La industria ante al reto de la ciberseguridad

La adopción de herramientas, técnicas y procedimientos para minimizar el acceso no autorizado desde el ciberespacio a la información utilizada para gestionar las empresas e infraestructuras industriales se ha generalizado solo, de momento, en las grandes compañías. En España, la mayor concienciación sobre la necesidad de implantar y mantener medidas de ciberseguridad industrial se concentra en los sectores eléctrico, nuclear, petrolero y gasista, aunque la tendencia empieza a ser palpable en otros sectores. Los especialistas en este campo están ya entre los profesionales más demandados

Mónica Ramírez

La revolución industrial es un hecho y ha venido para quedarse. Sin embargo, lo más reseñable de este panorama es que la transformación digital necesita ir acompañada de una "estrategia digital", y según el estudio España 4.0: el reto de la transformación digital de la economía, elaborado por Siemens PLM y Roland Berger, solo el 38% de las empresas cuenta con ella. Hablamos de la conexión integral de las distintas áreas de la economía y la manera en la que los profesionales de cada sector se adaptan a las nuevas condiciones que imperan en la economía digital, basada en los pilares de la información digital, la automatización de procesos mediante inteligencia artificial, computación en la nube, la conectividad y el internet de las cosas.

Los avances tecnológicos plantean a las empresas numerosos retos, a la vez que se convierten en generadores de nuevas oportunidades. Se vislumbra, por tanto, un nuevo modelo industrial en el que la innovación y el desarrollo serán más colaborativos, se reducirán los tiempos de respuesta, los medios productivos serán más flexibles y estarán conectados y los canales de distribución serán digitales. Cada vez es más frecuente que los procesos de fabricación automatizados incorporen sistemas integrados de gestión con máquinas conectadas en red e, incluso, con sistemas corporativos y remotos para permitir la gestión desde que se tramita el pedido hasta que se expide el producto al cliente.

Perjuicio económico y reputacional

Sin embargo, con la adopción de todos estos sistemas tecnológicos, las empresas industriales también se exponen a nuevos riesgos, ya que pueden ser detectados por ciberdelincuentes, que logran acceder a ellos y causar graves perjuicios, tanto económicos como de reputación, en las empresas a las que atacan. Por ello, es imprescindible conocer los riesgos a los que las empresas industriales están expuestas y poner en marcha mecanismos que eliminen o, al menos, reduzcan su impacto. La ciberseguridad se convierte, pues, en una prioridad, que aborda todo un proceso y, como tal, los planes para llevarlo a cabo deben revisarse periódicamente, ya que las amenazas cambian y evolucionan constantemente.

> Un informe de la firma de servicios profesionales PwC señala que el 74% de las pymes ha sufrido algún tipo de ataque cibernético

Lo recomendable es diseñar un plan director de ciberseguridad en el que se definan y prioricen los proyectos de seguridad necesarios para las empresas. Por ello, de estos planes se derivan, a su vez, una serie de normativas de uso interno y unos procedimientos para verificar su cumplimiento.

El término ciberseguridad industrial define "el conjunto de prácticas, procesos y tecnologías, diseñados para gestionar el riesgo del ciberespacio derivado del uso, procesamiento, almacenamiento y transmisión de información utilizada en las organizaciones e infraestructuras industriales, utilizando las perspectivas de personas, procesos y tecnologías".

Por desgracia, en España, la adopción de herramientas, técnicas y procedimientos enfocados a la resiliencia de las empresas, hoy en día solo se encuentra en las grandes empresas industriales, o en aquellas en las que debido a su alto perfil de exposición son objeto de ataques cibernéticos. A ellas podemos añadir otras empresas caracterizadas por la deslocalización de sus centros productivos y la consiguiente necesidad de acceder de forma remota a sus sistemas de control industrial, lo que hace que estén expuestas a un alto riesgo cibernético.

El Centro de Ciberseguridad Industrial (CCI) publicó recientemente, con la colaboración del CERTSI (CERT de Seguridad e Industria), un estudio titulado *Estado de la Ciberseguridad Industrial en España. Evolución y futuro* y en el que se refleja que la mayor concienciación sobre la necesidad de implantar y mantener medidas de ciberseguridad industrial se concentra en los sectores eléctrico, nuclear, petrolero y gasista. Sin embargo, también es cierto que esta tendencia comienza a hacerse palpable en otros sectores, como el del transporte, el químico y del agua, debido principalmente a los requisitos regulatorios de la Ley para la Protección de Infraestructuras Críticas (LPIC) española.

Mayor concienciación

Las empresas de menor tamaño, al ser menos probable que se vean afectadas por los requisitos regulatorios de la LPIC, no suelen contar con la ciberseguridad entre sus prioridades. No obstante, esta circunstancia está cambiando gracias a que hay un mayor nivel de concienciación general en los sectores industriales, debido, en parte, a que las organizaciones de mayor tamaño están siendo, lamentablemente, víctimas de ciberataques. En este sentido, un reciente informe publicado por la firma de servicios profesionales PwC, *Information security breaches survey*, señala que el 74% de las pymes ha sufrido algún tipo de ataque cibernético.

Por su parte, el citado informe del CCI revela que casi el 60% de las organizaciones analizadas están inmersas en la formalización de sus procesos de gestión e incidentes de ciberseguridad, o en mu-

Foto: Shutterstock.

chos casos, incluso, ya los tienen establecidos. Sin embargo, todavía hay más de un 10% de organizaciones en las que no existe dicha gestión de los riesgos tecnológicos, o en las que solo se aplican medidas de forma reactiva, cuando ya han sufrido algún ataque cibernético.

Modelo defensivo en profundidad

La industria 4.0 afecta a toda la cadena de valor industrial, incluyendo aspectos muy importantes como son las comunicaciones y la ciberseguridad. No podemos obviar el hecho de que cada vez existe una mayor conectividad de las máquinas y las plantas y, como consecuencia, han aparecido nuevos riesgos que deben ser mitigados.

"Para hacer frente a esta realidad con éxito, es recomendable que las empresas adopten un modelo de protección para asegurar la disponibilidad de las instalaciones. Uno los más utilizados es el llamado modelo de defensa en profundidad (*defense in depth*, en inglés), que ofrece una excelente protección y consigue unas ratios muy altas. Es un modelo que nace a partir de las recomendaciones del conjunto de normas ISA 99 y el estándar desarrollado a partir de estas: IEC 62443, que es el estándar líder en seguridad en la automatización industrial. Además, es un modelo que se basa en tres conceptos: seguridad de planta, seguridad de red e integridad del sistema", explica José Luis Doñoro Ayuso, responsable de Comunicaciones Industriales-Automatización Industrial de Siemens.

Además, los expertos en ciberseguridad indican una serie de medidas básicas que habría que considerar:

- Hacer un inventario de los sistemas y un análisis de riesgos para establecer un plan de seguridad.
- Bloquear el perímetro, limitando con firewalls todas las zonas que no deban tener conexión con el exterior.
- Actualizar todos los sistemas, incluidos los de seguridad como firewall, IPS, antimalware, etc.
- Reforzar los controles de acceso local y remoto.
- Monitorizar y registrar los incidentes.
- Gestionar la configuración de los sistemas y mantener backups actualizados.
- Llevar a cabo auditorías rutinarias.
- Estar preparado, con un buen plan de contingencia para peor de los casos.
- Preparar al personal para reconocer las amenazas y riesgos de las tecnologías que se vayan adoptando.

Departamentos coordinados

Los departamentos de tecnología de la información (TI), seguidos de los de seguridad física y operaciones, son los que más habitualmente asumen la responsabilidad de la ciberseguridad industrial. Con el fin de mejorar el conocimiento requerido para la gestión de la CI, es necesario fomentar el trabajo en equipo entre los departamentos de TI y OT (Operation Technology) de las organizaciones. Las áreas que más participan en las acciones de ciberseguridad industrial son las que tienen relación con algún tipo de seguridad, y las que son conscientes de los posibles impactos que los incidentes de ciberseguridad podrían tener sobre el negocio (operaciones, ingeniería). Por ello, es preciso concienciar a los directivos sobre la necesidad y las implicaciones de la ciberseguridad industrial.

La mayor parte de los proyectos de ciberseguridad industrial que se afrontan hoy en día están motivados por procesos de mejora continua y la respuesta a incidentes. Muchas organizaciones tienen previsto el desarrollo de acciones en ciberseguridad industrial de manera inminente y en todos los sectores de la industria, lo que conlleva que los presupuestos destinados a ello tenderán a crecer.

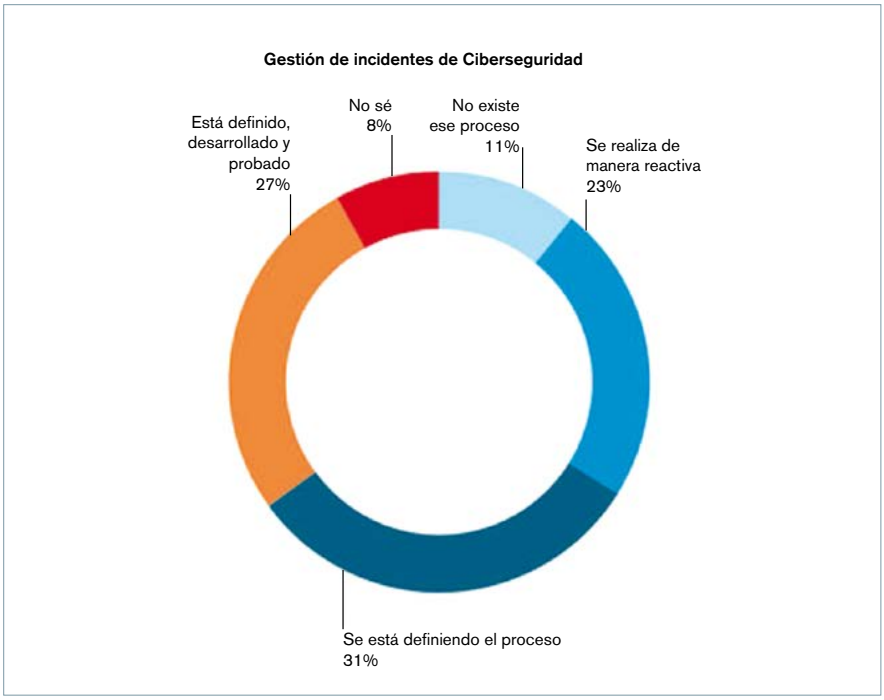
Reglamento de protección de infraestructuras críticas

Ante esta realidad, la seguridad industrial comienza a estar regulada, en parte, en diferentes países. Algunos ejemplos son la Ley de Seguridad de Alemania, la certificación ANSSI en Francia y la NERC CIP en EE UU. En España, tenemos el R. D. 704/2011, que aprueba el reglamento de protección de infraestructuras críticas, y servirá para desarrollar la citada Ley PIC. En el R. D. se definen las responsabilidades de organismos como el Instituto Nacional de Ciberseguridad (INCIBE) y el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), que desarrollan su labor para conseguir aumentar el nivel de protección de las empresas industriales, en general, y las infraestructuras críticas, en particular. En la actualidad, hay un acuerdo entre ambos organismos para gestionar el CERT de Seguridad e Industria (CERTSI) desde donde se gestionan las incidencias de ciberseguridad que puedan afectar a la prestación de los servicios esenciales. El CERTSI se constituyó en el año 2012 a través de un acuerdo marco de colaboración en materia de ciberseguridad entre la Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. Actualmente es regulado mediante acuerdo de 21 de octubre de 2015, suscrito por ambas Secretarías de Estado.

El CNPIC es el órgano responsable del impulso, coordinación y supervisión de todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas españolas y con la ciberseguridad en el seno del Ministerio del Interior. El CNPIC depende del secretario de Estado de Seguridad, máximo responsable del Sistema Nacional de Protección de las Infraestructuras Críticas y de las políticas de ciberseguridad del Ministerio.

El CNPIC fue creado en el año 2007, mediante Acuerdo de Consejo de Ministros de 2 de noviembre, y sus competencias están reguladas por la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y por el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el reglamento de protección de las infraestructuras críticas.

El director del CNPIC, Fernando Sánchez, ha asegurado que en lo que se refiere a los sectores estratégicos, el nivel de ciberseguridad es alto, aunque siempre existe opción de mejora, y ha garantizado que el más crítico, que es el energético y las TIC "está bien securizado".



Fuente: Informe Estado de la Ciberseguridad Industrial en España del CCI.

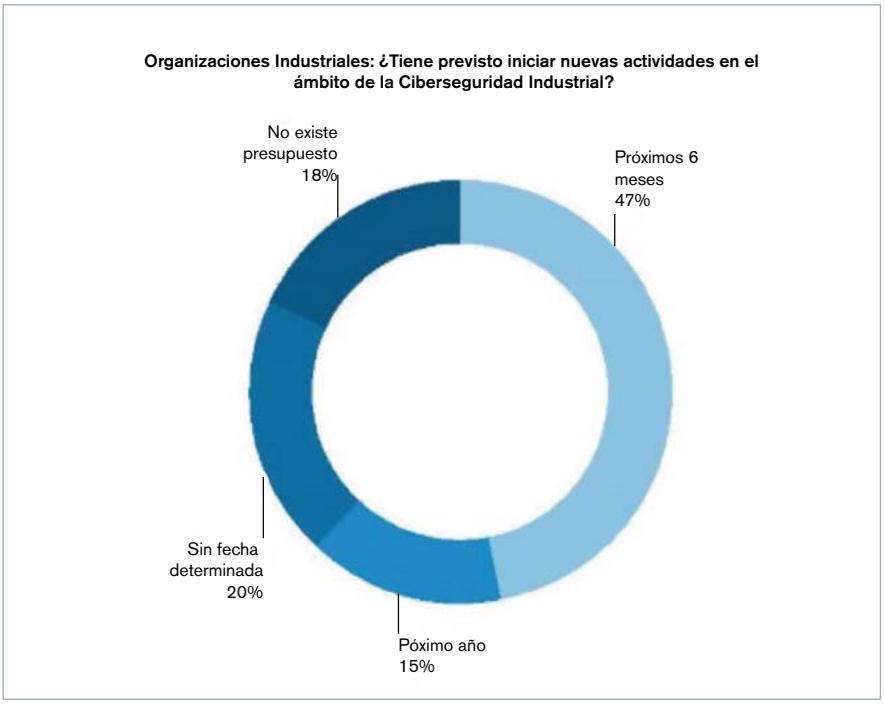
Sectores estratégicos

También ha anunciado que el organismo que dirige, encargado de la protección cibernética de sectores estratégicos como electricidad, agua potable, sanidad, transporte, telecomunicaciones, petróleo o alimentación, adscrito a la Secretaría de Estado de Seguridad, incorporará un plan estratégico para el ámbito de la salud este año. Fernando Sánchez ha señalado que España "está haciendo los deberes, aunque con carencias y áreas de mejoras" en el ámbito de su estrategia de ciberseguridad, que a su juicio está bien planteada. Asimismo, resalta el dato de que el año pasado se registraron un total de 885 ciberincidentes sobre sectores estratégicos, aunque no todos ellos fueron contra infraestructuras críticas, sino contra sus operadores, y fueron escasos los que resultaron problemáticos para los servicios esenciales. Para el director del CNPIC, el nivel de concienciación de los operadores estratégicos es alto, ya que más del 80% cumple perfectamente con el informe de incidentes y solo un 20 % va más retrasado, tanto por falta de medios y capacidades como por falta de concienciación, en ocasiones por una cuestión reputacional de las empresas.

Como consecuencia de la Directiva 2008/114/CE (NIS), relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y los sistemas de información en la Unión Europea (UE), España aprobó la Ley 8/2011 de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (Ley PIC), y su texto de desarrollo, el Real Decreto 704/2011, de 20 de mayo (Reglamento PIC), en el que se fue más allá de las exigencias de la propia Directiva PIC, regulando aspectos que no estaban considerados en la misma. Como resumen, la ley introducía las siguientes cuestiones:

• Sectores estratégicos. La Ley PIC establecía como sectores estratégicos los dos referidos en la Directiva PIC (Energía y Transporte) y otros en la misma línea que la Directiva NIS (sistema financiero y tributario, tecnologías de la información y las comunicaciones, salud y agua). Además, amplía sectores no considerados por la Directiva NIS (instalaciones de investigación, industria nuclear, espacio, Administración, industria química y alimentación). Al final crea 12 sectores críticos.

• Servicios esenciales. La esencia de ambas normas es proteger los servicios esenciales que se prestan en esos sectores estratégicos y garantizarlos en la mayor medida posible. La Directiva NIS establece que se deben valorar, como



Fuente: Informe Estado de la Ciberseguridad Industrial en España del CCI.

mínimo para cada uno de los subsectores que se indican en ella, qué servicios han de considerarse esenciales para el mantenimiento de actividades sociales y económicas vitales y determinar si las entidades enumeradas en los sectores y subsectores que prestan esos servicios cumplen los criterios de identificación de los operadores. En este sentido, la Ley PIC y su reglamento de desarrollo ya establecen mecanismos para identificar los servicios esenciales a través de los planes estratégicos sectoriales (PES).

• Operadores críticos y operadores de servicios esenciales. El concepto de operador crítico (entidad u organismo que presta un servicio esencial de carácter indispensable y que, en el caso de destrucción o perturbación, tendría un grave impacto) debe aprovecharse para identificar a los operadores esenciales NIS de primer orden. El concepto de operador esencial tiene un calado inferior al concepto de operador crítico, pero siempre que el servicio que preste dependa de las redes y los sistemas de información, debe ser considerado sujeto obligado en la Ley NIS. Por ello, es necesario alinear el contenido de la Ley PIC con el de la nueva Ley NIS, evitando de este modo crear inseguridad jurídica a los operadores.

Recientemente se ha aprobado una nueva directiva europea: Directiva 2016/1148/CE del Parlamento Europeo y del Consejo de 6 de julio de 2016, cuya trasposición a la legislación española está en trámite parlamentario y dará lugar a una nueva ley PIC. Su objetivo fundamental es "regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y digitales, así como establecer un sistema de notificación de incidentes".

En España, se ha establecido en el anteproyecto de ley sobre la Directiva NIS, publicado el 29 de noviembre de 2017, que esta estrategia "seguirá desarrollando el marco institucional de seguridad en la red, el cual estará compuesto, por una parte, por las autoridades públicas competentes y los CSIRT de referencia y, por otra, por la cooperación público-privada".

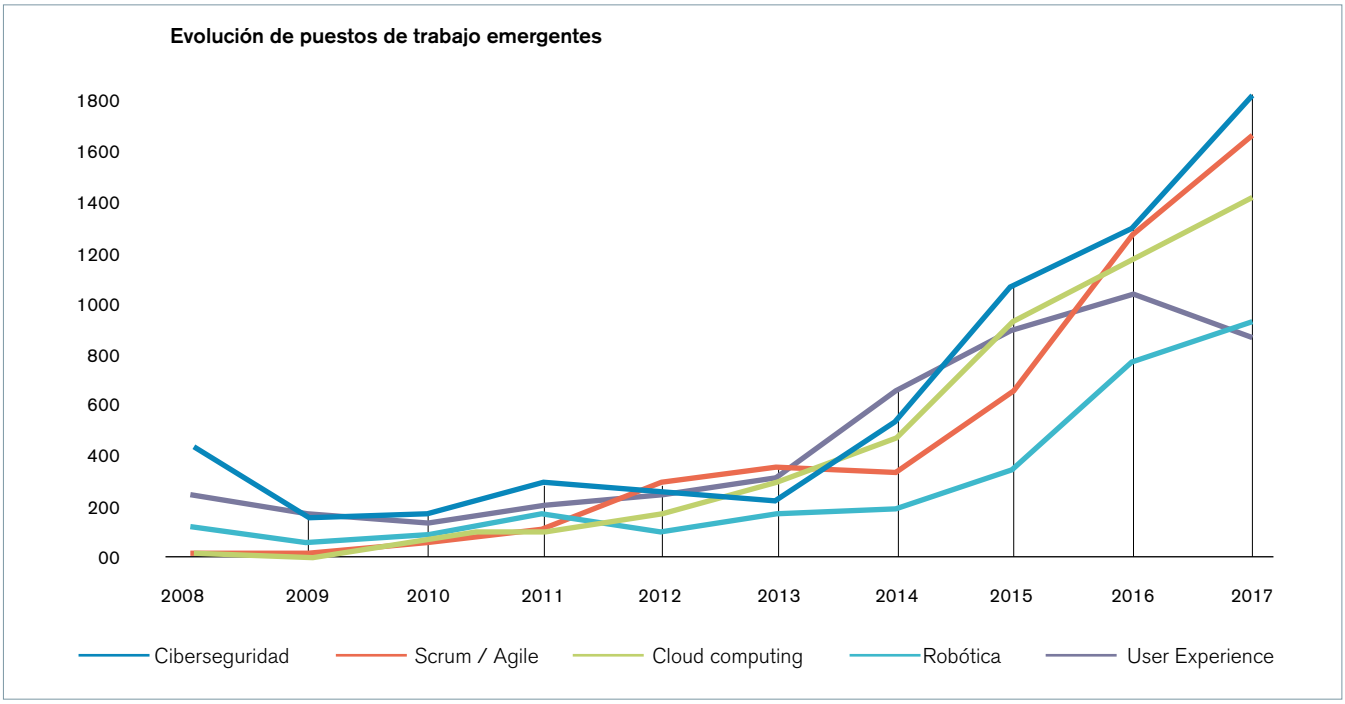
El borrador del anteproyecto sitúa por tanto al CCN-CERT (Centro Criptológico Nacional) como el CSIRT (Computer Security Incident Response Team) de referencia para el sector público y el coordinador nacional para respuestas técnicas en los supuestos de especial gravedad que se determinen.

En el caso de que la empresa no tenga ningún tipo de plan, siempre podrá recurrir a profesionales que les ayuden a gestionar el incidente, y en todo caso, podrán solicitar la ayuda del CERT-SI-CERT de Seguridad e Industria (www.certsi.es), pero siempre asumiendo que en cualquier caso la solución será más lenta y costosa.

La ciberseguridad, en general, y en el ámbito industrial, en particular, seguirá en su evolución a la propia tecnología. A medida que se introduzcan nuevos mecanismos y sistemas que mejoren los procesos (*machine learning,* inteligencia artificial, etc.), se generarán nuevos retos y por tanto, y de forma inevitable, se irán creando nuevos sistemas que palíen los riesgos y mejoren la seguridad. El gran reto será el de introducir todos esos avances en las pymes. Los operadores críticos (amparados por la Ley PIC) ineludiblemente estarán en el nivel de avance que les obligue la regulación que se vaya adaptando. El reto será para las pequeñas y medianas empresas que no disponen de normativa que les obligue, ni de grandes medios para hacerlo, y en la mayoría de los casos tampoco de los recursos económicos específicos para abordar este desafío. Aunque la industria 4.0 está hoy en día en todos los debates, un gran número de las pymes en nuestro entorno están todavía cerca del 2.0, y un incidente de ciberseguridad podría llegar a amenazar seriamente la supervivencia de la empresa.

Especialista en ciberseguridad del ámbito industrial

Belén Pérez Rodríguez es experta en ciberseguridad y coordinadora del Centro de Ciberseguridad Industrial (CCI) para la región de Galicia. En su opinión, durante mucho tiempo, los entornos industriales (OT) estaban aislados, sin ningún tipo de conexión al exterior, por lo que la seguridad pasaba por dos medidas: la seguridad por ocultación (si no sabes lo que pasa, no lo puedes atacar), y la seguridad física del perímetro (impedir sabotajes o accesos ilícitos a los procesos por parte de personal no autorizado). En los últimos años, debido a las mejoras de los sistemas de comunicaciones, tanto en el ámbito inalámbrico como en el cableado, se han ido incorporando dispositivos y mecanismos IT en el ámbito OT, ampliando la superficie de exposición. "Si analizas cada uno de los entornos desde el punto de vista del otro, es probable que cometas errores, básicamente por desconocimiento y premisas erróneas. En primer lugar, porque las necesidades en ciberseguridad son distintas en ambos entornos: IT es principalmente asegurar la confidencialidad de los datos, y OT es principalmente asegurar la disponibilidad, es decir, que los procesos no se paren", explica.



Fuente: Informe anual de Infojobs-ESADE 2017

En segundo lugar, debido a las características particulares del entorno OT, algunas de las soluciones típicas de seguridad del entorno IT no se puedan aplicar. "En los entornos OT hay sistemas en los que el tiempo de respuesta es muy crítico, y muchas de las medidas de seguridad clásicas de IT generan retardos, ya que necesitan analizar los tráficos, y esas latencias no se podrían asumir. Además, muchos de los protocolos industriales no son estándar y no se podrían analizar con herramientas para IT, por lo que hay que optar por otras medidas o soluciones", señala Belén Pérez.

Ciclos de vida largos

Por último, una de las premisas a tener en cuenta es que los ciclos de vida de los entornos industriales suelen ser muy elevados, en ocasiones más de 20 años. "Por este motivo, es muy complicado securizar un sistema que ya está funcionando, con ventanas de operación limitadas las escasas y breves paradas de mantenimiento, y con sistemas antiguos para los que en muchas ocasiones ya no hay soporte. Al final, la ciberseguridad no es una actividad, sino un proceso continuo que debe formar parte de la organización, como uno más, y que de forma constante y permanente analice riesgos, implemente medidas y verifique sus resultados. Es evidente que todo ello sólo será posible si hay profesionales designados y con partidas presupuestarias asignadas para conseguir esos objetivos", concluye.

Por otra parte, en términos de recursos humanos, los perfiles que hasta ahora no eran muy tecnológicos van a tener que conocer herramientas para analizar en tiempo real datos de manera masiva, de la misma forma que en la década de 1990 la ofimática dejó de ser un valor añadido en el currículum para convertirse en un conocimiento básico. El camino hacia la revolución digital y la transformación de las posiciones es inevitable.

Según el informe *Industria 4.0*, elaborado por la consultora PwC, un escaso 8% de las empresas españolas tiene en la actualidad un nivel de digitalización avanzado, frente al 33% de las empresas industriales globales. La previsión es que estas cifras aumenten en los próximos años, pero mantienen su diferencia para 2020: un 19% en España, y un 72% de media en todo el mundo.

Todo ello entraña la necesidad de contar con nuevos perfiles. Entre la lista de los nuevos puestos emergentes más demandados se encuentran los de diseñador de *software* y web, programador de *apps*, desarrollador de Big Data y especialistas en Agile/Srum, *cloud computing* (computación en la nube), *UX design* y en ciberseguridad. En este sentido, el último informe de Infojobs señala que los puestos vacantes para estos últimos (ciberseguridad) asciende a unos 1.300, y el sueldo bruto medio es de 32.400 € Sin embargo, todos estos perfiles son tan nuevos que no hay suficientes profesionales para cubrir la demanda del mercado laboral.

Puesto emergente más solicitado

El puesto de especialista en ciberseguridad encabezó la lista de los puestos emergentes más demandados en 2016, elaborada por Infojobs y recogida en su informe anual de 2017. Las 106 vacantes publicadas en 2009 pasaron a ser 1.270 en 2016, con una competencia de 20 inscritos por vacante. Además, según la empresa IDG, se calcula que en 2019 habrá una demanda de expertos en ciberseguridad de 6 millones de personas.

Nos encontramos ante el gran reto de llevar a cabo la transformación digital, en el que los ingenieros técnicos industriales y graduados en ingeniería de la rama industrial tienen todavía mucho que aportar. Para ello, es necesario llevar a cabo acciones formativas destinadas a dotar de conocimientos y capacidades a los alumnos de la rama industrial de la ingeniería, fundamentalmente en los principales conceptos y técnicas relacionadas con la ciberseguridad industrial. De este modo, podrán adquirir las competencias necesarias para incorporarlas a su actividad profesional en el marco de las empresas industriales.