



# Tres requisitos esenciales para una protección de datos perfecta

¿Desea un CASB mejor y una DLP más robusta? Debe comenzar con una buena base.



Quienes trabajan en TI o en seguridad de redes le dirán que la protección de datos solía ser mucho más sencilla cuando todos los datos estaban en el centro de datos y todos los empleados trabajaban en la oficina. Pero, definitivamente, los tiempos han cambiado.

Ahora, sus datos han salido del centro de datos y están en todas partes, distribuidos en cientos de aplicaciones en la nube. Y sus empleados están adoptando el trabajo a distancia, fuera de la red corporativa y lejos de sus controles de seguridad. Como si eso no causara suficientes problemas, la mayor parte del tráfico de Internet está cifrado y es difícil de inspeccionar, por lo que los atacantes ocultan allí sus amenazas. Y sus empleados están utilizando redes no seguras o dispositivos no administrados, algo que expone aún más sus datos.

En este "mundo feliz", las organizaciones necesitan una plataforma de protección de datos desarrollada especialmente para la nube y la movilidad, y debe incluir estos requisitos esenciales.

## Lo que debe saber



La protección de sus datos con un CASB y una DLP es tan buena como la arquitectura sobre la que se basa. Para tener éxito es esencial entender la receta.

## Requisito esencial n.º 1:

### Insista en una arquitectura SASE especialmente diseñada

Con la nube y la movilidad, los dispositivos de seguridad no pueden estar en todas partes. Cuando los usuarios salen de la red, usted se queda ciego y sus usuarios y datos quedan expuestos. Además, para ofrecer capacidades de agente de seguridad de acceso a la nube (CASB) sin filtraciones y protección contra la pérdida de datos (DLP), necesita una inspección SSL completa. Los dispositivos no pueden ofrecer esto debido a las restricciones del hardware.

Una plataforma SASE especialmente diseñada en la nube es el primer requisito que necesita para ofrecer conexiones seguras de alto rendimiento y siempre activas, independientemente de la ubicación del usuario. SASE unifica todos los servicios de CASB, DLP y de seguridad en una plataforma en la nube distribuida globalmente para que usted obtenga menos complejidad, mejor protección de los datos y una rápida experiencia de usuario.

### Lo que debe saber



Crear una arquitectura de protección de datos en línea de nivel empresarial que se amplía a través de SSL no es sencillo. Confíe su tráfico únicamente a un proveedor con la mayor experiencia, un historial comprobado y SLA de nivel empresarial.



## El modo de Zscaler™



Zscaler Zero Trust Exchange™ es un proxy nativo de la nube, construido desde cero para la protección de datos y la inspección SSL a escala en 150 centros de datos. Todos los usuarios obtienen una conexión rápida y segura. Y nuestra capacidad ilimitada de SSL significa que puede proteger todos sus datos en cada conexión de usuario, dentro o fuera de la red.

Como líder del mercado, Zscaler lleva más de una década realizando inspecciones en línea. Lo mejor de todo es que, dado que DLP, CASB y todos los demás servicios de seguridad están integrados, usted obtiene una política simplificada y un modelo unificado para la protección de datos y amenazas.

## Requisito esencial n.º 2:

Una mejor protección de datos requiere el mejor contexto

Para clasificar adecuadamente los datos que tiene, necesita un contexto, pero es la calidad del contexto lo que le ayuda a tomar las decisiones más informadas y mejores.

Antiguamente era sencillo: los usuarios accedían al correo electrónico desde un servidor Exchange o usted solo tenía unos pocos servidores de archivos. Todo lo que necesitaba para tomar decisiones informadas estaba allí y era de fácil acceso.

Ahora, sus datos se mueven por cientos de canales, desde aplicaciones en la nube hasta nubes públicas y plataformas para compartir archivos. Y todo el contexto que necesita en esos canales se oculta dentro del cifrado SSL.

### Lo que debe saber



El contexto es el alma de su CASB y DLP. Busque una plataforma con el motor de clasificación más potente que descubra la mayor cantidad de atributos en cada transacción en la nube, dentro o fuera de la red, y dentro de SSL.



## El modo de Zscaler

Cuando se trata del contexto, Zscaler no tiene igual.

Nuestro Zero Trust Exchange y nuestra aplicación Client Connector le ayudan a ofrecer protección de datos siempre activa en todas las conexiones dentro o fuera de la red. También proporciona visibilidad de TODO el tráfico SSL, lo que proporciona a las empresas un tesoro de contexto.

Y, aprovechando los diccionarios del sector y personalizados de Zscaler y utilizando técnicas avanzadas, como la individualización de Exact Data Match (EDM), puede clasificar rápidamente los datos de los formatos comunes del sector (PCI, HIPAA) y definiciones personalizadas.

<b>Contexto de un firewall o proxy</b>	172.16.1.12 IP de origen	64.81.2.24 IP de destino	TCP/443 Puerto de destino
	Protocolo SSL		Protocolo HTTPS

Los enfoques tradicionales en línea no proporcionan suficiente visibilidad del contexto.

<b>Contexto adicional que obtiene con el descifrado SSL completo</b>	JohnDoe usuario	grupo prodmgmt	Ubicación sede central
	cargar función de la aplicación	aplicación jumpshare	Tipo de archivo PowerPoint
	uso compartido de archivos Categoría URL		Confidencial Contenido

Cuando puede descifrar toda la SSL sin límites, obtiene el contexto necesario para tomar mejores decisiones de protección.

## Requisito esencial n.º 3:

Exija una plataforma unificada que proteja todos los canales

La protección de sus datos contra fugas y exfiltración requiere seguridad dondequiera que se encuentren sus datos. Si no puede controlar todos los canales, sus datos serán vulnerables y estarán expuestos a posibles amenazas.

Además, si no puede unificar todas las protecciones de CASB y DLP en una sola plataforma, ha complicado demasiado las cosas. Sin una visión única de la plataforma, tendrá una política desarticulada, brechas de seguridad y una mayor propensión a cometer costosos errores de configuración.

### Lo que debe saber

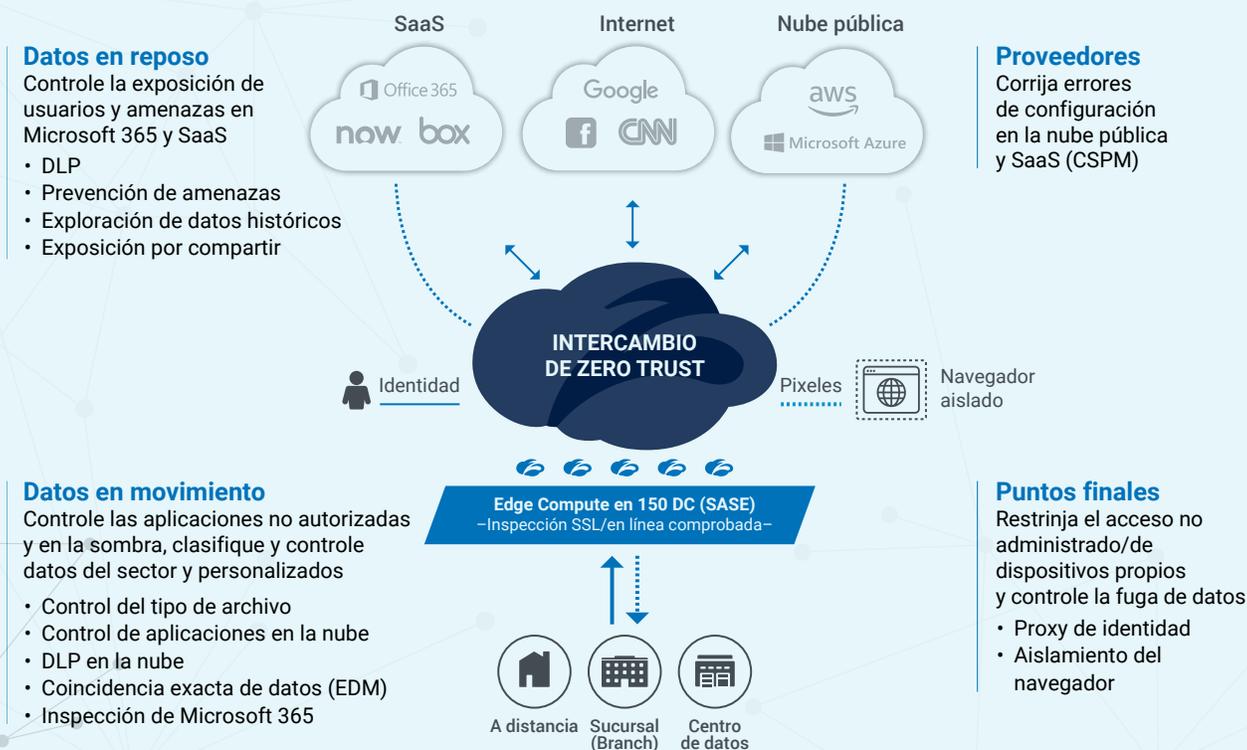


Para todos los canales de datos clave, en movimiento, en reposo, en los puntos finales y en los proveedores de nube, una plataforma unificada mejorará drásticamente la robustez de su política y simplificará sus flujos de trabajo.



## El modo de Zscaler

Debido a que todos los servicios en la nube de Zscaler están integrados en una arquitectura de nube en línea especialmente diseñada, todos los servicios trabajan juntos en armonía para unificar la política y optimizar la protección de sus canales de datos en la nube.



## He aquí cómo funciona:

**Datos en movimiento:** La inspección en línea de nivel empresarial es esencial para ofrecer protección de datos en tiempo real. Con la nube en línea de Zscaler, diseñada especialmente, puede seguir a todos los usuarios fuera de la red, y dentro de SSL. Clasifique y bloquee rápidamente los datos importantes, sin importar a dónde se dirijan, y bloquee las aplicaciones en la nube no autorizadas.

**Datos en reposo:** A medida que sus usuarios adoptan sus aplicaciones en la nube, debe verificar que estén tomando las decisiones correctas. Con el CASB fuera de banda de Zscaler, puede controlar fácilmente el uso compartido inadecuado de archivos en aplicaciones de Microsoft 365, como SharePoint y OneDrive, al tiempo que analiza los repositorios de archivos en busca de problemas de DLP y malware.

**Puntos finales:** Este canal trata de asegurar que solo las personas adecuadas tengan acceso a sus datos. Con el control de acceso a dispositivos propios, puede hacer una búsqueda rápida de SAML/SSO y bloquear el acceso no autorizado a los recursos de Microsoft 365. Además, Zscaler Cloud Browser Isolation le ayuda a prevenir la fuga en dispositivos no administrados (propios), ya que hace que los datos en los puntos finales sean solo píxeles. Esto significa que un contratista puede ver e interactuar con los datos, pero no los podrá guardar, descargar, copiar y pegar. Esto garantiza que nada se escape del dispositivo después de la sesión.

**Proveedores:** La desconfiguración accidental de las aplicaciones en la nube es una de las causas más comunes de la exposición de datos, lo que cuesta a las empresas tiempo y dinero. Zscaler Cloud Security Posture Management (CSPM) identifica y resuelve automáticamente las configuraciones erróneas de las aplicaciones en SaaS, IaaS y PaaS, para que su riesgo de pérdida de datos se reduzca y pueda mantener el cumplimiento.

## Resumen

La nube y la movilidad han cambiado el modo en que las empresas hacen negocios y la manera de trabajar de los empleados. Los datos se manejan de manera diferente ahora, por lo que deben protegerse de manera diferente. Los dispositivos de seguridad ya no ofrecen una protección adecuada para sus datos en el mundo actual. Necesita una plataforma de seguridad en la nube, con una base SASE, que proteja sus datos dondequiera que estén. Necesita Zscaler.

Vea nuestro CASB/DLP en línea en acción

[youtube.com/watch?v=R88TINEMgGE](https://www.youtube.com/watch?v=R88TINEMgGE)

Vea nuestro CASB fuera de banda en acción

[youtube.com/watch?v=1KtoW-IXgMs](https://www.youtube.com/watch?v=1KtoW-IXgMs)

Póngase en contacto con nosotros o reserve una demostración personalizada

[zscaler.com/company/contact](https://www.zscaler.com/company/contact)

### Acerca de Zscaler

Zscaler acelera la transformación digital con Zero Trust Exchange, una plataforma basada en SASE que proporciona conexiones rápidas y seguras entre usuarios, dispositivos y aplicaciones en cualquier red.

