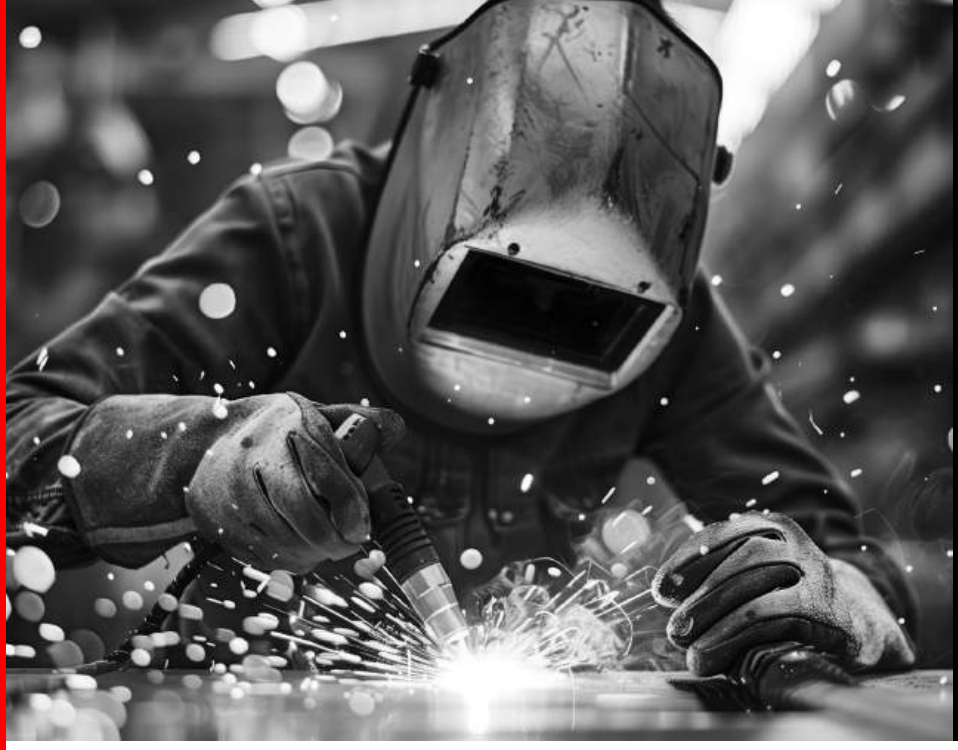


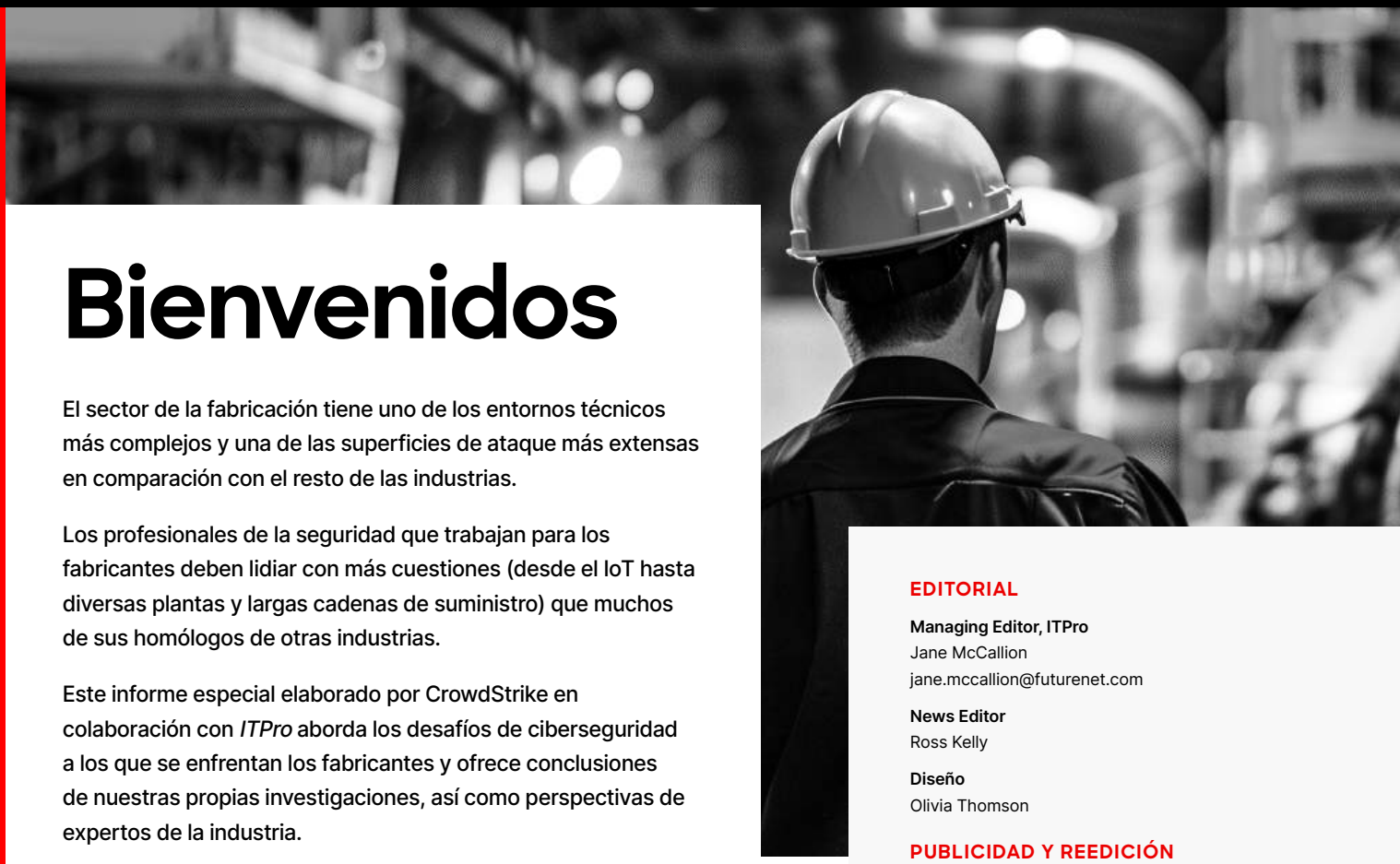
Asedio a la fábrica

Cómo sortear el complejo panorama de ciberamenazas

ITPro.
BY FUTURE B2B

en colaboración con

CROWDSTRIKE



Bienvenidos

El sector de la fabricación tiene uno de los entornos técnicos más complejos y una de las superficies de ataque más extensas en comparación con el resto de las industrias.

Los profesionales de la seguridad que trabajan para los fabricantes deben lidiar con más cuestiones (desde el IoT hasta diversas plantas y largas cadenas de suministro) que muchos de sus homólogos de otras industrias.

Este informe especial elaborado por CrowdStrike en colaboración con *ITPro* aborda los desafíos de ciberseguridad a los que se enfrentan los fabricantes y ofrece conclusiones de nuestras propias investigaciones, así como perspectivas de expertos de la industria.

Jane McCallion

Managing Editor, ITPro

Índice

EDITORIAL

Managing Editor, ITPro
Jane McCallion
jane.mccallion@futurenet.com

News Editor
Ross Kelly

Diseño
Olivia Thomson

PUBLICIDAD Y REEDICIÓN

Vicepresidente global, B2B, Tecnología
Amardeep Mangat
amardeep.mangat@futurenet.com

LICENCIAS Y DISTRIBUCIÓN

Equipo de licencias
licensing@futurenet.com

GESTIÓN

Chief Executive
Jon Steinberg

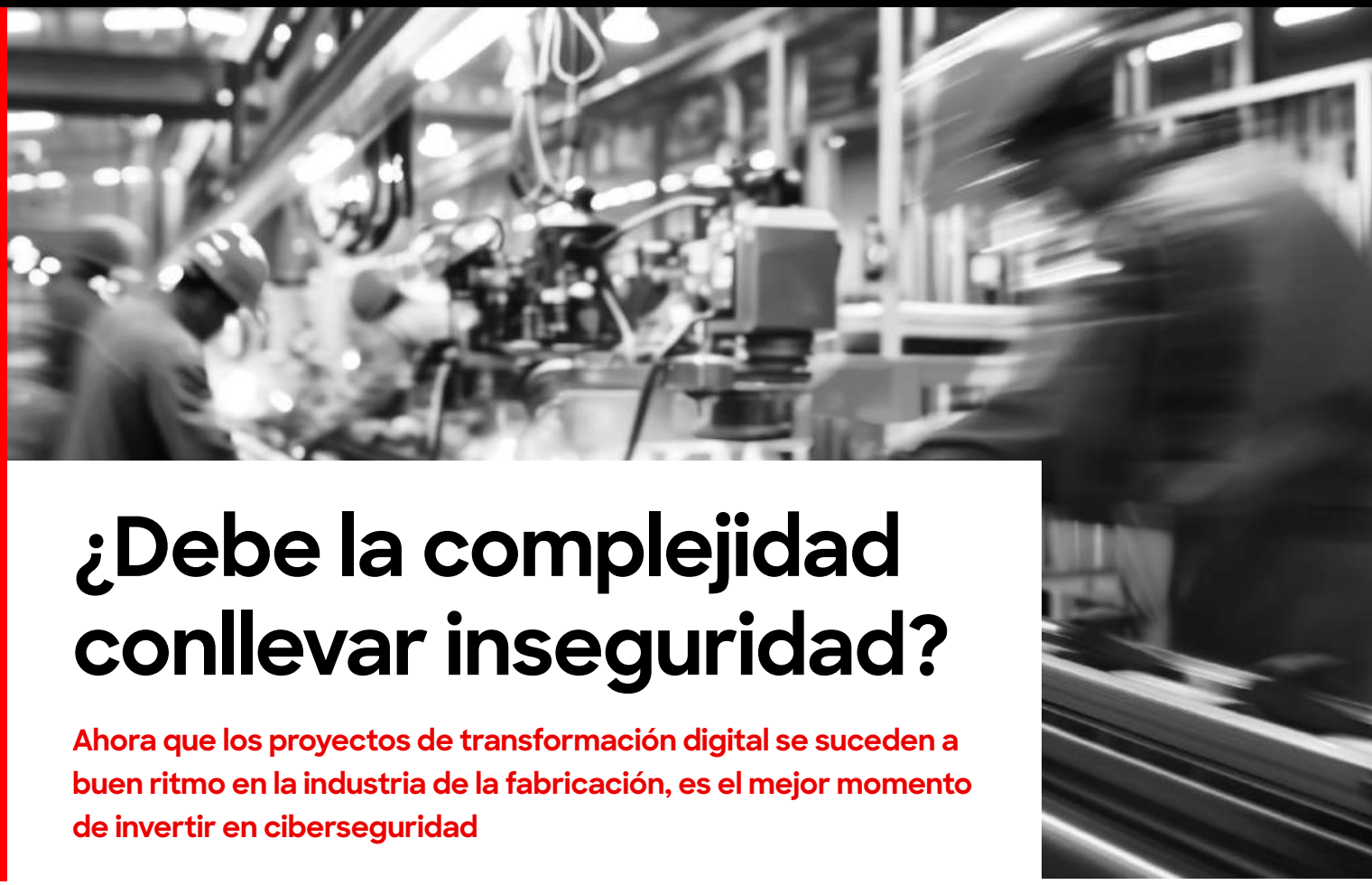
Vicepresidenta sénior y directora general, B2B
Amanda Darman-Allen

Vicepresidenta y Global Head of Content, B2B
Carmel King

Global Content Director, TI B2B
Maggie Holland

Vicepresidenta y Global Head of Strategy & Ops, B2B
Allison Markert

Head of Design, B2B
Nicole Cobban



¿Debe la complejidad conllevar inseguridad?

Ahora que los proyectos de transformación digital se suceden a buen ritmo en la industria de la fabricación, es el mejor momento de invertir en ciberseguridad

El periodo de expansión de la transformación digital por todo el sector de la fabricación ha permitido a las organizaciones mejorar notablemente la eficiencia operativa y optimizar las capacidades relacionadas con la producción.

A lo largo de la última década, cada vez más fabricantes han adoptado la nube. Esta tendencia se aceleró con el paso a las operaciones en remoto al que obligó la pandemia, según revela el informe *Cloud Radar* de InfoSys de abril de 2024.

En 2023, dos de cada tres encuestados por InfoSys afirmaron que habían aumentado el gasto en la nube, mientras que cuatro de cada cinco confirmaron que planeaban incrementar el gasto en el año 2024 y en el futuro.

Este cambio ha acelerado los avances en el ciclo de vida de fabricación, lo cual ha permitido a los operadores incorporar la automatización y la robótica a los procesos, así como adoptar tecnologías como el Internet de las Cosas (IoT), la tecnología operativa (TO) y la inteligencia artificial (IA) a gran escala.

El cambio ha sido profundo y ha aportado beneficios tangibles a las empresas. No obstante, aunque la transformación digital generalizada ofrece resultados positivos a los fabricantes, también conlleva una serie de preocupaciones nuevas y críticas en materia de ciberseguridad.

Según las estadísticas del informe *Building a Culture of Cyber Resilience in Manufacturing*, elaborado por el Foro Económico Mundial (FEM), el sector de la fabricación fue el que más ataques recibió durante tres años consecutivos, pues fue el blanco del 25,7 % de los ciberataques a nivel mundial.

El FEM destacó la rápida digitalización de la industria como un factor determinante en el aumento del nivel de amenazas.

"En la última década, la transformación digital se ha acelerado en el sector. Se ha invertido sin cesar en innovación y en tecnologías emergentes, como los gemelos digitales, la robótica, la IA generativa, la computación en la nube y el Internet Industrial de las Cosas (IIoT)", señala el informe.

"Aunque la digitalización progresiva fomenta el crecimiento, la eficiencia y la rentabilidad, también vincula las tecnologías industriales y operativas con el mundo digital, lo cual expone al sector a las ciberamenazas".

Las cifras mencionadas concuerdan con algunas conclusiones similares del *Informe sobre Threat Hunting* 2024 de CrowdStrike, en el que se indica que el sector de la fabricación es el sexto que más ciberintrusiones sufre en todo el mundo. Cabe destacar que, entre julio de 2022 y junio de 2024, el número de intrusiones aumentó en un 57 %.

En particular, los ciberataques contra la infraestructura de nube se han convertido en una de las principales preocupaciones de los profesionales de la seguridad en el ámbito de la fabricación.

En el *Informe Global sobre Amenazas 2024* de CrowdStrike, por ejemplo, se identifica una tendencia en auge de ataques orientados a la nube: muchos atacantes se están centrando deliberadamente en los entornos de nube.

Según CrowdStrike, los atacantes "orientados a la nube" son aquellos que son conscientes de las lucrativas oportunidades que presentan los entornos de nube vulnerables. Por lo tanto, usan ciertas funciones de estos entornos de forma indebida para atacarlos.

Esta evolución dio como resultado un aumento del 75 % de las intrusiones relacionadas con la nube entre 2022 y 2023, lo que pone de manifiesto las importantes amenazas a las que se enfrentan los fabricantes que desarrollan sus operaciones en la nube.

Sin embargo, los ataques contra la nube no son la única amenaza que afrontan los fabricantes en este momento. Dado que en el sector siguen desarrollándose iniciativas de transformación digital, los operadores se ven obligados a lidiar con una amplia gama de vectores de ataque.

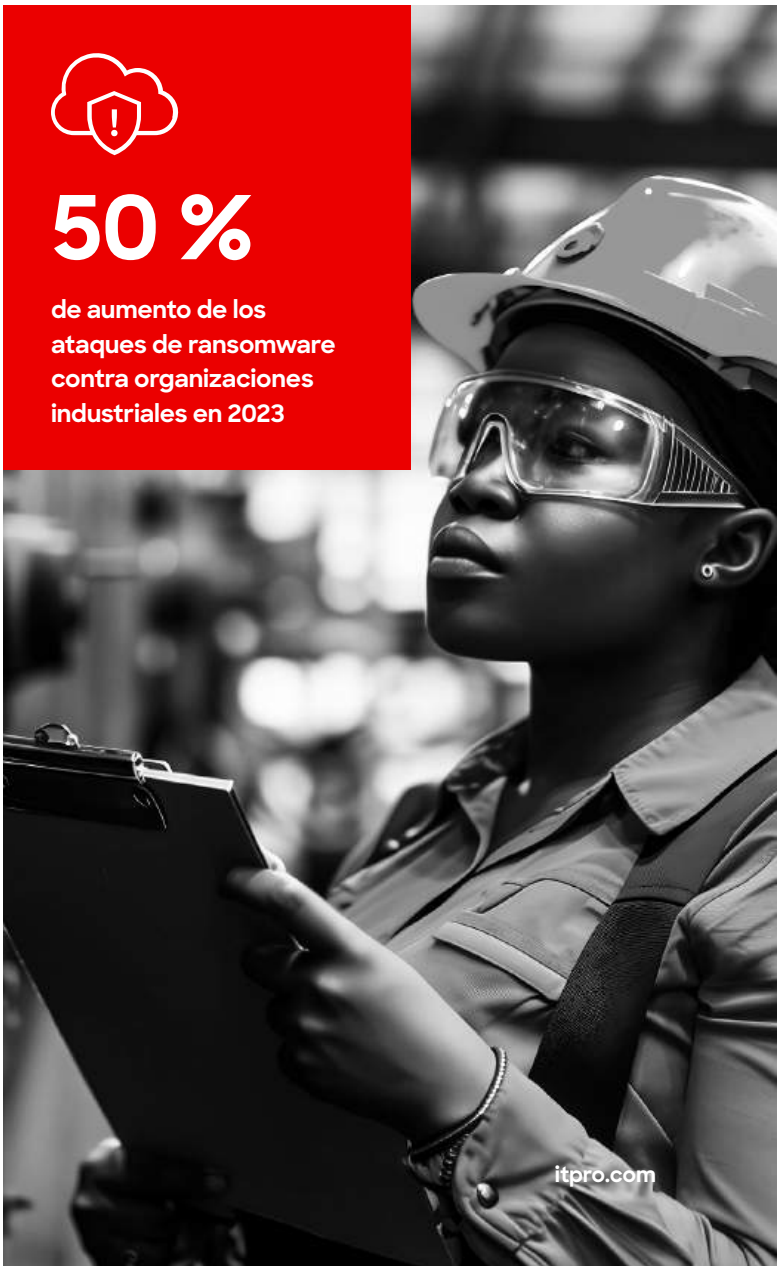
El ransomware sigue siendo una amenaza generalizada

Al igual que ocurre en otras industrias, el sector de la fabricación sufre una cantidad cada vez mayor de ataques de ransomware. Según el FEM, los ataques de este tipo contra organizaciones industriales aumentaron casi un 50 % en 2023, y el 71 % de estos se dirigieron específicamente contra fabricantes.

El FEM señala que el ransomware sigue siendo la "principal preocupación" de los fabricantes, y el 40 % de las personas que respondieron a su encuesta *Cyber Resilience in Manufacturing* ("Ciberresiliencia en el sector de la fabricación") lo califica como su principal amenaza.

50 %

de aumento de los ataques de ransomware contra organizaciones industriales en 2023



De hecho, la opinión de las partes interesadas de la industria sobre las amenazas relacionadas con la fabricación también se refleja en una encuesta que *ITPro* llevó a cabo en nombre de CrowdStrike.

Esta encuesta, que se realizó en junio de 2024 e incluye las perspectivas de 400 responsables de la toma de decisiones de TI de EMEA, revela que casi dos tercios (64 %) de los encuestados consideran que el sector de la fabricación se encuentra en un riesgo "ligeramente mayor" que otras industrias. Por otra parte, el 5 % de los encuestados afirman que el sector se expone a un riesgo mucho mayor que otras industrias.

En los últimos años, una gran cantidad de fabricantes han sufrido ataques de ransomware, los cuales se dirigen contra una amplia gama de organizaciones, como empresas de productos químicos y fabricantes de automóviles.

La causa raíz de dichos ataques también ha evolucionado considerablemente, pero ha surgido una corriente recurrente: la ingeniería social y el phishing.

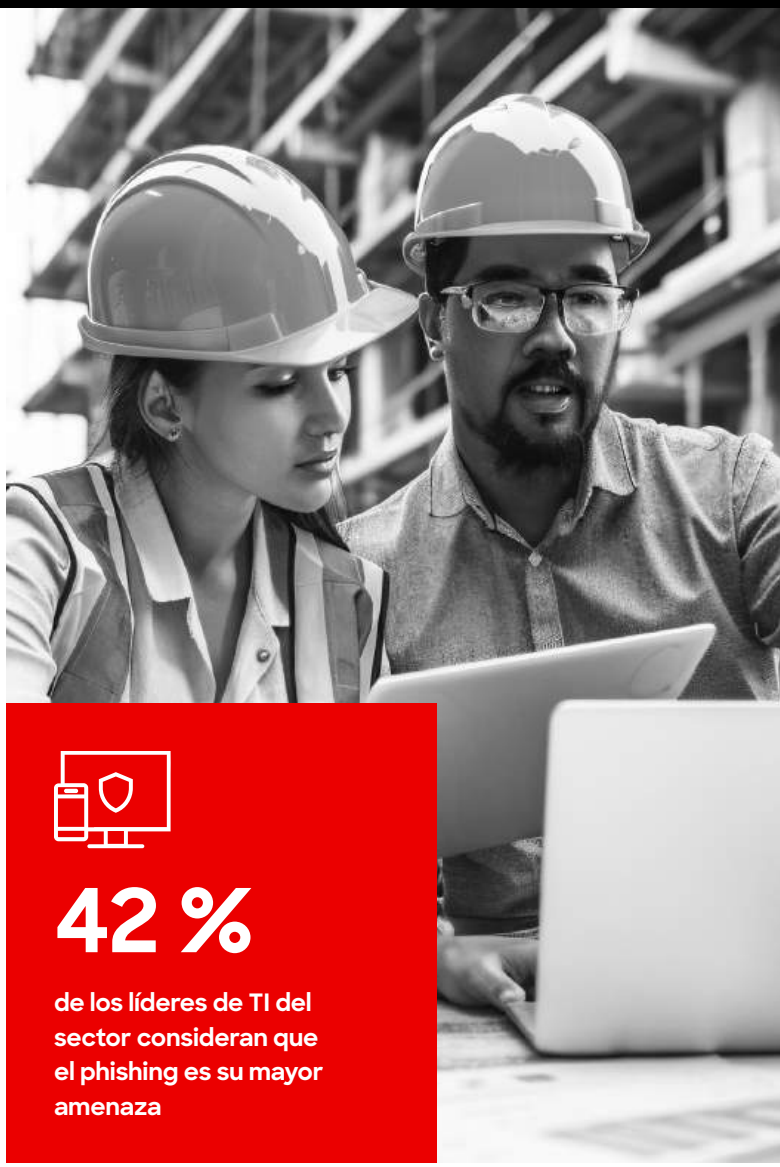
Phishing: una amenaza cada vez mayor

Los ataques de phishing e ingeniería social suelen preceder a los de ransomware y siguen siendo un método predilecto de los atacantes, que acechan a miembros incautos del personal con el objetivo de comprometer los sistemas corporativos.

Las partes interesadas de la industria de la fabricación son muy conscientes de las amenazas que presenta la ingeniería social y el phishing. Por ejemplo, más de un tercio (34 %) de los participantes de la encuesta *Cyber Resilience in Manufacturing* ("Ciberresiliencia en el sector de la fabricación") del FEM identificaron estas técnicas como la segunda ciberamenaza más destacada a la que se enfrentaban.

ITPro también halló que el 42 % de los líderes de TI del sector consideran que el phishing es su mayor amenaza.

Esta tendencia no da señales de aminorar. De hecho, los atacantes tratan de atacar cada vez más a los trabajadores de una amplia gama de industrias.



42 %

de los líderes de TI del sector consideran que el phishing es su mayor amenaza

Con esto en mente, los expertos en seguridad pronostican que el phishing seguirá siendo una amenaza importante y generalizada tanto en 2024 como en el futuro, y que el uso de tecnologías emergentes como la IA generativa desempeñará una función clave en esta tendencia.

En los últimos 18 meses, los investigadores de seguridad han advertido en varias ocasiones que las herramientas de IA pueden ayudar a elaborar correos electrónicos fraudulentos más convincentes.

Según un análisis de CrowdStrike, esta es una de las amenazas clave a la que se enfrentarán las organizaciones en adelante, y que la IA podría utilizarse para "automatizar la comunicación en tiempo real" entre el atacante y su víctima.

Aumento de los ataques contra el IoT

En los últimos años, el IoT se ha empezado a usar mucho más en la industria de la fabricación. En 2021, por ejemplo, el valor del IoT en el mercado de la fabricación ascendió a 50 000 millones de dólares (45 700 millones de euros), y se prevé que siga creciendo en 2024 y en adelante.

Se espera que para 2030 crezca más del doble y alcance los 129 420 millones de dólares (118 400 millones de euros).

La implementación del IoT en el ámbito de la fabricación permite a las organizaciones recopilar datos vitales, los cuales pueden difundir luego los trabajadores para proporcionar información detallada sobre la eficiencia operativa y, de ese modo, optimizar los procesos.

No obstante, aunque esta tecnología plantea ventajas, se ha identificado en repetidas ocasiones como un posible punto débil del ecosistema general de seguridad de las organizaciones.

> **"Una organización que se haya visto comprometida puede derivar en cientos de miles de objetivos de ataque secundarios".**
>
> "Informe Global sobre Amenazas" de CrowdStrike

Según el FEM, el IoT propicia "nuevos puntos de entrada" y amplía la superficie de ataque a merced de los ciberdelincuentes.

El informe *The Top Trends in IoT Security in 2024* ("Principales tendencias en seguridad del IoT en 2024") de Forrester Research señala que uno de los factores que más contribuye a la vulnerabilidad del IoT es el hecho de que estos productos están diseñados para que el análisis de datos en tiempo real cuente con una latencia baja.

La encuesta realizada por *ITPro* a fabricantes revela preocupaciones sobre los posibles riesgos de seguridad asociados al IoT: un tercio (37,16 %) de los participantes señalan que los ataques relacionados con el IoT representan el vector de ataque más importante para su organización.

Vulnerabilidades de la cadena de suministro

Las vulnerabilidades de la cadena de suministro han sido la causa raíz de algunos de los ciberataques más devastadores de los últimos tiempos.

Las cadenas de suministro modernas son sumamente complejas y están muy interconectadas, lo que significa que los atacantes que logran comprometer a un proveedor (un tercero o incluso un cuarto) pueden causar estragos en los ecosistemas posteriores.

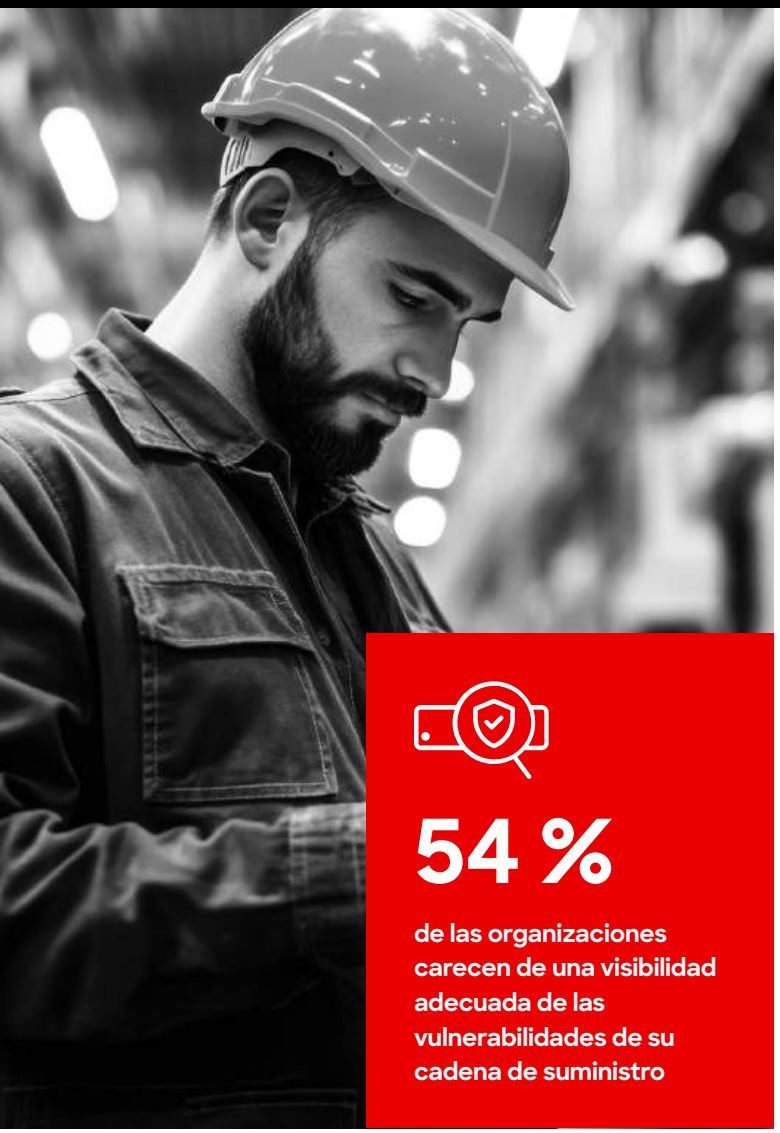
Básicamente, atacar a los proveedores de la cadena de suministro permite maximizar el retorno de la inversión en dicho ataque, tal y como se señala en el *Informe Global sobre Amenazas* de CrowdStrike, ya que el efecto acumulativo de un ataque puede ser enorme.

Según se afirma en el informe, "una organización que se haya visto comprometida puede derivar en cientos de miles de objetivos de ataque secundarios".

"Además, los ataques sigilosos pueden representar una oportunidad mayor para los atacantes cuyo objetivo final esté protegido".

Según el estudio *Global Cybersecurity Outlook* ("Perspectiva sobre la ciberseguridad mundial") del FEM, la visibilidad de la cadena de suministro es una de las principales preocupaciones de los líderes de fabricación hoy en día. El informe revela que más de la mitad (54 %) de las organizaciones carecen de una visibilidad adecuada de las vulnerabilidades de su cadena de suministro.

Cabe destacar que el 41 % de las organizaciones que sufrieron lo que el FEM describió como un "impacto material" debido a un ciberataque señalaron que la brecha se originó en el entorno de un tercero.



54 %

de las organizaciones carecen de una visibilidad adecuada de las vulnerabilidades de su cadena de suministro

Riesgos derivados del teletrabajo

Las plantillas distribuidas se han vuelto algo muy habitual tras la pandemia de COVID. Las organizaciones ahora combinan modelos de trabajo en remoto e híbrido y contratan a trabajadores repartidos por diversas ubicaciones del planeta.

La continuación de estas prácticas tras el fin de la pandemia ha sido beneficiosa tanto para el personal como para los empleadores. Sin embargo, aún persisten riesgos considerables, y muchas organizaciones siguen careciendo de las capacidades técnicas necesarias para proteger eficazmente a sus plantillas distribuidas.

Los teletrabajadores suele usar redes Wi–Fi domésticas que, si no se protegen, pueden suponer un riesgo importante para ellos y sus organizaciones. Durante el cambio generalizado y mundial al trabajo en remoto tras el inicio de la pandemia de COVID, los teletrabajadores se enfrentaron a un aumento de los ataques, según revela un análisis de EY de 2021.

Los dispositivos de trabajo obsoletos y las soluciones de software vulnerables son dos de los principales peligros para los teletrabajadores. Por ello, se recomienda encarecidamente a las organizaciones que cuenten con procesos sólidos de aplicación de parches.

Según las mejores prácticas del Centro de Ciberseguridad Nacional (NCSC) del Reino Unido, es recomendable actualizar los productos obsoletos periódicamente y aplicar parches de forma sistemática en consonancia con las directrices del proveedor.

Cómo combatir las ciberamenazas en el sector de la fabricación

Teniendo en mente esta confluencia de amenazas, hay varias formas en que las organizaciones pueden protegerse frente a los riesgos de ciberseguridad.

Por lo general, para ello es necesario combinar las tecnologías emergentes con la concienciación de la plantilla. Sin embargo, según el FEM, para que una organización adquiera conciencia sobre la seguridad, es determinante que las cúpulas directivas abanderen esta iniciativa.

"Para que un cambio cultural llegue a producirse, siempre es necesario que se origine desde arriba, por lo que es imperativo que los líderes de fabricación y de la cadena de suministro defiendan personalmente el cambio de mentalidad necesario y se erijan como modelos a seguir", tal y como se explica en el informe *Building a Culture of Cyber Resilience in Manufacturing* ("Forjar una cultura de ciberresiliencia en el sector de la fabricación").

Dicho esto, ¿por dónde deben empezar los responsables de seguridad?

Cultura de seguridad y formación de la plantilla

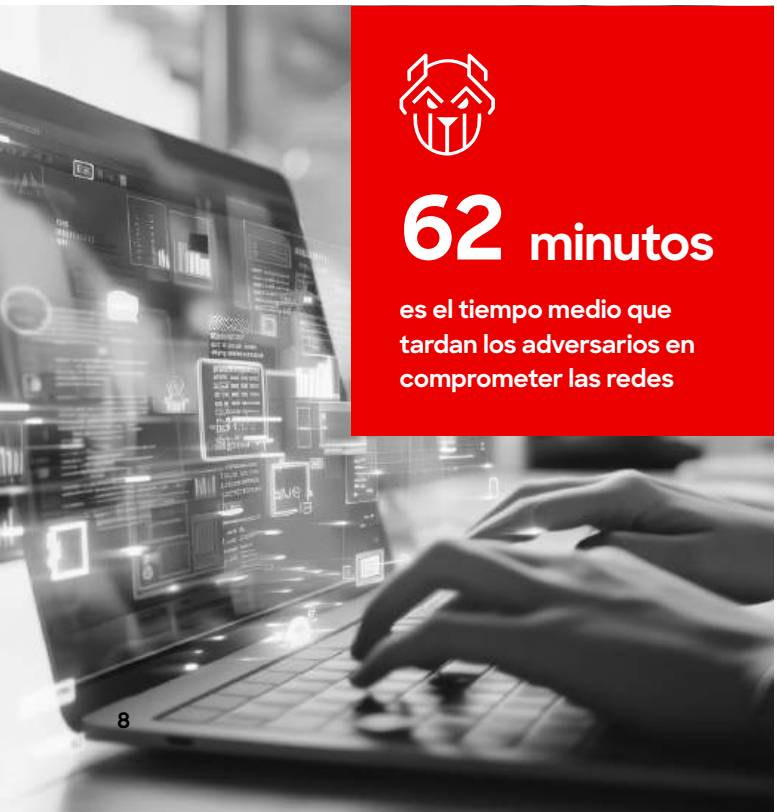
Comenzar desde la base y lograr que el personal integre una cultura de resiliencia y conciencia será fundamental para toda organización.

Formar al personal es vital para combatir las amenazas que plantean los ataques de phishing e ingeniería social, por ejemplo. Enseñarles a detectar las señales que delatan al phishing puede contribuir en gran medida a reforzar la ciberresiliencia básica.

Esto es algo esencial para las organizaciones. Como se indica en el *Informe Global sobre Amenazas 2024* de CrowdStrike, aunque la tecnología es crucial en la lucha por detectar y evitar las intrusiones, el "usuario final sigue siendo un eslabón vital de la cadena para frustrar las brechas de seguridad".

Para generar más conciencia, se deben realizar ejercicios de formación frecuentes con los miembros del personal de todas las funciones de la empresa que sirvan para que estén al día de las últimas amenazas y técnicas que emplean los atacantes.

"Deberían llevarse a cabo programas de concienciación de usuarios para combatir la continua amenaza del phishing y las técnicas de ingeniería social relacionadas", se explica en el *Informe Global sobre Amenazas*.



62 minutos

es el tiempo medio que tardan los adversarios en comprometer las redes

> **"Un cambio cultural efectivo siempre se origina desde arriba, por lo que es imperativo que los líderes de fabricación y de la cadena de suministro defiendan personalmente el cambio de mentalidad necesario y se erijan como modelos a seguir".**
>
> Informe "Building a Culture of Cyber Resilience in Manufacturing" ("Forjar una cultura de ciberresiliencia en el sector de la fabricación") del FEM

Protección de identidades

CrowdStrike considera que las herramientas de protección de identidades también son importantes en la lucha contra los atacantes. Los ataques de ingeniería social basados en la identidad han cobrado protagonismo, según CrowdStrike, lo que significa que es muy recomendable que las organizaciones inviertan en herramientas de autenticación multifactor (MFA) resistentes al phishing.

El módulo CrowdStrike Falcon® Identity Protection, por ejemplo, proporciona a los usuarios una mayor visibilidad de todo el panorama de identidades híbridas de una organización y ofrece una detección hiperprecisa de las amenazas basadas en la identidad.

Si se produce un ataque basado en la identidad, Falcon Identity Protection aplica requisitos de autenticación MFA a los usuarios al detectar actividad sospechosa.

Inversión en soluciones modernas de SIEM

Dado que los ciberataques son cada vez más rápidos, es vital invertir en herramientas de última generación. Los adversarios tardan una media de 62 minutos en comprometer las redes y comenzar a desplazarse lateralmente por los entornos de una organización, tal y como revela el *Informe Global sobre Amenazas* de CrowdStrike.

> **"Deberían llevarse a cabo programas de concienciación de usuarios para combatir la continua amenaza del phishing y las técnicas de ingeniería social relacionadas".**
>
> "Informe Global sobre Amenazas" de CrowdStrike

Es más, el informe señala que la propagación más rápida observada se realizó en solo dos minutos y siete segundos.

Ahora que los ciberataques se producen a velocidades vertiginosas, las soluciones tradicionales de gestión de eventos e información de seguridad (SIEM) pueden resultar ineficaces contra los atacantes y añadir una complejidad innecesaria para los profesionales.

Estas soluciones se diseñaron para una era en la que las organizaciones usaban volúmenes de datos mucho menores, apunta el *Informe Global sobre Amenazas*.

Existen opciones más modernas, como CrowdStrike Falcon® Next-Gen SIEM, que permiten a las organizaciones centralizar la detección, la investigación y la respuesta ante amenazas en una única plataforma. Esto incrementa la velocidad y la eficiencia, lo que permite a los profesionales de la seguridad seguir el ritmo de los adversarios.

IA generativa

Las herramientas de IA generativa han adquirido popularidad en los últimos 18 meses y ahora desempeñan una importante función para las organizaciones que quieren reforzar la ciberseguridad.

Las empresas de todo el mundo ya pueden recurrir a una variedad cada vez mayor de herramientas de asistencia basadas en IA y concebidas específicamente para las operaciones de seguridad.

Varios de los principales proveedores de la industria, entre los que se encuentra CrowdStrike, publicaron eficaces e intuitivas aplicaciones de seguridad basadas en IA para apoyar a las organizaciones y los profesionales cibernéticos durante dicho período.

CrowdStrike presentó en mayo de 2023 Charlotte AI, por ejemplo. Se trata de un asistente que el personal de seguridad puede utilizar en tareas cotidianas de identificación y mitigación de amenazas emergentes.

No obstante, aunque las herramientas de IA sean cada vez más populares (sobre todo en el ámbito de la seguridad), hay aspectos de esta tecnología que algunas organizaciones no tienen en cuenta.

La IA generativa ofrece muchas oportunidades, pero conlleva riesgos nuevos.

La dualidad de la IA

La aparición de la IA generativa ha sido tanto una maldición como una bendición para las organizaciones. Algunas han cosechado beneficios tangibles y, a su vez, se han enfrentado a amenazas cada vez más sofisticadas que se sirven de la IA.

El interés mundial por la IA se ha disparado en los últimos años, y organizaciones de diversas industrias están adoptando esta tecnología para potenciar la eficiencia operativa y dotar a los trabajadores de potentes herramientas que incrementen la productividad.

En el sector de la fabricación, la situación no es diferente. Teniendo en cuenta los rápidos cambios tecnológicos que se producen en la industria, la IA representa una oportunidad magnífica para optimizar las iniciativas de transformación digital a largo plazo.

Según un estudio de McKinsey de 2020, por ejemplo, la IA podría mejorar notablemente tanto la eficiencia como la calidad de la producción. Sin embargo, la aparición de la IA generativa a finales de 2022 ha propiciado una nueva ola de actividad.

Las estadísticas mostradas en *GenAI Awareness, Readiness, and Commitment (ARC) Survey* ("Encuesta sobre concienciación, preparación y compromiso respecto a la IA generativa") de IDC de 2023 revelaron que diversos fabricantes de Europa estaban evaluando activamente o implementando soluciones de IA generativa.

Alrededor del 30 % de los encuestados afirmaron que ya habían invertido mucho en esta tecnología y estaban en proceso de asignar partidas presupuestarias a

> **El auge de la IA generativa "tiene el potencial de reducir los obstáculos que impiden la entrada de adversarios poco cualificados".**
>
> "Informe Global sobre Amenazas" de CrowdStrike

formación, adquisición de herramientas de IA generativa y posibles consultorías.

Además, alrededor del 20 % ya habían comenzado las pruebas iniciales de modelos de IA para respaldar las operaciones y estaban creando pruebas de concepto.

Mientras tanto, en el Reino Unido existe un gran interés por las soluciones de IA generativa. Según el informe *Situación de la fabricación inteligente 2024* de Rockwell Automation, más de tres cuartas partes (79 %) de los fabricantes del Reino Unido esperan utilizar la IA generativa en sus operaciones en el próximo año.

Cabe destacar que el 88 % de los encuestados afirman que ya han invertido en iniciativas de IA o planean hacerlo en los próximos 12 meses.

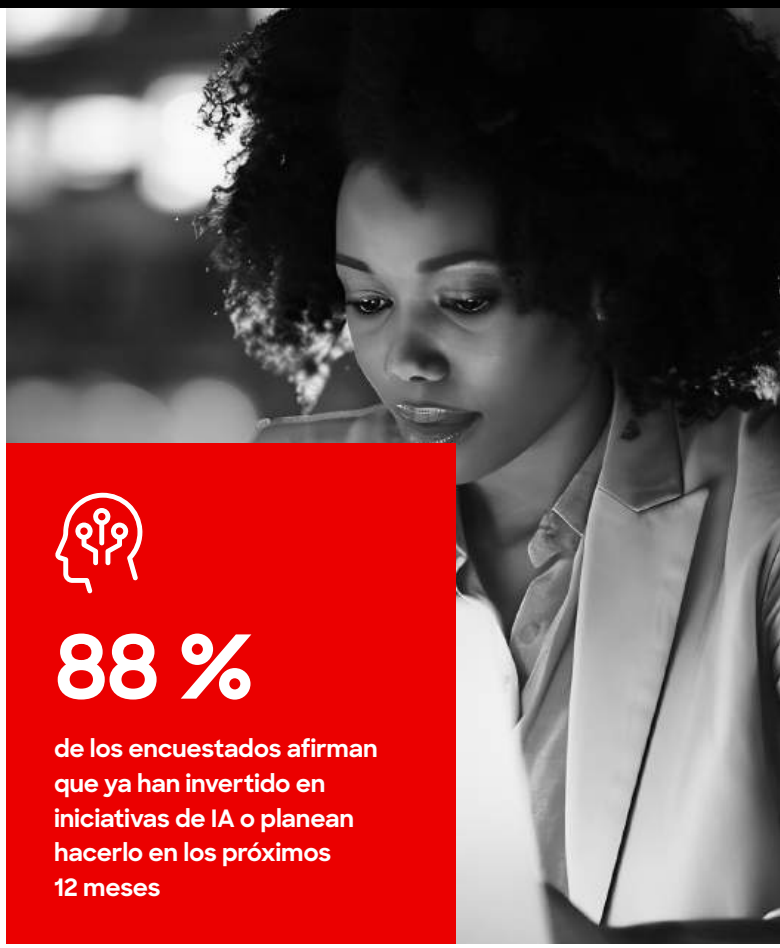
La IA en la fabricación plantea riesgos y oportunidades

Como ocurre con cualquier tecnología emergente, las expectativas infladas se ven atenuadas por los riesgos que incorpora, y existen preocupaciones de seguridad notables relacionadas con la IA generativa. Los expertos en seguridad han advertido reiteradamente sobre el posible uso indebido de la tecnología por parte de los atacantes en los últimos meses.

Un estudio de junio de 2024 del NCSC del Reino Unido advierte que la IA "muy probablemente incrementa el volumen y el impacto de los ciberataques" y que los grupos vinculados a Estados "ya están usando la IA en diversos grados" en sus operaciones.

En este sentido, también es igualmente preocupante el hecho de que la IA generativa está ayudando a los atacantes menos avezados. Esto concuerda en gran medida con las conclusiones del *Informe Global sobre Amenazas 2024* de CrowdStrike, que menciona que el auge de la IA generativa "tiene el potencial de reducir los obstáculos que impiden la entrada de adversarios poco cualificados" y facilitar ataques más punteros.

Esto significa que los atacantes menos avanzados, además de los cibercriminales más consolidados y competentes, pueden usar estas herramientas para perpetrar ataques.



88 %

de los encuestados afirman que ya han invertido en iniciativas de IA o planean hacerlo en los próximos 12 meses

Nuevas amenazas para el sector de la fabricación

El sector de la fabricación lleva varios años enfrentándose a amenazas cada vez mayores, en gran medida debido a la función esencial que desempeña en la economía mundial. Por ejemplo, un estudio de Netwrix de enero de 2024 reveló que casi dos tercios (64 %) de los operadores del sector sufrieron un ciberataque en 2023.

En un incidente ocurrido en febrero de 2024, un fabricante de baterías alemán fue víctima de un ataque que interrumpió la producción de cinco plantas durante más de dos semanas.

Estos incidentes y sus desastrosos efectos son solo una muestra de los peligros que acechan a los fabricantes hoy en día. El aumento de los ataques y un uso cada vez mayor de la IA generativa por parte de los atacantes plantearán grandes desafíos en materia de ciberseguridad para el sector de la fabricación.

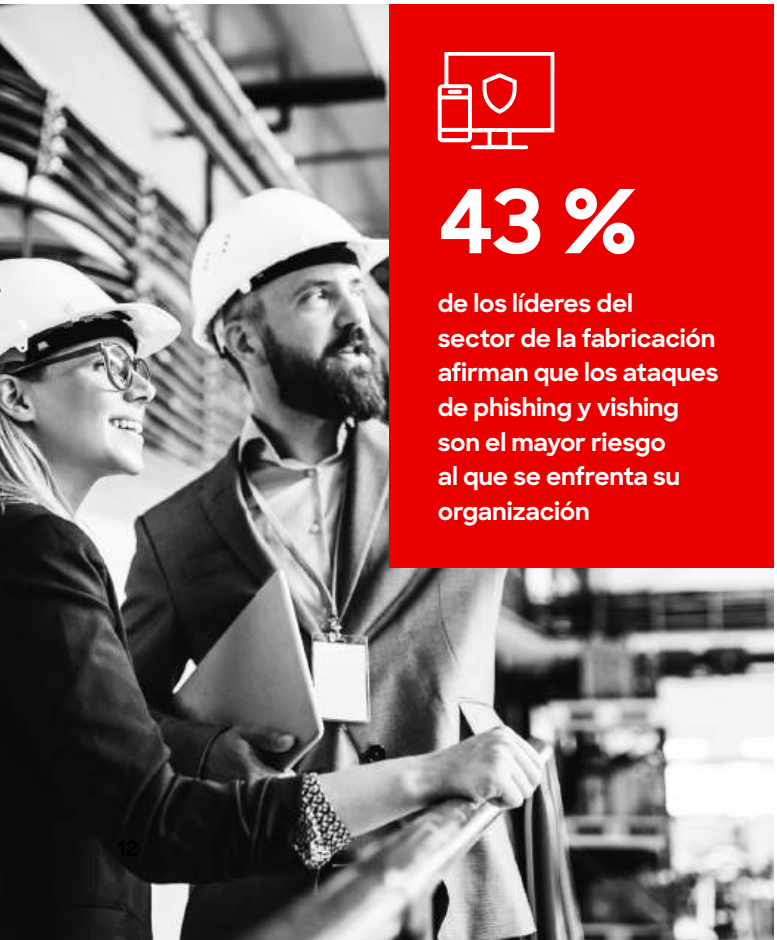
Las partes interesadas de la industria son muy conscientes de esta alarmante situación. De hecho, la encuesta de *ITPro* realizada a 400 responsables de TI del sector revela que el 40 % de los participantes consideran que la IA es el mayor riesgo al que se enfrenta su organización en lo que respecta a posibles vectores de ataque.

No obstante, ¿qué áreas exactamente están expuestas a ciberriesgos debido a la IA generativa? En la actualidad, el panorama es heterogéneo, pero están surgiendo temas comunes clave.

La IA y el auge del phishing

Los ataques de phishing llevan mucho tiempo siendo una pesadilla para organizaciones de todo el mundo. Casi la mitad (43 %) de los líderes del sector de la fabricación señalaron a *ITPro* que los ataques de phishing y vishing son el mayor riesgo al que se enfrenta su organización.

El objetivo de cualquier ataque de ingeniería social es pillar a una víctima desprevenida y engañarla para que revele información confidencial que pueda facilitar un ataque de mayor envergadura.



43 %

de los líderes del sector de la fabricación afirman que los ataques de phishing y vishing son el mayor riesgo al que se enfrenta su organización

La información puede ser, por ejemplo, datos de inicio de sesión, que podrían ayudar a un atacante a acceder a redes o sistemas corporativos. De manera similar, muchos ataques de ingeniería social tienen como objetivo engañar a las víctimas para que instalen archivos maliciosos en los dispositivos de trabajo y se abra otra vía de acceso a las redes de una organización.

Con la llegada de la IA generativa, los atacantes han identificado una oportunidad magnífica para intensificar sus ataques. Esta tecnología les permite perfeccionar sus técnicas y crear correos electrónicos fraudulentos más convincentes. El NCSC destacó específicamente esta preocupación en un aviso publicado a principios de año.

"Debido a la IA generativa y a los modelos de lenguaje grandes, a todo el mundo, independientemente de su nivel de conocimiento sobre ciberseguridad, le resultará muy difícil evaluar si un correo electrónico o una solicitud de restablecimiento de contraseña son genuinos, o identificar intentos de phishing, de suplantación de identidad o de ingeniería social", advierte el organismo.

La IA plantea importantes desafíos de vishing

De manera similar al aumento de las amenazas de phishing basadas en la IA, existen estudios que revelan que esta tecnología también podría usarse para realizar ataques de vishing (o de falsificación de voz) muy sofisticados.

En todo el mundo ya se han utilizado herramientas de IA generativa para crear contenido de "deepfake" muy creíble como parte de campañas de desinformación y para perpetrar ciberataques.

Un "deepfake" es un tipo de contenido generado por IA, que puede incluir vídeo, imágenes o audio, y que se utiliza con el propósito de engañar a alguien. En un contexto de ciberseguridad, los atacantes podrían usar secuencias de vídeo de deepfake para manipular a los empleados.

Este método de ataque ya se ha visto en circulación, y algunos atacantes lo han aplicado con éxito y con consecuencias devastadoras. Por ejemplo, en febrero de 2024, una entidad financiera de Hong Kong fue el blanco de un ataque de ingeniería social por el que los atacantes imitaron a los directores de la empresa para robar más de

25 millones de dólares (22,38 millones de euros). Aunque este incidente afectó a una empresa de servicios financieros, las conclusiones se pueden aplicar totalmente a la industria de la fabricación.

En este caso concreto, se manipuló a un trabajador para que asistiera a una videoconferencia con personas que creía que eran compañeros de trabajo. Más tarde se supo que eran atacantes que utilizaban recreaciones de deepfake.

El año pasado, algunos expertos de la industria destacaron la clonación de la voz mediante la IA como una de las principales amenazas. A finales de 2023, la Agencia de la Unión Europea para la Ciberseguridad (ENISA) anunció en su informe *Threat Landscape* ("Panorama de amenazas") que se esperaba un aumento del contenido generado mediante IA.

Aunque este aviso se centraba principalmente en el uso de contenido generado mediante IA para difundir desinformación electoral, se publicó después de un aviso similar de la Comisión Federal de Comercio de EE. UU. (FTC), que advertía acerca del aumento previsto de los ataques de clonación de voz generados mediante IA y dirigidos contra empresas.

En estas situaciones, un atacante podría usar una grabación de audio de un compañero o un responsable para generar una recreación convincente de su voz y ordenar a miembro del personal que cambie contraseñas, otorgue acceso a sistemas o, como en el incidente de Hong Kong, transfiera fondos.

> **"Debido a la IA generativa y a los modelos de lenguaje grandes, a todo el mundo, independientemente de su nivel de conocimiento sobre ciberseguridad, le resultará muy difícil evaluar si un correo electrónico o una solicitud de restablecimiento de contraseña son genuinos, o identificar intentos de phishing, de suplantación de identidad o de ingeniería social".**
>
> NCSC

Aprovechar la IA para combatir las amenazas emergentes

Si bien los atacantes pueden utilizar la IA generativa para perpetrar ataques cada vez más sofisticados y devastadores, los fabricantes también están usando esta tecnología con fines legítimos.

No obstante, los casos de uso de la IA generativa en el sector varían: según la encuesta de ITPro, el uso de esta tecnología se está extendiendo a una amplia variedad de funciones.

Alrededor del 60 % de los encuestados afirman que aplican la IA generativa al procesamiento del lenguaje natural de los análisis de logs, por ejemplo, mientras que un porcentaje similar de participantes aplican esta tecnología a la respuesta y la corrección automatizadas.

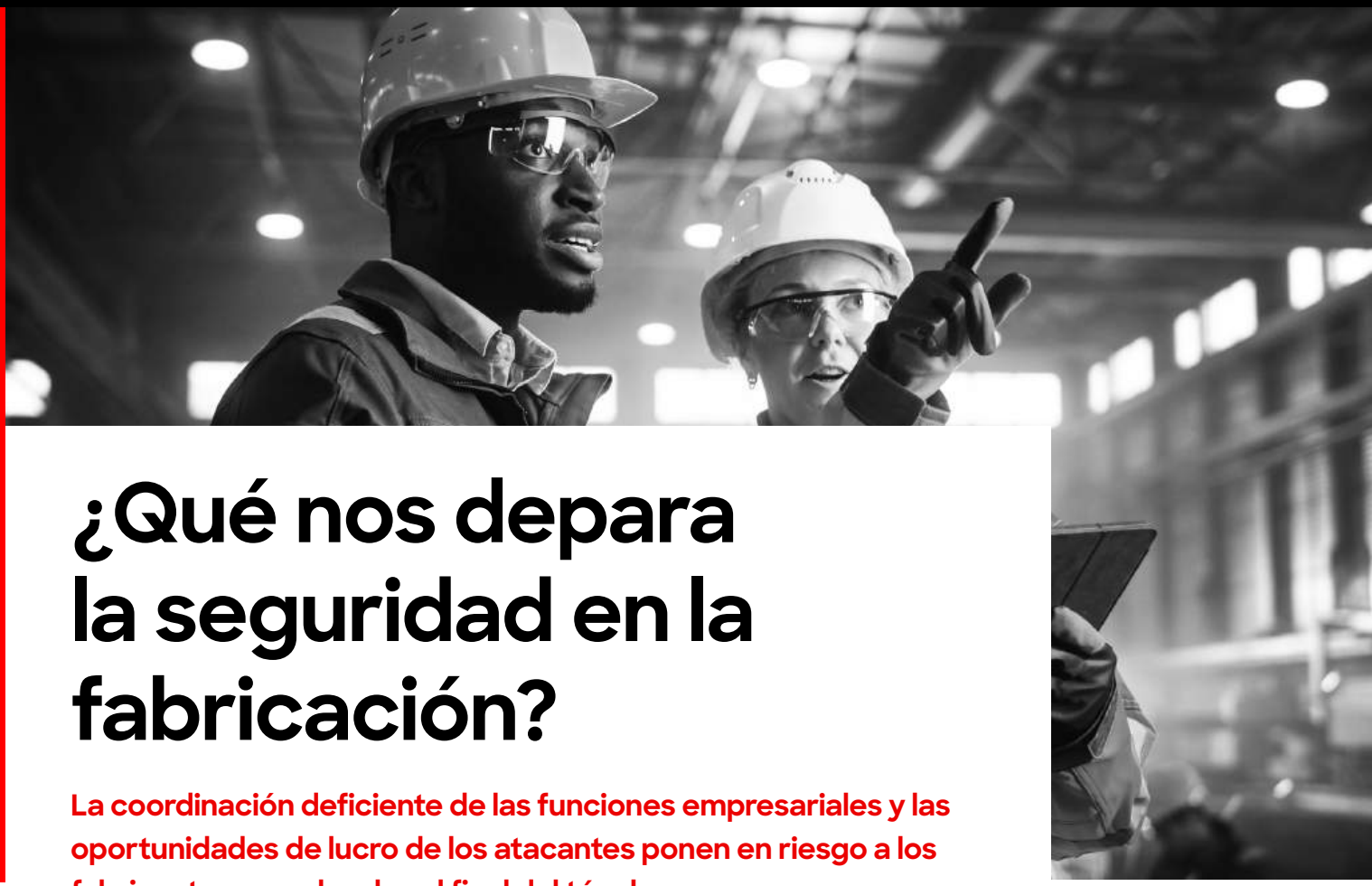
Los fabricantes también están utilizando la IA generativa para potenciar el análisis predictivo en la evaluación de riesgos y, de hecho, el 51 % aplica esta tecnología con este propósito.

Como ya se ha mencionado, la aparición de la IA generativa ha dado lugar a una gama de herramientas de seguridad basadas en IA, y varios proveedores importantes a nivel mundial han lanzado sus propios asistentes de IA.

A los profesionales de ciberseguridad estas herramientas les resultan de gran ayuda para reducir cargas de trabajo y optimizar procesos, así como para monitorizar y detectar amenazas.

Tanto a los profesionales como a las empresas les ha entusiasmado la idea de reducir las tareas manuales y repetitivas de los flujos de trabajo diarios, pues esto permite que el personal de seguridad centre su atención en la prevención de amenazas en lugar de en tareas administrativas.

Aunque la IA sí que representa para los atacantes la oportunidad de aprovechar una tecnología emergente con un propósito perverso, las organizaciones que puedan invertir en esta tecnología con fines de protección podrán combatir el fuego con fuego.



¿Qué nos depara la seguridad en la fabricación?

La coordinación deficiente de las funciones empresariales y las oportunidades de lucro de los atacantes ponen en riesgo a los fabricantes, pero hay luz al final del túnel

Aunque el sector de la fabricación ha evolucionado mucho en los últimos años en términos de tecnología, el panorama de amenazas ha avanzado a la par y cada vez es más peligroso.

Los operadores del sector se enfrentan a una variedad cada vez mayor de ataques devastadores perpetrados por grupos cibercriminales muy competentes. El ransomware sigue estando omnipresente y las amenazas basadas en ingeniería social, como el phishing y el vishing, potenciadas por el uso malicioso de herramientas de IA generativa, plantean un grave peligro para los profesionales de todo el mundo.

Aunque estas amenazas afectan a todas las industrias, los riesgos a los que se exponen los operadores del sector de la fabricación en concreto aumentan muy rápido. Como ya se ha dicho, según el FEM, el sector que recibió un mayor volumen de ataques durante tres años consecutivos es el de la fabricación.

Las partes interesadas de la industria dejaron claras sus preocupaciones en la encuesta de *ITPro* realizada a líderes de TI de este ámbito: casi dos tercios (64 %) de los participantes afirman que el sector se enfrenta a retos específicos en lo que respecta a la seguridad.

Zeki Turedi, CTO de CrowdStrike para EMEA, explica a *ITPro* que esta industria es un "espacio realmente único", lo que lo convierte en un excelente objetivo de ataque. Esto se debe a que dispone de una gran cantidad de organizaciones que desempeñan un papel esencial para que el mundo siga funcionando de manera eficiente, pues produce bienes y componentes que son vitales para la economía global.

"Normalmente, los fabricantes producen bienes cuya entrega debe ser bastante eficiente", afirma. "O bien tratan de controlar un mercado en el que los productos que fabrican lleguen a los proveedores, los usuarios finales o los clientes lo antes posible".

"Los atacantes saben todo esto. Básicamente, la amenaza es que si un atacante interrumpe la actividad de una organización, al fabricante le costará muchísimo dinero", añade Turedi. "Así que insta a la empresa a pagar el rescate para que reanude las operaciones bajo la premisa de que probablemente eso le resulte más barato y asequible que incurrir en pérdidas de beneficios o multas por no cumplir con sus contratos, por ejemplo".

Los ciberataques salen caros

Según el FEM, el coste del cibercrimen ha aumentado de media un 125 % al año. Por ejemplo, el coste medio de cada ataque perpetrado con éxito contra un entorno industrial se sitúa ahora mismo en 4,73 millones de dólares (4,3 millones de euros).

Según un estudio del FEM, se prevé que los costes asociados a los ciberataques aumenten en los próximos años y asciendan a los 10,5 billones de dólares (9,4 billones de euros) en todo el mundo para 2025, lo que representa a la perfección las desastrosas consecuencias financieras que tiene el cibercrimen.

125 %

de aumento del coste mundial de los ciberataques

4,3 M€

es el coste medio de una brecha de datos en entornos de fabricación

9,4 B€

son los costes previstos de los ciberataques mundiales en 2025

(FUENTE: FORO ECONÓMICO MUNDIAL)

Turedi señala que, en esencia, los cibercriminales saben que si logran interrumpir las operaciones de un fabricante, podrán causar estragos en fases posteriores de la cadena. Según sus cálculos, esta situación puede jugar en su favor a la hora de recibir los rescates.

Sin embargo, tal y como advierte Turedi, los fabricantes no tienen que lidiar únicamente con grupos cibercriminales con un móvil económico. También se está observando un aumento de la actividad de sofisticados grupos patrocinados por Estados que intentan robar valiosa propiedad intelectual (PI).

"Por otra parte, los atacantes se han dado cuenta de que la mayoría de los fabricantes poseen propiedad intelectual", explica. "Fabrican algo para ellos o para otras organizaciones, y usan información que probablemente sea el ingrediente secreto o la propuesta de venta única de una organización. Y puede que alguien esté dispuesto a pagar mucho dinero por esa PI".

"Ese es el segundo elemento que interesa a las organizaciones criminales: si acceden a esa información, pueden amenazar con difundirla para exigir un rescate. También hemos identificado un gran interés por parte de Estados nación que no quieren financiar la investigación y el desarrollo de PI, sino que prefieren robarla", añade Turedi.

"Esto se lleva observando durante muchos años a través de numerosas organizaciones y países".

La convergencia de funciones empresariales genera grandes retos

Tal y como apunta Turedi, el sector de la fabricación es "extremadamente complejo", tanto en términos de la cadena de suministro mundial como de las tecnologías que se usan en las operaciones cotidianas.

El uso del IoT en la industria se ha generalizado en años recientes y la inversión en TO también ha ido aumentando.

La TO es el punto de contacto con el mundo real y, en el contexto de la fabricación, incluye el software y el hardware que se usan para monitorizar y realizar el mantenimiento de los equipos y sistemas de control industrial.

De forma muy similar al IoT, la TO ha permitido a los fabricantes automatizar partes de sus procesos y recabar información detallada sobre la eficiencia operativa.

Aunque esto ha beneficiado a los operadores, también ha abierto nuevas vías de ataques de adversarios, según Turedi, y plantea aspectos nuevos y muy complejos que los fabricantes deben tener en cuenta.

"La mayoría de las empresas contarán con la TI para llevar a cabo sus operaciones de negocio. Sin embargo, en el ámbito de la fabricación [también] está la tecnología operativa", explica. "Dicha tecnología puede ser una interfaz gestionada por personas, sensores o incluso robots. Estos componentes se basan en una gran cantidad de tecnología que en última instancia podría ser algo muy similar a un ordenador, pero con mucha actividad a su alrededor".

"La complejidad no se puede actualizar. Tal vez se trate de software obsoleto porque la plataforma se creó hace 10 años y no se puede tocar por haberse creado específicamente para esa versión del sistema operativo y esos componentes", continúa Turedi. "Muchas de las amenazas informáticas con las que los equipos de seguridad de TI llevan un tiempo lidiando están comenzando a afectar a la TO".

ITPro, en su encuesta a líderes de fabricación, resalta que las amenazas relacionadas con el IoT son una de las principales preocupaciones en materia de ciberseguridad.

Los ataques contra la TO y el IoT suelen tener un impacto considerable en el mundo real según un estudio del FEM. Más de la mitad (57 %) de los ciberataques contra la TO en 2022 tuvieron consecuencias físicas".

> **"Esa complejidad implica que existen múltiples formas en las que los ciberdelincuentes pueden atacar a una organización de fabricación".**
>
> Zeki Turedi, CTO de CrowdStrike para EMEA

57 %

de los ciberataques contra la TO en 2022 tuvieron consecuencias físicas

Algunas de estas consecuencias fueron la interrupción de los procesos de producción y daños en la maquinaria industrial. Cabe mencionar que el FEM considera que estos incidentes ponen a los trabajadores en riesgo de sufrir daños físicos.

Turedi enfatiza que la confluencia entre la TO y la TI plantea un desafío significativo para los fabricantes que tratan de reforzar su ciberseguridad y, en última instancia, amplía la superficie de ataque expuesta a los ciberdelincuentes. En esencia, los puntos ciegos entre estas dos funciones presentan grandes oportunidades para que estos causen estragos.

"Esa complejidad implica que existen múltiples formas en las que los ciberdelincuentes pueden atacar a una organización de fabricación. Todo se reduce a la sofisticación del adversario. Por lo tanto, naturalmente los atacantes más comunes y corrientes puede que perpetren ataques de ransomware contra ella", señala.

"También hay atacantes con estrategias más personalizadas, sobre todo a la hora de atacar a

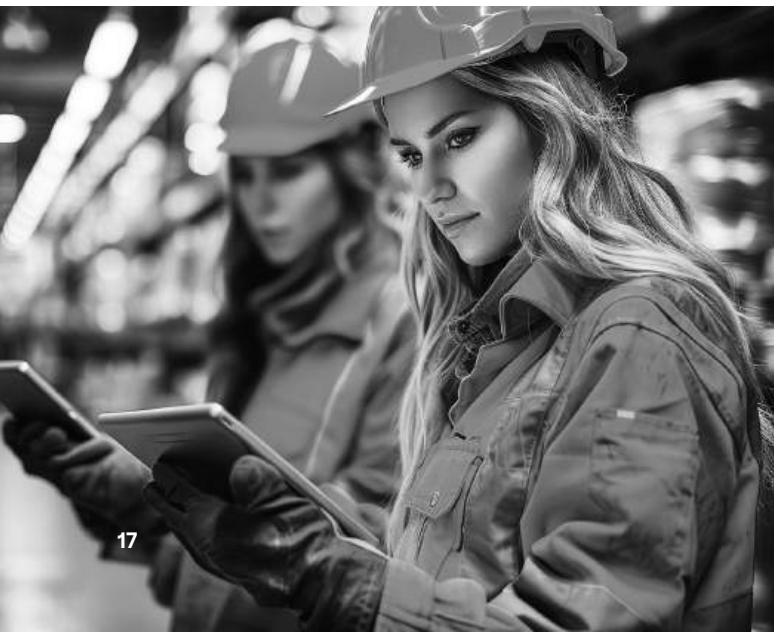
fabricantes", añade Turedi. "Además de eso, se empieza a percibir un gran incremento de lo que llamamos 'aprovechamiento de recursos existentes'".

Este término hace referencia al uso de herramientas ilegítimas ya instaladas en un ordenador para realizar actividades maliciosas.

"Este tipo de casos aumentan año tras año de forma constante, y ahora es lo que predomina".

Los ataques que aprovechan los recursos se han convertido en una de las principales preocupaciones para las agencias de seguridad a ambas orillas del Atlántico en los últimos meses. En febrero de 2024, el NCSC del Reino Unido y la alianza Five Eyes alertaron a los operadores de infraestructuras críticas sobre estas técnicas.

En particular, Five Eyes advirtió que, según se ha observado, hay ciberdelincuentes patrocinados por China y Rusia que han aplicado esta técnica en redes de infraestructuras críticas comprometidas.



Promover la colaboración para abordar la contaminación cruzada

Dado el riesgo cada vez mayor de que las amenazas de TO se propaguen a la TI, y viceversa, las organizaciones deben mejorar la colaboración para evitar la contaminación cruzada, afirma Turedi.

Las mejores prácticas y los procesos del ámbito de TO de la empresa deben compartirse con el departamento de TI, añade. Asimismo, algunas de las prácticas recomendadas de TI podrían ser beneficiosas para los equipos de TO. Esto, añade, "ofrece una excelente oportunidad para reforzar estas organizaciones".

"No cabe duda de que el ámbito del IoT y el de TI son independientes", afirma. "Muchas organizaciones de fabricación intentan cohesionar el trabajo de ambos equipos, en lugar de que operen totalmente por separado, especialmente en lo que respecta a la ciberseguridad".

"Además, eso brinda una excelente oportunidad para compartir inteligencia y conocimientos. No obstante, aunque la TO se ejecute en un dispositivo que parece un ordenador, debemos recordar que la forma en que se fabrica, se mantiene y se gestiona es muy diferente".

Consideraciones normativas y estándares de la industria

Los fabricantes ya se adhieren a numerosos estándares de la industria, como el conjunto de estándares ISA/IEC 62443. Estos describen los requisitos y procesos para mantener sistemas de control y automatización industrial (IACS) seguros, y se considera que son las prácticas recomendadas para mejorar la seguridad.

La existencia de más marcos normativos internacionales pone de manifiesto que los fabricantes se juegan más que nunca en lo que respecta a la seguridad. Las directrices normativas a ambas orillas del Atlántico imponen requisitos estrictos a los fabricantes para garantizar prácticas de seguridad sólidas.

Un ejemplo de ello es la Ley de Ciberresiliencia (CRA) de la UE. El incumplimiento de la CRA puede conllevar grandes multas de hasta 15 millones de euros (16,76 millones de dólares), o el 2,5 % del volumen de ventas mundiales.

Dada la función esencial de la industria de la fabricación, la Directiva relativa a la resiliencia de las entidades críticas (REC) de la UE también es un marco legislativo clave para los líderes de TI de este ámbito.

Dicha directiva pretende reforzar la resiliencia de las entidades de infraestructuras críticas frente a amenazas emergentes, tanto físicas como virtuales, incluidos el sabotaje, las amenazas internas y los desastres naturales. La REC entró en vigor en enero de 2023, y los Estados miembro tienen hasta el 17 de octubre de 2024 para promulgar nuevas leyes que les permitieran adaptarse a ella.

Quizás uno de los reglamentos de la UE más esenciales para los fabricantes sea la Directiva SRI 2.

Se trata de una revisión de la Directiva sobre sistemas y redes de información (SRI) de la UE, y tiene como objetivo endurecer los requisitos y estándares de ciberseguridad en un conjunto de sectores, incluido el de la fabricación.

En virtud la Directiva SRI 2, el sector de la fabricación se designa como "entidad importante" por su proximidad a la infraestructura crítica. Esto requerirá que los operadores del sector presten más atención a la seguridad de la cadena de suministro y que colaboren más con los proveedores de TI para promover mejoras de seguridad proactivas en el hardware y el software.

La actualización de la Directiva SRI 2 es solo uno de los diversos marcos regulatorios que los fabricantes deben tener en cuenta y cuyo cumplimiento plantea quebraderos de cabeza a las organizaciones, según señala el FEM.

"La descentralización de los entornos operativos y la fragmentación y diversidad de los panoramas regulatorios local, regional y sectorial añaden complejidad a los esfuerzos por garantizar la ciberseguridad", afirma el FEM en el informe *Building a Culture of Cyber Resilience in Manufacturing* ("Forjar una cultura de ciberresiliencia en el sector de la fabricación").

> **"La descentralización de los entornos operativos y la fragmentación y diversidad de los panoramas regulatorios local, regional y sectorial añaden complejidad a los esfuerzos por garantizar la ciberseguridad".**
>
> Informe "Building a Culture of Cyber Resilience in Manufacturing" ("Forjar una cultura de ciberresiliencia en el sector de la fabricación") del FEM

A pesar de estos desafíos, Turedi cree que la Directiva SRI 2 resultará positiva para el sector en última instancia, y señala que representa "toda una renovación en términos de regulación y cumplimiento en materia de ciberseguridad".

"Creo que la Directiva SIR 2 es fantástica. En primer lugar, si una organización se toma en serio la ciberseguridad, esta directiva no le causará ninguna molestia", afirma. "Favorece que las organizaciones tomen conciencia, si aún no lo han hecho, de que la ciberseguridad es importante para su negocio".

El cumplimiento de los reglamentos estadounidenses también será una prioridad para los líderes de TI del sector de la fabricación en adelante. En febrero de 2024, el Instituto Nacional de Normas y Tecnología (NIST) del gobierno de EE. UU. presentó una importante revisión de su Marco de Ciberseguridad (CSF).

El CSF 2.0 proporcionará a los fabricantes un marco voluntario concebido para ayudarles a mejorar sus capacidades de ciberseguridad.

Abordar las amenazas futuras con la IA

Para hacer frente a una variedad de amenazas nuevas y cada vez más sofisticadas, se necesitan herramientas igualmente potentes que respalden la labor de los profesionales de la ciberseguridad. Como ya se ha dicho, la IA generativa ofrece a los fabricantes una excelente oportunidad para incorporar capacidades líderes en la industria.

Desde que esta tecnología hizo su aparición a finales de 2022 con el lanzamiento de ChatGPT de OpenAI, se han identificado varios casos de uso notables en la empresa. Uno de los más populares y generalizados es el software diseñado para mejorar la productividad de los trabajadores.

En el ámbito de la ciberseguridad los miembros del personal de primera línea está disfrutando de las mismas ventajas gracias a herramientas nuevas y potentes que alivian la carga de tareas cotidianas.

Turedi considera que la IA generativa representa una "excelente oportunidad" para los equipos de seguridad, no solo por dotarlos de herramientas para hacer frente a las amenazas, sino también porque les ayuda a crear una estrategia de ciberseguridad mejor coordinada y que incluya a toda la empresa.

En pocas palabras, la IA puede solventar las carencias de las respectivas funciones, algo que resulta vital para los fabricantes teniendo en cuenta los problemas de coordinación entre la TO y la TI que se arrastran desde hace tiempo.

> **"Considero que la IA presenta una excelente oportunidad para mejorar la cohesión de esos equipos y la automatización de los flujos de trabajo".**
>
> Zeki Turedi, CTO de CrowdStrike para EMEA

"Considero que la IA presenta una excelente oportunidad para mejorar la cohesión de esos equipos y la automatización de los flujos de trabajo", afirma.

"Por ejemplo, no debemos olvidar que la IA y la ciberseguridad pueden resultar muy útiles si tenemos a un miembro del equipo de TO que, aunque conoce el entorno de TO y sus matices muy bien, no es un experto en ciberseguridad".

"La IA generativa nos permite integrar los conocimientos de ciberseguridad en otros equipos que tal vez no trabajan con ella todos los días. Posteriormente, esta tecnología puede proporcionar recomendaciones sobre qué hacer a continuación o presentar información adicional que permita a dichos equipos tomar buenas decisiones sobre fases y pasos posteriores como parte del ciclo de respuesta".

Turedi señala que, aunque las ventajas de la IA más destacadas tienen que ver con la productividad y las finanzas, usarla para mejorar las habilidades del personal y ofrecerle "formación pasiva" es lo que genera valor a largo plazo.

Aciertos del sector de la fabricación en materia de ciberseguridad

Turedi afirma que es vital centrarse en los posibles peligros a los que se enfrenta la industria de la fabricación. Sin embargo, reconocer lo que la industria hace bien es igualmente importante desde el punto de vista moral y de liderazgo.

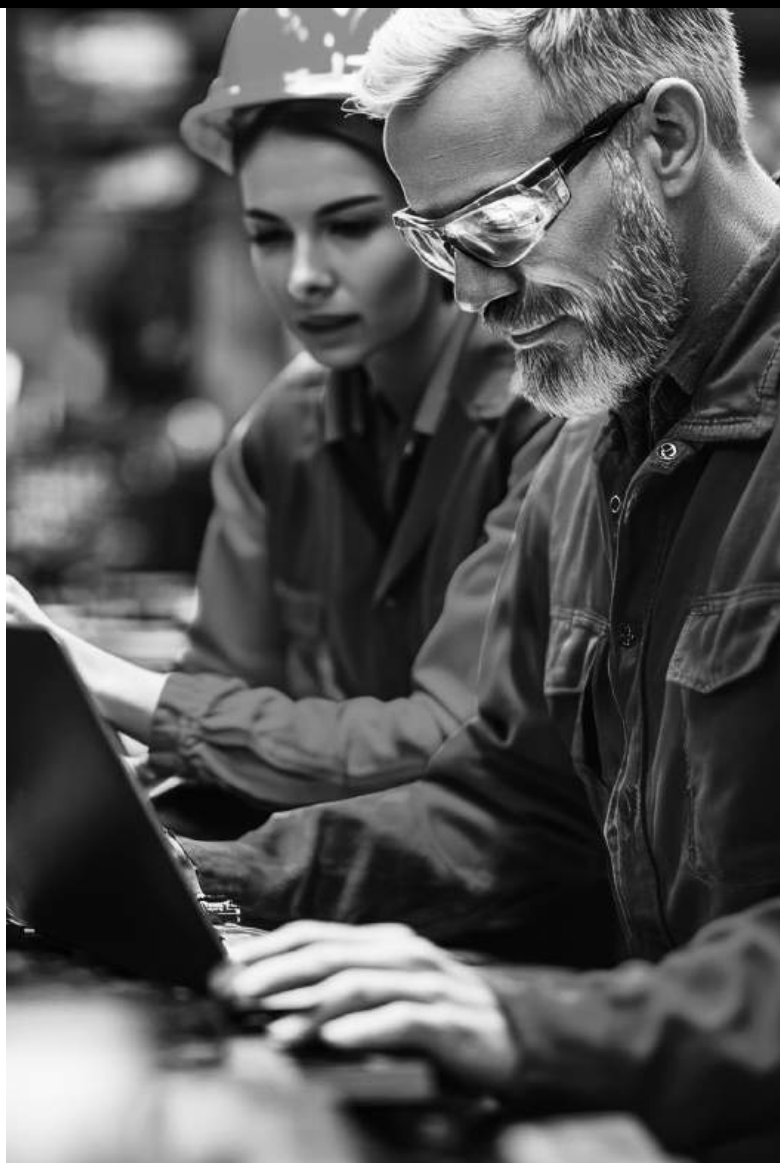
Considera que existen áreas clave en las que el sector de la fabricación sobresale, sobre todo con respecto a la transparencia, la comunicación de incidentes y su afán por aprender de los errores y participar en el intercambio de conocimientos con sus homólogos.

"Desafortunadamente, en los últimos años diversas organizaciones de fabricación han sido víctimas de ataques", apunta Turedi. "Y, una vez más, han publicado información sobre sus pérdidas".

Turedi considera que debemos aplaudir esta cultura de comunicación proactiva, ya que es lo que distingue a esta industria de las demás. Añade que las organizaciones de otros sectores suelen ser reticentes a revelar demasiados detalles tras sufrir un ciberataque.

No obstante, esto no ayuda mucho a sus compañeros de sector, e incluso tiene un efecto perjudicial sobre su capacidad para combatir amenazas futuras. En el panorama de amenazas moderno, intercambiar información es de vital importancia.

"Estos datos son muy valiosos y permiten a otras organizaciones de fabricación acceder a esa información y les ayuda a invertir en ciberseguridad de forma adecuada, además de proporcionar los datos adecuados para calcular el retorno de la inversión, mostrar el desastre que podría producirse y usar esas pruebas para que se invierta en ciberseguridad", explica.



"Esta situación es bastante excepcional, porque en otros sectores hay organizaciones que no comunican este tipo de información o que ocultan las vulneraciones de seguridad en lugar de hacerlas públicas".

"Para un sector que ha sido el blanco de ataques puede resultar muy difícil crear conciencia y transmitir correctamente [la importancia de invertir en ciberseguridad] a los jefes, los equipos y la junta directiva".

Entrevista: la función vital de la seguridad en la fabricación

Zeki Turedi, CTO de CrowdStrike para EMEA, explica la función de la IA y la Directiva SIR 2 en la protección de los fabricantes frente a los ciberataques

¿Cuáles son los mayores desafíos de ciberseguridad a los que se enfrentan las empresas en general en estos momentos?

Hay muchos. Desde el punto de vista técnico, los ataques a la nube se están disparando. Muchas organizaciones se apresuraron a migrar sus antiguos sistemas locales a la nube; pero, en muchos casos, la seguridad no se tuvo en cuenta como parte de ese proceso, sino que se pensó en ella después. La nube es fantástica y puede ser excelente en lo relativo a la seguridad, pero conllevará vulnerabilidades si no está integrada en el proceso.

Los atacantes también evolucionan: se han vuelto más sofisticados y muy pertinaces, e invierten grandes sumas en nuevas formas de atacar a las organizaciones. Por ejemplo, la identidad es una de las principales amenazas a las que se enfrentan las organizaciones.

Los atacantes pueden conseguir las credenciales mediante ingeniería social o buscarlas en la dark web, y usarlas para hacerse pasar por usuarios legítimos y acceder a la organización. Desafortunadamente, las organizaciones pueden caer en esa trampa de muchas formas y los atacantes se han vuelto mucho más rápidos.

El sector de la fabricación, ¿se enfrenta a desafíos únicos en lo que respecta al IoT y la TO, por ejemplo?

Sí. Esto se debe a la compleja función que desempeñan tanto el IoT como la TO en la arquitectura tecnológica, lo que también se refleja en el panorama de amenazas.

Además de eso, los fabricantes tienen que gestionar un entorno muy complejo. En algunos casos, dirigen sus propias fábricas, algunas de las cuales son nuevas y otras

son antiguas. También pueden ser alquiladas, con lo que el equipo podría ser propio o ajeno. Este panorama de seguridad es muy complicado a la hora de proteger una red. Además, quizás la fábrica deba estar interconectada con una organización cuya seguridad sea inferior, pero que tenga una herramienta específica que permita fabricar productos muy rápido. Estas cuestiones conllevan enormes riesgos para el sector de la fabricación.

¿Es este un problema mundial o hay ciertas regiones en las que el riesgo sea mayor?

Sin duda, las empresas de Europa y Norteamérica son el blanco de un volumen de ataques directos mucho mayor. No obstante, para ser sincero, los atacantes persiguen a todo el mundo.

Recordemos que, aunque tendemos a centrarnos en los atacantes que más estragos causan o en los secuestros de mayor envergadura, hay atacantes de todo tipo. Es decir, los hay que atacan a organizaciones pequeñas, a empresas de países concretos, etc.

La Directiva SIR 2, la normativa más reciente de la UE en materia de ciberseguridad, entra en vigor en octubre de 2024. ¿Cómo afectará a las empresas?

Si una organización se toma en serio la ciberseguridad y hace todo lo posible en este ámbito, la Directiva SIR 2 no le causará ninguna molestia. Creo que es muy importante entender que afectará a las empresas que no inviertan en ciberseguridad.

Ayudará a muchas organizaciones a tomar conciencia de que la ciberseguridad es vital para las empresas. Si esta todavía no se ha implementado y aún no se toma en serio, esta normativa será un motivo excelente para empezar a hacerlo.

Si una empresa ya cuenta con un programa de ciberseguridad, significa que es importante para ella y se la toma en serio. Si has nombrado a un CISO, informas a la junta directiva acerca de los eventos e incidentes y cuentas con un partner de seguridad como CrowdStrike, te encontrarás en la posición ideal para cumplir la Directiva SIR 2.

¿Cómo está influyendo la IA generativa en el panorama de ciberseguridad desde el punto de vista tanto ofensivo como defensivo?

Recordemos que la industria de la ciberseguridad lleva ya entre 10 y 15 años usando la IA. La IA es fantástica para identificar actividades maliciosas y malware a gran escala, por lo que muchas organizaciones de seguridad, como CrowdStrike, han basado sus plataformas en ella. Llevamos usándola mucho más tiempo que el adversario. Creo que la IA generativa abre vías completamente nuevas. Por ejemplo, podemos usarla para respaldar el trabajo de los analistas, ayudarles a automatizar tantas tareas como sea posible y simplificar la interacción con la tecnología al máximo. Puede incluso ayudarnos con la formación complementaria y multidisciplinar, así como a, simplemente, aguantar el ritmo de la gran cantidad de inteligencia que las organizaciones ven hoy en día.

Por otro lado, si a nosotros nos interesa esto tanto, a los atacantes también. Sabemos que quieren superarse y están invirtiendo en sus objetivos. De hecho, hemos leído conversaciones en foros de hackers sobre cómo usar la IA.

Recordemos que la tecnología de la que dispone quien defiende posiblemente también esté disponible para quien ataca. La IA generativa se puede utilizar para crear scripts fantásticos para un organismo de respuesta a incidentes, pero también se puede aplicar a la creación de un script que sirva para que un ciberdelincuente extraiga información confidencial rápidamente. Por lo tanto, debemos conocer los usos maliciosos que se pueden hacer de estas herramientas y tratar de protegernos contra los ataques.

¿Cómo afectaría a los equipos de seguridad que las organizaciones aplicaran más la IA a la ciberseguridad?

Creo firmemente que las herramientas de IA están aquí como complemento, no como reemplazo. Recordemos que las herramientas de IA son fantásticas, pero requieren entrenamiento. Hay que enseñarles la diferencia entre el bien y el mal, entre lo que es un incidente real y el ruido. No podemos prescindir de la intervención humana. Habrá mucha información importante sobre las empresas que no se podrá utilizar para entrenar la IA generativa, como conocimientos muy importantes que intercambian las personas, pero que no está documentado correctamente. Esa información es necesaria y es lo que necesitamos para abordar un incidente real rápidamente.

Si hemos visto un incidente antes, conocemos el proceso de investigación, y eso es algo que termina repitiéndose con frecuencia y se convertirá en un trabajo monótono para el que no necesitamos un analista. Queremos que estos se centren en lo que mejor saben hacer, en los matices, y que realicen aportaciones realmente únicas. Dejemos que la tecnología se ocupe del ruido y quite ese nivel de carga de los hombros del analista.

> **"Las herramientas de IA son fantásticas, pero requieren entrenamiento. Hay que enseñarles la diferencia entre el bien y el mal, entre lo que es un incidente real y el ruido. No podemos prescindir de la intervención humana".**
>
> Zeki Turedi, CTO de CrowdStrike para EMEA

Lo que más me preocupa cuando se empieza a pensar en reemplazar a los seres humanos en contextos de seguridad es que corremos el riesgo de pasar por alto cosas importantes o de clasificarlas mal. Y en el ámbito de la ciberseguridad no podemos permitirnos ese lujo.

¿Qué consejo daría a los profesionales de TI del sector de la fabricación que desean mejorar o reforzar su seguridad mediante la IA?

Por ejemplo, aunque se encuentren en el Reino Unido y no tengan que cumplir la Directiva SIR 2, sería muy buena idea que la consultaran de todas formas. Se trata de una referencia importante a la que todos los fabricantes deberían prestar atención. Además, también es un marco excelente para desarrollar una buena estrategia de seguridad empresarial.