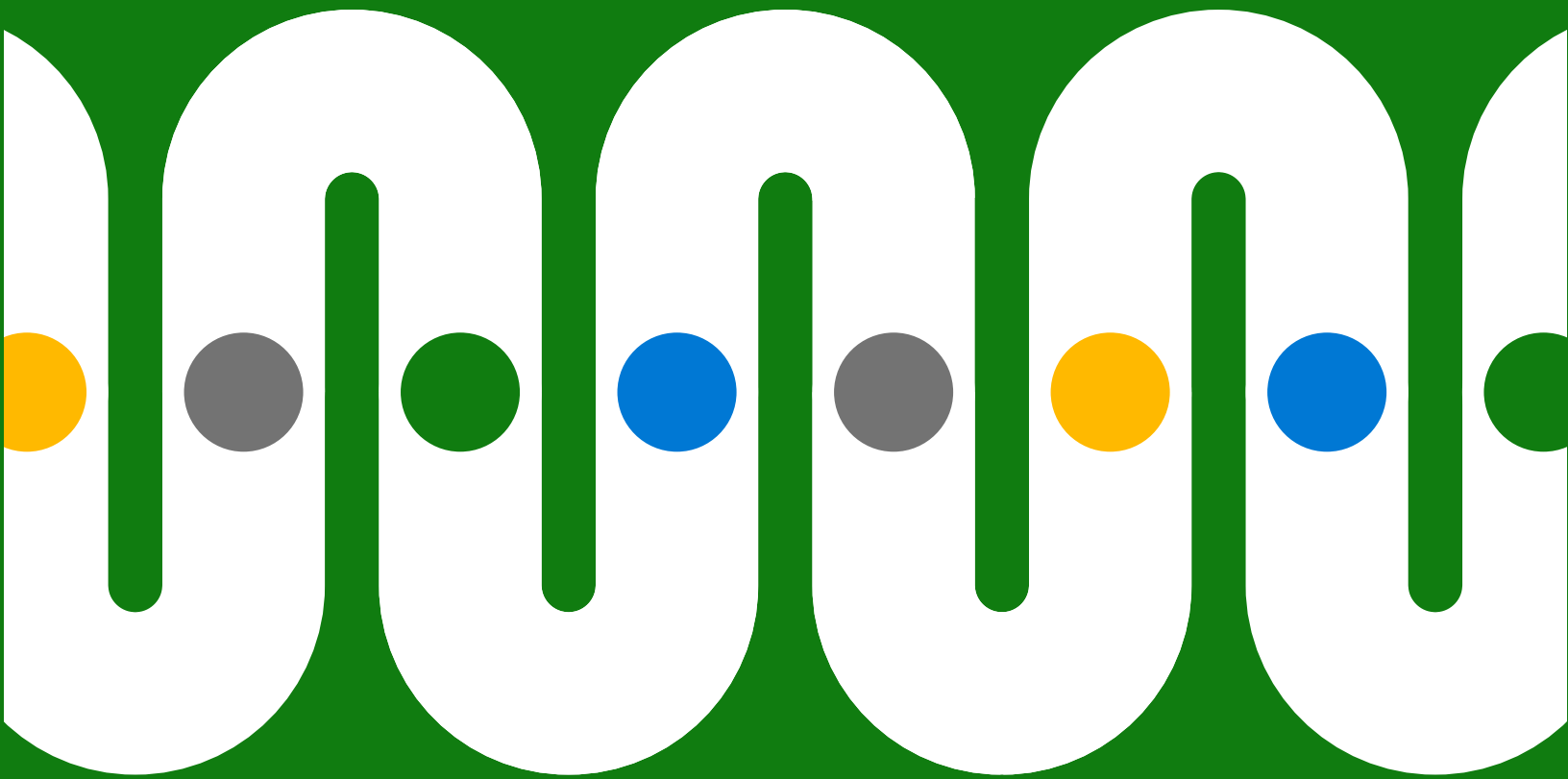
Microsoft Security

Tres pasos para proteger los datos de principio a fin



Índice

Una encuesta a los responsables de la toma de decisiones de cumplimiento constata que al 95 % le preocupa los desafíos de protección de datos.[2]

Introducción

El trabajo híbrido ha supuesto para las organizaciones un increíble aumento de su huella digital, que se extiende mucho más allá de la oficina tradicional.

Eso ha producido una mayor fragmentación y filtración de los datos, todo ello agravado por un rápido crecimiento de multitud de aplicaciones, dispositivos y ubicaciones. Muchos empleados también han cambiado de puesto en busca de una mayor realización profesional o flexibilidad, lo que constituye un nuevo desafío que crea nuevos puntos ciegos en el patrimonio de datos en continuo crecimiento.[1]

Todos estos factores han hecho que los directores de informática y de seguridad de la información se replanteen su enfoque de protección de la información. En una encuesta de seguimiento realizada a más de 500 responsables de la toma de decisiones de cumplimiento de EE. UU., a casi todos (el 95 %) les preocupaban los desafíos de protección de los datos.[2]

[1] "Cómo Microsoft puede ayudar a reducir los riesgos internos durante la Gran Renuncia", Alym Rayani, Seguridad de Microsoft 28 de febrero de 2022.

[2] "Encuesta de septiembre de 2021 a 512 responsables de la toma de decisiones de cumplimiento de EE. UU. encargada por Microsoft a Vital Findings".

Los equipos de TI y de seguridad buscan mejores formas de administrar el ciclo de vida completo de los datos en entornos multicloud, de cloud híbrido y on-premises. Este enfoque integral implica tres pasos clave:

Paso 1: Identificar los datos

Determina dónde residen tus datos, qué tipo de datos son y cómo se utilizan o comparten

Paso 2: Clasificar los datos

Clasifica y etiqueta los datos para saber las políticas y los procesos de mitigación de riesgos correctos que deben aplicarse

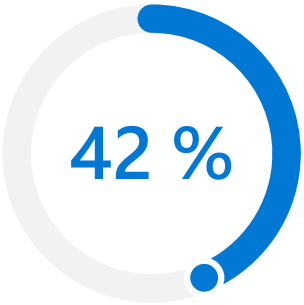
Paso 3: Prevenir la pérdida de datos

Busca un equilibrio entre la reducción de riesgos y la flexibilidad para tus empleados con detección y control inteligentes

¿Cuál es el objetivo de este enfoque? Cerrar las brechas y minimizar el riesgo sin sacrificar la productividad.

Paso 1

Identificar los datos



Cuando se les preguntó cuántos de sus datos "permanecen en la oscuridad", el 42 % de las organizaciones afirmó que al menos la mitad.[3]

Estos datos "ocultos" pueden ser de muchas formas, desde archivos adjuntos de correo electrónico y registros de llamadas de clientes hasta registros de máquinas e imágenes de vídeo.

Si no puedes identificar tus datos —dónde residen, de qué tipo son y cómo se usan o comparten— es imposible aplicar las políticas o protecciones correctas.

Las organizaciones modernas generan continuamente grandes cantidades de datos. No son solo documentos, correos electrónicos y mensajes, sino todo, desde imágenes de seguridad hasta datos de geolocalización, a lo que se suma la proliferación de aplicaciones, dispositivos y almacenamiento, on-premises y en el cloud.

Identificar todos estos datos puede ser difícil y el 42 % de las organizaciones afirma que al menos la mitad de sus datos "permanecen en la oscuridad"[3], es decir, es información recopilada pero desconocida o no utilizada para fines empresariales. A veces los datos se vuelven oscuros cuando el empleado que los creó cambia de proyecto o de función; a menudo, simplemente no hay ningún sistema para identificar los datos en el momento de su creación o modificación.

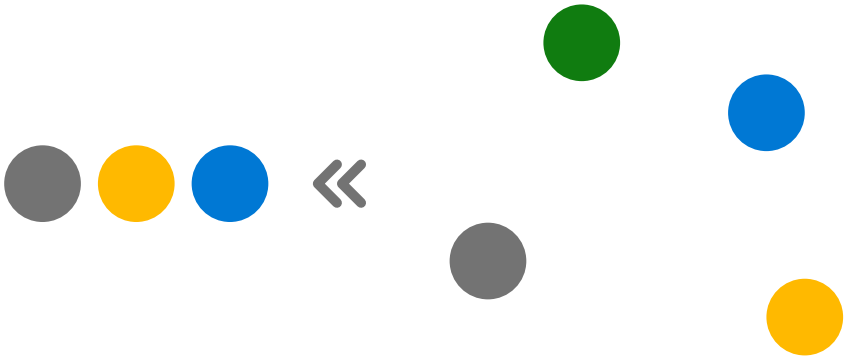
[3] "2022 State of Data Governance and Empowerment Report", Enterprise Strategy Group. Julio de 2022.

¿Quieres crear un flujo de trabajo de detección completo en una plataforma?

Obtén más información sobre la detección de datos de Microsoft Purview en **Microsoft.com**.

Este desafío será cada vez mayor. Se espera que la cantidad de nuevos datos que se crean, capturan, replican y consumen se dupliquen con creces en 2026 y que los datos empresariales crezcan más del doble que los datos de los consumidores.[4]

La inteligencia artificial (IA) y el machine learning (ML) pueden ayudar mediante el reconocimiento de los datos confidenciales (como direcciones de correo electrónico, datos sanitarios, números de tarjetas de crédito o propiedad intelectual) y su clasificación automática. La IA y el ML también pueden mejorar la precisión de la clasificación y revisar los datos de forma retroactiva. Estos procesos de identificación pueden abarcar todo tu patrimonio de datos, conservando, recopilando, analizando, revisando y exportando contenido dondequiera que este resida y en cualquier cloud.



[4] "Worldwide IDC Global DataSphere Forecast, 2022–2026: Enterprise Organizations Driving Most of the Data Growth", John Rydning, IDC. Mayo de 2022.

Paso 2

Clasificar los datos

Tanto las clasificaciones como las políticas deben seguir a los datos conforme viajan.

Por ejemplo, si un empleado copia números de tarjetas de crédito de un documento de Microsoft Word a Excel, la clasificación y las políticas deben aplicarse automáticamente a ambos documentos.

¿Quieres administrar y proteger mejor los datos confidenciales en tu entorno?

Obtén más información sobre la clasificación y protección de datos de Microsoft Purview en **Microsoft.com**.

Una clasificación adecuada de los datos te ayuda a determinar las políticas y los procesos de mitigación de riesgos correctos para garantizar que no se utilicen incorrectamente o se acceda a ellos de forma accidental o intencionada sin autorización. El cifrado y las marcas de agua pueden proteger aún más los datos, tanto si están en reposo como si se encuentran en tránsito o en uso.

Pero la clasificación y las políticas deben seguir a los datos conforme viajan por la organización. El etiquetado y las políticas de protección no se pueden limitar a documentos discretos; deben abarcar todo el patrimonio digital, desde los repositorios on-premises hasta los basados en el cloud y desde el software como servicio (SaaS) hasta las aplicaciones nativas del sistema operativo.

Los enfoques tradicionales de clasificación implican un trabajo manual considerable para clasificar todos estos datos, lo que entraña el riesgo de cometer errores o de pasar por alto los datos críticos sin querer. Los clasificadores integrados y entrenables pueden ayudar a automatizar este proceso, y una solución integrada permite a los administradores gestionar las políticas de forma centralizada en todos los sistemas.

Paso 3

Prevenir la pérdida de datos

Las políticas de DLP pueden evitar acciones que infrinjan las normativas.

Por ejemplo, si un empleado intenta descargar una hoja de cálculo con números de tarjeta de crédito en una unidad flash o cargarla en el almacenamiento en el cloud, la política de DLP podría identificar la actividad como infractora y evitarla.

¿Quieres funciones inteligentes de detección y control de la información confidencial?

Obtén más información sobre la prevención de pérdida de datos de Microsoft Purview en **Microsoft.com**.

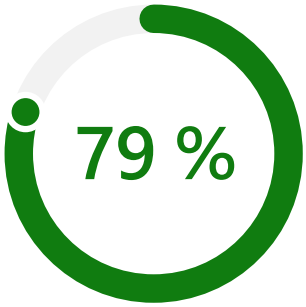
Una vez que hayas identificado y clasificado los datos, las soluciones de prevención de pérdida de datos (DLP) pueden aplicar políticas de protección integrales que mitiguen las amenazas como los datos oscuros y la filtración de datos, de modo que los empleados actuales y los exempleados no compartan, expongan o transfieran datos confidenciales de forma intencionada o involuntaria sin autorización.

Las soluciones de DLP inteligentes utilizan el contexto para encontrar un equilibrio entre proporcionar flexibilidad y bloquear acciones de alto riesgo. Por ejemplo, una persona puede continuar con una acción una vez que haya sido advertido de los riesgos potenciales y las políticas aplicables. Esto puede ayudar a proteger los datos confidenciales mientras se forma a los usuarios para que conozcan mejor los riesgos.

Las soluciones DLP ayudan a proteger la propiedad intelectual y otros datos empresariales críticos, además de mejorar el cumplimiento con normativas como el Reglamento General de Protección de Datos (GDPR), la Ley de Portabilidad y Responsabilidad de la Información Sanitaria (HIPAA) y la Ley de Privacidad del Consumidor de California (CCPA).

Un enfoque integral de DLP aplica las políticas sistemáticamente en toda la organización, lo que protege los “eslabones más débiles” del ciclo de vida de los datos.

No acumules soluciones de protección de datos. Intégralas.



Una encuesta a los responsables de la toma de decisiones de cumplimiento mostró que el 79 % había comprado varios productos de cumplimiento y protección de datos.

La mayoría había comprado tres o más.[5]

Muchas organizaciones han probado el enfoque de ir acumulando soluciones para la protección de la información, es decir, usar varias soluciones para administrar partes discretas del ciclo de vida de los datos. Pero esto obliga a los equipos de seguridad, gestión de los datos, de cumplimiento y jurídico a unir los retazos, lo que a menudo es ineficaz y ejerce presión en los recursos.

Un enfoque "integrado" puede cerrar las brechas, reuniendo la identificación de datos, la clasificación de datos y la DLP. Con una solución integrada, es más fácil administrar y hacer cumplir las políticas de forma centralizada. También reduce el tiempo de formación de los usuarios, quienes reciben las notificaciones de políticas en una manera que les resulta familiar y de forma nativa dentro de las aplicaciones.

[5] "Encuesta de febrero de 2022 a 200 responsables de la toma de decisiones de cumplimiento de EE. UU. (n=100 599-999 empleados, n=100 +1000 empleados) encargada por Microsoft a MDC Research".

Una solución integrada: Microsoft Purview

Microsoft Purview te ayuda a hacer frente a los desafíos del lugar de trabajo descentralizado y repleto de datos de hoy en día, con un conjunto completo de soluciones que te ayudan a controlar, proteger y administrar todo tu patrimonio de datos.

No te conformes con el gobierno.

Obtén más información sobre cómo proteger tus datos con Microsoft Purview >

¿Te interesa un área específica de protección de datos? Obtén información más detallada sobre cómo Microsoft Purview puede ayudarte con:

Detección de datos >

Clasificación y protección de datos >

Prevención de pérdida de datos >

Microsoft Security