# El nuevo estándar de confianza

## Un paradigma para las relaciones tecnológicas de confianza del futuro

# Contenido

# Resumen ejecutivo

¿Sus clientes pueden confiarle sus datos? ¿Cómo lo saben?

La confianza solía reducirse a un apretón de manos. Una promesa de una persona a otra. Pero los negocios se han vuelto demasiado complejos para basar la confianza únicamente en las relaciones personales. La confianza del cliente depende de la seguridad y la transparencia de toda la organización: sus productos, servicios, personal, procesos, ética y valores, sistemas internos, proveedores y contratistas. Que los clientes puedan confiar en usted depende no solo de sus políticas, sino también de los proveedores de sus proveedores. No solo de su ciberseguridad, sino también de lo que hace cuando se produce una vulneración. No solo de cómo almacena los datos privados de los clientes, sino también de cómo responde a una solicitud de una autoridad extranjera un viernes por la tarde.

En la economía digital actual, un parámetro objetivo para evaluar la confianza es fundamental. Requiere total transparencia. Los datos que fluyen a través de Internet (a veces hacia la nube de un proveedor) incluyen datos confidenciales, como credenciales de inicio de sesión, números de identificación gubernamental, información financiera, secretos comerciales, planes comerciales y detalles críticos de la infraestructura. Si la información confidencial llega a las manos equivocadas, las consecuencias pueden incluir violaciones a la privacidad, pérdida de propiedad intelectual, interrupciones en las operaciones e ingresos, apagón e incluso amenazas a la seguridad nacional.

**Ha llegado el momento de un nuevo estándar de confianza.** Es una recopilación de lo que hemos escuchado en conversaciones con miles de clientes en todo el mundo durante años. El nuevo estándar de confianza es un marco para las expectativas y la responsabilidad, donde las empresas y sus clientes pueden acordar nuevas reglas para las relaciones digitales de confianza.

La confianza no se trata de una cosa, como el cifrado, la certificación o la supervisión de la cadena de abastecimiento. Se trata de una combinación de cosas. Las que sean seguramente cambiarán con el tiempo en respuesta a las expectativas cambiantes de los clientes, la tecnología, las ciberamenazas y la gestión internacional de datos. Siga leyendo para conocer los elementos clave del nuevo estándar de confianza hoy mismo.

**Los componentes básicos del nuevo estándar de confianza**

- **Evitar la intrusión.** Filosofía de Zero Trust
- **Gestionar el riesgo del proveedor.** Cadena de suministro confiable
- **Respetar los derechos de datos.** Expectativas y regulaciones
- **Ser abierto sobre lo que hace.** Transparencia
- **Demostrarlo.** Certificaciones y pruebas periódicas de penetración

*"Nuestros clientes no solo necesitan innovación más que nunca, sino que también quieren partners en los que puedan confiar".*

**Chuck Robbins**
Presidente y director ejecutivo, Cisco

# Evitar la intrusión: filosofía de “Zero Trust”

## Verifique cada conexión, cada dispositivo en toda oportunidad

Escéptico, curioso, orientado al detalle. Estos son los requisitos laborales de los profesionales de seguridad, ya que la confianza comienza con una buena sospecha. Como su nombre lo indica, Zero Trust es una filosofía para “nunca confiar, siempre verificar”.

Al seleccionar una empresa, una mentalidad Zero Trust implica cuestionar las prácticas y políticas de seguridad de la organización. El nuevo estándar de confianza indica que tiene derecho a pedir, y esperar, respuestas claras. Si su empresa maneja datos confidenciales, una mentalidad Zero Trust significa siempre cuestionar sus suposiciones. ¿Los clientes son quienes dicen ser? ¿Sus dispositivos son seguros? ¿La aplicación A tiene un motivo válido para hablar con la aplicación B?

El enfoque de décadas de control de acceso y una red privada virtual (VPN) ya no se sostiene. Se supone que se puede confiar en cualquier dispositivo que se conecte desde dentro de la red corporativa. Y que una vez que un usuario y un dispositivo pasan un punto de control, es seguro permitirles conectarse a varias aplicaciones sin tener que volver a autenticarse. Hoy en día, ninguno de estos supuestos es válido. Una computadora portátil o tableta personal utilizada para el trabajo podría haber contraído una infección en el hogar. Un dispositivo que está limpio a las 8:00 a. m. puede verse comprometido a las 8:03 a. m. después de un ataque de suplantación de identidad (phising). Con el almacenamiento y el procesamiento de datos distribuidos en el perímetro de la red, ya no hay un castillo central para rodear con un foso. Además, más allá de autorizar conexiones de dispositivos de usuario a servidores, los equipos de TI también deben verificar si se permiten conexiones entre aplicaciones, dispositivos y sensores. Caso interesante: algo que parece una cámara de seguridad no tiene por qué conectarse a una base de datos de clientes.

El enfoque moderno para el control de acceso es una arquitectura de confianza cero. Trata todos los recursos como si fueran externos. Verifica la confianza antes de cada intento de acceso. Y otorga acceso solo al recurso requerido. Esto es así incluso si la solicitud proviene de la oficina del CEO. Incluso si el estado de seguridad del dispositivo se verificó hace 30 segundos cuando se conectó a una aplicación diferente.

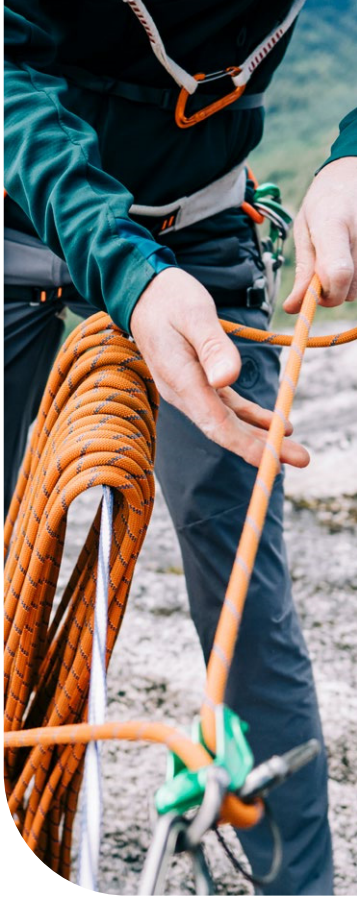
## Principios de Zero Trust

- Priorizar la experiencia del cliente. La autenticación no debería ser una carga. Los usuarios necesitan un acceso conveniente a las aplicaciones en las instalaciones y en la nube para realizar su trabajo.
- Verificar continuamente que los usuarios, los dispositivos y las aplicaciones sean de confianza.
- Usar el aprendizaje automático para identificar los intentos de inicio de sesión que se desvían del comportamiento típico del usuario. Los falsos positivos suceden, por lo que sopese los riesgos de bloquear intentos de acceso legítimos.
- Adaptar la solidez de la política de seguridad de la aplicación a la confidencialidad de los datos. Esto requiere una clasificación de datos precisa. También requiere una comprensión de cómo se ve el tráfico de aplicaciones normal para poder detectar las desviaciones.
- Conexiones seguras entre diferentes componentes de la aplicación, como la lógica de la aplicación y la base de datos.
- Hacer que sea más difícil para los atacantes con acceso a un servidor pasar a otros. Las técnicas incluyen segmentación de la red, autenticación y cifrado fuertes, y marcado de dispositivos de confianza.

> *"La mayoría de los proveedores de la nube ya verifican el estado de la seguridad del dispositivo antes de otorgar acceso. El nuevo estándar de confianza identifica inmediatamente los intentos sospechosos que predicen malos resultados y luego automatiza la respuesta".*
>
> **Den Jones**
> Director sénior de seguridad empresarial, Cisco

> *"Una arquitectura de Zero Trust es una inversión importante para comprender y administrar mejor el riesgo a través de controles y puntos críticos de gestión y para mejorar constantemente con el tiempo con aprendizaje automático".*
>
> **Brad Arkin**
> Vicepresidente sénior, director de seguridad y confianza, Cisco

# Gestionar el riesgo del proveedor



## Confíe en que el proveedor ha desarrollado una cadena de abastecimiento confiable

Al comprar un automóvil, usted confía en que el fabricante tome medidas razonables para evaluar la calidad de las piezas del proveedor, como los frenos y los cinturones de seguridad. Asimismo, los clientes esperan que sus proveedores de servicios conozcan todos los componentes de sus productos y tomen medidas razonables para detectar y mitigar las vulnerabilidades que podrían conducir a la manipulación de datos, el espionaje, la interrupción y la falsificación.

Es una tarea difícil. Los proveedores de servicios en la nube suelen utilizar software de terceros para el procesamiento de pagos, la autenticación, la administración de datos y el almacenamiento, etc. Incluso el código patentado generalmente incluye componentes de código abierto aportados por personas de todo el mundo, y muchos de estos componentes tienen varios componentes agrupados.

Lo que es “razonable” para los controles de proveedores sigue evolucionando. Los factores desencadenantes del cambio incluyen nuevos tipos de amenazas, nuevas prácticas de la industria y avances en ciberseguridad.

## Prácticas recomendadas de la cadena de suministro

**Defenderse de la modificación.** Ejecute un programa para asegurarse de que las soluciones que llevan su nombre sean genuinas, funcionen como los clientes les indican y no sean controladas o accesibles por terceros desconocidos.

**Requerir que los proveedores cumplan con los estándares correctos.** Trabaje con sus proveedores externos para evaluar, supervisar y mejorar sus prácticas de seguridad. Los estándares de la industria son un buen punto de partida. Algunos ejemplos incluyen NIST 800-53 para controles de seguridad y privacidad, ISO/IEC 27001 para administración de seguridad de la información, ISO 27018 para proteger información de identificación personal (PII) en nubes públicas e ISO 27701 para administración de información de privacidad.

**Establecer una cadena de confianza.** Lo fundamental es exigir a los proveedores de software y hardware que documenten el linaje o la procedencia de sus productos. Como un pasaporte, este registro muestra todas las partes en las que ha estado el producto, desde el diseño y el desarrollo hasta la fabricación y la entrega. Los proveedores de software documentan dónde se creó el código, quién lo firmó, los componentes utilizados para la administración de identidades, dónde se compiló el código, etc. Los proveedores de hardware registran detalles como el número de serie para cada montaje de placa de circuito impreso y quién lo embaló.

**Generar confianza en el contrato.** Responsabilice a los proveedores de los mismos estándares de seguridad y privacidad que usted se compromete a respetar. Defina requisitos para las pruebas de vulnerabilidad y la generación de informes. Incluya lenguaje en el contrato para proteger los datos de los clientes después de la finalización de una relación con el proveedor, por ejemplo, exigiendo la devolución o destrucción de esos datos.

**Probar las integraciones con productos propios o de otros proveedores.** Asegúrese de que la integración no haya creado una nueva vulnerabilidad.

**Realizar auditorías periódicas, incluidas pruebas de vulnerabilidad.** Trabaje con el proveedor para crear un plan de identificación y corrección de vulnerabilidades. Escriba el plan de respuesta en el contrato.

# Respetar los derechos de datos

## Adelántese a las cambiantes expectativas de los clientes y las regulaciones gubernamentales

Los clientes esperan que los proveedores mantengan sus datos protegidos y seguros, este es un requisito fundamental de confianza en el mundo digital. Más allá de eso, los clientes desean estar informados sobre cómo se recopilan, usan y administran sus datos, y, en última instancia, desean tener el control de sus datos. Este deseo de visibilidad y control abarca cualquier relación de datos, desde una persona que participa en las redes sociales hasta un hospital que almacena registros médicos y una empresa que utiliza servicios de colaboración basados en la nube. Cada vez más, los consumidores tomarán decisiones sobre sus proveedores teniendo en cuenta la privacidad y la transparencia.

### Expectativas del cliente

Para confiar en su proveedor, los clientes generalmente quieren garantías en estos puntos:

- Nuestro contenido es nuestro
- Está sujeto a las mismas leyes que nosotros
- Es accesible solo para las personas que autorizamos y esperamos

Los clientes dependen y, en general, son responsables de las regulaciones gubernamentales destinadas a proteger la privacidad. La gestión internacional de datos[1] se refiere a las leyes, regulaciones y normas globales colectivas asociadas con la protección, la privacidad, el intercambio y el uso de datos. El nuevo estándar de confianza sostiene que los proveedores de servicios deben ser transparentes sobre su enfoque de la soberanía de los datos, es decir, el concepto de que los datos están sujetos a las leyes del país donde se recopilan los datos. Se han promulgado leyes de privacidad en más de 130 países que buscan establecer el estándar de atención aplicable a los datos personales recopilados dentro de sus fronteras. Algunos ejemplos son el Reglamento General de Protección de Datos (RGPS) de la UE, la Ley de protección de datos personales de la India y la Ley de protección de datos personales de Tailandia.

Si bien los aspectos específicos de estas leyes varían, las preocupaciones detrás de ellas son universales. Una de ellas es la creencia, verdadera o no, de que los datos son más seguros en el propio país, protegidos por las leyes de su país. Otra es la preocupación de que las autoridades encargadas de hacer cumplir la ley, ya sean extranjeras o nacionales, puedan obligar a un proveedor de servicios a entregar los datos del cliente sin su conocimiento o participación. Las empresas que utilizan servicios en la nube deben sopesar estos riesgos con los beneficios de la nube: adopción rápida, escalabilidad e innovación continua.

## Formas de limitar la exposición de datos de clientes

**Aplicar controles técnicos.** Minimice los datos que recopila y guárdelos solo el tiempo que la empresa necesite o los requisitos legales. Utilice un cifrado y un control de acceso fuertes para proteger el contenido del cliente.

**Utilizar controles legales.** Si los gobiernos solicitan acceso a los datos del cliente, primero intente redirigir al solicitante hacia el cliente o propietario de los datos. Invoque el proceso legal disponible para impugnar las solicitudes que invadan de manera injustificada la privacidad u otros derechos del cliente.

**Ser estratégico con respecto a las ubicaciones de los centros de datos.** Considere cómo afectará a los clientes la ubicación de los centros de datos en diferentes partes del mundo. Si se hacen correctamente, los controles de gestión de datos pueden mejorar la experiencia general del usuario, por ejemplo, al darles a los clientes algo de control sobre su contenido y cómo administran los datos. Si es posible, considere permitir que los clientes elijan la región donde se almacenan sus datos para cumplir con sus requisitos de soberanía, privacidad o latencia.

## El futuro de los datos: soberanía digital

La misma tecnología que permite nuestro mundo interconectado y alimentado por Internet también ha creado complejidades sobre la soberanía de los datos. Los países están reaccionando a la digitalización de sus economías y al vasto tesoro de datos que crea, confiando en el concepto de soberanía para afirmar la autoridad suprema sobre los datos para garantizar el control y la protección de sus datos. “Mis datos, mi ley” ahora es la nueva norma. En todo el mundo, los nuevos marcos de datos apuntan a las barreras nacionales para el movimiento, el acceso, el uso y el almacenamiento de datos.

Aunque sea bien intencionado, este enfoque estrecho amenaza con disminuir los beneficios económicos que se hacen posibles gracias a la tecnología moderna. Debe surgir un marco nuevo y con visión de futuro, que refuerce los derechos de los propietarios de datos y la soberanía nacional, pero que dependa de la tecnología, no solo de la ley, para lograr ese objetivo. El cifrado avanzado, la computación confidencial, la ofuscación y otras técnicas y tecnologías de protección de intimidad (PET) conllevan la promesa de crear un modelo para la soberanía digital dentro de una Internet segura, abierta y dinámica.

[1]Principios de gestión de datos para la economía digital global, Centro de estudios estratégicos e internacionales

# Ser transparente

## Divulgar toda la información necesaria para que los clientes tomen decisiones informadas

**La transparencia ocurre cuando los hechos materiales sobre una empresa se ponen a disposición de los clientes de manera oportuna y eficiente.**

La transparencia va más allá del cumplimiento de las reglamentaciones sobre divulgaciones. Es abierto sobre cómo maneja las operaciones comerciales, el contenido del cliente y la información de privacidad, que incluye:

- Qué datos recopila y cómo los utiliza y protege
- Cómo respeta los derechos de los interesados
- Detalles clave de sus políticas sobre divulgación de violaciones y vulnerabilidades de seguridad
- Cómo responde a las solicitudes de datos del gobierno
- Cuáles son sus planes de continuidad comercial

En general, una empresa transparente confía en que su manejo de datos sea justo, ético y responsable. Toma las medidas adecuadas para proteger los datos de los clientes y respetar la privacidad. Y está dispuesto a ser público sobre las políticas, los procesos y la tecnología que utiliza para proteger los datos. Los titulares recientes han hecho que las empresas sean más conscientes de los costos financieros y de reputación de la seguridad inadecuada.

## Formas de aumentar la transparencia

**Facilitar a los clientes la búsqueda de la información.** Pregunte a los clientes qué es lo que quieren saber y luego ofrézcalo sin que lo busquen. Utilice un lenguaje simple y claro.

**Divulgar públicamente todas las vulnerabilidades críticas.** Esto se aplica independientemente de que la vulnerabilidad sea descubierta internamente o por un tercero. Ayude a los clientes a comprender y gestionar los riesgos.

**Notifique a todas las personas materialmente afectadas por una violación al mismo tiempo.** El derecho a la transparencia se aplica por igual a cada cliente afectado, sin importar su tamaño o sector.

**Abogar por los clientes cuando los gobiernos solicitan datos.** Demuestre que cumple con la ley y que intentará proteger la información del cliente de solicitudes ilegales. Cuando esté legalmente permitido, notifique al cliente sobre la solicitud. Siempre que sea posible, la solicitud debe ir directamente al cliente, no al proveedor de servicios de TI. Cuando su cliente lo solicite, ayúdelo a conservar o producir el contenido solicitado.

> *"Cuando surgen problemas de seguridad, es importante que los clientes comprendan cómo se abordarán. Cumplir esta promesa requiere un proceso estricto para administrar la recepción, la investigación y el reporte de la información sobre vulnerabilidades de seguridad".*
>
> **Anthony Grieco**
> Vicepresidente, director general de seguridad de la información, Cisco

> *"La transparencia comienza con la cultura. Es una expectativa que los empleados serán responsables por la manera en que interactúan con los clientes y el mundo en general".*
>
> **Noelle Warburton**
> Directora de comunicaciones estratégicas de confianza y seguridad, Cisco

# Demostrarlo

## Demostrar cumplimiento con la verificación independiente de terceros

Los otros pilares del nuevo estándar de confianza son los compromisos críticos: la transparencia, un enfoque Zero Trust para el acceso a la red, la soberanía de los datos y una cadena de abastecimiento confiable. Las certificaciones son la prueba de que la organización cumple con esos compromisos. Las certificaciones comunes de seguridad de productos incluyen el estándar internacional ISO/IEC 27001, los controles de sistemas y organizaciones (SOC 2) en América del Norte, FedRAMP en el sector público de EE. UU. y computación en la nube Catálogo de controles de cumplimiento (C5) en Alemania.

Para obtener certificaciones, los proveedores de productos y servicios de TI deben someterse a una auditoría por un tercero acreditado e independiente, a menudo una empresa de contabilidad. En los Estados Unidos, por ejemplo, los auditores reciben la acreditación de la Junta Nacional de Acreditación ANSI-ASQ (ANAB). Las certificaciones de privacidad demuestran a los clientes, los reguladores y otras partes interesadas que el proveedor mantiene principios de privacidad internacionalmente reconocidos y respeta los derechos fundamentales de los interesados al manejar su PII. Las certificaciones reconocidas incluyen las Reglas corporativas vinculantes de la UE, las Reglas de privacidad transfronterizas de APEC, el Reconocimiento de privacidad de APEC para procesadores y el Escudo de privacidad de EE. UU. (invalidado para las transferencias de la UE pero reconocidas por los EE. UU.). Estas certificaciones son administradas y verificadas por reguladores de privacidad o agentes de responsabilidad independientes aprobados por el regulador.

## Las certificaciones son cada vez más importantes en un mundo en la nube

Cuando compra hardware o software para implementar en su propio centro de datos, los datos de la empresa o del cliente nunca salen de su edificio. Solo debe confiar en que el producto hará el trabajo. Cuando se suscribe a un servicio en la nube, en cambio, los datos de clientes y empresas salen de sus instalaciones. Reside en los servidores del proveedor y viaja a través de la red del proveedor. Ahora también debe confiar en que el proveedor de servicios maneja los datos de los clientes de manera responsable. Realiza parches y actualizaciones a tiempo. Cumple con los requisitos de soberanía de datos. Administra las vulnerabilidades. Cumple con los acuerdos de nivel de servicio para disponibilidad. Respeta los derechos de privacidad de los interesados. La evolución constante de los servicios en la nube también incluye la evolución de los controles de seguridad. Las certificaciones anuales proporcionan una medida uniforme del perfil de seguridad de un proveedor y ofrecen a los clientes una manera más fácil de tomar decisiones informadas.

*"Las certificaciones de privacidad son importantes. El 90 % de las organizaciones encuestadas indicó que las certificaciones de privacidad de ISO, APEC y la UE son factores importantes que afectan la selección de proveedores y las decisiones de compra".*

**Harvey Jang**
Vicepresidente, director general de privacidad, Cisco

Fuente: Estudio de parámetros de privacidad de datos de Cisco de 2021

# Conclusión

*El nuevo estándar de confianza* afirma que la confianza ya no se trata solo de la intuición. Ya no es una declaración de aspiraciones en la página web de valores corporativos. Habiendo visto los riesgos cuando los datos confidenciales llegan a las manos equivocadas, los clientes actuales han elevado el nivel. Quieren garantía tangible de que las empresas con las que trabajan tienen el compromiso, la tecnología y los procesos para proteger sus datos. Cuán bien las empresas superen el desafío afectará no solo sus propios resultados, sino también la continuidad de la infraestructura crítica de la que depende la sociedad.

En Cisco, el nuevo estándar de confianza ha cambiado la forma en que hacemos negocios. Estamos escuchando lo que nuestros clientes desean, implementando la tecnología, los procesos, las políticas y las personas para la prestación y trabajando junto a ellos para planificar un futuro digital con la base de confianza.

Algunas de nuestras acciones: hemos desarrollado una arquitectura de Zero Trust. Redactamos nuestros contratos con los proveedores para hacerlos responsables de los mismos estándares de seguridad y privacidad que nos hemos comprometido a mantener. Publicamos y seguimos un enfoque basado en principios para las solicitudes de datos del gobierno. Publicamos Fichas de datos de privacidad para productos y servicios que procesan Datos personales, respondiendo preguntas comunes de los clientes con suficiente detalle para que los clientes decidan la mejor manera y la más segura de utilizar el producto para satisfacer sus necesidades. Y obtenemos certificaciones de seguridad y privacidad para que los clientes no necesiten basar su confianza en nuestros productos únicamente en la fe.

Iniciado por los clientes, el nuevo estándar de confianza es un desarrollo positivo para nuestro mundo cada vez más digital. La declaración explícita de lo que los clientes esperan de las empresas con las que hacen negocios convierte la confianza de un sentimiento en un parámetro objetivo.

Para obtener más información sobre el compromiso de Cisco con la confianza, visite trust.cisco.com