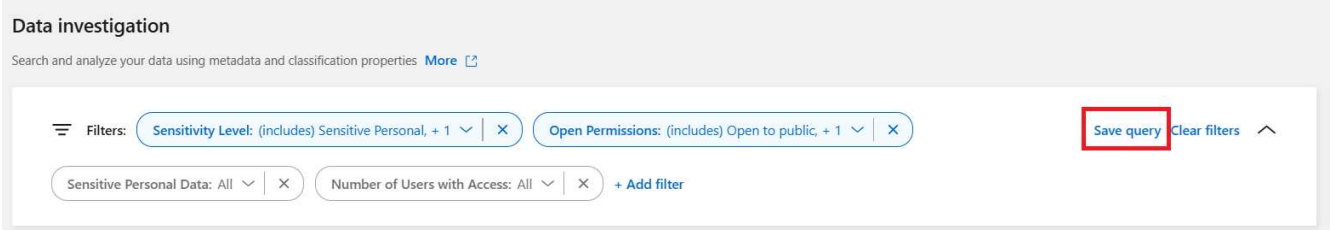
Para mostrar los resultados de una consulta guardada en la página Investigación, seleccione el icono Botón para una búsqueda específica y luego seleccione **Investigar resultados**.


## Crear consultas y políticas guardadas

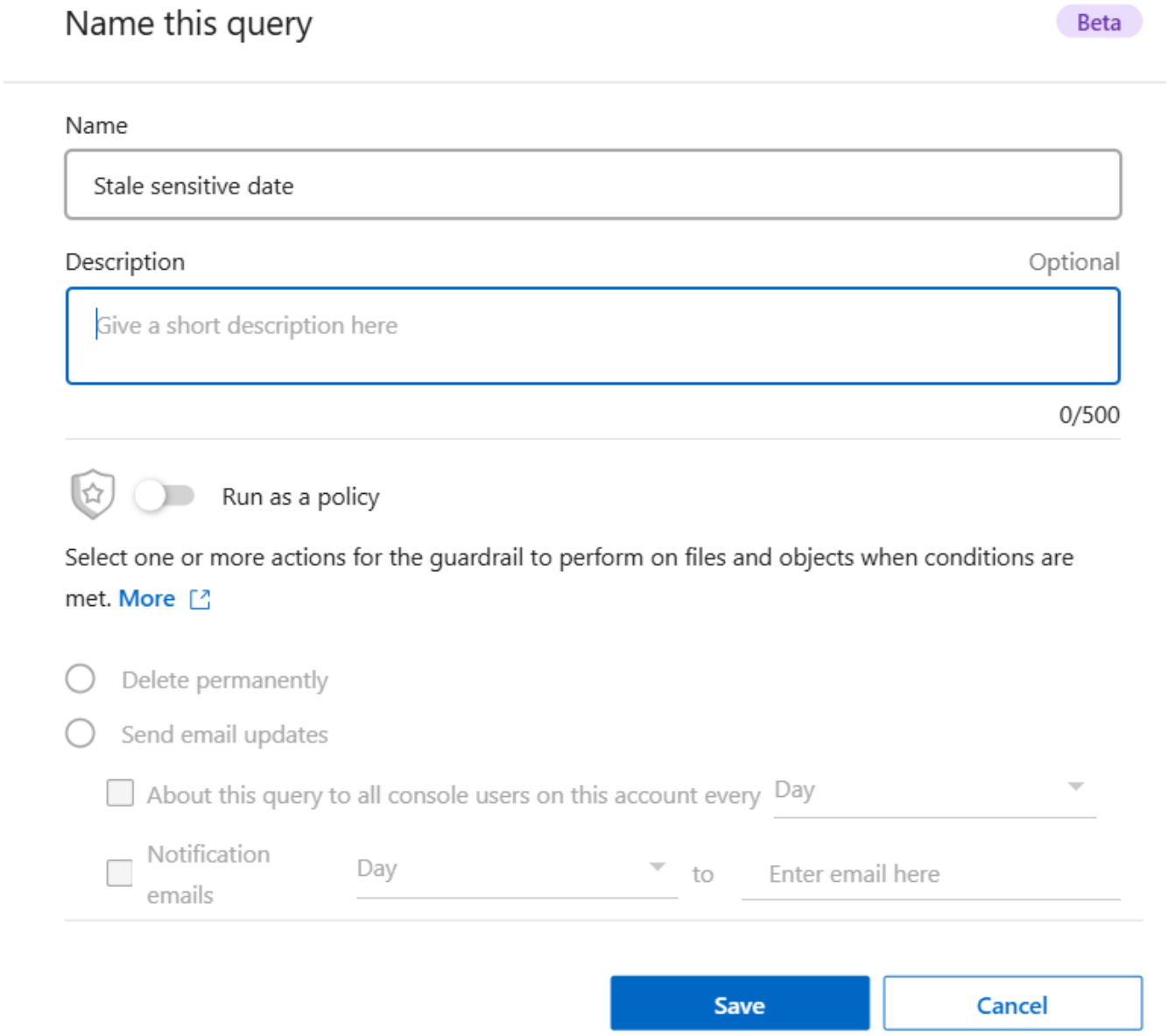
Puede crear sus propias consultas guardadas personalizadas que proporcionen resultados para consultas específicas de su organización. Se devuelven resultados para todos los archivos y directorios (recursos compartidos y carpetas) que coinciden con los criterios de búsqueda.

**Pasos**

1. En la pestaña Investigación, defina una búsqueda seleccionando los filtros que desea utilizar. Ver"Filtrado de datos en la página de Investigación" Para más detalles.
2. Una vez que tenga todas las características del filtro configuradas a su gusto, seleccione **Guardar consulta**.




3. Nombra la consulta guardada y agrega una descripción. El nombre debe ser único.
4. Opcionalmente, puede guardar la consulta como política:
   a. Para guardar la consulta como una política, cambie el interruptor **Ejecutar como política**.
   b. Elija **Eliminar permanentemente** o **Enviar actualizaciones por correo electrónico**. Si elige actualizaciones por correo electrónico, puede enviar por correo electrónico los resultados de la consulta a *todos* los usuarios de la consola con frecuencia diaria, semanal o mensual. Alternativamente, puede enviar la notificación a una dirección de correo electrónico específica con las mismas frecuencias.
5. Seleccione **Guardar**.




Una vez que haya creado la búsqueda o política, podrá verla en la pestaña **Consultas guardadas**.

## Editar consultas o políticas guardadas

Puede modificar el nombre y la descripción de una consulta guardada. También puede convertir una consulta en una política y viceversa.

No se pueden modificar las consultas guardadas predeterminadas. No se pueden modificar los filtros de una consulta guardada. Alternativamente, puede ver los resultados de la investigación de una consulta guardada, cambiar o modificar los filtros y luego guardarla como una nueva consulta o política.

**Pasos**

1. Desde la página Consultas guardadas, seleccione **Editar búsqueda** para la búsqueda que desea cambiar.


2. Realice los cambios en los campos de nombre y descripción. Para cambiar únicamente los campos de nombre y descripción.

   Opcionalmente, puede convertir la consulta en una política o convertir la política en una consulta guardada. Cambie el interruptor **Ejecutar como política** según sea necesario. .. Si está convirtiendo la consulta en una política, elija **Eliminar permanentemente** o **Enviar actualizaciones por correo electrónico**. Si elige actualizaciones por correo electrónico, puede enviar por correo electrónico los resultados de la consulta a *todos* los usuarios de la consola con frecuencia diaria, semanal o mensual. Alternativamente, puede enviar la notificación a una dirección de correo electrónico específica con las mismas frecuencias.

3. Seleccione **Guardar** para completar los cambios.

## Eliminar consultas guardadas

Puede eliminar cualquier consulta o política guardada personalizada si ya no la necesita. No puedes eliminar las consultas guardadas predeterminadas.

Para eliminar una consulta guardada, seleccione el Botón para una búsqueda específica, seleccione **Eliminar consulta**, luego seleccione **Eliminar consulta** nuevamente en el cuadro de diálogo de confirmación.

## Consultas predeterminadas

La clasificación de datos proporciona las siguientes consultas de búsqueda definidas por el sistema:

- **Nombres de los interesados - Alto riesgo**

  Archivos con más de 50 nombres de interesados

- **Direcciones de correo electrónico - Alto riesgo**

  Archivos con más de 50 direcciones de correo electrónico o columnas de base de datos con más del 50 % de sus filas que contienen direcciones de correo electrónico

- **Datos personales - Alto riesgo**

  Archivos con más de 20 identificadores de datos personales o columnas de base de datos con más del 50% de sus filas que contienen identificadores de datos personales

- **Datos privados - Obsoletos durante más de 7 años**

  Archivos que contienen información personal o información personal sensible, modificados por última vez hace más de 7 años

- **Protección - Alta**

  Archivos o columnas de base de datos que contienen una contraseña, información de tarjeta de crédito, número IBAN o número de seguro social

- **Protección - Baja**

  Archivos a los que no se ha accedido durante más de 3 años

- **Protección - Media**

  Archivos que contienen archivos o columnas de bases de datos con identificadores de datos personales, incluidos números de identificación, números de identificación fiscal, números de licencia de conducir, identificaciones médicas o números de pasaporte

- **Datos personales sensibles - Alto riesgo**

  Archivos con más de 20 identificadores de datos personales confidenciales o columnas de base de datos con más del 50 % de sus filas que contienen datos personales confidenciales

# Cambie la configuración del análisis de NetApp Data Classification para sus repositorios

Puede administrar cómo se escanean sus datos en cada uno de sus sistemas y fuentes de datos. Puede realizar los cambios sobre la base de un "repositorio", lo que significa que puede realizar cambios para cada volumen, esquema, usuario, etc., dependiendo del tipo de fuente de datos que esté escaneando.

Algunas de las cosas que puede cambiar son si se escanea o no un repositorio y si NetApp Data Classification está realizando una"escaneo de mapeo o escaneo de mapeo y clasificación" . También puede pausar y reanudar el escaneo, por ejemplo, si necesita dejar de escanear un volumen por un período de tiempo.

## Ver el estado del escaneo de sus repositorios

Puede ver los repositorios individuales que NetApp Data Classification está escaneando (volúmenes, depósitos, etc.) para cada sistema y fuente de datos. También puedes ver cuántos han sido "Mapeados" y cuántos han sido "Clasificados". La clasificación lleva más tiempo porque la identificación completa de la IA se realiza en todos los datos.

Puede ver el estado de escaneo de cada entorno de trabajo en la página de Configuración:

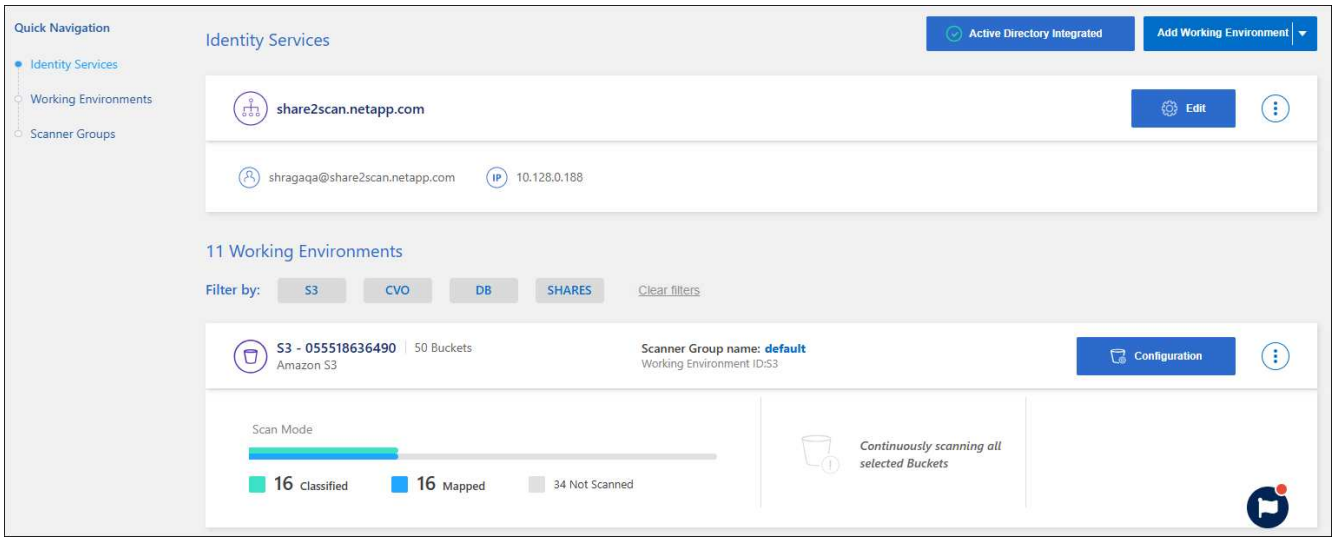
- **Inicializando** (punto azul claro): La configuración del mapa o clasificación está activada. Esto aparece brevemente antes de pasar al estado de "cola pendiente".
- **Cola pendiente** (punto naranja): la tarea de escaneo está esperando a ser incluida en la cola de escaneo.
- **En cola** (punto naranja): La tarea se agregó correctamente a la cola de escaneo. El sistema comenzará a mapear o clasificar el volumen cuando llegue su turno en la cola.
- **En ejecución** (punto verde): la tarea de escaneo, que estaba en la cola, está en progreso activo en el repositorio de almacenamiento seleccionado.
- **Terminado** (punto verde): El escaneo del repositorio de almacenamiento está completo.
- **Pausa** (punto gris): Has pausado el escaneo. Aunque los cambios en el volumen no se muestran en el sistema, la información obtenida mediante el escaneo permanece disponible.
- **Error** (punto rojo): El escaneo no puede completarse porque encontró problemas. Si necesita completar una acción, el error aparece en la información sobre herramientas debajo de la columna “Acción requerida”. De lo contrario, el sistema muestra un estado de “error” e intenta recuperarse. Cuando termina

el estado cambia.

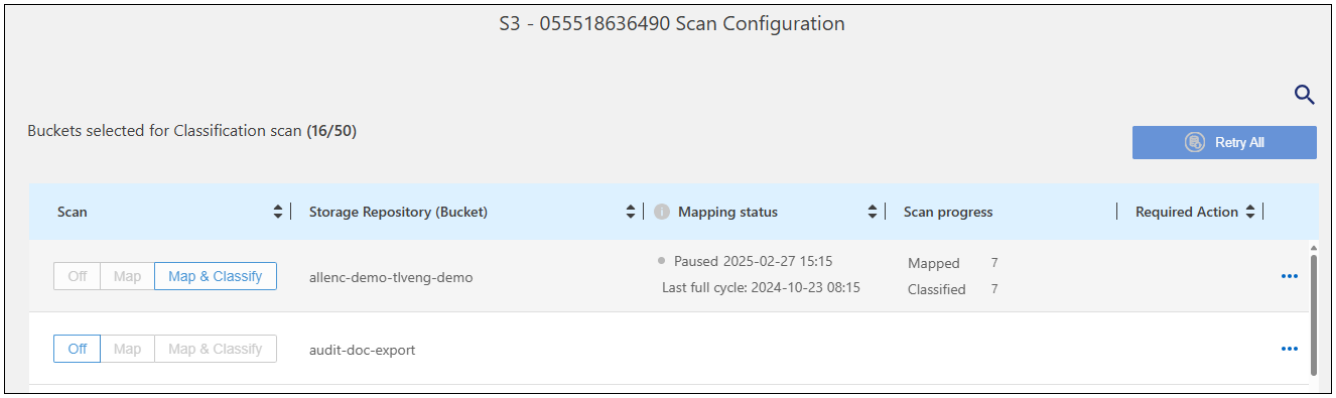
- **No escanea**: Se seleccionó la configuración de volumen “Desactivado” y el sistema no está escaneando el volumen.

**Pasos**

1. Desde el menú Clasificación de datos, seleccione **Configuración**.




2. Desde la pestaña Configuración, seleccione el botón **Configuración** para el sistema.
3. En la página Configuración de escaneo, vea las configuraciones de escaneo para todos los repositorios.




4. Durante un escaneo, coloque el cursor sobre la barra de progreso en la columna *Estado de mapeo* para ver la cantidad de archivos en la cola que se deben mapear o clasificar para ese repositorio.

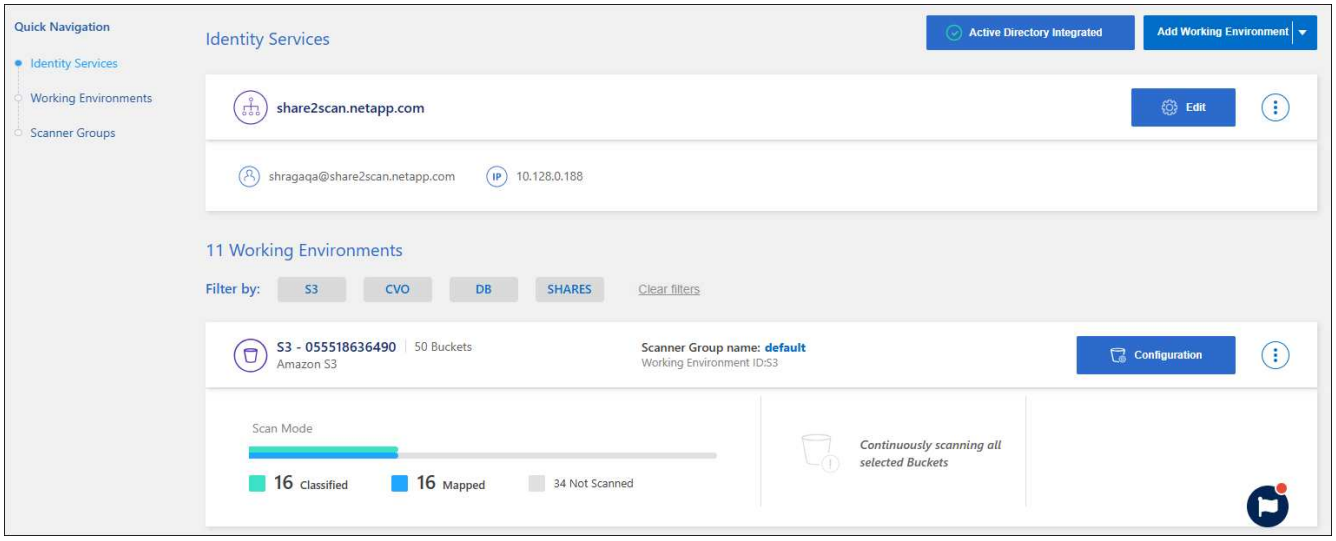
## Cambiar el tipo de escaneo de un repositorio

Puede iniciar o detener escaneos de solo mapeo, o escaneos de mapeo y clasificación, en un sistema en cualquier momento desde la página de Configuración. También puede cambiar de escaneos de solo mapeo a escaneos de mapeo y clasificación, y viceversa.

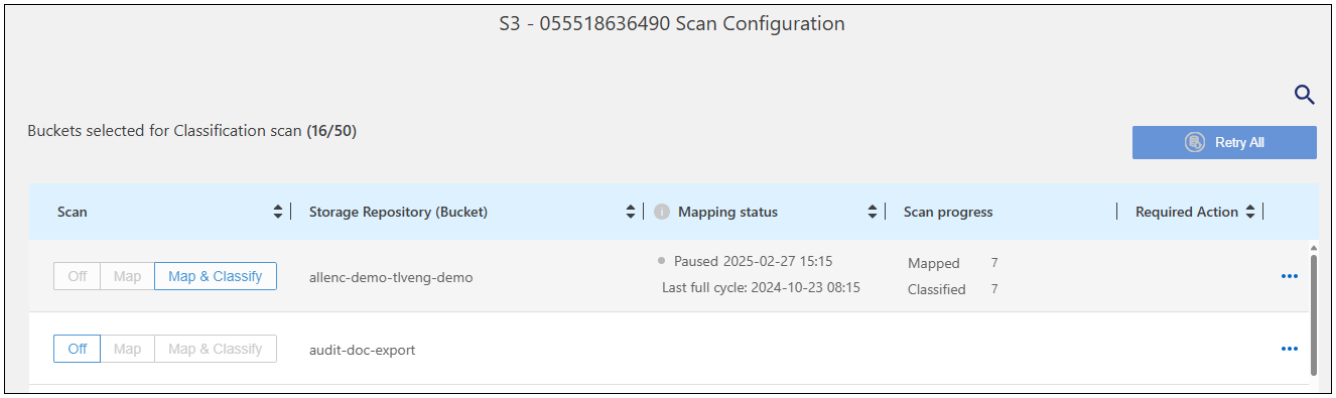
Las bases de datos no se pueden configurar para realizar exploraciones de solo mapeo. El escaneo de la base de datos puede estar Desactivado o Activado; donde Activado es equivalente a Mapear y clasificar.

**Pasos**

1. Desde el menú Clasificación de datos, seleccione **Configuración**.
2. Desde la pestaña Configuración, seleccione el botón **Configuración** para el sistema.

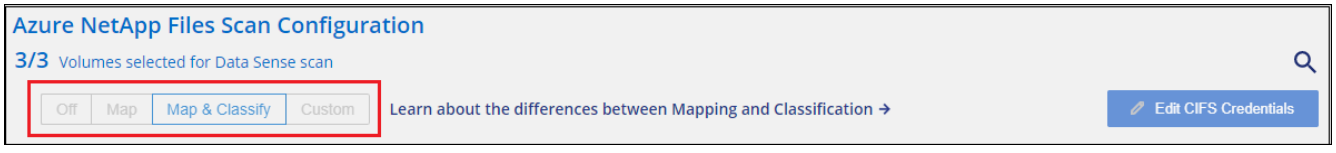



3. En la página Configuración de escaneo, cambie cualquiera de los repositorios (depósitos en este ejemplo) para realizar escaneos **Map** o **Map & Classify**.




Ciertos tipos de sistemas le permiten cambiar el tipo de escaneo globalmente para todos los repositorios usando una barra de botones en la parte superior de la página. Esto es válido para Cloud Volumes ONTAP, ONTAP local, Azure NetApp Files y Amazon FSx para sistemas ONTAP .

El siguiente ejemplo muestra esta barra de botones para un sistema Azure NetApp Files .




## Priorizar los escaneos

Puede priorizar los escaneos de solo mapeo más importantes o mapear y clasificar los escaneos para garantizar que los escaneos de alta prioridad se completen primero.

De forma predeterminada, los escaneos se ponen en cola según el orden en el que se inician. Con la capacidad de priorizar los escaneos, puede moverlos al frente de la cola. Se pueden priorizar múltiples

escaneos. La prioridad se designa en un orden de primero en entrar, primero en salir, lo que significa que el primer escaneo que prioriza pasa al frente de la cola; el segundo escaneo que prioriza pasa al segundo en la cola, y así sucesivamente.

La prioridad se concede por única vez. Los escaneos automáticos de datos cartográficos se realizan en el orden predeterminado.

**Pasos**

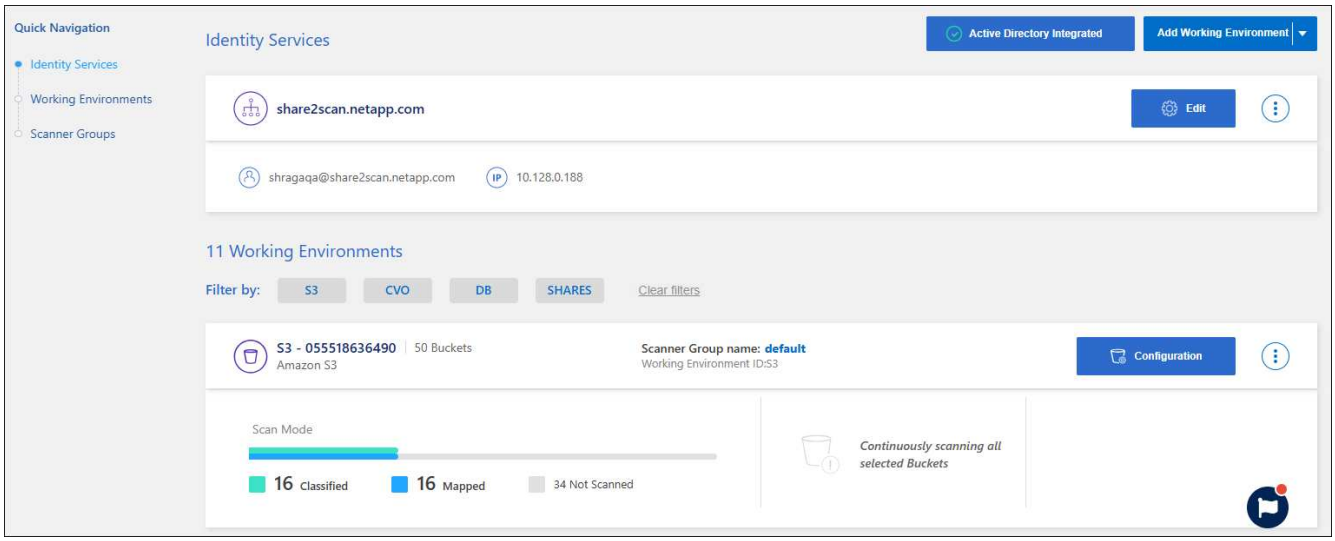
1. Desde el menú Clasificación de datos, seleccione **Configuración**.
2. Seleccione los recursos que desea priorizar.
3. De las acciones … opción, seleccione **Priorizar escaneo**.

## Detener la búsqueda de un repositorio

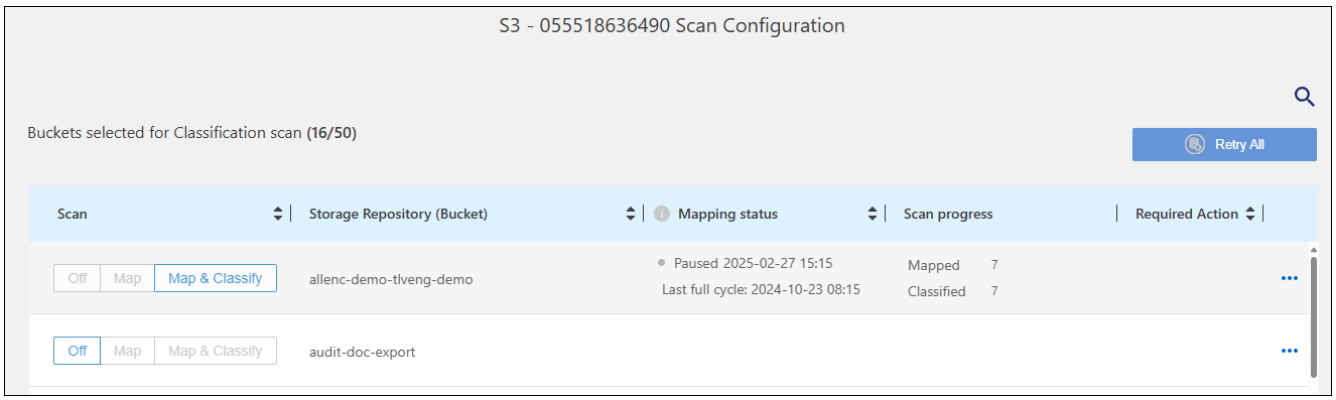
Puede dejar de escanear un repositorio (por ejemplo, un volumen) si ya no necesita supervisarlo para verificar su cumplimiento. Puedes hacer esto desactivando el escaneo. Cuando se desactiva el escaneo, se eliminan del sistema toda la indexación y la información sobre ese volumen y se detiene el cobro por escanear los datos.

**Pasos**

1. Desde el menú Clasificación de datos, seleccione **Configuración**.
2. Desde la pestaña Configuración, seleccione el botón **Configuración** para el sistema.




3. En la página Configuración de escaneo, seleccione **Desactivado** para detener el escaneo de un depósito en particular.




## Pausar y reanudar el escaneo de un repositorio

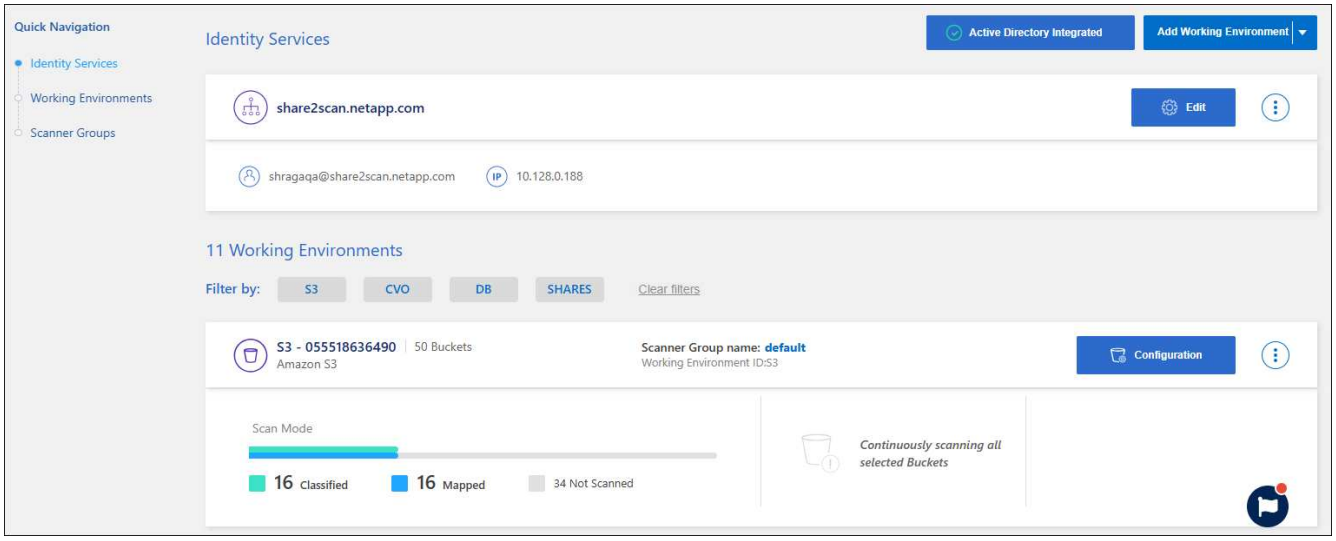
Puede "pausar" el escaneo en un repositorio si desea detener temporalmente el escaneo de cierto contenido. Pausar el escaneo significa que la Clasificación de Datos no realizará más escaneos para detectar cambios o adiciones al repositorio. Todos los resultados de escaneo actuales permanecen accesibles en la Clasificación de datos.

Si pausas los escaneos, no se eliminan los cargos de facturación porque los datos aún están en el sistema.

Puede reanudar el escaneo en cualquier momento.

**Pasos**

1. Desde el menú Clasificación de datos, seleccione **Configuración**.
2. Desde la pestaña Configuración, seleccione el botón **Configuración** para el sistema.




3. En la página Configuración de escaneo, seleccione Acciones ••• icono.
4. Seleccione **Pausa** para pausar el escaneo de un volumen, o seleccione **Reanudar** para reanudar el escaneo de un volumen que se había pausado previamente.

# Ver informes de cumplimiento de NetApp Data Classification

La NetApp Data Classification proporciona informes que puede utilizar para comprender mejor el estado del programa de privacidad de datos de su organización.

De forma predeterminada, los paneles de clasificación de datos muestran datos de cumplimiento y gobernanza de todos los sistemas, bases de datos y fuentes de datos. Si desea ver informes que contienen datos solo de algunos de los sistemas, puede filtrar para ver solo esos.

- Los informes de cumplimiento solo están disponibles si realiza un análisis de clasificación completo en sus fuentes de datos. Las fuentes de datos que hayan tenido un escaneo de solo mapeo solo pueden generar el Informe de mapeo de datos.
- NetApp no puede garantizar la precisión del 100% de los datos personales y los datos personales confidenciales que identifica la clasificación de datos. Siempre debes validar la información revisando los datos.

Los siguientes informes están disponibles para la clasificación de datos:

- **Informe de evaluación de descubrimiento de datos**: proporciona un análisis de alto nivel del entorno escaneado para resaltar los hallazgos del sistema y mostrar áreas de preocupación y posibles pasos de remediación. Este informe está disponible en el panel de Gobernanza.
- **Informe general de mapeo de datos completo**: proporciona información sobre el tamaño y la cantidad de archivos en sus sistemas. Esto incluye la capacidad de uso, la antigüedad de los datos, el tamaño de los datos y los tipos de archivos. Este informe está disponible en el panel de Gobernanza.
- **Informe de solicitud de acceso del interesado**: le permite extraer un informe de todos los archivos que contienen información sobre el nombre específico o un identificador personal del interesado. Este informe está disponible en el panel de Cumplimiento.
- **Informe HIPAA**: le ayuda a identificar la distribución de información de salud en sus archivos. Este informe está disponible en el panel de Cumplimiento.
- **Informe PCI DSS**: le ayuda a identificar la distribución de la información de tarjetas de crédito en sus archivos. Este informe está disponible en el panel de Cumplimiento.
- **Informe de evaluación de riesgos de privacidad**: proporciona información sobre la privacidad de sus datos y una puntuación de riesgo de privacidad. Este informe está disponible en el panel de Cumplimiento.
- **Informes sobre un tipo de información específico**: Se encuentran disponibles informes que incluyen detalles sobre los archivos identificados que contienen datos personales y datos personales sensibles. También puedes ver los archivos desglosados por categoría y tipo de archivo.

## Seleccione los sistemas para los informes

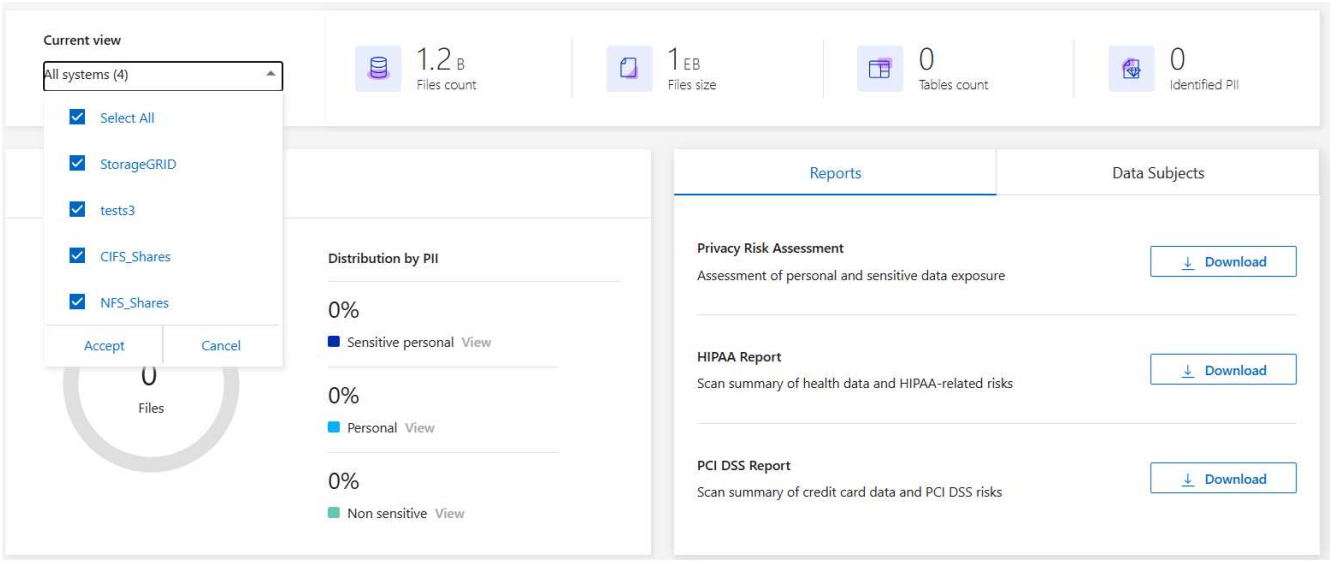
Puede filtrar el contenido del panel de Cumplimiento de clasificación de datos para ver los datos de cumplimiento de todos los sistemas y bases de datos, o solo de sistemas específicos.

Al filtrar el panel, la Clasificación de datos limita los datos de cumplimiento y los informes solo a aquellos sistemas que usted seleccionó.

**Pasos**

1. En el menú Clasificación de datos, seleccione **Cumplimiento**.

2. Seleccione el filtro de sistemas en el menú desplegable y luego seleccione los sistemas.
3. Seleccione **Aceptar** para confirmar su selección.




## Informe de solicitud de acceso del interesado

Las regulaciones de privacidad como el RGPD europeo otorgan a los interesados (como clientes o empleados) el derecho a acceder a sus datos personales. Cuando un interesado solicita esta información, esto se conoce como DSAR (solicitud de acceso al interesado). Las organizaciones están obligadas a responder a estas solicitudes "sin demoras indebidas" y, a más tardar, dentro del mes siguiente a su recepción.

Puede responder a una DSAR buscando el nombre completo de un sujeto o un identificador conocido (como una dirección de correo electrónico) y luego descargando un informe. El informe está diseñado para ayudar a su organización a cumplir con el requisito de GDPR o leyes de privacidad de datos similares.

¿Cómo puede la clasificación de datos ayudarle a responder a una DSAR?

Cuando se realiza una búsqueda de un interesado, la Clasificación de datos encuentra todos los archivos que contienen el nombre o identificador de esa persona. La clasificación de datos verifica los últimos datos preindexados en busca del nombre o identificador. No inicia un nuevo escaneo.

Una vez completada la búsqueda, puede descargar la lista de archivos para un informe de solicitud de acceso del interesado. El informe recopila información de los datos y la expresa en términos legales que usted puede enviar a la persona.

Actualmente no se admite la búsqueda de interesados en las bases de datos.

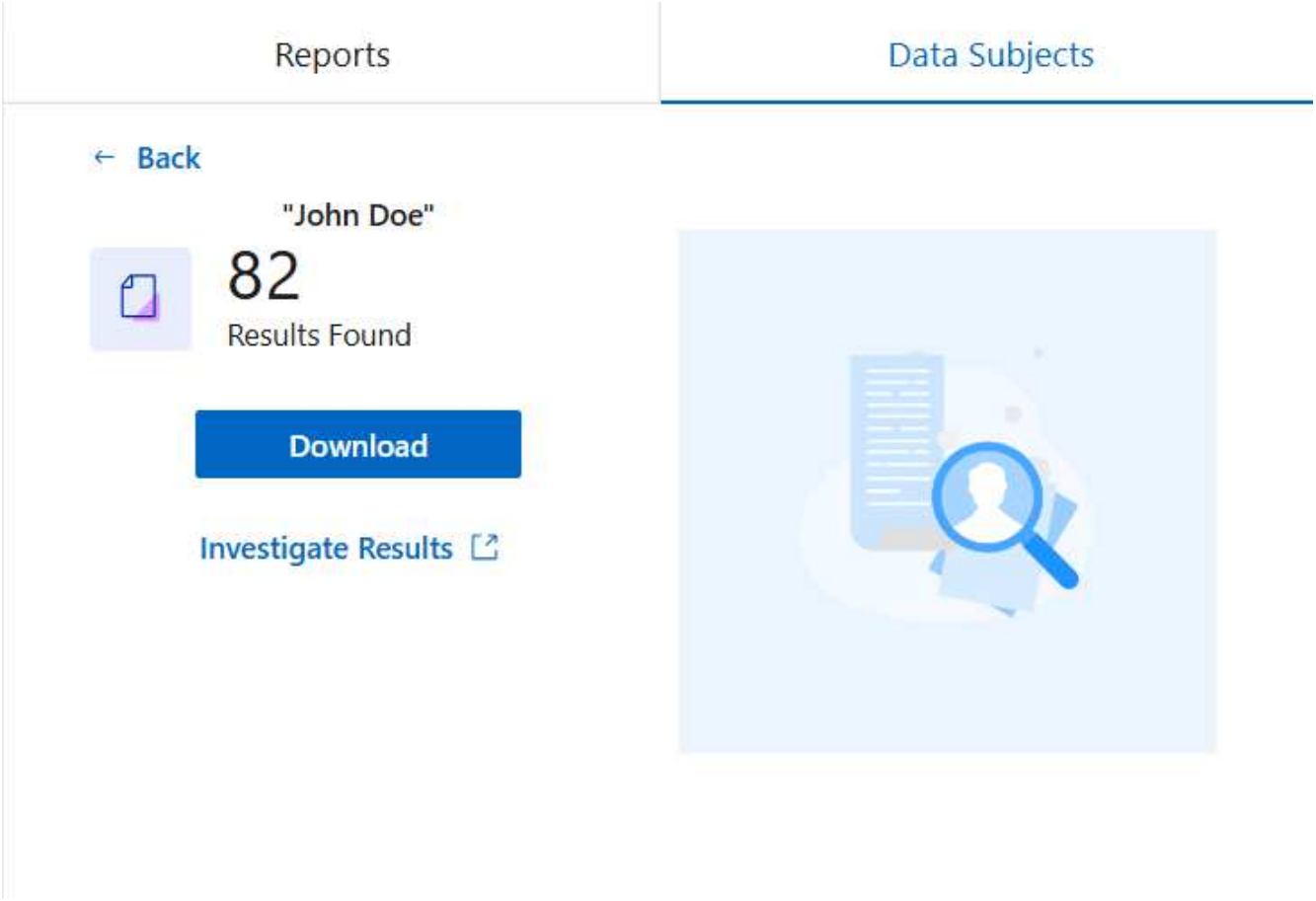
### Búsqueda de interesados y descarga de informes

Busque el nombre completo del interesado o un identificador conocido y luego descargue un informe de lista de archivos o un informe DSAR. Puedes buscar por"cualquier tipo de información personal" .

Al buscar nombres de interesados se admiten los idiomas inglés, alemán, japonés y español. Más adelante se añadirá soporte para más idiomas.

**Pasos**

1. En el menú Clasificación de datos, seleccione **Cumplimiento**.
2. Desde la página de Cumplimiento, busque la pestaña **Sujetos de datos**.
3. En la sección **Sujetos de datos**, ingrese un nombre o identificador conocido y luego seleccione **Buscar**.
4. Cuando se complete la búsqueda, seleccione **Descargar** para acceder a la respuesta a la solicitud de acceso del interesado. Seleccione **Investigar resultados** para ver más información en la página Investigación de
datos.



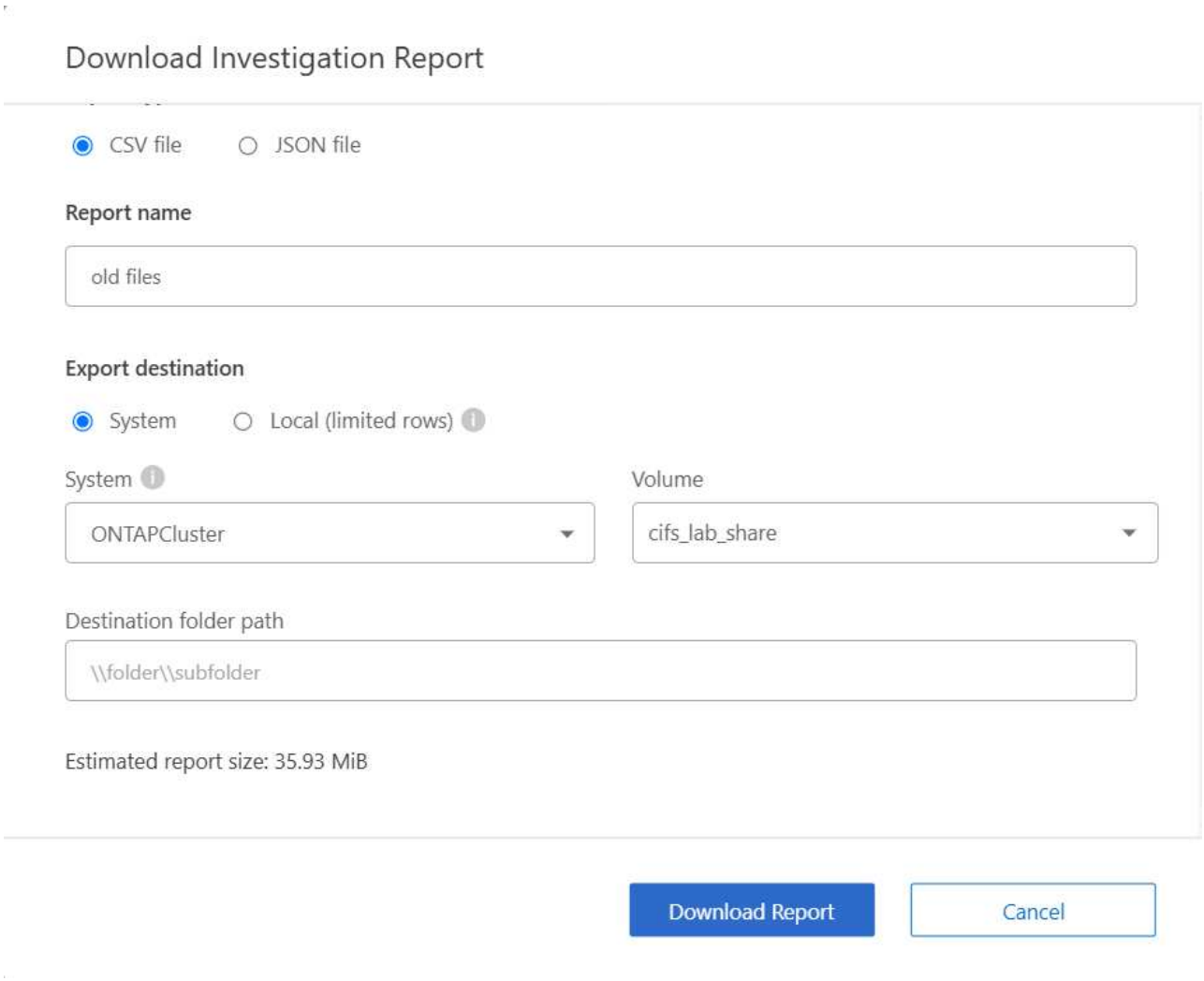

5. Revise los resultados en Clasificación de datos o descárguelos como informe seleccionando el ícono de descarga.

   a. Cuando seleccione el icono de descarga, configure sus ajustes de descarga:
      - Elija el formato de la película: CSV o JSON
      - Introduzca un **Nombre del informe**
      - Elija el destino de la exportación: **Sistema** o su máquina **Local**.

        Si elige sistema, se descargarán todos los datos. También debe seleccionar la ruta de **Sistema**, **Volumen** y **Carpeta de destino**.

   Si elige **Local**, limitará el informe a las primeras 10 000 filas de datos no estructurados; 5000 filas de datos no estructurados y 1000 filas de datos estructurados.

   a. Seleccione **Descargar informe** para iniciar la descarga.




## Informe de la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA)

El Informe de la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA) puede ayudarle a identificar archivos que contienen información de salud. Está diseñado para ayudar a su organización a cumplir con los requisitos de privacidad de datos de HIPAA. La información que busca la clasificación de datos incluye:

- Patrón de referencia de salud
- Código médico CIE-10-CM
- Código médico CIE-9-CM
- RRHH - Categoría Salud
- Categoría de datos de aplicaciones de salud

El informe incluye la siguiente información:

- Descripción general: ¿Cuántos archivos contienen información de salud y en qué sistemas?
- Cifrado: el porcentaje de archivos que contienen información de salud que se encuentran en sistemas cifrados o no cifrados. Esta información es específica de Cloud Volumes ONTAP.
- Protección contra ransomware: el porcentaje de archivos que contienen información de salud que se encuentran en sistemas que tienen o no habilitada la protección contra ransomware. Esta información es

específica de Cloud Volumes ONTAP.

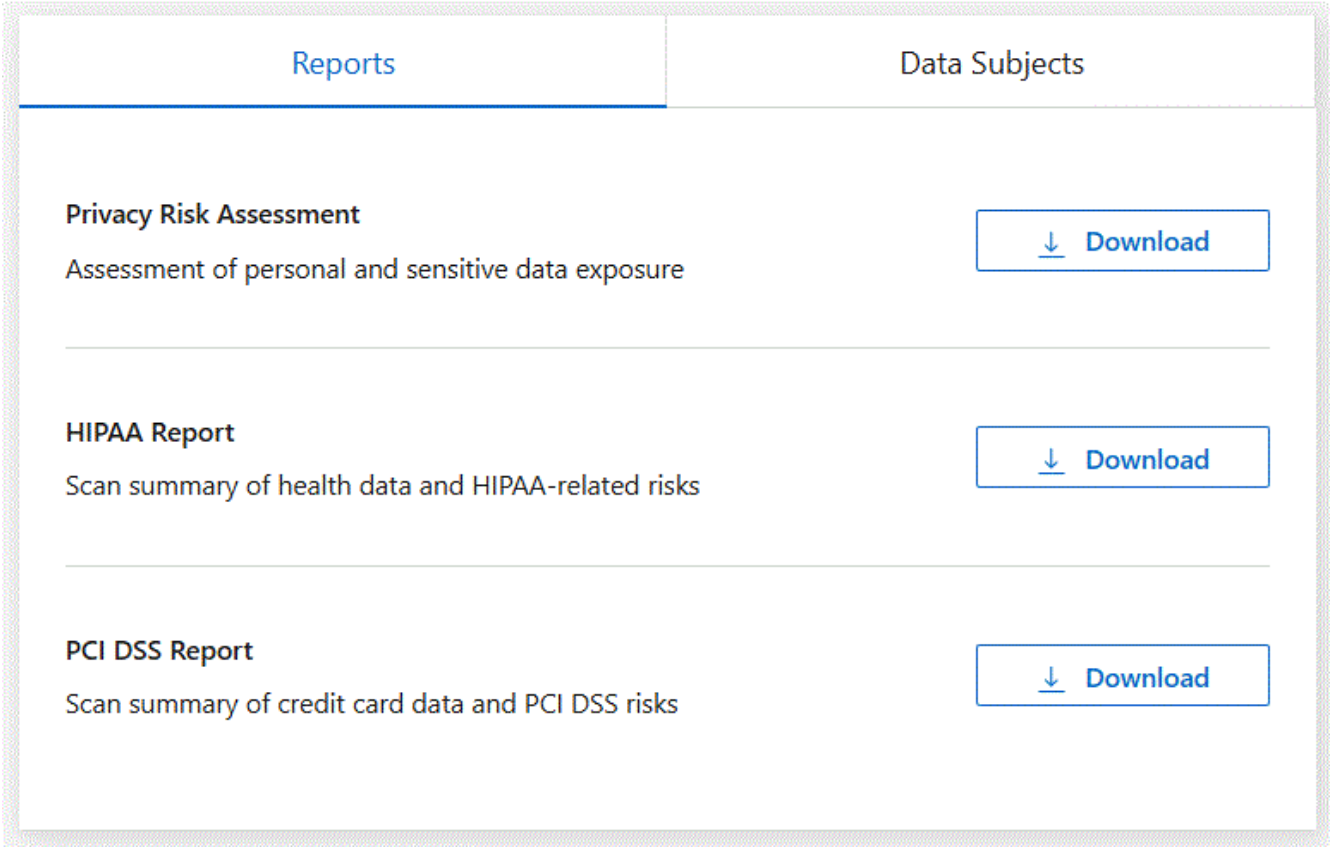
- Retención: El período de tiempo en el que se modificaron los archivos por última vez. Esto es útil porque no debe conservar la información de salud durante más tiempo del necesario para procesarla.
- Distribución de información de salud: los sistemas donde se encontró la información de salud y si el cifrado y la protección contra ransomware están habilitados.

**Generar el informe HIPAA**

Vaya a la pestaña Cumplimiento para generar el informe.

**Pasos**

1. En el menú Clasificación de datos, seleccione **Cumplimiento**.
2. Localice el **panel Informes**. Seleccione el ícono de descarga junto a **Informe HIPAA**.




**Resultado**

La clasificación de datos genera un informe en PDF.

## Informe sobre el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS)

El informe del Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) puede ayudarle a identificar la distribución de la información de tarjetas de crédito en sus archivos.

El informe incluye la siguiente información:

- Descripción general: ¿Cuántos archivos contienen información de tarjetas de crédito y en qué sistemas?

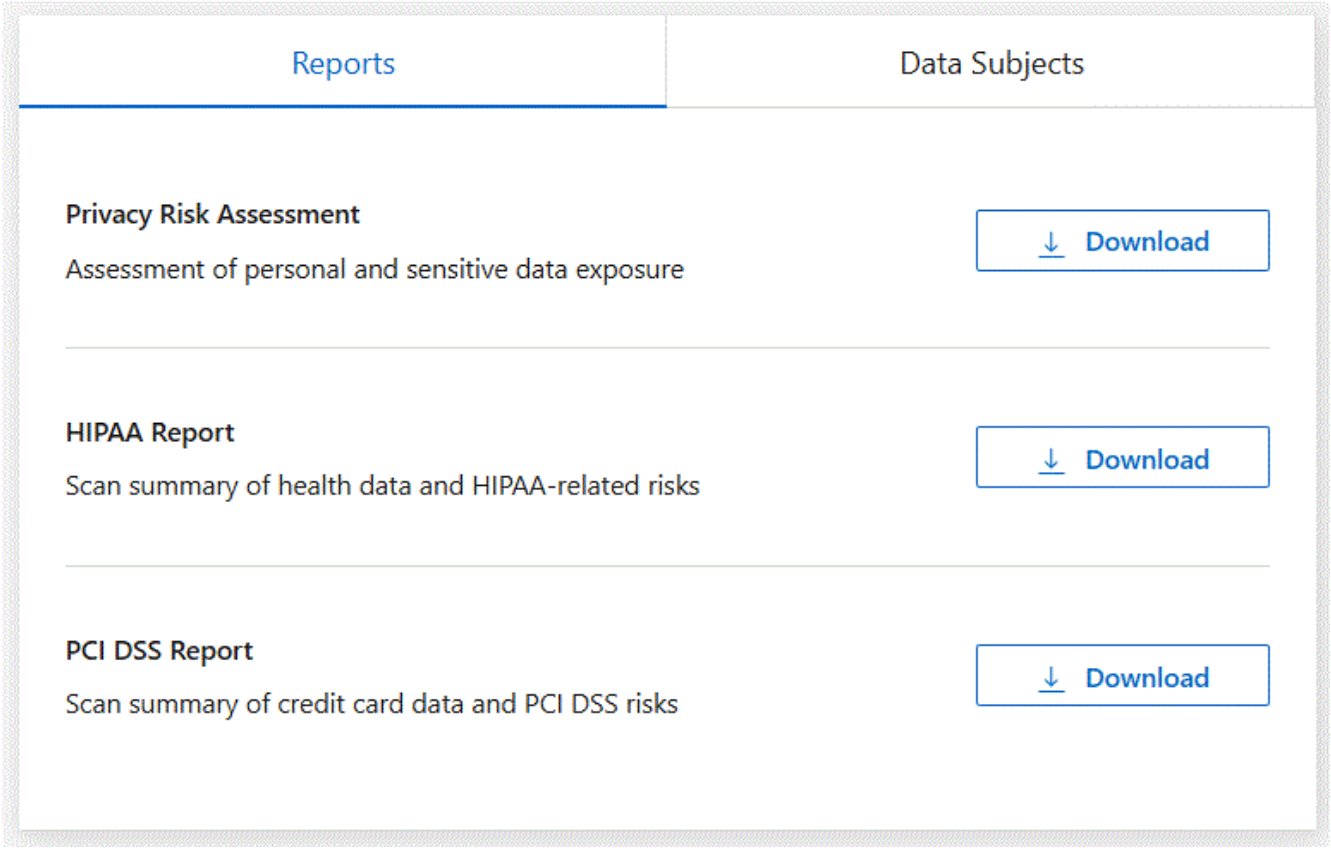
- Cifrado: el porcentaje de archivos que contienen información de tarjetas de crédito que se encuentran en sistemas cifrados o no cifrados. Esta información es específica de Cloud Volumes ONTAP.
- Protección contra ransomware: el porcentaje de archivos que contienen información de tarjetas de crédito que se encuentran en sistemas que tienen o no habilitada la protección contra ransomware. Esta información es específica de Cloud Volumes ONTAP.
- Retención: El período de tiempo en el que se modificaron los archivos por última vez. Esto es útil porque no debe conservar la información de la tarjeta de crédito durante más tiempo del necesario para procesarla.
- Distribución de información de tarjetas de crédito: los sistemas donde se encontró la información de la tarjeta de crédito y si el cifrado y la protección contra ransomware están habilitados.

### Generar el informe PCI DSS

Vaya a la pestaña Cumplimiento para generar el informe.

**Pasos**

1. En el menú Clasificación de datos, seleccione **Cumplimiento**.
2. Localice el **panel Informes**. Seleccione el icono de descarga junto a **Informe PCI DSS**.




**Resultado**

La clasificación de datos genera un informe en PDF que puede revisar y enviar a otros grupos según sea necesario.

## Informe de evaluación de riesgos de privacidad

El Informe de evaluación de riesgos de privacidad proporciona una descripción general del estado de riesgo de privacidad de su organización, según lo exigen las regulaciones de privacidad como GDPR y CCPA.

El informe incluye la siguiente información:

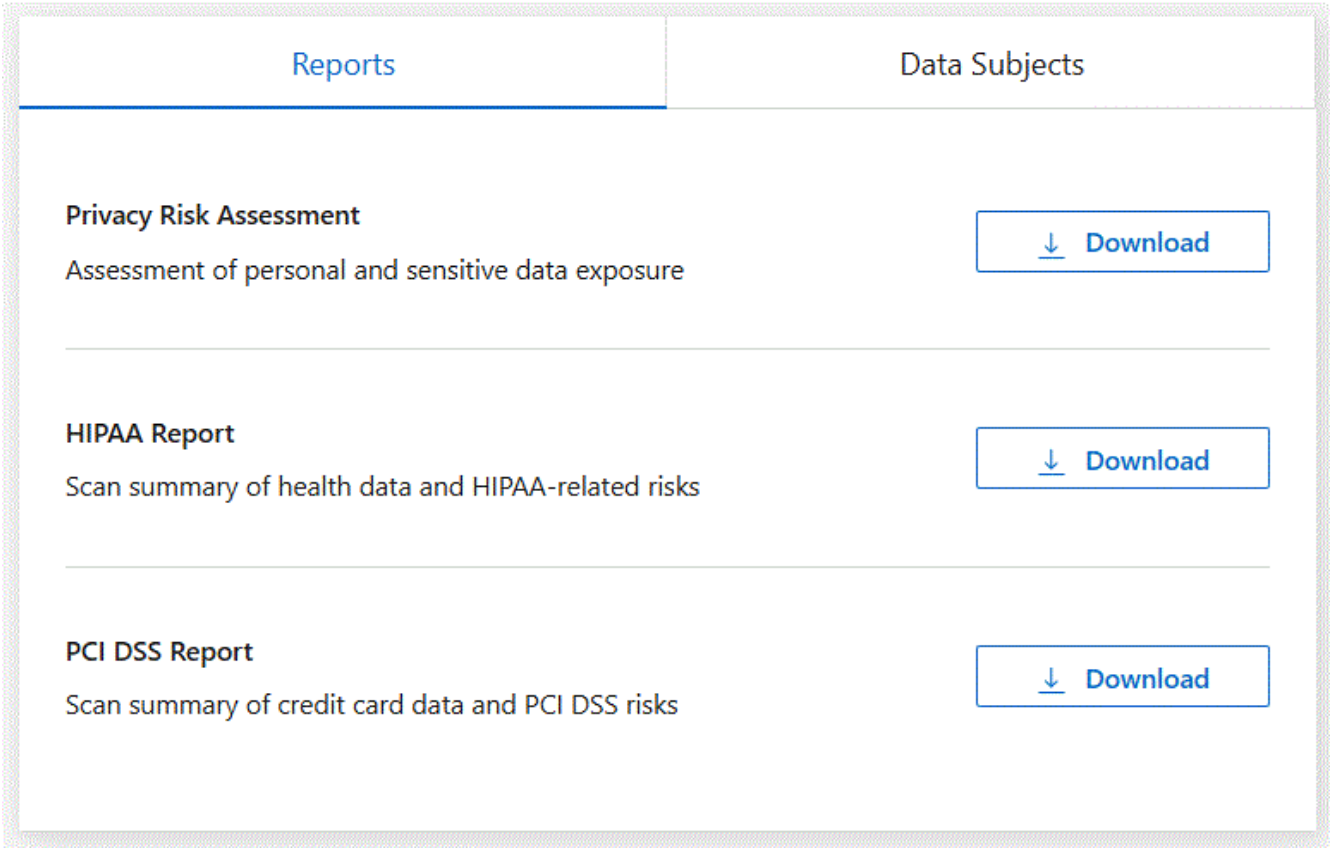
- Estado de cumplimiento: una puntuación de gravedad y la distribución de datos, ya sean no confidenciales, personales o personales confidenciales.
- Descripción general de la evaluación: un desglose de los tipos de datos personales encontrados, así como las categorías de datos.
- Sujetos de datos en esta evaluación: El número de personas, por ubicación, para las que se encontraron identificadores nacionales.

### Generar el Informe de Evaluación de Riesgos de Privacidad

Vaya a la pestaña Cumplimiento para generar el informe.

**Pasos**

1. En el menú Clasificación de datos, seleccione **Cumplimiento**.
2. Localice el **panel Informes**. Seleccione el icono de descarga junto a **Informe de evaluación de riesgos de privacidad**.




**Resultado**

La clasificación de datos genera un informe en PDF que puede revisar y enviar a otros grupos según sea necesario.

**Puntuación de gravedad**

La clasificación de datos calcula la puntuación de gravedad del Informe de evaluación de riesgos de privacidad basándose en tres variables:

- El porcentaje de datos personales sobre todos los datos.
- El porcentaje de datos personales sensibles sobre todos los datos.
- El porcentaje de archivos que incluyen interesados, determinado por identificadores nacionales como documentos de identidad nacionales, números de seguridad social y números de identificación fiscal.

La lógica utilizada para determinar la puntuación es la siguiente:

| Puntuación de gravedad | Lógica |
|---|---|
| 0 | Las tres variables son exactamente 0%. |
| 1 | Una de las variables es mayor que 0% |
| 2 | Una de las variables es mayor al 3% |
| 3 | Dos de las variables son mayores al 3% |
| 4 | Tres de las variables son mayores que 3% |
| 5 | Una de las variables es mayor al 6% |
| 6 | Dos de las variables son mayores al 6% |
| 7 | Tres de las variables son mayores al 6% |
| 8 | Una de las variables es mayor al 15% |
| 9 | Dos de las variables son mayores al 15% |
| 10 | Tres de las variables son mayores al 15% |

# Supervisar el estado de la NetApp Data Classification

El panel de control del estado de NetApp Data Classification proporciona supervisión en tiempo real e información sobre el rendimiento. El Monitor de salud captura información sobre su infraestructura de clasificación de datos, el estado del sistema, las métricas de uso y los datos de utilización, lo que le permite identificar y solucionar problemas.

## Información sobre el Monitor de Salud

El panel de control del Monitor de salud presenta información en cuatro categorías.

- **Estado de la infraestructura**

  Ver información, incluido el estado de la versión, la estabilidad del sistema, el tipo de implementación y la escala de la máquina.

- **Contenedores problemáticos**

  Revise el campo de contenedores problemáticos para obtener información sobre los contenedores que se detienen o se reinician con frecuencia. Utilice esta información para investigar los contenedores

específicos.

- **Información del sistema**

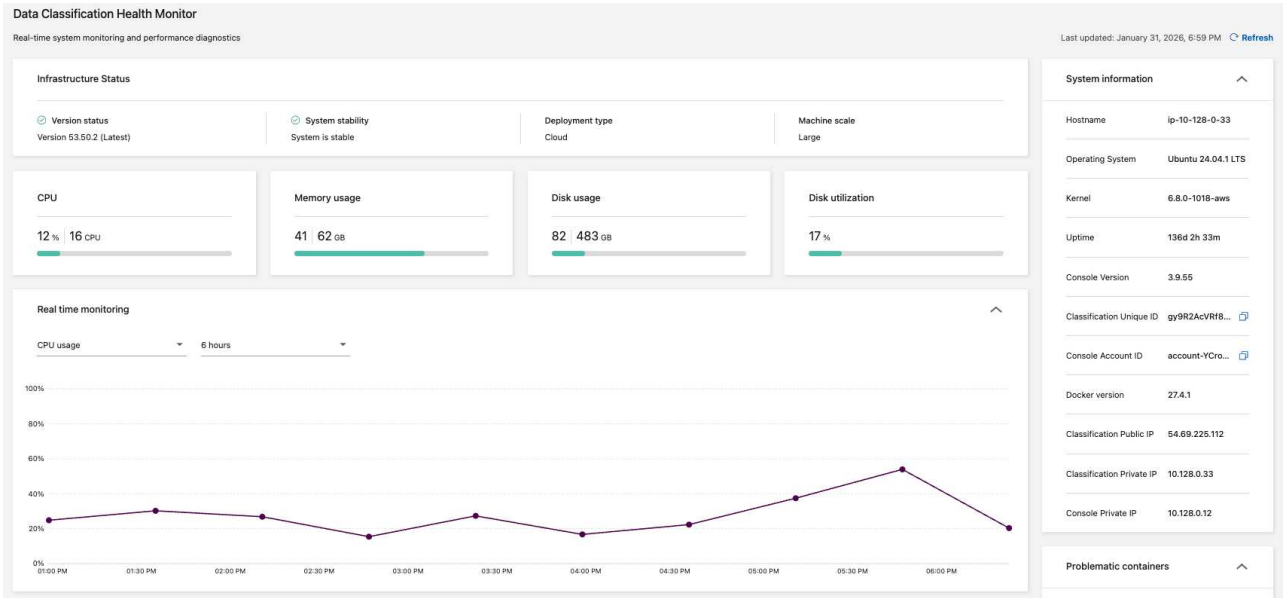
  El panel de información del sistema captura información crítica sobre la NetApp Console y la clasificación de datos, como las direcciones IP públicas y privadas, el nombre del host, el sistema operativo, la versión de la consola y el ID de la consola.

- **Uso y utilización**

  Revise el uso de la CPU, el uso del disco, el uso del disco y el uso de la memoria. Estos valores se muestran en unidades de almacenamiento (GB) o porcentajes del uso total. Si algún campo muestra una advertencia, selecciónela para obtener información y recomendaciones de solución.

## Acceda al panel de control del Monitor de salud

1. En Clasificación de datos, seleccione **Configuración**.
2. En el encabezado **Configuración**, seleccione **Monitor de estado de clasificación de datos**.
3. En el panel de control del Monitor de salud, puedes:
   - Revisar el uso y utilización. Si alguna métrica de uso o utilización muestra advertencias, seleccione la advertencia para obtener recomendaciones para resolver el problema.
   - Alterne el gráfico para mostrar el uso de la CPU, el uso del disco, el uso del disco y el uso de la memoria. Puede cambiar el eje x para mostrar el contenido en horas (6, 12 o 24) o días (2, 7 o 14).
   - Actualice el panel para ver las métricas de datos más recientes.



## Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

## Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.