ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

Informe de Ciberintel·ligència

La ciberseguretat en el sector de l'automoció

TLP: WHITE

JUNY 2024

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	21/06/2024	26/05/2024

Registre de canvis			
Versió	Pàgines	Data Modificació	Motiu del canvi

Propietari del document	ANC-AD

ÍNDEX

1. METODOLOGIA

Aquest informe aplica els principis de Traffic Light Protocol (TLP). És un esquema creat per fomentar un intercanvi més bo d'informació delicada (però no classificada) en l'àmbit de la seguretat de la informació.

A través d'aquest esquema, d'una manera àgil i senzilla, s'indica fins on pot circular la informació més enllà del receptor immediat, i aquest ha de consultar l'Agència Nacional de Ciberseguretat d'Andorra quan cal distribuir la informació a tercers.

Codi	Com es fa servir	Com es comparteix
TLP: RED	S'ha de fer servir **TLP:RED** quan la informació està limitada a persones concretes, i podria tenir impacte en la privacitat, la reputació o les operacions si es fa servir malament.	Els receptors no han de compartir informació designada com a **TLP:RED** amb cap tercer fora de l'àmbit on va ser exposada originalment.
TLP: AMBER	S'ha de fer servir **TLP:AMBER** quan la informació ha de ser distribuïda de manera limitada, però suposa un risc per a la privacitat, la reputació o les operacions si és compartida fora de l'organització.	Els receptors poden compartir informació indicada com a **TLP:AMBER** només amb membres de la seva pròpia organització que necessiten conèixer-la, i amb clients, proveïdors o associats que necessiten conèixer-la per protegir-se a si mateixos o evitar danys. L'emissor pot especificar restriccions addicionals per compartir aquesta informació.
TLP: GREEN	S'ha de fer servir **TLP:GREEN** quan la informació és útil per a totes les organitzacions que hi participen, com també amb tercers de la comunitat o el sector.	Els receptors poden compartir la informació indicada com a **TLP:GREEN** amb organitzacions afiliades o membres del mateix sector, però mai a través de canals públics.
TLP: WHITE	S'ha de fer servir **TLP:WHITE** quan la informació no suposa cap risc de mal ús, conforme a les regles i procediments establerts per a la seva difusió pública.	La informació **TLP:WHITE** pot ser distribuïda sense restriccions, únicament subjecta a controls de copyright.

2. INTRODUCCIÓ

A l'era digital actual, la ciberseguretat s'ha convertit en una preocupació fonamental en diversos sectors, inclòs el sector de l'automoció. A mesura que els vehicles moderns es fan més connectats i integrats amb tecnologies avançades, la superfície d'atac per a possibles amenaces cibernètiques augmenta considerablement.

Els automòbils actuals, a més de mitjans de transport, són sistemes tecnològics complexos que combinen programari, maquinari i xarxes de comunicació. Per altra banda, s'està avançant cap a la conducció autònoma i l'oferta de vehicles elèctrics i connectats va creixent. Per tant, els automòbils avui dia són objectius potencials de ciberatacs i la necessitat d'enfortir les defenses cibernètiques s'ha intensificat considerablement.

Considerem que la ciberseguretat al sector automotriu és de vital importància atès que els ciberatacs poden comprometre no només la privacitat de les dades dels usuaris, sinó també la seguretat física dels passatgers i la integritat dels vehicles. Els riscos són diversos i poden tenir conseqüències devastadores.

El sector està responent a aquests desafiaments mitjançant el desenvolupament de tecnologies avançades, la col·laboració amb experts en el camp de la ciberseguretat i l'adopció d'estàndards de seguretat. No obstant això, és essencial continuar millorant la ciberseguretat per assegurar que els vehicles connectats siguin segurs i estiguin protegits.

Aquest informe té com a objectiu examinar l'estat actual de la ciberseguretat en el sector motriu, i identificar les amenaces principals, les vulnerabilitats més comunes i les millors pràctiques per mitigar els riscos. A més, s'analitzaran les regulacions i les normatives que busquen establir un marc de seguretat més sòlid per al sector. Amb aquesta informació, els actors del sector podran prendre mesures proactives per protegir els seus sistemes i garantir la seguretat dels usuaris en un entorn cada vegada més digitalitzat.

3. PANORAMA ACTUAL

Com hem esmentat, el sector de l'automoció està experimentant una transformació profunda, marcada per l'adopció de tecnologies cada vegada més sofisticades i interconnectades. Els vehicles moderns incorporen una àmplia gamma de sistemes avançats, com ara dispositius d'assistència al conductor, sensors d'estacionament, sistemes d'informació i entreteniment, entre d'altres. A més a més, un nombre creixent d'automòbils disposa de connectivitat amb Internet i funcions de comunicació avançades, com ara la telemàtica.

En aquest context, la ciberseguretat juga un paper fonamental en el sector de l'automòbil, i protegeix els sistemes informàtics dels automòbils i les infraestructures connectades. Això inclou prevenir, detectar i respondre a ciberatacs, com també protegir les dades delicades dels conductors i usuaris d'automòbils connectats.

3.1. Evolució tecnològica en el sector de l'automoció

L'evolució del sector de l'automoció ha fet que els vehicles actuals depenguin, en gran manera, del programari, les xarxes i les tecnologies de la comunicació. Avui dia, tots els vehicles estan connectats d'alguna manera. Exemples d'això són la trucada d'emergència eCall (que s'activa en cas d'accident), la geolocalització mitjançant GPS, entre d'altres. Aquesta connectivitat augmentarà en el futur, i s'integrarà amb altres vehicles i amb la infraestructura de transport. A més a més, ja hi ha vehicles en els quals algunes funcions de conducció es fan de manera automàtica, i anticipen l'arribada de vehicles totalment autònoms. Els podem dividir de la manera següent:

- **Vehicles connectats:** fan servir tecnologies com ara la telemàtica i la connexió a Internet per proporcionar als conductors informació real sobre el trànsit, les rutes alternatives i les condicions climàtiques. Aquests vehicles també poden estar equipats amb funcions d'entreteniment a bord, com ara la connexió Bluetooth per a la transmissió de música i accés a serveis en línia.
- **Vehicles elèctrics:** la tendència és inclinar-se més cap als vehicles elèctrics, que fan servir motors alimentats per bateries recarregables en lloc de combustibles fòssils.
- **Tecnologies de seguretat avançades:** la indústria està intentant millorar la seguretat dels automòbils mitjançant la implementació de tecnologies de seguretat avançades, com ara els sistemes de detecció de punts cecs, sensors d'estacionament, sistemes de monitoratge de pressió dels pneumàtics i d'altres.
- **Informació i entreteniment:** Els sistemes moderns d'informació i entreteniment per a automòbils ofereixen una àmplia gamma de funcions d'entreteniment, com ara la connexió a Bluetooth per transmetre música, navegació per satèl·lit, veure missatges de correu electrònics i d'altres.
- **Vehicles autònoms:** els automòbils autònoms fan servir tecnologies avançades de conducció autònoma per conduir sense intervenció humana. Això requereix l'ús de sensors avançats, com ara sensors de radar i LiDAR, per detectar obstacles a la carretera i per a la navegació autònoma.
- **Tecnologies d'assistència al conductor:** el sector està invertint en tecnologies avançades d'assistència al conductor, com ara el sistema automàtic de frenada d'emergència i el sistema de manteniment de carril. Aquestes tecnologies ajuden a prevenir accidents de trànsit i redueixen el nombre de morts a les carreteres.

Els vehicles equipats amb Sistemes Avançats d'Assistència al Conductor (ADAS en anglès) ja estan disponibles al mercat de la UE (nivells 1 i 2). Igualment, els vehicles autònoms que poden operar en un nombre limitat de situacions de conducció (nivells 3 i 4) estan essent testats en condicions reals. Les proves per al nivell 5 també estan en marxa, tal com ha anunciat WAYMO (anteriorment conegut com a Projecte de Vehicle Autònom de Google) i Tesla, que va un pas més enllà quan parla de proves amb flotes de vehicles sense conductor.

Per donar suport a aquests desenvolupaments, el sector automotriu està invertint en tecnologies de comunicació avançades, com ara la connectivitat 5G i l'Internet de les Coses (IoT), que permeten que els vehicles es comuniquin entre si i amb la infraestructura viària. Aquestes tecnologies contribueixen a prevenir accidents de trànsit i reduir el nombre de morts a les carreteres. Tanmateix, aquestes transformacions també presenten desafiaments, com ara la ciberseguretat i la necessitat d'una infraestructura de càrrega elèctrica més àmplia i accessible.

3.2. Amenaces i vulnerabilitats principals

Els ciberdelinqüents poden explotar les vulnerabilitats del sistema per accedir a les dades personals dels conductors, prendre el control dels vehicles i fins i tot provocar accidents. Segons el Global Automotive Cybersecurity Report 2024, el nombre d'incidents d'escala alta i massiva es va duplicar de 2022 a 2023. Aquest informe també va revelar que el 13 % de les activitats se centren en eines de manipulació de vehicles, 12 % en obtenir accés a dades delicades i gairebé el 50 % estan relacionats amb les vulnerabilitats.

Per l'altra banda, l'informe d'Upstream de les activitats de ciberseguretat automotriu en el web fosc va fer un seguiment dels 300 actors d'amenaces més actius. Gairebé el 50 % es dirigia a més d'un proveïdor de l'Organitzacions de Mobilitat Intel·ligent (OEM, en anglès) o automotriu, i el 37 % tenia el potencial d'influir en els actius de mobilitat de molts actors interessats a escala mundial.

3.2.1 Vulnerabilitats i vies d'accés dels ciberdelinqüents

El sector de l'automoció presenta nombroses vulnerabilitats des del punt de vista de la ciberseguretat i la seguretat de la informació. Tot seguit, esmentem els elements dels vehicles moderns que més tendeixen a rebre ciberatacs, segons la informació publicada l'any 2022:

- Sistema d'accés sense clau: 47 %
- Servidors: 17 %
- Aplicacions mòbils: 6 %
- Sistemes d'informació: 4 %
- Unitat de control del motor (ECU): 4 %
- Sistemes d'infoentreteniment: 4 %
- Ports de comunicació entre unitats de comandament: 4 %
- Bluetooth: 2 %

Pel que fa a les coses que s'accedeixen a través d'Internet, per exemple, per escoltar música, parlar pel mòbil o buscar una ruta, són una de les vies d'entrada que pot succeir mitjançant un port USB, Bluetooth, una targeta SD o amb el wifi.

Les vulnerabilitats poden afectar diverses àrees, inclosos:

- **Sistema de control electrònic del vehicle:** el sistema de control electrònic del vehicle (conegut com a ECU), és el cervell de l'automòbil i controla totes les funcions del vehicle, inclòs el motor, els frens, la transmissió, etc. Aquest sistema pot ser vulnerable a atacs cibernètics, que poden provocar fallades en el funcionament del vehicle i comprometre'n la seguretat.
- **Sistema d'infoentreteniment:** els sistemes d'informació i entreteniment en els automòbils moderns poden ser vulnerables i comprometre la privacitat i la seguretat de les dades dels conductors i els passatgers. Aquesta atacs poden permetre que els ciberdelinqüents obtinguin accés a dades personals i informació de geolocalització de vehicles.
- **Sensors avançats:** els sensors avançats que es fan servir als vehicles autònoms, com ara el LiDAR i sensors de radar, poden ser vulnerables als atacs cibernètics. Aquests atacs poden interferir amb la capacitat del vehicle per detectar obstacles a la carretera i comprometre la seguretat del vehicle.
- **Infraestructura connectada:** els automòbils connectats poden ser vulnerables als atacs cibernètics a través de la infraestructura connectada, com ara les estacions de càrrega i les xarxes de comunicació. Aquests atacs poden comprometre la seguretat de les dades i la funcionalitat del vehicle.
- **Proveïdors de tercers:** els proveïdors externs de programari i maquinari que es fan servir als vehicles poden representar una vulnerabilitat per a la ciberseguretat dels vehicles. És possible que aquests proveïdors no tinguin les mateixes mesures de seguretat estrictes que els fabricants d'automòbils, cosa que crea una vulnerabilitat potencial.

3.2.2 Tipus de ciberatacs i impacte

Les vies principals de ciberatac són el **programari de segrest** i les **filtracions de dades**. L'impacte d'ambdós a la fase de producció dels vehicles és bastant alt, atès que això genera que la producció se suspengui o s'aturi durant els incidents. Per tant, pot haver-hi retards en els lliuraments dels vehicles per causa de la vulnerabilitat als ciberatacs.

Tot seguit, es presenten alguns exemples de ciberatacs fets a vehicles en els darrers anys:

- **Atacs al sistema sense clau (Keyless):** aquesta mena d'atac s'adreça a la unitat de control del sistema sense clau, com una centraleta, que interpreta les comunicacions entre els dispositius del vehicle. Els atacants repliquen el senyal enviat pel comandament a la centraleta per obrir el cotxe i robar els objectes de l'interior o, fins i tot, el mateix vehicle.
- **Atacs de denegació de servei (DDoS):** els sistemes de transport intel·ligents són vulnerables a atacs DDoS, que poden bloquejar totes les comunicacions dels automòbils connectats, cosa que representa un risc alt per a la seguretat de les persones.
- **Vulnerabilitats no resoltes:** algunes vulnerabilitats descobertes en els vehicles no es resolen per causa de la dificultat d'actualitzar tots els dispositius. Això pot deixar els vehicles exposats a ciberatacs.
- **Sistemes d'entreteniment:** les interfícies com ara l'Appel CarPlay o l'Android Auto es poden fer servir per prendre el control de la consola del vehicle si no està degudament protegida.
- **Infeccions des de dispositius externs:** els vehicles poden ser infectats a través de dispositius externs com ara estacions de recàrrega o dispositius infectats a les plantes de fabricació.
- **Ports USB:** els ports USB del vehicle es poden emprar maliciosament per executar codi, instal·lar aplicacions no autoritzades o obtenir informació delicada.

- **Manipulació del GPS:** els sistemes GPS poden ser vulnerables a atacs de suplantació i interferència, que manipulen el senyal GPS, i anul·len l'autèntica o la substitueixen.
- **Atacs a sensors:** els sensors instal·lats en els cotxes, com els acústics i els odomètrics, es poden atacar mitjançant sorolls intensos i interferències magnètiques per afectar-ne el funcionament.

Segons Statista, entre el 2020 i el 2023, el 42 % dels ciberatacs al sector de l'automoció van provocar la interrupció del servei i del negoci, com també retards o aturades a la producció. Un 22 % d'aquests ciberatacs va ser a causa de la violació de dades i de la privacitat. Altres ciberdelictes van tenir a veure amb el frau i el robatori de vehicles.

3.2.3 Casos d'estudi

Tot seguit, esmentem tres casos de ciberatacs al sector de l'automoció que considerem rellevants.

Jeep Cherokee (2015)

L'any 2015, els investigadores de seguretat Charlie Miller i Chris Valasek van revelar una vulnerabilitat crítica al Jeep Cherokee, fabricat per Fiat Chrysler Automobiles (FCA). A través d'una connexió a Internet, van aconseguir prendre el control remot del vehicle, inclosa la manipulació de l'accelerador, els frens i la direcció. L'atac es va dur a terme a través del sistema d'entreteniment Uconnect del cotxe, cosa que va obligar a FCA a retirar 1,4 milions de vehicles de 7 models diferents per actualitzar el programari i tancar la vulnerabilitat. Aquesta retirada va afectar gairebé la meitat dels models venuts aquell anys als Estats Units i va ser el primer cas significatiu d'atac cibernètic, amb pèrdues estimades en gairebé 600 milions de dòlars per a l'empresa.

Tesla Model S Hack (2016)

L'any 2016, un equip d'investigadors de Keen Security Lab, una divisió de l'empresa tecnològica xinesa Tencent, va aconseguir piratejar remotament un Tesla Model S. Van aconseguir prendre el control del vehicle en moviment, i manipular els frens, les finestres, les portes i el sistema d'entreteniment. Tesla va respondre ràpidament amb una actualització de programari per corregir les vulnerabilitats descobertes.

Nissan Leaf Vulnerability (2016)

L'any 2016, l'investigador de seguretat Troy Hunt va descobrir una vulnerabilitat a l'aplicació mòbil del vehicle elèctric popular Nissan Leaf. Aquesta fallada permetia que els pirates informàtics accedissin i controlessin remotament les funcions del cotxe, com ara el sistema de calefacció i aire condicionat, a més d'obtenir informació sobre els últims viatges del vehicle. Nissan va resoldre el problema tancant temporalment l'accés a l'aplicació fins que es van implementar les mesures de seguretat necessàries.

Altres casos

- L'any 2018, una empresa xinesa de seguretat informàtica va revelar més de 14 vulnerabilitats en els vehicles de marca europea.
- El juny de 2023, un fabricant de semiconductors amb seu a Taiwan va informar d'un incident de ciberseguretat. Aquest fet, que va involucrar un grup de programari de segrest i a un dels proveïdors de maquinari de TI, va provocar una filtració d'informació delicada relacionada amb la configuració inicial del sistema. Segons Upstream, els atacants van afirmar que tenien accés a documents interns amb informació confidencial i van exigir un rescat de 70 milions de dòlars per evitar el seu llançament en línia. Aquest cas es va convertir en la demanda més gran de rescat coneguda a la història.

4. NORMATIVA I DIRECTRIUS

Hi ha diverses directrius i normatives en matèria de ciberseguretat per al sector de l'automoció. Les directrius se centren en la gestió de riscos de ciberseguretat, la prevenció de ciberatacs i la resposta a incidents de seguretat. Les recomanacions específiques se centren en la gestió de riscos, la protecció de dades, la seguretat dels vehicles connectats i la prevenció de ciberatacs. Tot seguit, presentem les normes que considerem més rellevants:

- **Directiva UE 2022/2025:** aquesta directiva representa un avenç clau per unificar la normativa de ciberseguretat de la UE i s'enfoca, sobretot, en el sector de l'automoció. Amb aquesta norma s'estenen les responsabilitats de ciberseguretat més enllà dels fabricants de vehicles i s'incorpora una gamma més àmplia d'operadors en el transport per carretera.

- **Millors pràctiques d'Auto-ISAC:** aquesta guia ofereix una sèrie de millors pràctiques de seguretat cibernètica per a fabricants d'automòbils i proveïdors de components, amb recomanacions específiques per gestionar els riscos de ciberseguretat i prevenir els ciberatacs.

- **ISO/SAE 21434:** aquesta norma estableix pautes per a la gestió de la seguretat dels vehicles des del disseny fins a la producció i el manteniment. Defineix els requisits per identificar i avaluar els riscos de seguretat de la informació i la implementació de mesures de seguretat adequades.

- **Millors pràctiques de ciberseguretat de l'NHTSA per a vehicles moderns**: aquesta guia proporciona recomanacions específiques per a fabricants d'automòbils, proveïdors de components i reguladors. S'enfoca a la gestió de riscos de ciberseguretat, la prevenció de ciberatacs i la resposta a incidents de seguretat.

- **SAE J3061:** aquesta norma defineix les pautes per a la ciberseguretat dels vehicles des de la fase de disseny fins al final de la seva vida útil. Estableix els requisits per a la identificació i avaluació dels riscos de seguretat de la informació i la implementació de mesures de seguretat adequades.

- **WP.29 Ciberseguretat i actualitzacions de programari per aire:** aquest document del Fòrum Mundial de les Nacions Unides per a l'Harmonització de les Regulacions dels Vehicles (WP.29) proporciona recomanacions per a la seguretat cibernètica de vehicles connectats i actualitzacions de programari sense fils (OTA). S'enfoca a la protecció de dades i la seguretat dels vehicles connectats.

- **UNECE/R155:** aquesta normativa exigeix que es compleixin els protocols següents: identificar i gestionar els riscos de ciberseguretat en el disseny de vehicles; verificar que es gestionin els riscos, incloses les proves; assegurar que les avaluacions de riscos es mantinguin actualitzades; monitorar els ciberatacs i que se'n respongui efectivament; analitzar els atacs amb èxit o intents d'atac; i avaluar si les mesures de ciberseguretat continuen essent efectives a la llum de les noves amenaces i vulnerabilitats.

- **UNECER/R156:** aquesta normativa està més enfocada a la seguretat del programari. Alguns requeriments d'aquesta normativa són: l'objectiu d'actualització; els impactes que

poden succeir al cotxe quan es fa aquesta actualització; si l'actualització del programari modifica algun requisit complert anteriorment; en quines condicions es pot fer aquesta actualització; confirmar que l'actualització del programari hagi tingut una verificació i una validació correctes.

- **ISO TC22/SC32/WG11 o ISO TC22/SC32/WG12:** segons el país en el qual es fabriqui o en el qual es faci servir podrien estar obligats a complir unes normatives o unes altres.

Restriccions per a les empreses del sector de l'automoció

Segons assenyala Reuters, els Estats Units han plantejat la possibilitat d'imposar restriccions o fins i tot prohibir els vehicles connectats a marques xineses. Això s'emmarca en una investigació llançada per l'Administració Biden el febrer destinada a determinar si les importacions de vehicles xinesos representen riscos per a la seguretat nacional.

El 2021 i 2022 l'exèrcit xinès va prohibir l'entrada de cotxes Tesla a les seves instal·lacions perquè les seves càmeres podien captar informació delicada i es pensava que podrien ser una font de filtracions de la seguretat nacional.

5. REPTES I DESAFIAMENTS

Un dels desafiaments de la digitalització del sector de l'automoció és la seguretat i la privacitat. La digitalització augmenta l'exposició a amenaces cibernètiques i planteja desafiaments en termes de protecció de dades delicades i privacitat del client. Un d'aquests riscos és l'amenaça d'un ciberatac directe a un vehicle o a una flota de vehicles. Per aquest motiu és importantíssim considerar els riscos de ciberseguretat en els vehicles connectats.

Per abordar aquests desafiaments, el sector està desenvolupant tecnologies de seguretat avançades i està treballant amb experts en ciberseguretat per garantir que els vehicles connectats estiguin protegits. També s'està treballant en la implementació de regulacions i estàndards de seguretat per garantir que els vehicles compleixin amb les millors pràctiques de seguretat.

El sector de l'automoció s'enfrontarà a diferents desafiaments en el futur, inclosos:

- **La intel·ligència artificial:** la intel·ligència artificial està adquirint cada vegada més importància en el sector de l'automoció, especialment per al desenvolupament de vehicles autònoms. Els desafiaments aquí és desenvolupar sistemes d'IA confiables i segurs que puguin funcionar en diferents situacions de conducció.

- **Sensors:** Els sensors són un altre repte tecnològic en el sector de l'automoció, especialment per als vehicles autònoms. Els sensors han de ser precisos, confiables i capaços d'operar en una varietat de condicions ambientals.

- **Infraestructura de càrrega:** per als vehicles elèctrics, el desafiament és crear una infraestructura de càrrega que sigui de fàcil accés, ràpida i rendible.

- **Seguretat cibernètica:** amb l'auge de les tecnologies connectades i els vehicles autònoms, la ciberseguretat es converteix en un repte tecnològic més per al sector de l'automoció. Els vehicles han d'estar protegits de ciberatacs i vulnerabilitats, que podrien comprometre la seguretat dels conductors i els passatgers.

- **Producció sostenible:** fabricar vehicles requereix una gran quantitat d'energia i recursos, cosa que pot tenir un impacte significatiu en el medi ambient. Un desafiament tecnològic per al sector automotriu és trobar modes de produir vehicles de manera més sostenible i reduir-ne l'impacte mediambiental.

En resum, el sector de l'automoció s'enfrontarà a diversos reptes en el futur, entre els quals hi ha el desenvolupament de vehicles elèctrics i autònoms, la ciberseguretat, la integració amb l'Internet de les coses (IoT), la sostenibilitat i l'evolució dels models de negoci. Tanmateix, aquests desafiaments també presenten oportunitats per a la innovació i el desenvolupament de solucions innovadores per al sector.

6. CONCLUSIONS I RECOMANACIONS

Per augmentar-ne la resiliència, es recomana dur a terme les accions següents:

- El sector de l'automoció ha de concebre des del disseny la ciberseguretat dels vehicles, dels seus punts de càrrega, de les infraestructures per les quals transitaran i de la cadena de subministraments.
- Invertir en tecnologies i solucions específicament dissenyades per protegir els seus vehicles i sistemes electrònics.
- A més a més, és fonamental enfortir la defensa contra amenaces cibernètiques mitjançant la implementació de pràctiques de disseny segur des de les etapes inicials de desenvolupament, com també fer proves exhaustives de seguretat cibernètica abans de la comercialització dels vehicles.
- L'educació i la conscienciació exerceixen un paper crucial. Els fabricants han de col·laborar estretament amb els usuaris finals per proporcionar-los la informació i el suport necessaris per protegir-se contra possibles atacs. Això implica fomentar les bones pràctiques de seguretat, com ara la utilització de contrasenyes robustes i l'actualització periòdica del programari del vehicle.

7. CLÀUSULA DE CONFIDENCIALITAT

Aquest document és propietat de l'Agència Nacional de Ciberseguretat d'Andorra. Tota la informació que conté és confidencial, aquesta informació s'actualitzarà regularment per reflectir els possibles canvis dels productes i no podrà ser copiada o revelada a terceres persones sigui totalment o en part, sense consentiment previ exprés de l'Agència Nacional de Ciberseguretat d'Andorra.