Publicado en Madrid el 10/10/2019

# [Ciberseguridad industrial: el coste de no tomar las medidas adecuadas](http://www.notasdeprensa.es)

## Secure informa de que las pérdidas por ciberdelitos en industria se han duplicado en los últimos dos años. No tomar las medidas adecuadas puede suponer un coste incalculable para las industrias

 Los sistemas industriales y la tecnología operativa (también conocida como OT, por sus siglas en inglés) están cada vez más conectados y esto supone un aumento exponencial de las ciberamenazas en la industria. Los equipos de automatización industrial han heredado las tecnologías de la informática corporativa y, con ellas, sus problemas en lo que a seguridad de la información se refiere. La transformación del entorno industrialA lo largo de la historia, se han conocido multitud de vulnerabilidades, asociadas tanto al hardware como al software que componen los sistemas de control industrial (Industrial Control System o ICS). Lo cierto es que esas vulnerabilidades no son nuevas, siempre han estado ahí, pero se asumían porque había poca probabilidad de que fueran explotadas. El motivo era sencillo: los sistemas estaban aislados. En lo que a seguridad se refiere, podemos decir que en los ICS se ha primado la disponibilidad y la funcionalidad (las tecnologías de la información tratan de priorizar la confidencialidad de los datos por encima de otros aspectos). Pero, no se puede seguir en esa línea; el hecho de no tomar las medidas adecuadas puede suponer un coste incalculable para las industrias. En la Industria 4.0 esta tendencia cambia; cada vez más dispositivos de control industrial utilizan tecnologías de la información (TI) genéricas: interfaces y protocolos estándar; PCs o sistemas operativos como Windows o Linux. Con ellas, se heredan también sus vulnerabilidades. Y, no solo se heredan, se agravan, porque en estos entornos no es sencillo realizar paradas, ni siquiera para llevar a cabo el mantenimiento, la actualización, el parcheado o el aislamiento de los sistemas de control. El hecho de que los entornos industriales estén conectados los hace más vulnerables y, por tanto, los convierte objetivo de los ciberdelincuentes. De hecho, algunas encuestas revelan que las pérdidas por ciberdelitos se han duplicado en los últimos dos años y las ciberamenazas se sitúan en primer plano de las preocupaciones del sector. A este ámbito afectan también el ciberespionaje (por motivos económicos o políticos, entre otros) o el ciberterrorismo. En general, proteger o securizar los sistemas industriales es más complejo. Hay una falta de convergencia entre las tecnologías; existe una falta de seguridad en las fases iniciales de diseño de los sistemas; tienen un ciclo de vida elevado; es difícil detener los sistemas para aislarlos, actualizarlos, parchear, etc.; entre los expertos en la operación suele haber desconocimiento ante ciberamenazas o ciberseguridad y, por todo ello, son de más fácil acceso. En definitiva, las amenazas aumentan. Apoyo de expertosLos ciberdelincuentes han puesto sus miras en la industria, por eso, es importante que los responsables de las compañías tomen conciencia y apuesten por la ciberseguridad industrial como una inversión. El hecho de contar con una empresa especializada en esta materia aporta importantes beneficios: sistemas protegidos, configurados y gestionados; continuidad de procesos y de negocio; garantía de cumplimiento normativo; anticipación, mitigación de los potenciales riesgos; implementación de nuevos métodos y procedimientos de Seguridad Industrial, y mejora de la imagen e incremento del prestigio ante terceros. Algunas administraciones públicas (entre ellas las de la Comunidad de Madrid o el Gobierno Vasco) subvencionan proyectos de ciberseguridad en industria, llegando incluso a cubrir el 50 por ciento del gasto. Pero, es importante contar con el apoyo de una compañía especializada: permite conocer el estado de tu infraestructura, detectar riesgos, comprobar la eficacia de los controles que se aplican, elaborar e implantar un plan estratégico, llevar a cabo iniciativas para la concienciación y la formación de la plantilla en materia de ciberseguridad y, además, seguir un proceso de mejora continua. Secure and IT ha creado escenarios de simulación de ataque, para que las compañías puedan comprobar cómo afectan a la disponibilidad. De esta forma, los usuarios pueden conocer de primera mano qué aporta la ciberseguridad industrial a las organizaciones y cómo hay que defenderse de los ataques.

**Datos de contacto:**

Comunicación Secure

911 196 995

Nota de prensa publicada en: [https://www.notasdeprensa.es/ciberseguridad-industrial-el-coste-de-no-tomar](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorias: Telecomunicaciones E-Commerce Ciberseguridad Otras Industrias



[**http://www.notasdeprensa.es**](http://www.notasdeprensa.es)