



# Opinión de los expertos: Seguridad para los servicios financieros

Marco estratégico para abordar las crecientes amenazas

El panorama de una realidad cada vez más conectada ha cambiado el juego para los servicios financieros. Ahora existe un mundo de oportunidades, pero esto conlleva nuevos riesgos. Hay más datos (y más acceso a los mismos) en más lugares. Los clientes exigen con mayor frecuencia pagos y transacciones más sencillos. Y esto aumenta el panorama de riesgos.

Ahora más que nunca, usted necesita una seguridad avanzada para proteger a sus clientes y a su marca. Si trabaja con los líderes de seguridad y de TI, usted podrá encontrar las soluciones correctas para sus necesidades únicas de negocios y para innovar, mientras crea una experiencia de mayor conexión para sus clientes.

*Aunque diariamente se disparan miles de alertas de seguridad, solo el*

**55%**

*de estas son investigadas por las organizaciones de servicios financieros.<sup>1</sup>*



**1**

Esté un paso adelante de las amenazas de seguridad.

**2**

Proteja los datos y mantenga satisfechos a sus clientes.

**3**

Simplifique el cumplimiento y enfóquese en la innovación.

**4**

Comience: 5 pasos para tener una mejor seguridad.

# 1

## Esté un paso adelante de las amenazas de seguridad.

La industria de los servicios financieros está rebasada en el tema de la ciberseguridad. Los clientes buscan un acceso simple a sus datos, y el aumento en los servicios basados en la nube y en la tecnología del IoT (hay cada vez más dispositivos en más lugares) implica una complejidad que va en aumento.

55%

de las organizaciones han tenido que enfrentarse al escrutinio público debido a una falla de seguridad.<sup>1</sup>

Más de la mitad de los ataques resultan en daños por un valor de \$500,000 dólares o más.<sup>1</sup>

\$500 mil

### Tome una postura clara

Asegúrese de que el departamento de TI tenga un enfoque integral de seguridad para:

- Identificar y bloquear las amenazas rápido: incluso en el tráfico encriptado.
- Encontrar y mitigar las amenazas rápidamente para minimizar sus efectos.

### Para saber más.

[Obtenga visibilidad y control para contrarrestar ataques avanzados >](#)

[Contrarreste los ataques avanzados con defensas avanzadas >](#)

## Seguridad de próxima generación

### Inteligencia líder contra amenazas de la industria

Cisco® Talos™ recurre a una amplitud y profundidad sin igual de análisis colectivos para capitalizar las tecnologías de Seguridad de Cisco.

- Detecta miles de millones de amenazas y las detiene en segundos.
- Entrega actualizaciones dinámicas de seguridad cada 3 a 5 minutos.
- Capitaliza la mejor protección con la mejor inteligencia contra amenazas.

## 2

## Proteja los datos y mantenga satisfechos a sus clientes.

Los clientes de hoy en día esperan tener un acceso ilimitado a sus datos, desde cualquier lugar, en cualquier dispositivo. Podría ser difícil alcanzar un equilibrio entre contar con una seguridad avanzada y ofrecer este nivel de flexibilidad.

57%

de las organizaciones de servicios financieros utilizan soluciones de al menos seis proveedores, y

29%

utilizan más de 10 proveedores.<sup>1</sup>

### Mejorar la administración de los accesos y el control

Ahora existe una manera más simple de lograr estos dos objetivos. Con una administración de acceso por identidad desde una sola ubicación central, el departamento de TI puede controlar de manera dinámica quién y qué tiene acceso a su red. Una solución integral, un proveedor y cero dolores de cabeza para el departamento de TI.

Para saber más.

[Simplifique el cumplimiento con políticas fortalecidas >](#)

[Segmente los activos cruciales de negocios en un “cuarto de seguridad” >](#)

## Seguridad de próxima generación

### Visibilidad superior y cumplimiento

El 82 por ciento de las compañías desean un portafolio integrado de seguridad. Pero solo una compañía lo está desarrollando: Cisco. Nuestro portafolio de seguridad trabaja en conjunto, para que usted pueda estar más seguro y pueda responder de una forma más rápida.

- Contener amenazas en redes VPN, alámbricas o inalámbricas.
- Escalar y hacer cumplir las políticas en toda su red.
- Restringir los movimientos laterales de las amenazas.
- Ganar con inteligencia a las nuevas amenazas mediante la implementación de tecnologías de aprendizaje automático líderes en la industria.

[Ver video >](#)

# 3

## Simplifique el cumplimiento y enfóquese en la innovación.

Conforme las regulaciones sigan cambiando y expandiéndose, el cumplimiento se hace cada vez más difícil. No hay tiempo para avanzar con las iniciativas digitales de negocios, aunque la diferenciación competitiva dependa de ello.



Sin visibilidad en tiempo real, los atacantes pueden permanecer desapercibidos...

...y hasta el 20% de los dispositivos conectados permanentemente a la red no son detectados por los equipos de seguridad.<sup>1</sup> **20%**

### Implementar una red esencialmente ágil

Al implementar un modelo operativo sostenible y preparado para los cambios del futuro, su organización puede enfrentar los cambios de las necesidades de cumplimiento. Puede permanecer tranquilo y enfocado en la innovación que hará destacar a su negocio.

### Para saber más.

[Optimice su red de sucursales de venta al detalle >](#)

[Aprenda cómo la innovación afecta en el riesgo >](#)

## Seguridad de próxima generación

### DNA para servicios financieros

Digital Network Architecture de Cisco (Cisco DNA™) hace que la administración de la red sea más simple, inteligente y automatizada.

- Experiencias contextualizadas y personalizadas basadas en análisis en tiempo real.
- Una toma de decisiones más rápida, que convierte los datos en información útil en segundos, no en horas.
- Visibilidad de 360 grados de sus redes corporativas y de las sucursales.

[Descubra más >](#)

1. Cisco 2017 Midyear Cybersecurity Report, Cisco, julio de 2017.

# 4

## Comience: 5 pasos para tener una mejor seguridad.

Los productos integrados de seguridad de Cisco están diseñados para trabajar juntos desde un enfoque de arquitectura única. Obtenga la seguridad avanzada que necesita, con la flexibilidad que sus clientes desean, en un solo portafolio integral.

### ✓ 01

#### Proteja contra amenazas avanzadas.

Obtenga la tranquilidad que conlleva tener la [inteligencia contra amenazas líder del mercado](#).

### ✓ 02

#### Aumente la protección y el control.

NSS Labs menciona a Cisco como un líder constante por bloquear más amenazas con mayor rapidez que cualquier otro proveedor.<sup>1</sup>

### ✓ 03

#### Virtualice para conseguir visibilidad y velocidad.

La posibilidad de una violación de seguridad importante es de una en cuatro.<sup>2</sup> Obtenga la [visibilidad de red y el cumplimiento](#) que necesita.

### ✓ 04

#### Elija a un líder confiable.

A la mayoría de las organizaciones les toma 100 días detectar una amenaza. A Cisco le toma 4.6 horas.<sup>2</sup>

### ✓ 05

#### Obtenga ayuda de los expertos.

Encuentre la estrategia adecuada para su negocio con las opiniones de los expertos de los [Servicios de Seguridad de Cisco](#).



1. Test Methodology: Breach Detection Systems (BDS), NSS Labs, 2016.

2. 2017 Cost of Data Breach Study: United States, Ponemon Institute, junio de 2017.



## Comience: 5 pasos para tener una mejor seguridad.

### Obtenga ayuda de los expertos.

Imagine lo que podría hacer si tuviera otro par de ojos solo para administrar la seguridad. Con los Servicios de Seguridad de Cisco, usted obtendrá acceso a consultores y expertos técnicos que pueden ayudarle a evaluar su ambiente y determinar la estrategia de seguridad más eficaz.

[Para saber más sobre los Servicios de Seguridad >](#)



La compañía global de investigación IDC incluyó a Cisco dentro de los tres primeros lugares de FINTECH en 2017...

...por lograr un cambio genuino, mensurable y con visión de futuro.



*La ciberseguridad debe ser algo arraigado en el pensamiento de la gente sobre las nuevas capacidades y oportunidades de negocios. No puede ser solamente algo que los expertos en tecnología van a solucionar.<sup>1</sup>*

– Joe Nocera, líder de ciberseguridad en los servicios financieros, PwC

Nuestro portafolio de seguridad trabaja en conjunto, para que usted pueda estar más seguro y responder con mayor rapidez.

[Para comenzar >](#)

[Informe Anual de Ciberseguridad Cisco 2018 >](#)

1. "Cybersecurity in Financial Services," PwC. <https://www.pwc.com/us/en/industries/financialservices/research-institute/top-issues/cybersecurity.html>

Visite nuestro sitio

Únase a la conversación     

Oficinas Centrales en América: Cisco Systems, Inc. San José, CA

Oficinas Centrales en Asia Pacífico: Cisco Systems (USA) Pte. Ltd. Singapur

Oficinas Centrales en Europa: Cisco Systems International BV Amsterdam Holanda

Argentina: 0800 555 3456 • Bolivia: 800 10 0682 • Chile: 1230 020 5546 • Colombia: 1 800 518 1068 • Costa Rica: 0800 011 1137 República Dominicana: 866 777 6252 • El Salvador: 800 6600 • Guatemala: 1 800 288 0131 • México: 001 888 443 2447 • Panamá: 001 866 401 9664 • Perú 0800 53967 • Venezuela: 0800 102 9109

Cisco cuenta con más de 200 oficinas en todo el mundo. Las direcciones, los números de teléfono y fax están listados en el sitio de Cisco en la siguiente dirección web: [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

© 2018 Cisco y/o sus filiales. Todos los derechos reservados. Cisco, el logo de Cisco, Disco DNA y Talos son marcas registradas de Cisco y/o sus filiales en los Estados Unidos y otros países. Para ver una lista de las marcas de Cisco, consulte la página de Marcas registradas de Cisco en el sitio web de Cisco. Las marcas de terceros mencionadas son propiedad de sus respectivos dueños. El uso de la palabra "socio" no implica asociación entre Cisco y cualquier otra compañía. (1804R)