Ciberseguridad orientada al futuro

Protección de alta resistencia para su empresa

kaspersky

#bringonthefuture

El corazón palpitante de la empresa

Las empresas de la industria pesada están presentes, de un modo u otro, en la mayoría de las actividades humanas, desde en la forma en que vivimos, trabajamos e interactuamos hasta en nuestros medios de producción y transporte. A menudo se las subestima, pero son el núcleo de las infraestructuras nacionales y los principales impulsores de la economía mundial.

En casi todos los sectores de la industria pesada se realizan enormes inversiones en grandes plantas, maquinaria avanzada y la última tecnología. Este es probablemente el principal argumento de aquellos que las critican de un modo u otro. Sin embargo, no se trata, en ningún caso, de un fenómeno nuevo.

¿Qué abarca exactamente el término "industria pesada"? Hay cierto debate sobre la amplitud de su definición, pero, en general, y para el propósito de este documento, la industria pesada incluye los siguientes sectores:

- **Energía: especialmente el petróleo y el gas, pero también el carbón, la electricidad, la energía nuclear y las energías renovables.**
- **Minería: desde metales preciosos hasta acero, cobre y otros metales y minerales.**
- **Construcción naval, automóviles, aeronáutica y otros medios de transporte.**
- **Extracción química, fabricación y desarrollo.**
- **Cualquier actividad industrial que implique máquinas, equipos o infraestructura pesados.**

Luditas

El término "ludita" se utiliza generalmente para describir a las personas que son contrarias a las nuevas tecnologías o que, simplemente, no están familiarizadas con ellas. Pero, antiguamente, el término tenía una definición mucho más precisa.

La Revolución Industrial comenzó a mediados del siglo XVIII, cuando las sociedades predominantemente rurales y agrarias se convirtieron en industriales y urbanas, y la producción pasó de ser manual a realizarse con máquinas.

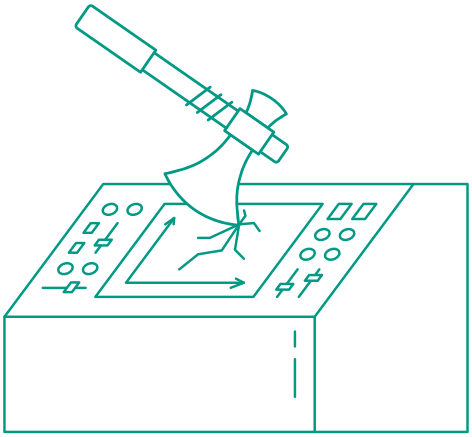
La revolución la impulsó principalmente el sector textil, que, a principios del siglo XIX, era la principal industria pesada de la época.

Los luditas eran una organización secreta de trabajadores de la industria textil en Inglaterra. Les preocupaba ser relegados de sus puestos por la tecnología y decidieron tomar las riendas de la situación destruyendo la maquinaria textil.

La rebelión comenzó en Nottingham en 1811 y se extendió por otras áreas industriales hasta su fin en 1816. Los propietarios de talleres y fábricas recurrían a las armas contra los protestantes para frenar el vandalismo. Finalmente, fueron los tribunales, la nueva legislación y los medios militares los que pusieron fin a la rebelión.

Uno de los pocos personajes relevantes que apoyaron a los luditas fue el poeta romántico Lord Byron. Irónicamente, fue su hija Ada Lovelace quien combinó la tecnología del motor analítico con el telar de Jacquard para producir tejidos complejos con mayor facilidad, convirtiéndose así en la primera programadora informática de la

historia. Así que, en su caso, no se cumple el dicho "de tal palo, tal astilla".



De los luditas a los cibercriminales

Los primeros luditas se movían por la amenaza, o más bien la realidad, de perder sus trabajos y utilizaban los medios más primitivos para destruir la tecnología de la época.

En la actualidad, por el contrario, los cibercriminales hacen uso de la tecnología más reciente y, por lo general, son expertos a la hora de utilizarla. En los casos en los que los luditas utilizaban la fuerza de sus cuerpos, un cibercriminal moderno solo necesita mover un dedo para causar estragos.

Pero, ¿qué motiva a alguien en la actualidad a atacar o destruir la industria pesada?

El ejército estadounidense y el FBI utilizan para clasificar a los cibercriminales el acrónimo MICE, que representa las iniciales de los términos en inglés "Money" (dinero), "Ideology" (ideología), "Compromise" (poner en peligro) y "Ego" (ego).

Más tarde, Max Kilger dio un giro al acrónimo original y acuñó el acrónimo MEECES, que se corresponde con los siguientes términos:

- **Money (dinero)**: beneficios económicos, simple y llanamente.
- **Ego (ego)**: afán por producir algo elegante, innovador o notable de algún otro modo.
- **Entertainment (entretenimiento)**: diversión a costa de otro.
- **Cause (causa)**: persecución de un objetivo político, religioso, social o fundamental.
- **Entrance (entrada)**: acceso a un grupo social o de cualquier otro tipo u obtención de su reconocimiento.
- **Status (estado)**: logro de reconocimiento como uno de los mejores, si no el mejor, en su campo.

Las personas y los grupos que tengan la industria pesada como objetivo de su ataque tienen una o más de estas motivaciones. Sin embargo, algunas son más prevalentes que otras y pueden constituir amenazas particulares para las organizaciones de este sector.

Partiendo de la anterior lista de motivaciones, el profesional de la ciberseguridad **Mark C. Stafford** identificó ocho "actores de amenazas": usuarios legítimos, hackers, grupos criminales organizados, periodistas, grupos de presión, inteligencia extranjera y terroristas.

Por "usuarios legítimos" Stafford se refiere a aquellos que buscan atacar a los sistemas en respuesta a una pérdida real o percibida, igual que los luditas de antaño, o por coerción. Sin embargo, como veremos, los usuarios también pueden plantear una ciberamenaza a través de otros medios, a menudo de forma involuntaria, ya sea a través de la tecnología personal o de la empresa, o de algún otro modo.

En esta documentación técnica, analizaremos seis tendencias clave asociadas al actual sector de la industria pesada y destacaremos algunos de los riesgos que representan:

Un gran objetivo cada vez mayor

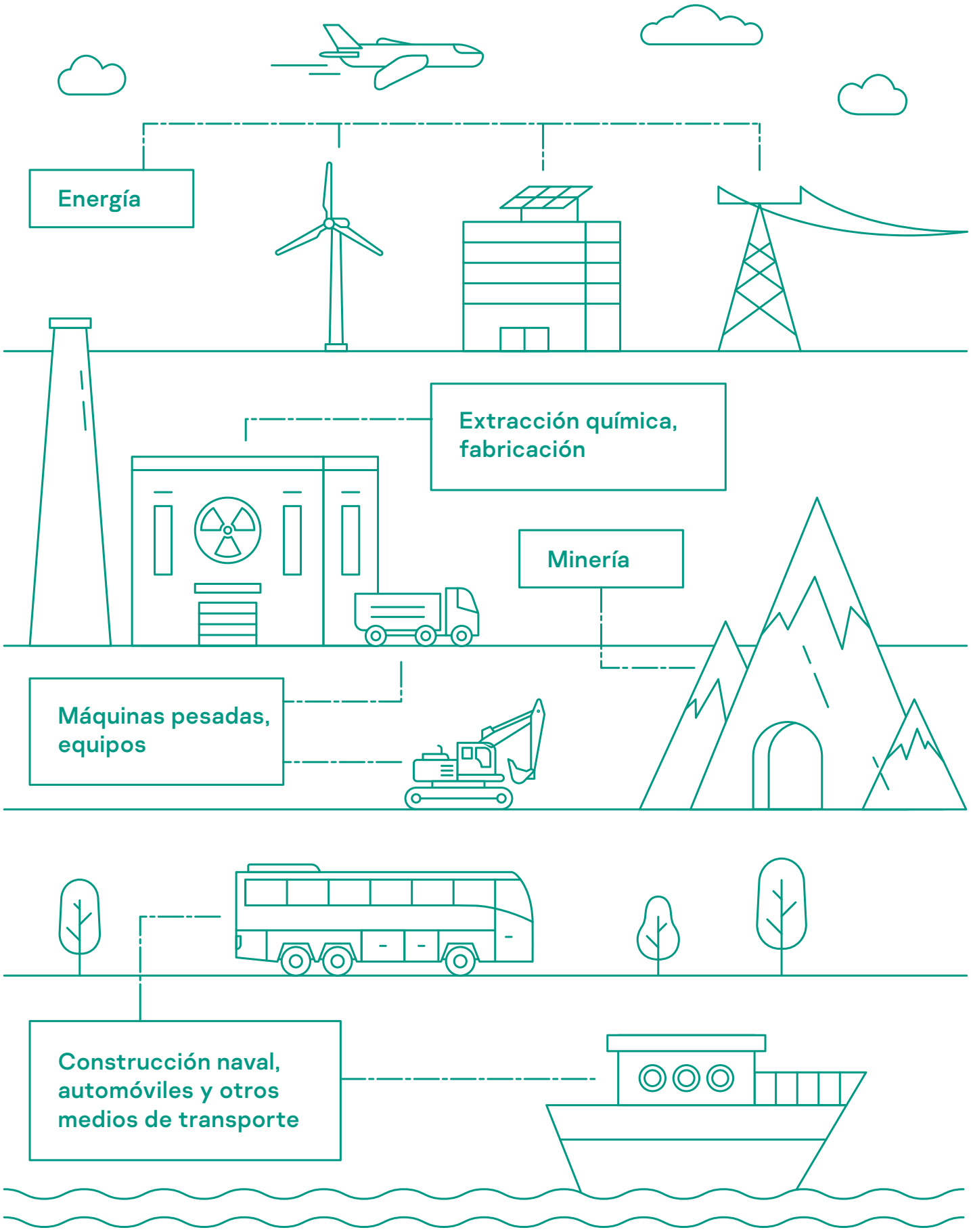
El auge de la digitalización

Aumento del acceso externo a TI y OT

Sector industrial 4.0

El Internet industrial de las cosas

¿Dónde está el talento?


Energía
Extracción química, fabricación
Minería
Máquinas pesadas, equipos
Construcción naval, automóviles y otros medios de transporte

Tendencia núm. 1: Un gran objetivo cada vez mayor

Si observamos las motivaciones detalladas anteriormente, el interés por la industria pesada actual como objetivo es evidente.

También está claro que las empresas de la industria pesada están potencialmente amenazadas por todos los actores de amenazas que aparecen en la lista, de un modo que no suele afectar a las empresas de otros sectores.

Por un lado, influye su tamaño. Su escala de operaciones, su dispersión geográfica y la infraestructura crítica que representan hacen que las organizaciones de la industria pesada resulten atractivas para cualquiera que desee dejar una huella importante o lograr un enorme impacto.

En los últimos años ha habido varios ejemplos de perfil alto de países que han sucumbido a los ciberataques.

Sin embargo, el problema no se limita a los países tradicionalmente grandes y poderosos. La ciberguerra tiene el potencial de desequilibrar el poder en las relaciones internacionales y naciones pequeñas pueden ser capaces de utilizar ciberequipos para enfrentarse a otras más grandes.

Es difícil determinar si el mayor tamaño y número de recursos de países de mayor tamaño será decisivo en este frente de batalla. Lo que es cierto es que la ciberguerra se ha convertido en una realidad internacional. Y al formar parte de la infraestructura nacional, o al operar dentro de ella, la industria pesada se encuentra en primera línea de fuego.

El foco en las amenazas: pequeños errores pueden tener graves consecuencias

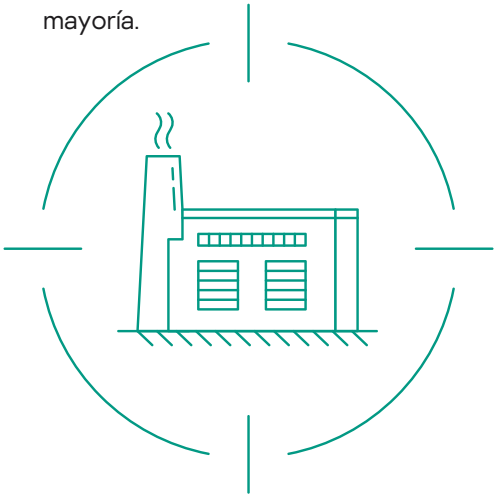
Hay todo tipo de fuentes de ciberamenazas que afectan a la industria pesada, desde estados-nación a actores mucho más pequeños. A continuación, analizaremos algunas de las más serias y comunes. Un buen punto de partida podría ser observar uno de los factores potencialmente más débiles pero más costosos de la cadena: los empleados individuales.

Los errores simples, la ignorancia y la falta de cuidado pueden tener importantes repercusiones. Por ejemplo, un informe de **CyberX** de 2018 sobre los sistemas de control industrial globales puso de manifiesto que el 69 % tenía contraseñas que atravesaban las redes

de OT en texto sin formato, lo que supone un enorme riesgo de seguridad.

De hecho, todas las empresas deben prestar mucha más atención a los datos confidenciales y personales, especialmente a raíz del aumento en los últimos años del nivel de los requisitos de notificación del robo de datos y de los informes por medios online.

Ahora, los hackers pueden dirigirse no solo a empleados individuales, sino también a grupos de trabajadores, con diversos métodos y de forma regular. Una encuesta **realizada por EY en 2019** a 40 participantes del sector del petróleo y el gas reveló que el 43 % de los incidentes de ciberseguridad significativos se debió a la falta de concienciación de los usuarios finales, que sufrieron el ataque mediante phishing. Esto resulta particularmente preocupante, dado que este sector es más vulnerable al terrorismo que la mayoría.



Por lo que respecta al sector de la minería (pero aplicable igualmente a muchos otros operadores de la industria pesada), otro **informe de EY** concluyó que:
"Para el sector de la minería y los metales, esto a menudo se traduce en información personal de los departamentos de recursos humanos, higiene médica, HSE y sistemas de gestión de contratistas, así como información comercial confidencial en dispositivos de usuario final sénior y repositorios de datos basados en la nube".

Tendencia núm. 2: El auge de la digitalización

Ya son un objetivo importante, pero los cambios en la forma en que las empresas de la industria pesada operan las hacen aún más vulnerables.

Muchas organizaciones utilizan tecnología digital para generar valor. Como Duane Dickson señaló en un informe sobre el panorama **del petróleo, el gas y los productos químicos para Deloitte**:

"Cada vez son más las empresas que se esfuerzan por implementar inteligencia artificial, análisis, robótica y cadenas de bloques para aumentar la eficacia, productividad, fiabilidad y capacidad de predicción de las operaciones".

En el sector de la energía, la tecnología digital está presente en todo, desde plataformas sin personal hasta la tecnología de yacimientos petrolíferos, así como en el auge de la tecnología de drones. El riesgo es aún mayor por el aumento del número de dispositivos conectados en los entornos operativos. Por poner solo un ejemplo, las instalaciones terrestres y marinas del sector del petróleo y el gas utilizan dispositivos móviles y remotos para colaborar: un punto débil en potencia.

Sobre todo, existe el problema de la tecnología operativa (OT), que desempeña un papel fundamental en la mayoría de las operaciones del sector, pero que se suele utilizar y proteger completamente por separado de los sistemas de TI, lo que supone un riesgo de ciberseguridad en sí mismo.

Sin embargo, a pesar de todo esto, **según LNS Research**, el 38 % de las empresas de la industria pesada ni siquiera supervisa sus redes en busca de comportamientos sospechosos.

El foco en las amenazas: ataques a la tecnología operativa (OT)

Los riesgos del aumento de la digitalización afectan a todas las empresas de la industria pesada. Un buen ejemplo puede ser el sector minero, pues muchos, si no la mayoría, de los problemas que lo afectan se dan en otros sectores.

En un artículo de **EY de 2019, el experto en el sector global de la minería** y los metales Paul Mitchell informó de que las nuevas ciberamenazas a la OT son una gran preocupación para los directivos y ejecutivos de los sectores que utilizan muchos activos, así como para quienes los regulan. Su primera y principal preocupación radica en los sistemas de OT de misión crítica en las plantas de procesamiento y los centros operativos. Le siguen las principales redes y sistemas de TI y OT que permiten operaciones integradas, supervisión y control remotos, y planificación y apoyo a la toma de decisiones sensibles a la producción.

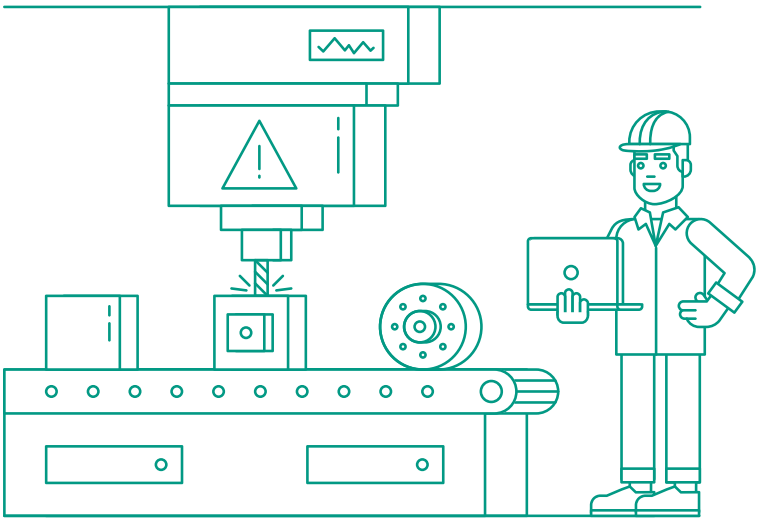
Los equipos e infraestructuras de minería que hasta la fecha no estaban conectados, como perforadoras, camiones y trenes, ahora están integrados. El control y la eficiencia pueden ser mayores, pero también los riesgos. Cada proceso y cada tecnología representan un tipo diferente de peligro que debe contrarrestarse.Otras industrias pesadas tendrán sus propias formas de trabajar, pero algunos procesos, como la gestión de existencias y el envío, son comunes a muchas. Con frecuencia, los entornos operativos de la industria pesada son intrínsecamente peligrosos, por

lo que también puede haber un riesgo importante para la seguridad. Y los problemas de una productividad reducida, las pérdidas económicas y los daños a la reputación son comunes a todos.

Como Inmarsat **señaló en 2018** al comentar su informe The Future of IoT in Enterprise:

"Mientras que hace una década una intrusión o robo de datos habría sido una molestia, hoy en día, una explotación minera podría detenerse por completo, por lo que es preocupante que tantas empresas mineras tengan dificultades en esta área".

No es de extrañar, por tanto, que el mismo informe de EY mencionado anteriormente también destacara que el 97 % de las empresas mineras admite que sus actuales sistemas de ciberseguridad no satisfacen sus necesidades.



Tendencia núm. 3: Aumento del acceso externo a TI y OT

El aumento de la digitalización ha ampliado el acceso a lo que antes eran dispositivos aislados. Usuarios del sistema de TI, terceros con acceso físico o remoto a OT e incluso usuarios de Internet públicos, todos tienen ahora el potencial de causar problemas, ya sea a través de malware (identificado por **Ponemon** como el riesgo más preocu-

pante) o de ransomware, botnets o por cualquier otra vía. Ha pasado mucho tiempo desde que la simple denegación de servicio era la principal amenaza.

La industria pesada tiene más motivos para preocuparse que la mayoría, con más que proteger y menos soluciones adecuadas para protegerse. Incluso algo tan universal y aparentemente sencillo como Microsoft Windows puede ser un problema: muchos entornos de OT siguen utilizando versiones de Windows para las que Microsoft ya no proporciona parches de seguridad.

El entorno de OT está además muy personalizado, dado que sirve de apoyo a operaciones muy específicas. Por este motivo, las empresas tienden a confiar en los fabricantes de equipos originales (OEM) para el mantenimiento y las actualizaciones.

Como señala un informe de **McKinsey** de 2019, la forma en que se protege la OT, incluso cómo funciona, puede ser un misterio para sus usuarios. No pueden ocuparse ellos mismos, por lo que el OEM o un tercero deben acceder a las redes de usuario para el mantenimiento. Según McKinsey, varias empresas del sector de la industria pesada confirma que terceros conectan con frecuencia ordenadores portátiles y dispositivos USB directamente a redes de OT sin comprobaciones previas de ciberseguridad, a pesar de los peligros de una posible infección.

Las revisiones de ciberseguridad no suelen incluirse en los contratos con los OEM. Los estándares de seguridad rara vez se aplican, y los proveedores OEM manifiestan que los compradores operativos rara vez quieren o utilizan funciones de seguridad, ni siquiera si están integradas.

El foco en las amenazas: ataques más graves con un coste menor

La ampliación del acceso externo y la falta de conocimientos internos sobre cómo protegerse son las razones clave por las que los ataques a la industria pesada están creciendo en número y gravedad. Por poner algunos ejemplos recientes de todo el mundo:

— En 2014, un ataque de phishing causó graves daños en el entorno operativo de una fábrica de acero de Europa Occidental. El ataque entró primero en su red de TI y, a continuación, en su red de OT, y los atacantes se hicieron con el control de los equipos de la planta.

— En 2015 y 2016, alrededor de 230 000 personas de Europa del Este perdieron el suministro eléctrico tras los ataques a una red de distribución de energía. El punto débil fue la red de un proveedor externo, que estaba conectada a la red de OT de una empresa energética. Esto permitió a los atacantes realizar cambios en el sistema de control.

— En 2017, los atacantes accedieron al sistema de control industrial de una planta petroquímica de Oriente Medio. En este caso, la intención no era acceder a los datos ni destruirlos, ni siquiera detener la actividad de la planta. El plan era sabotear las operaciones y desencadenar una explosión.

Y la escala del problema parece estar empeorando. En 2019, **Tenable y Ponemon Institute** utilizaron una encuesta anónima para sondear a más de 700 profesionales de la seguridad de EE. UU., el Reino Unido, Alemania, Australia, México y Japón. Todos ellos trabajan para proteger la infraestructura nacional y confían en los sistemas de control industrial y otras formas de OT.

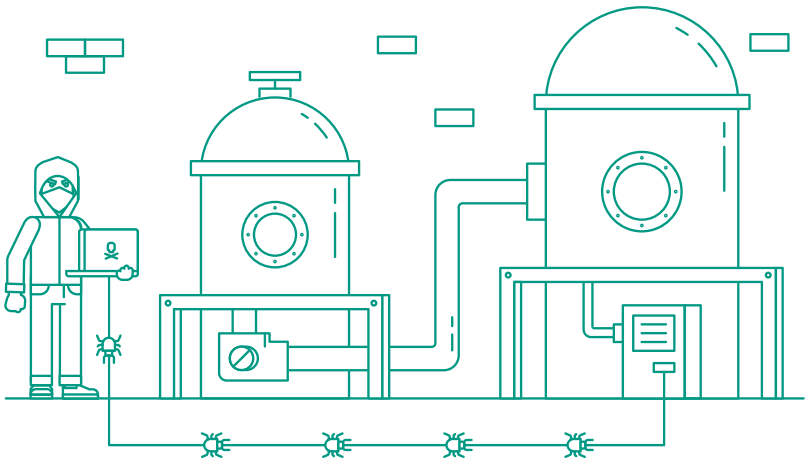
De los que respondieron, 9 de cada 10 afirmaron que la organización para la que trabajaban había sufrido daños causados por un ciberataque en los últimos dos años. Muchos manifestaron incluso haber experimentado varios incidentes.

Los encuestados informaron de que alrededor de la mitad de los ataques exitosos habían causado tiempo de inactividad en sistemas críticos, pues los operadores tuvieron que apagar los sistemas para reparar los daños.

Además, más de una quinta parte de las organizaciones que utilizan OT señalaron el ataque de un estado-nación como una de las amenazas que más les preocupan.

Estas estadísticas se asemejan a los datos arrojados por otras fuentes. Por ejemplo, una encuesta realizada en **2018 por Forrester Consulting** reveló que casi el 60 % de las organizaciones encuestadas había experimentado un incidente de seguridad en sus sistemas de control industrial (ICS) o control de supervisión y adquisición de datos (SCADA).

Sin embargo, sorprendentemente, la mayoría de las empresas del sector gasta menos que las de otros sectores donde el riesgo es menor. En 2018, una encuesta de **Gartner sobre las métricas clave de TI** reveló que el gasto medio en ciberseguridad en todos los sectores es del 6,2 % como proporción del gasto general en TI, con un gasto medio de las compañías energéticas de solo el 4,9 % y un 4,3 % en el sector de la fabricación industrial.



Tendencia núm. 4: Sector industrial 4.0

El sector de la industria pesada ha estado a la vanguardia de la adopción de nuevas tecnologías en su búsqueda de una mayor eficiencia y de la apertura de nuevas fuentes de ingresos y esferas de explotación.

Como **señala IBM**, en la era de la "fabricación cognitiva" de la Industria 4.0:

"Es fundamental que los fabricantes desplieguen el potencial de los datos heredados, en tiempo real y no estructurados para tomar decisiones diarias que equilibren la calidad y el rendimiento. Dado que en un sitio de fabricación medio se ejecutan más de cien aplicaciones de software, es un enorme desafío hacer que los datos sean accesibles y procesables".

Todo ello puede ser cierto, pero también supone unos riesgos de ciberseguridad increíbles, y más teniendo en cuenta el volumen total de aplicaciones de software por sitio.

Incluso para las empresas de la industria pesada menos implicadas en la fabricación, la Industria 4.0 presenta desafíos excepcionales, desde el doble reto de los entornos de TI y OT hasta el número de sitios operativos y la extensión geográfica e internacional que abarcan.

IBM puede estar en lo cierto con respecto a la fabricación cognitiva, pero también es justo decir que las empresas de la industria pesada tienen más cosas en las que pensar que la mayoría en lo que respecta a la ciberseguridad asociada.

El foco en las amenazas: la protección sigue siendo 3.0

Es así de simple: las herramientas y los enfoques de seguridad que utiliza la industria pesada no están a la altura. Por poner un ejemplo, la mayoría de las redes de OT actuales consta de equipos antiguos diseñados originalmente para protegerse de redes no seguras mediante la protección perimetral, como firewalls.

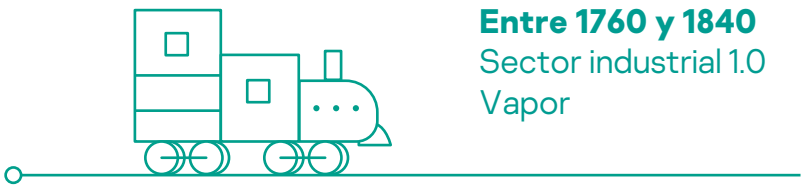
Todo esto ha sido eficaz hasta ahora, pero ¿qué ocurre cuando los ataques se originan dentro de una red, por ejemplo, a través de malware procedente de un dispositivo USB o software de un dispositivo de red?

Como señala el informe de **McKinsey de 2019**, muchas herramientas de seguridad tradicionales no se pueden aplicar a un entorno de OT. De hecho, pueden dañar los dispositivos que controlan los equipos de la planta. Incluso su uso para el análisis puede provocar importantes interrupciones en la planta.

La aplicación de parches de seguridad para corregir vulnerabilidades conocidas presenta más riesgos, ya que pocos sitios tienen sistemas de copia de seguridad representativos en los que probar los parches.

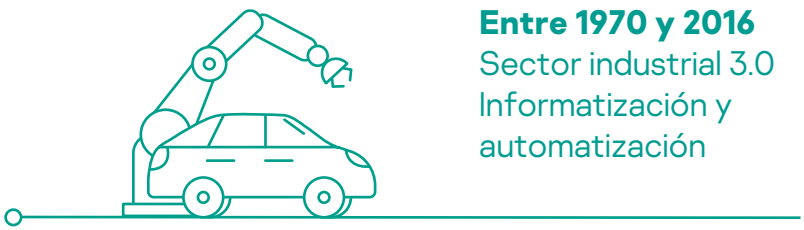
Las nuevas tecnologías, como los servicios en la nube, las redes inalámbricas y los dispositivos industriales móviles, aumentan la complejidad y los riesgos.

No es extraño que los líderes de unidades operativas sean reacios a permitir cambios en sus entornos de OT, ni siquiera con el objetivo de mejorar la ciberseguridad.



Entre 1760 y 1840
Sector industrial 1.0
Vapor

Entre 1870 y 1914
Sector industrial 2.0
La línea de montaje



Entre 1970 y 2016
Sector industrial 3.0
Informatización y automatización

Hoy
Sector industrial 4.0
Sistemas cibernéticos físicos

Tendencia núm. 5: El Internet industrial de las cosas

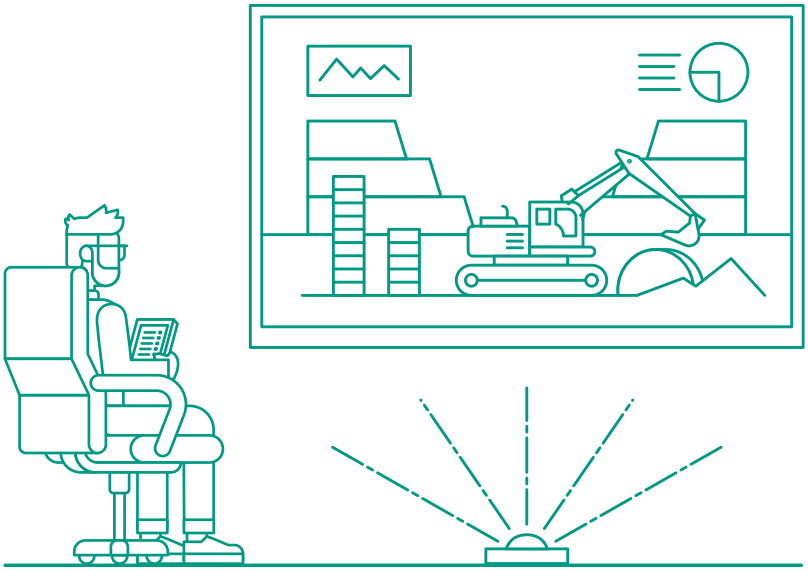
Un componente clave de la Industria 4.0 es el Internet de las cosas (IoT) y su subconjunto asociado, el Internet de las cosas industrial (IIoT).

En 2018, el **Internet of Things Institute** calculó que el IIoT podría sumar 14 billones de dólares a la economía mundial para 2030.

El IIoT, que es ya un fenómeno masivo, se ha dado a conocer a los consumidores a través de aplicaciones como Alexa y los monitores de salud, pero ahora hay muchos otros productos cotidianos con chips que interactúan con el entorno.

Otras aplicaciones, en gran medida desconocidas para el público en general, incluyen cadenas de suministro, logística y transporte. Se utilizan cada vez más en la industria pesada, que también está desarrollando aplicaciones de IIoT propias.

Los medidores, los sensores y las alarmas son especialmente importantes, con aplicaciones que incluyen análisis de datos en tiempo real y supervisión de equipos, inteligencia de ubicación, mantenimiento predictivo, automatización de máquinas y supervisión de personal o de terceros.



El foco en las amenazas: más posibilidad de error y más riesgos cuando se produce

Los retos del Internet de las cosas se han comparado con la construcción de un avión mientras vuela. Cuando se trata del Internet industrial de las cosas, ese avión metafórico es mucho más grande, más complejo y con una carga mucho más valiosa a bordo. Además, sobrevuela zonas densamente pobladas.

Como ocurre de forma generalizada, la mayoría de las empresas de la industria pesada está luchando por adoptar las prácticas y tecnologías necesarias para protegerse en lo que respecta a la ciberseguridad. Las amenazas se siguen analizando y las evaluaciones de riesgos, si las hay, se realizan de forma aleatoria.

Al analizar el problema desde un punto de vista más amplio, un **informe del IBM Institute for Business Value** reveló que el 98 % de las implementaciones de IoT se realiza sin una cuantificación completa de los riesgos. Además, puso de manifiesto que se necesitan, de media, 28 días para detectar un incidente de ciberseguridad, responder a él y recuperarse de sus consecuencias.

Este y muchos otros estudios ponen de relieve la grave amenaza de ciberseguridad que conlleva la adopción de las tecnologías de Industria 4.0 e IIoT. Pero hay también otra forma de verlo.

En 2018, la Agencia de Seguridad de las Redes y de la Información de la Unión Europea publicó un **estudio sobre buenas prácticas para la seguridad del IoT** centrado en la fabricación inteligente. En él se descubrió que, cuando se toma en serio e implementa a fondo, la ciberseguridad también puede actuar como catalizador para la adopción de la tecnología de la Industria 4.0. Razón de más, por tanto, para invertir en ella.

Tendencia núm. 6: ¿Dónde está el talento?

La necesidad de ciberseguridad no deja de crecer, pero el número de profesionales experimentados y cualificados disponibles para proporcionarla no puede seguir el ritmo. En 2017, una encuesta realizada a más de 19 000 profesionales de ciberseguridad llevada a cabo **por el Centro para la Ciberseguridad y Educación** y patrocinada por ISC reveló la cruda realidad. Se prevé que haya un déficit de 1,8 millones de trabajadores de ciberseguridad en todo el mundo en 2022. Solo en Europa, la previsión es de 350 000.

Otra encuesta realizada por **CyberSeek** entre abril de 2017 y marzo de 2018 descubrió que había una vacante por cada 6,5 empleados en Estados Unidos.

Sin embargo, ese número caía hasta 2,5 empleados por cada vacante en el ámbito de la ciberseguridad. Eso supone más de 300 000 vacantes en puestos relacionados con la ciberseguridad durante ese periodo de 12 meses.

Todo ello se traduce en un gran quebradero de cabeza por lo que respecta a la contratación para cualquier organización que desee protegerse.

De hecho, las empresas del sector de la industria pesada no solo carecen de suficientes profesionales de ciberseguridad; muchas no reconocen totalmente la necesidad de determinados puestos clave. Por ejemplo, a menudo, solo se contratan arquitectos de seguridad después de la introducción de un nuevo sistema.

Además, un **informe de LNS Research** de 2017 sobre ciberseguridad industrial reveló que solo el 35 % de más de 1000 organizaciones encuestadas contaba con un director de seguridad de la información dedicado. El resto simplemente consideraba el trabajo como parte de las obligaciones del director de TI.

El foco en las amenazas: por qué la industria pesada se ve más afectada que la mayoría

La escasez global de profesionales de ciberseguridad es un problema particular para las empresas de la industria pesada, ya que necesitan protección tanto para los sistemas de TI como para los sistemas de OT. No solo afecta a los procedimientos y controles actuales, sino también a la implementación de nuevas herramientas y formas de trabajar.

La mayoría de las organizaciones del sector de la industria pesada está dispuesta a aumentar sus equipos de ciberseguridad. Muchas también desean seguir la tendencia de integrar sus sistemas y equipos de TI y OT, pero no pueden contratar a las personas adecuadas.

Afortunadamente, el empleo de la tecnología de ciberseguridad adecuada y la experiencia que lo acompaña pueden marcar una gran diferencia. Por eso, las soluciones de Kaspersky no solo cubren la instalación, el mantenimiento y la gestión de soluciones técnicas avanzadas, sino también la formación del personal actual y futuro, tanto para personal general de TI como para personal especializado. Además, proporcionamos acceso ininterrumpido a nuestra base de conocimientos global, con partners cualificados de Kaspersky preparados para responder a incidentes complejos y graves en cualquier momento.

Cómo proteger su negocio: elija lo que mejor cubra sus necesidades

Las soluciones de Kaspersky garantizan una protección probada contra ciberataques para todo tipo de organizaciones de la industria pesada, incluidas opciones que aumentan de forma significativa los paquetes de ciberseguridad de valor añadido que se ofrecen a los clientes.

Como ya hemos visto, en lo que respecta a la ciberseguridad, la industria pesada no solo es un importante objetivo, sino que supone algunos desafíos únicos. Es difícil imaginar un sector en el que la protección y la continuidad del negocio sean más vitales, no solo para las propias organizaciones, sino también para las comunidades y los países en los que operan.

En los entornos extremadamente volátiles y problemáticos actuales, Kaspersky ofrece las soluciones perfectas para proteger sus datos, su negocio y su reputación. Utilice la siguiente tabla para elegir la solución que mejor se adapte a su empresa.

Cómo utilizar la tabla

Todas nuestras soluciones garantizan una protección demostrada para su empresa, pero como cada organización tiene su propio conjunto de necesidades, hemos dividido nuestras recomendaciones en tres grupos para que pueda elegir fácilmente la opción perfecta.

La clasificación **Buena** ofrece protección suficiente para una amplia gama de requisitos de ciberseguridad.

La clasificación **Mejor** incluye defensas adicionales y productos de inteligencia de amenazas.

La clasificación **Ideal** proporciona la protección más avanzada y exhaustiva de todo el mundo, además de herramientas de gestión mejoradas.

Solución	Buena	Mejor	Ideal
 **Kaspersky Endpoint Security**	**Qué** Kaspersky Endpoint Security for Business + Kaspersky Maintenance Service Agreement Plus **¿Cómo?** — Se adapta a sus necesidades únicas de negocio y ofrece protección total incluso contra las amenazas más avanzadas y desconocidas. Ahorra tiempo gracias a la reducción de incidentes de seguridad, las alertas y la solución de problemas, lo que elimina complicaciones para el usuario y reduce el tiempo de inactividad. — Las tecnologías integradas reducen el MTTR (tiempo medio de respuesta) al mínimo, sin necesidad de operadores altamente cualificados; mantienen el TCO bajo y el ROI alto, proporcionando cobertura contra la mayoría de las amenazas. — Protege los datos civiles y la confidencialidad, y ayuda a lograr objetivos de cumplimiento clave, incluido el GDPR, gracias a las funciones de cifrado con certificación y gestión del cifrado integrado en el sistema operativo. — Acceso a los programas de asistencia Premium y ampliada, con cobertura de hasta 12 incidentes al año y un tiempo de respuesta garantizado de 6 horas laborables.	**Qué** Kaspersky Endpoint Security for Business + Kaspersky Cybersecurity for IT Online + Kaspersky Maintenance Service Agreement Business **¿Cómo?** — Formación interactiva para profesionales de IT generales (asistencia de IT, servicio técnico, etc.), donde los programas de concienciación estándar no son suficientes, pero no se requiere una gran experiencia en seguridad. — Se adapta a sus necesidades únicas de negocio y ofrece protección total incluso contra las amenazas más avanzadas y desconocidas. Ahorra tiempo gracias a la reducción de incidentes de seguridad, las alertas y la solución de problemas, lo que elimina complicaciones para el usuario y reduce el tiempo de inactividad. — Las tecnologías integradas reducen el MTTR (tiempo medio de respuesta) al mínimo, sin necesidad de operadores altamente cualificados; mantienen el TCO bajo y el ROI alto, proporcionando cobertura contra la mayoría de las amenazas. — Protege los datos corporativos y la confidencialidad, y ayuda a lograr objetivos de cumplimiento clave (incluido el GDPR) y mejorar la preparación para las auditorías, permitiendo al departamento de IT realizar un seguimiento de las "alteraciones en la configuración", identificar vulnerabilidades o dispositivos sin cifrar y actuar rápidamente respecto de los resultados de la auditoría llevando a cabo las correcciones disponibles.	**Qué** Kaspersky Endpoint Security for Business + Kaspersky CyberSafety Management Games + Kaspersky Maintenance Service Agreement Business **¿Cómo?** — Taller interactivo que permite a los superiores inmediatos centrarse en la importancia de la ciberseguridad en sus trabajos y desarrollar las competencias esenciales para mantener unas prácticas de trabajo seguras en sus divisiones. — Se adapta a sus necesidades únicas de negocio y ofrece protección total incluso contra las amenazas más avanzadas y desconocidas. Ahorra tiempo gracias a la reducción de incidentes de seguridad, las alertas y la solución de problemas, lo que elimina complicaciones para el usuario y reduce el tiempo de inactividad. — Las tecnologías integradas reducen el MTTR (tiempo medio de respuesta) al mínimo, sin necesidad de operadores altamente cualificados; mantienen el TCO bajo y el ROI alto, proporcionando cobertura contra la mayoría de las amenazas. — Protege los datos corporativos y la confidencialidad, y ayuda a lograr objetivos de cumplimiento clave (incluido el GDPR) y mejorar la preparación para las auditorías, permitiendo al departamento de IT realizar un seguimiento de las "alteraciones en la configuración", identificar vulnerabilidades o dispositivos sin cifrar y actuar rápidamente respecto de los resultados de la auditoría llevando a cabo las correcciones disponibles.

Solución	Buena	Mejor	Ideal
		— Acceso permanente a los programas de asistencia Premium y ampliada, con cobertura de hasta 36 incidentes al año y un tiempo de respuesta garantizado de 2 horas laborables.	— Los componentes de defensa contra amenazas móviles (MTD) y gestión de amenazas móviles (MTM) protegen los datos confidenciales y críticos para el negocio mientras los trabajadores están sobre el terreno. — Acceso permanente a los programas de asistencia Premium y ampliada, con cobertura de hasta 36 incidentes al año y un tiempo de respuesta garantizado de 2 horas laborables.
Kaspersky Hybrid Cloud Security	**Qué** Kaspersky Hybrid Cloud Security **¿Cómo?** — Protege las cargas de trabajo de los servidores y los VDI con la mejor protección de red y endpoints de su clase. — Proporciona una visibilidad completa de los activos de TI mediante una combinación perfecta de las herramientas de detección de Kaspersky y las nativas de la nube. — Optimiza la implantación de agentes de seguridad; simplifica la gestión de la seguridad mediante el control detallado, la automatización de la seguridad y las configuraciones y políticas predefinidas. — Se basa en partners de tecnología para eliminar las barreras y los problemas de seguridad en la nube híbrida que, de no eliminarse, podrían paralizar la ejecución de la estrategia en la nube y aumentar los ciberriesgos.	**Qué** Kaspersky Hybrid Cloud Security + Kaspersky Security for Storage **¿Cómo?** — Un nivel adicional de defensa para datos en reposo ofrece protección contra malware persistente, ransomware activo y ataques Wiper de tipo ransomware realizados a través de la red.	**Qué** Kaspersky Hybrid Cloud Security Enterprise + Kaspersky Security for Storage **¿Cómo?** — Completos controles de seguridad sin ninguna renuncia, supervisión de la integridad de los datos y SO en tiempo real, refuerzo de los sistemas y protección de redes avanzada e IDS para satisfacer las rigurosas exigencias de numerosos reglamentos internacionales relativos a la seguridad de los datos. — Diseñado para gestionar enormes cantidades de datos corporativos y proteger las infraestructuras de mayor tamaño y complejidad, al tiempo que se mantiene una visibilidad plena y un control detallado.

Solución	Buena	Mejor	Ideal
 **Kaspersky Threat Management and Defense**	**Qué** Kaspersky Secure Mail Gateway + Kaspersky Secure Web Gateway **¿Cómo?** — Funciona como parte de un enfoque preventivo de los ataques dirigidos. Proporciona prevención de amenazas de correo electrónico automatizada y ofrece una excelente protección para el tráfico que discurre a través de los servidores de correo electrónico contra spam, phishing y amenazas de malware genéricas y sofisticadas. — Protección integral frente a los peligros de Internet, bloqueando todo contenido peligroso en el tráfico web.	**Qué** Kaspersky Anti Targeted Attack Platform + Kaspersky Endpoint Detection and Response **¿Cómo?** — Protección especializada contra amenazas avanzadas y ataques dirigidos que permite la detección de amenazas multidimensionales automatizada en el proxy, la web, el correo electrónico y los endpoints. — Un sólido núcleo de correlación de eventos basado en el aprendizaje automático y el análisis de datos retrospectivos crea una imagen muy completa de todas las fases del ataque y proporciona capacidades de respuesta centralizada, mientras simplifican y agilizan la contención de amenazas cruciales y los procedimientos de neutralización.	**Qué** Kaspersky Anti Targeted Attack Platform + Kaspersky Endpoint Detection and Response + Kaspersky Cybersecurity Services **¿Cómo?** — Protección especializada contra amenazas avanzadas y ataques dirigidos que permite la detección de amenazas multidimensionales automatizada en el proxy, la web, el correo electrónico y los endpoints. — Un sólido núcleo de correlación de eventos basado en el aprendizaje automático y el análisis de datos retrospectivos crea una imagen muy completa de todas las fases del ataque y proporciona capacidades de respuesta centralizada, mientras simplifican y agilizan la contención de amenazas cruciales y los procedimientos de neutralización. — Los productos mejoran aún más gracias al acceso a la base de conocimientos global de Kaspersky sobre amenazas, junto con la formación de especialistas, el análisis continuo de los eventos de seguridad de la información y la rápida respuesta a incidentes, lo que ayuda a las organizaciones a detectar rápidamente actos malintencionados y a evitar futuros ataques.
 **Kaspersky IoT Security**	**Qué** Kaspersky Embedded Systems Security	**Qué** Kaspersky Embedded Systems Security + Kaspersky Maintenance Service Agreement	**Qué** Kaspersky Embedded Systems Security + Kaspersky Maintenance Service Agreement + equipo basado en KasperskyOS

Solución	Buena	Mejor	Ideal
	¿Cómo? — Proporciona protección obligatoria incluso para los dispositivos con hardware débil y software antiguo, y facilita el cumplimiento de los requisitos normativos.	**¿Cómo?** — La adición de servicios gestionados garantiza el buen funcionamiento de la seguridad en todo momento y reduce las probabilidades de una interrupción devastadora de los procesos. — Proporciona protección obligatoria incluso para los dispositivos con hardware débil y software antiguo, y facilita el cumplimiento de los requisitos normativos.	**¿Cómo?** — Los equipos de red con un sistema operativo de Kaspersky seguro desde el diseño reducen el riesgo de ataque y del espionaje o sabotaje/denegación del servicio posteriores. — La adición de servicios gestionados garantiza el buen funcionamiento de la seguridad en todo momento y reduce las probabilidades de una interrupción devastadora de los procesos. — Proporciona protección obligatoria incluso para los dispositivos con hardware débil y software antiguo, y facilita el cumplimiento de los requisitos normativos.
Kaspersky Cybersecurity Services	**Qué** Industrial Control Systems (ICS) Security Assessment, Penetration Testing, Customer-specific Threat Intelligence Reporting, Incident Response **¿Cómo?** — El servicio Kaspersky ICS Security Assessment identifica fallos de seguridad en los ICS en todos los niveles, proporcionando información sobre la gravedad de los fallos junto con información suficiente para solucionarlos y mejorar la seguridad. Penetration Testing expone los fallos de seguridad ocultos que, de otro modo, podrían permitir a los delincuentes acceder a los equipos de ICS, así como a cualquier sistema conectado a ellos, incluida la red de la empresa en su conjunto.	**Qué** Customer-specific Threat Intelligence Reporting + Incident Response retainer + Threat Data Feeds + Threat Lookup + Cloud Sandbox + Smart Technologies and IoT Security Assessment **¿Cómo?** — La inteligencia frente a amenazas externas asigna eventos internos a agentes externos, lo que permite contar con estrategias de defensa eficaces contra los ataques de ransomware, genéricos y avanzados. — Garantiza la seguridad de dispositivos y sistemas IoT.	**Qué** Customer-specific Threat Intelligence Reporting + Incident Response Training + Threat Data Feeds, Threat Lookup + Cloud Sandbox + Incident Response Retainer + Smart Technologies and IoT Security Assessment + APT Intelligence Reporting + Malware Analysis + Digital Forensics and Incident Response Trainings **¿Cómo?** — Los servicios Incident Response, Digital Forensics and Malware Analysis y Reverse Engineering Trainings crean capacidades internas vitales, potenciadas por un partner de Kaspersky cualificado a su disposición para

Solución	Buena	Mejor	Ideal
	— Customer-specific Threat Intelligence utiliza métodos pasivos para descubrir a qué información confidencial podría obtener acceso un atacante externo en fuentes abiertas (incluidos recursos web profundos), al tiempo que ayuda a identificar fugas de información en la web oscura y cualquier amenaza dirigida a la cadena de suministro, así como a proporcionar directrices sobre soluciones procesables. — Incident Response proporciona el análisis experto e independiente de Kaspersky de las pruebas de incidentes, reconstruyendo la cronología de los incidentes, determinando las posibles fuentes y los fundamentos, y desarrollando un plan para la corrección y la limitación de daños.		responder a incidentes más complejos y sofisticados. — La inteligencia frente a amenazas externas asigna eventos internos a agentes externos, lo que permite contar con estrategias de defensa eficaces contra los ataques de ransomware, genéricos y avanzados.
Kaspersky Industrial Cybersecurity	**Qué** Kaspersky Industrial Cybersecurity for Nodes **¿Cómo?** — KICS for Nodes es una solución de protección industrial de endpoints. — Proporciona un alto nivel de ciberseguridad para redes y nodos industriales "listos para usar", por lo que es ideal para empresas industriales que se encuentran al principio de su viaje por la ciberseguridad de OT, o para aquellas con recursos humanos limitados.	**Qué** Kaspersky Industrial Cybersecurity for Nodes + Kaspersky Industrial Cybersecurity for Networks **¿Cómo?** — KICS for Networks es un software de detección industrial de vulnerabilidades y anomalías que proporciona monitorización pasiva de redes industriales en tiempo real. — Detecta las intrusiones típicas en la red de TI (análisis de redes, tráfico de malware accidental, etc.), así como cualquier APT que se dirija a PLC y	**Qué** Kaspersky Industrial Cybersecurity for Nodes + Kaspersky Industrial Cybersecurity for Networks + Machine Learning for Anomaly Detection **¿Cómo?** — La tecnología Machine Learning for Anomaly Detection (MLAD) está diseñada para proteger la OT en función del análisis de telemetría. — Mediante el uso de correlaciones en las señales de tráfico industrial, la tecnología MLAD puede entrenar a

Solución	Buena	Mejor	Ideal
		sistemas de seguridad; lleva a cabo la gestión de activos, mantiene la integridad de la red industrial, y supervisa y registra acciones de terceros. — Proporciona un único punto de acceso para abordar y resolver tareas de seguridad y no relacionadas con la seguridad por igual.	una red neural recurrente para que reconozca el comportamiento de la señal en condiciones de funcionamiento normales. — Después de recibir la formación, la tecnología MLAD predice los valores de todas las señales en tiempo real y los compara con los valores observados. Si el error de predicción es mayor que un umbral, MLAD detecta una anomalía y envía una alerta. — MLAD se integra con KICS for Networks.

Noticias de ciberamenazas: www.securelist.com
Noticias de seguridad de IT: business.kaspersky.com

www.kaspersky.es

kaspersky

BRING ON THE FUTURE