safetica

Tu guía para una estrategia DLP integral: procesos, herramientas y proveedores

2026

Tabla de contenidos

EL CAMBIO EN EL PANORAMA DE DLP 4

Proveedores, SaaS y el amplio ecosistema de terceros 4

Código open source e IDEs 5

Políticas de trabajo remoto e híbrido 5

LA VISIBILIDAD ES DIFÍCIL EN UN ENTORNO DE DATOS DISPERSO 6

LA CONSOLIDACIÓN DE LA SEGURIDAD DE DATOS ES UN DESAFÍO EN SÍ MISMA 8

GESTIÓN DEL RIESGO INTERNO 8

QUÉ PRIORIZAR PARA UN DLP EFECTIVO: GUÍA DE PROCESOS 9

Comienza con la visibilidad 9

Implementar una supervisión efectiva 10

Priorizar la consolidación y una arquitectura de datos simplificada 10

No sobrecargues a tu equipo 11

Introducción a las herramientas DLP 11

Herramientas de descubrimiento y clasificación 12

MDM (gestión de dispositivos móviles) 12

Gestión del Riesgo Interno (IRM) 13

DÓNDE LOS PROVEEDORES PUEDEN AYUDAR CON DLP 14

@2026 Safetica Technologies Inc. | Proprietary and Confidential

Tu guía para una estrategia DLP integral: procesos, herramientas y proveedores

La Prevención de Pérdida de Datos (DLP, por sus siglas en inglés) existe desde principios de los años 2000, impulsada por diversas startups que se enfocaban principalmente en controles basados en la red para bloquear filtraciones en el perímetro.

Muchos de los primeros adoptantes implementaron DLP como un elemento fundamental de su postura de ciberseguridad, a menudo junto con firewalls y sistemas de detección de intrusiones, para aplicar políticas sobre los datos en tránsito.

Lamentablemente, la actitud hacia DLP ha cambiado desde aquellos primeros días. Regulaciones como el RGPD en 2018 y la CCPA en 2020 exigieron una gestión de datos más estricta, lo que llevó a las organizaciones a utilizar DLP para auditorías e informes en lugar de una prevención pura de amenazas. Las multas por incumplimiento eran severas e implacables.

Sin embargo, cuando el cumplimiento normativo se vuelve más importante que la gestión del riesgo, las prioridades **se desalinean**. Este panorama ha provocado que DLP se convierta, en gran medida, en un simple ejercicio de verificación por motivos de cumplimiento.

Otro problema es que las primeras formas de DLP, que dependían en gran medida de reglas estáticas y de datos en reposo, simplemente no eran adecuadas para afrontar las nuevas realidades empresariales. Los profesionales de seguridad quedaron atrapados en un dilema: implementaban las mejores soluciones disponibles en ese momento, pero aun así recibían multas por brechas de datos porque la tecnología DLP todavía no era lo suficientemente avanzada.

En la actualidad, es posible gestionar el riesgo y mantener el cumplimiento normativo cuando se utiliza el sistema adecuado. DLP ha cambiado significativamente a lo largo de los años, y las organizaciones deberían reevaluar sus necesidades de DLP, así como cómo debería ser una solución DLP moderna. El truco está en utilizar un sistema que haya sido diseñado desde cero teniendo en cuenta ambas necesidades.

El DLP moderno incorpora analítica de comportamiento para detectar anomalías, a diferencia de los sistemas heredados basados en reglas que suelen generar una alta tasa de falsos positivos.

Los volúmenes globales de datos han alcanzado niveles asombrosos y seguirán creciendo a medida que el mundo dependa cada vez más de los datos digitales. Todo, desde contratos hasta documentación, se está trasladando a Internet, lo que incrementa significativamente el riesgo potencial de pérdida de datos.

Los líderes de seguridad deben evaluar las implementaciones actuales frente a estas evoluciones para cerrar brechas de protección. Esto incluye mapear sus ecosistemas de datos, identificar puntos de exposición, realizar evaluaciones de riesgo que prioricen activos de alto valor, incorporar el comportamiento del usuario en la aplicación de políticas e integrar todo en un único sistema que supervise constantemente los datos en reposo y en tránsito.

Si suena como mucho trabajo, lo es. Pero también es posible con una solución DLP moderna e integral.

Prepararse para esta nueva realidad requiere comprender cómo es el nuevo panorama de riesgos, qué herramientas y procesos debería considerar una organización y cómo abordar a los proveedores.

Considera el hecho de que **el 70% de la pérdida de datos ocurre en el endpoint**, lo que da una pista de dónde debería concentrarse la mayor parte de las medidas de protección. Sin embargo, la respuesta simplista de “centrarse en los endpoints” no tiene en cuenta la naturaleza compleja del almacenamiento y la transferencia de datos. Aunque los datos se pierdan con mayor frecuencia en los endpoints, el compromiso que conduce a la pérdida de datos no comienza ni termina allí; a menudo se origina en otro lugar.

Este ejemplo deja claro por qué los profesionales de seguridad deben reevaluar sus prácticas actuales de DLP, al tiempo que seleccionan herramientas que proporcionen información contextual.

La protección basada en contexto requiere visibilidad en toda la red, aplicaciones en la nube y comportamiento de los usuarios, no solo en el endpoint. Esta guía abordará el nuevo panorama de DLP, cómo es un DLP efectivo y cómo convertirse en un comprador más informado cuando se trata de proveedores de DLP.

El cambio en el panorama de DLP

El alcance de dónde residen los datos de una organización ha aumentado drásticamente. El mayor uso de herramientas SaaS y de terceros que nunca antes hace que los datos graviten de forma natural hacia la nube. Esto ha provocado dispersión de datos y ROT (datos redundantes, obsoletos o triviales), lo que a menudo da como resultado que las organizaciones tengan demasiados datos en demasiados lugares.

Este problema se agrava en entornos híbridos, especialmente cuando los activos se trasladan continuamente de infraestructuras locales a la nube. Esta migración expone los datos a nuevos riesgos y, dado que los proveedores de la nube gestionan el almacenamiento pero las organizaciones conservan la responsabilidad de las configuraciones de seguridad, los proveedores de almacenamiento en la nube inseguros trasladan la mayor parte del riesgo a la organización.

Proveedores, SaaS y el amplio ecosistema de terceros

Las organizaciones han aumentado su dependencia de proveedores externos, y la empresa promedio utiliza **106 aplicaciones SaaS en 2024**. Las grandes empresas promedian 131 herramientas SaaS. Eso solo incluye herramientas SaaS, sin contar otros proveedores.

106
Número promedio de soluciones SaaS usadas das por empresa

131
Número promedio de soluciones SaaS utilizadas por empresa enterprise

Los proveedores a menudo pueden acceder a datos sensibles, creando posibles puntos de fuga si carecen de controles estrictos. Aunque los equipos suelen auditar el acceso de los proveedores, los estándares inconsistentes entre socios pueden complicar la

aplicación de políticas. Además, la adopción generalizada de SaaS y la implementación simplificada pueden hacer que los proveedores SaaS se incorporen en cuestión de días sin que el equipo de seguridad siquiera lo sepa o pueda evaluarlos adecuadamente.

Código open source e IDEs

Los entornos de desarrollo open source son otra área de riesgo. Los componentes de código abierto pueden contener vulnerabilidades conocidas y desconocidas. Cuando estos componentes se utilizan en sistemas de desarrollo o producción, los atacantes pueden explotarlos para obtener acceso no autorizado y potencialmente exfiltrar datos.

Un estudio exhaustivo de extensiones de VS Code descubrió que más de 2.000 extensiones (aproximadamente el **8,5% de todas las extensiones** analizadas) son propensas a la filtración de datos. Estos componentes open source son especialmente riesgosos porque, debido a su naturaleza, los actores maliciosos pueden desarrollar fácilmente kits de explotación o ataques dirigidos a ellos. Al identificar un componente ampliamente utilizado, los atacantes pueden afectar a miles de empresas a través de una sola vulnerabilidad.

Políticas de trabajo remoto e híbrido

Las políticas de trabajo remoto e híbrido han descentralizado el acceso a los datos. Los empleados acceden a los sistemas desde diversas ubicaciones y dispositivos, lo que incrementa el riesgo en los endpoints. Múltiples ubicaciones y fuerzas laborales globales también pueden fragmentar la gestión de datos, contribuyendo aún más a la dispersión de la información.

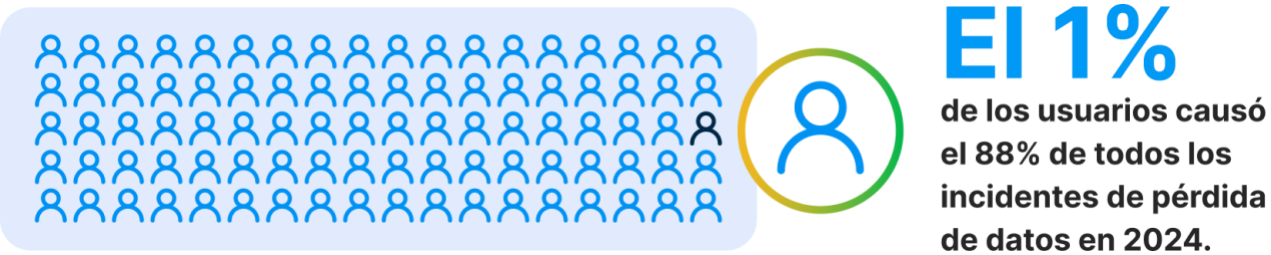
Una fuerza laboral ampliamente distribuida también puede ser una pesadilla para el cumplimiento normativo. Diferentes países tienen leyes distintas sobre dónde se pueden almacenar o procesar los datos, lo que genera complicaciones cuando se accede a los datos desde fuera de esas jurisdicciones.

Diferentes equipos pueden tener preferencias específicas por herramientas de colaboración, como el uso de WhatsApp en LATAM frente a Slack o Teams en EE. UU., lo que complica un proceso DLP estandarizado y la visibilidad general de los datos.

Estos factores hacen que DLP sea aún más difícil de lo que ya era, dando lugar a un panorama en el que **más del 50% de las empresas ha sufrido interrupciones del**

negocio debido a la pérdida de datos, mientras que solo el 35% considera que cuenta con un programa DLP “maduro”.

Por qué un DLP efectivo requiere visibilidad completa



El 88% de todos los eventos de pérdida de datos en 2024 fue causado por el 1% de los usuarios, lo que destaca lo imperativo que es proteger *cada* dispositivo y *cada* punto potencial de pérdida. Todo lo que necesita un infiltrado es un único punto débil para obtener suficiente acceso y causar un daño significativo.

La visibilidad es difícil en un entorno de datos disperso

Teniendo en cuenta el nuevo panorama de datos, decir que la visibilidad es un desafío difícil y complejo es quedarse corto. Los datos ahora residen en endpoints, aplicaciones SaaS, plataformas IaaS, herramientas de terceros, plataformas de colaboración, dispositivos personales, múltiples dispositivos propiedad de empleados, dispositivos IoT y almacenamiento en la nube.

Las herramientas tradicionales de visibilidad basadas en el perímetro no pueden rastrear ni aplicar políticas de forma coherente en todas estas capas, y los empleados pueden usar servicios no autorizados para compartir archivos o facilitar su trabajo, a menudo sin que TI lo sepa.

Los datos estadísticos relacionados con la falta de visibilidad de una organización son reveladores.

Los departamentos de seguridad no fueron diseñados originalmente para rastrear datos en los tipos de entornos en los que operan hoy en día y han tenido dificultades para adaptarse a esta nueva normalidad. La visibilidad se deteriora porque las herramientas no están integradas, los datos no tienen límites claros y la mayoría de las clasificaciones son superficiales. Lo que suele considerarse “clasificación” a menudo se limita a la coincidencia de palabras clave o a etiquetar un archivo como “confidencial” una sola vez, asumiendo que seguirá siéndolo incluso cuando se copie o se comparta.

Incluso con una excelente clasificación, aplicar una higiene de datos sólida puede ser complicado. En muchas organizaciones, la propia capa de datos está fragmentada y desvinculada de los sistemas destinados a observarla. Hasta que los profesionales de seguridad replanteen dónde y cómo instrumentan el uso de los datos, la visibilidad integral seguirá fallando.

@2026 Safetica Technologies Inc. | Proprietary and Confidential

La consolidación de la seguridad de datos es un desafío en sí misma

DLP solo es efectivo si cubre todos los datos de una organización, lo cual puede ser un reto cuando el almacenamiento está fragmentado, lo que conduce a una protección incompleta.

Las empresas modernas sufren dispersión de datos debido a los problemas descritos anteriormente, con activos de datos cada vez más distribuidos en numerosos sistemas y ubicaciones de almacenamiento. Las soluciones DLP tradicionales fueron diseñadas para infraestructuras más antiguas y simples, como servidores locales, endpoints gestionados y redes corporativas. A medida que el trabajo se ha trasladado a aplicaciones SaaS, almacenamiento en la nube, herramientas basadas en navegador, nubes híbridas y trabajo remoto, esos supuestos heredados ya no se sostienen.

Como resultado, gran parte de los datos sensibles de una empresa ahora residen o se mueven a través de canales que el DLP tradicional no puede supervisar. Por ejemplo, los empleados pueden usar aplicaciones SaaS o herramientas web para editar, cargar o compartir archivos sensibles. Las soluciones DLP heredadas ubicadas únicamente en los límites del endpoint a menudo pasan por alto estos canales por completo.

Esta fragmentación crea puntos ciegos donde pueden producirse fugas de datos fuera del alcance de la cobertura tradicional de DLP, lo que da lugar a implementaciones parciales, como solo en endpoints o sistemas locales. No es de extrañar que esto resulte en una protección incompleta, lo que obliga a los líderes de seguridad a buscar soluciones más integrales, si es que logran identificar estas limitaciones en primer lugar.

Gestión del riesgo interno

La gestión del riesgo interno (IRM, por sus siglas en inglés) es una extensión crítica de cualquier estrategia DLP integral. A diferencia de las amenazas externas, los riesgos internos provienen de personas que ya tienen acceso a sistemas internos o credenciales. Esto incluye empleados, contratistas y socios, ya sea que sus acciones sean intencionales o resultado de negligencia.

Los factores humanos dominan los eventos de pérdida de datos. Según el Informe de Investigaciones de Brechas de Datos de Verizon 2024, **el 68% de las brechas de datos**

involucran un elemento humano no malicioso, como caer en una estafa de ingeniería social.

La IRM es una extensión necesaria del alcance de DLP. Un DLP sin conciencia del riesgo interno no tiene en cuenta las causas más comunes de exposición de datos. Las estrategias DLP integrales deben incluir herramientas y procesos capaces de identificar y responder rápidamente al riesgo interno.

Qué priorizar para un DLP efectivo: Guía de procesos

Un DLP efectivo comienza con la priorización; de lo contrario, los esfuerzos serán demasiado amplios y diluidos.

> "Las organizaciones suelen imaginar que proteger los datos mediante soluciones DLP es solo cuestión de configurar una herramienta y todo estará bien," afirma Ján Lakatoš, Director de Producto en Safetica. "En realidad, implica integrar un proceso de seguridad completamente nuevo en su entorno de trabajo y encontrar un equilibrio entre una seguridad estricta y la habilitación del negocio. Alcanzar ese equilibrio es casi imposible porque intervienen demasiadas variables."

Comienza con la visibilidad

La visibilidad es la base de cualquier estrategia DLP eficaz. Sin ella, las organizaciones no pueden descubrir dónde residen los datos sensibles, cómo se mueven ni quién interactúa con ellos.

Una visibilidad efectiva requiere un descubrimiento continuo de datos en todos los entornos. También debe estar basada en la identidad, vinculando el acceso a los datos con usuarios y dispositivos específicos. Esto es esencial tanto para la aplicación de políticas en tiempo real como para la investigación posterior a incidentes.

Ningún sistema DLP puede aplicar controles o detectar usos indebidos sin saber primero qué datos existen y cómo están almacenados.

@2026 Safetica Technologies Inc. | Proprietary and Confidential

Implementar una supervisión efectiva

Una vez establecida la visibilidad, la supervisión permite a la organización rastrear el acceso y el movimiento de los datos en tiempo real. Sin supervisión, la visibilidad sigue siendo pasiva, lo que puede ser útil para auditorías, pero no para la prevención o detección de incidentes.

Una supervisión efectiva captura tanto dónde se encuentran los datos como cómo se comportan. Determina *quién* accedió a ellos, *qué* acciones realizó y si esas acciones se alinean con la política de la empresa. Idealmente, la supervisión debería extenderse a herramientas autorizadas y no autorizadas, incluidas herramientas basadas en navegador y plataformas SaaS.

La supervisión debe ser contextual, porque registrar simplemente que un archivo fue accedido no es suficiente. El sistema debe capturar quién accedió, desde dónde, en qué dispositivo y si fue compartido o exfiltrado. Este contexto es crítico para la detección de riesgos, ya que es la única forma de alimentar herramientas DLP más sofisticadas capaces de detectar indicadores de compromiso o ataques de riesgo interno mediante patrones de comportamiento anómalos, en lugar de reglas o firmas basadas en usuarios.

Sin una supervisión continua y multinivel, los controles DLP no pueden responder a amenazas reales ni aplicar políticas de forma dinámica.

Priorizar la consolidación y una arquitectura de datos simplificada

Los entornos fragmentados crean puntos ciegos y ralentizan los tiempos de respuesta, lo que hace necesaria la consolidación. Una arquitectura de datos unificada proporciona visibilidad clara de todas las interacciones con los datos. Esta claridad mejora la precisión de detección y reduce el número de posibles puntos de fallo.

Tener múltiples reglas en distintas plataformas para la clasificación de datos o políticas de retención, o políticas separadas basadas en bases de datos o entornos distintos, puede generar conflictos. La consolidación y estandarización garantizan que estas reglas se apliquen de manera uniforme y eliminan brechas de configuración.

Esto se traduce en una respuesta a incidentes más rápida, ya que solo existe un único lugar donde revisar los registros y ajustar los controles. La consolidación también debe incluir una auditoría que garantice que los datos no estén almacenados en bases de

datos públicas o inseguras y que no se hayan pasado por alto ubicaciones donde puedan residir los datos. Haz de la consolidación una prioridad reduciendo fuentes de datos dispersas en un único punto de información autorizado, para que las decisiones y acciones se tomen con rapidez y claridad.

No sobrecargues a tu equipo

La complejidad de los proveedores y el exceso de herramientas pueden aumentar significativamente las probabilidades de pérdida de datos. Las herramientas heredadas dificultan la implementación de un DLP efectivo, por lo que **el 78% de las organizaciones** tuvo dificultades con las herramientas DLP en 2024.

Esto no solo afecta a la organización, sino también al equipo. La falta de personal y las brechas de habilidades son generalizadas. Casi todos los CISOs informan que sus equipos están subdimensionados, y **el 90% de los profesionales de ciberseguridad** reporta brechas de habilidades en sus equipos. Sin embargo, muchos líderes de seguridad ven esta brecha y creen que la solución es añadir más herramientas.

Esto puede provocar agotamiento del equipo y un exceso de complejidad, lo que impacta negativamente en la efectividad. En su lugar, céntrate en la automatización para manejar tareas rutinarias y limita la proliferación de herramientas a integraciones esenciales. Esto aumenta la capacidad sin generar sobrecarga.

No añadas complejidad de herramientas a un equipo que ya está bajo presión.

Introducción a las herramientas DLP

Existen muchas herramientas DLP, y es responsabilidad del líder de ciberseguridad ser un comprador informado; de lo contrario, podrías adquirir una herramienta que no se adapte bien a tu empresa, a tu equipo de seguridad o a tu perfil de riesgo.

No todas las herramientas son iguales ni sirven a todas las empresas. Los líderes de seguridad deben buscar herramientas que faciliten la proactividad y se alineen con las prioridades identificadas como parte de su estrategia de seguridad DLP.

A continuación, proporcionamos una lista de los tipos de herramientas que te ayudarán a construir una pila tecnológica DLP efectiva.

Herramientas de descubrimiento y clasificación
Las herramientas de descubrimiento y clasificación escanean los datos de una organización, identifican dónde se almacena la información y la organizan en categorías significativas. Su propósito principal es hacer visibles los datos ocultos en todas las ubicaciones (nube, local, terceros) y etiquetarlos correctamente para aplicar la protección adecuada.

Estas herramientas analizan ordenadores, servidores, almacenamiento en la nube, sistemas de correo electrónico, carpetas compartidas y, en algunos casos, incluso archivos antiguos. Identifican registros de clientes, datos de pago, identidades personales, documentos internos y propiedad intelectual.

Una vez identificados, aplican etiquetas claras a los datos que permiten que las reglas de seguridad se apliquen automáticamente, como bloquear descargas o impedir el uso compartido externo.

MDM (gestión de dispositivos móviles)
Las herramientas de Gestión de Dispositivos Móviles (MDM) crean un entorno controlado para cualquier teléfono, tableta o incluso portátil que acceda a información empresarial.

Estas herramientas permiten a la organización establecer reglas sobre cómo se comportan los dispositivos, independientemente de dónde se encuentren. Esto es clave para la prevención de pérdida de datos, ya que el mayor riesgo de los dispositivos móviles es su movilidad: salen de la oficina, se conectan a redes inseguras, se pierden y almacenan archivos sensibles que pueden caer fácilmente en manos equivocadas.

Una solución MDM resuelve varios problemas a la vez, como:

- Asegurar que cada dispositivo tenga protección sólida en la pantalla de bloqueo.
- Separar el contenido personal del contenido laboral.
- Controlar qué aplicaciones pueden abrir o copiar documentos de trabajo.
- Rastrear dispositivos para recuperarlos o borrarlos.
- Permitir la eliminaci√≥n remota de datos corporativos.
- Proporcionar una vista centralizada de la actividad de los dispositivos y alertas tempranas de riesgo.

Gestión del Riesgo Interno (IRM)
Las herramientas de IRM se centran en prevenir la pérdida de datos causada por personas dentro de la organización, incluidos empleados, contratistas y cualquier persona con acceso legítimo a los sistemas.

Estas herramientas supervisan acciones que podrían conducir a la extracción o uso indebido de datos, como descargas inusualmente grandes, intentos de eludir restricciones, copias masivas de archivos, accesos fuera de horario o transferencias a ubicaciones no propiedad del empleador.

El comportamiento anómalo no siempre implica mala intención, pero el riesgo sigue existiendo. En el peor de los casos, una cuenta puede haber sido comprometida; en el mejor, los datos corporativos quedan fuera del alcance de visibilidad de la organización. El resultado no cambia: el riesgo de pérdida de datos y brecha de seguridad sigue presente.

Las amenazas internas no siempre son maliciosas; de hecho, a menudo no lo son. Sin embargo, la negligencia inocente o una mala higiene de seguridad no reducen la necesidad de abordar el riesgo interno.

La gestión del riesgo interno suele tratarse por separado de las herramientas de pérdida de datos porque se enfoca en el comportamiento humano más que en el movimiento de archivos o reglas de dispositivos. No obstante, debe considerarse junto con la prevención de pérdida de datos, ya que muchos incidentes ocurren incluso cuando existen controles tradicionales. Al complementar ambas disciplinas, se logra un entorno y una organización más seguros.

Dónde los proveedores pueden ayudar con DLP

Estos pasos deberían proporcionarte una base sólida para implementar una estrategia DLP moderna y efectiva.

> "Es importante entender cuáles son los objetivos y expectativas," afirma Miloš Blata, Director de Ingeniería de Ventas en Safetica. "¿Se trata de clasificación de datos, protección de datos, controles de perímetro seguros, descubrir dónde residen los datos en reposo, cumplir con regulaciones o estándares, saber qué está ocurriendo en general, registrar y gestionar eficazmente esa información (idealmente usando IA), una combinación de algunos de estos elementos o todo junto? Una vez aclarado este paso cero, gestionar una configuración DLP se vuelve mucho más sencillo"

Al evaluar proveedores, plantéate las siguientes preguntas:

- ¿El proveedor aborda una prioridad clave descrita aquí?
- ¿Aumenta la complejidad de la gestión o mejora la eficiencia y reduce la carga operativa?
- Considerando el alcance completo de tu estrategia DLP, ¿qué impacto real tiene este proveedor?
- ¿Ofrece DLP e IRM integrados en una sola plataforma o requerirá múltiples herramientas e integraciones?

Estas preguntas te ayudarán a identificar qué proveedores generarán mayor impacto en tu organización.

Al continuar desarrollando tu estrategia DLP, recuerda centrarte en los fundamentos. Una estrategia sólida cubre todos los aspectos de la protección de datos e incorpora los nuevos riesgos derivados de una huella digital amplia y de la evolución constante del riesgo interno. Con una base sólida, tu estrategia DLP podrá adaptarse a estos nuevos desafíos. Construye primero esa base y luego estarás listo para elegir las herramientas y el proveedor adecuados.