## Tendencias en ciberseguridad

# *Protección de las redes industriales inteligentes y Smart Grids*

La necesidad de protección de las redes de sensores industriales radica en **protocolos de autenticación, cifrado de conexiones M2M, eliminación de redundancias y procesado seguro de datos cifrados** como medidas de seguridad en las redes de sensores industriales. Las Smart Grids y las redes de sensores interconectadas inalámbricamente son susceptibles de sufrir ataques contra su configuración. Dependiendo del escenario de aplicación, éstas requieren la protección de seguridad basada en la **integridad, disponibilidad, confidencialidad, no repudio y privacidad de sus datos.**

## ORIGEN DE LA TENDENCIA

| ECONÓMICO/EMPRESARIAL | DEMANDA | NORMATIVA | TECNOLOGÍA |
|---|---|---|---|

La **Estrategia Europa 2020** contempla la necesidad de un uso más eficiente de la energía en las economías modernas a través de sistemas inteligentes y define unos objetivos a cumplir en el 2020: reducir las emisiones de gases de efecto invernadero en un 20%, alcanzar el 20% de fuentes renovables en el consumo energético de la UE y un 10% en el sector del transporte, y aumentar la eficiencia energética con el fin de ahorrar un 20% del consumo energético de la UE. Asimismo, surge la demanda de nuevos y mejorados servicios, que permitan adecuar la tarificación en tiempo real y la libertad para elegir los suministradores energéticos de acuerdo al **nuevo modelo eléctrico en el que se producen grupos de generación más pequeños y cercanos a los consumidores** (generación distribuida), con los que se logra una mejoría en los flujos energéticos. Esos sistemas inteligentes y conectados requieren la garantía del cumplimiento de unos estándares de seguridad y protección.

## UBICACIÓN EN LA CADENA DE VALOR DE LA CIBERSEGURIDAD

**Fabricación** → Comercialización → Servicios

Esta tendencia engloba, principalmente, a los **fabricantes de componentes electrónicos y proveedores tecnológicos**. La incorporación de soluciones y medidas de ciberseguridad afecta tanto en los dispositivos y sensores, como a las redes de comunicaciones que interconectan dichos dispositivos y que, en última instancia, conforman las Smart Grids.

## IMPACTO EN BENEFICIARIOS

| USUARIO/PARTICULAR | EMPRESAS | ADMINISTRACIÓN PÚBLICA |
|---|---|---|
| Impacto en usuarios ● ○ ○ | Impacto en suministradores ● ● ○ | Impacto en gobiernos ● ○ ○ |
| Las medidas de seguridad en las redes inteligentes industriales o de medidores energéticos repercuten en los usuarios de la red, aumentando el **nivel de fiabilidad y calidad** en el suministro de energía eléctrica, **protegiendo la seguridad e integridad** de sus datos personales como usuario. | Para las empresas suministradoras, la gestión en seguridad de las redes inteligentes ofrece una oportunidad de **mejora de la gestión del fraude y errores energéticos** y como consecuencia, aumenta la eficacia y flexibilidad en la distribución de los flujos de energía. | Los suministradores energéticos se consideran **infraestructuras críticas**, desde el punto de vista estratégico del país, por lo que la protección y **garantía de seguridad física y lógica** de los sistemas energéticos es una prioridad para gobiernos y administraciones públicas. |

## CLASIFICACIÓN DE LA TENDENCIA

SISTEMAS DE PREVENCIÓN | **SISTEMAS DE CONTROL** | SISTEMAS DE MITIGACIÓN

La tendencia trae consigo soluciones concretas de **protección de los dispositivos**, en su mayoría sensores o medidores, o la seguridad en las aplicaciones de **conexión y control remoto a éstos**. Además, la toma de medidas de seguridad contra la manipulación de dichos dispositivos lleva consigo la mitigación y detección de fraude en los flujos energéticos.

## CICLO DE VIDA DE LA TENDENCIA

DESARROLLO | **INTRODUCCIÓN** | CRECIMIENTO | MADUREZ

Debido a la convergencia de los sistemas de control industrial en la generación energética y los sistemas informáticos empresariales dentro de las Smart Grid o la Industria 4.0, los agentes energéticos están comenzando a considerar **el riesgo producido por fallos de seguridad** de los sistemas informáticos tradicionales y su **impacto en los sistemas de control**, que hasta la fecha se encontraban centralizados y aislados.

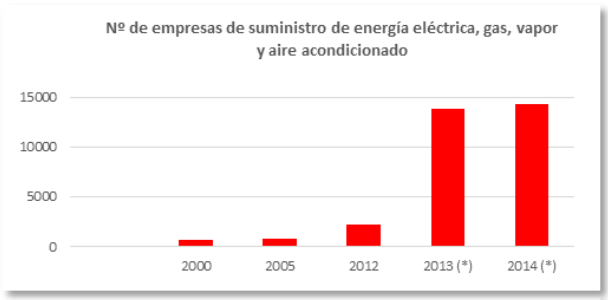
Tendencias en ciberseguridad

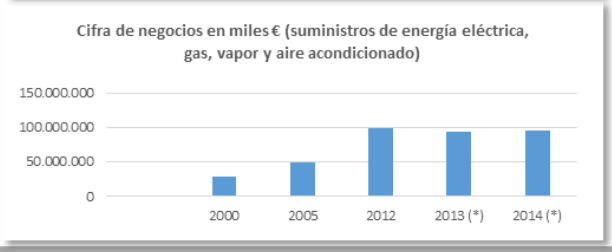
# *Protección de las redes industriales inteligentes y Smart Grids*

## ÁMBITO DE APLICACION

El sector de aplicación de la tendencia es el **sector energético**, concretamente los **operadores energéticos que gestionan redes inteligentes.** La evaluación de los riesgos, así como la identificación de las brechas tecnológicas y problemas de organización son algunos de los principales retos a los que las Smart Grids se enfrentan. Concretamente, la sensibilización y el fomento de la formación y el intercambio de conocimientos son algunas medidas necesarias para brindar seguridad a estas redes.

## CARACTERIZACIÓN DEL SECTOR




- En las últimos décadas, la demanda eléctrica se ha duplicado, la potencia instalada ha crecido dos veces y media y se ha producido una **diversificación tecnológica en la generación**, incorporándose a ella las energías renovables y los ciclos combinados.
- La hoja de ruta marcada por la Agencia Internacional de la Energía (IAE) estima que, sólo en actividades de I+D+i, será necesario invertir más de **10.000 millones de dólares hasta 2050 en el área de las Smart Grids.** Sus aplicaciones mejorarán la eficiencia del sistema eléctrico y aportarán un beneficio de entre 1.100 y 1.800 millones de euros.
- Hasta ahora, sólo el **17% de las empresas industriales en España cuenta con un plan de gestión frente a ciberataques**, según Buguroo.

## PREVISIONES DE DEMANDA

### CRECIMIENTO

- El Plan de Sustitución de Contadores prevé que en 2018, **25 millones de contadores domésticos sean inteligentes**.
- Iberdrola llevará a cabo la sustitución de 10,5 millones de contadores y 90.000 centros de transformación. Endesa ha sustituido el 60% de los contadores del parque actual de 11,6 millones de dispositivos. Gas Natural Fenosa, dispone de un parque de 3,6 millones de contadores que sustituir.

### CLIENTES

- Empresas suministradoras de energía: eléctrica, agua, gas, etc.
- Empresas de fabricación industrial.
- Empresas de telecomunicaciones.
- Gobiernos y Administraciones Públicas.

## MODELOS DE NEGOCIO

DIFERENCIACIÓN EN COSTE

DIFERENCIACIÓN EN PRESTACION DE SERVICIOS

DIFERENCIACIÓN EN VALOR AÑADIDO

## CASO DE ÉXITO

IBERDROLA

- Iberdrola ha impulsado el **proyecto PRIME,** con la intención de desarrollar una **infraestructura de telegestión de contadores de carácter público, abierta y estándar**, cuyo objetivo es el de abordar la dificultad a la hora de lograr una comunicación segura y fiable con los centros de control y de las comunicaciones en tiempo real.
- Las empresas líderes industriales en las áreas de medida, telecomunicaciones y fabricantes de silicio se han unido para el lanzamiento de un nuevo modelo de arquitectura de comunicaciones pública, abierta y no propietaria, que ofrezca soporte a las nuevas funcionalidades de telegestión de contadores y permita avanzar en la construcción de las redes eléctricas del futuro.