



Informe



de riesgos

Para SERVICIOS PROFESIONALES FINANCIEROS 2019
SL.

Creado el 18 de marzo de 2026 por SPF Correduría de
seguros



Más información sobre Stoik: www.stoik.com

Introducción

Sobre el informe

Este informe contiene un análisis personalizado de las ciberamenazas que podrían afectar a SERVICIOS PROFESIONALES FINANCIEROS 2019 SL..

Ha sido elaborado a través del **escáner externo**, una herramienta de prevención diseñada por los expertos en ciberseguridad de Stoik.

A lo largo de este informe encontrará una serie de recomendaciones específicas destinadas a reforzar la seguridad de SERVICIOS PROFESIONALES FINANCIEROS 2019 SL..

01 Resumen

02 Situación de riesgo

Vulnerabilidades
Filtraciones de datos
Configuración del correo electrónico
Infraestructura

03 ¿Por qué elegir Stoik?

Seguro cibernético
Prevención activa
Gestión de siniestros

04 Preguntas frecuentes

05 Glosario técnico

Acerca de Stoik

La misión de Stoik es proteger el tejido económico europeo contra los riesgos cibernéticos a través de un enfoque global e innovador:



Un seguro especializado en riesgos cibernéticos

respaldado por las principales compañías de seguros (Tokio Marine HCC, Swiss Re, Axeria)



Herramientas de prevención

incluidas en la póliza de seguro y accesibles a través de Stoik Protect, una plataforma diseñada para controlar el riesgo en todo momento



Asesoramiento de principio a fin en caso de incidente

gracias a nuestros equipos internos de expertos en respuesta ante incidentes y gestión de siniestros



24h/7 días

Disponibilidad de nuestros expertos en ciberseguridad en caso de incidente

< 3 minutos

Tiempo medio de respuesta en caso de ciberataque

Mitad

de probabilidad de sufrir un incidente de ciberseguridad al utilizar Stoik Protect

Resumen



ELEGIBLE
al seguro Stoik

☑ **SERVICIOS PROFESIONALES FINANCIEROS 2019 SL.** es elegible para el seguro cibernético de Stoik

Nota: obtener una puntuación de riesgo satisfactoria no protege frente a ciberataques provocados por errores humanos o configuraciones incorrectas. Las herramientas cibernéticas disponibles en Stoik Protect ofrecen una protección continua contra las amenazas cibernéticas. La elegibilidad es válida durante 90 días.

Resumen de la situación de riesgo



**Puntuación de
riesgo**

100/100

Esta puntuación se calcula en función de las vulnerabilidades detectadas en la infraestructura de SERVICIOS PROFESIONALES FINANCIEROS 2019 SL., tal y como se explica en las siguientes páginas.

Situación de riesgo

Vulnerabilidades

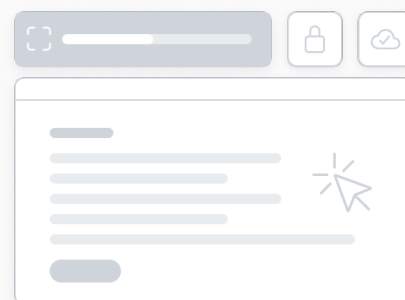
En esta sección puede consultar la lista de vulnerabilidades encontradas en la infraestructura de SERVICIOS PROFESIONALES FINANCIEROS 2019 SL., que influyen directamente en la puntuación de 100/100.

Resumen

 Crítica	0 Constituye un riesgo importante para el sistema informático y puede ser explotada. Es necesario actuar de inmediato.	 Alta	0 Puede dañar el sistema informático si es explotada (compromiso parcial del sistema, pérdida de información, etc.).
 Media	0 Puede afectar a la seguridad del sistema informático y suponer un riesgo potencial (acceso no autorizado, filtración de datos, etc.).	 Baja	0 Puede tener un impacto moderado, pero indica una vulnerabilidad en el sistema informático que puede ser explotada en determinadas circunstancias.

Acerca de Stoik Protect

Una buena puntuación de riesgo no basta para protegerse contra los ciberataques provocados por errores humanos o una mala configuración: las herramientas incluidas en la plataforma Stoik Protect (escáner externo, escáner interno, simulación de phishing, formación continua) proporcionan una protección completa contra las ciberamenazas.

stoik | **PROTECT**

Situación de riesgo

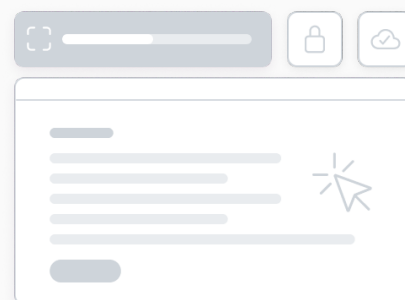
Vulnerabilidades

NO SE HA DETECTADO NINGUNA VULNERABILIDAD

Acerca de Stoik Protect

Una buena puntuación de riesgo no basta para protegerse contra los ciberataques provocados por errores humanos o una mala configuración: las herramientas incluidas en la plataforma Stoik Protect (escáner externo, escáner interno, simulación de phishing, formación continua) proporcionan una protección completa contra las ciberamenazas.

stoik | **PROTECT**



Situación de riesgo

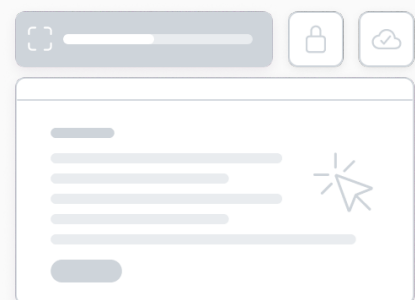
Filtraciones de datos

NO SE HA DETECTADO NINGUNA FILTRACIÓN DE DATOS

Acerca de Stoik Protect

Una buena puntuación de riesgo no basta para protegerse contra los ciberataques provocados por errores humanos o una mala configuración: las herramientas incluidas en la plataforma Stoik Protect (escáner externo, escáner interno, simulación de phishing, formación continua) proporcionan una protección completa contra las ciberamenazas.

stoik | **PROTECT**



Situación de riesgo

Configuración del correo electrónico

En esta sección encontrará la configuración de las aplicaciones de correo electrónico de SERVICIOS PROFESIONALES FINANCIEROS 2019 SL.: un error de configuración puede exponer al cliente a ataques de phishing y estafas. Estos datos no influyen en la puntuación de riesgo.

DMARC

Riesgo detectado

Domain-based Message Authentication, Reporting & Conformance (DMARC) es un protocolo de seguridad del correo electrónico. Permite a los destinatarios definir cómo tratar los correos electrónicos cuya autenticidad no puede ser verificada. En ausencia de una política DMARC, el tratamiento de estos correos se deja en manos de los sistemas de mensajería de los destinatarios, cuyas políticas de seguridad pueden variar, permitiendo que posibles intrusos lleguen a las bandejas de entrada.

DMARC dispone de tres niveles de configuración. El modo "none" desactiva la política, lo que equivale a no tener ninguna configuración específica. Los modos "quarantine" y "reject" ponen en cuarentena o rechazan los correos electrónicos sospechosos, proporcionando una mayor protección contra los mensajes fraudulentos.

- **DMARC está mal configurado en 1 recurso:** spfcorreduria.com

Registro SPF

No se ha detectado ningún riesgo

El Sender Policy Framework (SPF) es un protocolo de seguridad del correo electrónico. Permite a los propietarios de los dominios especificar qué servidores están autorizados a enviar correos electrónicos en su nombre. Este protocolo funciona a través de un registro SPF, que recopila las direcciones IP o los nombres de dominio autorizados. Cuando un servidor destinatario recibe un correo electrónico, el protocolo comprueba si la dirección IP del remitente coincide con las autorizadas en el registro SPF.

Existen tres niveles de rigor para una política de registro SPF. El modo "+all" indica una política permisiva, que no da lugar a ningún fallo. El modo "~all" indica un "softfail", es decir, una sospecha de fallo, pero permite que se entregue el mensaje, a menudo con una indicación especial. El modo "-all" indica un "hardfail", que es más estricto y propone rechazar el mensaje. La ausencia de una política SPF constituye una mala configuración, ya que expone el dominio a una posible suplantación de identidad.

- **¡El registro SPF está configurado correctamente!**

Situación de riesgo

Infraestructura

Esta sección muestra los dominios y subdominios asociados e identificados a partir del dominio principal proporcionado por SERVICIOS PROFESIONALES FINANCIEROS 2019 SL., así como los servicios web y de red.

Índice

3

DOMINIOS Y SUBDOMINIOS

10

DIRECCIONES IP

8

SERVICIOS

En detalle

DOMINIOS Y SUBDOMINIOS

spfcorreduria.com

autodiscover.spfcorreduria.com

www.spfcorreduria.com

DIRECCIONES IP

13.248.243.5 y 1 más

52.98.207.152 y 7 más

13.248.243.5 y 1 más

SERVICIOS

unknown

Microsoft Internet Information Services (IIS) 10.0

DIRECCIONES IP

76.223.105.230 y 3 más

52.98.207.152 y 3 más

¿Por qué elegir Stoik?

La póliza de seguro más completa del mercado

Stoik propone una cobertura completa para que las empresas puedan mantener su actividad frente a los riesgos cibernéticos, además de ayudarles a reanudar su actividad con rapidez y serenidad en caso de incidente.

La póliza incluye:



Asistencia y gestión de crisis

Respuesta ante incidentes 24h/7 días a la semana, asistencia legal, comunicación de crisis, remediación del sistema, recuperación de datos.



Daños y pérdidas

Pérdida de beneficios, gastos de explotación adicionales, extorsión cibernética, gastos de notificación, gastos de monitorización y vigilancia, investigaciones y sanciones, ciberfraude.



Responsabilidad civil

Filtración de datos, daño mediático, transmisión de virus.



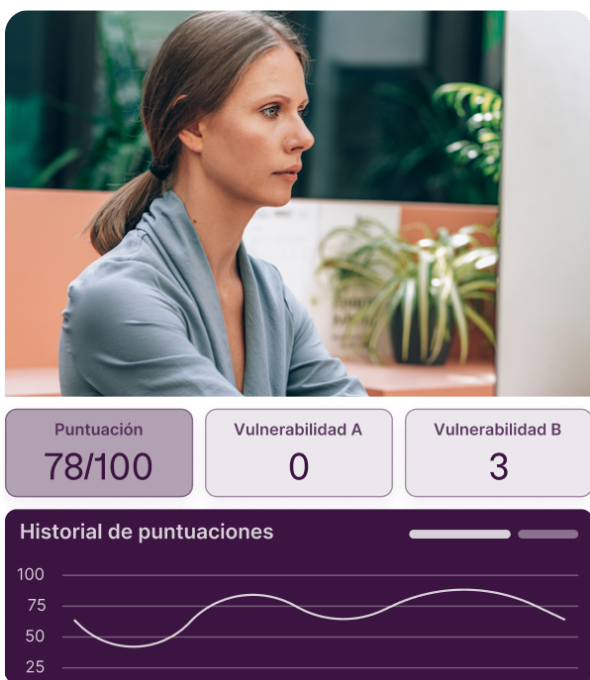
Nuestras pólizas de seguros están respaldadas por las principales compañías de seguros: Tokio Marine HCC (calificada A++ por AM Best), Swiss Re (2ª mayor reaseguradora mundial) y Axeria (calificada A- por AM Best).



¿Por qué elegir Stoik?

Una prevención **activa** para controlar los riesgos a diario

Las empresas aseguradas por Stoik tienen acceso a Stoik Protect, una plataforma online que hemos diseñado para controlar sus riesgos cibernéticos. Stoik Protect es mucho más que un software de ciberseguridad: es una combinación de herramientas proactivas y fáciles de utilizar.



Escáner externo

Análisis semanal del sistema informático para detectar fallos de seguridad



Escáner interno

Mapeo del Cloud y del Active Directory para detectar vulnerabilidades



Simulación de phishing

Falsos correos de phishing para aprender a detectar los mensajes fraudulentos



Formación continua

Tutoriales sencillos y útiles para adquirir buenas prácticas cibernéticas

Stoik Protect ayuda a reducir los riesgos cibernéticos interviniendo en cada etapa de un ciberataque:

1

La intrusión es propiciada por una vulnerabilidad o por un empleado

→ Los **escáneres** detectan fallos de seguridad, la **simulación de phishing** y la **formación continua** conciencian a los equipos

2

El atacante se propaga por el sistema hasta obtener el control

→ Los **escáneres internos** comprueban los derechos de los usuarios y las políticas de contraseñas poco seguras para frenar la toma de control

3

El intruso procede al ataque: ransomware, filtración de datos, etc.

→ En caso de ataque, los **escáneres** proporcionan información crucial para facilitar la investigación de nuestro equipo de respuesta ante incidentes



Certificación de AWS - Security Specialty & Architecting



Certificación SOC 2 Tipo I (en proceso)



Certificación de GCP - Professional Cloud Security Engineer

¿Por qué elegir Stoik?

Expertos especializados en la gestión de siniestros, 24h/7 días

En Stoik, nos ocupamos de gestionar los siniestros de principio a fin, desde la respuesta ante incidentes 24h/7 días a la semana, hasta la indemnización. Nuestros equipos están en contacto permanente con una amplia red de asociados técnicos y jurídicos, así como con más de 700 equipos CERT (Computer Emergency Response Teams) en todo el mundo.



Descubra los testimonios de nuestros asegurados y cómo les hemos ayudado:



Filtración de datos

A CARGO DE STOİK

El empleado de un editor de softwares cayó en la trampa de un correo electrónico de phishing, permitiendo que un atacante accediera a los datos de sus clientes.

→ Nuestros expertos consiguieron neutralizar al atacante y restablecieron el sistema, además de asesorar a la empresa sobre las diferentes acciones legales. El asegurado recibió una indemnización para hacer frente a los gastos legales y a la responsabilidad civil generada por la filtración de datos.

115.000 €



Ransomware

A CARGO DE STOİK

Durante las rebajas, la web de comercio electrónico de un minorista quedó inaccesible: se pedía un rescate a cambio de restablecer la conexión.

→ Nuestros expertos constataron que el bloqueo era consecuencia de un ataque informático a escala mundial. Reconstruyeron la infraestructura, permitiendo que la web volviera a funcionar en tan solo unas horas. A continuación, nuestro equipo de gestión de siniestros indemnizó al vendedor por la pérdida de beneficios ocasionada.

250.000 €



Estafa por falsa orden de pago

A CARGO DE STOİK

El empleado de una notaría recibió una orden de pago destinada a un proveedor de servicios: el correo electrónico había sido pirateado, por lo que los fondos se transfirieron a una cuenta fraudulenta.

→ Nuestros expertos iniciaron inmediatamente una investigación y en pocas horas averiguaron cómo se había infiltrado el atacante en el sistema, procediendo a su expulsión. La empresa recibió una indemnización por el importe de los fondos robados.

50.000 €

Preguntas frecuentes

¿Qué es el escáner externo?

Este informe de riesgos se ha elaborado gracias al escáner externo, una herramienta de ciberseguridad diseñada por Stoik. Su objetivo es analizar los recursos del sistema informático expuestos en Internet, con el fin de detectar cualquier vulnerabilidad cibernética potencialmente explotable por los atacantes.

¿Cómo funciona?

El escáner externo realiza varias pruebas en la infraestructura externa del sistema informático, a la que todo el mundo puede acceder fácilmente a través de Internet. Es como si un ladrón observara desde la calle si la puerta principal de una casa está abierta o si el sistema de alarma está desconectado.

¿Por qué se utiliza durante el proceso de suscripción?

El escáner externo simplifica el proceso de suscripción al seguro cibernético de Stoik, reemplazando los clásicos cuestionarios largos y complicados. Una vez que la empresa esté asegurada, podrá acceder a él a través de la plataforma Stoik Protect.

¿De dónde procede la información sobre las vulnerabilidades?

El sistema CVE de MITRE se utiliza para identificar las vulnerabilidades y el sistema CVSS de FIRST para evaluar la gravedad de estas.

¿Cómo se ha recopilado la información sobre la infraestructura?

Para maximizar la efectividad de los resultados, Stoik descubre automáticamente activos y servicios adicionales asociados con los dominios y direcciones IP proporcionados.

¿Qué hago si falta algún dato o hay algún error?

Puede pedir a su corredor que se ponga en contacto con Stoik para actualizar el análisis y reiniciar el escáner.

Preguntas frecuentes

¿Por qué la puntuación de riesgo de Stoik es diferente de la que ofrecen los análisis de la competencia?

La puntuación de riesgo de Stoik se enfoca en las vulnerabilidades y errores de configuración que tienen un impacto directo en su seguridad, garantizando así que las recomendaciones sean claras. En cambio, algunos informes de la competencia también muestran información general o pequeños fallos de configuración (cookies de sesión, TLS, HSTS, etc.), haciendo que los resultados sean más difíciles de entender.

Glosario técnico

Dirección IP

Etiqueta numérica asignada a cada dispositivo conectado a una red informática que utiliza el Protocolo de Internet para comunicarse. Sirve como identificador único de dicho dispositivo.

CVE

Common Vulnerabilities & Exposures. Clasificación y descripción de una vulnerabilidad de software o hardware, que incluye: un número de identificación único, información detallada sobre la vulnerabilidad y al menos una referencia pública.

Dominio

Área específica de Internet asociada a una organización y utilizada para encontrar páginas web o servidores (por ejemplo: "stoik.com").

Recursos

Cualquier elemento que pueda utilizarse para realizar acciones o proporcionar información dentro de un sistema.

Subdominios

Parte de un dominio de mayor extensión que se utiliza para organizar diferentes áreas de una página web o para alojar diferentes servicios (por ejemplo: en el dominio "app.ejemplo.com", "app" es un subdominio de "ejemplo.com").

Vulnerabilidad

Fallo en la creación, implementación o configuración de un sistema informático que puede ser explotado por un atacante.

Creado por Stoïk

Seguro y ciberseguridad



Stoïk asume el papel de CISO de Europa, reforzando la resiliencia cibernética de las empresas europeas mediante un modelo basado en inteligencia artificial que combina ciberseguro, prevención activa y respuesta a incidentes con equipos internos.

stoïk

www.stoik.com

contacto@stoik.io

Stoïk Iberia. C/Pinar 5. Madrid 28006