JOSÉ IGNACIO ARMESTO QUIROGA

Profesor de Ingeniería de Sistemas y Automática, Universidad de Vigo

"EN CIBERSEGURIDAD, DAR ALGUNOS PASOS EN LA BUENA DIRECCIÓN NO ES CARO, Y LA DIFERENCIA PUEDE SER MUY GRANDE"

Doctor Ingeniero Industrial por la Universidad de Vigo, en la que es profesor titular, así como director del Área de Formación Permanente, el pasado 13 de enero José Ignacio Armesto daba el pistoletazo de salida al inicio del curso que permitirá la obtención del primer título de Especialista en Ciberseguridad Industrial (ECSI) existente en España. Además de todo ello, sobre lo que nos hablará en esta entrevista, José Ignacio Armesto es coordinador también del Máster Universitario en Mecatrónica y, desde 2004, presidente del Comité Organizador del Congreso Internacional Jornadas sobre tecnologías y soluciones para la Automatización Industrial (JAI), que en noviembre de este mismo año 2022 celebrará su octava edición.

Redacción Industria Química

El pasado mes de enero se iniciaba el curso para la obtención del título de Especialista en Ciberseguridad Industrial, que imparte la Universidad de Vigo y del que Vd. es su promotor. ¿Qué factores han incidido para que sea esta universidad la primera que imparta esta titulación?

Pues hay dos factores especialmente relevantes que "dispararon" esta iniciativa. Uno de ellos fue el informe realizado por la Fundación Empresa-Universidad Gallega (FEUGA) para la Secretaría Xeral de Universidades de la Xunta de Galicia, en el que se estudia el catálogo de perfiles profesionales del futuro y nuevas titulaciones y especialidades universitarias. En dicho informe aparece específicamente el perfil de especialista en ciberseguridad industrial como una necesidad en el ámbito empresarial. En segundo lugar, otro factor decisivo fue un artículo de Ignacio Álvarez, director del Área de Sistemas de Comunicación y Ciberseguridad Industrial de Siemens España, en el que manifestaba la necesidad de crear una nueva especialidad universitaria para profesionales de la ciberseguridad industrial. Todo ello derivó en unas primeras conversaciones con Ignacio Álvarez para perfilar el proyecto formativo, la entrada de Adriel Regueira (director de IT y Ciberseguridad en Tecdesoft) en el equipo como motor para la definición del programa de contenidos y, poco a poco, fuimos avanzando hasta definir lo que hoy es el primer título propio en España dedicado a formar especialistas en el ámbito específico de la ciberseguridad industrial.

¿Qué papel considera que debe realizar una entidad académica como es la universidad en la capacitación de los profesionales en ciberseguridad que no estén ya realizando otro tipo de entidades, públicas o privadas?

La universidad debe participar de forma activa en la formación continua de los profesionales de nuestra sociedad, pues es una de sus misiones. Precisamente para dinamizar este apartado se creó en la Universidad de Vigo la Escuela Abierta de Formación Permanente, con el objetivo estratégico de abrir la formación permanente a la sociedad mediante una oferta de títulos propios coordinada, de calidad y adaptada a la demanda, con el fin último de generar nuevas oportunidades profesionales y personales.

Las universidades pueden, gracias a los títulos propios, organizar de forma ágil y flexible formaciones adaptadas a las necesidades de la sociedad en las que participen tanto expertos universitarios en la materia como reconocidos profesionales con amplia experiencia en ese ámbito, como es el caso de este título de especialista en ciberseguridad industrial. Y a todo ello se suma el rigor y los procedimientos de garantía de calidad que se aplican en las instituciones universitarias públicas.

¿A qué tipo de estudiantes se dirige este curso y cuáles son los objetivos del mismo?

Este título propio de especialista en ciberseguridad industrial está orientado, principalmente, a titulados universitarios de primer y segundo ciclo y profesionales del sector que reúnan los requisitos de habilitación de acceso a la universidad, y cuya dedicación esté encaminada a la implantación, mantenimiento y gestión de sistemas automáticos en el ámbito industrial y acrediten un mínimo de tres años de experiencia profesional.

Esta edición del título propio, en concreto, ha tenido los siguientes requisitos de acceso: estar en posesión de un título universitario dentro del Espacio Europeo de Educación Superior (EEES) que otorgue el acceso a enseñanzas oficiales de posgrado; estar en posesión de un título extranjero, ajeno al EEES, homologado a un título universitario oficial del EEES; estar en posesión de un título extranjero, ajeno al EEES, no homologado, pero que acredite un nivel equivalente a un título universitario de grado dentro del EEES que faculte, en el país de expedición del título, para el acceso a las enseñanzas de posgrado; tener superados un mínimo de 120 ECTS en una titulación universitaria oficial dentro del EEES; ser profesionales de reconocida y acreditada experiencia laboral, siempre que la citada experiencia esté relacionada con las competencias inherentes al título y cumplan los requisitos de acceso a la universidad segundo la normativa vigente.

La titulación de especialista en ciberseguridad industrial pretende ser una amplia introducción sobre el estado actual de las técnicas de ciberseguridad aplicadas en las plantas industriales (OT). Los conocimientos teóricos impartidos en este curso llevarán a la práctica utilizando herramientas y tecnologías de diversos fabricantes (Fortinet, Microsoft, Nozomi Networks, Vmware y Siemens, entre las más destacadas). El objetivo final de esta formación es proporcionar al profesional de este sector conocimientos prácticos, actualizados y eficaces, sobre algunas de las soluciones actuales del mercado de la ciberseguridad industrial en el campo del control, operación y comunicación de procesos industriales.

¿Cómo articulará o qué relación mantendrá una universidad pública, como es la de Vigo, la relación con las empresas privadas que gestionan, por lo general, el campo de la ciberseguridad industrial?

La universidad debe mantener una relación lo más neutra y abierta posible con todos los agentes sociales y empresariales. No obstante, a la hora de trabajar con titulaciones tan prácticas como la que nos ocupa, es necesario aterrizar los contenidos teóricos en equipamiento utilizado en los entornos profesionales, por lo que la colaboración de firmas como las mencionadas anteriormente es estratégica para su éxito. Por supuesto, al menos en el título que nos ocupa, estaremos atentos y abiertos a cualquier otra oferta de colaboración que permita aportar un valor formativo y/o técnico adicional a su alumnado, que es el verdadero fin último.

En la memoria de presentación del título de Especialista en Ciberseguridad Industrial señalan que dicho curso "pretende cubrir el hueco que hay entre los perfiles formativos industrial y de las tecnologías de la información y comunicaciones, generando un nuevo perfil especialista en ciberseguridad industrial". ¿Cómo definiría a este nuevo especialista? ¿Qué diferencias establecería con el modelo existente en el momento actual?

Antes de lo que denominamos cuarta revolución industrial, la conexión entre el mundo IT y el mundo OT era algo inexistente, los equipos de control industrial (PLC, DCS, etc.) no disponían, por lo general, de capacidades de comunicación con los sistemas IT de la empresa. La llegada de la industria 4.0 trajo consigo, entre otras muchas cosas, que los equipos de control industrial comenzasen a integrar tecnologías de comunicaciones compatibles con las existentes en el mundo IT, lo que ha posibilitado que estos mundos, antes disjuntos, puedan conectarse entre sí hoy en día. Este hecho aporta innumerables ventajas, pero también conlleva nuevos riesgos que es preciso abordar, entre ellos el de la ciberseguridad industrial.

Este título de especialista en ciberseguridad industrial pretende precisamente cubrir este gap, tanto para el profesional que proviene del mundo OT y que quiere conocer la problemática que hasta ahora le era ajena como para el profesional que proviene del mundo IT y que quiere conocer las particularidades que tiene la aplicación de las técnicas de ciberseguridad aplicadas en el mundo IT en el ámbito de la planta industrial.

Por explicarlo en términos prácticos, habremos logrado uno de los grandes objetivos perseguidos en este curso si al mismo asistieran los responsables de IT

y OT de una empresa y, al finalizar el título, ambos se pudiesen entender mejor que antes utilizando la jerga técnica del este ámbito, empatizar con las problemáticas y necesidades del otro, etc.

En un momento en donde la transversalidad se define como clave para el desarrollo de los nuevos profesionales, ¿hacía donde debería mirar también el nuevo profesional de la ciberseguridad industrial?

El entorno de la ciberseguridad es muy cambiante, teniendo que actualizar a diario sus conocimientos y brechas descubiertas, a la vez que las mejores técnicas y las que han probado ser las más eficaces contra los riesgos conocidos y las que se creen mejores frente a los riesgos no conocidos. Para poder lograr con éxito esta protección, el profesional debe entender muy bien las necesidades de negocio que está protegiendo para centrarse en los sistemas clave de la organización que esté abordando. En este sentido, para poder entender bien el núcleo de los sistemas industriales, desde nuestro punto de vista, faltaba formación específica para poder abordarlo correctamente.

¿Cómo considera que evolucionará este título de Especialista en Ciberseguridad Industrial? ¿Ve factible su impartición también en otras universidades?

En el fondo, se tratará de una cuestión de oferta y demanda. Los títulos propios universitarios deben autofinanciarse, por lo que será el propio mercado el que regule si es preciso crear este título en más universidades españolas o es suficiente con esta oferta. Por lo que nos indican muchas empresas (entre ellas las que participan en el título), todo apunta a que sí será necesaria una mayor oferta, porque la necesidad de profesionales en ciberseguridad industrial irá creciendo en las empresas. Para nosotros es un orgullo, en todo caso, haber sido los primeros en atrevernos a ofertarlo. Y el que da primero -y bien- siempre da dos veces. Además, al ofertarlo en la modalidad *online*, nuestro ámbito formativo no se restringe a lo local, sino que es global (en especial España y Latinoamérica).

En esta primera edición se han agotado las plazas disponibles. Además, el 90% de las personas matriculadas en esta primera edición del título son profesionales del sector, lo que, desde nuestro punto de vista, indica que hemos acertado con la propuesta de contenidos, que han resultado ser, como esperábamos, atractivos para profesionales en activo. El círculo virtuoso se alcanzará si la formación recibida es bien valorada por los profesionales que cursan esta formación (ellos serán los verdaderos embajadores del mismo) y la demanda de sus titulados por parte de las empresas es elevada, lo que visibilizará esta formación ante el alumnado universitario y hará que, gradualmente, aumente su porcentaje en la matrícula del título.

¿En qué momento nos encontramos en el desarrollo de la ciberseguridad industrial? ¿Podemos abordar de forma efectiva con las herramientas actuales los problemas que se suceden en el mundo industrial? ¿Qué debería cambiar?

Estamos en un cambio de inflexión en el desarrollo industrial. Las organizaciones se han dado cuenta que no podían seguir mirando hacia otro lado, y se están lanzando poco a poco a abordarla, fijándose en las industrias más puntera y sus casos de éxito, que ya son numerosos y permiten utilizar estrategias y herramientas que han probado ser efectivas salvaguardando la disponibilidad de la fábrica. Dentro de este contexto, la demanda de profesionales en este ámbito se está duplicando año tras año para poder abordar todos estos proyectos.

Aun así, siguen existiendo empresas que creen que todavía no es su momento para invertir en esta área, arriesgándose a ser los más vulnerables de su entorno, ya que no perciben el riesgo, quizá por falta de concienciación.

Animamos a todas las empresas que aborden la cuestión de la ciberseguridad. Dar algunos pasos en la buena dirección no es caro, y la diferencia puede ser muy grande.

Recientemente la vicepresidenta primera y ministra de Asuntos Económicos y Transformación Digital, Nadia Calviño, aseguraba que en 2022 llegaría al Congreso la ley de ciberseguridad 5G. ¿Qué supondrá esta nueva normativa? ¿De qué forma considera que tiene que actuar la Administración en la gestión y desarrollo de la ciberseguridad industrial?

Las infraestructuras de comunicación celulares ya son hoy en día esenciales para todos nosotros, pero las redes 5G se van a convertir también en elementos fundamentales para muchos procesos industriales, logísticos, etc. Es decir, van a ser elementos que no pueden fallar para no afectar procesos esenciales. Por este motivo es adecuado que se establezcan los mecanismos que formalicen los procedimientos para garantizar la seguridad de este tipo de redes, intentando minimizar los riesgos que las puedan afectar. La Administración debe establecer normas y recomendaciones que garanticen que los productos comercializados y los procedimientos de instalación, uso y mantenimiento, aseguren un funcionamiento estable incluso ante ataques externos.

Siendo como es la seguridad de las plantas en el sector químico un factor prioritario en el desarrollo de estas instalaciones, ¿considera que la ciberseguridad necesitaría contar en este sector con normativas o estándares especiales, dado el peligro potencial que supone el acceso a datos muy sensibles?

Afortunadamente, el sector industrial cuenta ya con compendios de buenas prácticas, directivas y normativas específicas al respecto, como la ISA/IEC 62443, que fue creada originalmente por ISA, y que permite a la empresa abordar de una forma estructurada y estandarizada la gestión de los ciber-riesgos en lo que denominan IACS (Industrial Automation and Control Systems). De esta forma, se incluye también los procedimientos del proceso industrial. Esta forma holística de verlo ayuda a proteger tanto el *safety* cómo la continuidad de negocio de la corporación.