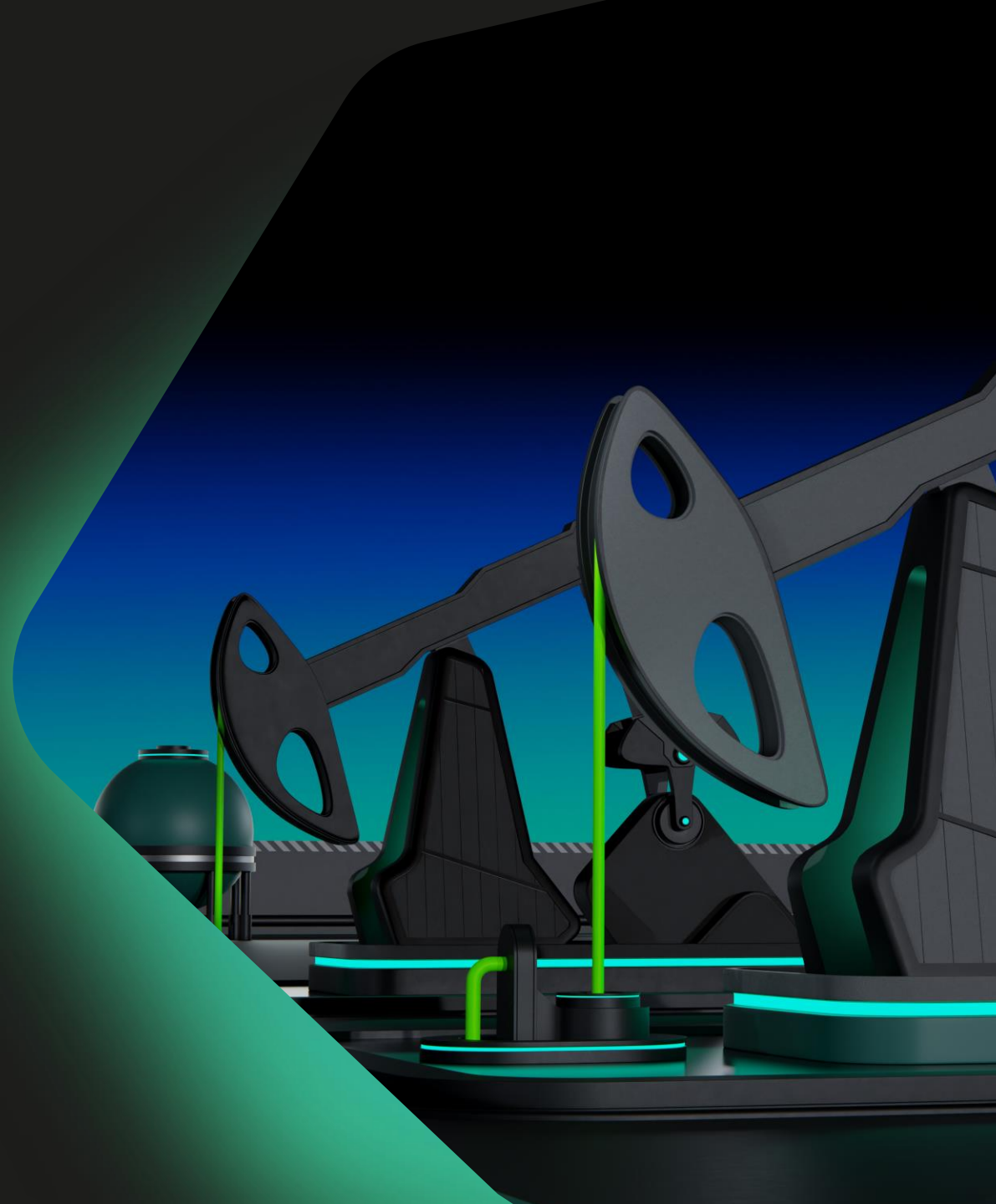


Kaspersky OT CyberSecurity

Ofertas del mercado
vertical para empresas
de petróleo y gas



Resumen del sector

El sector de petróleo y gas domina el mercado de la energía y tiene un gran impacto en la economía global. La alta demanda de mano de obra y el creciente consumo de calefacción y electricidad resaltan la importancia de este sector. Más allá del sector energético, el petróleo, el gas y el GNL son indispensables para lo siguiente:



Construcción y materiales de alta tecnología



Químicos y fertilizantes



Ciencias biológicas y farmacéutica



Muchos otros ámbitos vitales

En los últimos años, las empresas de petróleo y gas también desempeñaron un papel importante en la transición a la sostenibilidad al sacar provecho de sus amplios recursos, experiencia e infraestructura para facilitar este cambio.

Las estrategias se concentran en lo siguiente:



Transformación de factores ESG



Los 17 objetivos de desarrollo sostenible (SDG) de la ONU⁽¹⁾

Acciones y tecnologías facilitadoras que respaldan una estrategia de sostenibilidad

Tendencias de digitalización

- Soluciones de aprendizaje automático e inteligencia artificial utilizadas en el mantenimiento predictivo y para mayor confiabilidad
- Convergencia de sistemas de TI y TO
- IIoT y sensores para monitoreo
- Gemelos digitales para simular la optimización de procesos
- Tecnologías de realidad aumentada y realidad virtual para la capacitación de empleados
- Robotización y automatización para gestionar tareas peligrosas

Acciones digitales

- Cumplimiento con iniciativas y directivas
- Electrificación, solarización y eficiencia energética
- Aumento de la ciberseguridad
- Renovación de equipos

Seguir la estrategia de sostenibilidad mediante la implementación de instrumentos de digitalización resulta imposible sin una ciberseguridad estable, ya que esta minimiza el riesgo que proviene de las interrupciones de la producción.

Una mayor inversión en la ciberseguridad dio lugar a una reciente disminución de la cantidad de ataques.

Iniciativas de sostenibilidad de empresas de petróleo y gas

- Energía baja en carbono
- Neutralidad de carbono
- Conservación del agua (evitar derrames)
- Reducción de residuos (circularidad de productos)
- Protección de la biodiversidad
- Aseguramiento de la seguridad de las personas (cero accidentes fatales y menor tasa total de incidentes registrables⁽²⁾)
- Respeto por los derechos humanos
- Lucha contra la corrupción
- Colaboración con las partes interesadas



Disminución de equipos de ICS atacados en el sector de petróleo y gas en la segunda mitad de 2023 (en comparación con la segunda mitad de 2021)⁽³⁾

(1) — Las Naciones Unidas adoptaron los objetivos de desarrollo sostenible como llamado a la acción para garantizar la paz mundial y la prosperidad para 2030.
(2) — Tasa total de incidentes registrables. (3) — Según el panorama de amenazas de Kaspersky para las estadísticas de los sistemas de automatización industrial de la segunda mitad de 2023.

Digitalización en el sector de petróleo y gas

Aplicación de tendencias de transformación digital

IloT y nube

- 1 Adquisición y procesamiento de datos sísmicos
- 2 Optimización de perforaciones
- 3 Detección de fugas en oleoductos
- 4 Supervisión de refinerías
- 5 Optimización de las rutas y supervisión de almacenamiento

Robotización y 5G

- 1 Drones y robots submarinos y aéreos no tripulados para la inspección y realización de perforaciones
- 2 Supervisión de la condición de los oleoductos en lugares difíciles de llegar, y adquisición de datos
- 3 Inspección de plantas y capacidad para cierres rápidos en caso de un problema

Hiperautomatización, IA, aprendizaje automático y automatización robótica de procesos

- 1 Búsqueda y definición de sitios de perforación
- 2 Predicciones de fallos en la bomba
- 3 Análisis de datos de oleoductos y transporte
- 4 Predicción de fallos en refinerías
- 5 Pronósticos de demanda de clientes

Metaverso industrial: realidad aumentada, realidad virtual

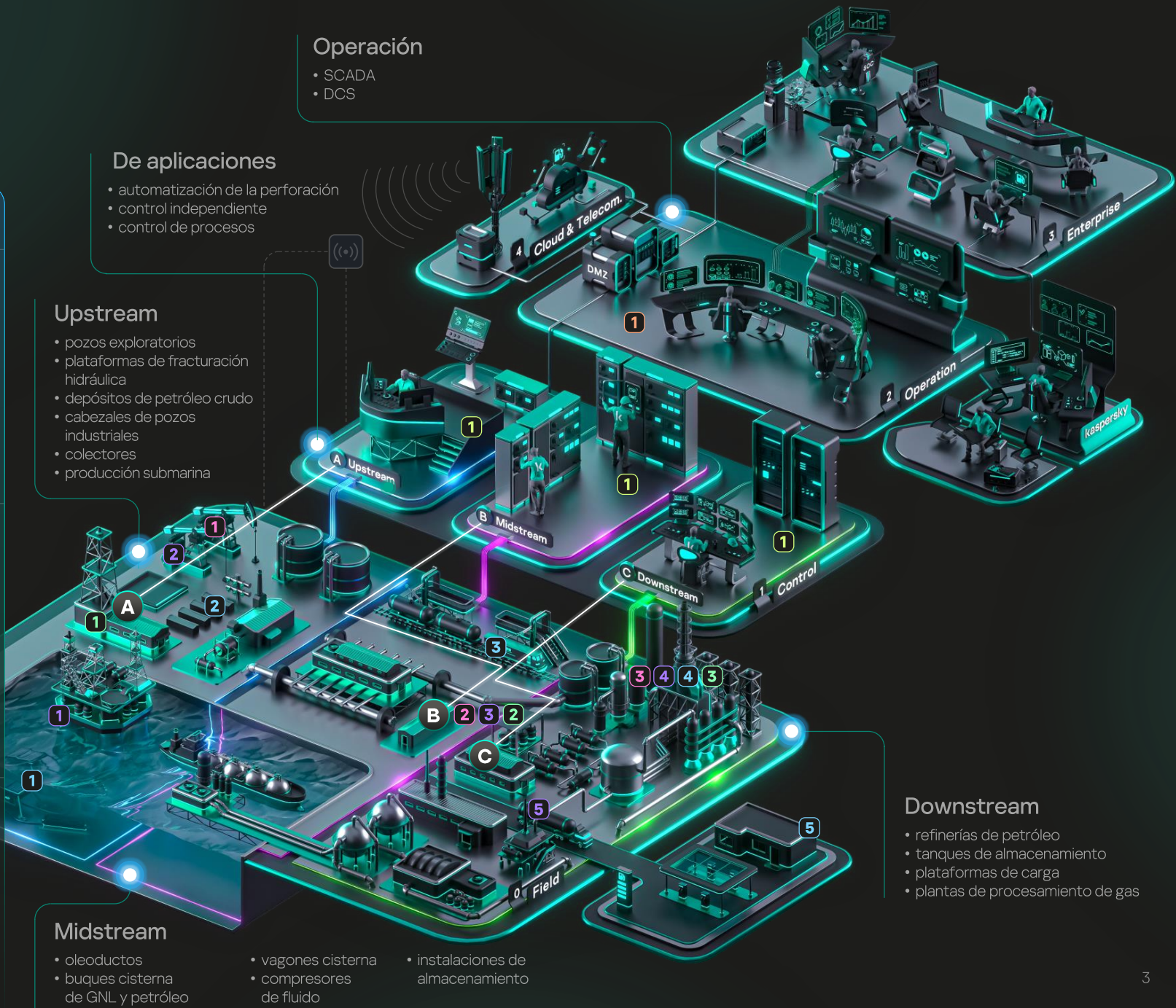
- 1 Capacitación del personal, colaboración, mantenimiento en entornos virtuales

Gemelos digitales

- 1 Modelado de escenarios de perforación
- 2 Réplicas del sistema de oleoductos para su supervisión
- 3 Modelado de procesos de refinerías petroleras para detectar obstáculos

Convergencia de TI/TO

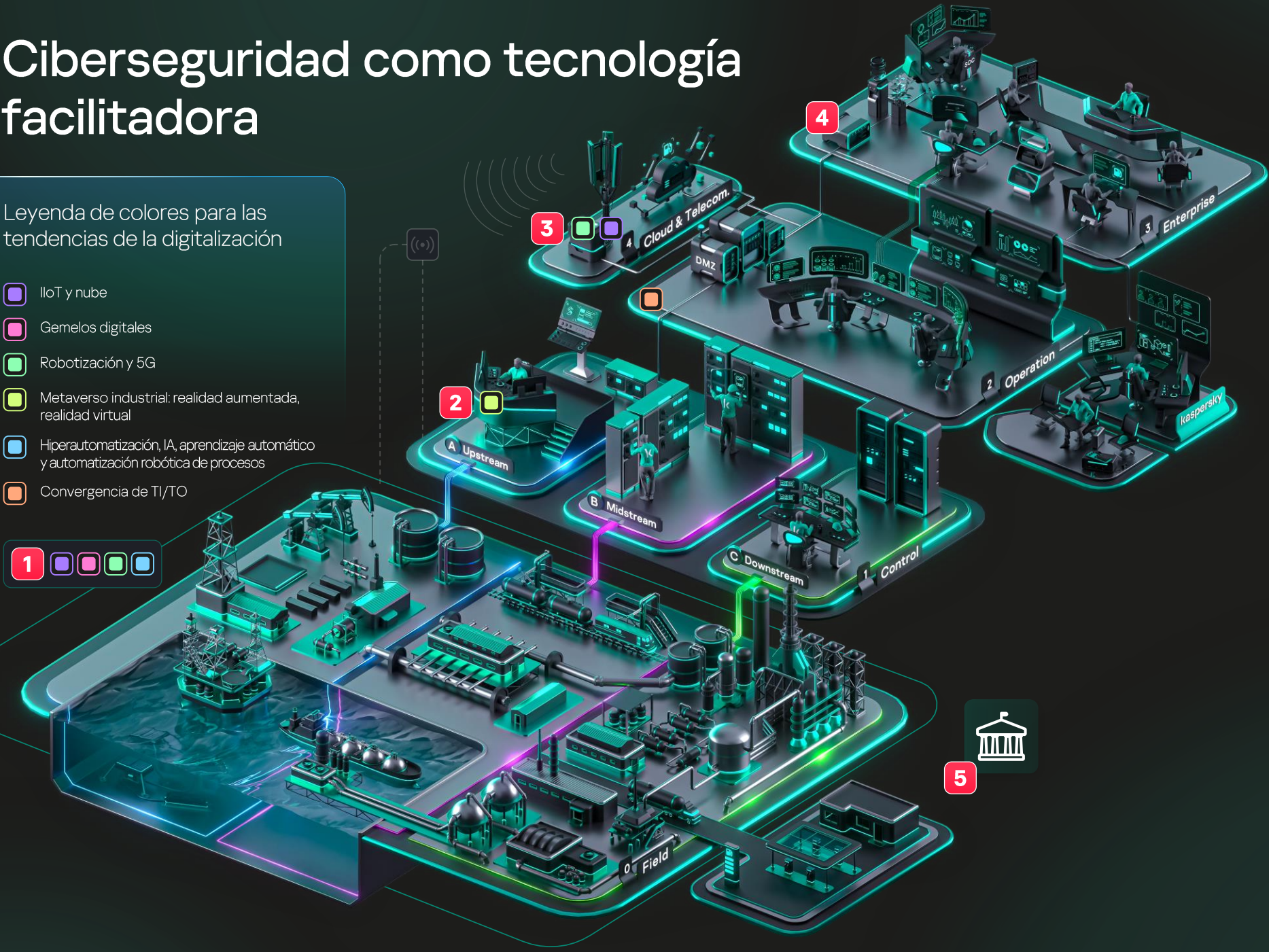
- 1 Análisis de datos en tiempo real de sensores y equipos



Ciberseguridad como tecnología facilitadora

Legenda de colores para las tendencias de la digitalización

- IoT y nube
- Gemelos digitales
- Robotización y 5G
- Metaverso industrial: realidad aumentada, realidad virtual
- Hiperautomatización, IA, aprendizaje automático y automatización robótica de procesos
- Convergencia de TI/TO



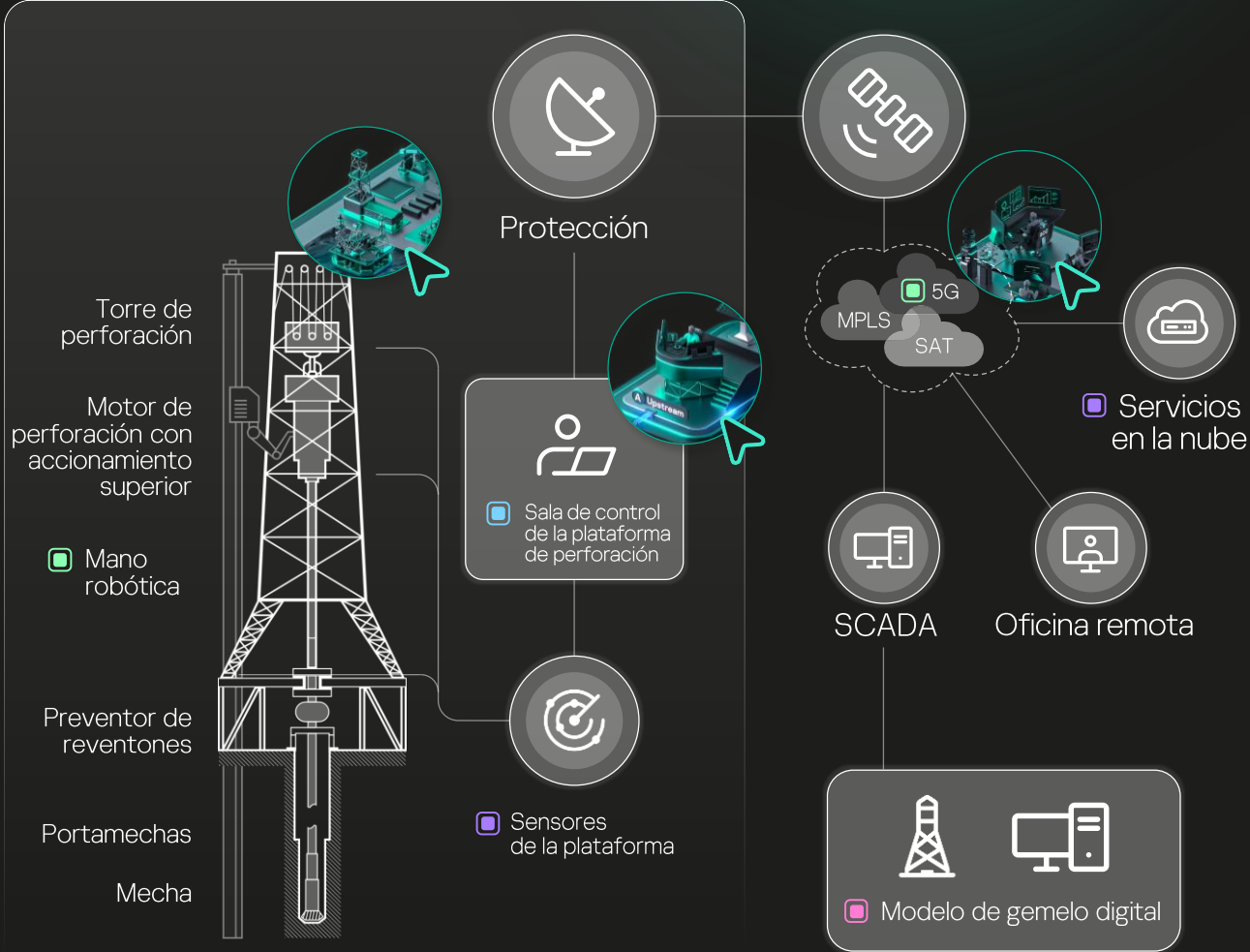
Al mismo tiempo, la transformación digital en el sector de petróleo y gas conlleva problemas y desafíos relativos a la seguridad.

- 1 Expansión de la superficie de ataque
- 2 Infraestructura heredada y convergencia de TI/TO fuera de control
- 3 Acceso externo a la infraestructura de TO
- 4 Escasez de personal
- 5 Reglamentos de protección de infraestructuras vitales

Haga clic en el elemento para continuar

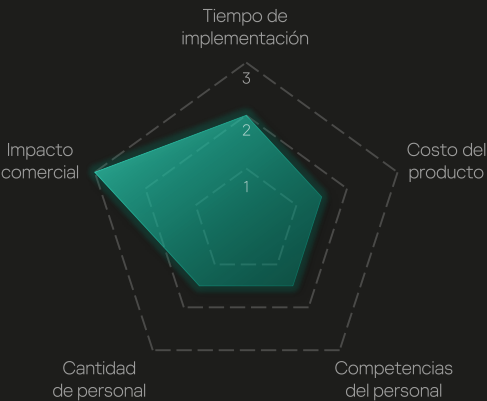
1. Expansión de la superficie de ataque

Ejemplo de un proceso upstream



Los sistemas de control industrial (SCI) ejecutan y supervisan sitios, oleoductos y refinerías, lo que crea un entorno complejo de procesos. Este sistema está tan interconectado que se vuelve vulnerable a los ciberataques, ya que la conexión a un equipo o terminal concede acceso a una superficie más amplia de infraestructura

Características de la solución



¿Cómo Kaspersky puede ayudar?

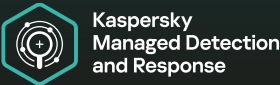


- Cobertura de infraestructura de TO/IIoT integral
- Visibilidad de sistemas y redes
- Auditorías de seguridad exhaustivas periódicas

Ecosistema de servicios de respaldo



- Identificación de fallas de seguridad en infraestructuras de sistemas de control industrial (SCI)
- Verificación de componentes críticos



- Detección de amenazas proactiva
- Respuesta automatizada y guiada
- Experiencia en ciberseguridad de SCI

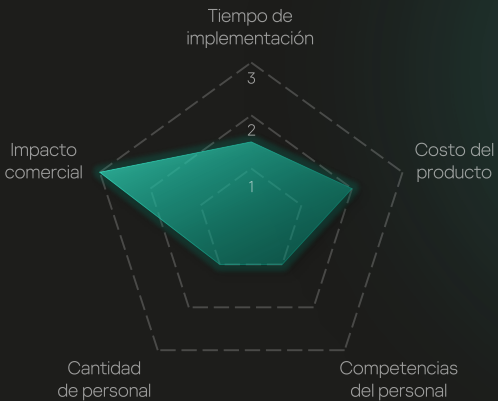
2. Infraestructura heredada y convergencia de TI/TO fuera de control



La integración de TI y TO se convirtió en un elemento clave de la arquitectura de los procesos de petróleo y gas, pero su implementación puede enfrentarse a riesgos de seguridad

- Infraestructura heredada no protegida con tecnología obsoleta
- Disparidad de prioridades entre la ciberseguridad de los sistemas, lo que puede dar lugar a mecanismos de protección contradictorios
- La TI se enfoca en la confidencialidad y la integridad de los datos
- La TO se enfoca en las operaciones y la disponibilidad en tiempo real

Características de la solución



¿Cómo Kaspersky puede ayudar?



- Detección de amenazas y anomalías, medidas de respuesta seguras para hosts y redes
- Administración centralizada de riesgos, políticas de seguridad y activos en todos los niveles de los IACS



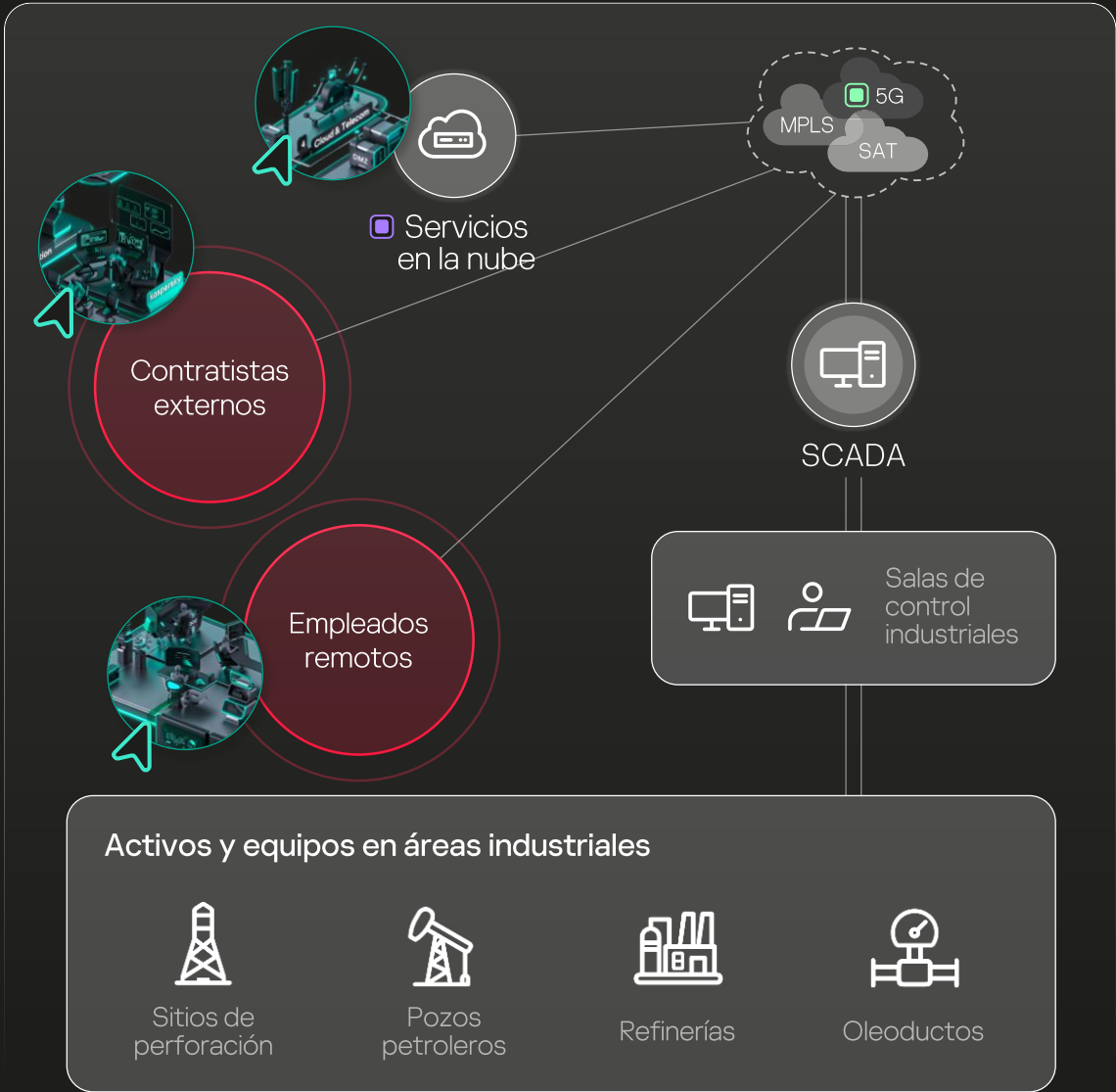
- Protección sólida de endpoints frente a ransomware, malware, ataques sin archivos y APT
- Visibilidad integral y defensas superiores en todos los endpoints de la organización

Ecosistema de servicios de respaldo



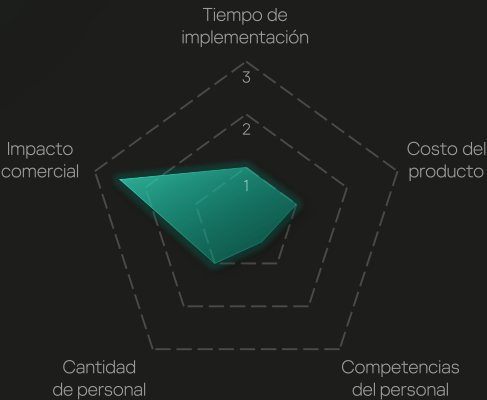
- Detección de amenazas
- Investigaciones y búsquedas de amenazas activas
- Información exhaustiva de amenazas y vulnerabilidades

3. Acceso externo a la infraestructura de TO



Conceder acceso remoto a los oleoductos, las refinerías y otros sistemas de petróleo y gas permite supervisar, gestionar y analizar datos de los procesos industriales para los empleados y proveedores que trabajan de forma remota, gracias a la convergencia de TI y TO. Esta optimización requiere proteger la conexión externa, ya que los usuarios con acceso ampliado a la infraestructura TO podrían exponerla a mayores riesgos de ciberataques

Características de la solución



¿Cómo Kaspersky puede ayudar?



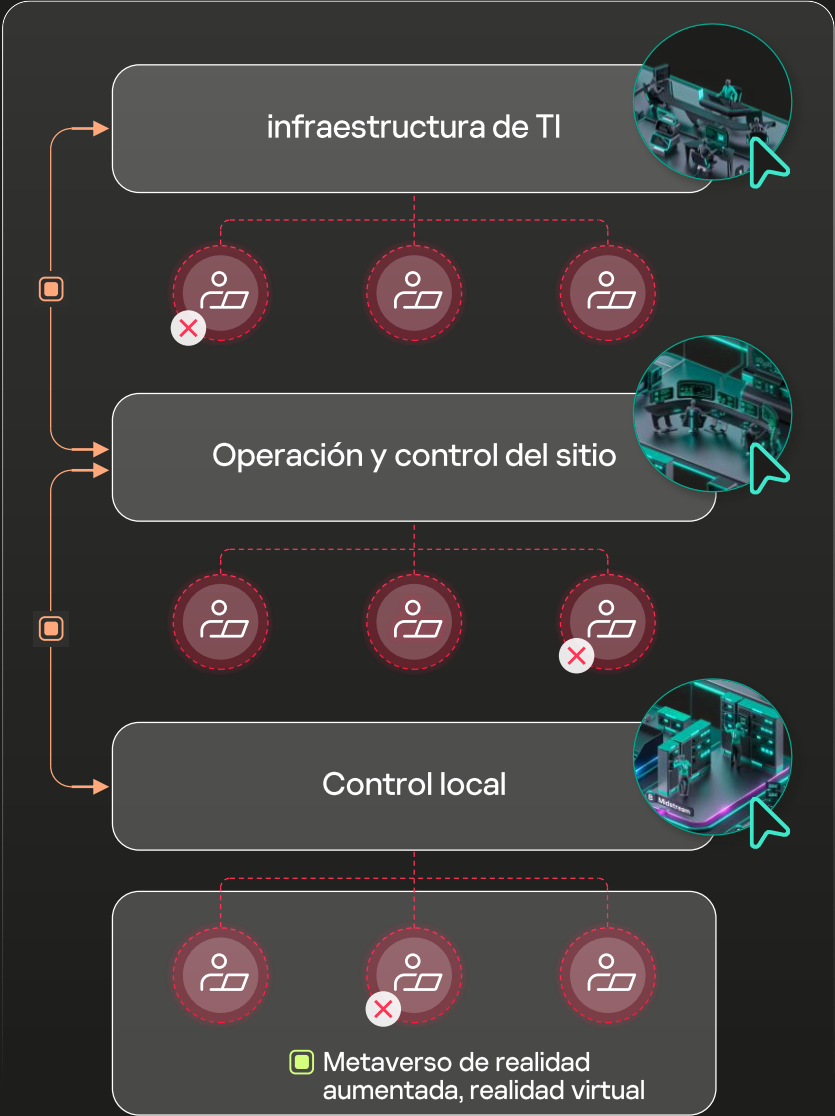
Implementación rápida de la red distribuida

- Escalabilidad sencilla
- Administración conveniente
- Seguridad centralizada



- Clientes ligeros con inmunidad cibernética para el acceso remoto seguro
- Herramienta de administración centralizada para simplificar la administración de la infraestructura de cliente ligero

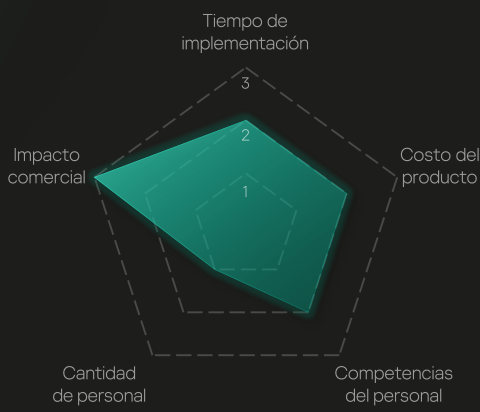
4. Escasez de personal



Durante más de una década, el sector de petróleo y gas se enfrentó al desafío de reclutar y retener profesionales capacitados. Este problema se está agravando con la transformación digital y la alta demanda de trabajadores con experiencia híbrida digital y técnica.

43 %
de los trabajadores encuestados mundialmente en 2020 querían abandonar el sector de energía en los siguientes cinco años¹
(1) — Pronóstico para la primavera de 2022

Características de la solución



¿Cómo Kaspersky puede ayudar?

Kaspersky Industrial CyberSecurity

- Menor carga de trabajo para el personal responsable de la ciberseguridad
- Respuesta más rápida a amenazas

Kaspersky Extended Detection and Response

- Plataforma de administración única abierta
- Ciberseguridad unificada en todos los segmentos industriales y corporativos

Ecosistema de servicios de respaldo

Kaspersky Security Awareness

- Materiales de capacitación
- Capitación basada en juegos a través de simulaciones comerciales
- Módulos de aprendizaje interactivos y ataques de phishing simulados

ICS CERT Kaspersky ICS CERT

Habilidades prácticas de expertos

- Análisis forense digital y respuesta a incidentes
- Exploración de vulnerabilidades
- Programas de capacitación interdisciplinarios

Haga clic en el producto para obtener más información

8

5. Regulaciones del CIP

Las regulaciones de ciberseguridad para el sector de energía, y en especial de petróleo y gas, aborda las amenazas y vulnerabilidades emergentes, y define el parámetro del sector para la protección de sistemas de TO. Los países de todo el mundo implementan estándares y directivas particulares, que suelen incluir lo siguiente:

- Evaluación y administración de riesgos
- Políticas y procedimientos
- Seguridad de sistemas
- Respuesta ante incidentes y generación de informes
- Capacitación del personal



- ISA/IEC 62433
- ISO/IEC 27001
- ISA99



- Directiva NIS2
- Pautas de Ciberseguridad para TO e ICS de la ENISA
- Estrategia de Ciberseguridad de la UE
- Ley de Ciberseguridad de la UE
- Ley de Ciberresiliencia de la UE



- Marco de Ciberseguridad del NIST
- NIST SP 800-82
- Directiva de la Seguridad de las Tuberías de la TSA
- Norma API 1164
- Modelo de Madurez de Capacidad de Ciberseguridad del DOE



- Estrategia Nacional de Ciberseguridad
- Marco de Evaluación Cibernética del NCSC



- Ley de Seguridad de TI 2.0 BSI KritisV
- Compendio de Seguridad de los ICS de la BSI
- DVGW
- VDMA 66418



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



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



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



- Ley de Ciberseguridad de Suecia
- Ley de Protección de Seguridad de Suecia
- Guía de la MSB



- Estrategia Nacional de Ciberseguridad
- Ley de Ciberseguridad n.º 362/2018
- Reglamentos de la Agencia Nacional Reguladora de la Energía



- Plan de Acción y Estrategia Nacional de Ciberseguridad
- BTK CIPR
- Reglamento de Ciberseguridad de la EPDK



- Estrategia Nacional de Ciberseguridad
- Marco normativo de la PNSI
- Reglamento de la ANP



- Pautas del NCIIPC
- Ley de Tecnologías de la Información (TI) de 2000



- GB/T 44462.1-2024
- GB/T 22239-2019
- GB/T 32919-2016
- GB/T 25070-2019



- Estrategia Nacional de Ciberseguridad de la BSSN
- Norma n.º 4/2021 de la BSSN
- Norma presidencial n.º 82/2022



- Reglamento de Garantía de la Información
- Marco normativo del Consejo de Ciberseguridad
- Estándar de seguridad IoT
- Política CIIP de los EAU



- NCA OTCC-1:2022
- NCA ECC-2:2024
- NCA CGLIoT-1:2024

Comuníquese con nosotros para obtener más información acerca de los estándares y las regulaciones regionales

¿Cómo Kaspersky puede ayudar?

Kaspersky proporciona servicios y soluciones basados en una "defensa profunda", como lo recomiendan los proveedores de soluciones de seguridad industrial, así como los organismos reguladores de diferentes países



Kaspersky Industrial CyberSecurity

Los productos están diseñados para que las empresas de petróleo y gas cumplan con **IEC 62443, NIS2, NERC CIP, SOC 2 Tipo 2, ISO/IEC 27001**



Compatibilidad probada con:



Más de 130



sistemas de más de 50 proveedores

Kaspersky Security Awareness y capacitaciones para expertos

Solución diseñada para capacitar a los empleados con capacidades esenciales de ciberseguridad y **promover la conformidad con los requisitos de la Directiva NIS 2**

Obtenga más información acerca de la Directiva NIS 2 y la conformidad de nuestros productos

Ciberresistencia con el ecosistema de TO de Kaspersky



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



Experiencia de Kaspersky en el sector de petróleo y gas

Más de 10

años

de experiencia en el sector
de petróleo y gas

138 proyectos

completados

12 %

Protegemos las
empresas de petróleo
y gas con el 12 %
de la producción
mundial total

60 empresas

ya están bajo protección

El ecosistema de Kaspersky OT CyberSecurity proporciona una protección integral de la infraestructura industrial para las empresas de petróleo y gas. La plataforma tiene la capacidad de detectar ataques complejos y responder a ellos de forma central en toda la red industrial.

Casos de estudio de clientes típicos

- Ayudar a integrar sectores corporativos e industriales en una infraestructura unificada segura con seguridad integral
- Centralizar todas las funciones de seguridad de la información en redes distribuidas geográficamente para mejorar la visibilidad de las actividades de la infraestructura y brindar un uso más efectivo de los recursos humanos
- Asistir en la protección de los sistemas integrados en sistemas operativos desactualizados y no admitidos que tienen equipos de sistema de seguridad obsoletos
- Garantizar el funcionamiento estable del sistema de seguridad de la información con requisitos de alta disponibilidad y limitaciones de consumo de recursos

¿Por qué las empresas del sector petróleo y gas eligen a Kaspersky?

- Experiencia profunda en ciberamenazas con supervisión continua del panorama de amenazas
- Sistemas de seguridad de la información diseñados tomando en consideración las tendencias digitales más recientes
- Ayuda para cumplir con los requisitos normativos
- No afecta el flujo de trabajo industrial y el funcionamiento del dispositivo
- Ofertas de productos que normalmente participan en pruebas llevadas a cabo por institutos de investigación internacionales y obtienen los primeros puestos
- Soluciones que se sometieron a pruebas de compatibilidad con productos de los principales proveedores



>80 %

de todos los requisitos
de seguridad
IEC 62443-3
cubiertos por
Kaspersky



242

sistemas de
57 proveedores
de ICS
certificados

Casos de estudio exitosos del sector de petróleo y gas

En los últimos 10 años de experiencia, Kaspersky:



Protegió propiedades integradas grandes con **80 campos** ubicadas a miles de kilómetros entre sí



Garantizó la seguridad de una terminal única en la región con una capacidad de **205.000 toneladas** de productos petroquímicos y proporcionó control de transporte del tren al mar



Implementó un sistema de ciberseguridad en una importante empresa de transporte de gas, que forma parte de una infraestructura crítica y suministra gas a más de **20 millones** de personas



Las 5 empresas de petróleo y gas más grandes de Rusia

- Protección del APCS con la solución Kaspersky Industrial CyberSecurity
- Completó la capacitación especial "Concientización en ciberseguridad industrial" basada en la experiencia real de investigación de ciberincidentes industriales

12 años trabajando con Kaspersky

[Más información](#)



RN-BashNIPneft: principal centro de I+D en exploración y producción

El sistema de seguridad de la información centralizado está integrado en todo el ecosistema de productos Kaspersky, lo que permite garantizar una protección sólida frente a ciberamenazas y optimizar la carga de trabajo del personal de ciberseguridad.

[Más información](#)



Una de las refinerías de petróleo más grandes del mundo

Elegir XDR de Kaspersky Industrial CyberSecurity (KICS) proporcionó los siguientes resultados:

- Seguridad más sólida de la información de la refinería
- Mayor ciberseguridad y análisis y supervisión de los procesos de producción
- Detección rápida de amenazas potenciales y respuesta veloz frente a ellas

[Más información](#)

SIA VARS

La única terminal petroquímica de la región báltica

Utilizar la solución Kaspersky Industrial CyberSecurity para garantizar la protección confiable de sistemas de control de líneas automáticas para el transbordo y almacenamiento de productos químicos

[Más información](#)

www.kaspersky.es

© 2024 AO Kaspersky Lab.
Las marcas registradas y las marcas de servicio pertenecen a sus respectivos propietarios.

Administre su seguridad con Kaspersky y conviértase en socio

Comuníquese con nosotros y participe de nuestra conferencia mundial para clientes

Más información



#kaspersky
#bringonthefuture