Tendencias en ciberseguridad

Sistemas ciber-resilientes para infraestructuras críticas industriales

Un modelo de gestión de seguridad asentado en la ciber-resiliencia se basa en el diseño de sistemas con capacidad para hacer frente a una **crisis de seguridad** sin que su actividad se vea afectada. Dado que la destrucción o perturbación de cualquier infraestructura estratégica o crítica cuyo funcionamiento es indispensable tendría graves consecuencias sobre servicios esenciales, dichas infraestructuras críticas, especialmente aquellas industriales y que operan en el **sector energético**, requieren de soluciones ciber-resilientes con una alta especialización en el sector objetivo y que reduzca posibles riesgos de seguridad.

ORIGEN DE LA TENDENCIA

ECONÓMICO/EMPRESARIAL | DEMANDA | NORMATIVA | TECNOLOGÍA

En la UE y España, el desarrollo normativo de las Infraestructuras Críticas parte de la Directiva EC 114/2008 sobre identificación y designación de Infraestructuras Críticas Europeas a partir de la que se aprueba la **Ley 8/2011 y el Real Decreto 704/2011 sobre Protección de Infraestructuras Críticas**. La **Estrategia de Ciberseguridad Nacional** establece 7 líneas de actuación estratégicas con el objetivo de mejorar la seguridad de las infraestructuras críticas entre las que se encuentra la resiliencia. En 2016, el Gobierno ha aprobado el nuevo **Plan de Protección de las Infraestructuras Críticas**. En normativa internacional, destaca la Orden Ejecutiva 13636 y la Directiva de Política Presidencial 21 de EEUU, que destaca la necesidad de aplicar los principios de resiliencia en dichas infraestructuras ante ciberataques. Alcanzar ciber-resiliencia ha de ser un objetivo tanto del Estado como empresarial, se debe garantizar un entorno estable entre entidades públicas y privadas.

UBICACIÓN EN LA CADENA DE VALOR DE LA CIBERSEGURIDAD

Fabricación → Comercialización → Servicios

Esta tendencia afecta, principalmente, a los **fabricantes de tecnologías diseñada específicamente para el desarrollo de sistemas de gestión de infraestructuras críticas**. Además, los principales servicios demandados por las infraestructuras críticas son soluciones industriales integrales, con una alta especialización en el sector.

IMPACTO EN BENEFICIARIOS

USUARIO/PARTICULAR	EMPRESAS	ADMINISTRACIÓN PÚBLICA
Impacto en ciudadanos ○○○	Impacto en suministradores ●●○	Impacto en gobiernos ●○○
Las medidas de seguridad en las infraestructuras críticas industriales repercuten en los usuarios de éstas en la eficacia y calidad en el suministro del servicio. Los sistemas ciber-resilientes en dichas infraestructuras previenen del colapso de los **servicios ciudadanos esenciales** asociados.	El desarrollo tecnológico en seguridad incorporado al sector industrial, y concretamente los **registros de eventos** y el **cifrado de las comunicaciones**, facilitando a los proveedores industriales y a los operadores críticos la producción y control de sus procesos.	La gestión de la ciber-resiliencia desde los gobiernos, repercute en un impulso administrativo y legislativo hacia los operadores críticos estableciendo una barrera de seguridad en los servicios públicos. Generan un ámbito de actuación y confianza ante amenazas relacionadas con la ciber-seguridad.

CLASIFICACIÓN DE LA TENDENCIA

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

Dada la característica ciber-resiliente, el sistema industrial de control y operación de la infraestructura crítica debería **mitigar y adaptase a los problemas de ciberseguridad detectados**, continuando con la actividad habitual del servicio asociado. Asimismo, la utilización estos sistemas cuenta con una componente preventiva de detección previa de dichos riesgos.

CICLO DE VIDA DE LA TENDENCIA

DESARROLLO | INTRODUCCIÓN | **CRECIMIENTO** | MADUREZ

La protección de las infraestructuras críticas aparece en el debate sobre la seguridad nacional española a partir del impulso dado por las iniciativas de la Unión Europea, a través, de la aprobación de la **Comunicación del 20 de Octubre de 2004** sobre Protección de las infraestructuras críticas en la lucha contra el terrorismo y de la **Directiva 2008/114/CE del Consejo** sobre La identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.

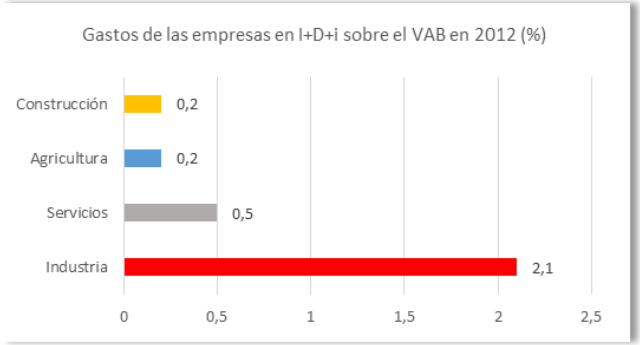
Tendencias en ciberseguridad

Sistemas ciber-resilientes para infraestructuras críticas industriales

ÁMBITO DE APLICACION

Los distintos sectores o ámbitos de aplicación de dicha tendencia vienen definidos en el Catálogo Nacional de Infraestructuras Críticas que está compuesto por empresas, instalaciones e infraestructuras agrupadas en los siguientes 12 sectores: **Energético**, Tecnologías Información (TIC), Transportes, **Hídrico**, Salud, **Alimentación**, Finanzas, **Nuclear, Químico, Investigación, Espacial** y Administración, entre los que mayoritariamente se hace referencia a sectores que conforman el sector industrial nacional.

CARACTERIZACIÓN DEL SECTOR DESTINATARIO



- 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, en 5,6% de ellas afirma no saber si lo tiene.
- Según datos del Ministerio de Industria, Energía y Turismo (tabla) el gasto en I+D+i en empresas industriales es superior al gasto empresarial en otros sectores.

- Según datos del Ministerio del Interior, el balance de los últimos cuatro años en materia de seguridad de infraestructuras públicas es el siguiente:
  - ❑ Por una parte, se han nombrado **93 operadores críticos y se han identificado más de 300 infraestructuras críticas** de sectores como la energía, la industria nuclear, el sistema financiero, el transporte y el agua.
  - ❑ Por otra parte, se hn multiplicado los instrumentos de planificación con la puesta en marcha de **10 planes estratégicos sectoriales.**

PREVISIONES DE DEMANDA

CRECIMIENTO

- El Centro de Respuesta a Incidentes de Seguridad e Industria (Certsi) gestionó en 2015, **50.000 incidencias de ciberseguridad**, de las que 134 iban dirigidas contra infraestructuras críticas de España, lo que supone el triple de casos que en 2014, que ya registró el doble que 2013.
- Está previsto que a lo largo de 2016 los ciberataques asciendan a **100.000**, de los cuales, 300 serían contra infraestructuras críticas.

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

S21sec

cuevaaliente ingenieros

- **S21Sec y Cuevavaliente**, ofrecen servicios necesarios para la creación de un **sistema de gestión de la seguridad corporativa que le permite el cumplimiento de la normativa vigente en materia de protección de infraestructuras críticas.**
- Ayudan al operador en la definición de las estrategias más adecuadas para la gestión integral de la seguridad en aquellas infraestructuras definidas como críticas por el CNPIC.
- Los servicios ofertados en común son: un sistema de gestión de la seguridad corporativa, análisis integral de riesgos, plan director de seguridad integral, definición del plan de seguridad del operador (PSO) y de los planes de protección específicos (PPE) y formación específica.