# 3 Requisitos esenciales para una protección inmejorable de los datos

¿Quiere un mejor CASB y un DLP más fuerte? Tiene que empezar con la base correcta.

Cualquiera que trabaje en TI o seguridad de red le dirá: la protección de datos solía ser mucho más fácil cuando todos los datos estaban en el centro de datos y sus empleados estaban trabajando en la oficina. Pero los tiempos definitivamente han cambiado.

Ahora, sus datos han salido del centro de datos y están en todas partes, repartidos en cientos de aplicaciones de la nube. Y sus empleados están adoptando el trabajo remoto fuera de la red corporativa y lejos de sus controles de seguridad. Y por si eso no fuera suficientemente problemático, la mayoría del tráfico de Internet está encriptado y es difícil de inspeccionar, por lo que los malhechores esconden sus amenazas allí. Y sus empleados están utilizando redes no seguras o dispositivos no administrados, lo que abre sus datos a aún más oportunidades de exposición.

En este nuevo mundo feliz, las organizaciones necesitan una plataforma de protección de datos que se construyó desde el principio para la nube y la movilidad y debería incluir estos requisitos esenciales.

## Información relevante

La protección de sus datos con un CASB y un DLP será tan buena como la arquitectura sobre la que se asienta. Es esencial entender la receta del éxito.

# Requisito esencial n.º 1:

## Insista en una arquitectura SASE construida ex profeso

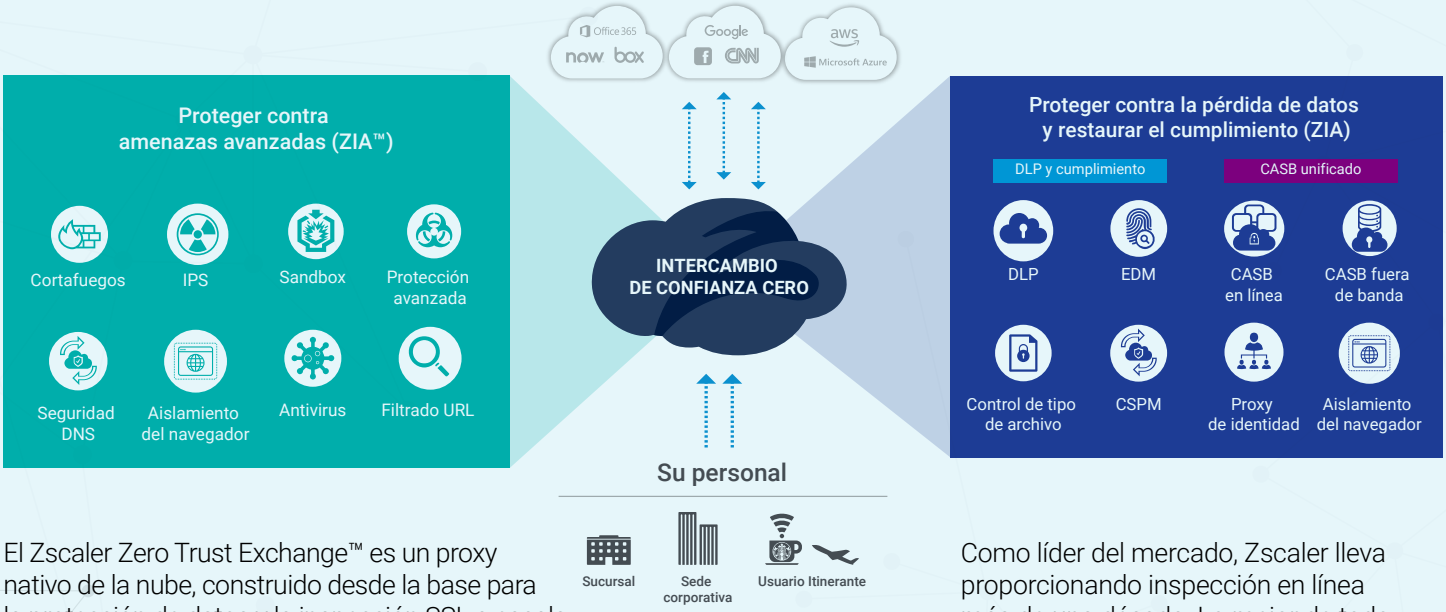
Con la nube y la movilidad, los dispositivos de seguridad no pueden estar en todas partes. Cuando los usuarios se caen de la red, se queda ciego y sus usuarios y datos quedan expuestos. Además, para ofrecer capacidades de agente de seguridad de acceso a la nube (CASB) y protección contra la pérdida de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

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

### Información relevante

Crear una arquitectura de protección de datos en línea de nivel empresarial que se escale a través de SSL no es fácil. Confíe su tráfico exclusivamente a un proveedor con la mayor experiencia, un historial probado y SLA de grado empresarial.

## El modo Zscaler™




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

Como líder del mercado, Zscaler lleva proporcionando inspección en línea más de una década. Lo mejor de todo es que, debido a que DLP, CASB y todos los demás servicios de seguridad están integrados, se obtiene una política simplificada y un enfoque unificado de la protección de datos y amenazas.

## Requisito esencial n.º 2:

Una mejor protección de datos requiere el mejor contexto

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

Era fácil en los viejos tiempos: los usuarios accedían al correo electrónico desde un servidor de Exchange o solo tenía unos pocos servidores de archivos. Todo lo que necesitaba para tomar decisiones informadas estaba ahí y era fácil de acceder.

Sus datos se mueven a través de cientos de canales, desde aplicaciones en la nube a nubes públicas hasta plataformas de intercambio de archivos.
Y todo el contexto que necesita en esos canales se oculta dentro de la encriptación SSL.

### Información relevante

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

## El modo Zscaler™

Cuando se trata de 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 en TODO su tráfico SSL, dando a las empresas un tesoro oculto de contexto.

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


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

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

# Requisito esencial n.º 3:

## Exigir una plataforma unificada que proteja todos los canales

La protección de sus datos contra la fuga y la exfiltración requiere que la seguridad esté en todos los lugares donde se encuentren sus datos. Si no puede controlar todos los canales, sus datos son vulnerables y están expuestos a posibles amenazas.

Además, si no puede unificar todas las protecciones CASB y DLP en una sola plataforma, ha hecho las cosas demasiado complejas. Sin una sola vista de la plataforma, termina con una política desarticulada, lagunas de seguridad y una mayor propensión a cometer costosos errores de configuración.

### Información relevante

Para todos los canales de datos clave (en movimiento, en reposo, en puntos finales y proveedores de nubes) una plataforma unificada mejorará drásticamente la solidez de sus políticas y simplificará sus flujos de trabajo.

## El modo Zscaler™

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

**Datos en reposo**
Control de usuario y exposición a amenazas en Microsoft 365 y SaaS

- DLP
- Prevención de amenazas
- Escaneos de datos históricos
- Compartir la exposición


**Proveedores**
Remediar las malas configuraciones de en la nube pública y SaaS (CSPM)

**Datos en movimiento**
Controlar las aplicaciones de sombra no autorizadas y clasificar y controlar la industria y los datos personalizados

- Control del tipo de archivo
- Control de la aplicación de nube
- DLP de nube
- Coincidencia exacta de datos
- Inspección de Microsoft 365

**Puntos finales**
Restringir no administrado/BYOD acceso y control fuga de datos

- Proxy de identidad
- Aislamiento del navegador

**Así es como funciona:**

**Datos en movimiento:** La inspección en línea de grado empresarial es esencial para la protección de datos en tiempo real. Con la nube en línea construida ex profeso por Zscaler, puede seguir a todos los usuarios fuera de la red y dentro de SSL. Rápidamente clasifica y bloquea datos críticos, sin importar hacia dónde se dirigen y bloquea aplicaciones de nube no autorizadas.

**Data en reposo:** A medida que sus usuarios adoptan sus aplicaciones en la nube, debe verificar que estén tomando las decisiones correctas. Con Zscaler CASB fuera de banda, puede controlar fácilmente el uso compartido inadecuado de archivos en aplicaciones de Microsoft 365, como SharePoint y OneDrive, mientras que también se analizan los depósitos 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 de BYOD, puede hacer una rápida búsqueda SAML/SSO y bloquear el acceso no autorizado a los recursos de Microsoft 365. Además, Zscaler Cloud Browser Isolation le ayuda a prevenir fugas en los dispositivos no gestionados (BYOD), ya que muestra los datos de los puntos finales solo como píxeles. Esto significa que un contratista puede ver e interactuar con los datos, pero no podrá guardar, descargar o copiar y pegar los datos. Esto asegura que nada se aleje del dispositivo después de la sesión.

**Proveedores:** La configuración errónea accidental de las aplicaciones en la nube es una de las causas más comunes de la exposición de datos, que cuesta tiempo y dinero a las empresas. Zscaler Cloud Security Posture Management (CSPM) identifica y remedia automáticamente las malas configuraciones de las aplicaciones en SaaS, IaaS y PaaS, de modo que su riesgo de pérdida de datos se reduce y puede mantener el cumplimiento.

## Resumen

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

Vea nuestro CASB/DLP en línea en action
**youtube.com/watch?v=R88TlNEMgGE**

Vea nuestro CASB fuera de banda en action
**youtube.com/watch?v=1KtoW-IXgMs**

Contacte con nosotros o reserve una demo personalizada.
**zscaler.com/empresa/contacto**

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



**Zscaler, Inc.**
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
**www.zscaler.com**