



SOLUCIÓN DE CIBERSEGURIDAD APLICADA AL VEHÍCULO CONECTADO

AGENDA

1 Objetivos y enfoque

- 1.1 Objetivos
- 1.2 Enfoque

2 Metodología

- 2.1 Fases del proyecto
- 2.2 Calendario

3 Estado del arte

- 3.1 Tecnologías de comunicación
- 3.2 Marco regulatorio

4 Desarrollo

- 4.1 Estudio del vehículo
- 4.2 Diseño de la solución

5 Prueba de concepto

- 5.1 Definición del caso de uso
- 5.2 Experimento

6 Cierre

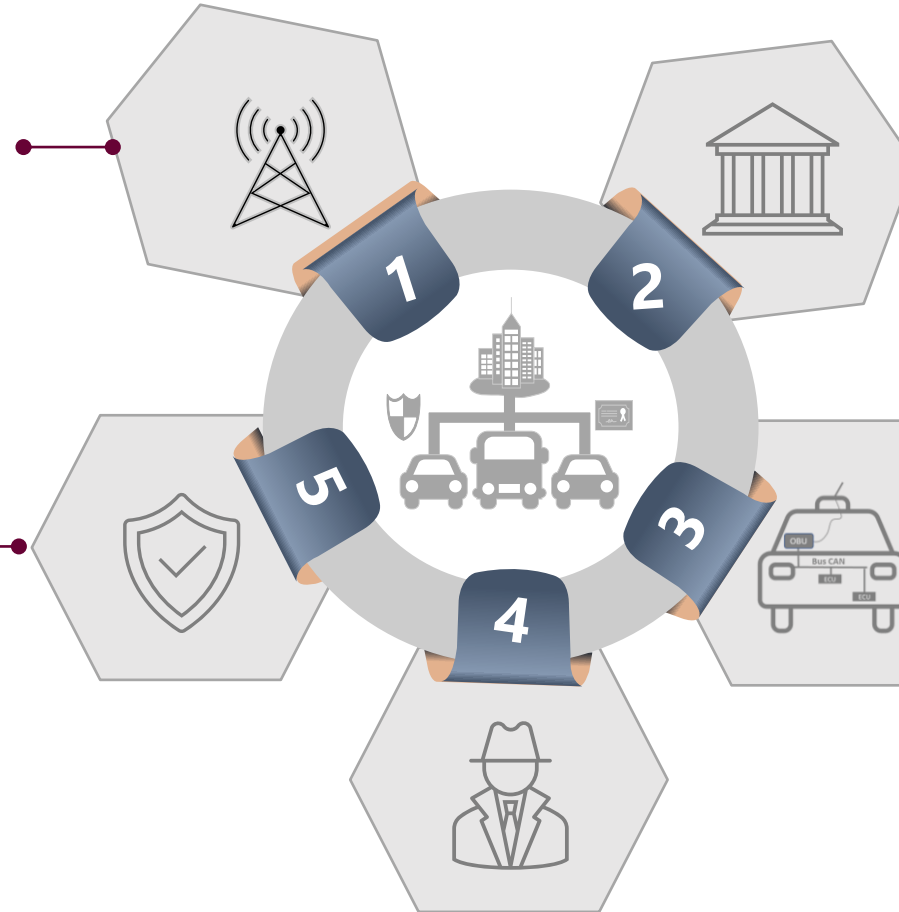
- 6.1 Conclusiones
- 6.2 Próximos pasos

Objetivos y enfoque

Comprender los riesgos de ciberseguridad del Vehículo Conectado, y cómo abordarlos

Tecnologías de comunicación

Análisis de los protocolos DSRC, ITS-G5 y 5G-V2X desde el punto de vista de los riesgos vinculados a posibles intrusiones a través de las comunicaciones.



Marco regulatorio

Estudio de la normativa de seguridad UNECE WP.29, aplicable en la industria del automóvil, sus actuales retos y plazos de cumplimiento.

Solución de ciberdefensa

Evaluación de los requisitos, selección de la tecnología, definición de la arquitectura, e implementación de un caso de uso en el laboratorio.

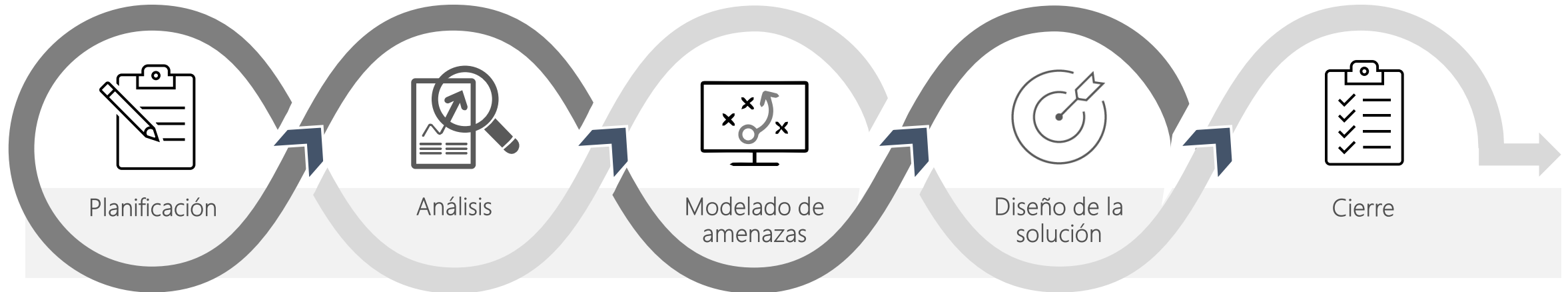
Anatomía del vehículo

Análisis de la arquitectura de comunicaciones inter e intra-vehiculares y sus componentes principales: bus CAN, ECUs y OBU.

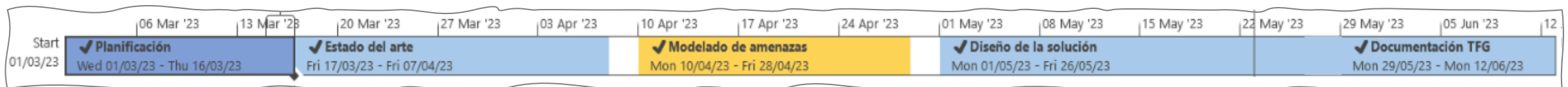
Amenazas de ciberseguridad

Investigación de las posibles vulnerabilidades y amenazas de ciberseguridad, y de las tácticas, técnicas y procedimientos de los adversarios.

Metodología – Fases y actividades



3 semanas	3 semanas	3 semanas	4 semanas	2 semanas
Definición de objetivos, enfoque, alcance y entregables. Elaboración del calendario de trabajo.	Estado del arte de las comunicaciones y del marco regulatorio. Selección de la línea de investigación.	Estudio de vulnerabilidades. Estrategias de gestión de riesgos. Análisis de dos casos de estudio.	Definición de los requisitos. Diseño de la arquitectura. Implementación de un caso de uso.	Elaboración de las conclusiones. Documentación de la memoria. Autoevaluación.

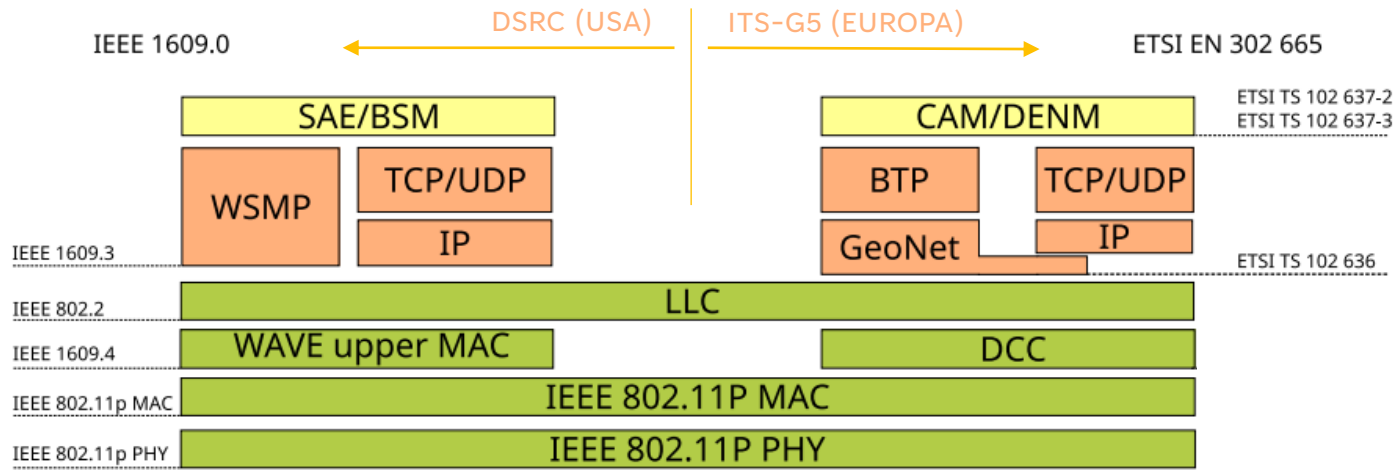


Tecnologías de comunicación v2x

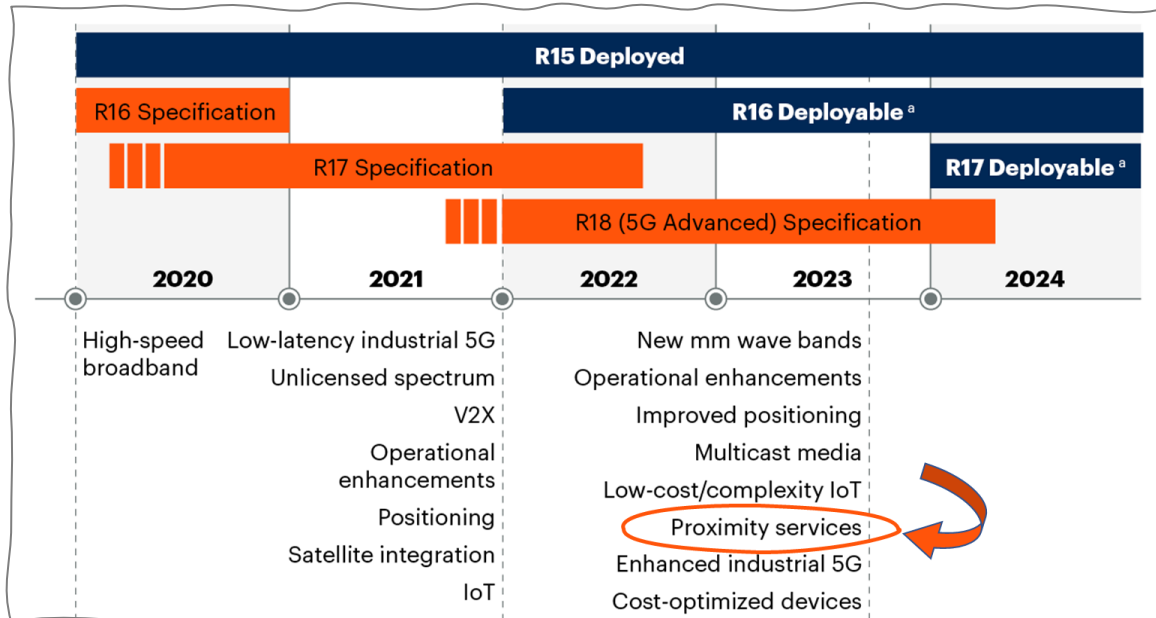


Tecnologías de comunicación V2X

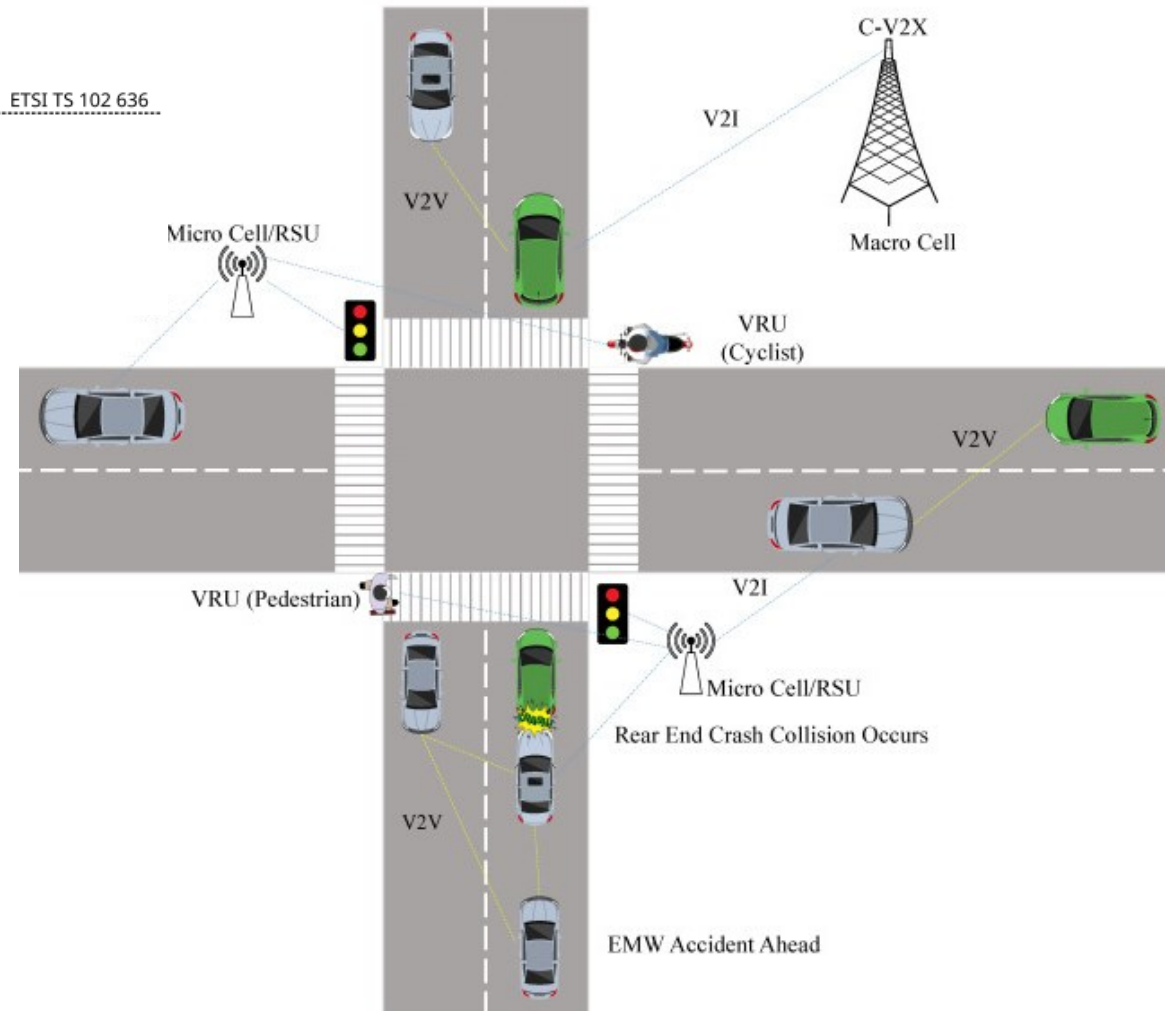
BASADAS EN WIFI



HOJA DE RUTA DEL 3GPP



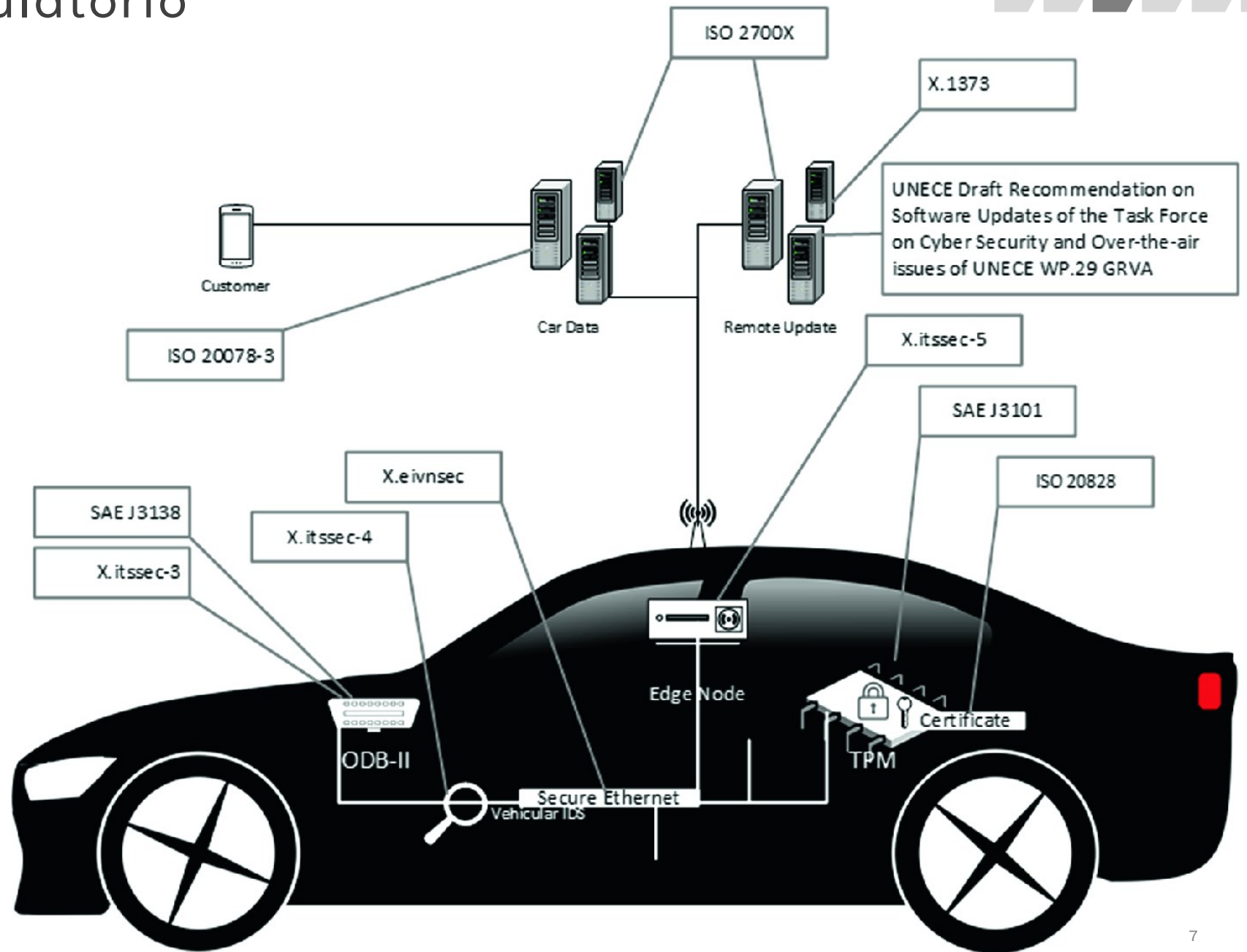
ESCENARIO V2X



Marco regulatorio

A lo largo del tiempo, diferentes organismos (ISO, SAE, ETSI, ITU...) han ido desarrollando distintos grupos de estándares a medida que aparecían nuevos elementos en el ecosistema de los Sistemas Inteligentes de Transporte.

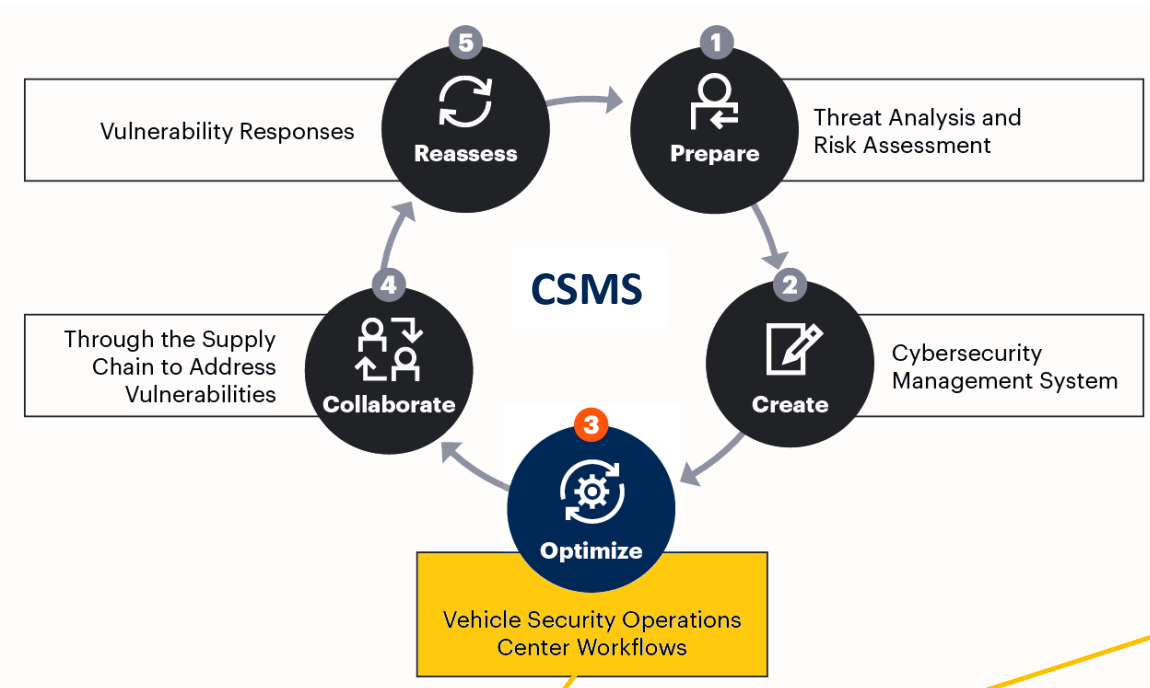
La falta de una regulación global ha provocado carencias y también solapes entre los distintos organismos, y por ese motivo la Comisión Económica de las Naciones Unidas para Europa ha desarrollado nuevos aspectos en su acuerdo **UN ECE WP.29** para la armonización de la reglamentación sobre Vehículos, centrados principalmente en la **implantación de un Sistema de Gestión de la Ciberseguridad**.



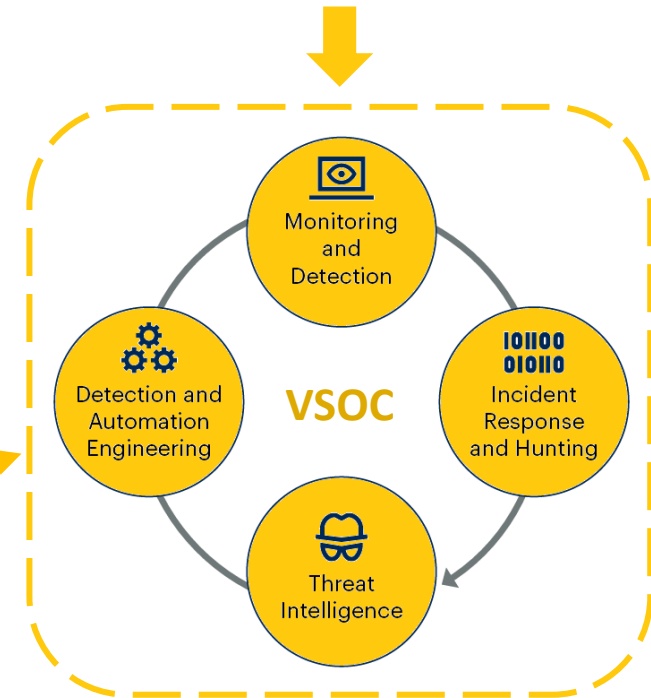
Marco regulatorio

La normativa **UN ECE WP.29** establece 2 requisitos de **cumplimiento obligatorio** para todos los vehículos que se fabriquen a partir de **julio de 2024**:

- **R155 (CSMS)**: Gestión de la ciberseguridad
- **R156 (SUMS)**: Gestión de las actualizaciones del software

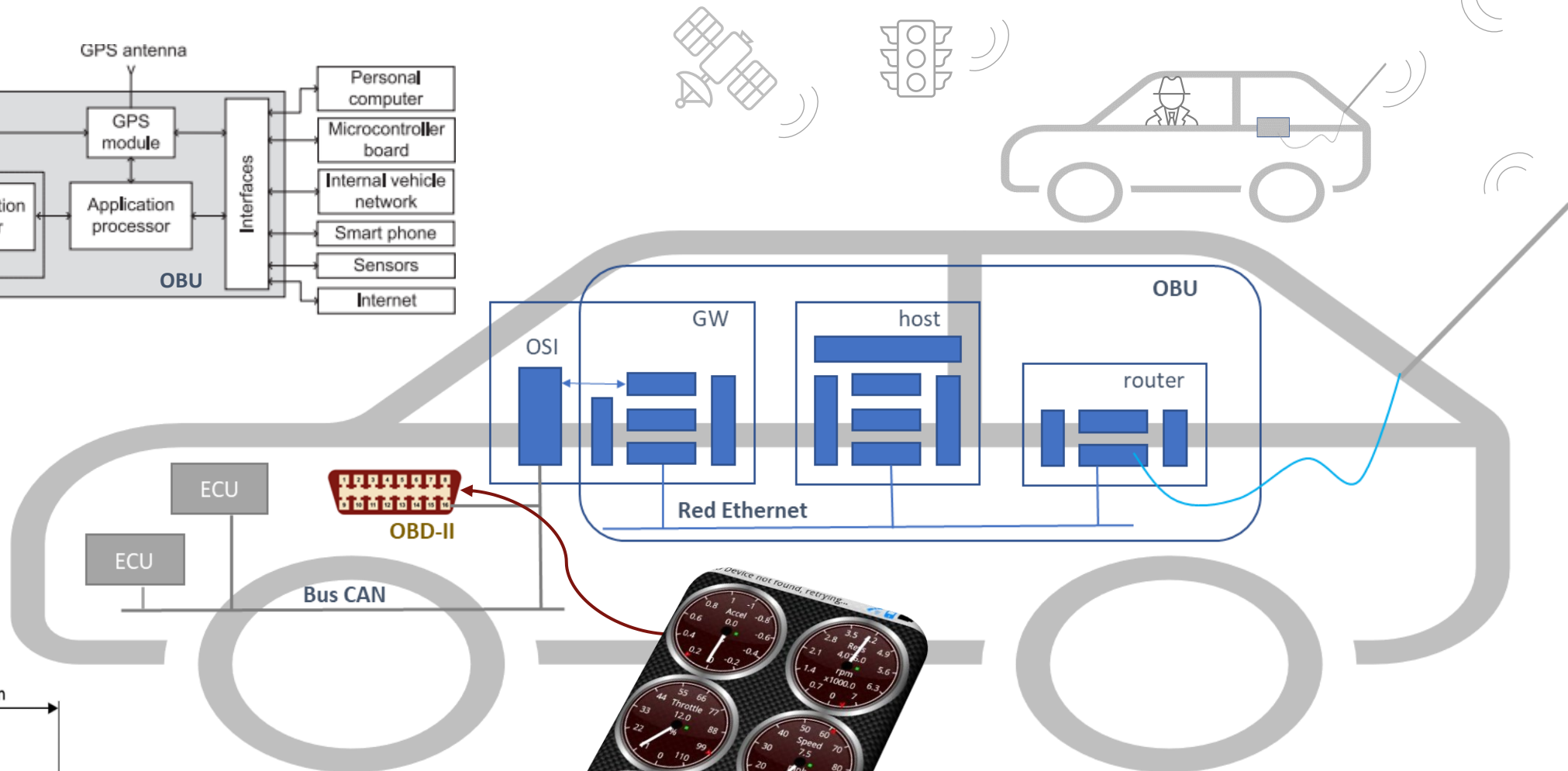
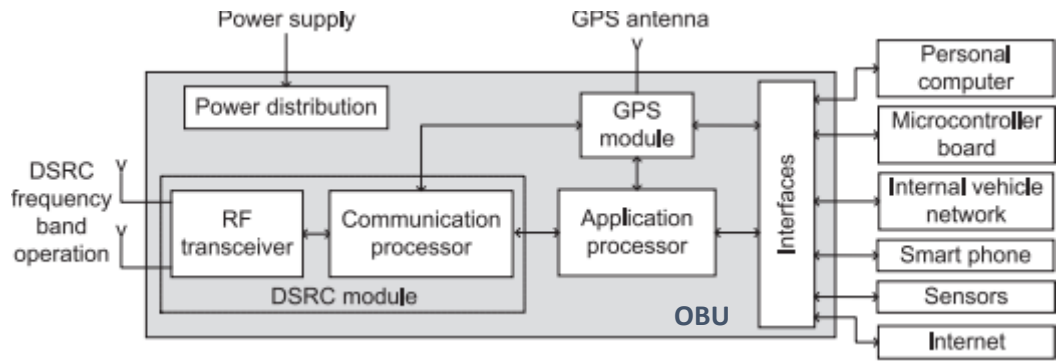


Línea de investigación



“La ciberseguridad es una lucha sin fin, en la que sólo es cuestión de tiempo que una vulnerabilidad llegue a ser explotada.”

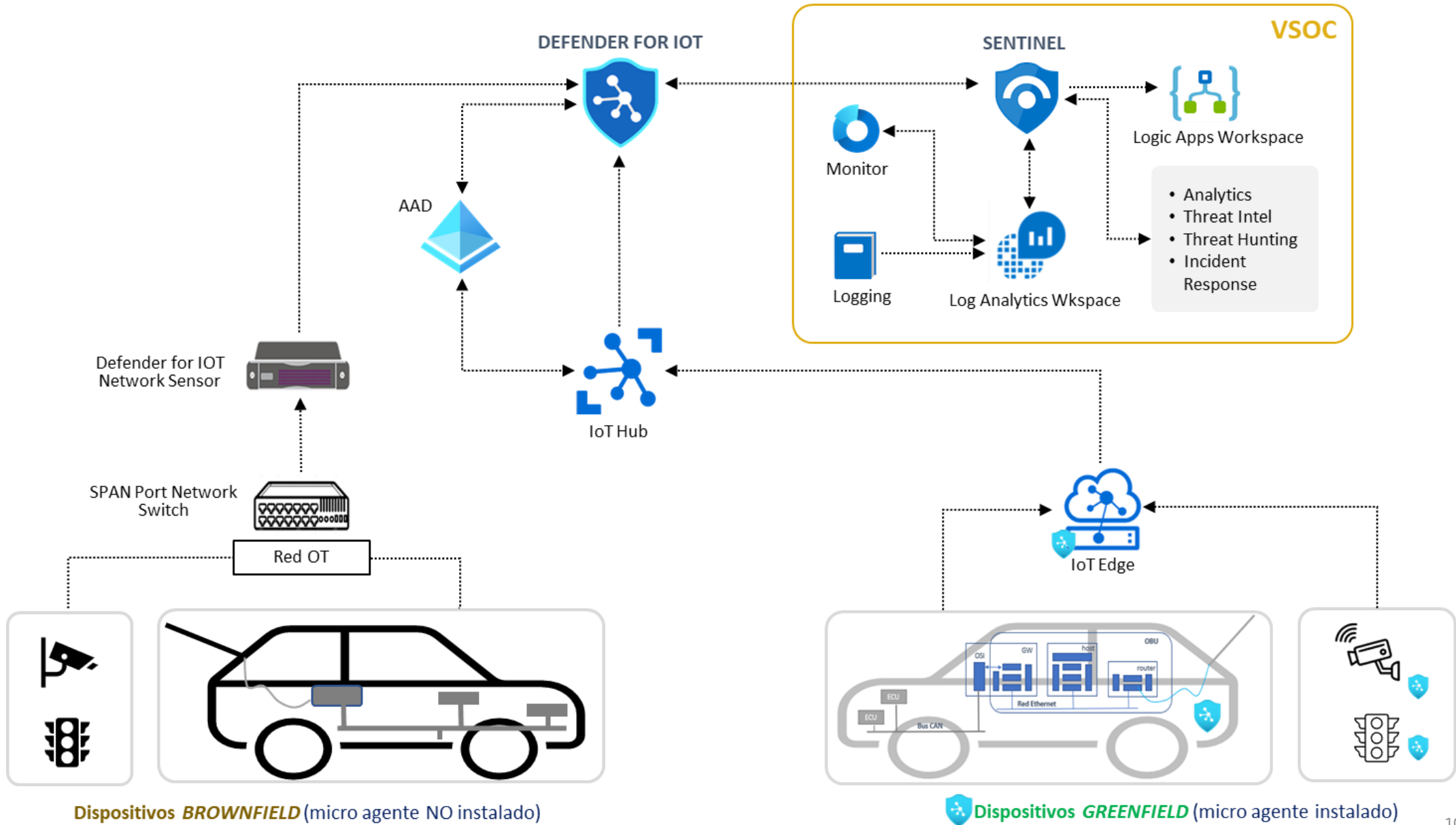
Anatomía del vehículo conectado



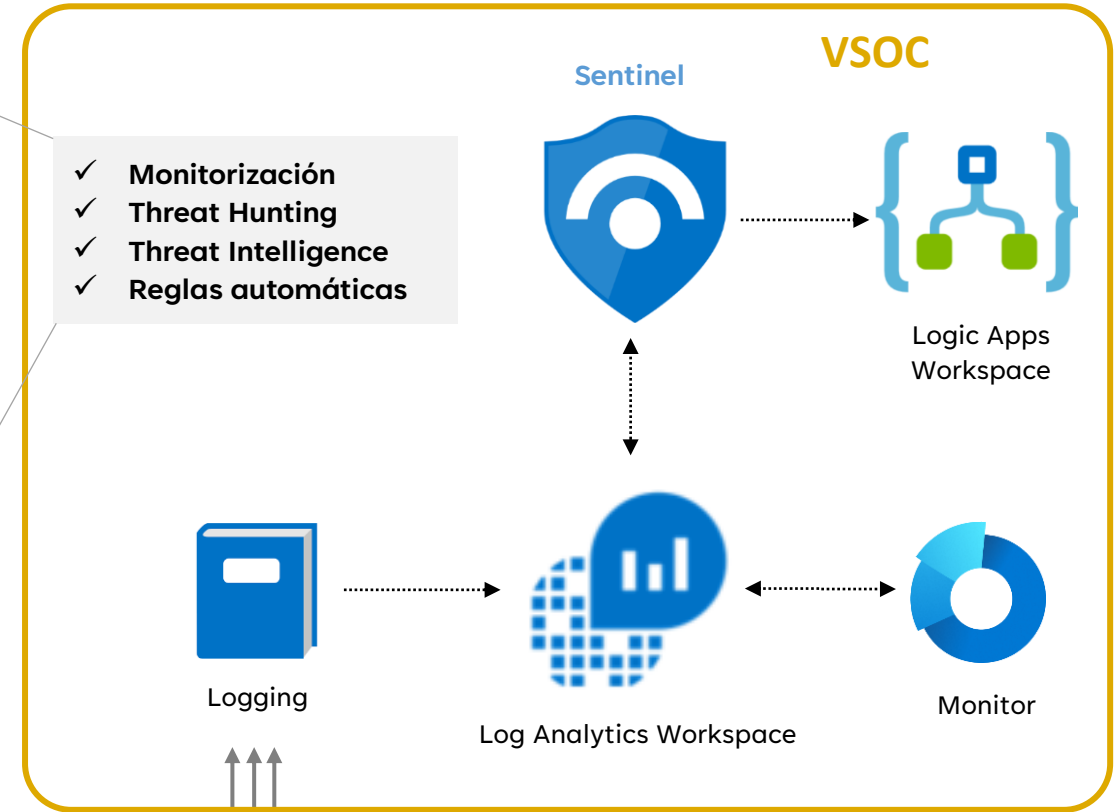
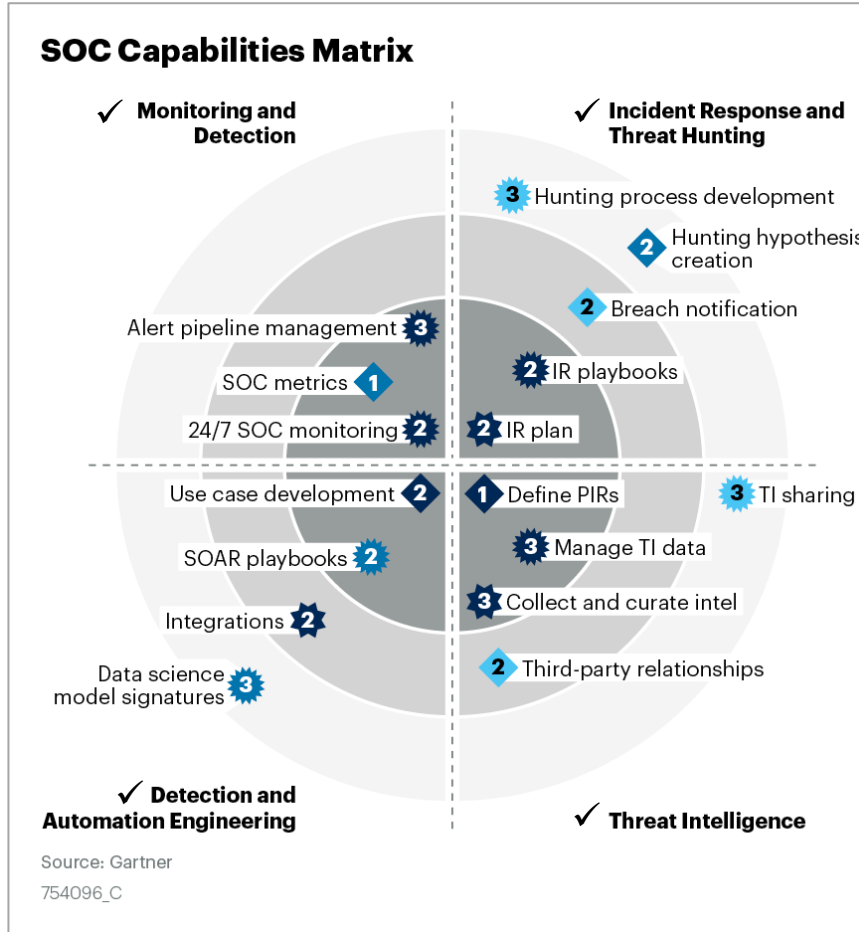
Base Arbitration		Extended Arbitration						
S O F	BASE Identifier	S R R	I D E	Extended Identifier	Control Field	Data Field	CRC Field	ACK Field
1bit	11bit	1bit	1bit	18bit	6bit	0 to 64bit	16bit	2bit



Ecosistema de la solución

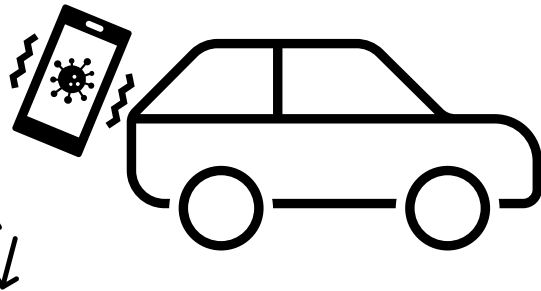


Solución VSOC



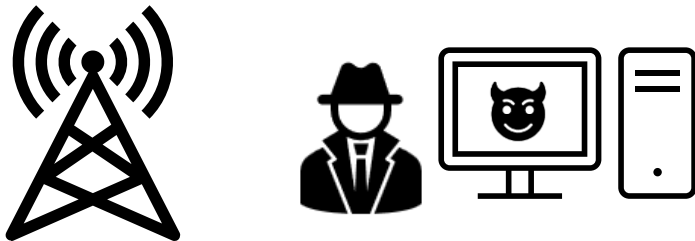
Escenario: Presencia de mensajes maliciosos en la red interna del vehículo

1



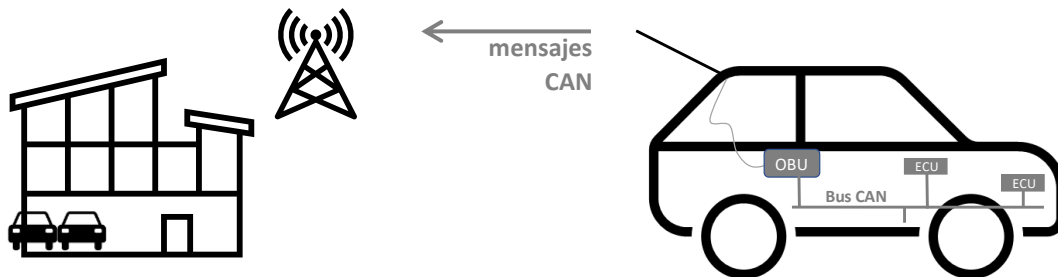
La víctima ha instalado en su smartphone una **aplicación de diagnósticos** sin advertir que es falsa (**maliciosa**). El smartphone infectado se empareja por Bluetooth al conector OBD-II de su vehículo a través de un adaptador ELM327.

2



La aplicación se conecta por Internet a un servicio web malicioso desde el que el atacante puede **obtener información del vehículo** y controlar su comportamiento mediante el **envío de comandos AT**.

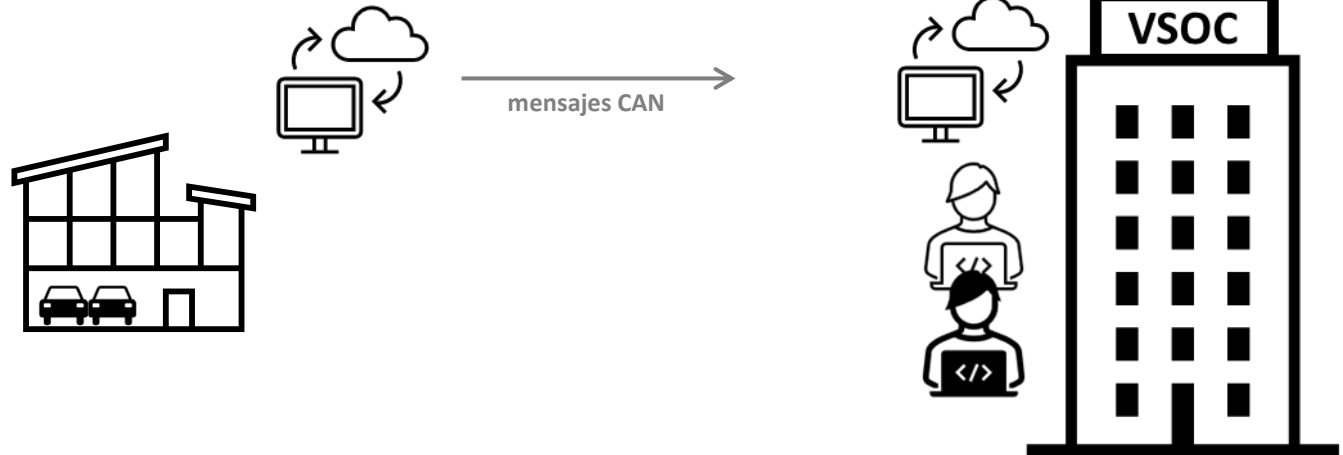
3



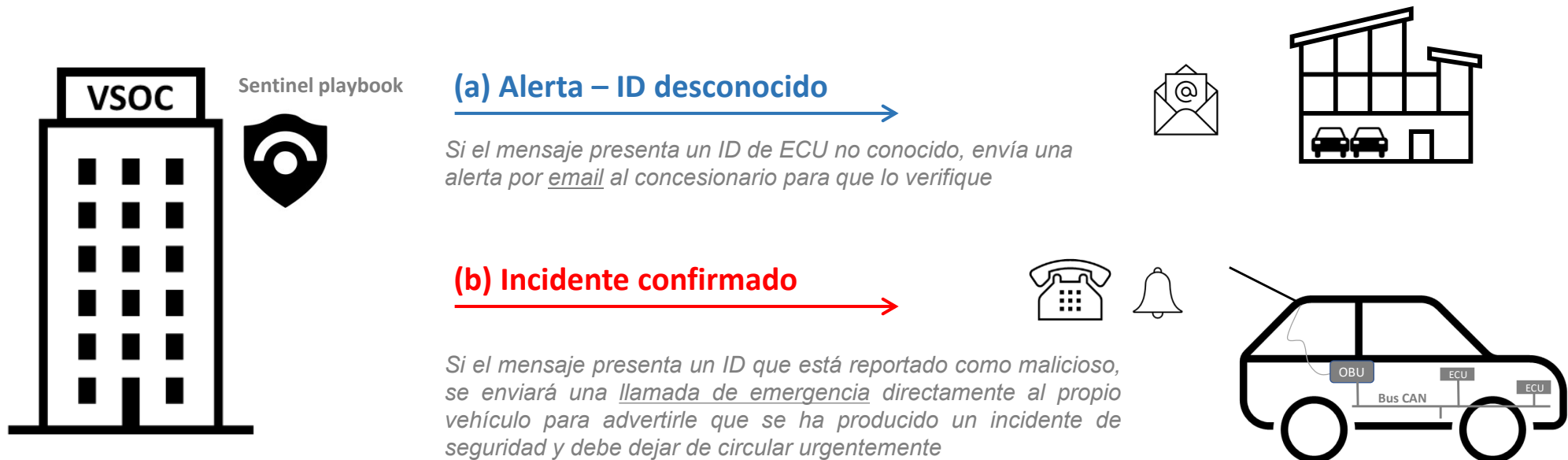
El automóvil incorpora una tarjeta eSIM para conexión telefónica con el concesionario, y le **envía muestras de los mensajes** de diagnóstico que circulan por el bus CAN.

Caso de uso - Solución

1 El concesionario transforma y reenvía en tiempo real al VSOC los mensajes de de la flota.

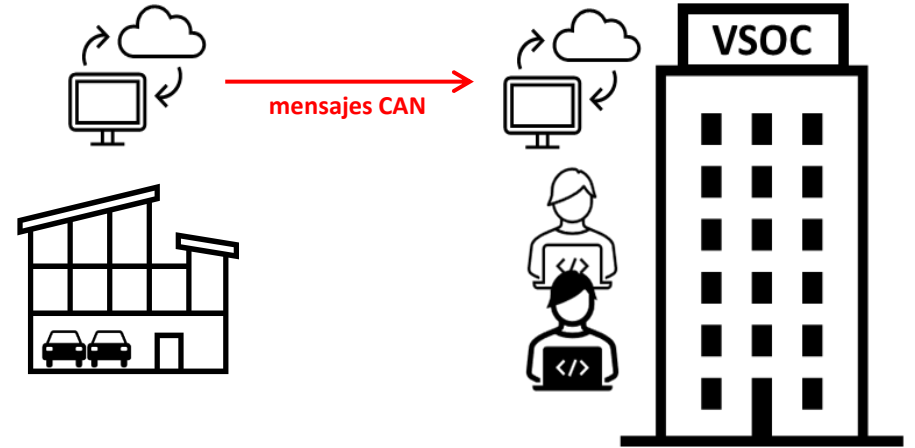


2 El VSOC dispondrá de un automatismo para este caso de uso, y actuará en función del nivel de severidad del incidente.



Experimento (1/4)

Envío de los mensajes CAN desde el concesionario al VSOC



```
Administrator: c:\windows\system32\windowspowershell\v1.0\powershell.exe
PS C:\Users\jordi.nogues\OneDrive\Documentos\UOC\TFG_experimento\ficheros> .\envio_log.ps1
logtype: Log_Concesionarios
[
  {
    "timestamp0": "2023-04-13T22:33:00.000Z",
    "ID_Vehiculo": "Vehiculo001",
    "ID_ECU": "0x123",
    "longitud": 8,
    "datos": ["0x12", "0x34", "0x56", "0x78", "0x9a", "0xbc", "0xde", "0xf0"]
  },
  {
    "timestamp0": "2023-04-13T22:33:01.000Z",
    "ID_Vehiculo": "Vehiculo001",
    "ID_ECU": "0x128",
    "longitud": 8,
    "datos": ["0x12", "0x34", "0x56", "0x78", "0x9a", "0xbc", "0xde", "0xf0"]
  },
  {
    "timestamp0": "2023-04-13T22:33:03.000Z",
    "ID_Vehiculo": "Vehiculo002",
    "ID_ECU": "0x123",
    "longitud": 8,
    "datos": ["0x12", "0x34", "0x56", "0x78", "0x9a", "0xbc", "0xde", "0xf0"]
  },
  {
    "timestamp0": "2023-04-13T22:33:04.000Z",
    "ID_Vehiculo": "Vehiculo002",
    "ID_ECU": "0x333",
    "longitud": 8,
    "datos": ["0x33", "0x34", "0x35", "0x78", "0x9a", "0xbc", "0xde", "0xf0"]
  },
  {
    "timestamp0": "2023-04-13T22:33:05.000Z",
    "ID_Vehiculo": "Vehiculo003",
    "ID_ECU": "0x666",
    "longitud": 8,
    "datos": ["0x66", "0x66", "0x66", "0x78", "0x9a", "0xbc", "0xde", "0xf0"]
  },
  {
    "timestamp0": "2023-04-13T22:33:06.000Z",
    "ID_Vehiculo": "Vehiculo003",
    "ID_ECU": "0x128",
    "longitud": 8,
    "datos": ["0x44", "0x44", "0x56", "0x78", "0x9a", "0xbc", "0xde", "0xf0"]
  }
]
200
PS C:\Users\jordi.nogues\OneDrive\Documentos\UOC\TFG_experimento\ficheros>
```



Microsoft Azure | Search resources, services, and docs (G+)

Home > WK-SentinelDemo

WK-SentinelDemo | Logs

Log Analytics workspace

New Query 1* | Run | Time range: Last 24 hours

WK-SentinelDemo | Select scope | Save | Share

Log_Concesionarios_CL

TimeGenerated [UTC]	timestamp0_t [UTC]	ID_Vehiculo_s	ID_ECU_s	lo...	datos_s
> 4/14/2023, 10:08:19.154 AM	4/13/2023, 10:33:00.000 PM	Vehiculo001	0x123	8	["0x12", "0x34", "0x56", "0x78", "0x9a", "0xbc", "0xde", "0xf0"]
> 4/14/2023, 10:08:19.154 AM	4/13/2023, 10:33:01.000 PM	Vehiculo001	0x128	8	["0x12", "0x34", "0x56", "0x78", "0x9a", "0xbc", "0xde", "0xf0"]
> 4/14/2023, 10:08:19.154 AM	4/13/2023, 10:33:03.000 PM	Vehiculo002	0x123	8	["0x12", "0x34", "0x56", "0x78", "0x9a", "0xbc", "0xde", "0xf0"]
> 4/14/2023, 10:08:19.154 AM	4/13/2023, 10:33:04.000 PM	Vehiculo002	0x333	8	["0x33", "0x34", "0x35", "0x78", "0x9a", "0xbc", "0xde", "0xf0"]
> 4/14/2023, 10:08:19.154 AM	4/13/2023, 10:33:05.000 PM	Vehiculo003	0x666	8	["0x66", "0x66", "0x66", "0x78", "0x9a", "0xbc", "0xde", "0xf0"]
> 4/14/2023, 10:08:19.154 AM	4/13/2023, 10:33:06.000 PM	Vehiculo003	0x128	8	["0x44", "0x44", "0x56", "0x78", "0x9a", "0xbc", "0xde", "0xf0"]

Experimento (2/4)

Definición de la *blacklist*, y creación de la regla

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft Sentinel | Watchlist >

Watchlist wizard

Create new watchlist

General **Source** Review and create

Source type: Local file

File type: CSV file with a header (.csv)

Number of lines before row with header: 0

Upload file *
✓ ECU_blacklist.csv

SearchKey *
ID_ECU

The SearchKey is used to optimize query performance when using watchlists for joins with other data. For example, enable a column with IP addresses to be the designated SearchKey field, then use this field to join in other event tables by IP address. [Learn more and get examples about SearchKey](#)

	A	B	C	D	E	F	G	H
1	ID_ECU_s							
2	0x665							
3	0x666							

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft Sentinel > Microsoft Sentinel | Analytics >

Analytics rule wizard - Edit existing scheduled rule

regla_Vehiculo_infectado

General **1 Set rule logic** **2 Incident settings** **3 Automated response** Review and update

Create an analytics rule that will run on your data to detect threats.

Analytics rule details

Name *
regla_Vehiculo_infectado

Id
4a536064-9a9c-462f-9f19-d699ffe057e9

Description
Esta regla detecta si el vehículo está infectado, es decir, si se ha detectado un identificador de ECU que está denunciado como malicioso en la blacklist.

Tactics and techniques
0 selected

Severity
High

Status
Enabled Disabled

Next : Set rule logic >

Experimento (3/4)



Detección del incidente

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft Sentinel > Microsoft Sentinel | Analytics > Analytics rule wizard - Edit existing scheduled rule >

Logs

WK-SentinelDemo

New Query 1* x New Query 2* New Query 3* New Query 4* New Query 5* New Query 6* New Query 7* + Feedback Queries

WK-SentinelDemo Run Time range: Custom Save Share + New alert rule Export Pin to Format query

```
1 Log_Concesionarios_CL
2 | where ID_ECU_s in (
3   (_GetWatchlist('ECUs_blacklist')
4   | project SearchKey))
5 | extend Incidente_Mensaje = strcat("El vehículo ", tostring(ID_Vehiculo_s), " está comprometido.")
6 | extend Incidente_Detalle = pack_all()
7 | extend Incidente_Titulo = strcat("Vehículo comprometido: ", tostring(ID_Vehiculo_s))
8 | extend Severity = "Critical"
9 | extend Recommendation = "Investigar el vehículo de inmediato."
10 | extend Confidence = 100
11 | extend ConfidenceLevel = "High"
12 | extend Classification = "Malware"
13 | project
14   Incidente_Mensaje,
15   Incidente_Detalle,
16   Incidente_Titulo,
17   Severity,
18   Recommendation,
19   Confidence,
20   ConfidenceLevel,
21   Classification
```

Schema and Filter

Results Chart Add bookmark

<input type="checkbox"/>	Incidente_Mensaje	Incidente_Detalle	Incidente_Titulo	Severity	Recommendation	Confidence	ConfidenceLevel	Classification
<input type="checkbox"/>	> El vehículo Vehiculo003 está comprometido.	{\"TenantId\":\"57ef24b6...	Vehículo comprometido: Vehiculo003	Critical	Investigar el vehículo de inmediato.	100	High	Malware

Columns

Experimento (4/4)



Respuesta automática (playbook)



The screenshot shows the Microsoft Azure Logic Apps Designer interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and the user profile 'jordi.nogues@iberiaher...'. The main content area shows a 'Microsoft Sentinel incident' trigger. The 'Method' is set to 'POST' and the 'URI' is set to 'https://api.twilio.com/2010-04-01/Accounts/{AccountSID}/Calls.json'. The 'Headers' section is expanded, showing 'Authorization' and 'Content-Type'.

The screenshot shows the Microsoft Azure Logic Apps overview page for the 'LlamarVehiculoJN' Logic app. The top navigation bar includes the Microsoft Azure logo, a search bar, and the user profile 'jordi.nogues@iberiaher...'. The main content area shows the Logic app details, including the resource group 'RG-SECURITY-TEAM', location 'West Europe', and subscription 'SA-MAPS-Iberia Lab'. The 'Runs history' tab is selected, showing a table of runs.

Status	Start time	Identifier	Duration	Static Results
Succeeded	4/18/2023, 10:21 PM	08585197576178950960018825897CU...	498 Milliseconds	

En cada etapa de este proyecto se han generado reflexiones de diversa índole:

Etapa	Conclusiones
Estado del arte de las comunicaciones V2X	<ul style="list-style-type: none">• La continua evolución del 3GPP en su hoja de ruta habilita de forma sistemática nuevos escenarios de uso y de negocio, lo que a su vez origina nuevas superficies de ataque.
Análisis del marco regulatorio	<ul style="list-style-type: none">• 60 países –incluyendo España- han adoptado la reglamentación de las Naciones Unidas UNECE WP.29, la cual impone unos requisitos de seguridad para la industria automotriz que serán de obligado cumplimiento a partir de julio de 2024. Entre ellos, la implantación de un Centro de Operaciones de Seguridad Vehicular (VSOC).
Arquitectura de la solución	<ul style="list-style-type: none">• Según el último Magic Quadrant de Gartner, la tecnología líder para la implantación de un SOC es Microsoft Sentinel, por sus capacidades SIEM y SOAR.• En la seguridad IoT, se pueden aplicar soluciones análogas a las de las redes de ordenadores, pero se requieren estrategias específicas en varios aspectos, principalmente en los procesos de recolección de los registros de actividad y en los de detección de amenazas.

Aunque se han logrado los objetivos establecidos, la contribución de este proyecto como guía para la implementación de un Centro de Operaciones de Seguridad en el ámbito del vehículo conectado solamente representa un primer paso dentro de un proceso mucho más amplio y complejo.

Se ha desarrollado un caso de uso relativamente sencillo, basado en la identificación de códigos de dispositivo (ECUs) reportados como maliciosos en una “blacklist”, para gestionarlos de forma análoga a los IoCs (Indicadores de Compromiso) que típicamente proporcionan las fuentes de *Threat Intelligence* con direcciones IP o hashes de archivos identificados como maliciosos, pero existen muchos más casos de uso a explorar, como aquellos basados en mecanismos de inteligencia artificial, por ejemplo:

- Recepción de códigos no habituales
- Contenido atípico en los mensajes
- Frecuencia de envíos atípica

En resumen, se ha aplicado un enfoque de “producto mínimo viable” para ilustrar adecuadamente los beneficios potenciales de la solución y su lógica de funcionamiento, pero limitado por los plazos que exige un Trabajo de Final de Grado. Por lo tanto, este proyecto está abierto a una posible continuidad, quizás en un futuro Trabajo de Fin de Máster.





Gracias!