Hablemos de la ciberseguridad industrial

Ana Ayerbe | Directora del Área de Negocio TRUSTECH de Tecnalia | @AnaAyerbe

Tema

Las industrias españolas deben tomarse en serio la ciberseguridad para no verse afectadas por ciberataques, pero también para aprovechar las oportunidades del emergente mercado global de ciberseguridad.

Resumen

La ciberseguridad tiene una doble dimensión industrial: por un lado, las industrias y sus productos corren el riesgo de verse afectados por ciberataques y, por otro, la necesidad de protegerse está desarrollando un emergente mercado de ciberseguridad del que debe aprovecharse la industria española. La transformación digital en marcha, dentro de Industria Conectada 4.0, y el incremento de la conectividad aumentan la exposición industrial a los riesgos cíber, económicos y de reputación que se describen en este ARI. A la reivindicación de hacer frente a los retos de ciberseguridad industrial se une el llamamiento a aprovechar el crecimiento del mercado de la ciberseguridad para desarrollar las capacidades tecnológicas e industriales que se pueda en beneficio del sector industrial español.

Análisis

Actualmente, el peso de la industria española en el PIB es del 16,3 % y el estudio de la CEOE “La industria, motor de crecimiento: análisis y recomendaciones” destaca su efecto arrastre sobre otros sectores de la economía, dado que un incremento de 1 € en la demanda final del sector industrial genera un incremento de 3,11 € en el valor de la producción del conjunto de la economía. Por otro lado, si tenemos en cuenta que el 40 % de las empresas que innovan pertenecen al sector industrial y que éste realiza unos gastos en innovación del 47,5 % de los gastos en I+D (datos de 2015), el sector industrial es clave para el desarrollo de la actividad innovadora, la inversión en I+D, el crecimiento del empleo y el desarrollo económico español en su conjunto.

Las empresas industriales necesitan crecer, expandirse y beneficiarse de la transformación digital en lo que conocemos como la industria 4.0, la internet industrial o la Industria Conectada 4.0. En estos casos, hablamos de digitalización, de conectar máquinas, sistemas, empresas, de recoger cantidades ingentes de datos que permitan tomar decisiones de la forma más precisa y en el menor tiempo con el objetivo final de crear productos nuevos y mejores e incrementar la productividad generando en la empresa un diferencial que le permita ser más competitiva en el contexto global.

Las ventajas de la digitalización y la conectividad son enormes, pero, al mismo tiempo, han aumentado la superficie de exposición de las empresas a ciberataques, y las consecuencias de un ciberataque pueden ir desde el secuestro de datos para pedir un rescate, el robo de IPR, la parada de máquinas o el mal funcionamiento de las mismas hasta una modificación de valores prefijados (*setpoints*) que haga que el producto fabricado no salga con la calidad prevista o que se tomen decisiones equivocadas debido a la manipulación de los datos. Sus consecuencias pueden ser económicas, pero pueden llegar a producirse daños medioambientales o incluso provocar lesiones de diferente consideración a las personas, por no mencionar la proyección de una mala imagen de la empresa.

En este sentido, la iniciativa Industria Conectada 4.0 del Ministerio de Industria, Comercio y Turismo del Gobierno de España sitúa la ciberseguridad entre los habilitadores digitales de la industria 4.0 (Figura 1). La ciberseguridad, como habilitador tecnológico, se debe considerar en cualquier proyecto de Industria Conectada 4.0 desde el mismo momento de la conceptualización del proyecto. Esto permitirá crear una industria resiliente a ciberataques al utilizar tecnología y sistemas que han considerado la ciberseguridad desde el diseño.

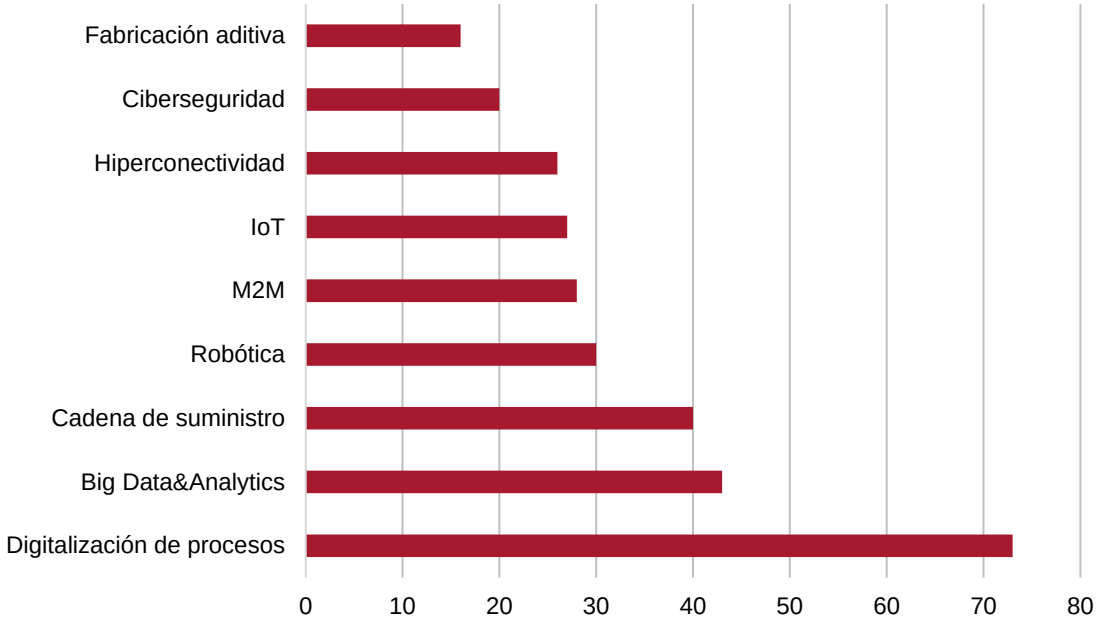
Figura 1. Habilitadores digitales de la Industria Conectada 4.0

Fuente: Habilitadores Digitales, Ministerio de Industria, Comercio y Turismo, http://www.industriaconectada40.gob.es/Paginas/index.aspx#habilitadores.

Actualmente estamos lejos de esta situación y, aunque se están haciendo esfuerzos considerables en el ámbito industrial, muchas empresas empiezan a preocuparse por la ciberseguridad únicamente en el momento en el que empiezan a observar las consecuencias de un ciberataque. Según el informe “Perspectivas del sector industrial”, realizado por KPMG en mayo de 2018, entre las prioridades empresariales en la transformación digital hacia la industria 4.0 (Figura 2) aparece la ciberseguridad con un 20 % y al mismo nivel que el resto de las prioridades, sin tener en cuenta que, si se implementan la hiperconectividad, *Big Data*, *analytics*, digitalización de procesos y, en

definitiva, cualquiera del resto de las prioridades sin considerar la ciberseguridad, estaremos aumentando la superficie de exposición de nuestras industrias a los ciberataques. Esto debe alertarnos porque en las empresas se ve la ciberseguridad como algo independiente de la incorporación de nuevas tecnologías relativas a la Industria Conectada 4.0.

Figura 2. Prioridades empresariales en la transformación digital hacia la industria 4.0



Fuente: Elaboración propia con datos de "Perspectivas del sector industria", KPMG, mayo de 2018, p. 6, https://assets.kpmg/content/dam/kpmg/es/pdf/2018/05/Perspectivas_Industria-2018.pdf.

La ciberseguridad en el entorno industrial

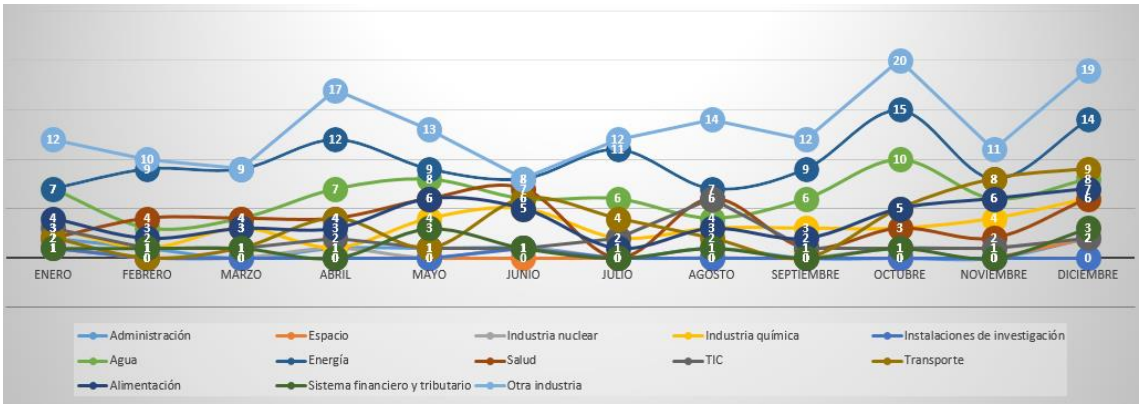
Profundicemos en la realidad de la ciberseguridad en el entorno industrial, teniendo en cuenta que la industria abarca sectores muy diferentes y que esto plantea diferencias sustanciales a la hora de hablar de la ciberseguridad industrial. Por ejemplo, si hablamos de la distribución de energía, estamos hablando de una infraestructura crítica que ofrece un servicio esencial que posibilita el normal funcionamiento de otras industrias y de la vida ciudadana, por lo que su protección está sujeta al marco normativo estricto de la Ley de Protección de Infraestructuras Críticas (PIC). En este caso, el objetivo de la protección de las infraestructuras críticas es desarrollar e implantar las medidas de seguridad necesarias para que los operadores de esas infraestructuras o quienes estén al cargo de su gestión garanticen un nivel de protección adecuado tanto frente a amenazas físicas como cíber mediante tecnologías de ciberseguridad industrial, de seguridad física o una combinación de ambas.

Sin embargo, si por ejemplo hablamos del sector de máquina herramienta o automoción, estaremos hablando de ciberseguridad industrial en un contexto diferente, en el que el objetivo principal es prevenir, monitorizar y mejorar la resiliencia de los sistemas industriales ante acciones hostiles provenientes del ciberespacio y/o mejorar la resiliencia ante ciberamenazas de los productos fabricados.

La industria es vulnerable fundamentalmente a dos tipos de amenazas informáticas. Una de ellas es la amenaza a las tecnologías de la información (*Information Technologies*, IT) que se utilizan para fines comerciales y administrativos. Estos son los ataques de los que se oye a menudo y en los que se comprometen equipos de oficina con el resultado de robo o destrucción de datos. Mientras que este tipo de amenazas está relativamente bien entendido y existen soluciones avanzadas de protección en forma de aplicaciones antivirus o para la detección y prevención de intrusiones (*Intrusion Detection/Prevention Centre*, IDS/IPS), el segundo tipo de amenazas, que tiene como objetivo la tecnología operacional (*Operational Technology*, OT), que hace referencia a los sistemas de producción y control, carece todavía de soluciones integrales de seguridad. Además, es necesario tener en cuenta que la gran mayoría de los sistemas industriales en uso fueron desarrollados hace más de una década con la práctica ausencia de consideraciones sobre ciberseguridad.

En este sentido, la publicación *infoPLC* informa en su artículo sobre el "Estado de la Ciberseguridad Industrial 2018 en España" de las vulnerabilidades que afectan a diferentes tipos de dispositivos y sistemas de fabricantes industriales que están instalados en muchas de nuestras industrias (Figura 3). El artículo utiliza los datos del servicio de alerta temprana del Incibe mediante avisos de sistemas de control industrial (SCI). Según esta fuente, a lo largo de 2018 se han publicado 227 avisos de vulnerabilidades en el sector industrial frente a los 199 de 2017 que afectaron a dispositivos/sistemas multipropósito utilizados en prácticamente todos los sectores industriales.

Figura 3. Vulnerabilidades reportadas por sectores



Fuente: "Estado de la ciberseguridad industrial en España", *infoPLC*, 3 de febrero de 2019, http://www.infoplc.net/actualidad-industrial/item/106194-estado-ciberseguridad-industrial-2018-espana.

Entre los fabricantes con más avisos nos encontramos con Schneider Electric, Siemens, ABB, Philips, Delta Electronics, Moxa, Rockwell Automation y GE. Estar a la cabeza en este *ranking* no quiere decir estar haciéndolo mal en el ámbito de la ciberseguridad; puede que estén realizando más esfuerzos en validar sus equipos o que dispongan de una amplia gama de ellos, tal y como se señala en el informe anterior.

Es importante sensibilizar a la industria para que sea consciente de las vulnerabilidades reportadas por los fabricantes de equipamientos industriales con los que está trabajando su empresa, las medidas que esos fabricantes sugieren para minimizar su impacto en

las instalaciones en las que su equipamiento esté implantado o en qué plazo plantean resolver esas vulnerabilidades y cómo. Dado que muchos de los avisos publicados hacen referencia a vulnerabilidades que pueden explotarse remotamente, sigue siendo necesario insistir a las empresas industriales en que protejan su perímetro de red.

Es importante mencionar que cada vez más fabricantes de sistemas y equipamientos industriales disponen de departamentos especializados en la ciberseguridad de sus productos para identificar sus vulnerabilidades, resolverlas, informar sobre ellas y asesorar a sus clientes sobre cómo solucionarlas, y diseñar sus nuevos sistemas de una forma más cibersegura. En este último aspecto cabe mencionar la iniciativa denominada *Charter of Trust*, creada en marzo de 2018 por grandes industrias aprovechando la Conferencia de Seguridad de Múnich[1].

El mercado de la ciberseguridad industrial

Según el informe de MarketsandMarkets de 2018[2], se espera que el tamaño del mercado de la seguridad de los sistemas de control industrial (SCI) crezca de 10.200 millones de dólares en 2018 a 18.000 millones en 2023 (6,5 % de crecimiento anual) debido al crecimiento exponencial de los ciberataques y de las amenazas a la seguridad de la red gracias a grandes inversiones en tecnologías inteligentes y al apoyo de organizaciones gubernamentales a la seguridad en los sistemas de control industrial a nivel mundial. En este sentido, muchos fabricantes están empezando a vislumbrar un mercado de ciberseguridad en crecimiento para el que se está desarrollando, más allá del ámbito tecnológico, una industria de la ciberseguridad de la que la industria española de fabricación debería ser partícipe.

Volviendo a cómo abordan la ciberseguridad las empresas industriales, debemos decir que no es una tarea fácil. El Centro de Ciberseguridad Industrial (CCI) en su informe titulado “Ciberseguridad en Infraestructuras Críticas e Industria 4.0” señala que las industrias se encuentran en un estado de madurez elemental a la hora de implantar medidas que puedan gestionar los riesgos de ciberseguridad, ya que hasta no hace mucho tiempo la ciberseguridad no se encontraba entre las prioridades y los ámbitos de actuación de estas empresas. Por otro lado, se enfrentan a dificultades añadidas y conflictos internos por la necesidad de proporcionar recursos destinados a la ciberseguridad, en algunos casos difíciles de encontrar, y a la dificultad de asignar responsabilidades de ciberseguridad a personal que puede no estar suficientemente preparado.

A todo lo anterior debe añadirse, como se menciona en el informe sobre el “Estado de la Ciberseguridad en Euskadi 2018”, que hay cierta reticencia entre las empresas industriales a reconocer y notificar los impactos que haya podido tener un ciberincidente en sus empresas, y esto es importante si se quiere que la dirección de la organización

[1] Forman, por ahora, el *Charter of Trust*: AES, Airbus, Allianz, Daimler, Deutsche Telekom, ENEL, ATOS, CISCO, Dell, IBM, NXO, Siemens, SOS, TOTAL y TÜV Rheinland, https://assets.new.siemens.com/siemens/assets/public.1549982918.55badda4-4340-46d3-b359-f570e7d1f4c2.charter-of-trust-presentation-en.pdf.

[2] MarketsandMarkets, “Industrial Control Systems (ICS) Security Market”, 2018, https://www.marketsandmarkets.com/PressReleases/industrial-control-systems-security-ics.asp.

y las áreas de negocio conozcan las dimensiones reales del problema para poder tomar las medidas apropiadas dentro de la organización involucrando a todos los ámbitos organizativos. Para ayudar a las empresas en este contexto, el CCI, junto con la ISA Sección Española y el Centro Vasco de Ciberseguridad, ha desarrollado la "Guía SGCI para el responsable de construir un sistema de gestión de la ciberseguridad industrial", consistente en seis etapas (Figura 4) de entre las que me quiero centrar en esta ocasión en las dos primeras, de "gestión de los riesgos de la ciberseguridad industrial" y de "promoción de una cultura de la ciberseguridad"[3].

Figura 4. Fases de una estrategia de ciberseguridad industrial

Fuente: "Guía SGCI", CCI, ISA Sección Española y Centro Vasco de Ciberseguridad.

Entre las prioridades de las empresas se encuentran la mejora de los productos y servicios, el cumplimiento de regulaciones y estándares y la gestión de riesgos, pero las empresas todavía no están viendo que existe un tipo de riesgo diferente a los que venían considerando hasta el momento y que está asociado con el riesgo proveniente del mundo virtual: el ciberriesgo.

En el caso de un ciberataque, se pueden producir pérdidas económicas y daños a la imagen de la empresa. Empieza a existir una estrecha relación entre el riesgo financiero y el riesgo cibernético (ciberriesgo), que puede llegar a provocar una caída de hasta el 5 % del valor de las acciones, una pérdida de la facturación de las empresas por valor de unos 2,7 millones de euros y, en el caso de filtraciones de datos o de su robo, con la aplicación del Reglamento General de Protección de Datos (RGPD), pueden llegar a imponer multas de hasta 20 millones de euros o el 4 % de la facturación total anual del ejercicio anterior, según datos de la *Harvard Business Review* en 2017[4].

Por estos motivos, intentar evitar un ciberataque o, al menos, minimizar su impacto es importante si se desea gestionar la continuidad del servicio que se esté prestando, la continuidad del negocio e incluso la propia supervivencia de la organización industrial. Dado que los ciberriesgos están cada vez más ligados a los riesgos financieros, el papel

[3] CCI y Centro Vasco de Ciberseguridad, "Estado de la Ciberseguridad en Euskadi 2018, https://www.basquecybersecurity.eus/archivos/201810/bcsc_ciberseguridad_industrial_en_euskadi_2018_v1.pdf?1, y "Guía SGCI para el responsable de construir un sistema de gestión de la ciberseguridad industrial", noviembre de 2018, https://www.basquecybersecurity.eus/es/actualidad-bcsc/bcsc-pone-disposicion-guia-sgci-empresas-vascas.html.

[4] Alex Bau, "The Behavioral Economics of Why Executives Underinvest in Cybersecurity", *Harvard Business Review*, 7/VI/2017, https://hbr.org/2017/06/the-behavioral-economics-of-why-executives-underinvest-in-cybersecurity.

del responsable de finanzas (*Chief Financial Officer*, CFO) es entender dónde se encuentran los ciberriesgos que pueden afectar financieramente a la empresa y en qué medida los presupuestos e inversiones en seguridad solicitados por parte del director de seguridad de la información (*Chief Information Security Officer*, CISO) o del director de tecnologías de la información (*Chief Information Officer*, CIO) pueden ayudar a disminuir las vulnerabilidades y los riesgos financieros asociados.

Por otro lado, aunque en las empresas existen múltiples vías posibles de infección, la necesidad de crear una cultura de la ciberseguridad viene motivada porque uno de los primeros pasos que suelen utilizar los ciberatacantes es obtener información del sistema y de sus usuarios utilizando técnicas de ingeniería social para poder perpetrar los ciberataques de la forma más eficiente y con el menor riesgo posible. Por ejemplo, un empleado también puede acceder a sitios web maliciosos, responder a emails de tipo *phishing*, dejar claves en sitios visibles, conectar un USB u otro tipo de dispositivo infectado, mostrar falta de precaución al abrir o ejecutar ficheros desconocidos o ejecutar programas infectados y abrir con ello puertas a los ciberatacantes.

Otro ejemplo entre los ataques dirigidos a empresas multisector es el de las estafas *Business Email Compromise* (BEC), que es un tipo de ataque que consiste en suplantar la identidad de una persona vía *email* para engañar a otra con el fin de que realice una transferencia económica a una cuenta controlada por el estafador. Estos ataques están diseñados específicamente para cada víctima y este nivel de personalización provoca que superen los filtros de *spam* y otras protecciones. Todo esto plantea que la educación a todos los niveles del personal de la empresa en medidas higiénicas de ciberseguridad es fundamental como medida preventiva frente a ciberataques.

La capacitación de las personas en materia de ciberseguridad industrial es un tema relevante para las industrias, ya que, a diferencia de la relacionada con la ciberseguridad de las redes TI, que está muy avanzada, las empresas se enfrentan con la dificultad de formar a su personal con una oferta formativa escasa, a veces muy orientada hacia la ciberseguridad digital con ciertas nociones de temáticas industriales o muy centrada en el itinerario formativo disponible por el momento para la ciberseguridad industrial. Al mismo tiempo, en el caso de que la empresa quiere contratar profesionales en ciberseguridad, se va a encontrar con una gran escasez de profesionales expertos.

Conclusiones

Trabajar para lograr una Industria Conectada 4.0 resiliente implica entender y potenciar la ciberseguridad en las empresas industriales considerando la ciberseguridad en el diseño, despliegue y operación de cualquier proyecto de Industria Conectada 4.0. Tampoco hay que olvidar que, si se vende un producto, es importante asegurar su ciberseguridad en las instalaciones en las que se utilice teniendo en cuenta técnicas de desarrollo de *software* a lo largo de todo el ciclo de vida del producto y a lo largo de la cadena de suministro.

Es necesario pensar en alcanzar la soberanía tecnológica sobre algunas tecnologías habilitadoras clave de la Industria Conectada 4.0 considerando la ciberseguridad desde su diseño; por ejemplo, la inteligencia artificial en la Industria Conectada 4.0 o para la ciberseguridad industrial.

Se hace preciso aprovechar la oportunidad que brinda el creciente mercado de la ciberseguridad para desarrollar una industria española de ciberseguridad apalancada en un conjunto de empresas que llevan ya un largo recorrido trabajando en ese ámbito, *startups* del sector y empresas fabricantes de productos industriales con inteligencia embebida que desarrollen la ciberseguridad de sus productos y ofrezcan esos servicios al exterior.