Tendencias en ciberseguridad

Ciberseguridad en Sistemas de Control Industrial: ICS/SCADA

La complejidad de los sistemas ICS/SCADA radica principalmente en su **naturaleza multidisciplinaria** y en la amplia variedad de sectores que utilizan estos sistemas industriales. Por ello, surge la tendencia centrada en la necesidad de implantar altos niveles de ciberseguridad en los sistemas SCADA, basándose en la comprensión del **riesgo de negocio**, la implementación de una arquitectura segura, establecimiento de **capacidades de respuesta** frente amenazas, concienciación de seguridad en el control de procesos dentro de las propias organizaciones y definición de una dirección permanente en los marcos de gobierno.

ORIGEN DE LA TENDENCIA

ECONÓMICO/EMPRESARIAL | DEMANDA | NORMATIVA | **TECNOLOGÍA**

Entre 1982 y 2001, sólo el 29% de los incidentes de seguridad en ICS se habían catalogado como externos. Sin embargo, el informe Control Systems Cyber Security Awareness de 2005 (US-CERT) analizaba que, entre los años 2002 y 2004, el 66% de los incidentes de seguridad ocurridos con sistemas SCADA se debían a ataques externos. Este incremento se debió principalmente a que los sistemas SCADA comenzaron a trabajar con **tecnologías y protocolos estándar**. Como estos sistemas suelen estar distribuidos geográficamente. se conectan a centros de control mediante tecnologías y protocolos estándar que a su vez suelen estar conectados a la red corporativa de la empresa. Por este motivo la preocupación por la seguridad de los sistemas SCADA ha sido creciente. Algunos ejemplos son las **nuevas normativas, certificaciones (ENISA), instituciones (CCI),** etc. Además, dentro de la protección de infraestructuras críticas, la protección de los sistemas ICS/SCADA es un punto clave.

UBICACIÓN EN LA CADENA DE VALOR DE LA CIBERSEGURIDAD

Fabricación | Comercialización | Servicios

Esta tendencia engloba principalmente a los **fabricantes de productos ICS y de tecnologías**. La incorporación de soluciones y medidas de ciberseguridad afecta tanto a los dispositivos y sistemas que conforman la estructura, como a las redes de comunicaciones que interconectan dichos dispositivos y que, en última instancia, componen el sistema de control industrial.

IMPACTO EN BENEFICIARIOS

USUARIO/PARTICULAR	EMPRESAS	ADMINISTRACIÓN PÚBLICA
Impacto en usuarios ○○○	Impacto en industria ●●○	Impacto en gobiernos ●○○
Las medidas de seguridad en los sistemas industriales repercuten indirectamente en los usuarios de estas redes y servicios industriales, aumentando el **nivel de fiabilidad** dada su capacidad de adaptación a las necesidades del usuario sin perjuicio de la seguridad de sus datos.	El desarrollo tecnológico en seguridad incorporado al sector industrial, y concretamente los **registros de eventos** y el **cifrado de las comunicaciones**, proporcionan a las empresas industriales un mayor soporte y facilitan la producción y control seguro y real de sus procesos.	Las amenazas de ciberseguridad referentes a los **sistemas de control industrial** son un problema para los gobiernos, ya que un ciberataque podría llegar a afectar a la seguridad de plantas de generación de energía o infraestructuras críticas, repercutiendo finalmente en el servicio al ciudadano.

CLASIFICACIÓN DE LA TENDENCIA

SOLUCIONES DE PREVENCIÓN | **SOLUCIONES DE CONTROL** | SOLUCIONES DE MITIGACIÓN

La tendencia trae consigo soluciones concretas de **protección en los procesos de los sistemas ICS/SCADA** y la seguridad en los mecanismos de **conexión y control remoto** a éstos. La toma de medidas de seguridad en dichos sistemas llevan consigo, en gran parte, la detección y mitigación de amenazas externas que pongan en peligro el correcto funcionamiento del sistema.

CICLO DE VIDA DE LA TENDENCIA

DESARROLLO | INTRODUCCIÓN | **CRECIMIENTO** | MADUREZ

Tradicionalmente, los sistemas SCADA se referían a aquellos que supervisaban y controlaban procesos industriales, tratándose de sistemas aislados que permitían una gestión centralizada y eficiente. Sin embargo, este enfoque ha evolucionado y se ha ampliado a lo largo del tiempo. Aparecieron los sistemas SCADA para la monitorización y control de otro tipo de dispositivos y se **eliminó su aislamiento, estando expuestos y conectados a redes externas y públicas como Internet.**

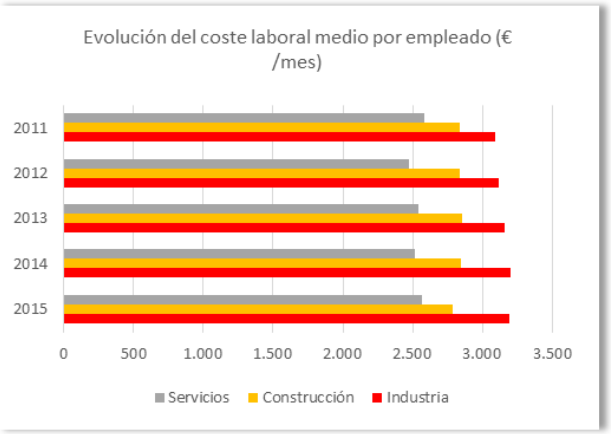
Tendencias en ciberseguridad

Ciberseguridad en Sistemas de Control Industrial: ICS/SCADA

ÁMBITO DE APLICACION

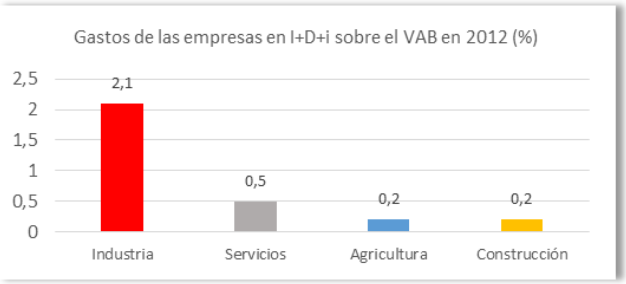
El sector de aplicación de dicha tendencia **es el sector industrial**. Dicha tendencia afecta a cualquier sector de actividad industrial (energía, metalurgia, industrias minerales, industria química, gestión de residuos y aguas residuales, fabricación y transformación de papel y madera, industria alimentaria y de las bebida, tratamiento de productos textiles, fabricación de grafito, etc.) cuyo control de procesos se lleve a cabo mediantes sistemas de control industrial: ICS/SCADA.

CARACTERIZACIÓN DEL SECTOR DESTINATARIO



- De acuerdo a los datos del INE registrados en la tabla anterior, la retribución media a los empleos industriales es un 20% superior a la de otros sectores.

- En 2014, la industria española generó el 17,5% del valor añadido bruto (VAB) total de la economía, mientras que en la zona euro esta cifra se situó en el 19,5%.
- Según Buguroo, sólo el **17% de las empresas industriales en España cuenta con un plan de gestión frente a ciberataques**. Además, un 5,6% de ellas afirma no saber si lo tiene.
- Según datos del Minetur (tabla) el gasto en I+D+i en empresas industriales es superior al gasto empresarial en otros sectores.



PREVISIONES DE DEMANDA

CRECIMIENTO

- Según el informe "*Global Industry Analysis Size Share Growth Trends and Forecast 2015-2021*", el mercado mundial de sistemas de control industrial fue valorado en **58 billones de dólares** en 2014 y se espera que llegue a 81 billones de dólares en 2021. Además en 2014, el **sector de la energía eléctrica** fue el mayor contribuyente en el mercado mundial de controles industriales con una cuota del **18,3%**.

CLIENTES

- Empresas suministradoras de energía: eléctrica, agua, gas, etc.
- Empresas de fabricación industrial: metalurgia, química, alimentaria, madereras, textil, etc.
- Gobiernos y Administraciones Públicas.
- Otras Infraestructuras críticas.

MODELOS DE NEGOCIO

DIFERENCIACIÓN EN COSTE

DIFERENCIACIÓN EN PRESTACION DE SERVICIOS

DIFERENCIACIACIÓN EN VALOR AÑADIDO

CASO DE ÉXITO

KASPERSKY lab

TANECO

- **TANECO es una refinería de petróleo rusa.** El éxito de TANECO está estrechamente relacionado con la continuidad de los procesos de fabricación. La compañía utiliza sistemas de control industrial (ICS) que le permiten obtener ventajas tecnológicas sobre la competencia y reducir al mínimo los costes de producción.
- En este sentido, solicitaron a Kaspersky Lab la implementación de un proyecto para demostrar la funcionalidad de ciberseguridad para estaciones de trabajo de operador/construcción y servidores SCADA en la refinería. Parte del sistema de ciberseguridad también debía supervisar la **integridad de la red industrial** y control de los parámetros críticos del flujo del proceso. Además, dicha solución no debía interferir con el sistema de control industrial existente.