Tendencias en ciberseguridad

Protección de los coches inteligentes

La protección de los coches inteligentes hace referencia a la **seguridad en los sistemas de control** de los coches conectados y de los coches sin conductor, así como de **los sistemas inteligentes** que se comunican con éstos. La protección de estos coches tiene en cuenta tecnología que aporte soluciones frente a ataques que comprometan el vehículo y frente a ataques sobre las redes de comunicaciones inalámbricas que comunican a los vehículos a través de un **módulo de comunicación integrado** u otros dispositivos. Estas redes deben protegerse contra el bloqueo de la señal, ataques de denegación de servicio, y la transmisión de datos falsos a los coches conectados y sus conductores.

ORIGEN DE LA TENDENCIA

ECONÓMICO/EMPRESARIAL | DEMANDA | NORMATIVA | TECNOLOGÍA

En la actualidad, un porcentaje muy elevado de clientes elige el coche en función de su **equipamiento en conectividad,** lo que supone un cambio de tendencia respecto a los criterios de compra tradicionales. La conectividad permite intercambiar datos entre vehículos y el entorno, reducir costes, acceder a aplicaciones de entretenimiento, y otros servicios relacionados con la seguridad vial, como el sistema de llamada de emergencia (eCall). Éste último, deberá implantarse en todos los coches fabricados en Europa para 2018, siguiendo las **directrices del Reglamento (UE) 2015/758 del Parlamento y el Consejo Europeo**. En los vehículos autónomos o sin conductor, la ciberseguridad se convierte en una preocupación aún mayor, en el que el **software y la conectividad juegan un papel mucho más crítico para la conducción segura de los vehículos**.

UBICACIÓN EN LA CADENA DE VALOR DE LA CIBERSEGURIDAD

Fabricación → Comercialización → Servicios

La tendencia de protección o seguridad en vehículos inteligentes se orienta hacia el desarrollo y fabricación de soluciones tanto de hardware como de software basadas en soluciones como la firma digital, autenticación, comunicaciones seguras, cifrado, etc.. Estas soluciones se diseñan para proteger las redes de conexión de los vehículos y todos sus elementos asociados y proporcionar una conexión segura a las mismas, quedarían englobadas en la cadena de valor dentro de **fabricación mixta**.

IMPACTO EN BENEFICIARIOS

USUARIO/PARTICULAR	EMPRESAS	EMPRESAS
Impacto en conductores ●●●	Sector de componentes ●○○	Sector de fabricantes ●●○
La protección de: las comunicaciones, los sistemas de infoentretenimiento, los sistemas de seguridad, las app de interactividad con el sistema, etc. tiene como **principales beneficiarios** a los conductores, ocupantes, usuarios o propietarios de los vehículos inteligentes.	La ciberseguridad proporciona al sector de componentes una **herramienta habilitadora** para ampliar y mejorar su cartera de productos a través de la seguridad y protección de datos de los servicios derivados de la instalación de software en el automóvil.	En la adaptación del sector a la era digital, la **seguridad y la eficiencia** son los ámbitos que experimentarán mejoras significativas disminuyendo los riesgos en caso de accidente, facilitando la asistencia a los ocupantes y reduciendo el impacto en su salud.

CLASIFICACIÓN DE LA TENDENCIA

SOLUCIONES DE PREVENCIÓN | SOLUCIONES DE CONTROL | SOLUCIONES DE MITIGACIÓN

La tendencia exige **soluciones concretas de protección de las comunicaciones**, tanto a nivel de los propios componentes internos del vehículo, como del vehículo con su entorno (otros dispositivos, aplicaciones, señales, vehículos, etc), que sepan adaptar su nivel de seguridad a las condiciones dinámicas de cada instante. Además, se incorporan **soluciones de control de acceso y de mitigación** en caso de que el atacante comprometa la seguridad del vehículo.

CICLO DE VIDA DE LA TENDENCIA

DESARROLLO | INTRODUCCIÓN | **CRECIMIENTO** | MADUREZ

En el mercado español, los coches conectados están en un período de crecimiento, siendo ya una realidad en el mercado automovilístico. No obstante, las constantes innovaciones que se producen en este ámbito, justifican que las soluciones de ciberseguridad de los coches conectados se encuentren en **continua evolución**, adaptándose a las nuevas necesidades.

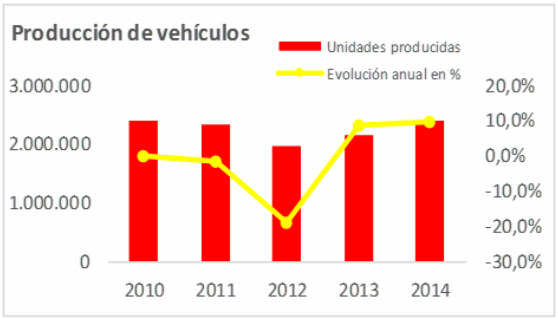
Tendencias en ciberseguridad

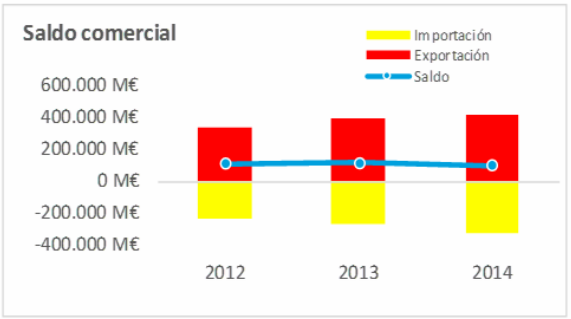
Protección de los coches inteligentes

ÁMBITO DE APLICACION

Coches inteligentes: vehículos conectados a Internet a través de un módulo de comunicación integrado u otros dispositivos, como los smartphones, que ofrece servicios relacionados con la seguridad vial, infoentretenimiento, eficiencia del tráfico (plazas libres, mejores precios de carburantes, tráfico en tiempo real), abaratamiento de costes e interactividad con el sistema, o como los dispositivos smart o wearables que proporcionan perfiles de conducción personalizados según el conductor

CARACTERIZACIÓN DEL SECTOR DESTINATARIO





- La automoción es un **sector estratégico** de la economía española. España es el **segundo fabricante** de coches de Europa sólo por detrás de Alemania, y **noveno del mundo**, además de **liderar la producción de vehículos industriales** en Europa. España cuenta con **17 centros de fabricación de vehículos** distribuidos a lo largo de toda la geografía española y pertenecientes a **10 empresas fabricantes** diferentes.
- El sector de fabricantes de **equipos y componentes** para automoción es un sector muy relevante dentro del panorama industrial español. Tiene un peso fundamental en la cadena de valor del vehículo, ya que aporta en torno al **75% del valor total del mismo**. El sector de los componentes está conformado por empresas principalmente españolas, lo que supone una oportunidad para las empresas de ciberseguridad ya que los centros de decisión están localizados en el país.

PREVISIONES DE DEMANDA

CRECIMIENTO

- La conectividad es hoy en día un elemento importante; en **2018**, y gracias a la introducción del sistema eCall, no habrá en Europa ningún vehículo nuevo sin unidad de comunicación con **módulo SIM integrado**.
- Se estima que el número total de vehículos con conectividad integrada aumentará del 10% del mercado global en la actualidad al **90% en 2020**.

CLIENTES

- Empresas del sector de automoción.
- Empresas del sector de componentes de automoción.
- Empresas del sector de los Integradores de sistemas.
- Empresas del sector de los semiconductores.
- Empresas digitales.
- Compañías de seguros.

MODELOS DE NEGOCIO

DIFERENCIACIÓN EN COSTE | DIFERENCIACIÓN EN PRESTACION DE SERVICIOS | **DIFERENCIACIACIÓN EN VALOR AÑADIDO**

CASO DE ÉXITO

- **IBM** y **Giesecke & Devrient (G&D)** desarrollan conjuntamente una nueva solución de seguridad criptográfica para vehículos conectados, basada en: gestión de identidades de confianza en un entorno seguro; gestión de servicios de confianza para garantizar la seguridad y privacidad de los datos del conductor; gestión de la conectividad altamente flexible con la solución de gestión de suscripciones de G&D.
- Esta nueva solución incluye: **componentes de hardware** altamente protegidos con elementos de seguridad integrados para almacenar claves criptográficas; **soluciones de inteligencia de seguridad** del sistema de administración basadas en centros de operaciones de seguridad, inteligencia de seguridad y gestión de eventos.