Publicado en Madrid el 12/01/2023

# [La producción robotizada se paralizaría semanas tras un ciberataque](http://www.notasdeprensa.es)

## La mayoría de los empleados no se ven preparados para dotar a los robots de autonomía total, tal y como revela un estudio de Kaspersky. Las investigaciones acerca de las consecuencias de la automatización con robots y sistemas basados en Inteligencia Artificial reflejan que la mayoría de los empleados españoles no cree que la producción pueda recuperarse de forma inmediata en caso de ciberataque o un fallo en el funcionamiento. El 75% considera que la recuperación total llevaría días o incluso semanas

 Los ciberdelincuentes atacan a las empresas a través de correos electrónicos, espacios virtuales y otros sistemas. Buscan continuamente nuevas formas de vulneración, algo que las empresas deben tener en cuenta al implementar nuevas tecnologías como la robótica en el caso de sus procesos productivos. Y es que, aunque aumentan la eficiencia, plantean serias preocupaciones en el ámbito de la ciberseguridad y la confianza. Sobre esta base, Kaspersky ha realizado una encuesta para recoger las opiniones de empleados que trabajan con robots en España, a fin de comprender los desafíos y problemas de seguridad derivados del uso de este tipo de dispositivos en los entornos de trabajo. Según el estudio, la mayoría de los empleados de empresas españolas que usan robots en la producción son conscientes de los riesgos que esto implica para la ciberseguridad. Solo un 8% de ellos cree que los robots que dejan de funcionar por un ciberataque pueden repararse al momento. La mitad (50%) considera que las operaciones de recuperación durarán semanas, mientras que los encuestados más optimistas (25%) opinan que la producción podría recuperarse en solo unos días. Preocupación por la falta de control y regulación de robots y su autonomíaTeniendo en cuenta los riesgos que puede implicar la rápida robotización de los entornos de trabajo, más de la mitad de los encuestados (60%) en España dice que no está claro quién asumirá la responsabilidad final en el caso de que los robots fallen por un fallo o ciberataque. Este es uno de los motivos por los cuales los empleados prefieren a humanos en los puestos de responsabilidad. La mayoría (76%) cree que los robots pueden aumentar la eficiencia en la producción, pero solo con supervisión humana, y menos de una quinta parte de los trabajadores (17%) está dispuesta a confiar cualquier proceso productivo a robots. "En este estudio, los encuestados no solo evaluarán el nivel de robotización de las empresas, sino la capacidad para resistir a los riesgos cibernéticos que estas tecnologías implican. Muchos empleados tenían sentimientos encontrados sobre el nivel de protección de los robots. Son conscientes de que se debe prestar mayor atención a su seguridad y se muestran escépticos sobre la rapidez con la que pueden recuperarse tras un ciber incidente. Se hace frente a las preocupaciones sobre el funcionamiento y protección de los sistemas industriales basados en Internet de las Cosas (IoT) con una gran variedad de dispositivos inteligentes dentro del ecosistema. En Kaspersky hay soluciones de Ciber Inmunidad, capaces de proteger unidades empresariales específicas o todo el sistema TI de la organización, lo que se dota de inmunidad frente a ciberataques a robots, y todo sin utilizar herramientas de seguridad específicas. Por ejemplo, Kaspersky IoT Secure Gateways protege el sistema TI y recopila y transmite datos de campo a otras plataformas digitales de una forma segura, ofreciendo una imagen completa y de confianza del equipo y los procesos de producción", asegura Andrey Suvorov, director de la unidad de negocio de KasperskyOS. Para mantener los sistemas de computación industrial protegidos frente amenazas, los expertos de Kaspersky recomiendan: Realizar evaluaciones periódicas de seguridad de los sistemas OT (Operation Technology) para identificar y eliminar posibles problemas de ciberseguridad. Establecer análisis continuos de vulnerabilidades y triajes como base de unos procesos efectivos de gestión de amenazas. Las soluciones dedicadas como Kaspersky Industrial CyberSecurity pueden ser un asistente eficaz y una fuente única de información. Realizar las actualizaciones pertinentes en los componentes clave de la red OT de la compañía; aplicar correcciones y parches de seguridad o implementar medidas técnicas apropiadas tan pronto como sea posible. Esto es crucial para prevenir incidentes que pueden costar millones por la interrupción del proceso productivo. Usar soluciones industriales EDR como Kaspersky Industrial Cybersecurity for Nodes para la detección temprana de amenazas muy sofisticadas, su posterior investigación y una resolución efectiva de incidentes. Mejorar la respuesta frente a las nuevas técnicas maliciosas desarrollando y fortaleciendo la prevención, detección y respuesta a incidentes de su fuerza laboral. La capacitación específica en seguridad OT para equipos de seguridad TI y el propio personal OT es una de las medidas cruciales para alcanzar este objetivo. El informe completo con más claves acerca de las consecuencias de la automatización y el aumento del uso de robots está disponible en este link.

**Datos de contacto:**

Mónica Iglesias

690 196 537

Nota de prensa publicada en: [https://www.notasdeprensa.es/la-produccion-robotizada-se-paralizaria\_1](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorias: Inteligencia Artificial y Robótica E-Commerce Ciberseguridad



[**http://www.notasdeprensa.es**](http://www.notasdeprensa.es)