# Palabra de experto: los desafíos de la ciberseguridad industrial

A medida que las tecnologías de control y automatización avanzan y ganan protagonismo en la industria, también en la vida cotidiana de las personas, las preguntas acerca de la seguridad de los datos cobran mayor relevancia y urge obtener buenas respuestas. En este contexto, AADECA entrevistó a Roger A. Roa, Cybersecurity Sales en Schneider Electric para Latinoamérica

**Schneider Electric**
*www.se.com*

¿Por qué las industrias deberían preocuparse por la ciberseguridad?, ¿qué tan importante es para las PyMEs?

*Hoy, más que nunca, las empresas deben estar en condiciones de preservar la seguridad digital de sus empleados y clientes. La línea entre TI (tecnologías de la Información) y TO (tecnología operacional en los sistemas de control) es cada vez más delgada y esto exige fortalecer la estrategia de seguridad para la infraestructura de las plantas. La ciberseguridad es parte de la nueva normalidad.*

*Reducir las amenazas y los riesgos de las operaciones es fundamental para mejorar la continuidad del negocio y el crecimiento en escala. Especialmente para las pymes, que buscan crecer y expandirse en un mundo cada vez más digital, la seguridad de sus plataformas es la llave para un crecimiento prolijo y sin fallas.*

¿En qué sectores/rubros de la industria existen las mejores perspectivas para implementar ciberseguridad?

*Muchos de los sistemas que controlan las operaciones más críticas del mundo se instalaron y desarrollaron hace décadas antes del surgimiento del IoT industrial*

*(IIoT), y estaban destinados a un uso a largo plazo. A medida que la digitalización prolifera rápidamente, se vuelve fundamental empezar la evaluación del riesgo en los sectores que tienen más sistemas heredados, y posteriormente un plan de ciberseguridad de extremo a extremo que permita abordar otros sistemas de control.*

*Cada dispositivo conectado a la red podría usarse como punto de entrada a la infraestructura para infiltrarse y manipular todo el ecosistema digital. Piense en esto: las fábricas inteligentes de hoy en día tienen cientos, e incluso miles, de sensores conectados. Es por esto que se requiere adoptar un enfoque holístico de la ciberseguridad, desde la seguridad misma del producto hasta la protección de toda la cadena de suministro.*

*"Especialmente para las pymes, que buscan crecer y expandirse en un mundo cada vez más digital, la seguridad de sus plataformas es la llave para un crecimiento prolijo y sin fallas".*

¿Cuáles son los conceptos fundamentales de la ciberseguridad industrial?

*Por muchos años, la tradicional tecnología de la información y los sistemas de operaciones tecnológicas se mantuvieron separados porque sus dominios eran manejados por distintas fuentes. Sin embargo, este paradigma está cambiando radicalmente ya que los sistemas de operaciones tecnológicas están ahora conectados a la misma red, con direcciones IP, es decir que el control y el manejo de estas interfaces están expuestos.*

¿Qué protege la ciberseguridad?, ¿datos, equipos, personas?

*La ciberseguridad industrial no solo protege los datos de las empresas, sino también a las personas que trabajan en dichas industrias, sus procesos y los equipos que llevan adelante las operaciones.*

*Además, protege infraestructura de tecnologías de Información como los centros de datos, como la infraestructura que gestiona iluminación y aire acondicionado y en general infraestructura industrial que permiten la operación.*

*"Piense en esto: las fábricas inteligentes de hoy en día tienen cientos, e incluso miles, de sensores conectados. Es por esto que se requiere adoptar un enfoque holístico de la ciberseguridad".*

¿Qué papel juegan los dispositivos industriales en la ciberseguridad?, ¿protegen, hay que protegerlos?

*La seguridad no puede ser un pensamiento posterior, debe estar en el centro de las operaciones. En Schneider Electric consideramos la seguridad desde cero, utilizando componentes que cumplen con estándares reconocidos. EcoStruxure es nuestra arquitectura de sistema abierta e interoperable, habilitada para IIoT y centrada en el valor. Ayuda a las empresas*

*a pasar de maximizar solo la eficiencia del proceso al control, en tiempo real, de otras variables comerciales importantes, incluido el riesgo de ciberseguridad, el riesgo de seguridad (incluidos los riesgos ambientales), el riesgo de confiabilidad y, lo que es más crítico, la rentabilidad operativa.*

¿Cuáles son los desafíos actuales de la ciberseguridad industrial?

*Muchas empresas llevan años en el mercado y aseguran no haber realizado una consultoría de ciberseguridad nunca en su vida. Es esencial pasar de la reacción a la planificación y prevención proactivas específicamente para fortalecer la ciberseguridad industrial. El riesgo es demasiado grande para ignorarlo.*

*Algunos pasos recomendados incluyen los siguientes:*

- *segmentación de la red;*
- *políticas para modelos operativos y personas;*
- *planes y medidas para evitar el efecto cascada;*
- *asegurar la infraestructura heredada; y*
- *asumir* la responsabilidad compartida.

*Según una encuesta de Accenture, el 79% de los directores ejecutivos dice que su organización está "adoptando tecnologías nuevas y emergentes más rápido de lo que pueden abordar los problemas de seguridad relacionados".*

¿Cuáles son las estrategias actuales para defenderse de los ciberataques?

*Schneider ofrece asesoramiento y, además, productos específicos para proteger los procesos contra ataques externos. Específicamente, el Modicon M580 ePAC permite a las industrias proteger sus accesos contra ataques gracias a la comunicación encriptada y asegurando un alto nivel de trazabilidad con su fácil configuración.*

*Como decimos en Schneider Electric, cualquier estrategia de ciberseguridad es tan fuerte como su eslabón más débil. Por eso, es fundamental identificar y mitigar riesgos aplicando soluciones de ciberseguridad 360, que fortalezcan nuestra seguridad de punta a punta y las buenas prácticas en cada uno de los eslabones de la cadena.*

*Una de las medidas clave de prevención es la debida respuesta. ¿Cuáles son las lecciones aprendidas de todos y cada uno de los ataques? ¿Cómo podemos fortalecer el ecosistema digital? El ataque de ransomware Wannacry en 2017, por ejemplo, fue sorprendente mucho más allá del incidente, ya que finalmente reveló que todos los actores industriales necesitaban trabajar juntos para garantizar un camino hacia la seguridad en el mundo industrial. La necesidad de una colaboración ardiente llevó a Schneider Electric a convertirse en miembro fundador de la ISA Global Cybersecurity Alliance, por ejemplo, así como de la Coalición de Ciberseguridad.*

> *"La ciberseguridad industrial no solo protege los datos de las empresas, sino también a las personas que trabajan en dichas industrias, sus procesos y los equipos".*

¿Puede relatar y analizar algún caso concreto de aplicación?

*Hemos trabajado con clientes de diferentes segmentos en la construcción y validación de su estrategia de ciberseguridad. Con algunos de ellos comenzamos realizando un asesoramiento, con el objetivo de identificar el nivel de madurez de su organización.*

*Con base en los hallazgos y determinadas las prioridades de cada punto, planteamos una serie de soluciones y servicios con el objetivo de minimizar los riesgos operativos y posibles ataques cibernéticos. De la misma manera, acompañamos a algunas compañías en la construcción de soluciones a temas puntuales como, por ejemplo: manejar accesos remotos, tener visibilidad permanente de las diferentes amenazas a las que están expuestos los diversos sistemas de control, entre otros.*