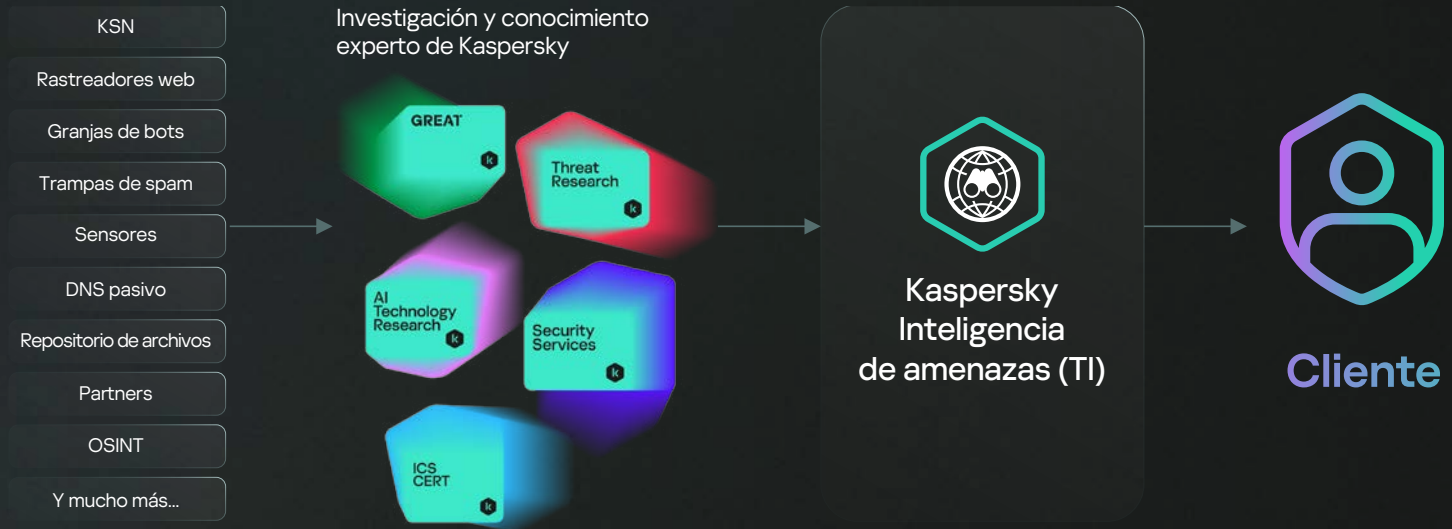
Kaspersky Threat Intelligence

Anticípese a sus adversarios

kaspersky

Fuentes de Kaspersky Threat Intelligence



Kaspersky Threat Intelligence ofrece acceso a una amplia variedad de información recopilada por nuestro equipo de análisis e investigación de clase mundial con el fin de ayudar a las organizaciones a contrarrestar de manera efectiva las ciberamenazas actuales.

Inteligencia de amenazas basada en una experiencia y conocimiento global únicos

Cada centro contribuye a las soluciones y los servicios de Kaspersky

Investigación de amenazas

Investigación de incidentes

Equipo de análisis e investigación global de Kaspersky

- Investigación de las amenazas más complejas: APT, campañas de ciberespionaje, epidemias cibernéticas mundiales, etc.
- Seguridad en las tecnologías para el futuro
- Investigación de ciberdelitos financieros sofisticados

Kaspersky Investigación de amenazas

- Investigación antimalware
- Investigación del filtrado de contenido
- Metodologías SSDLC y de seguridad por diseño

Kaspersky AI Technology Research

- Ciberseguridad para IA
- Investigación en IA generativa
- Soluciones de detección de amenazas con IA

Kaspersky Servicios de seguridad

- MDR
- Evaluación de seguridad
- Digital Footprint Intelligence
- Respuesta a incidentes
- Consultoría SOC

Kaspersky ICS CERT

- Análisis de ciberamenazas a infraestructuras críticas
- Estándares, análisis y asociaciones tecnológicas
- Evaluación e investigación de vulnerabilidades en sistemas de control industrial (ICS)

Aspectos destacados de Kaspersky Threat Intelligence

Gracias a nuestro vasto conocimiento y experiencia en la investigación de ciberamenazas, así como a la comprensión de las características únicas de cada aspecto de la ciberseguridad, somos un socio de confianza para empresas de todo el mundo y un aliado valioso para organizaciones gubernamentales y agencias de seguridad, incluidas la Interpol y numerosas unidades CERT (equipos de respuesta ante emergencias informáticas).

Cobertura de amenazas globales y experiencia de años en la investigación de amenazas en las regiones desde donde provienen la mayoría de los ataques

Contribución continua de especialistas de Kaspersky

Inteligencia de amenazas para segmentos IT y OT

Aspectos destacados de Kaspersky Threat Intelligence

Hacemos seguimiento de:

Más de 300

ciberdelincuentes

Más de 500

ciberespionaje

Más de 200

informes privados se redactan al año

Más de 170.000

IoC relacionados con los informes

Más de 2.500

reglas YARA relativas a los informes

Niveles de datos de la inteligencia de amenazas

Tácticos

Información de bajo nivel y muy perecedera que respalda las operaciones de seguridad y la respuesta a incidentes. Un ejemplo de inteligencia táctica son los IOC relacionados con la ejecución de un ataque recientemente detectado.

Funciones:

- Analista de SOC

Sistemas:

- SIEM
- NGFW
- SOAR
- IPS
- IDS

Procesos:

- Búsqueda de amenazas
- Monitoreo

Operativos

Este nivel suele incluir datos sobre campañas y TTP de orden superior. Puede incluir información sobre atribuciones de ciberdelincuentes específicos, así como sobre las capacidades e intenciones de adversarios.

Funciones:

- Analista L3 de SOC
- Analista de DFIR
- Analista de IR

Sistemas:

- SIEM
- NTA
- TIP
- EDR/XDR

Procesos:

- Respuesta a incidentes
- Búsqueda de amenazas

Estratégico

Este nivel apoya al personal ejecutivo y a las juntas directivas en la toma de decisiones serias sobre evaluación de riesgos, asignación de recursos y estrategia de la organización. Esta información incluye tendencias, motivaciones de los ciberdelincuentes y sus clasificaciones.

Funciones:

- CISO
- Director de tecnología
- Director de información
- CEO

Procesos:

- Creación de una estrategia de IS
- Mayor conciencia

Formatos para la entrega de inteligencia de amenazas

Inteligencia de amenazas legible por máquinas

Kaspersky Threat Data Feeds

Más de 30 fuentes de datos sobre diferentes necesidades con cobertura IT y OT, junto con una plataforma de inteligencia de amenazas

Inteligencia de amenazas procesable por personas humanas

Kaspersky Threat Intelligence Portal

La cartera principal de Kaspersky Threat Intelligence para entornos IT y OT con un único punto de acceso desde Kaspersky Threat Intelligence Portal

Inteligencia experta de Threat Intelligence

Kaspersky Takedown Service

Kaspersky Ask the Analyst

Guía experta de profesionales con experiencia

Kaspersky Threat Intelligence

Inteligencia de amenazas legible por máquinas

- Kaspersky Threat Data Feeds
- Kaspersky CyberTrace

Inteligencia experta de Threat Intelligence

- Kaspersky Takedown Service
- Kaspersky Ask the Analyst

Kaspersky Inteligencia de amenazas (TI)

- Tácticos
- Operativos
- Estratégico

○ Disponible desde

Kaspersky Inteligencia de amenazas (TI) Portal

Inteligencia de amenazas procesable por personas humanas

- Kaspersky Threat Lookup
- Kaspersky Digital Footprint Intelligence
- Kaspersky Threat Analysis
  - Sandbox
  - Atributos
  - Similitud
- Informes de Kaspersky Threat Intelligence
  - APT
  - Crimeware
  - ICS
- Kaspersky Threat Infrastructure Tracking

Kaspersky Threat Data Feeds

Más de 30 fuentes de datos de amenazas inmediatas para distintas tareas.

También hay disponibles fuentes de datos de amenazas a la medida de las necesidades de su organización.

- TI táctica
- TI operativa

Fuentes de datos de amenazas generales

- Direcciones URL maliciosas
- URL de ransomware
- Direcciones URL de phishing
- URL de C&C de botnets
- Botnet móvil C&CRL
- Hashes maliciosos
- Hashes maliciosos móviles
- Reputación de IP
- Direcciones URL de IoT
- Hashes de ICS
- Hashes de APT
- IP de APT
- URL de APT
- Hashes de crimeware
- Direcciones URL de crimeware

Kaspersky Threat Data Feeds

SIEM, SOAR / IRP, TIP, EDR / XDR

Plataforma de inteligencia de amenazas

Active las diversas fuentes de inteligencia de amenazas y reduzca la carca de trabajo de SIEM con rapidez

Kaspersky CyberTrace

Fuentes de datos de amenazas específicas

Fuentes de datos de Network Security	Fuente de reglas de Suricata	Fuente de datos de reglas Sigma	Fuentes de datos de reglas Yara	Fuente de vulnerabilidades	Fuente de datos de amenazas a software de código abierto
NGFW	IDS / IPS	SIEM / EDR	YARA-analizador	SBOM, CMDB	OSA / CSA / ASOC

Portal de Kaspersky Threat Intelligence

Un único punto de acceso a Kaspersky Threat Intelligence desde una IU o API única: los servicios funcionan en conjunto, y se fortalecen entre sí. Al tener todo el conocimiento experto y la experiencia en ciberamenazas de Kaspersky en un único sitio, pueden supervisarse las amenazas relevantes para una organización específica mediante las tecnologías de normalización y procesamiento de datos privados. Además, pueden analizarse muestras de malware y determinar sus respectivas atribuciones..

- TI táctica
- TI operativa
- TI estratégica

Versión gratis de Kaspersky Threat Intelligence Portal

Panorama de amenazas en Kaspersky Threat Intelligence Portal

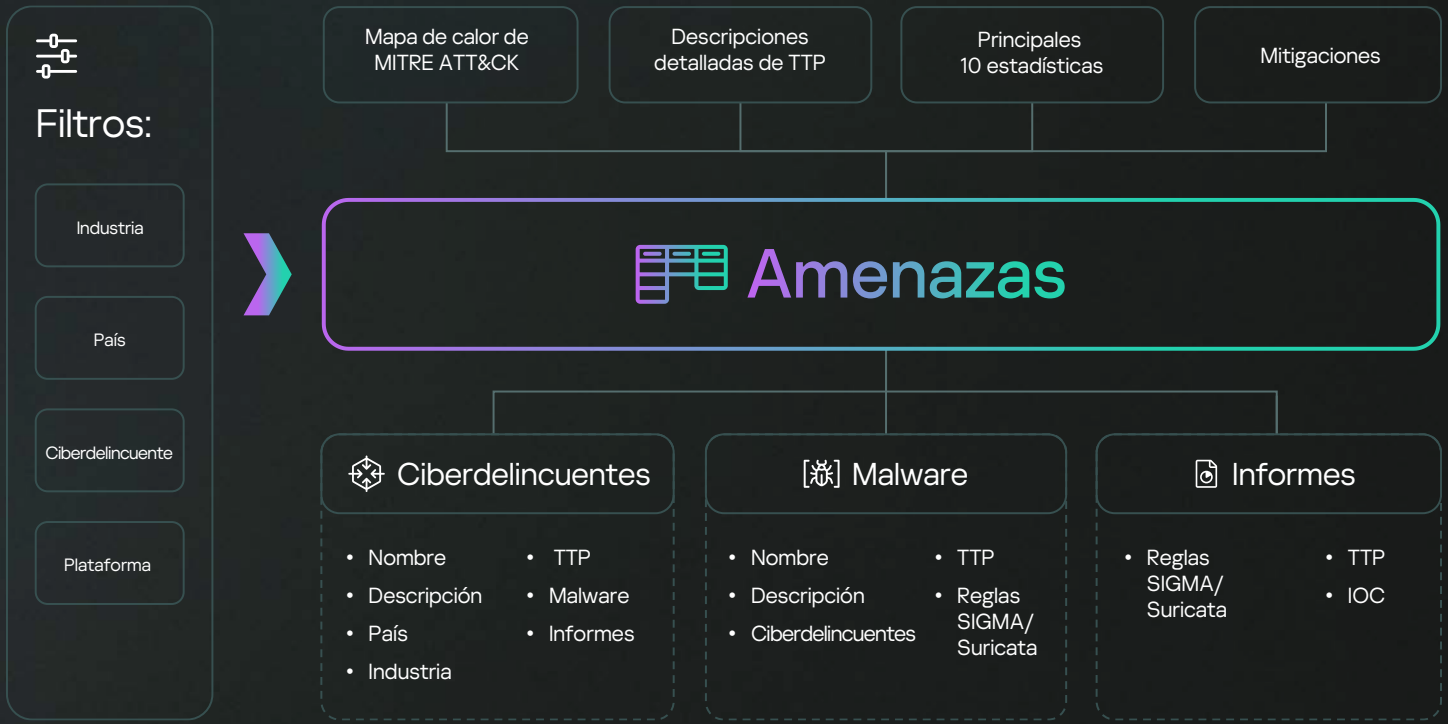
Inteligencia de amenazas específica según la región y la industria para comprender cuáles son las amenazas que enfrenta suorganización

- Alineación con MITRE ATT&CK
- Actualizaciones en tiempo real según las investigaciones en curso de Kaspersky
- Perfiles de software y de ciberdelincuentes completados automáticamente
- Repositorio de reglas de detección

Más de 400.000

archivos detectados diariamente

¿Cómo funciona el panorama de amenazas?



Asistencia experta de Kaspersky Threat Intelligence

Kaspersky Ask the Analyst

- TI operativa
- TI estratégica

El servicio Kaspersky Ask the Analyst amplía nuestra cartera de inteligencia de amenazas para que pueda solicitar asesoramiento e información sobre amenazas específicas a las que se enfrenta o en las que está interesado.

Le brindamos acceso a un grupo de investigadores de Kaspersky para cada caso en particular. El servicio ofrece una comunicación integral entre expertos para aumentar sus capacidades actuales con nuestros conocimientos y recursos únicos.

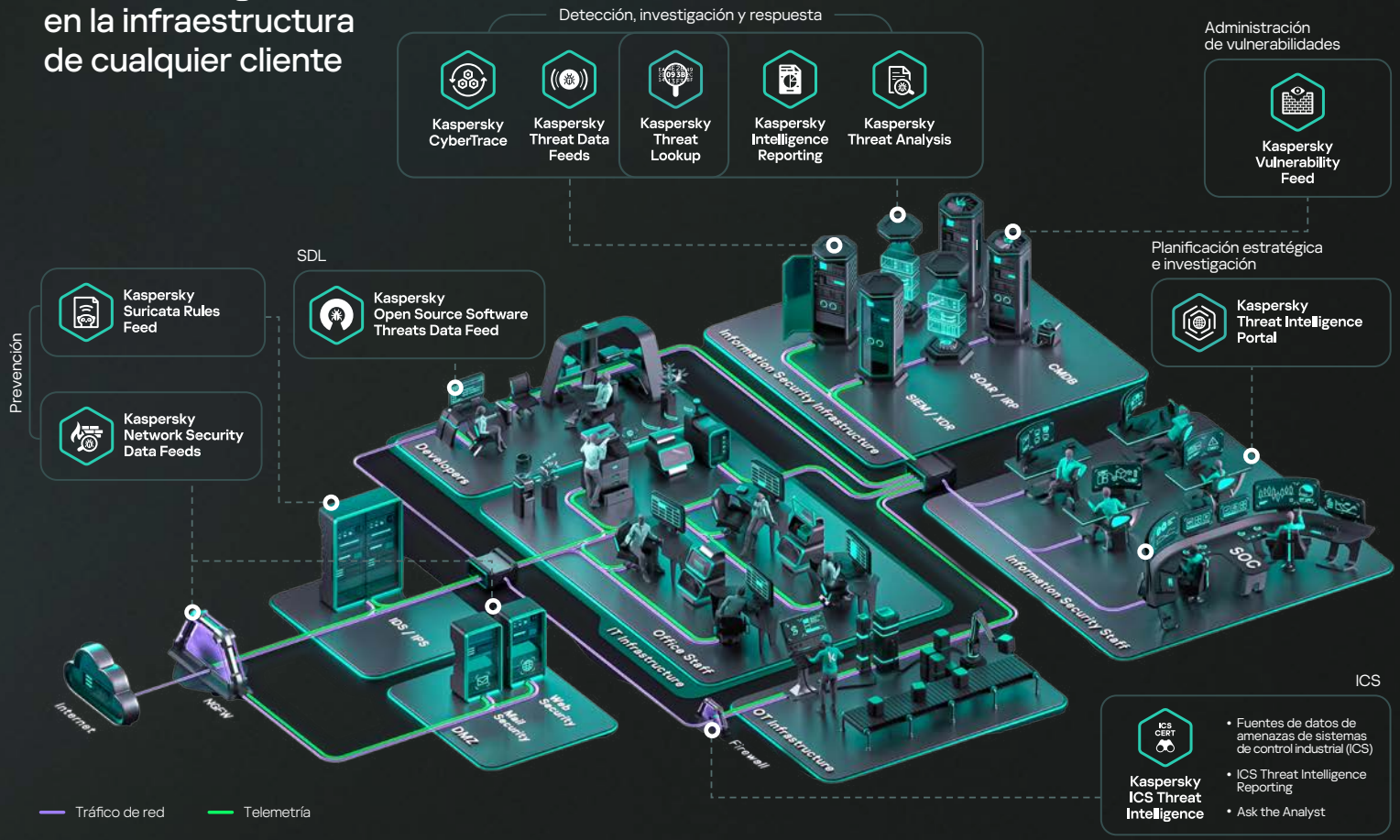
Kaspersky Takedown Service

- TI operativa

Kaspersky Takedown Service mitiga rápidamente las amenazas que representan los dominios maliciosos y de phishing antes de que causen algún daño a la marca y la empresa de cualquier cliente. Gracias a la vasta experiencia en el análisis de dominios, sabemos cómo recopilar toda la evidencia necesaria para comprobar que son maliciosos. Nos encargaremos de gestionar su eliminación.

El servicio se ofrece en todo el mundo con la cooperación de organizaciones internacionales y agencias de seguridad nacionales y regionales.

Ejemplo de Kaspersky Threat Intelligence en la infraestructura de cualquier cliente



Oferta industrial de Kaspersky Threat Intelligence

Inteligencia de amenazas legible por máquinas

Kaspersky Threat Data Feeds

Datos legibles por máquinas sobre amenazas y vulnerabilidades de ciberseguridad:

Fuentes de datos de hashes de ICS de Kaspersky
Fuentes de datos de vulnerabilidades de ICS de Kaspersky
Fuentes de datos de vulnerabilidades de ICS de Kaspersky en formato OVAL

Inteligencia de amenazas procesable por personas humanas

Kaspersky ICS Intelligence Reporting

Acceso a publicaciones periódicas sobre vulnerabilidades y amenazas a la ciberseguridad industrial en Kaspersky Threat Intelligence Portal.

Asistencia experta de Threat Intelligence

Kaspersky Ask the Analyst

Consulte directamente con especialistas del ICS CERT de Kaspersky para recibir consejos profesionales sobre vulnerabilidades y amenazas a la ciberseguridad industrial, las estadísticas y el panorama de amenazas, los estándares de la industria y más.

Tácticos · TI operativa · TI estratégica

¿Por qué elegir Kaspersky Threat Intelligence?

Una oferta de TI líder reconocida por analistas de la industria	Verificada por analistas de diversas empresas internacionales de investigación, como Frost & Sullivan, Quadrant Knowledge Solutions, Forrester, IDC, entre otras.
Diversas fuentes únicas y creíbles para generar inteligencia de amenazas confiable	La infraestructura de Kaspersky Security Network cubre más de 100 millones de sensores en 200 países: son los repositorios más grandes de archivos maliciosos y legítimos, la web oscura, actividades continuas de búsqueda de amenazas y respuesta ante incidentes, rastreadores web, trampas para correo no deseado, entre otras.
Reconocida experiencia de profesionales en IT y OT	Más de 200 especialistas con certificación provenientes de 5 centros de especialización, que incluyen el equipo GReAT y ICS-CERT ubicados en todo el mundo, que hablan más de 20 idiomas. Cada especialista de Kaspersky siempre está entre las primeras personas en descubrir las amenazas más notorias: desde Stuxnet y WannaCry a Operation Triangulation.
Presencial global	Una fuerte presencia en las regiones desde donde provienen la mayoría de los ataques (Rusia, la Comunidad de Estados Independientes, China, entre otros) nos da la habilidad única de recopilar y analizar inteligencia de amenazas en su totalidad y distribuirla a organizaciones de cualquier país.
Experiencia única en las tecnologías de detección de malware	Como el proveedor más grande de soluciones antivirus (nuestros productos son los más galardonados), procesamos millones de muestras de malware a diario, con nuestras propias tecnologías de detección de amenazas.
Experiencia única en investigación de APT	Supervisamos cientos de campañas y delincuentes de APT, publicamos más de 200 informes estratégicos y detallados de inteligencia de amenazas al año y poseemos la colección de archivos APT más grande de la industria, con más de 70.000 muestras.
TI con tecnología IA para mejorar la detección, respuesta y generación de informes ante amenazas	Con tecnologías de IA y AA, podemos extraer información práctica, generar informes personalizados y automatizar análisis, lo que nos ahorra tiempo y recursos.
Proveedor sólido y de confianza	Tolerancia a fallas, infraestructura transparente con amplias capacidades de supervisión y ANS (desarrolladas mediante metodologías SDLC), y evaluaciones independientes y periódicas de organizaciones externas (SOC tipo 2 o ISO 27001).

Historias de éxito públicas

Esto nos ofrece una gran visibilidad de las amenazas a las que se enfrentan nuestros clientes. Cuando se produce una alerta, tener a disposición esa información confiable y referenciable, con todos los datos colaterales que se obtienen de ella, es vital para crear una descripción completa de lo que está ocurriendo y lo que podemos aprender.

Paul Colwell
CyberGuard Technologies

CyberGuard Technologies

Leer la historia

Kaspersky suele ser el primero en identificar una amenaza emergente, incluso antes de que quienes fabrican el software se enteren.

Kaspersky tiene la experiencia necesaria para informarnos sobre nuevas amenazas, aquello que desconocemos y acecha en las penumbras, en lugar de simplemente bombardearnos con noticias recicladas que no aportan nada nuevo a lo que ya sabemos.

Juan Andrés Guerrero Saade
Investigador, Chronicle Security

chronicle

Leer la historia

Kaspersky superó mis expectativas al presentarnos sus características y escuchar nuestras necesidades. Su producto y el equipo detrás de él nos transmitieron confianza, lo que nos permitió contar con una red más segura.

Rashid AlNahlawi
Asesor de seguridad IT,
Comité Olímpico de Catar

قطر
QATAR

Leer la historia

Tareas que permite Kaspersky Threat Intelligence

Identificar y prevenir amenazas de forma proactiva

Kaspersky Threat Intelligence le brinda información actualizada sobre las amenazas y vulnerabilidades más recientes, para que pueda tomar medidas proactivas a fin de proteger sus sistemas antes de que ocurra un ataque.

Mejorar sus capacidades de detección de amenazas

Kaspersky Threat Intelligence le brinda ayuda para mejorar sus soluciones de seguridad existentes con la inteligencia de amenazas más reciente con el fin de que pueda incrementar su capacidad para detectar y bloquear amenazas avanzadas.

Mejorar la respuesta ante incidentes

Kaspersky Threat Intelligence ofrece información en tiempo real sobre amenazas emergentes e indicadores de riesgo, permitiéndole responder de manera rápida y eficaz a los incidentes.

Obtener visibilidad de los rastros digitales

Kaspersky Threat Intelligence proporciona una visión integral de sus rastros digitales, incluidos aquellos activos que puedan ser vulnerables a un ataque o estar en riesgo.

Ampliar sus conocimientos internos

El equipo de especialistas de Kaspersky está entre los investigadores más experimentados y reconocidos de la industria, aportando valiosos conocimientos a los equipos de seguridad de la información.

Cumplir con las regulaciones y normas

Todas las empresas están sujetas a diversas regulaciones y normas dentro de su industria. Kaspersky Threat Intelligence apoya el cumplimiento de normativas al ayudarlo a cumplir con estos requisitos.

Gracias.

Kaspersky Threat Intelligence Portal,
donde vive el conocimiento
de la ciberseguridad

Kaspersky Threat Intelligence Portal

Más información

Solicite una demo