



# Cumplimiento normativo en el sector de los servicios financieros

5 objetivos empresariales clave



# Tabla de contenido

---

Simplificar el cumplimiento	<b>02</b>
Aumentar la productividad	<b>03</b>
Mejorar la atención al cliente	<b>04</b>
Gestionar los costes de seguridad y cumplimiento de forma eficaz	<b>05</b>
Crear resiliencia y confianza	<b>06</b>
Un banco internacional logra el cumplimiento de SWIFT en dos semanas	<b>07</b>
Conclusión	<b>08</b>

## Cuando mejora el cumplimiento normativo en los servicios financieros también mejora la experiencia del cliente, la productividad y el crecimiento.

En el vertiginoso mundo de los servicios financieros, resulta fundamental cumplir las normativas y mantener la resiliencia operativa. Este libro electrónico ofrece un enfoque estructurado para simplificar el cumplimiento, aumentar la productividad, mejorar la experiencia del cliente, gestionar los costes de seguridad de forma eficaz y generar resiliencia y confianza. Si bien el cumplimiento por sí solo no garantiza una seguridad total, sigue siendo una prioridad para los equipos ejecutivos, ya que si no se supera una auditoría puede haber interrupciones en el negocio y graves repercusiones económicas.

Los equipos de seguridad dedican mucho tiempo y recursos a las evaluaciones de cumplimiento. Además, el cambio a entornos digitales sin perímetro y el aumento del teletrabajo no hacen más que aumentar el desafío. Las instituciones financieras deben aislar sus entornos y acordonar sus activos regulados para satisfacer distintos requisitos, como el Estándar de Seguridad de Datos del Sector de las Tarjetas de Pago (PCI-DSS), el Reglamento sobre la Resiliencia Operativa Digital del sector financiero (DORA) y el sistema de la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT). Este libro electrónico proporciona información y estrategias para ayudar a una institución financiera a superar estas complejidades y alcanzar los siguientes **cinco objetivos empresariales clave**:



## Akamai para el sector financiero

En la actualidad, las marcas más importantes del ámbito de la banca, el mercado de capitales, los seguros y la tecnología financiera confían en Akamai para transformar una nube caótica, de rendimiento impredecible y plagada de amenazas ocultas, en un entorno seguro, fiable y rentable para los negocios.

### Entre nuestros clientes se incluyen:

Los **20** mayores servicios de corretaje

**17** de los **20** mayores bancos

**7** de las **10** mayores empresas de tecnología financiera

1



## Simplificar el cumplimiento

Al dividir las redes en perímetros más pequeños y aislar las cargas de trabajo individuales, las soluciones de microsegmentación pueden poner más límites en los entornos de cumplimiento, agilizar las auditorías reglamentarias y restringir el acceso a la información confidencial, al tiempo que ofrecen una visibilidad sin precedentes del tráfico de red y los flujos de datos.

### Reducción del entorno de cumplimiento

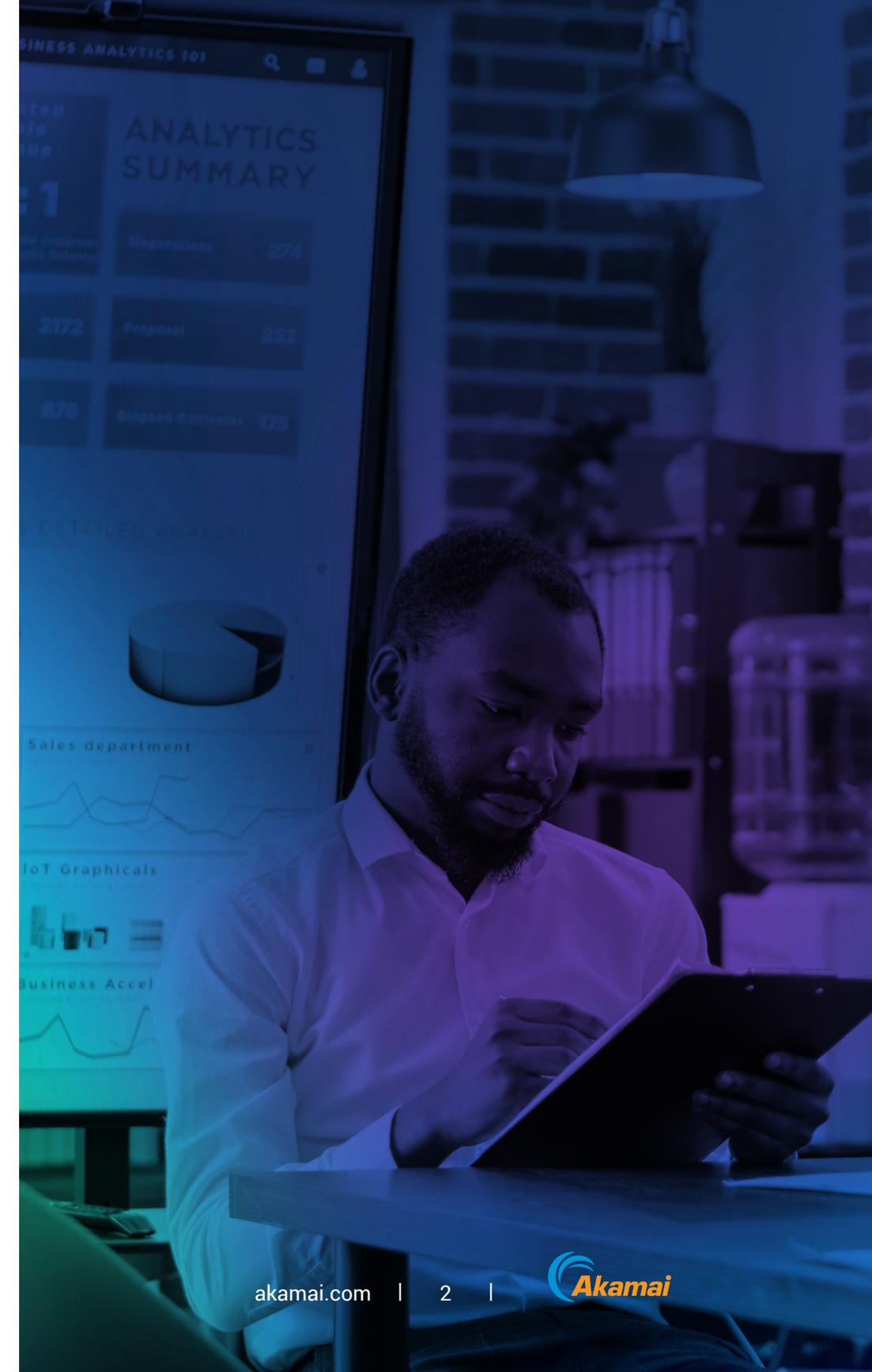
Segmentar los datos relacionados con el cumplimiento de otros activos de TI simplifica considerablemente las tareas relacionadas con dicho cumplimiento y reduce la complejidad y los costes. Las instituciones financieras pueden centrar sus actividades de cumplimiento en segmentos específicos de la red, lo que mejora la eficiencia y reduce los recursos necesarios.

### Optimización de las iniciativas sobre cumplimiento y los procesos de auditoría

La microsegmentación simplifica la labor de cumplir con las solicitudes y los procesos de auditoría al reducir el ámbito de los entornos de cumplimiento y facilitar la demostración de que se actúa conforme a las normas. Este enfoque optimizado no solo ahorra tiempo, sino que también mejora la precisión en el cumplimiento de los requisitos normativos.

### API protegidas

La implementación de sólidas medidas de seguridad de API, como se describe en el último Manual de examen de tecnología de la información del Consejo Federal de Certificación de Instituciones Financieras (FFIEC), ayuda a las instituciones financieras a proteger las API y los datos confidenciales, así como a defenderse de los ataques. Esto resulta fundamental para mantener el cumplimiento de las estrictas normativas de seguridad de API.



2



## Aumentar la productividad

### Gestión unificada de la seguridad

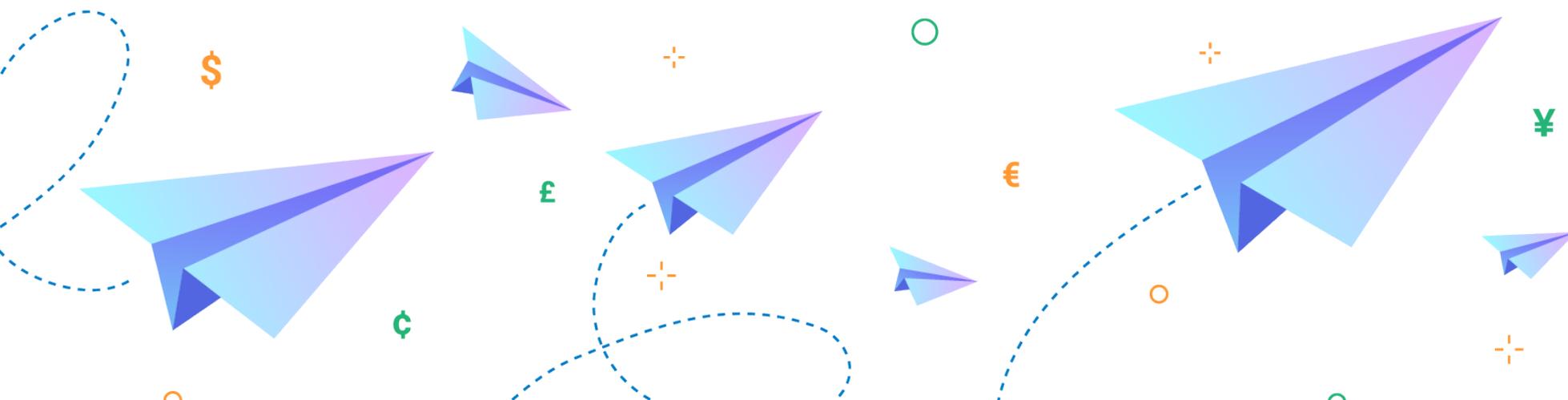
Al consolidar la gestión de la seguridad con la plataforma unificada de Akamai se reduce el tiempo de gestión, por no tener ya varias soluciones, y se mejora la eficiencia operativa. Este enfoque permite a los equipos de seguridad centrarse en iniciativas estratégicas en lugar de en la solución de problemas operativos.

### Búsqueda proactiva de amenazas

La mejora de la productividad mediante la búsqueda proactiva de amenazas identifica y neutraliza las amenazas antes de que afecten a las operaciones, lo que garantiza una continuidad empresarial más fluida. Las capacidades avanzadas de detección y mitigación de amenazas de Akamai permiten una asignación de recursos eficiente.

### Protección avanzada de API

Mediante el uso de funciones de protección del tiempo de ejecución basadas en inteligencia artificial (IA) y aprendizaje automático (ML), las instituciones financieras pueden detectar y bloquear ataques avanzados de API en tiempo real, lo que permite frustrar los sofisticados ataques de los ciberdelincuentes y mejorar la productividad general.



3



## Mejorar la atención al cliente

### Acceso de usuario eficiente

Garantizar una experiencia de cliente segura y fluida con las soluciones de seguridad en el Edge de Akamai significa proteger los datos de los usuarios y mantener un alto rendimiento, independientemente de dónde se encuentren esos usuarios. La mejora de la disponibilidad del servicio a través de la protección frente a ataques distribuidos de denegación de servicio (DDoS) y el balanceo de carga garantiza un servicio continuo, algo fundamental para mantener la confianza y la satisfacción del cliente.

### Políticas de seguridad personalizadas

La implementación de políticas de seguridad personalizadas que se adaptan a los comportamientos y las necesidades específicas de los usuarios mejora la experiencia general del cliente al tiempo que mantiene una seguridad sólida. Las soluciones de Akamai garantizan que las instituciones financieras puedan ofrecer una experiencia segura y personalizada a sus clientes.

### Supervisión de API en tiempo real

La auditoría del comportamiento de las API mediante análisis en tiempo real permite a las instituciones financieras detectar y responder rápidamente a las amenazas para proteger los datos confidenciales y garantizar una experiencia del cliente fluida y segura.



4



## Gestionar los costes de seguridad y cumplimiento de forma eficaz

### **Soluciones de seguridad escalables**

Las soluciones escalables de seguridad en la nube de Akamai crecen con las necesidades de su empresa, y ofrecen una protección rentable sin necesidad de realizar una inversión de capital significativa. Esta escalabilidad garantiza que las instituciones financieras puedan gestionar eficazmente sus gastos de seguridad y cumplimiento.

### **Reducción de los costes operativos**

Se reducen los costes operativos gracias a los servicios basados en la nube de Akamai, y ya no hay que mantener una costosa infraestructura local. El completo marco de gestión de riesgos de Akamai ayuda a identificar, evaluar y mitigar los riesgos de forma eficiente, lo que puede reducir las posibles pérdidas financieras derivadas de las infracciones de seguridad.

### **Simplificación de las auditorías de cumplimiento normativo**

Al estructurar mejor los entornos de cumplimiento y facilitar la demostración de que se actúa conforme a norma, las soluciones de microsegmentación de Akamai simplifican el proceso de auditoría, ahorrando tiempo y reduciendo el coste general asociado a la gestión de dicho cumplimiento.

También proporcionan la agilidad que necesitan las instituciones financieras actuales para ajustar rápidamente las interfaces, optimizar las visualizaciones, adaptar las reglas empresariales e integrar nueva información. El resultado es una solución mucho más completa y adaptable, capaz de seguir el ritmo que exige la gestión de casos.



5



## Crear resiliencia y confianza

### Mejora de la resiliencia operativa

Lograr un alto nivel de resiliencia operativa digital resulta fundamental para que las instituciones financieras puedan hacer frente al panorama de amenazas en constante evolución. Las soluciones de Akamai ayudan a las instituciones a prevenir y atajar los incidentes de ciberseguridad, así como a recuperarse de ellos, lo que garantiza un funcionamiento continuo y fomenta la confianza de los clientes.

### Medidas de seguridad sólidas

Las entidades reguladoras de todo el mundo hacen hincapié en la necesidad de adoptar medidas de ciberseguridad sólidas. La completa cartera de seguridad de Akamai se ajusta a estos requisitos normativos, lo que proporciona a las instituciones las herramientas necesarias para mantener la resiliencia operativa y protegerse frente a amenazas avanzadas.

### Confianza y estabilidad

Las soluciones de seguridad de Akamai no solo protegen contra las amenazas actuales, sino que también crean una base de confianza y estabilidad. Al integrar la seguridad en el núcleo de sus operaciones, las instituciones financieras pueden garantizar la resiliencia a largo plazo y mantener la confianza de sus clientes.

“

Comprender la exposición de la empresa y poder gestionarla es clave. Ver lo que está pasando en nuestro entorno es una forma esencial de identificar el riesgo. Mediante simulación de ciberataques, hemos podido crear rápidamente políticas para bloquear los vectores de ataque comunes.

– CISO, corredor-distribuidor de valores certificado

# Un banco internacional logra el cumplimiento de SWIFT en dos semanas

Entidades reguladoras externas requerían que un cliente de Akamai, un banco global, acordara todas sus aplicaciones críticas para cumplir los requisitos de SWIFT, un proceso seguro para transferir dinero entre instituciones financieras. Normalmente, una aplicación como esta requiere más de 100 servidores implementados en ubicaciones diferentes, incluidos servidores bare metal y virtuales. De media, este proceso tardaría entre 8 y 12 meses en planificarse y ejecutarse para un banco de este tamaño, ya que tendría que crearse una red de área local virtual (VLAN) para su segmento en distintas ubicaciones. Determinar las dependencias de la aplicación SWIFT y asegurarse de que el conjunto de reglas fuera correcto habría implicado aún más tiempo.

Mientras tanto, el proyecto también suponía la compra de nuevos equipos de firewalls. Y, dado que la aplicación SWIFT es fundamental para las actividades bancarias, la entidad no podía permitirse ningún tiempo de inactividad. En general, la expectativa era que el proyecto de segmentación conllevara un esfuerzo masivo por parte de muchas personas.

Sin embargo, con Akamai, para el proceso completo solo se necesitó que un ingeniero dedicara unas dos semanas. No fue necesario aplicar ningún cambio en la red y el banco no tuvo que hacer cambios en sus aplicaciones ni interrumpir sus servicios.

TIEMPO AHORRADO

**226–351 días**

REDUCCIÓN DE EMPLEADOS  
A TIEMPO COMPLETO

**>4**

CON UN TIEMPO DE INACTIVIDAD  
GARANTIZADO DE

**0**

Y VISIBILIDAD MEJORADA

## Ahorro de tiempo y visibilidad mejorada

Una institución financiera necesitaba acordar su aplicación SWIFT en un entorno complejo que incluía infraestructura bare metal, VMware y OpenStack. Los métodos de segmentación tradicionales resultaban un desafío, pues requerían entre 8 y 12 meses y más de cinco empleados a tiempo completo para completarlos, con problemas adicionales de tiempo de inactividad y falta de visibilidad de las aplicaciones y dependencias. Con la implementación de Akamai Guardicore Segmentation, la institución completó la asignación de aplicaciones SWIFT en cuestión de horas, con políticas de segmentación sugeridas y ajustadas automáticamente. No se necesitaron hardware ni firewalls nuevos, y todo el proceso se completó en dos semanas con un solo empleado a tiempo completo.

# Conclusión

---

Akamai proporciona soluciones completas que ayudan a las instituciones financieras a enfrentarse al complejo panorama del cumplimiento de normativas y la ciberseguridad. Con tecnologías avanzadas como la microsegmentación, las instituciones financieras pueden simplificar el cumplimiento, mejorar la productividad y la experiencia del cliente, gestionar los costes de seguridad y cumplimiento de forma eficaz, y generar resiliencia y confianza. La probada trayectoria de Akamai y sus innovadoras soluciones la convierten en el partner ideal para las instituciones financieras que buscan reforzar su estrategia de seguridad y garantizar el cumplimiento de las normativas.

**Obtenga más información sobre nuestras soluciones para el sector de los servicios financieros.**

La seguridad de Akamai protege las aplicaciones que impulsan su negocio en cada punto de interacción sin comprometer el rendimiento ni la experiencia del cliente. Gracias a la escala y la visibilidad de nuestra plataforma global, colaboramos con usted para prevenir, detectar y mitigar las amenazas, de forma que pueda generar confianza en la marca y cumplir su visión.

