STORMSHIELD

ARTÍCULOS DE OPINIÓN

INDUSTRIA 5.0: ¿DÓNDE ENCAJA LA CIBERSEGURIDAD?

Khobeib Ben Boubaker
Head of Industrial Security Business Line, Stormshield

Mientras que la Industria 4.0 se centraba en mejorar la productividad a través de Big Data, tecnologías IoT y máquinas inteligentes, la Industria 5.0 promete ser humana, sostenible, resiliente, con un enfoque renovado en las personas y la sociedad. Entonces, ¿cómo encaja la ciberseguridad en este panorama?

Diez años después de la introducción del término oficial «Industria 4.0», ha llegado el momento de una nueva revolución industrial con la Industria 5.0. Su objetivo es volver a **situar a las personas en el centro de los procesos industriales, ahora digitalizados en su inmensa mayoría**. Pero la interacción entre el ser humano y la máquina exige la aplicación de fuertes medidas de seguridad en los entornos industriales. ¿Dónde encaja entonces la ciberseguridad? ¿Y en qué plazos? Le explicamos más.

LAS PROMESAS DE LA INDUSTRIA 5.0

La idea de que las máquinas y las tecnologías acabarán por eliminar a las personas en las fábricas y en el corazón de los procesos industriales es una visión de la industria que ya no se sostiene. Centrada en el aumento de la productividad, la Industria 4.0 pretendía que las fábricas fueran «inteligentes», controlando y supervisando la producción a distancia.

¿Qué es la Industria 5.0? El nuevo paradigma de la Industria 5.0 pretende volver a centrarse en las personas. «*La primera prioridad es mejorar las condiciones cotidianas de los trabajadores con nuevas soluciones técnicas y máquinas robotizadas de alto rendimiento*», explica **Vincent Nicaise**, responsable de asociaciones industriales y ecosistema de Stormshield. A continuación, hace hincapié en otra cuestión:«*Recuperar la imagen de la actividad industrial en un momento de la historia propicio al tema de la reindustrialización en Europa. Se trata también de aumentar el atractivo de un sector que sufre desde hace varios años atrayendo a los trabajadores del mañana, así como el conocimiento de ingeniería*». **El mantra de la Industria 5.0: beneficiar a los trabajadores, las empresas y el planeta**. Esto implica «*utilizar las nuevas tecnologías para garantizar la prosperidad en términos de empleo y crecimiento, pero también (y, sobre todo) teniendo en cuenta los límites de producción del planeta*», subraya **Stéphane Potier**, responsable de ciberseguridad IoT y OT en Advens. En este sentido, este nuevo paradigma industrial es el polo opuesto a la amenaza de una fábrica 100% automatizada que destruya puestos de trabajo. El robot no se ve como un ente autónomo, ni sustituye la pericia humana. «*Los robots colaboran, liberando a los operarios de tareas tediosas*», prosigue. El objetivo principal de la máquina es ayudar a los operarios en sus tareas proporcionándoles nuevas capacidades funcionales mediante la inclusión de inteligencia artificial, realidad aumentada, robótica e IoT. Firmemente centrada en un enfoque de producción sostenible que tenga en cuenta el imperativo climático, la Industria 5.0 incorpora nuevos criterios como la eficiencia energética de las tecnologías, la priorización de las energías renovables y un enfoque de autosuficiencia. La energía es una cuestión clave para los agentes de la Industria 5.0. Deben tener en cuenta el consumo energético no sólo de las máquinas, sino también del sistema de producción en general. «La cuestión de las tierras raras, presentes en muchos componentes y máquinas industriales, se está convirtiendo en un tema crucial», afirma Stéphane. «*Por ejemplo, los motores actuales utilizan muchos menos recursos de tierras raras y se fabrican con materiales más fáciles de conseguir*».

El factor resiliencia también es fundamental para la Industria 5.0, que se adapta a un entorno macroeconómico y geopolítico que demuestra constantemente la necesidad de poder adaptarse a cambios repentinos. **Marc Bagur**, responsable de Human-Machine Performance en Airudit, cree que esto representa una enorme oportunidad estratégica para el sector manufacturero. «*Quienes optan por centrarse en los valores humanos, en lugar de en la tecnología, están adoptando un enfoque general y un modelo estructural que rinde mejor a largo plazo*». Ya no se trata simplemente de digitalizar el entorno

industrial a toda costa, sino de aspirar a una«*robustez sistémica que sea social, humana y ecológicamente aceptable*». Señala a continuación que esta exigencia «*coincide perfectamente con las de las nuevas generaciones de ingenieros y trabajadores para quienes la adecuación a los valores ecológicos, la cuestión de los recursos energéticos y la estabilidad social son hoy cuestiones cruciales*».

Sin embargo, como los niveles de madurez de los distintos sistemas industriales varían, sigue siendo difícil evaluar con precisión cuándo será realmente operativo este nuevo paradigma. Y la Industria 4.0 es aun relativamente nueva...

INDUSTRIA 4.0 VERSUS INDUSTRIA 5.0: ¿SUSTITUCIÓN O COMPLEMENTARIEDAD?

La Industria 5.0 no es una iteración más en la marcha forzada hacia el progreso. **Este nuevo paradigma debe considerarse un complemento del paradigma de la Industria 4.0 y pretende situar la cuestión de la innovación tecnológica en un marco específico, centrado en el triángulo ser humano-sostenibilidad-resiliencia.** Para lograrlo, la Industria 5.0 se basa en la eficacia de las tecnologías de la Industria 4.0; por ejemplo, para resolver problemas vinculados a criterios de sostenibilidad. «*Para reducir el consumo de energía de una máquina, ya sea nueva o antigua, primero hay que poder medir su consumo. La Industria 4.0 nos proporciona las herramientas para hacerlo, mediante sensores, contadores y sistemas IoT*», subraya Stéphane.«*Además, podemos intentar mejorar el funcionamiento de una máquina que consume demasiada energía. En primer lugar, con mantenimiento predictivo para influir en la vida útil de la máquina, y, en segundo lugar, con inteligencia artificial para reducir el consumo*» En su informe «Industria 5.0 - Hacia una industria europea sostenible, centrada en las personas y resistente», la Comisión Europea hace hincapié en esta sinergia. **También tenemos que abordar los puntos débiles de la Industria 4.0, que hasta ahora se ha desarrollado de una manera demasiado alejada de las cuestiones sociales.** El objetivo es crear fabricantes que no solo sean productivos y eficientes, sino también capaces de inspirar confianza a través de valores que reflejen los tiempos actuales y los retos que plantean las nuevas generaciones.

¿Cómo podemos utilizar estas directrices estratégicas para **prepararnos para la industria del mañana?** La actual Fábrica 4.0 está fuertemente digitalizada, con Big Data para la gestión de datos, IoT para mediciones precisas, 5G para la conexión en red de los centros industriales y computación en el borde para desplegar una mayor capacidad informática a nivel de máquina. Sin embargo, también debe tener en cuenta un contexto macroeconómico y geopolítico especialmente complejo, marcado por el aumento de los precios de la energía y la urgencia de los problemas medioambientales. **Preparar una respuesta industrial a estos retos a escala de la civilización requiere, por tanto, no sólo orientar las inversiones adecuadas en los lugares adecuados, sino también revisar los procesos en cada etapa de la cadena de producción.** Vincent considera que esta modernización de las instalaciones industriales requiere tanto «*nuevos conocimientos vinculados a protocolos y procesos técnicamente innovadores, como nuevas competencias para los trabajadores – que son los actores clave de la*

cadena de producción». Como la Industria 5.0 introduce una nueva capa de información, crea nuevas necesidades, y esto tiene un impacto directo en la cuestión de la formación del personal. «*Podemos optar por crear nuevos puestos, como representantes locales encargados de aplicar los nuevos protocolos de seguridad en las máquinas de plantas repartidas por todo el mundo, u optar por aumentar las competencias de los operarios*», explica.

¿Es ésta una oportunidad para dar por fin a la ciberseguridad un papel central en la industria?

¿QUÉ PAPEL DEBERÍA JUGAR LA CIBERSEGURIDAD EN LA INDUSTRIA 5.0?

En el Foro Internacional de la Ciberseguridad 2022, la cuestión de la ciberseguridad en entornos industriales estuvo en boca de todos. **Esto se debe a que la fábrica conectada tiene una superficie de ataque muy ampliada y, por tanto, problemas de seguridad igualmente ampliados**. La combinación de un número creciente de máquinas robotizadas, una interconexión cada vez mayor, la integración de IoT, una dosis de realidad aumentada y nuevas interfaces hombre-máquina significa que el número de posibles fallos de seguridad en los sistemas va en aumento.

Un informe de Claroty afirma que 82 fabricantes industriales sufrieron ataques solo en 2021. En el mismo año, el número de vulnerabilidades detectadas aumentó bruscamente de 637 a 787. Todos ellos son puntos de entrada críticos... A menudo citados como ejemplo, los sistemas operativos obsoletos que se ejecutan en los equipos de las fábricas se encuentran entre las causas más frecuentes de vulnerabilidad en términos de ciberseguridad industrial. El viejo clásico Windows XP sigue siendo un sistema esencial para ciertos entornos industriales, y requiere herramientas de ciberseguridad especiales para reducir el riesgo. Las consecuencias de un ciberataque en un entorno operativo tienen un impacto masivo, desde la paralización total de las líneas de producción hasta la puesta en peligro real de los trabajadores – por no hablar del importante impacto en la reputación de las empresas afectadas. Por no hablar de los riesgos medioambientales, a los que la Industria 5.0 es especialmente sensible.

Así que la pregunta es: **¿qué soluciones de ciberseguridad deben utilizarse para proteger los entornos industriales del mañana?** Se están estudiando dos escenarios para abordar el reto de la Seguridad Industrial 5.0. El primero es un escenario de «renovación» en el que la cadena de producción se actualiza integrando la cuestión de la ciberseguridad en los propios equipos. En este primer escenario, la instalación de «*componentes de tipo cortafuegos es una buena manera de segmentar los flujos y analizar los protocolos*», afirma Vincent Nicaise, al igual que "*una protección más estricta de las estaciones de trabajo, apoyada con una gestión exhaustiva de los puertos USB, las redes Wi-Fi y los accesos*". Por encima de todo, elegir soluciones de ciberseguridad soberanas es en este caso una forma de garantizar la transparencia y evitar cualquier riesgo de que los datos puedan ser explotados con fines malintencionados. El objetivo en este caso es tener acceso a información soberana bien

controlada, mitigando así los riesgos de compromiso y ataques por parte de entidades extranjeras. Es la única manera de garantizar una defensa en profundidad sin eslabones débiles. El segundo escenario de la Industria 5.0 se refiere a los dispositivos más recientes que incorporan la ciberseguridad como característica nativa. Pero para lograrlo, el aspecto humano y un enfoque colaborativo serán clave; mucho más que una mera concienciación, exige la implantación de sistemas de colaboración significativos entre los equipos humanos de todos los nuevos proyectos. Esto abarca, por un lado, las necesidades de seguridad de los equipos humanos cibernéticos y, por otro, las limitaciones operativas de los departamentos de informática. Se necesita un enfoque conjunto para comparar puntos de vista y alcanzar compromisos que satisfagan tanto las limitaciones cibernéticas como las OT.

Esto supone, por supuesto, que los fabricantes estén preparados para una Industria 5.0 cibersegura de este tipo.

LA INDUSTRIA DEL MAÑANA Y LA CIBERSEGURIDAD: ¿ESTÁN PREPARADOS LOS FABRICANTES?

Según un estudio realizado en abril de 2023 por Wavestone, la madurez cibernética de las grandes organizaciones en Francia sigue siendo baja: sólo el 49% de los encuestados se consideran maduros. Esta media es similar **solo en el sector industrial, con un 49,4% de los encuestados que se declaran maduros en materia de ciberseguridad**. Y aunque el sector industrial sube 4,6 puntos respecto al año pasado, la seguridad de los sistemas industriales es una de las asignaturas pendientes que las grandes empresas se esfuerzan por abordar (junto con la gestión de terceros y la seguridad en la nube).

En un intento por exigir a estas organizaciones que adopten normas de ciberseguridad, pronto se aplicarán leyes y reglamentos europeos, como la directiva NIS2 para la gestión de subcontratistas en entornos sensibles y la Ley de Ciber Resiliencia para el fortalecimiento de los productos digitales conectados. En opinión de Vincent Nicaise, estas leyes ayudarán a los profesionales a adoptar una serie de medidas prácticas de seguridad: «*Una vez que la Ley de Ciber Resiliencia se aplique a escala europea, los fabricantes estarán obligados – por ejemplo – a incorporar elementos de seguridad en sus equipos*». Al mismo tiempo, normas como MITRE ATT&CK o NIST también pueden contribuir a aumentar la madurez de los fabricantes en materia de ciberseguridad. Independientemente del medio utilizado, un diagnóstico técnico completo y exhaustivo debería permitir a los fabricantes aumentar rápidamente su resiliencia frente a los ataques en el avance hacia la Industria 5.0.

«Una persona consciente vale el doble. Y esto, creo, es un punto que enlaza con los principios de la Industria 5.0, que marca la colaboración entre el ser humano y la máquina.»

Stéphane Potier, responsable de ciberseguridad IoT y OT, Advens

En términos operativos, esta capacidad puede adoptar la forma de la segmentación de redes y entornos de producción, el uso de cifrado para los flujos de datos sensibles, la implantación de sistemas de autenticación fuertes y la supervisión continua de las infraestructuras sensibles. Por lo tanto, **es absolutamente crucial concienciar y formar al personal sobre cómo detectar los ciberataques**. «*Los operadores están familiarizados con sus máquinas y saben perfectamente cómo reaccionan normalmente sus herramientas*», insiste Stéphane Potier. «*Si se les sensibiliza sobre el tema de la ciberseguridad explicándoles los distintos tipos de ataques y las posibles repercusiones en su entorno de trabajo, se les mantiene alerta. Así, los operadores podrán detectar muy rápidamente una situación anómala e informar a sus CISO*». Señala, sin embargo, que la concienciación en el entorno OT no está tan implementada como en el entorno TI. «*Contrariamente al adagio popular de ciberseguridad de que la principal vulnerabilidad se encuentra entre la silla y el teclado, creo que la solución se encuentra entre la silla y el teclado*», señala. Y prosigue:«*Una persona consciente vale el doble. Y esto, creo, es un punto que enlaza con los principios de la Industria 5.0, que marca la colaboración entre el ser humano y la máquina*».

Por tanto, para ser eficaz, la Industria 5.0 deberá combinar sus principios cardinales – las personas, la sostenibilidad y la resiliencia – con una mayor concienciación en materia de ciberseguridad, junto con la integración de dispositivos robustos en el corazón de sus sistemas. En otras palabras, la ciberseguridad tendrá que ser parte integrante de este nuevo paradigma industrial para todas las empresas que deseen acelerar en esta dirección.