

# Acronis Data Loss Prevention(DLP)

## Para **Acronis** Cyber Protect Cloud

### Proteja los datos confidenciales de los clientes con la facilidad y la agilidad que necesita

Las empresas llevan años sin conseguir proteger con eficacia los datos confidenciales para evitar el acceso no autorizado y las filtraciones provocadas por ataques externos o riesgos internos, como los errores de configuración de TI o humanos, o las amenazas. Esto las deja expuestas a consecuencias como su aparición en noticias embarazosas, pérdida de confianza de clientes y partners, pérdidas de patrimonio, problemas de recursos humanos y sanciones normativas.

Desafortunadamente, los principales obstáculos para adoptar la tecnología DLP (complejidad, costos

de implementación y largo plazo de amortización debido a que las directivas de DLP no son universales sino específicas para las empresas) siguen siendo insuperables para la mayoría de las empresas, a excepción de las más grandes.

Acronis DLP le ofrece una simplicidad sin igual en el aprovisionamiento, la configuración y la gestión, lo que le permite evitar la fuga de datos de los workloads de los clientes y reforzar el cumplimiento normativo. Una tecnología exclusiva basada en comportamientos crea automáticamente y mantiene continuamente las directivas específicas de la empresa, sin necesidad de meses de implementación, mantenimiento de equipos o conocimiento del derecho de la privacidad.

### Amplíe su pila de servicios con una prevención de pérdida de datos simplificada

Controles de DLP basados en el contenido en más de 70 canales	Creación y ampliación automáticas de directivas de DLP basadas en comportamientos	Respuesta rápida a eventos de DLP
Proteja los datos confidenciales de los clientes e impida filtraciones de datos desde los recursos informáticos a través de dispositivos periféricos y comunicaciones de red, mediante el análisis del contenido y el contexto de las transferencias de datos, y la implementación de controles preventivos basados en directivas.	No es necesario analizar los detalles de la empresa del cliente ni definir las directivas manualmente. Los flujos de datos confidenciales se identifican automáticamente para crear y ajustar en forma continua las directivas de DLP según las circunstancias concretas de la empresa en cada momento, garantizando la protección contra las causas de fugas de datos más habituales.	Facilite una respuesta y una investigación forense rápidas, y simplifique el mantenimiento de directivas de DLP mediante registros de auditoría centralizados y alertas en tiempo real de los incidentes de seguridad. Rápida notificación de incidentes con widgets detallados.

Acceda a nuevas oportunidades de rentabilidad	Menos esfuerzos para obtener valor	Mitigación del riesgo de filtraciones de datos y mejora del cumplimiento de normativas	Directivas específicas para cada cliente	Mejor capacidad de reacción ante los eventos de DLP
Mejore los ingresos por cliente y atraiga más clientes con servicios de DLP gestionados (o una solución de DLP, para los VAR) accesible para las pymes y los clientes de segmento medio.	Amplíe su cartera con un servicio DLP que no aumenta la complejidad de la gestión, los costos ni el personal, lo que le permite optimizar sus esfuerzos.	Detecte y evite las filtraciones de información confidencial en una amplia variedad de canales locales y de red.	Identifique los flujos de datos confidenciales para brindar a cada cliente directivas específicas para la empresa.	Responda rápidamente a los incidentes de DLP y aproveche la sólida función de auditoría que incluye alertas y registros basados en directivas en un registro centralizado.

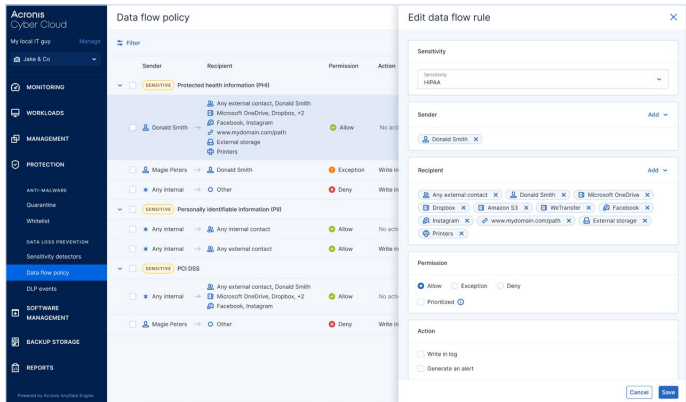
Cronología: Cómo aprovisionar sus servicios con Acronis DLP

10 minutos ●	~ 2-6 semanas ●	~ 1-2 días ●	Automática ●	~ 1-3 horas/mes/cliente ●
Desplegar el agente Acronis Cyber Protect Cloud	Generación inicial de directivas de DLP	Validación con los clientes	Ampliación automática de directivas	Comunicación y ajuste

Qué hace Acronis DLP

Protección integral que satisface las necesidades del cliente con un nivel de simplicidad nunca visto:

- Protege los datos confidenciales transferidos a través de una amplia variedad de comunicaciones de usuarios y del sistema, incluidas las comunicaciones de red, como la mensajería instantánea, y dispositivos periféricos, como USB.
- Ofrece clasificadores de datos confidenciales prediseñados para usar con marcos normativos comunes, incluidos el RGPD, la HIPAA y la PCI DSS.
- Identifica flujos salientes de datos confidenciales transferidos desde los workload, para crear, recomendar y habilitar automáticamente el ajuste de directivas, de manera que se garantice la protección contra las causas más habituales de transferencias de datos a destinos no autorizados.
- Brinda supervisión continua para descubrir incidentes de DLP, con múltiples opciones de implementación de directivas.
- Facilita continuos ajustes automáticos de directivas según las circunstancias concretas de la empresa.
- Permite una rápida respuesta e investigación forense de los incidentes tras una violación de seguridad, con funciones robustas de auditoría y registro.
- Usa la consola unificada y el agente de Acronis Cyber Protect Cloud para obtener visibilidad y opciones de clasificación de los datos.



Canal controlado

- Almacenamiento extraíble
- Impresoras
- Unidades asignadas redirigidas
- Portapapeles redirigidos
- Cualquier mensaje de correo electrónico SMTP, Microsoft Outlook (MAPI), IBM Notes (NRPC)
- 7 servicios de mensajería instantánea
- 16 servicios de correo web
- 28 servicios para compartir archivos
- 12 redes sociales
- Recursos de archivos compartidos locales, acceso web y transferencias de archivos FTP

Características principales

- Reglas de DLP personalizables
- Controles de DLP basados en el contexto y el contenido
- Creación y ampliación automáticas de directivas de DLP
- Clasificadores de datos prediseñados para PII, PHI y PCI DSS, así como documentos marcados como confidenciales
- Implementación estricta y adaptable de directivas de DLP
- Posibilidad de omitir directivas en bloque si se requieren excepciones
- Control de transferencias de datos independiente del navegador web
- Reconocimiento óptico de caracteres (OCR) residente en el agente
- Alertas en tiempo real
- Registro y alertas basadas en directivas
- Registro de auditoría centralizado, nativo en la nube
- Visor de eventos del registro de DLP con sencillas funciones de filtrado y búsqueda
- Notificaciones detalladas
- Notificaciones en pantalla para los usuarios finales