# Prevención de pérdida de datos y transformación digital

## INTRODUCCIÓN

La era digital actual ha producido cantidades de datos sin precedentes. Gran parte de estos datos se consideran confidenciales, como información personal sobre clientes y empleados, datos financieros y propiedad intelectual que las empresas deben mantener a salvo. En el pasado, esta información se imprimía en papel y se protegía en un archivador cerrado con llave. Ahora, estos ceros y unos tan valiosos van de un lugar a otro y son más vulnerables que nunca.

La necesidad de proteger estos datos es indiscutible. Son el alma de una organización e incluyen información que se ha confiado a la organización para que la mantenga a salvo. Por ello, ciertos tipos de datos están regulados y las empresas se enfrentan a duras sanciones por un mal manejo de los mismos. No es de extrañar que los datos también sean valiosos en la red oscura, donde se alcanzan hasta cinco dólares por un solo número de tarjeta de crédito con su dirección, el tipo de información que numerosas bases de datos almacenan en gran cantidad. Por todos estos motivos, se ha convertido en una obligación para las organizaciones implementar soluciones integrales de prevención de pérdida de datos (DLP).



## LA NECESIDAD DE DLP

Una solución de DLP es un conjunto de tecnologías y procesos que supervisa e inspecciona los datos en la red corporativa para garantizar que los datos confidenciales no se pierdan o sean robados. Una herramienta de DLP siempre debe formar parte de una iniciativa de protección de datos para la organización en su totalidad, que reúne a los líderes empresariales y de TI para identificar cuáles son realmente "datos confidenciales" y para acordar cómo deben manejarse estos datos así como el aspecto que tendría una violación de los mismos. Estas pautas se pueden traducir en un conjunto de reglas dentro de una herramienta de DLP. Las soluciones de DLP abordan tres grandes retos organizativos: el cumplimiento de la normativa, la protección frente la pérdida de datos y la visibilidad.

1

**Cumplimiento de la normativa:**

De acuerdo con Gartner[1], el cumplimiento de la normativa es, con diferencia, el caso de uso más común de DLP, al que se hace referencia en el 75 por ciento de todas las implementaciones de DLP registradas. A partir de mayo de 2018, el RGPD (el Reglamento General de Protección de Datos de la Unión Europea) ha incorporado soluciones de DLP al radar de los especialistas en protección de datos en organizaciones ajenas a los sectores regulados (en el caso de estas últimas siempre se ha requerido que cuenten con ciertas medidas para proteger la información de identificación más personal (PII) y la información de salud protegida (PHI)). Aunque el reglamento no requiere explícitamente el uso de una solución de DLP, los requisitos de protección de datos a menudo presentan el concepto de DLP para ayudar con el cumplimiento.

## Suena a DLP...

El Departamento de Servicios Financieros del Estado de Nueva York (NYDFS), en su regulación 23 NYCRR 500 alude al uso de una DLP de datos en movimiento, pero no lo detalla:

**Sección 500.15 (a)**

"(...) cada entidad cubierta implementará controles, incluido el cifrado, para proteger la información no pública que dicha entidad cubierta tiene o transmite, tanto en tránsito a través de redes externas como en reposo".

[1] Guía de mercado para la prevención de la pérdida de datos en las empresas: https://www.gartner.com/en/documents/3890116/market-guide-for-enterprise-data-loss-prevention

# LA NECESIDAD DE DLP

## 2 Protección frente la pérdida de datos

Los motivos para proteger la información confidencial de su exposición a partes no autorizadas van mucho más allá del cumplimiento de la normativa. Es un objetivo frecuente para el robo. Un buen indicador de su valor es la disposición de los actores maliciosos a pagar precios mucho más elevados en la web oscura por datos no regulados, como cifras de afiliaciones a premios y programas de fidelización, en comparación con los números de la Seguridad Social de Estados Unidos[2].

Si bien las organizaciones tienen incentivos para cumplir con la normativa, como evitar multas o restricciones en sus operaciones comerciales, la pérdida de datos conlleva riesgos financieros y de reputación mucho más amplios, como perder clientes, reembolsar o devolver puntos de afiliaciones perdidas, incurrir en daños a la marca o incluso enfrentarse a ramificaciones legales.

De acuerdo con el estudio Ponemon 2019 Cost of a Data Breach[3], el 30 por ciento de las organizaciones experimentarán una filtración de sus datos en el plazo de dos años que, de media, se traduce en:

**un costo de $3,9 millones de dólares estadounidenses** **25 000 registros perdidos**

Los sectores que están sujetos al cumplimiento de la normativa, como la sanidad y los servicios financieros, experimentan filtraciones de datos más costosas. El coste medio por registro robado fue de

**429 USD** Cuidado de la salud

**210 USD** servicio financiero

**150 USD** todos los sectores

Las soluciones de DLP son especialmente importantes para evitar la pérdida accidental de datos bien por errores humanos, como compartir involuntariamente datos confidenciales con terceros a través de archivos compartidos o medios sociales, o bien por fallos en los procesos informáticos o empresariales[4]. A pesar de las estrictas regulaciones para el manejo de la información sanitaria, la pérdida accidental de datos es especialmente elevada en el sector sanitario, donde representa el 57,5 por ciento[5] de la divulgación involuntaria de datos, según el Informe de Verizon sobre la filtración de datos de información sanitaria protegida de 2018. Verizon señaló que es el único sector en el que las personas de la propia organización representan una mayor amenaza de pérdida de datos que los actores externos maliciosos.

[2] https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/; https://www.comparitech.com/blog/information-security/how-much-are-stolen-frequent-flyer-miles-worth-on-the-dark-web/#gref

[3] [4] Estudio Ponemon 2019 Cost of a Data Breach https://databreachcalculator.mybluemix.net/

[5] Informe de filtración de datos de información sanitaria protegida: http://www.verizonenterprise.com/resources/protected_health_information_data_breach_report_en_xg.pdf



# LA NECESIDAD DE DLP

## 3 Visibilidad de los datos

La transformación digital hace que las organizaciones y, específicamente los CISO, se enfrenten a desafíos relacionados con la visibilidad de lo que está sucediendo con los datos en sus redes. Con una cantidad de datos cada vez mayor, numerosos propietarios de datos diferentes y aún más lugares donde residen esos datos, es difícil identificar toda la información confidencial y establecer medidas para protegerla; después de todo, no se puede proteger lo que no se puede ver. Hay tres tendencias significativas que causan puntos ciegos para las organizaciones: la adopción de la nube, la movilidad de los usuarios y el cifrado.

**La adopción de la nube** está obligando a las organizaciones a controlar todos los datos almacenados no solo en el centro de datos, sino también en toda la organización. Antes de poder trasladar sus datos a la nube, debe saber qué datos tiene.

Los empleados ya no están vinculados a sus escritorios, lo que significa que ahora acceden a sus aplicaciones y archivos de trabajo desde casi cualquier lugar y en cualquier momento. Estos **usuarios móviles** pueden acceder a los datos y almacenar archivos fuera del centro de datos, a menudo dejando a la organización en la oscuridad en lo relativo a estos datos.

Cada vez más, las organizaciones emplean técnicas de **cifrado** en un intento por proteger los datos. No obstante, los sistemas de seguridad basados en hardware no pueden verificar el contenido de los archivos cifrados, lo que deja a las organizaciones ciegas con respecto al tipo de datos que contienen.

# LA NECESIDAD DE DLP

**Los datos se mueven a través de varios canales**

En nuestro mundo digitalizado, los datos se mueven con más libertad que nunca. En cualquier momento, se pueden encontrar en uno de los tres canales: un punto final, en el almacenamiento (o reposo) o en tránsito. Cada canal en el que se almacenan los datos o por el que pasan requiere un conjunto diferente de herramientas o técnicas para evitar la pérdida de datos. Las soluciones de DLP se segmentan de acuerdo con los tres canales que protegen:

**Datos en el punto final:** las soluciones de DLP de punto final se basan en agentes y supervisan los datos que se procesan en el punto final. Su funcionalidad varía, pero generalmente incluye restricciones de impresión, prevención del copiado/pegado entre aplicaciones y de descarga a un almacenamiento portátil, como un USB.

**Datos en reposo:** todos los datos que se encuentran en servidores de archivos, bases de datos o almacenamiento en la nube se consideran en reposo. La DLP de datos en reposo analiza todo el contenido del repositorio para detectar información confidencial.

**Datos en tránsito:** también conocida como DLP de la web o DLP de la red, las soluciones de datos en tránsito inspeccionan todo el tráfico que se mueve del punto A al B a través de la web (Internet) o del correo electrónico (por ejemplo, los datos que pasan desde el almacenamiento en la nube a un punto final).

La transformación digital ha creado un cambio en el comportamiento de los usuarios y en los patrones de tráfico, que ha afectado a los canales de punto final y de datos en reposo. A medida que más datos se trasladan a la nube, las soluciones de datos en reposo se están volviendo irrelevantes básicamente porque su funcionalidad se puede sustituir por las soluciones de los proveedores de seguridad de acceso a la nube (CASB). Además, son menos los datos y las aplicaciones que permanecen en los puntos finales, lo que confiere más importancia a la seguridad de los datos que fluyen entre los puntos finales, las aplicaciones en la nube y el almacenamiento con una solución para **datos en tránsito**.



## ¿POR QUÉ LA DLP NO HA CUMPLIDO SU PROMESA?

**El mercado de la DLP está evolucionando**

Las soluciones de DLP llevan 15 años disponibles y el mercado está maduro. Las diferencias entre las diversas soluciones de DLP empresariales rivales del mercado ha llevado a la empresa de investigación y análisis líder Gartner a retirar su Cuadrante Mágico para la prevención de pérdida de datos corporativos. En su lugar, Gartner se centra en una guía de mercado que destaca la importancia de una estrategia holística de protección de datos y ofrece instrucciones sobre el uso de soluciones integradas de DLP.

En comparación con las soluciones de **DLP empresarial**, que generalmente proporcionan diversos productos (agentes, dispositivos físicos y virtuales) en todos los canales, las soluciones integradas de **DLP** se entregan de forma nativa mediante tecnologías como puertas de enlace web seguras, sistemas de administración de contenido, cifrado de correo electrónico o tecnología CASB y, por lo tanto, tienen un enfoque más específico.

Las soluciones de DLP empresarial son notoriamente complejas y costosas. Las organizaciones que compran DLP empresarial a menudo terminan utilizando solo un pequeño subconjunto de sus capacidades y abordan solo los casos de uso básicos que podrían resolverse con una solución de DLP integrada, evitando así que la organización tenga que realizar una configuración e integración costosas y lentas.

> **De acuerdo con las estimaciones de Gartner,** para finales de 2021, el 90 % de las organizaciones habrán implementado al menos una forma de DLP integrada, lo que supone un aumento del 50 % con respecto a la situación actual. [6]

Sin embargo, la DLP empresarial y la DLP integrada no son mutuamente excluyentes. Las organizaciones que ya han realizado inversiones en dichos productos deben trabajar con su infraestructura existente. No obstante, cualquier organización debería plantearse la posibilidad de añadir una DLP integrada para abordar otros casos de uso y así cubrir las lagunas de su actual estrategia de protección provocadas por la transformación digital.

[6] How to Choose Between Enterprise DLP and Integrated DLP Approaches
https://www.gartner.com/doc/3757464?ref=mrktg-srch



# ¿POR QUÉ LA DLP NO HA CUMPLIDO SU PROMESA?

**La prevención de la pérdida de datos es una iniciativa que afecta a la totalidad de la organización, no una herramienta informática**

A pesar de ser una solución madura, las organizaciones siguen informando de problemas en sus implantaciones de DLP, muchos de ellos derivados de una mala planificación y otros problemas organizativos.

La mayoría de las organizaciones creen erróneamente que la DLP debe ser implantada y gestionada a largo plazo únicamente por el área de seguridad informática. Una vez establecidas las reglas de la DLP, la responsabilidad de la solución de DLP debe transferirse a las operaciones empresariales. Además, quienes implementan soluciones de DLP necesitan asegurar la aceptación de la directiva a fin de obtener visibilidad de las unidades de negocio o de los equipos de gestión de riesgos empresariales.

Para evitar tener que buscar patrocinadores y casos de uso adicionales para justificar el proyecto, lo que inevitablemente añade demandas y complejidades a las implementaciones, los equipos deben asegurarse de contar con la aceptación interna y vincular los proyectos de DLP con iniciativas u objetivos específicos.



## REQUISITOS DE DLP EN LA NUBE

A medida que las organizaciones se trasladan a la nube, su seguridad también debe hacerlo. Sin embargo, simplemente volver a configurar una pila de hardware tradicional para la nube no resulta eficiente ni proporciona las protecciones y los servicios de una solución desarrollada en y para la nube. Esto es perfectamente aplicable a la DLP. Para abordar los desafíos de protección de datos que han surgido con la transformación digital y superar las deficiencias de la DLP tradicional, una solución de DLP basada en la nube debe contar con los siguientes tres elementos:

**1. Protección idéntica para todos los usuarios dentro o fuera de la red**

Con las soluciones de DLP tradicionales ancladas en el centro de datos, el nivel de visibilidad y protección depende de dónde se encuentren sus usuarios. Los usuarios remotos pueden evitar la inspección cuando están fuera de la red, conectarse directamente a las aplicaciones en la nube y evadir las VPN y cualquier otra medida de protección de datos. Para brindar una protección de datos integral, una solución de DLP debe proporcionar protección idéntica a todos los usuarios, independientemente de su ubicación, tanto si se encuentran en la oficina como en una sala de espera del aeropuerto o en un despacho en su casa.

**2. Inspección del tráfico cifrado**

Dado que más del 70 por ciento del tráfico actual utiliza cifrado, corresponde a las organizaciones inspeccionar este tráfico. Sin embargo, puesto que el cifrado se creó originalmente como una medida de seguridad, las soluciones de seguridad tradicionales no inspeccionan este tráfico de forma nativa. Como resultado, las organizaciones tienden a inspeccionar solo una fracción de su tráfico cifrado, y ¿de qué sirve una solución de DLP si es posible que solo vea el 30 por ciento del tráfico total? Aumentar su postura de seguridad añadiendo dispositivos SSL probablemente no es viable desde el punto de vista financiero, ni tampoco es aceptable en términos de complejidad informática. La única manera de obtener visibilidad del tráfico cifrado es utilizar una solución de DLP que inspeccione SSL de forma nativa.

**3. Escalabilidad elástica para la inspección en línea**

El tremendo crecimiento del tráfico de Internet requiere actualizaciones constantes de las soluciones de DLP tradicionales basadas en dispositivos, ya que su capacidad de inspección finita se agota rápidamente. En un intento por superar la complejidad y el costo de esta tarea, muchas organizaciones se resisten a implementar una solución de DLP en línea desde el principio. Lamentablemente, esto solo permite a las organizaciones controlar los daños después de que sus datos se han visto comprometidos. Una solución en la nube ofrece una capacidad de inspección elástica y escalable que puede prevenir la pérdida de datos inspeccionando todo el tráfico en línea, antes de que los datos puedan verse comprometidos.



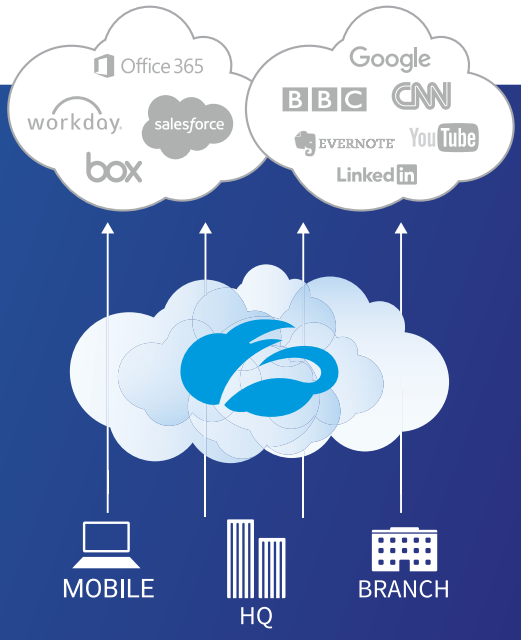
# ZSCALER™ CLOUD DLP

**Parte de Zscaler Internet Access**

Zscaler Internet Access™ (ZIA™) es una puerta de enlace segura a Internet y a la web que se entrega como un servicio desde la nube. ZIA se coloca entre sus usuarios e Internet, inspeccionando cada byte de tráfico en línea a través de múltiples técnicas de seguridad, incluso dentro de SSL, proporcionando así una protección completa frente a las amenazas de Internet. Esta plataforma especialmente diseñada para la nube incluye Cloud Sandbox, Next-Generation Firewall y Cloud Application Visibility and Control, así como Cloud DLP.

## Perspectiva general de Cloud DLP

Zscaler Cloud DLP ofrece una protección de datos completa con inspección integral de contexto y contenido para todos los datos en movimiento, así como características avanzadas, entre las que se incluyen Exact Data Match, aprendizaje automático y políticas granulares para una protección óptima.




**Zscaler Cloud DLP cumple con los tres requisitos**

Zscaler Cloud DLP proporciona el mismo nivel de seguridad a todos sus usuarios al trasladar la seguridad de sus datos a la nube. Zscaler se coloca entre sus usuarios y las aplicaciones a las que se conectan. La política de Cloud DLP sigue a los usuarios allí donde trabajen, dentro o fuera de la red, y brinda el mismo nivel de protección a todos los usuarios en todo momento.



También proporciona una inspección completa del tráfico cifrado. Alrededor del 70 por ciento del tráfico saliente está encriptado y, por tanto, no está sujeto a la inspección de las soluciones de DLP tradicionales. Con Zscaler, no hay limitaciones de capacidad para permitir la interceptación de SSL a escala. Zscaler es un proxy por diseño, que realiza inspección SSL de todo el tráfico sin las limitaciones de inspección de los dispositivos.

Además, Zscaler está diseñado para funcionar en línea, de modo que puede bloquear información confidencial antes de que salga de su red, en lugar de limitarse al control de daños después de que los datos se hayan visto comprometidos. La arquitectura de seguridad de Zscaler se creó en la nube desde cero y el servicio se basa en el usuario, no en la capacidad, lo que permite que su inspección Cloud DLP se adapte de manera elástica con el rendimiento garantizado por los SLA.

## CONCLUSIÓN

La DLP debe considerarse como un proceso de seguridad bien definido que se ve reforzado por una tecnología de soporte bien gestionada. Sin embargo, incluso en esta última etapa de madurez de la solución de DLP, las organizaciones siguen teniendo problemas con las implementaciones de DLP. Esto se debe principalmente a la desinformación acerca de las soluciones de DLP a nivel interno en el contexto de un programa de seguridad. Además, una buena parte del mercado sobrevalora la sencillez de las implementaciones, el nivel de precisión inmediata en la identificación de contenido y visibilidad, así como el control sobre todas las aplicaciones.

Con el aumento de los riesgos y la ampliación de la reglamentación para la protección de datos, las organizaciones deben cerrar las brechas de seguridad creadas por la nube y la movilidad. En el pasado, eso significaba añadir más dispositivos a una pila de seguridad ya compleja. Zscaler ofrece una forma mejor de hacerlo. Con Zscaler Cloud DLP, puede cerrar las brechas de protección de datos, independientemente de dónde se conecten los usuarios o dónde se alojen las aplicaciones, sin necesidad de costosos y complejos dispositivos.

# Sobre Zscaler

Zscaler permite a las organizaciones transformar de forma segura sus redes y aplicaciones para un mundo móvil y ser pioneros en la nube. Zscaler conecta a los usuarios con aplicaciones y servicios en la nube, independientemente del dispositivo, la ubicación o la red, a la vez que proporciona seguridad integral y una experiencia de usuario rápida. Todo ello sin dispositivos de entrada costosos y complejos.



zscaler™