

Kaspersky OT CyberSecurity

Ofertas del mercado vertical
para operadores de redes y
sistemas eléctricos, centrales
eléctricas y servicios públicos

kaspersky



Resumen del sector

El sector de energía y servicios públicos es fundamental para la sociedad, dado que desempeña un papel central en el impulso del crecimiento económico, la mejora de la calidad de vida y el apoyo de los avances tecnológicos. La electricidad es un recurso esencial debido a que alimenta diversas áreas clave, incluidas las siguientes:



Uso residencial y ciudades inteligentes
(alumbrado público, HVAC, etc.)



Transporte
(vehículos eléctricos, carga)



Industria manufacturera

El sector desempeña un papel importante para lograr la neutralidad de carbono en consonancia con los objetivos del Acuerdo de París (ONU). El sector respalda la electrificación en otros sectores e impulsa la transición hacia la energía renovable.

La tendencia del sector hacia la energía limpia exige redes inteligentes eficientes y sólidas.

~2 veces más

inversión mundial en energía limpia en comparación con combustibles fósiles¹

(1) Inversión mundial en energía 2024, informe de IEA

Objetivos de la digitalización

La digitalización es un facilitador de los objetivos de sostenibilidad del sector, ya que ofrece soluciones digitales que respaldan los objetivos estratégicos de los protagonistas del sector:



Mejorar la seguridad y eficiencia de los activos



Impulsar la descarbonización y electrificación globales



Agilizar la implementación de infraestructura con energía renovable



Garantizar condiciones laborales seguras

Principales casos de uso de la solución digital en el sector

- Dispositivos de Internet de la energía (IoE)
Facilitar la automatización en áreas extensas para llevar a cabo la supervisión y el control en tiempo real de las operaciones de la red
- Nube de energía
Análisis en tiempo real, infraestructura escalable, administración remota e integración de tecnologías nuevas
- Gemelos digitales eléctricos
Simulación del modo de la red, información predictiva, supervisión en tiempo real y diagnóstico de los equipos
- Red inteligente con tecnología de aprendizaje automático e IA
Optimización, mantenimiento predictivo y supervisión de las condiciones
- Robotización
Inspecciones robóticas y aéreas de la planta, administración de vegetación

A medida que la digitalización transforme el sector, las operaciones se enfrentarán inevitablemente a desafíos relativos a la seguridad.

Los sistemas eléctricos necesitarán contar con capacidades ampliadas de comunicación y automatización que sean seguras, confiables y efectivas.

2.3 p.p.

Disminución en la cantidad de computadoras del ICS en el sector energético en las que se bloquearon objetos maliciosos en el primer trimestre de 2025 (en comparación con el primer trimestre de 2024)²

(2) Informe de ICS CERT sobre el panorama de amenazas para los sistemas de automatización industrial

Tendencias digitales en el sector energético y de servicios públicos

Salas de control integradas

A. Generación de energía

- Central nuclear
- Central térmica
- Central de energía solar
- Central hidroeléctrica
- Granjas eólicas

Corporativo

- Sistemas y redes de TI
- Sistema de administración de mercados

Centro de control

- SCADA/EMS/GMS
- ADMS/WAMS/DERMS/OMS

B. Transmisión de energía

- Tendido eléctrico
- Transformadores eléctricos automáticos
- Subestaciones de HV aisladas de aire y gas
- Transformadores eléctricos de HVDC
- Almacenamiento y conversión de energía
- Subestaciones marinas y HVDC

C. Distribución de energía

- Consumidores industriales y sociales
- Redes eléctricas de media tensión en los suburbios
- Ciudades y redes inteligentes

IoT

- 1 Medición inteligente de energía y calor
- 2 Supervisión del estado de equipos principales
- 3 Administración de recursos energéticos distribuidos (DER)
- 4 Supervisión del estado de la línea de transmisión y distribución (T&D)
- 5 Supervisión de estaciones de carga y vehículos conectados

Nube de energía

- 1 Análisis predictivo del suministro mediante pronósticos meteorológicos y otros datos
- 2 Las WAN facilitan la comunicación en tiempo real entre los sistemas de TO, los sensores y los centros de control de la red
- 3 Los sistemas de información de red (NIS) proporcionan las rutas y la topología de la red a los operadores de la red de distribución

Gemelos digitales eléctricos

- 1 Administración del rendimiento de los activos con supervisión de equipos y análisis de causa raíz
- 2 Asignación de grupos de riesgo para visualizar áreas con riesgos concentrados y evitar fallas en cascada
- 3 Simulación del almacenamiento de energía para optimizar planes de suministro y análisis de picos de demanda

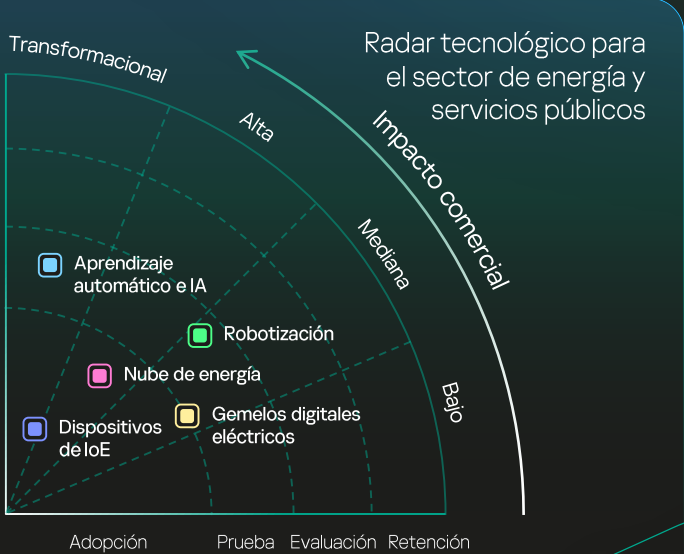
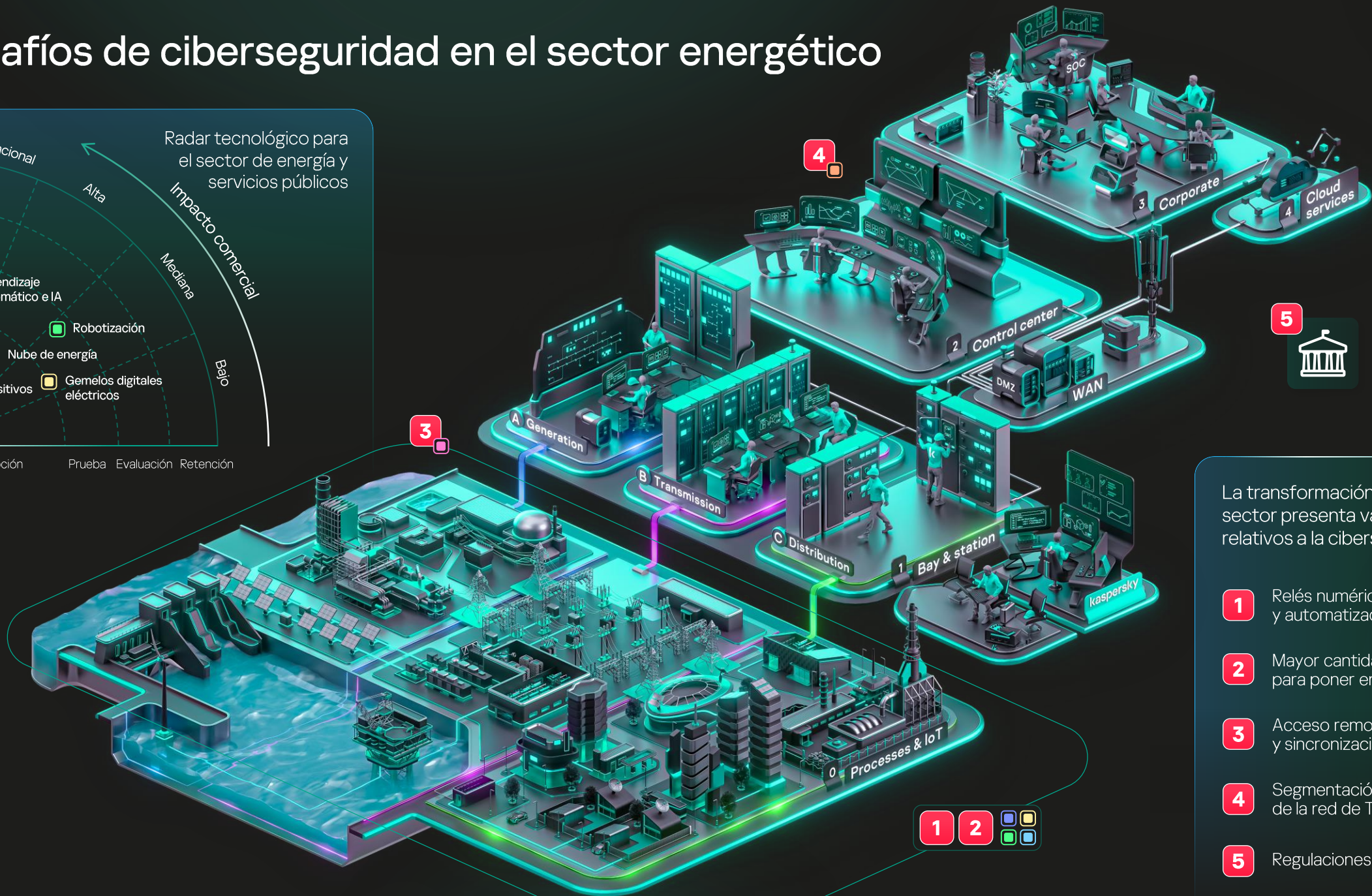
Aprendizaje automático e IA

- 1 Balanceo de redes mediante el ajuste dinámico de los flujos de energía, la disminución de pérdidas y la prevención de sobrecargas
- 2 Optimización de potencia reactiva y control de tensión para evitar bajas de voltaje
- 3 Análisis de datos provenientes de infraestructuras de medición inteligente para optimizar la comercialización y equilibrar los picos de demanda
- 4 Predicción de patrones climáticos para ajustar las posiciones de las aspas

Robotización

- 1 Drones con sensores integrados para topografía aérea
- 2 Automatización de actividades de inspección para identificar problemas potenciales (p. ej., zonas calientes, fugas, tendidos eléctricos, etc.)
- 3 Inspección submarina de granjas eólicas marinas

Desafíos de ciberseguridad en el sector energético

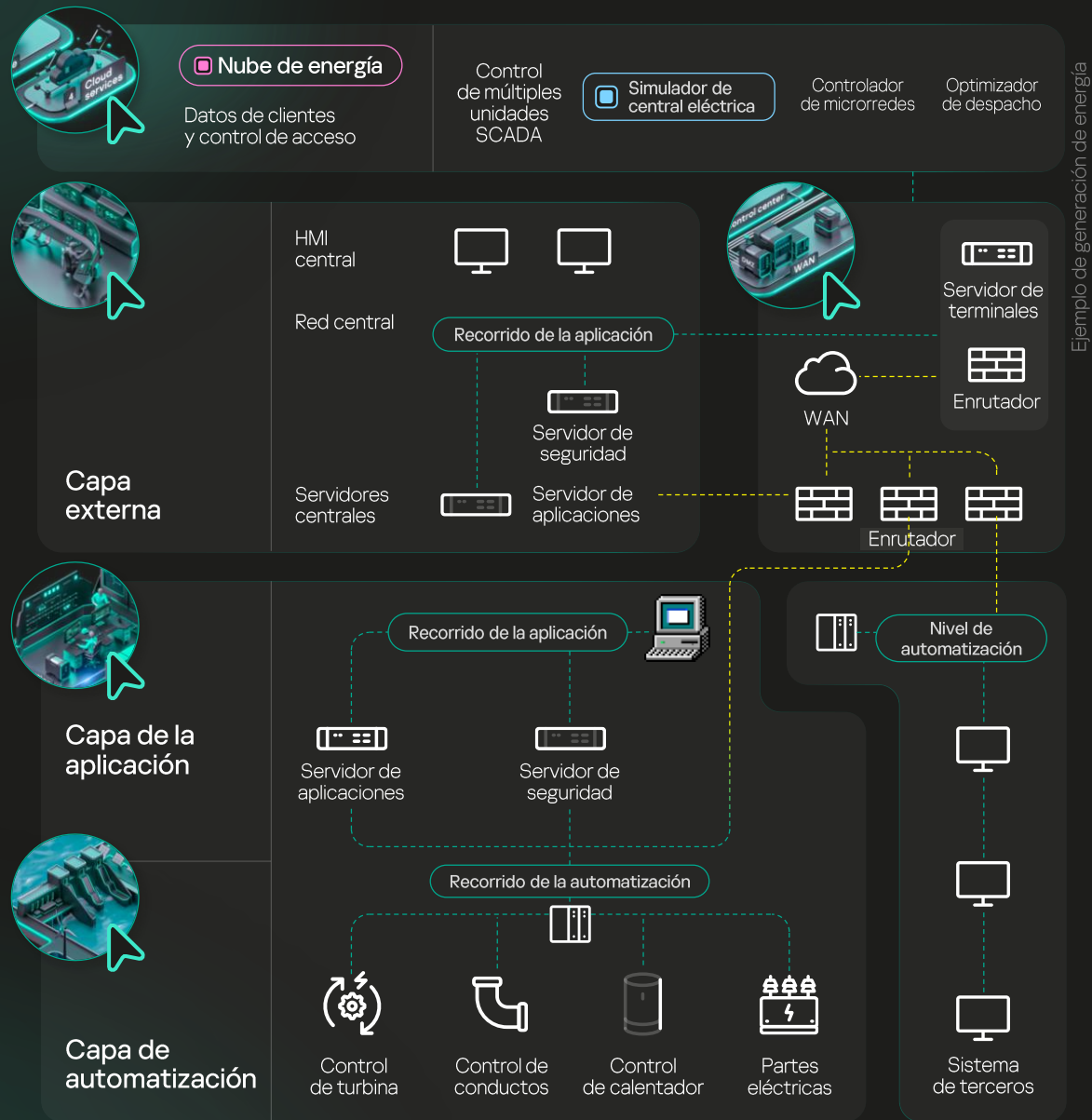


La transformación digital en el sector presenta varios desafíos relativos a la ciberseguridad

- 1 Relés numéricos desactualizados y automatización
- 2 Mayor cantidad de nodos para poner en riesgo
- 3 Acceso remoto en riesgo y sincronización de tiempo
- 4 Segmentación deficiente de la red de TI y TO
- 5 Regulaciones del CIP

Relés numéricos desactualizados y automatización

■ Nube de energía ■ Aprendizaje automático e IA



La integración de sistemas desactualizados con tecnologías modernas como el aprendizaje automático, la IA y la nube presenta varios desafíos clave. Pueden producirse problemas de compatibilidad cuando los sistemas más antiguos tienen dificultades para interactuar con tecnologías más recientes. La interoperabilidad limitada puede interrumpir las operaciones y reducir las ganancias de eficiencia que ofrecen las soluciones modernas. En particular, los sistemas heredados a menudo no pueden comunicarse de forma efectiva con las plataformas en la nube o las herramientas de automatización con tecnología de IA.

El hardware heredado representa actualmente

>1/3

del consumo de energía total de las organizaciones⁽¹⁾

(1) Estudio de Daisy Corporate Services

Características de la solución

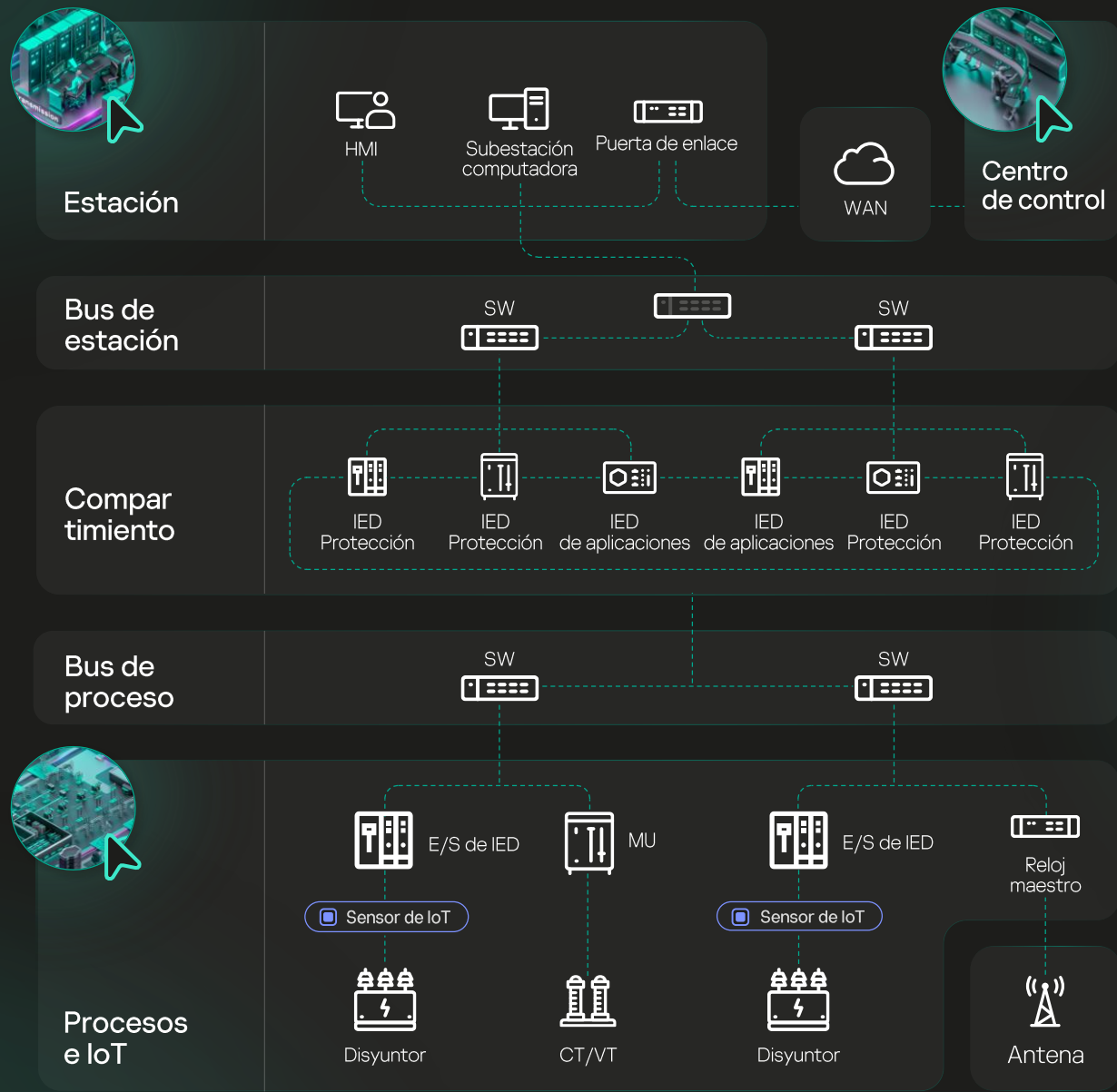
Característica	Valor (1-3)
Tiempo de implementación	3
Costo del producto	2
Competencias del personal	1
Cantidad de personal	1
Impacto comercial	2

¿Cómo lo ayuda Kaspersky?

Kaspersky Industrial CyberSecurity	Kaspersky Machine Learning for Anomaly Detection	Kaspersky ICS Threat Intelligence
<ul style="list-style-type: none">Supervisión continua de redes industriales para detectar vulnerabilidadesDetección y respuesta en endpointsAuditorías de seguridad regulares	<ul style="list-style-type: none">Predice fallas en sistemas de relé antiguos mediante el aprendizaje automáticoDetecta ciberamenazas que apuntan a relés desactualizados	<ul style="list-style-type: none">Análisis integral para identificar y evaluar la exposición a riesgos y los niveles de seguridad de las infraestructuras de redes industriales

Ecosistema de servicios de respaldo

Mayor cantidad de nodos para poner en riesgo

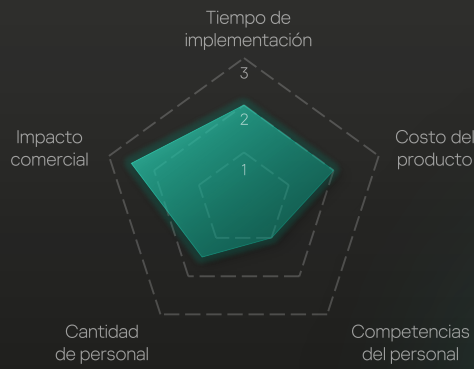


Ejemplo de subestación digital

La integración de robótica e IoT en las subestaciones crea más puntos de entrada para los ciberataques, ya que cada dispositivo no protegido es un potencial objetivo.

La administración y la aplicación de parches en diferentes dispositivos conectados es desafiante, y una única vulneración puede tener repercusiones en todos los sistemas y provocar una interrupción generalizada.

Características de la solución



¿Cómo lo ayuda Kaspersky?



- Visibilidad de la red y detección de anomalías
- DPI de comunicaciones industriales con capacidades de aprendizaje automático
- Auditoría detallada del sistema

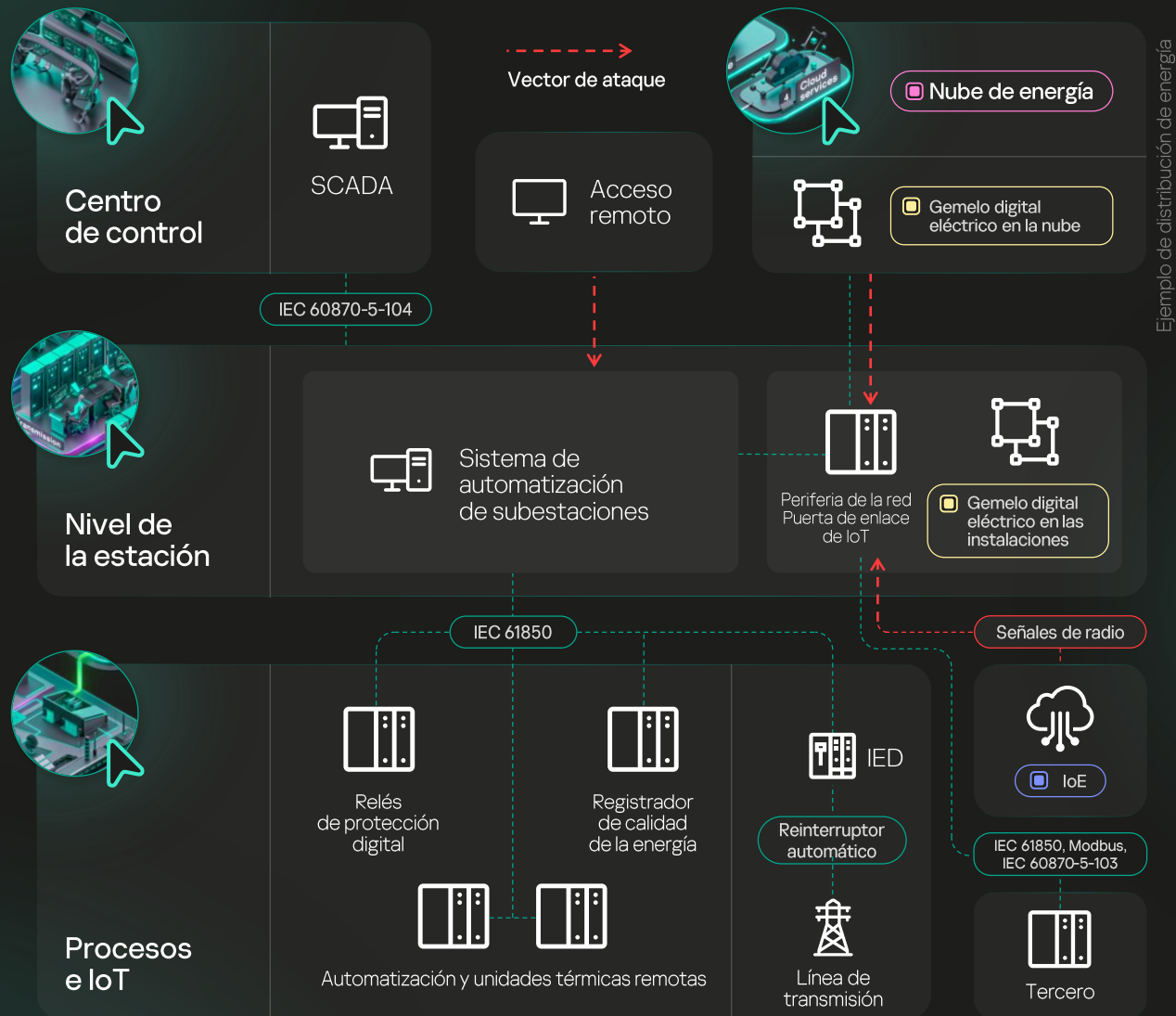
Ecosistema de servicios de respaldo



- Búsqueda de amenazas e investigación de incidentes
- Supervisión de seguridad

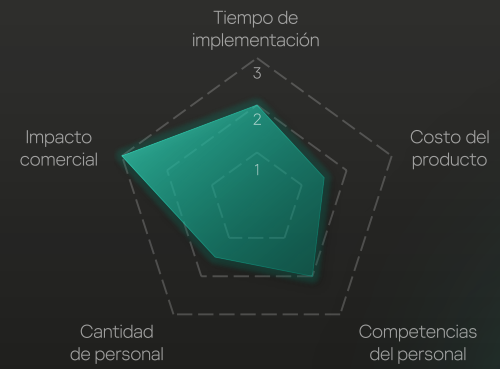
Conexiones en riesgo y sincronización de tiempo

- IoE
- Nube de energía
- Gemelos digitales eléctricos



La integración de tecnologías como IoE, gemelos digitales y servicios en la nube en las subestaciones de energía aumenta el riesgo de recibir ciberataques debido a las conexiones en riesgo, que pueden permitir el acceso no autorizado a las redes de control y los sistemas SCADA. Además, es fundamental mantener una sincronización de tiempo precisa para los relés de protección y las unidades de medición de fasores, ya que un error puede dar lugar al funcionamiento defectuoso de los dispositivos de la red

Características de la solución



¿Cómo lo ayuda Kaspersky?

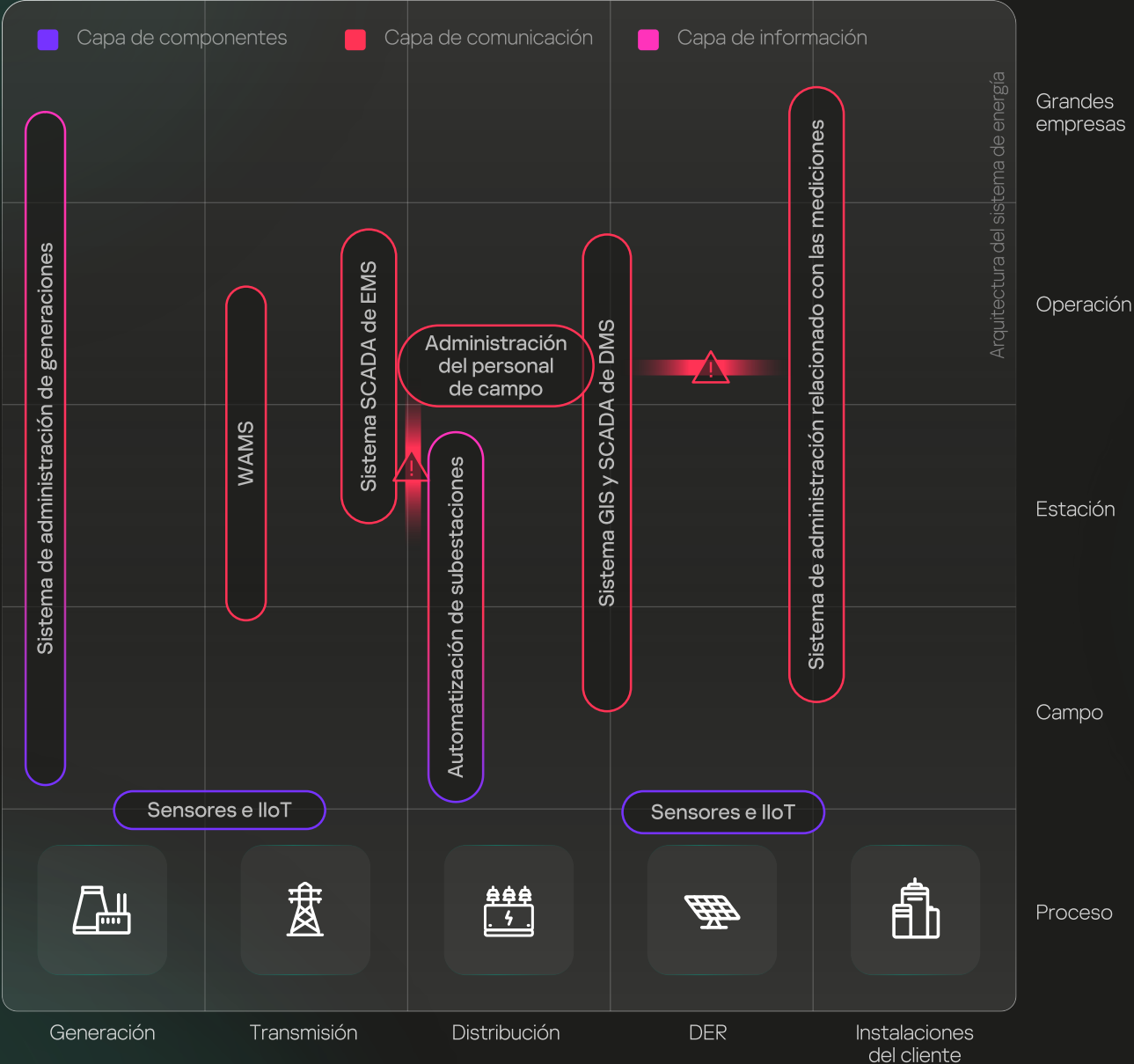


- Protección sólida de endpoints físicos y virtuales
- Cobertura integral en todas las infraestructuras complejas



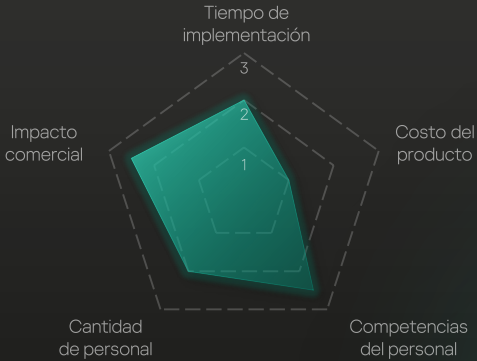
- Conexión y diseño remotos del personal y los contratistas
- Supervisión y administración centralizadas de todos los eventos de la infraestructura de clientes ligeros

Segmentación deficiente de la red de TI y TO



La segmentación inadecuada de la red en redes eléctricas, especialmente con la integración de gemelos digitales, puede generar vulnerabilidades de seguridad significativas. Cuando estas redes no se segmentan adecuadamente, la naturaleza interconectada de los gemelos digitales puede aumentar el riesgo de los ciberataques que abarcan de sistemas de TI a infraestructuras críticas de TO. Esto puede interrumpir la distribución de energía y provocar cortes generalizados

Características de la solución



¿Cómo lo ayuda Kaspersky?



Kaspersky Industrial CyberSecurity

- Análisis del tráfico de red para identificar anomalías y amenazas
- Protección, detección y respuesta en endpoints
- Segmentación de red y cumplimiento del uso



Kaspersky SD-WAN

- Supervisión en tiempo real de la red distribuida
- Visibilidad de la red
- Seguridad y administración unificadas de la red



Kaspersky ICS Security Assessment

- Identifica las deficiencias de seguridad en la arquitectura de la red
- Proporciona recomendaciones prácticas para la resolución
- Prueba de penetración interna

Ecosistema de servicios de respaldo

Regulaciones del CIP

Las regulaciones de ciberseguridad para el sector de energía y servicios públicos varían mundialmente, pero comparten un objetivo en común: mejorar la resiliencia, proteger la infraestructura importante y garantizar la continuidad del servicio. Muchos países implementaron regulaciones para garantizar que los proveedores de electricidad y los operadores de redes adopten prácticas sólidas de ciberseguridad, lleven a cabo evaluaciones de vulnerabilidad regulares y se adhieran a protocolos estandarizados de respuesta ante incidentes.



Global

- ISA/IEC 62443
- IEC 62351 (IEC 61850 TR)
- ISO/IEC 27019
- IEEE 1547.3-2023, C37.240, 1686
- Serie n.º 17-T de seguridad nuclear de IAEA



Emiratos Árabes Unidos

- Estrategia Nacional de Ciberseguridad
- Marco de protección de la infraestructura de información crítica (CI) de DESC
- Política CIIP de NESA



Arabia Saudita

- Controles de ciberseguridad de TO-1:2022
- Controles de ciberseguridad esenciales ECC-1:2018



India

- Directrices y regulaciones de ciberseguridad de CEA
- Pautas del NCIIPC
- Directrices CERT-In
- Directrices y códigos de seguridad de AERB



Brasil

- Estrategia de ciberseguridad nacional (E-Ciber)
- Resolución n.º 964/2021 de ANEEL
- PRODIST módulo 8 de ANEEL



China

- GB/T 44462.1-2024
- GB/T 36572-2018
- GB 42250-2022
- GB/T 36627-2018



Indonesia

- PR 47/2023 Estrategia de ciberseguridad nacional y administración de crisis cibernéticas
- BSSN Reg. 1/2024 Administración de ciberincidentes
- BSSN Reg. 2/2024 Administración de crisis cibernéticas



Turquía

- Plan de ciberseguridad de NDK para centrales de energía nuclear
- Regulación BTK CIPR
- Ley de Ciberseguridad n.º 7545



Sudáfrica

- Ley de Protección de Infraestructuras Críticas
- Directrices RG-0014 de NNR
- Marco de política de ciberseguridad nacional



Malasia

- Directrices CNII de NACSA
- Directrices de ciberseguridad de Malasia (MyVAC)
- Reglas de ciberseguridad de Suruhanjaya Tenaga



Egipto

- Directrices técnicas de ENRRA para la ciberseguridad de instalaciones nucleares



Tailandia

- NCSA B.E. 2566
- NCSA B.E. 2562
- NCSA B.E. 2564



Europa

- Directiva NIS2
- Directiva CER
- Directrices ENISA
- Código de red sobre ciberseguridad para flujos de electricidad transfronterizos



EE. UU.

- NERC CIP
- Marco de Ciberseguridad del NIST
- Guía normativa de NRC



Alemania

- IT-Sicherheitsgesetz 2.0
- Energiewirtschaftsgesetz
- BSI KritisV/BDEW- B3S



España

- Esquema Nacional de Seguridad
- Real Decreto 704/2011 de CNPIC
- Guías de Seguridad CCN-STIC



Francia

- Estrategia Nacional de Ciberseguridad
- Marco normativo de Ciberseguridad para ICS de la ANSSI
- Ley de Protección de la Infraestructura de Información Crítica



Países Bajos

- Estrategia de Ciberseguridad de los Países Bajos (NLCS)
- Ley de Seguridad de Redes y Sistemas de Información (WBNII)
- Guía para las Medidas de Ciberseguridad del NSCS



UK

- Normas de seguridad de industrias nucleares (NISR)
- NCSC CAF
- Directrices de TO de NCSC
- Ciberseguridad para IACS (OG86)

¿Cómo lo ayuda Kaspersky?

Las soluciones de Kaspersky protegen centrales eléctricas, subestaciones, redes y otros elementos del sistema de energía para mantener la continuidad de las operaciones críticas de industrias y servicios públicos mediante un enfoque de defensa en profundidad.



Kaspersky Industrial CyberSecurity

Soluciones para redes eléctricas que cumplen con ISA/IEC 62443, NIS2, SOC 2 Tipo 2, ISO/IEC 27001, GB 42250-2022



Compatibilidad probada:



Más de 150

sistemas de más de 50 proveedores

Kaspersky Security Awareness y capacitación para expertos

Capacite a los empleados con capacidades de ciberseguridad esenciales para cumplir con los requisitos de la directiva NIS2.

Obtenga más información acerca de la Directiva NIS2 y la conformidad de nuestro producto

Ciberresiliencia con el ecosistema de TO de Kaspersky

					
Inventario y activos	Seguridad esencial	Detección de amenazas avanzadas, auditorías y cumplimiento	Segmentación de red	Operaciones de seguridad maduras	Tolerancia a las fallas y capacidad de respuesta
Experiencia	Tecnología	Conocimientos + Tecnología + Experiencia	Conocimientos + Tecnología + Experiencia	Conocimientos + Tecnología + Experiencia	Tecnología
Detección de activos de la red <ul style="list-style-type: none">Identifique todos los activos de hardware y software dentro de la infraestructura de TOCree un inventario detallado para planificar su estrategia de ciberseguridad Inventario de endpoints <ul style="list-style-type: none">Catalogue los componentes de hardware y softwareMantenga un inventario actualizado para identificar los activos y las vulnerabilidades críticas Desarrollo de políticas <ul style="list-style-type: none">Desarrolle políticas y procedimientos integrales.Utilice el análisis de riesgos e impactos para establecer niveles de ciberseguridad e identificar los controles requeridos.	Consolidación del SO <ul style="list-style-type: none">Configure los sistemas de forma segura y aplique parches y actualizaciones con regularidadImplemente controles adicionalesPrevención de exploits y comprobación de dispositivos extraíbles Control de aplicaciones <ul style="list-style-type: none">Restrinja aplicaciones no autorizadas para mantener la integridad del sistema Protección de endpoints <ul style="list-style-type: none">Implemente soluciones antimalware para proteger los dispositivos dentro de los entornos de ICS y TO	Visibilidad de la red <ul style="list-style-type: none">Supervise el tráfico de la red para detectar anomalías y comprender los patrones de ataque. Detección de anomalías y amenazas <ul style="list-style-type: none">Utilice el aprendizaje automático y la DPI para identificar intrusiones y anomalías de la redUtilice la tecnología EDR para supervisar la telemetría del host de TO Auditorías de seguridad <ul style="list-style-type: none">Lleve a cabo auditorías de cumplimiento y análisis de vulnerabilidades. Control de configuración <ul style="list-style-type: none">Mantenga auditorías detalladas del sistema y controle las configuraciones. Administración de cumplimiento <ul style="list-style-type: none">Garantice el cumplimiento de requisitos regulatorios y estándares de la industria.	Prevención de intrusiones <ul style="list-style-type: none">Mejore las capacidades de prevención y detección de amenazas avanzadas al integrarlas con el equipo de red existente. Flujo de datos restringido <ul style="list-style-type: none">Utilice SD-WAN y VLAN para optimizar la segmentación y el flujo de datosAplique controles de seguridad, incluso en ubicaciones remotas y más pequeñas. Controles de IIoT <ul style="list-style-type: none">Implemente visibilidad de los controles de seguridad con puertas de enlace avanzadas seguras por diseño y protocolos para dispositivos IIoT Acceso remoto <ul style="list-style-type: none">Utilice clientes ligeros y puertas de enlace seguros para el acceso remoto controlado	Inteligencia de amenazas para SOC industriales <ul style="list-style-type: none">Utilice la inteligencia de amenazas en tiempo real para protegerse de malware, phishing, vulnerabilidades y exploits. Consultoría SOC <ul style="list-style-type: none">Interactúe con expertos para mejorar la capacidad de su SOC para gestionar amenazas sofisticadas. Detección y respuesta entornos de convergencia de TI/TO <ul style="list-style-type: none">Integre la seguridad de TI y TO para la detección y respuesta unificadas de amenazas Protección administrada <ul style="list-style-type: none">Utilice los servicios administrados de detección y respuesta para la supervisión continua y la gestión experta de incidentes	Capacitación con expertos <ul style="list-style-type: none">Proporcione capacitación especializada en ciberseguridad para que el personal gestione y mitigue las fallas de forma eficaz Capacitación de concientización <ul style="list-style-type: none">Lleve a cabo sesiones de capacitación regulares para aumentar la tolerancia general a las fallas y la preparación entre todos los empleados Análisis del rendimiento de los activos <ul style="list-style-type: none">Utilice las herramientas y metodologías para analizar el rendimiento de los activos, garantizar la confiabilidad e identificar fallas potenciales

Obtenga más información acerca del enfoque de Kaspersky en torno a la ciberseguridad integral en todos los niveles



Trayectoria de Kaspersky en el sector de energía y servicios públicos

<div>Más de 10 años</div> <div>de experiencia activa en el sector</div>	<div>Más de 80 proyectos</div> <div>completados en los sectores nuclear, térmico, hidráulico y otros sectores de energía, incluidas las renovables</div>	<div>Más de 40 empresas de energía y servicios públicos</div> <div>protegidas por Kaspersky</div>	<div>Más de 60.000 licencias</div> <div>emitidas a los clientes</div>
<div>Kaspersky OT CyberSecurity proporciona protección integral para la infraestructura industrial de las empresas de energía en todos los niveles</div> <div>Por qué las empresas de energía y servicios públicos eligen Kaspersky</div>	<div></div> <div>Respalda el cumplimiento y la compatibilidad</div> <div><ul style="list-style-type: none">Soluciones que se sometieron a pruebas de compatibilidad con productos de los proveedores más importantesProporciona medidas de ciberseguridad que cumplen con varios estándares regulatorios</div>	<div></div> <div>Desarrollo de arquitecturas escalables</div> <div><ul style="list-style-type: none">Mejora la transparencia en el ICS y tiene en cuenta las necesidades específicas de las empresas de redes eléctricasRespalda los sistemas heredados y contemporáneos, y garantiza que todos los componentes del ICS estén protegidos</div>	<div></div> <div>Se integra en un ecosistema sólido</div> <div><ul style="list-style-type: none">Solución de un único proveedor que ofrece protección integral a través de un ecosistema unificadoIntegra sectores corporativos e industriales en una infraestructura unificada segura con seguridad integral</div>

Casos de estudio exitosos del sector de energía y servicios públicos

Solo en la última década, Kaspersky:

 Entregó servicios de ciberseguridad para la **cuarta empresa de producción de electricidad más grande del mundo** que cuenta con uno de los cinco complejos de energía hidroeléctrica por capacidad instalada

 Implementó soluciones de protección en el proveedor de electricidad nacional más grande responsable de la generación del **17 % de la electricidad total del país**

 Ejecutó un proyecto de protección de infraestructura industrial para **uno de los 5 principales productores de energía renovable** con más de 600 instalaciones de generación de energía

www.kaspersky.es

© 2025 AO Kaspersky Lab.
Las marcas registradas y las marcas de servicio pertenecen a sus respectivos propietarios.



El operador de energía más grande de Serbia

[Más información](#)

Eligió las soluciones de Kaspersky después de una evaluación exhaustiva de las ofertas de los competidores. Los factores decisivos para la selección incluyeron las propuestas de un socio local y la compatibilidad completa con la infraestructura de TI existente.

Implementó KICS for Nodes y KICS for Networks, y tiene planificado implementar nuestra plataforma SIEM de KUMA.

€500 M de ventas **34** subestaciones reservadas para la implementación de KICS



Empresa de transmisión de energía grande

[Más información](#)

KICS for Nodes protege más de 150 servidores y estaciones de trabajo en el ciclo de procesos de Grid Company Group, mientras que 10 servidores de KICS for Networks supervisan segmentos clave de la red industrial.

19239 MVA Capacidad instalada **388** Subestaciones



Generador y minorista de electricidad

[Más información](#)

Evaluación de vulnerabilidades de sus redes industriales para identificar debilidades y áreas de mejora en la seguridad.

Simulación de vectores de ataque específicos del sector para detectar vulnerabilidades, actividades maliciosas y anomalías.

1 M hogares suministrados **10 %** de la generación de electricidad total de Singapur



La central nuclear n.º 1 de Rusia por capacidad instalada

[Solicitud Estudio de caso](#)

Implementó Kaspersky Industrial CyberSecurity para proteger la infraestructura en todos los niveles, de servidores y estaciones de trabajo SCADA a controladores lógicos programables (PLC) y equipos de red.

4.337 MW de potencia **7 M** consumidores

Administre su seguridad con Kaspersky y conviértase en socio

Comuníquese con nosotros y participe de nuestra conferencia mundial para clientes

Más información 

#kaspersky
#bringonthefuture