

Kaspersky OT CyberSecurity

Un ecosistema de seguridad ciberfísica
para empresas industriales





Kaspersky
OT CyberSecurity

Concepto de seguridad industrial unificada



Tecnologías

Una selección robusta de soluciones en seguridad industrial que han sido examinadas, aprobadas y conformes a la norma



Conocimiento

Análisis confiable de amenazas y capacitación integral en ciberseguridad industrial



Experiencia

Una gama completa de servicios profesionales para ofrecer ciberseguridad industrial integral

Convergencia IT/OT



Kaspersky
Extended Detection
and Response

Tecnologías

Soluciones especializadas



Kaspersky
Antidrone



Kaspersky
Aprendizaje automático
en la detección
de anomalías



Kaspersky
SD-WAN



Kaspersky
Industrial
CyberSecurity

KICS XDR



for Nodes
Protección,
detección y
respuesta en
endpoints



for Networks
Análisis,
detección y
respuesta del
tráfico en la red

Soluciones con KasperskyOS



Kaspersky IoT
Secure
Gateway



Kaspersky
Secure Remote
Workspace



Kaspersky
Automotive Secure
Gateway

Conocimiento

Higiene Cibernética



Kaspersky
Security
Awareness

Inteligencia de amenazas



Kaspersky
ICS Threat
Intelligence

Entrenamiento



Capacitaciones
especializadas
de ICS CERT de
Kaspersky

Experiencia

Detección



Evaluación
de seguridad
para SSI de
Kaspersky

Servicio administrado



Kaspersky
Incident
Response

Respuesta



Kaspersky
Managed
Detection and
Response



Kaspersky OT CyberSecurity



Kaspersky Industrial CyberSecurity

KICS XDR



for Nodes
Protección, detección y respuesta en endpoints



for Networks
Análisis, detección y respuesta del tráfico en la red



Kaspersky SD-WAN



Kaspersky IoT Secure Gateway

Convergencia IT/OT



Kaspersky Extended Detection and Response



Kaspersky Machine Learning for Anomaly Detection



Kaspersky Antidrone



Kaspersky Automotive Secure Gateway

Technological process

1 Automation & Protection

2 Monitoring & Control

3 IT systems



Kaspersky Secure Remote Workspace

Experiencia

Detección



Evaluación de seguridad para SCI de Kaspersky

Servicio administrado



Kaspersky Incident Response

Respuesta



Kaspersky Managed Detection and Response

Conocimiento

Higiene Cibernética



Kaspersky Security Awareness

Inteligencia de amenazas



Kaspersky ICS Threat Intelligence

Entrenamiento



Capacitaciones especializadas de ICS CERT de Kaspersky

Visite el sitio web



Kaspersky
Industrial
CyberSecurity

XDR

TECNOLOGÍA

Plataforma XDR nativa que protege los sistemas de automatización

- Revela amenazas, anomalías, vulnerabilidades e intentos de intrusión ocultos mucho antes de que supongan un peligro para sus operaciones
- Certificado por entidades reguladoras y proveedores de sistemas de automatización
- Sin efectos adversos en procesos tecnológicos. Evita daños inaceptables
- Hace más fácil la administración de infraestructuras de automatización distribuidas y complejas, así como la respuesta ante incidentes
- Ayuda a mitigar los riesgos y mantener un registro de las violaciones

Ventajas de la plataforma XDR



Cobertura completa de los sistemas de control y automatización industrial (IACS). Protección para computadoras Linux, Windows, aisladas o de terceros, así como detección de anomalías y amenazas en la red.



Auditorías de seguridad activas o pasivas de endpoints y redes. Administración centralizada de riesgos, políticas de seguridad y activos en todos los niveles de los IACS.



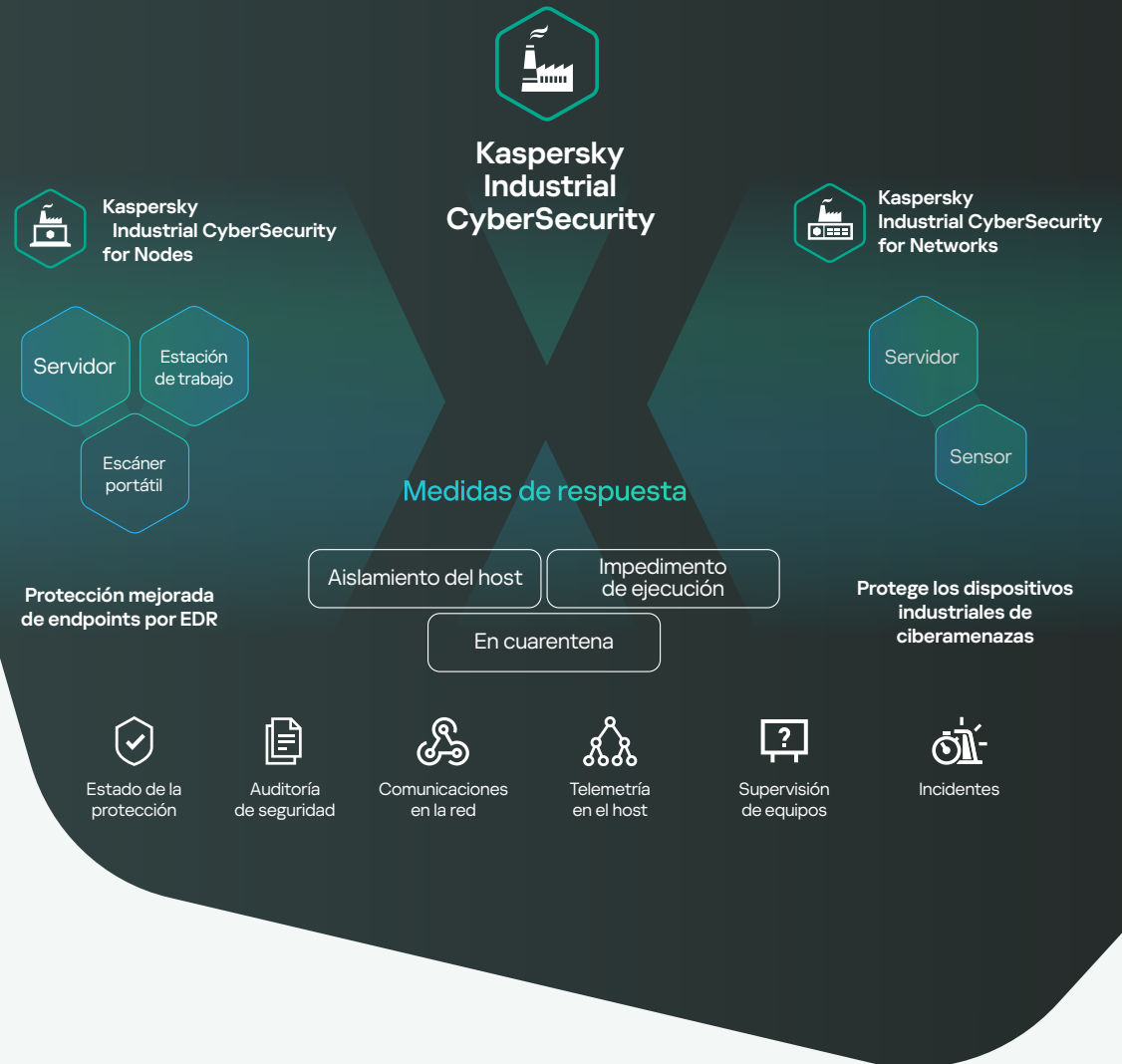
Visibilidad excepcional de sistemas y redes. Investigación y reconstrucción de toda la cadena de ataque. Visualización de la progresión de incidentes en todas las redes industriales y nodos diferentes.

[Compre a través de uno de nuestros socios](#)

[Solicite una demo](#)

[Ficha Técnica](#)

ics.kaspersky.com



Visite el sitio web



Kaspersky
Extended Detection
and Response

TECNOLOGÍA

Ciberseguridad unificada en todos los segmentos industriales y corporativos de la empresa

Gracias a una integración estrecha con Kaspersky Extended Detection and Response, la plataforma de Kaspersky Industrial CyberSecurity habilita nuevos escenarios que incluyen interacciones con soluciones de terceros y capacidades mejoradas de investigación y respuesta. La plataforma no solo protege su empresa en entornos industriales, sino también en lugares donde los entornos industriales y corporativos se superponen. Esto se logra gracias a la estrecha relación con el portafolio de ciberseguridad IT de Kaspersky, el mejor de su clase.

De esta forma, los equipos de seguridad pueden formarse una imagen holística del desarrollo de un incidente e identificar sus causas raíz, a fin de evitar incidentes similares en el futuro.

[Contáctenos](#)

[Ficha Técnica](#)

Plataforma de administración única abierta

Gestión
de casos

Automatización
y orquestación
(manuales)

Investigación

Kit de
herramientas
para la
implementación

Detección
de amenazas
y correlación
cruzada

Gestión
de activos

Tableros
e informes

Gestión de
registros y lago
de datos

Conectores
de terceros

API abierta

datos

respuesta

enriquecimiento

respuesta

datos

respuesta

Productos Kaspersky



Kaspersky
Anti Targeted Attack



Kaspersky
Endpoint Detection
and Response



Kaspersky
Endpoint Security

Productos de terceros



Endpoints

Servidores

Red

Aplicaciones

OS

Máquinas
virtuales

Otros



Kaspersky
Inteligencia
de amenazas



Kaspersky
Security Awareness



Kaspersky
Industrial
CyberSecurity

Ejemplos de respuesta con KICS:

- ✓ Análisis y actualización de las bases de datos de antivirus
- ✓ Activación de tareas
- ✓ Modificación en la autorización de nodos
- ✓ Aislamiento de nodos y procesos

Visite el sitio web



Kaspersky
Machine Learning
for Anomaly Detection

TECNOLOGÍA

Detección temprana de anomalías y análisis predictivo

- Detecta fallas en el equipo y errores humanos mucho antes de que se vuelvan críticos, lo que permite evitar errores y accidentes
- Identifica acciones de empleados u operaciones de equipos atípicas, como indicios de un ataque especializado o de sabotaje.
- Combina la detección de anomalías con el análisis predictivo y el ciclo de vida del equipo.

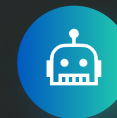
Ecosistema e inteligencia artificial



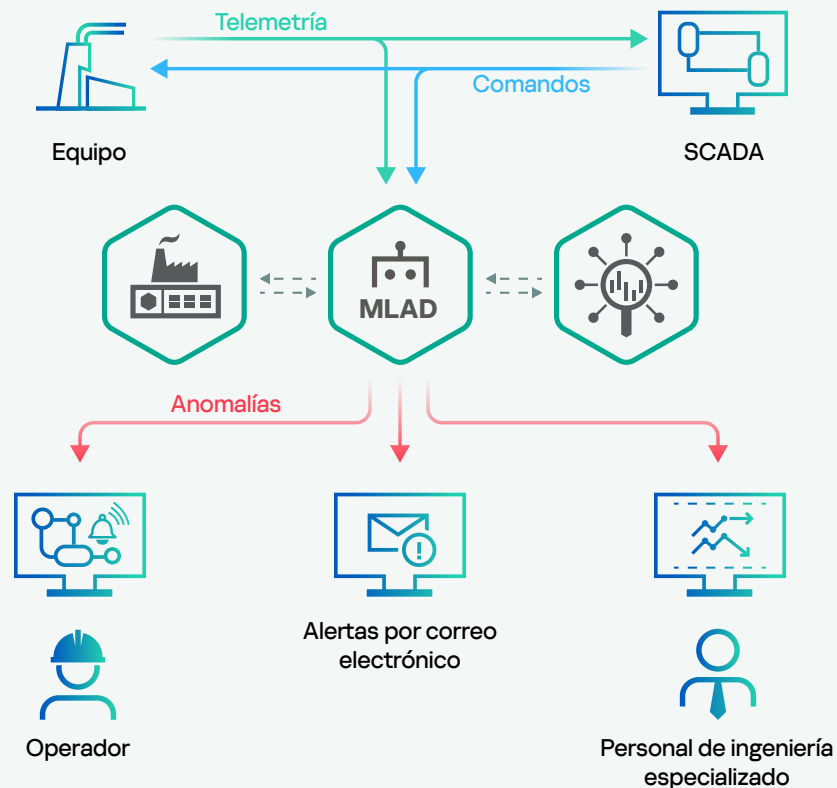
Integración con KICS for Networks y KUMA: esta recibe telemetría y eventos de estos sistemas y, a su vez, reenvía alertas sobre anomalías que han sido detectadas.



Aplica reglas de diagnóstico a los síntomas predefinidos del problema y aprendizaje automático para detectar cualquier desviación del comportamiento habitual del equipo.



Utiliza IA para analizar la telemetría de los procesos y eventos relacionados con las acciones de los empleados



Visite el sitio web



Kaspersky SD-WAN

TECNOLOGÍA

Características de Kaspersky SD-WAN:



Escalabilidad sencilla



Administración conveniente



Optimización de costos



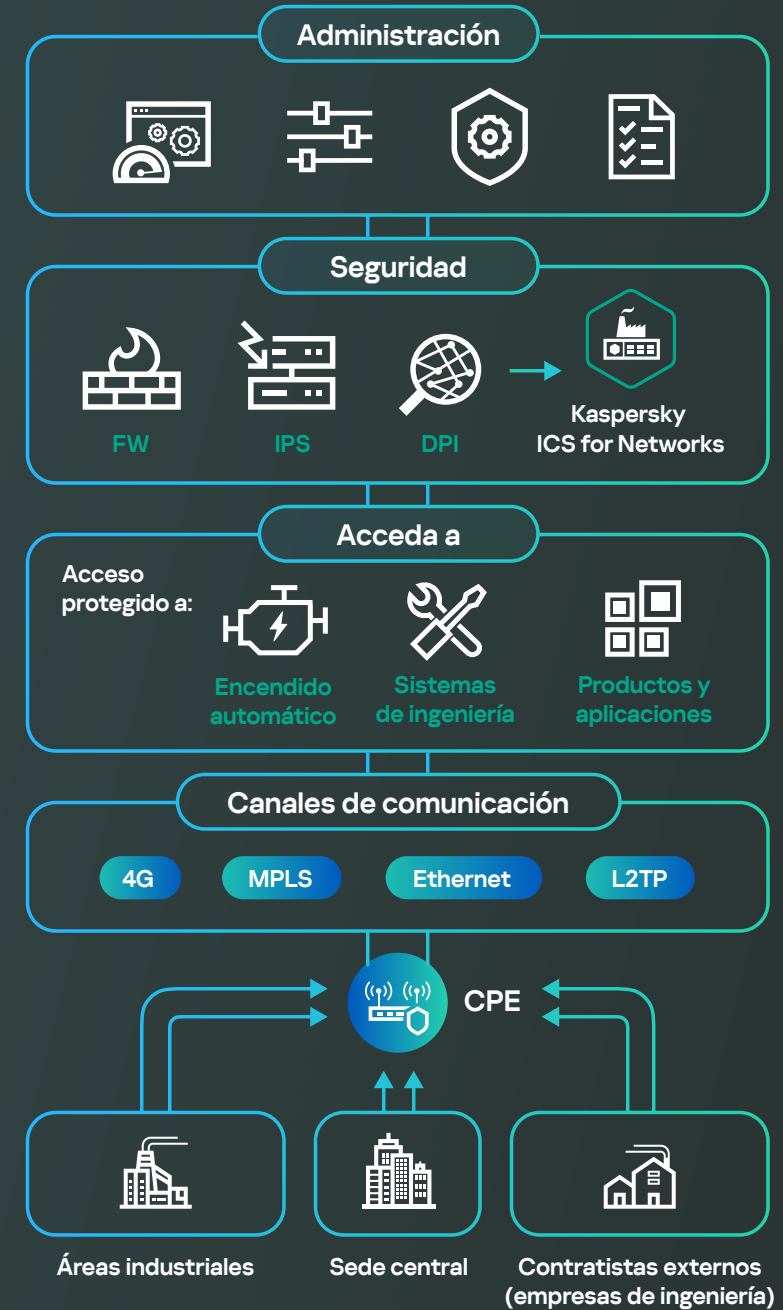
Seguridad centralizada

Una solución única para redes industriales confiables

Kaspersky SD-WAN les permite a las empresas construir una red distribuida en diferentes regiones geográficas y tolerante a fallas, con administración centralizada, mientras garantiza la continuidad de los procesos productivos. La arquitectura de Kaspersky SD-WAN le permite integrar herramientas de seguridad de Kaspersky y terceros con facilidad a través del administrador de Funciones de red virtual (VNF).

Gracias a la infraestructura de SD-WAN, en conjunto con Kaspersky ICS for Networks, puede organizar un sistema de protección y supervisión centralizado para numerosas instalaciones industriales distribuidas.

[Contáctenos](#)



Visite el sitio web



Kaspersky
Antidrone

TECNOLOGÍA

Características clave

- Detección y rastreo de drones
- Clasificación de drones mediante redes neuronales
- Interferencia direccional y omnidireccional

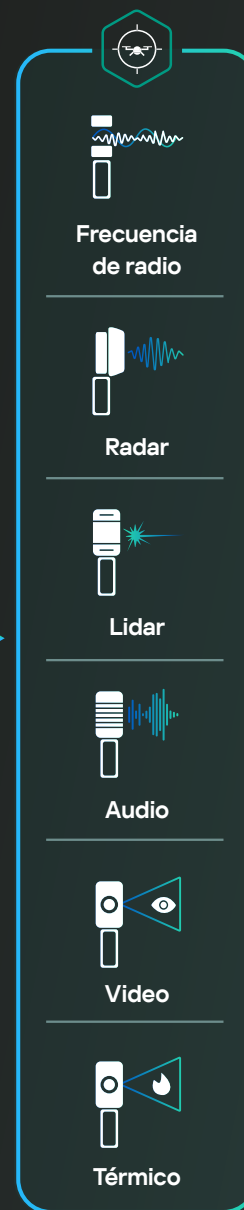
Solución de defensa y supervisión de drones

Kaspersky Antidrone reduce la probabilidad de las interrupciones de procesos en empresas industriales, al evitar el ingreso de drones no autorizados a su territorio. El sistema analiza el espacio aéreo de manera automática, detectando y clasificando drones. Además, puede encontrar información acerca de lo que está ocurriendo en la interfaz web. En caso de que haya una amenaza, y con los permisos apropiados, el operador puede neutralizar el drone.

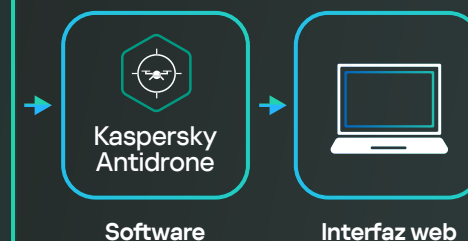
Kaspersky Antidrone es modular y puede aplicarse a instalaciones industriales de cualquier tamaño. La solución también es compatible con un modo de operación llamado "friend-or-foe", el cual permite a los clientes usar sus propios drones y evitar la intervención de vehículos aéreos no tripulados ilícitos.

[Solicite una demo](#)

[Ficha Técnica](#)



Módulos de hardware



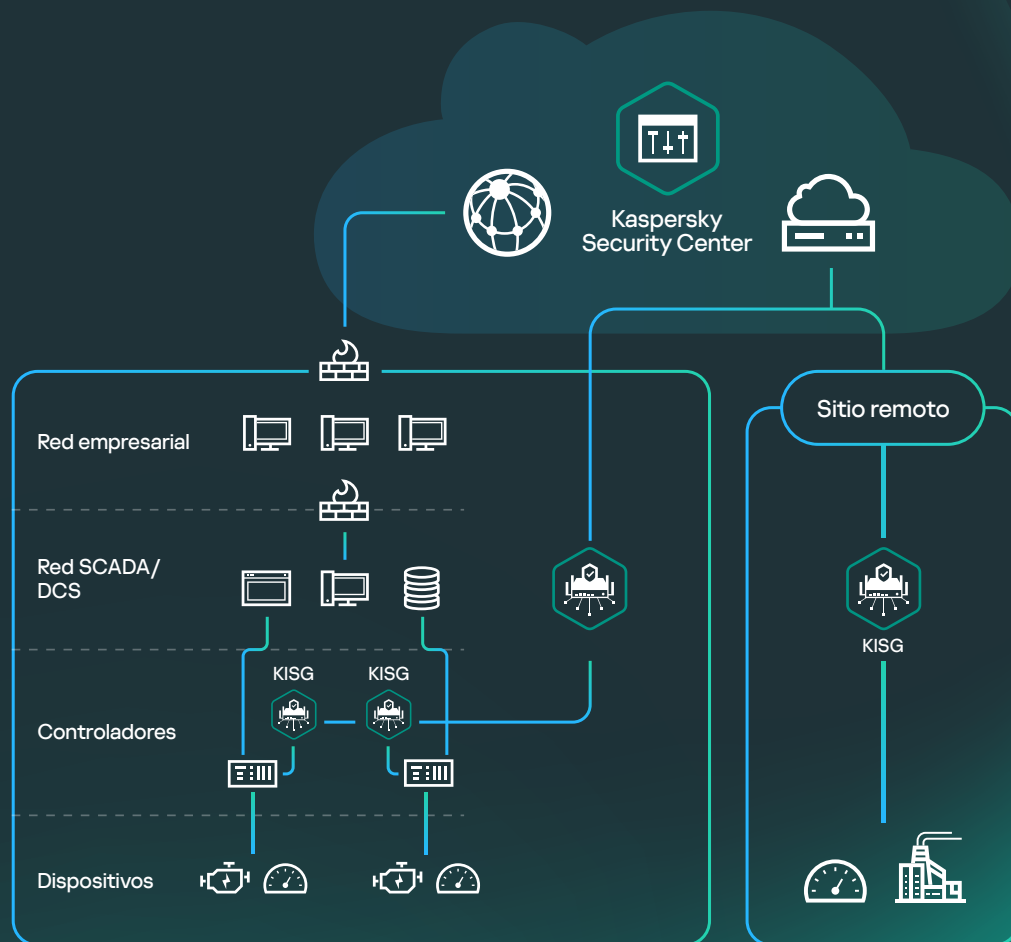
antidrone.kaspersky.com

Visite el sitio web



Kaspersky
IoT Secure
Gateway

TECNOLOGÍA



Características clave

- Recopilación y transporte seguro de datos desde dispositivos IoT a plataformas digitales y en la nube
- Kaspersky Cyber Immunity, con KasperskyOS, brinda una resistencia "innata" a la gran mayoría de tipos de ciberataques, sin necesidad de herramientas de seguridad adicionales
- Infraestructura transparente, administración centralizada de eventos y optimización de la producción

Datos confiables para el desarrollo empresarial en la Industria 4.0

La solución está formada por Kaspersky IoT Secure Gateway, con KasperskyOS, y la consola de administración de Kaspersky Security Center (KSC). Las puertas de enlace recopilan y transfieren datos de manera segura desde el equipo a las plataformas digitales o en la nube, lo que ofrece inteligencia empresarial de alta calidad para optimizar la producción y prevenir incidentes. La consola permite el mapeo de eventos de diferentes fuentes y la administración de hasta 100.000 estaciones de trabajo físicas, virtuales y en la nube.



El desarrollo comercial y tecnológico de esta solución está a cargo de Adaptive Production Technologies LLC (Aprotech, una filial de Kaspersky).

[Contáctenos](#)

[Solicite una demo](#)

[Ficha Técnica](#)

Visite el sitio web



**Kaspersky
Secure Remote
Workspace**

TECNOLOGÍA

Aplicación de producto

Riesgo

Las estaciones de trabajo de los usuarios son uno de los objetivos más comunes de los ciberataques.

Solución

Kaspersky Secure Remote Workspace (KSRW) es una solución para la construcción de una infraestructura funcional y administrada en clientes ligeros, con el sistema operativo con microkernel de Kaspersky: KasperskyOS.

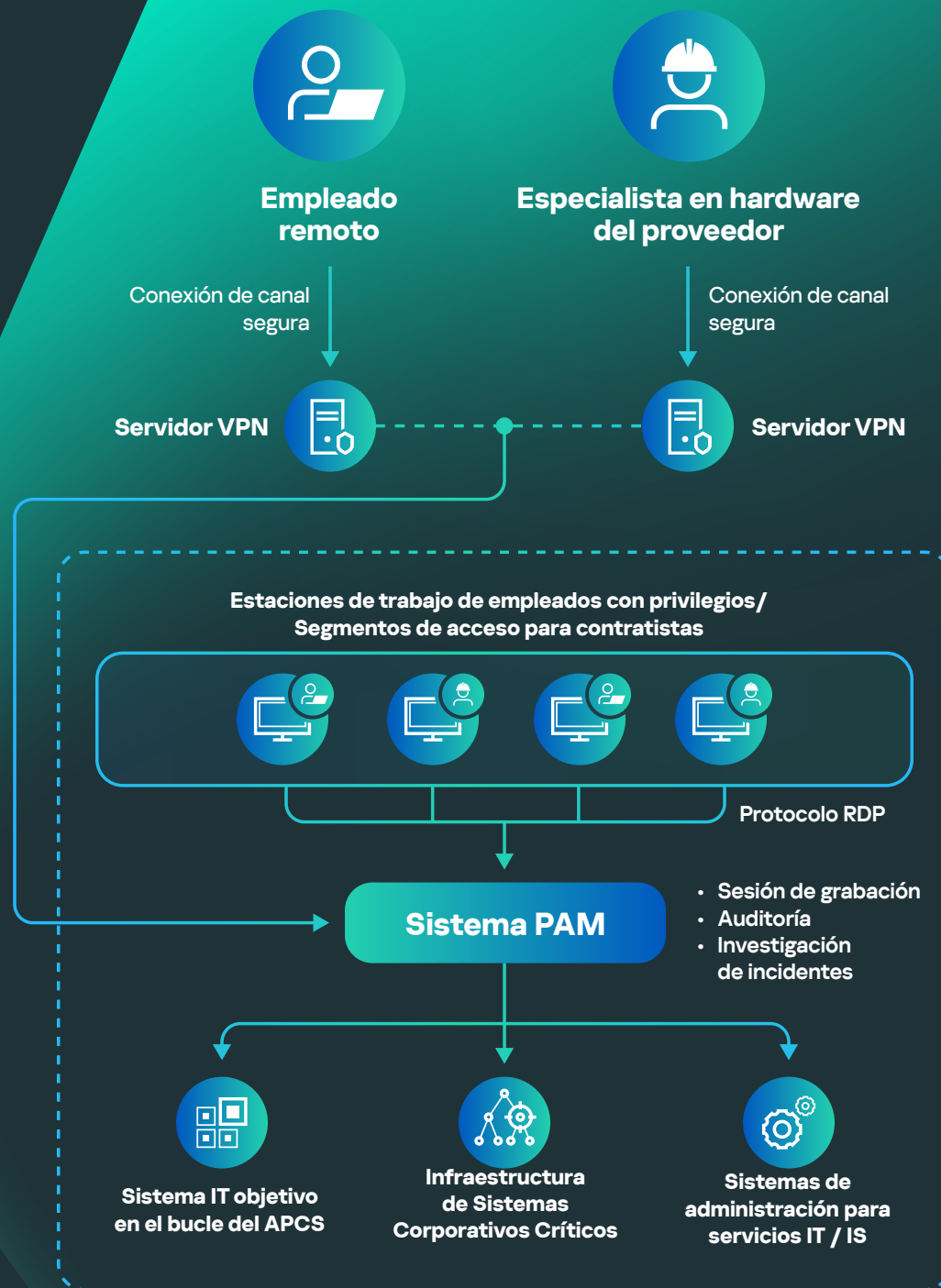
Infraestructura de Cliente Ligero Inmune a Ciberataques

Los Clientes Ligeros Ciberinmunes, como parte de Kaspersky Secure Remote Workspace, establecen una conexión segura con escritorios virtuales, incluyendo una zona confiable para conectar a los usuarios con la infraestructura industrial.

[Descripción general de la solución](#)

[Solicite una demo](#)

[Ficha Técnica](#)



[Visite el sitio web](#)

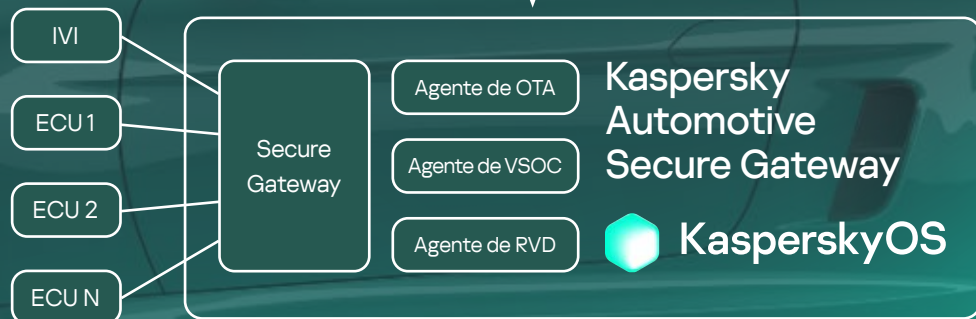


**Kaspersky
Automotive
Secure Gateway**

TECNOLOGÍA



Infraestructura de OEM en la nube



Protección de vehículos

- Acceso no autorizado
- Ataques dirigidos a unidades de control electrónicas (ECU)
- Ataques a través de sistemas de adquisición de información de vehículos (IVI)
- Diagnósticos maliciosos
- Sistema de actualización en riesgo
- Conexiones y flujos de datos no controlados, interrupción de la comunicación

Beneficios clave

- Solución "segura por diseño"
- Permite cumplir con las regulaciones de ciberseguridad
- Cuatro en uno: puerta de enlace conectada, puerta de enlace de seguridad, agente principal de OTA y agente de VSOC
- Cumplimiento con ISO 21434, ISO 26262, AUTOSAR Adaptive y Uptane

AUTOSAR

[Contáctenos](#)

[Ficha Técnica](#)

Visite el sitio web



Kaspersky
ICS Threat
Intelligence



CONOCIMIENTO

Comprensión profunda de las amenazas y vulnerabilidades de ciberseguridad industrial para una evaluación de riesgos eficiente, una detección de ataques, una investigación de incidentes y una respuesta exitosa.

Respaldo por la experiencia sin igual del ICS CERT de Kaspersky, el primer CERT privado en ciberseguridad industrial.

Características clave

- Detección rápida de amenazas y amplias capacidades analíticas
- Aumenta la eficacia de las investigaciones y las búsquedas activas de amenazas
- Información integral sobre amenazas y vulnerabilidades para una toma de decisiones informada

[Solicite una demo](#)

[Descripción general
de la solución](#)

[Contáctenos](#)

Adelántese a sus adversarios con una visibilidad en profundidad de las ciberamenazas que apuntan a su organización



Kaspersky
ICS Threat
Data Feeds

Un conjunto de flujos de datos de inteligencia de amenazas actualizados de manera regular, diseñados para satisfacer las necesidades específicas de la ciberseguridad industrial.

Inteligencia de amenazas

Flujos de datos automáticos



Kaspersky ICS
Threat Intelligence
Reporting

Proporciona un mayor conocimiento de las campañas maliciosas que apuntan a las organizaciones industriales, así como información sobre las vulnerabilidades que se encuentren en los sistemas de control industrial más populares.



Kaspersky
Ask the
Analyst

Un servicio para clientes que deseen solicitar orientación y conocimientos especializados acerca de amenazas específicas que enfrentan o que les interesa saber.

Visite el sitio web



**Kaspersky
ICS Threat Data
Feeds**



CONOCIMIENTO

El servicio Kaspersky Threat Data Feed ofrece información sobre la inteligencia frente a amenazas en tiempo real para permitirles a las organizaciones industriales proteger sus redes y sistemas de las ciberamenazas. Estas fuentes de datos incluyen información sobre malware conocido, sitios web de phishing, exploits, vulnerabilidades recientes y otros tipos de ciberamenazas. Cuando se contextualizan, los datos pueden proporcionar una visión más completa y ser utilizados para responder las preguntas de 'quién, qué, dónde y cuándo', lo que permite identificar a los adversarios, tomar decisiones rápidas y actuar.

Lo que obtiene:

Fuente de Datos Hashes de Kaspersky para ICS

Inteligencia actualizada sobre amenazas para ICS y otros sistemas usados en OT con el fin de simplificar y automatizar la detección y la investigación oportuna de ataques.

#prevención

#detección

#investigación

Suministro de Datos de Vulnerabilidades Kaspersky ICS

Datos verificados y perfeccionados acerca de las vulnerabilidades halladas en el software y hardware de sistemas ICS y otros dispositivos empleados en entornos industriales, ofrecidos en un formato legible por máquinas.

#prevención

#detección

#investigación

Fuente de Datos de Vulnerabilidades ICS en formato OVAL

Fuente de datos actualizada periódicamente que contiene definiciones en formato OVAL para la detección automatizada de vulnerabilidades conocidas en sistemas SCADA y otros tipos de software industriales.

#detección

[Contáctenos](#)

[Más información acerca del servicio](#)

Visite el sitio web



Kaspersky ICS Threat Intelligence Reporting



CONOCIMIENTO

Kaspersky ICS Threat Intelligence Reporting proporciona inteligencia detallada y un mayor grado de conocimiento sobre las campañas maliciosas que atacan a las organizaciones industriales, así como información sobre las vulnerabilidades que se encuentran en los sistemas de control industrial más populares y las tecnologías subyacentes. La información detallada y adaptada a las organizaciones industriales permite a los clientes proteger activos críticos, incluidos componentes de software y hardware, y garantizar la seguridad y la continuidad de los procesos tecnológicos.

Los informes se envían a través de **Kaspersky Threat Intelligence Portal** y también se puede acceder a ellos a través de una API.

Lo que obtiene:



Informes APT

Informes sobre nuevas campañas de APT (Amenazas Persistentes Avanzadas) y ataques de alto volumen dirigidos a organizaciones industriales, así como actualizaciones sobre amenazas activas.



El entorno de amenazas

Informes sobre cambios significativos en el entorno de amenazas para los sistemas de control industrial, factores críticos recién detectados que afectan los niveles de seguridad de ICS y la exposición de ICS a amenazas, con información regional, nacional y sectorial.



Vulnerabilidades encontradas

Informes sobre vulnerabilidades identificadas por Kaspersky en los productos más populares utilizados en sistemas de control industrial, el Internet Industrial de las Cosas y las infraestructuras de diversos sectores.



Análisis y mitigación de vulnerabilidades

Nuestras asesorías proporcionan recomendaciones prácticas por parte de nuestros especialistas Kaspersky para ayudar a identificar y mitigar amenazas.

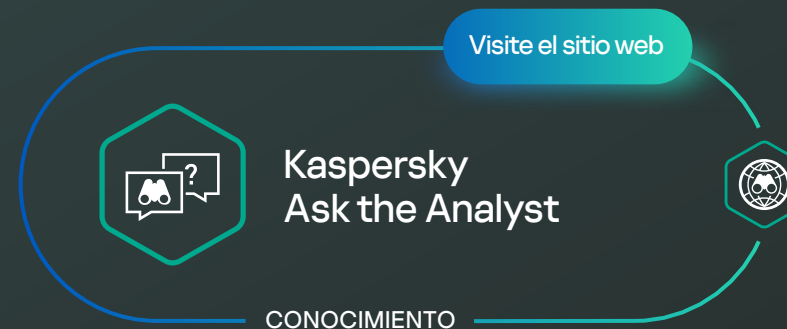
[Contáctenos](#)

[Más información acerca del servicio](#)



*** Información adicional sobre informes publicados:**

- Información sobre vulnerabilidades en el ICS
- Estadísticas de amenazas en el sistema de control de procesos y nuevas tendencias por región e industria
- Análisis de malware dirigido al ICS
- Información acerca de requisitos y estándares regulatorios



Lo que obtiene:

Kaspersky Ask The Analyst complementa nuestra cartera de Kaspersky Threat Intelligence. Gracias a este servicio, podrá comunicarse con especialistas para obtener asistencia e información útil sobre amenazas y vulnerabilidades específicas a las que se enfrenta o que le interesan. Con estos datos, puede mejorar sus defensas contra las amenazas que se dirigen tanto a su organización como a su infraestructura industrial.

Beneficios clave



Acceso a los principales especialistas en inteligencia sobre amenazas, incluidos los expertos en seguridad industrial de ICS CERT Kaspersky



Información contextualizada, detallada y personalizada para realizar investigaciones efectivas



Instrucciones detalladas de nuestros expertos sobre cómo responder con rapidez ante las amenazas y vulnerabilidades

[Contáctenos](#)

[Más información acerca del servicio](#)

Visite el sitio web



Kaspersky Security Awareness

CONOCIMIENTO

Incremente los conocimientos en ciberseguridad de los empleados

- Materiales de capacitación que brindan a sus empleados los conocimientos necesarios acerca de los aspectos más importantes de la ciberseguridad industrial, lo que aumenta el nivel de conciencia en todos los niveles de la organización.
- Kaspersky Interactive Protection Simulation: capacitación basada en juegos, mediante simulaciones de empresas con numerosos escenarios en diferentes industrias: energía termoeléctrica, energía hidroeléctrica, petróleo y gas, productos petroquímicos, holdings de petróleo, etc.
- Kaspersky Automated Security Awareness Platform (ASAP): módulos de aprendizaje interactivo y ataques de phishing simulados diseñados para inculcar un comportamiento de seguridad en el ciberespacio.

Principales temas tratados

- Correo
- Sitios web e Internet
- Contraseñas y cuentas
- Redes sociales y servicios de mensajería instantánea
- Industrial cybersecurity
- Seguridad del equipo
- Dispositivos móviles
- Datos confidenciales
- Seguridad de tarjetas bancarias y PCI DSS
- RGPD



[Contáctenos](#)

[Pruébalo ahora](#)

[Catálogo de entrenamientos](#)

Visite el sitio web

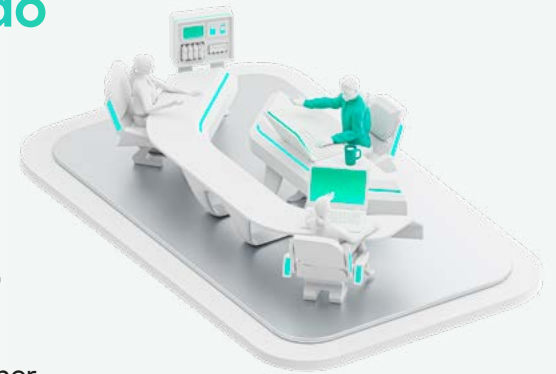


Capacitaciones especializadas en ICS CERT de Kaspersky

CONOCIMIENTO

Aprendizaje aplicado

Nuestro programa de capacitación sobre ICS está diseñado especialmente para garantizar que los profesionales de tecnología de la información (IT), tecnología operativa (OT) y seguridad de la información (IS), así como gerentes y otros empleados, puedan expandir sus conocimientos sobre ciberseguridad industrial y obtener habilidades prácticas especializadas.

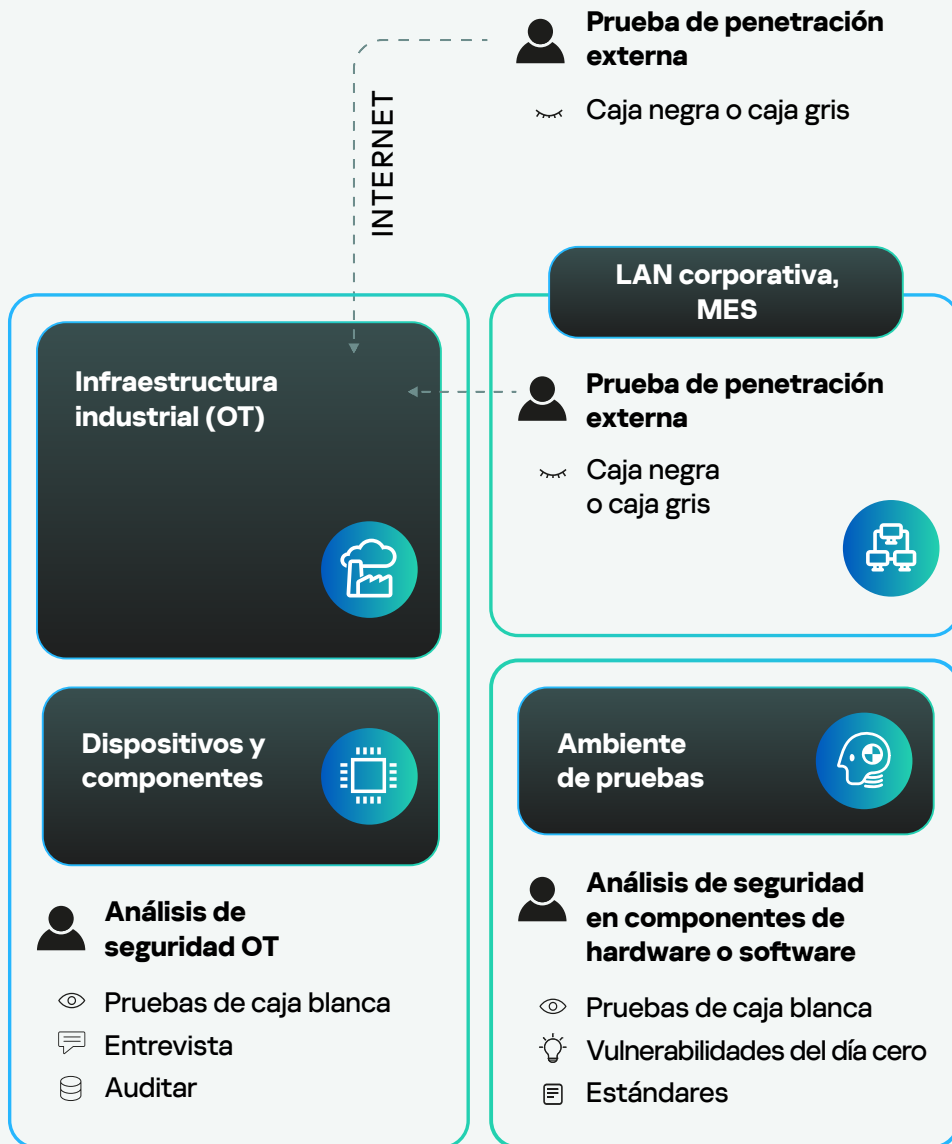


Habilidades prácticas de especialistas de Kaspersky

- Análisis forense digital y respuesta a incidentes
- Exploración de vulnerabilidades en dispositivos OT/IoT y software industrial
- Programas de capacitación multidisciplinaria para especialistas en IT, OT y IS.

[Contáctenos](#)

[Catálogo de entrenamientos](#)



[Visite el sitio web](#)



**Kaspersky
ICS Security
Assessment**

EXPERIENCIA

Análisis de seguridad en su infraestructura industrial

Se trata de un enfoque integral para identificar vulnerabilidades y debilidades de seguridad en infraestructuras industriales, e incluye lo siguiente:

- Superficie de ataque
- El nivel de seguridad de la infraestructura de la red industrial, DCS y dispositivos industriales
- Amenazas de sistemas críticos en riesgo

Verificación de componentes críticos

- Tráfico de la red, incluyendo protocolos industriales
- Componentes de control de procesos: SCADA, PLC, medidores inteligentes, etc.
- Elementos físicos del sistema de control de procesos automatizados
- Arquitectura de red, incluidas las redes de ACS

[Más información acerca del servicio](#)

[Contáctenos](#)



Kaspersky Managed Detection and Response

EXPERIENCIA

Visite el sitio web

Características clave

- Detección proactiva de amenazas: indicadores de ataque patentados permiten rastrear amenazas no detectadas dentro del sistema de control
- Respuesta guiada y automatizada (con investigación forense completa y análisis de malware disponible a pedido)
- Experiencia en ciberseguridad de ICS: respaldada por uno de los equipos de detección de amenazas proactiva con más experiencia y éxito de la industria

Lo que obtiene:

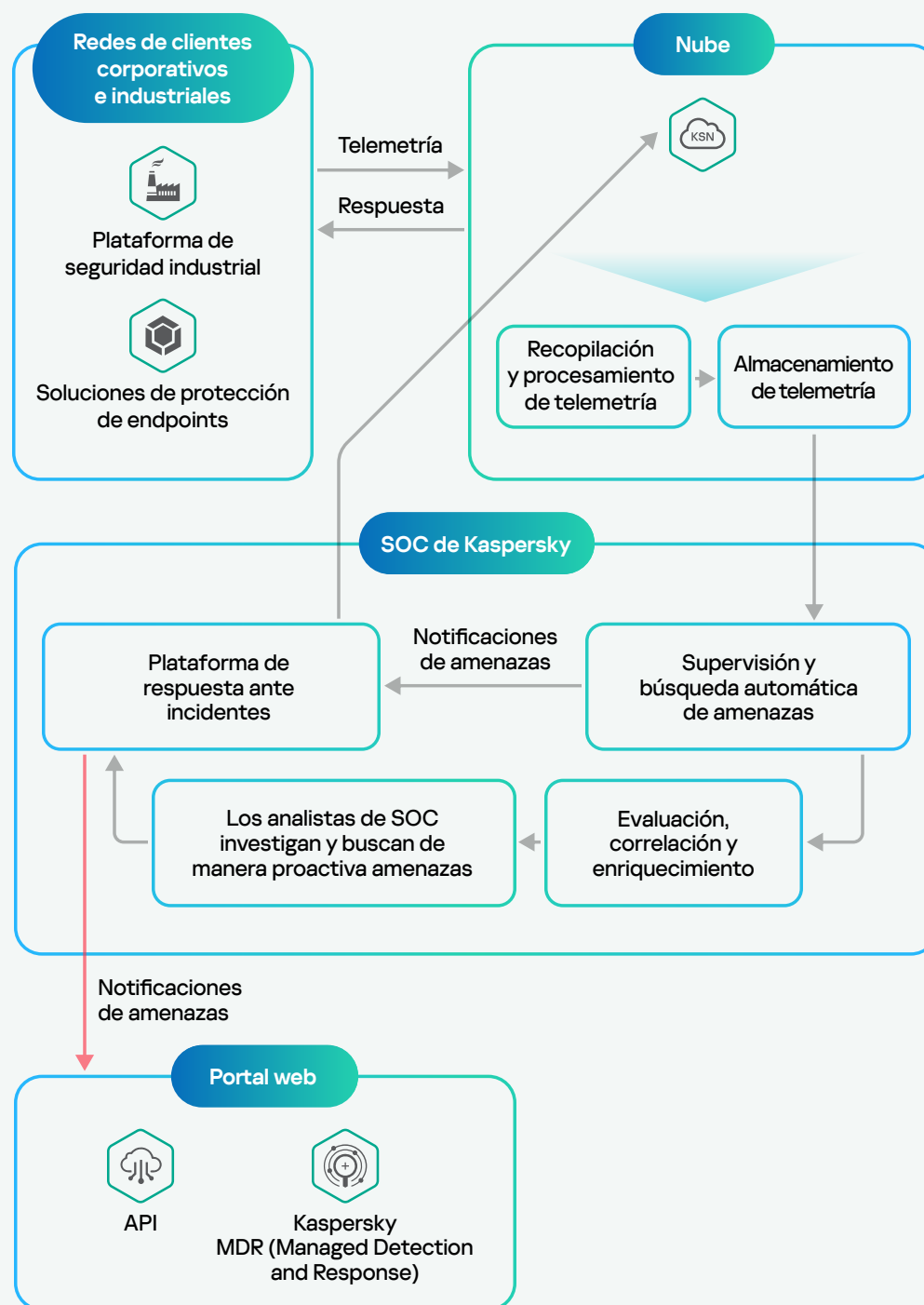
- Búsqueda, detección y eliminación continuas de amenazas que tienen como objetivo a su organización industrial
- Menos costos de seguridad, al eliminar la necesidad de contratar a nuevos expertos en ciberseguridad
- Todos los beneficios de un SOC, sin tener que establecer uno en su organización

Un 25 % de nuestros clientes protegidos pertenece al sector industrial

Consulte el [informe de MDR](#) para obtener más información

[Contáctenos](#)

[Más información acerca del servicio](#)



Visite el sitio web



Kaspersky Incident Response

EXPERIENCIA

Respuesta a incidentes

Riesgo

Una sola vulnerabilidad es suficiente para que los ciberdelincuentes tomen el control de los sistemas industriales en su totalidad

Solución

- Eliminación rápida de las consecuencias de un incidente por parte del equipo global de respuesta a emergencias (GERT) de Kaspersky
- Análisis de las causas, fuentes y consecuencias del incidente
- Vista detallada del malware utilizado
- Soporte adicional por ICS CERT de Kaspersky

Componentes del servicio



Respuesta a incidentes:
investigación y eliminación de amenazas



Investigación forense digital:
análisis de evidencia digital



Análisis de malware:
vista detallada de los archivos utilizados en un ataque

[Solicite el Manual de Respuesta ante incidentes de ICS CERT de Kaspersky](#)

[Más información](#)

[Contáctenos](#)



Descubra las tendencias de respuesta a incidentes en la investigación del equipo global de respuesta a emergencias de Kaspersky (GERT).

Un partner en quien puede confiar



26 años de experiencia de clase mundial y petabytes de datos de amenazas



ICS CERT: división internacional propia de investigación en seguridad sobre tecnología operativa (OT) e Internet de las cosas (IoT)



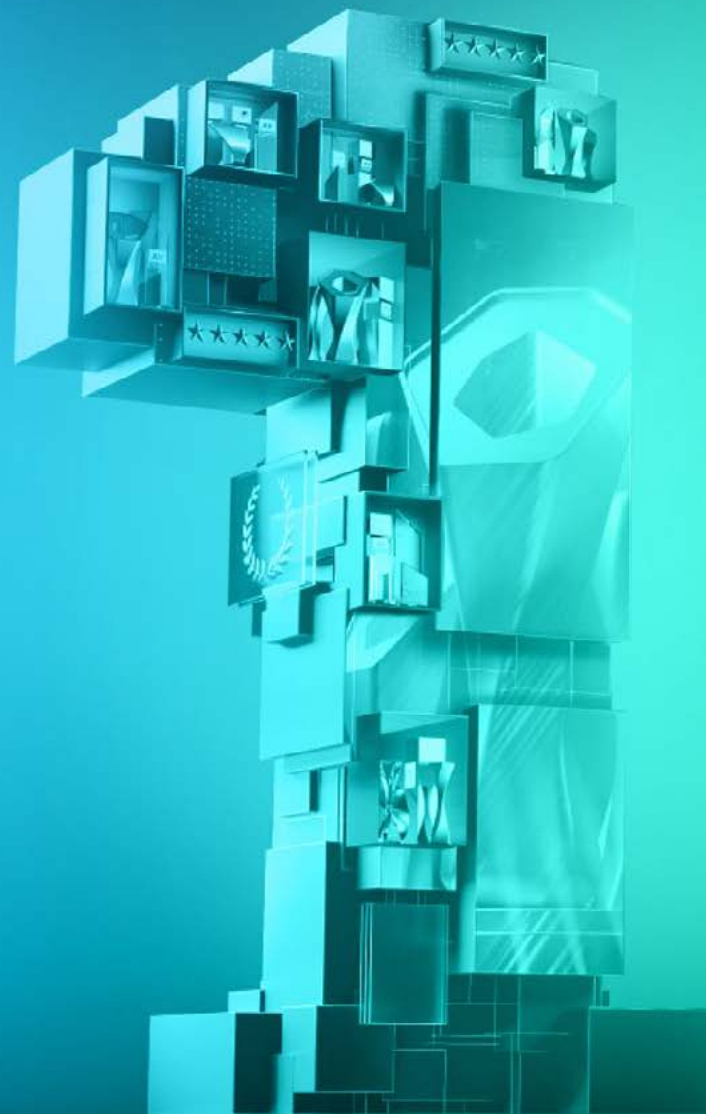
Experiencia probada en la industria de la seguridad de IT y OT, con numerosos premios y logros



Más de 100 certificados de interoperabilidad con soluciones de automatización



Efectividad de la tecnología probada y cumplimiento con estándares y requisitos



[Más información
acerca del entorno OT](#)

[Más información
acerca del entorno IT](#)

[Contáctenos](#)