Acronis

DOCUMENTO TÉCNICO

# Lanzar y ampliar los servicios de DLP: guía para los MSP

Durante años, las empresas de todos los tamaños no han podido enfrentar los riesgos de filtración de datos, a pesar de haber mayor concienciación, protocolos de seguridad y normativas. De hecho, estos riesgos están en aumento: de acuerdo con el informe 2021 Year End Report: Data Breach QuickView de Risk Based Security, en 2021 se expusieron más de 22 mil millones de registros, lo que convierte a ese año en el segundo con mayor cantidad de datos confidenciales afectados, desde 2005. La inmensa mayoría de estos registros quedaron expuestos debido a la filtración de datos. Una filtración de datos se define como una infracción a la seguridad en la que se proporcionan datos confidenciales o protegidos de forma accidental o deliberada a un entorno no confiable o a usuarios no autorizados, ya sea fuera o dentro de la empresa.

# Entonces, ¿qué provoca la filtración de datos? Hay dos causas principales:

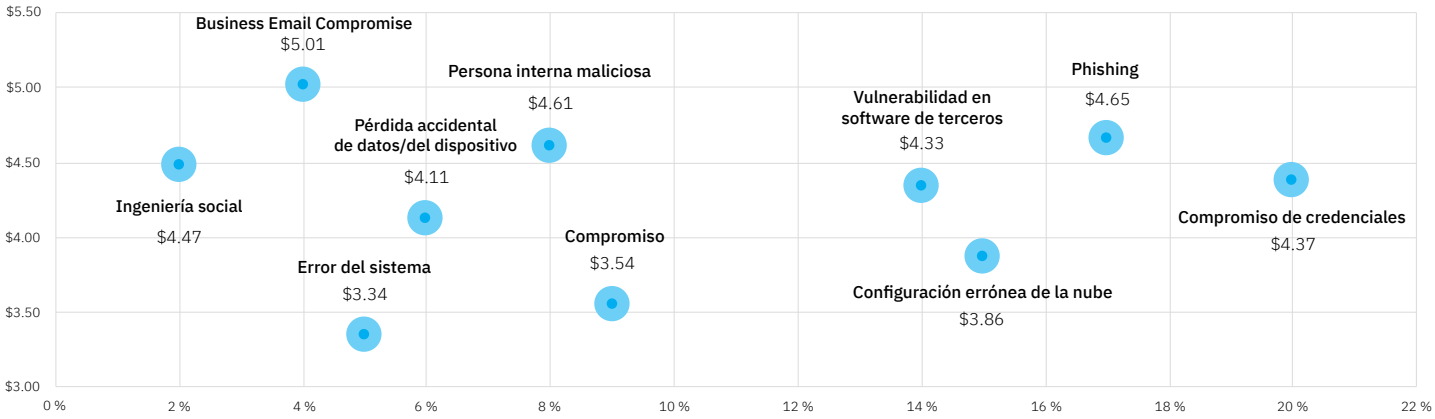
## 1. Ciberamenazas externas

Como se define en el marco MITRE ATT&CK, la filtración de datos está entre las últimas tácticas que los adversarios maliciosos realizan durante un ataque. El motivo de los actores en más del 80 % de los casos es el beneficio económico, de acuerdo con el informe Verizon 2022 Data Breach Investigation Report.

Por eso los datos confidenciales son el objetivo principal de la mayoría de los ataques. Una vez que los ciberdelincuentes establecen el acceso al entorno corporativo, pueden intentar extraer los datos a través de varios canales. A medida que los ataques crecen en complejidad y son cada vez más capaces de eludir las capas de seguridad, los riesgos para los datos de las empresas aumentan exponencialmente.

## 2. Riesgos internos

Aunque el antimalware y otras tecnologías de seguridad para endpoints pueden detectar y detener los ataques externos, otros riesgos para los datos de las empresas (relacionados con ataques internos) están cobrando fuerza. Un ejemplo común es el de los usuarios finales que, sin saberlo, proporcionan datos a partes no autorizadas (p. ej., al reenviar un correo electrónico). Esto puede ocurrir debido a errores accidentales de los empleados, a configuraciones incorrectas de TI o a través de personas internas maliciosas, todo lo cual puede representar una grave amenaza para las empresas, provocando las fugas de datos más costosas.




Es importante señalar que, aunque algunas empresas subestiman el impacto de los riesgos internos, el Informe sobre el costo de fugas de datos de 2021 del Ponemon Institute afirma claramente que alrededor de un tercio de las fugas de datos involucran a personas internas.

# ¿Cuál es el impacto de las filtraciones de datos en las empresas?

## La filtración de datos representa un riesgo grave para las empresas. La filtración de datos confidenciales a destinatarios no autorizados provoca:

- **Incumplimiento de las normativas**: el almacenamiento, el acceso y la protección de datos confidenciales, como la información de identificación personal (PII) de empleados y clientes, la información de salud protegida (PHI) o los datos de los titulares de tarjetas, están estrictamente regulados por normativas locales e internacionales, como el RGPD, la Ley de Privacidad del Consumidor de California (CCPA), la HIPAA, el PCI-DSS, etc. Algunas normativas, como el RGPD, incluso exigen que las fugas se informen dentro de un plazo estricto. En el caso de una demora en el informe de una fuga de datos regulada, las empresas pueden enfrentarse a cuantiosas multas e incluso pueden perder sus certificaciones de cumplimiento.
- **Daños financieros**: una vez que se filtran los datos, además de las multas normativas a las que podrían enfrentarse los clientes de los proveedores de servicios gestionados (MSP), los proveedores de servicios también podrían estar expuestos a la amenaza de sufrir daños financieros como consecuencia de la responsabilidad por la seguridad de los clientes, que podría derivar en litigios. Además, la filtración de secretos comerciales o propiedad intelectual podría causar pérdidas financieras adicionales a las empresas e incluso desestabilizar su posición en el mercado.
- **Riesgos reputacionales**: terminar en los titulares de las fugas de datos puede ser perjudicial para las empresas. Esto no solo podría generar una tasa de cancelación de sus clientes, sino que también podría afectar a alianzas existentes y a la capacidad de adquirir nuevos clientes. La filtración de datos de sus clientes también puede afectar su reputación y su negocio.

# ¿Qué es la prevención de pérdida de datos?

**La prevención de pérdida de datos** es una categoría de soluciones de seguridad establecida hace mucho tiempo, que representa sistemas de tecnologías integradas de seguridad de la información que detectan e impiden el uso, la transmisión y el almacenamiento no autorizados de datos confidenciales.

**Las soluciones de DLP** realizan esto aplicando una combinación de controles de flujo de datos y métodos de análisis de contenido. Dichas tecnologías aplican políticas de uso y manejo de datos aceptables para la empresa en toda la organización que impiden la filtración de datos confidenciales a destinatarios no autorizados (tanto internos como externos).

Aunque la protección de datos se asocia principalmente con las copias de seguridad y la recuperación ante desastres, existen otras tecnologías esenciales, como la DLP, la certificación y el cifrado, que protegen la información sensible contra una mayor variedad de amenazas, incluida la filtración de datos.

**La DLP es la única tecnología** capaz de proporcionar visibilidad y control de los datos confidenciales que fluyen y se almacenan en una empresa, para evitar su filtración a entidades no autorizadas.

## Estados de datos y cómo los protegen las diferentes DLP funcionales

Hay **tres estados principales** en los que pueden residir los datos dentro de una empresa:

- **Datos en uso:** datos que se están utilizando o transfiriendo en canales locales (p. ej., periféricos, almacenamiento extraíble) o a través de aplicaciones en computadoras endpoints. Un ejemplo de estos datos serían los archivos que se están transfiriendo desde un endpoint a una unidad USB.
- **Datos en movimiento:** este término se refiere a los datos que se mueven o se transfieren entre sistemas informáticos. Por ejemplo, los datos que se transfieren de un almacenamiento de archivos local a un almacenamiento en la nube, o los datos que se transfieren de una computadora endpoint a otro endpoint a través de mensajería instantánea o correo electrónico se consideran datos en movimiento.
- **Datos en reposo:** describe los datos que se almacenan localmente o en una red y a los que no se accede o los que no se transfieren actualmente. Un ejemplo de datos en reposo son los que se almacenan en recursos compartidos de red o en servidores locales.

Es importante señalar que los datos cambian de estado de forma frecuente y continua, aunque algunos datos pueden permanecer en un estado único durante todo el ciclo de vida de un endpoint. Comprender los diferentes estados de los datos, sus particularidades y diferencias puede ayudar a los clientes a manejar sus datos organizativos de forma más segura y protegerlos contra las filtraciones.

Respectivamente, hay tres tipos principales de DLP "funcionales" dedicados a proteger cada uno de los estados de los datos:

- **DLP de datos en uso**
- **DLP de datos en movimiento**
- **DLP de datos en reposo**

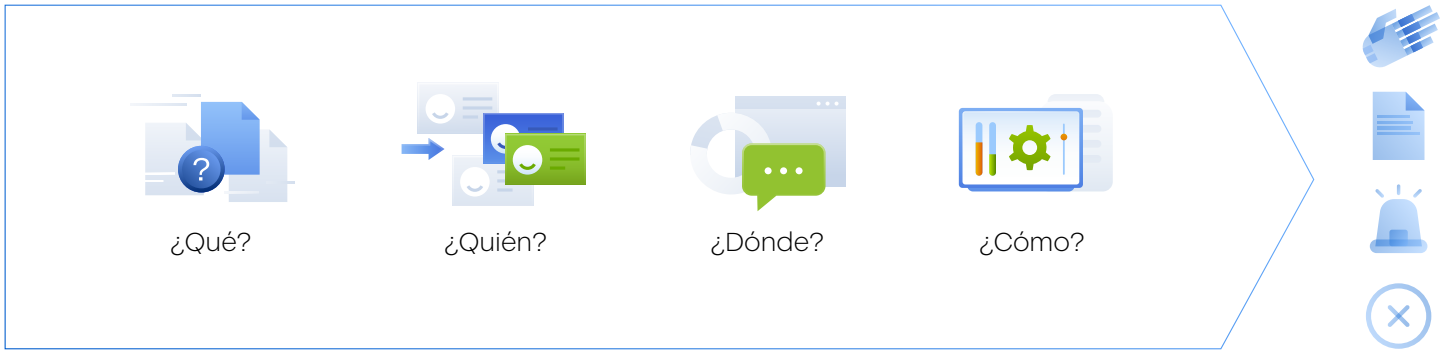
Es importante mencionar que hay otras tecnologías que pueden abordar diferentes riesgos de los datos (p. ej., la accesibilidad, los riesgos para la privacidad), como la gestión de identidad o el cifrado. Sin embargo, la DLP es la única tecnología capaz de proteger los datos en varios estados con el solemne propósito de evitar su filtración, mientras brinda visibilidad a los flujos de datos.

## Controles de DLP: contenido frente a contexto

Cada flujo de datos en una empresa tiene su contexto y su contenido. El contexto se refiere a factores del entorno, como los usuarios que participan en un flujo de datos, los canales que se utilizan, la dirección del flujo, etc. El contenido describe el tipo o la categoría de información que se transfiere, por ejemplo, los registros médicos de los pacientes, la PII de los empleados, etc.

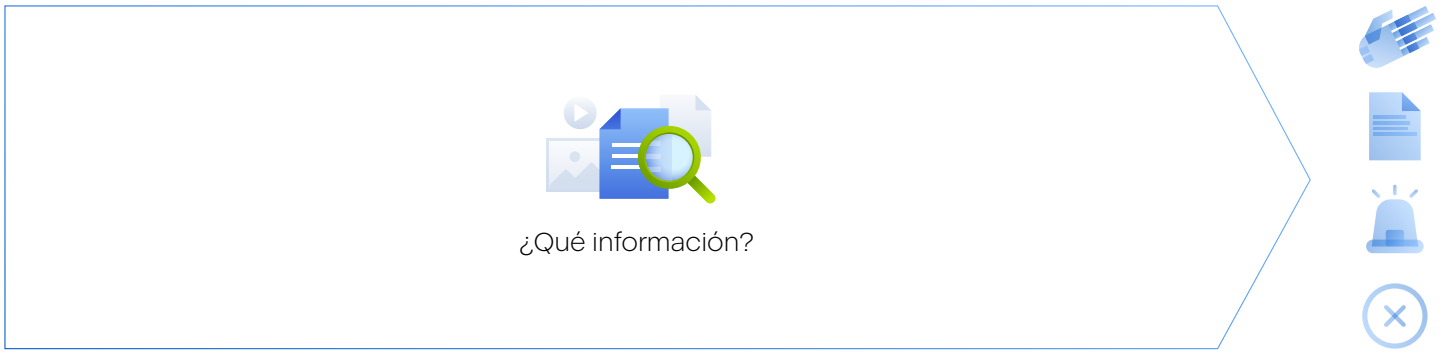
**Una solución de DLP eficaz debe implementar controles sobre los flujos de datos basados en su contexto y en su contenido:**

- **Controles de DLP basados en contexto**: controlar las operaciones de transferencia de datos según el contexto, utilizando atributos como los usuarios implicados, los canales utilizados, la dirección de los datos transferidos, el destino, la hora, etc.




**Ejemplo:** políticas que permiten la copia de datos (qué) por parte de los usuarios (quién) en dispositivos USB cifrados (dónde) y bloquean la copia de datos en dispositivos USB no cifrados.

- **Controles de DLP adaptados al contenido**: un control más profundo sobre los flujos de datos se basa en el tipo y la confidencialidad de la información (contenido) real que se transfiere.

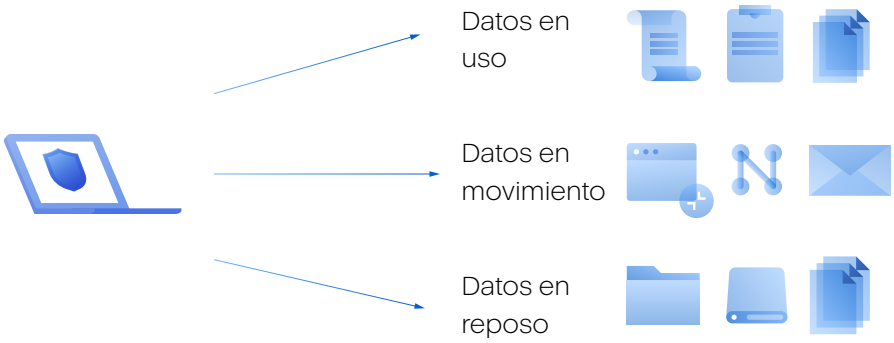



**Ejemplo:** está prohibido copiar en cualquier dispositivo USB los documentos que contengan información relacionada con la HIPAA (qué información).

## Tipos de arquitectura de DLP

**Hay tres tipos principales de DLP según las maneras en que se implementan y manejan:**

- **DLP de endpoint**: soluciones que utilizan agentes de DLP en computadoras endpoints y evitan la filtración de datos en uso, datos en movimiento y datos en reposo de estas computadoras, independientemente de que se utilicen dentro de la red corporativa o en Internet.




- **DLP de red o de nube**: soluciones con solo componentes residentes en la red, que incluyen puertas de enlace y servidores de DLP virtuales o de hardware que protegen los datos en movimiento o los datos en reposo en computadoras ubicadas en la red corporativa, evitando la filtración de datos a destinatarios y destinos no autorizados fuera de la red corporativa.


- **DLP híbridas**: soluciones que utilizan componentes de DLP de red y de endpoints para realizar todas las funciones de las arquitecturas de DLP de endpoints y de red.

Lo que es importante recordar es que las DLP de red no pueden proteger los datos en uso, debido a su arquitectura, y solo controlan la filtración de datos a partes no autorizadas fuera de la red corporativa, mientras que las DLP de endpoints e híbridas pueden proteger los datos en todos los estados y evitar la filtración a partes no autorizadas, tanto internas como externas.

**Para el propósito de esta guía, nos centraremos en el lanzamiento, la ejecución y la ampliación de un servicio de DLP basado en la arquitectura de DLP de endpoints.**

# Por qué los clientes necesitan DLP

Según el Informe sobre el costo de fugas de datos de 2021 del Ponemon Institute, el costo total promedio mundial de una fuga de datos es de $4.24 millones, lo cual es un 10 % más alto que en 2020. Mientras vemos que el costo de las fugas de datos aumenta, el tiempo promedio real para identificar y contener una fuga es de 287 días, lo que habla de los enormes riesgos a los que se enfrentan sus clientes antes de que se contenga la fuga. Estos riesgos pueden generar costos financieros, reputacionales y de cumplimiento.

**Las principales maneras en las que podrá reducir los riesgos para los clientes con un servicio de DLP son las siguientes:**

- **Ayudar a lograr el cumplimiento** con normativas y proteger la información regulada: PII (RGPD, CCPA), PHI (HIPAA), información de tarjetas de pago (PCI DSS), etc.
- **Proteger** la propiedad intelectual y los secretos comerciales de los clientes
- **Minimizar el riesgo** de filtración de datos mediante malware y ataques debido a la ingeniería social
- **Reforzar la seguridad del trabajo remoto** y de los dispositivos de uso personal (BYOD) y evitar la transferencia de datos confidenciales al almacenamiento privado en la nube
- **Evitar la filtración de datos** causada por empleados debido a errores accidentales, negligencia o mala conducta
- **Permitir una respuesta rápida** a los incidentes de filtración de datos y facilitar las investigaciones posteriores a la filtración, con una visibilidad continua sobre los incidentes de DLP

# Flujo de provisión de servicios de DLP

Antes de entrar en más detalles sobre cómo lanzar, ejecutar y ampliar un servicio de DLP, es importante señalar primero que, debido a sus particularidades, los servicios de DLP tienen un flujo de provisión concreto que incluye los siguientes pasos:

- **Implementación de agentes de DLP:** decidir qué endpoints se deben proveer con servicios de DLP a fin de garantizar una protección completa de los datos de la empresa e implementar agentes de DLP en estos endpoints son algunos de los primeros pasos en su proceso de provisión de servicios. Tenga en cuenta que se recomienda tener agentes de DLP provistos en todas las cargas de trabajo en las que se crean, almacenan o utilizan datos confidenciales. Si dichas cargas de trabajo permanecen desprotegidas, crean posibles brechas de seguridad de los datos en el sistema de seguridad de TI de la empresa.

- **Creación de políticas de DLP:** otro paso inicial es crear las políticas de DLP que garanticen el uso adecuado de los datos y las políticas de manejo para evitar la filtración de datos. Tenga en cuenta que, según la tecnología de DLP utilizada, este paso puede preceder a la implementación. **Lo que es importante señalar** es que las políticas de DLP no son universales, siempre son específicas del cliente, ya que las diferentes empresas tienen distintos procesos internos, se rigen por diferentes normativas y tienen necesidades específicas de acceso e intercambio de datos. Debido a estas particularidades de la creación de políticas de DLP, las soluciones tradicionales de DLP que requieren una administración manual de las políticas presentan desventajas importantes en cuanto a complejidad y costo para los proveedores de servicios.
- **Validación de políticas de DLP**: un paso importante después de la creación de las políticas iniciales de DLP es validarlas con los clientes para asegurarse de que estas políticas se ajusten a los requisitos de la empresa, ya que los MSP no pueden adquirir un conocimiento tan profundo de las particularidades comerciales de cada cliente. Cuanto más compleja y "técnica" sea la representación visual de la política, más tiempo y experiencia necesitarán los clientes para validarla.
- **Aplicación y administración de políticas de DLP:** cuando las políticas de DLP se validan con el cliente, pueden aplicarse para empezar a proteger contra las filtraciones los datos confidenciales de la empresa. Tenga en cuenta que las tecnologías de DLP controlan los flujos de datos confidenciales de una empresa y bloquean los no autorizados. Sin embargo, las empresas evolucionan constantemente, se introducen nuevos procesos, surgen nuevas normativas de datos y las antiguas pueden modificarse. Debido a esto, las políticas iniciales de DLP deben ajustarse continuamente a las necesidades empresariales en constante cambio, a fin de garantizar que no se bloqueen nuevos flujos de datos esenciales, mientras se evitan todos los intentos de filtración de datos. Esto se puede lograr mediante la adaptación manual de las políticas o utilizando los métodos automáticos de ajuste de políticas adaptables.
- **Informes sobre el valor del servicio de DLP:** los informes continuos sobre las transferencias bloqueadas de datos confidenciales y las acciones de los usuarios finales relacionadas con la DLP para demostrar el valor de los servicios de DLP ayudan a impulsar la retención de clientes e ilustran la reducción de riesgos para los clientes que no son conscientes de sus problemas de filtración de datos.

# Desafíos de los MSP con soluciones de DLP actuales

El mercado de DLP es maduro, centrado en las grandes empresas y con actores establecidos hace mucho tiempo. El mercado más amplio (como los proveedores de servicios y sus clientes del sector de las PYMES) ha tenido dificultades para acceder a él, debido a que se requiere un conocimiento continuo y profundo de las particularidades de la empresa y la correspondiente adaptación de los controles de DLP, y una comprensión de los requisitos normativos y de cumplimiento de datos, necesarios para manejar dichas tecnologías. Esto ha provocado que la industria de DLP se centre fundamentalmente en las grandes empresas que pueden afrontar el costo de profesionales internos dedicados a la administración de DLP.

**Los principales desafíos a los que se enfrentan los MSP a la hora de implementar y ejecutar un servicio de DLP son:**

- **La ejecución de un servicio de DLP es costosa y compleja:** debido a que las soluciones tradicionales de DLP requieren procesos manuales complejos para la creación de políticas iniciales y los posteriores ajustes, el tiempo y los esfuerzos necesarios para implementar una DLP eficiente en los clientes hacen que el servicio sea demasiado costoso. Además, esta complejidad requiere la contratación de expertos en DLP, una tarea mucho más difícil y costosa que en el caso de especialistas en seguridad de TI en general.

- **Una DLP eficaz requiere políticas específicas para el cliente:** como se mencionó anteriormente, los procesos empresariales y la confidencialidad de los datos de cualquier empresa son únicos y cambian constantemente, lo cual requiere un ajuste continuo de las políticas de DLP a las particularidades del negocio. Sin embargo, los MSP carecen de un conocimiento profundo de los procesos empresariales de cada cliente y no pueden adquirirlo ni mantenerlo continuamente. Esto se convierte en un obstáculo que plantea un importante desafío de escalabilidad para los MSP con tecnologías de DLP tradicionales.
- **Las políticas de DLP mal configuradas pueden interrumpir la continuidad de la actividad empresarial:** por un lado, es fácil cometer errores en la creación y configuración manual de políticas de DLP, debido a su complejidad y granularidad. Por otro lado, las tecnologías de DLP bloquean cualquier flujo de datos no autorizado. La fusión de esta complejidad y las capacidades de prevención de DLP puede interrumpir los procesos comerciales esenciales al bloquear por error los flujos de datos necesarios para el negocio si las políticas de DLP están mal configuradas o los nuevos procesos comerciales no se asignan de forma coherente a estas políticas.
- **Los empleados son el eslabón más débil de los clientes:** aparte de que las tecnologías de DLP son apenas accesibles para los MSP y sus clientes, los errores humanos y los ataques externos dirigidos a los empleados son las causas principales de las filtraciones de datos. Incluso si los proveedores de servicios son capaces de limitar el riesgo de las amenazas externas con otras capas de protección de endpoints, ellos serán los responsables si los usuarios proporcionan datos confidenciales sin saberlo, provocando una fuga de datos.
- **Los clientes pueden desconocer el problema de la filtración de datos:** debido al difícil acceso histórico a la DLP, es posible que los clientes no sean conscientes del problema de la filtración de datos. Lanzar un servicio de DLP significa que los proveedores de servicios también tendrían que educar a los clientes sobre los riesgos de filtración de datos a los que se enfrentan e informarles de que la DLP es la única tecnología capaz de abordar esos riesgos, que suponen amenazas importantes para empresas de cualquier tamaño.

Las nuevas tendencias y tecnologías del mercado, como la creación, ampliación y supervisión automáticas de políticas, basadas en el comportamiento, están enfrentando los desafíos de cambiar rápidamente las reglas de DLP para adaptarse a los procedimientos comerciales en constante evolución, además de los requisitos normativos. Estas nuevas capacidades están democratizando eficazmente el mercado de la DLP y permitiendo el acceso a los proveedores de servicios y a sus clientes. Este es un buen momento para pensar en ampliar su cartera con servicios de DLP.

# Planificación y lanzamiento de un servicio de DLP

## El primer paso en la planificación y el lanzamiento de un servicio de DLP es verificar si sus clientes realmente necesitan DLP.

**Los clientes requieren un servicio de DLP para reducir sus riesgos de filtración de datos en caso de que cumplan alguna o todas las condiciones siguientes:**

- Crean, almacenan o trabajan en sus cargas de trabajo con datos confidenciales que están sujetos a normativas.
- Tienen secretos comerciales o propiedad intelectual que se deben proteger contra las filtraciones.
- Operan en industrias muy reguladas.
- Han sufrido una fuga de datos y quieren proteger su entorno y reducir los riesgos.
- Tienen o necesitan certificaciones de cumplimiento.
- Están pagando o considerando un ciberseguro para reducir sus responsabilidades.
- Carecen de personal dedicado a la seguridad y de experiencia

**Además, los clientes de las siguientes industrias han demostrado históricamente un mayor interés en la DLP:**

- Servicios bancarios y financieros
- Atención médica
- Sector legal
- TI y telecomunicaciones
- Gobierno y sector público
- Fabricación
- Comercio minorista y logística
- Educación
- Energía

En caso de que tenga clientes que cumplan estas condiciones o que operen en las industrias antes mencionadas, es un buen momento para considerar la incorporación de DLP a su cartera de servicios a fin de satisfacer las crecientes necesidades de reducción de riesgos de filtración de datos y reforzar el cumplimiento de las normativas.

## Planificación de servicios y estimación de costos

**Los tres factores principales que determinan el precio de su servicio son los costos de mano de obra, los costos del producto y su margen deseado. Así es como cada uno de ellos puede afectar a su presupuesto:**

- **Costos de mano de obra:** la complejidad de la solución elegida determinará el tiempo que sus técnicos de mantenimiento dedicarán al aprovisionamiento y la administración del servicio, así como el nivel requerido de experiencia en seguridad de TI.
- **Costos del producto:** las soluciones de DLP, tradicionalmente utilizadas por grandes empresas, implican costos elevados por lo que no son asequibles para las pequeñas y medianas empresas. Si sus clientes son principalmente PYMES, debe elegir una solución que no genere un costo excesivo del servicio para ellos.
- **Margen deseado:** el MSP promedio obtiene márgenes brutos de hasta el 50 % en los servicios prestados de forma remota y vendidos bajo el modelo de ingresos recurrentes.

# Un servicio de DLP con el paquete Acronis Advanced DLP

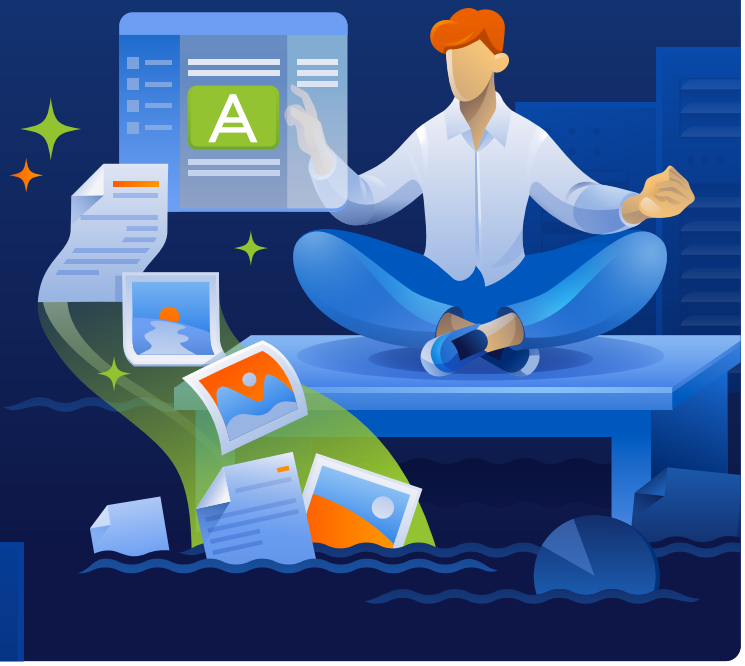
Acronis ofrece DLP basada en el comportamiento que crea automáticamente y mantiene continuamente la coherencia de las políticas específicas del cliente, sin necesidad de meses de implementación, equipos de mantenimiento o un doctorado en derecho de la privacidad para entenderlo.

**Con el paquete Acronis Advanced DLP, puede brindar a los clientes protección de DLP completa para datos en movimiento y datos en uso, con un nivel de simplicidad nunca visto, que le permite hacer lo siguiente:**

- **Disfrutar de nuevas oportunidades de rentabilidad** ampliando su cartera para atraer a más clientes y aumentar sus ingresos por cliente con servicios de DLP que antes solo estaban disponibles para las grandes empresas.
- **Minimizar los esfuerzos para obtener valor** agregando fácilmente la DLP a su oferta, sin aumentar la complejidad de administración, los costos ni el personal.
- **Mitigar los riesgos de seguridad para los clientes** evitando la filtración de datos confidenciales.
- **Reforzar el cumplimiento de las normativas por parte del cliente** con plantillas de clasificación de datos listas para usar para los marcos normativos comunes, incluido el RGPD, la HIPAA y el PCI DSS.
- **Simplificar el aprovisionamiento y la administración de servicios** automatizando el aprovisionamiento del servicio de DLP, la configuración inicial de políticas y los ajustes de seguimiento.
- **Garantizar las políticas de DLP específicas del cliente a cualquier escala** alineando automáticamente las políticas de DLP con las particularidades de la empresa con tecnología basada en el comportamiento, garantizando así una fácil validación de las políticas con los clientes antes de su aplicación.
- **Reaccionar más rápidamente ante los eventos de DLP** y simplificar las operaciones del servicio de DLP, el mantenimiento de las políticas, las auditorías de seguridad de TI y las investigaciones de incidentes con alertas de seguridad y registros de auditoría centralizados y basados en políticas.

## Paquete Acronis Advanced DLP

El paquete Acronis Advanced DLP para Acronis Cyber Protect Cloud ayuda a sus clientes a dormir mejor por la noche sabiendo que sus datos confidenciales están protegidos contra filtraciones a partes no autorizadas. Su exclusiva tecnología basada en el comportamiento permite la creación y la ampliación continua de las políticas de DLP según las particularidades de cada cliente y facilita el lanzamiento de su servicio con una sencillez nunca vista y un esfuerzo mínimo.



Acronis

Encontrará más información en www.acronis.com