CIBERSEGURIDAD AL VOLANTE

Paula Espinar Verdugo

Tabla de contenido

1. Introducción

Montarnos en el coche y conectar nuestros dispositivos es un gesto tan natural que ya ni nos planteamos la idea de que ese tipo de acciones y conexiones ponen en peligro la seguridad de nuestros datos (HackerCar, 2025a). Al fin y al cabo, utilizamos estos dispositivos, como por ejemplo el móvil, para todo y poder conectarlo a otros dispositivos facilita cualquier tarea (HackerCar, 2025a).

No obstante, es importante saber que los coches se pueden hackear (González de la Mora, 2024) y en algunos casos lo único necesario para hackearlo es el número de bastidor, algo que fácilmente se puede encontrar puesto que se muestra en el parabrisas (Coches.net, 2025). Siguiendo con el tema principal de este artículo sobre la conexión de dispositivos al coche, como se ha dicho, existe un riesgo al usar este tipo de conexiones. En el caso de los móviles, por ejemplo, "si un atacante logra comprometer la seguridad de tu teléfono móvil y está vinculado al sistema de tu automóvil, podría obtener acceso sin ninguna restricción al vehículo" (HackerCar, 2025a).

En otras palabras, los coches son otro objetivo de los ciberatacantes y si el vehículo además está conectado a otros dispositivos, los datos compartidos pueden ser interceptados. A esta exposición de datos personales hay que sumarle que el hackeo de un coche puede suponer también un riesgo para la seguridad física (González de la Mora, 2024; Coches.net, 2025).

Una escena muy común en este aspecto ocurre en las películas de acción cuando se hackean coches inteligentes y se hace que se muevan por la ciudad solos. Esto, aunque increíble, es algo que cada día se acerca más a la realidad.

La ciberseguridad de los coches es algo que cada vez está más en el foco de atención. Con los avances tecnológicos, nuestros coches y dispositivos están cada vez más conectados. Y, aunque aún no estemos en una película de acción los riesgos son cada vez mayores y más reales.

Para tener una visión más clara, el Informe Global de Ciberseguridad de Automoción y Movilidad Inteligente de Upstream, solo en 2024 hubo 409 ciberataques a coches (ElEconomista, 2025). Teniendo en cuenta este dato y los avances tecnológicos, me atrevo a decir que este número no va a hacer más que aumentar.

En este artículo vamos a explicar varias formas de conexión entre los coches inteligentes y otros dispositivos, principalmente dispositivos móviles. Asimismo, se presentarán los riesgos asociados a estas conexiones. Seguidamente se explicarán los tipos de ciberataques que se pueden producir por estas conexiones y las buenas prácticas que se pueden llevar a cabo para reducir el riesgo de ser víctima de uno de ellos. Además, se dará unas recomendaciones generales que pueden tener en cuenta para mantener nuestros dispositivos y coches más seguros. Después de esto, se hará una referencia especial a la IA en los coches y su rol en los ciberataques a estos. Finalmente, se expondrán las conclusiones en base a todo lo explicado a lo largo del artículo.

2. Información clave

- Conectar nuestros dispositivos como el móvil al coche puede conllevar varios riesgos de los que no solemos ser conscientes o, si lo somos, no lo consideramos una prioridad.
- No obstante, existen varias formas de conexión y cada una conlleva diversos riesgos que pueden poner en peligro los datos compartidos entre ambos dispositivos.
- Además de tener en cuenta las formas de conexión, se ha de tener presente la gran variedad de ataques que se pueden sufrir. Por ejemplo, ataques por bluetooth, por radio frecuencia o, los más comunes, ataques al sistema keyless.
- Ante esta situación, existen muchas recomendaciones de acciones que se pueden incorporar en nuestra rutina que harán que nos mantengamos más protegidos ante los ciberataques a coches y que roben los datos compartidos con otros dispositivos.
- Algunas de las recomendaciones son: no sincronizar los dispositivos si no es necesario, mantener actualizados todos los sistemas y borrar los datos almacenados en el coche.
- La incorporación de IA en los coches es cada vez más común. Este hecho abre la puerta a tanto un nuevo abanico de ciberataques como una nueva forma de protegernos.
- Aunque las empresas del sector automovilístico están invirtiendo cada vez más en ciberseguridad, este tema está aún muy poco explorado. Por ello, es necesario que se le dé más importancia para reducir el riesgo de ser víctima de un ataque a nuestro coche.

3. Formas más habituales de conexión y riesgos

Existen varias formas en las que podemos conectar nuestro coche a otros dispositivos o incluso a redes externas. En este artículo se nombrarán algunas de las formas de conexión con el objetivo de dar a conocer la gran cantidad de puentes que conectar nuestros datos con otros dispositivos. Con esto, además, se pretende concienciar sobre la gran cantidad y el potencial de los riesgos a los que estamos expuestos.

Así, lo primero que se debe tener en cuenta es que las vías de acceso a tu coche o móvil son conocidos como vectores. Los datos obtenidos por estos vectores están limitados y regidos por el tipo de conexión y el dispositivo conectado. Uno de los ejemplos de datos que se pueden robar es la ubicación. Otro tipo de datos son los biométricos almacenados en nuestros dispositivos móviles (HackerCar, 2025a) y normalmente utilizados para desbloquear nuestro dispositivo o incluso para firmar operaciones bancarias. Estos datos servirían para la apertura de puertas o el arrancado del motor (Coches.net, 2025). Además, si esta información no es almacenada de forma segura pueden ser robados para acceder de forma física al coche (HackerCar, 2025a).

No obstante, estos riesgos no solo hacen peligrar nuestros datos personales, sino también nuestra seguridad vial pues existe, por ejemplo, la posibilidad de que accedan a los sistemas de conducción autónoma, lo que puede provocar accidentes y poner en peligro incluso la vida de las personas en carretera (Coches.net, 2025).

Algunos de los vectores más comunes presentados por el INCIBE (2019) de conexión al coche incluyen:

- Wi-Fi: En este caso, el coche actúa como punto de acceso Wi-Fi y si un dispositivo se conecta a esta red, los datos compartidos entre ambos dispositivos pueden quedar expuestos.
- Control remoto: Muchos coches permiten el control remoto del vehículo a través de otros dispositivos. Esto siempre conlleva un riesgo. Si se accede a este dispositivo, se podría tener acceso también a nuestro coche.
- Sistema TPMS (Sistema de monitoreo de presión de neumáticos): Si un atacante tiene acceso a este sistema, podría desactivar las alertas de presión, lo cual podría distraer al conductor mientras conduces e incluso provocarte un accidente.

- Pantalla de infoentretenimiento: Los sistemas de infoentretenimiento permiten ver aplicaciones, el GPS y recibir llamadas o mensajes. Es un punto de acceso al móvil, por lo que, de nuevo, un ciberatacante podrían interceptar datos compartidos entre ambos dispositivos.
- Puerto USB: Los puertos USB permiten ejecutar códigos o instalar aplicaciones. Esto abre la posibilidad de instalar malware en el coche o en el dispositivo conectado.
- Bluetooth: Es una de las formas más comunes de conexión. Como con otros vectores, los datos compartidos por este medio también pueden ser interceptados.
- Puerto OBD-II (sistema de diagnóstico): Este puerto de diagnóstico permite acceder al sistema de control del vehículo. Si un atacante tiene acceso a este puerto, podría inyectar códigos maliciosos o incluso tomar control físico del vehículo.
- Móvil: En este caso, la importancia reside en la propia seguridad del móvil. Si éste no está debidamente asegurado, los datos que se comparten entre ambos dispositivos están en riesgo.

4. Tipos de ataques y buenas prácticas

Ahora que hemos visto los vectores de ataque, es hora de explicar los tipos de ciberataques más comunes según el INCIBE (2019) y cómo podemos protegernos.

- Rogue Acces Point para Wi-Fi. En este caso, el atacante crea una red Wi-Fi falsa que imita a la original y, a través de ella accede a los datos de todos los dispositivos conectados a ella.

  Para protegernos de este tipo de ataques en específico, se recomienda verificar siempre la red Wi-Fi a la que se está conectando, tal y cómo se haría en cada con el móvil o con el ordenador.
- Manipulación de la ECU (Engine Control Unit). Este ataque se centra en los sistemas del coche inyectándole o incluso controlando físicamente el vehículo.

Para reducir la posibilidad de este tipo de ataques es importante mantener siempre actualizado el software del vehículo (González de la Mora, 2024) y usar un sistema de autenticación fuerte en tus dispositivos (HackerCar, 2025a).

- Ataque por Bluetooth. En este caso, si un atacante tiene acceso al Bluetooth de tu coche, puede robar datos personales compartidos con el móvil, como mensajes o información de contacto.

Por tanto, a este respecto, si no necesitas usar Bluetooth, desactívalo. Y, en caso de que lo necesites, asegúrate de que tu móvil está actualizado con los últimos parches de seguridad o haz uso de un cable (HackerCar, 2025a)

- Aplicaciones infectadas con malwares. Las aplicaciones descargadas desde fuentes no oficiales pueden contener malware, lo que pone en riesgo tanto tu coche como tu móvil.

La recomendación dada en este caso es no descargar aplicaciones de fuentes no verificadas. También, en caso de querer obtener una nueva aplicación, se recomienda investigarla antes de descargarla (HackerCar, 2025a)

- Ataques por radio frecuencia (RF). Algunos vehículos son vulnerables a la intercepción de señales RF, como las señales de la llave inteligente. Los atacantes pueden robar las claves de acceso al vehículo.

Para evitar esto se puede usar claves automáticas con cifrado a la vez que se evita reutilizar las mismas claves.

- Ataques al sistema keyless. Según Coches.net (2025) el 47% de los ataques a vehículos están dirigidos a este sistema. Este sistema consiste en el uso de transmisores que permiten la apertura o el cierre del coche a distancia (Sanz Bartolomé, 2024).

Para esto se debe intentar mantener el transmisor lo más lejos posible del coche (HackerCar, 2025b)

Poniendo un ejemplo de ciberataque a automóviles, en 2015, un equipo consiguió hackear un Jeep haciendo unas pruebas de seguridad. Tuvieron el control de varios mecanismos del coche como por ejemplo el cambio de velocidad o la activación del parabrisas. Pero lo más impactante fue la posibilidad de detener el coche en medio de la autopista. Cierto es, que después se volvió a recuperar el control del coche pero el ataque fue posible (BBC, 2015).

Este no es más que un ejemplo de que los ciberataques a coches que, además de ser un riesgo a nivel digital, también suponen un riesgo para la seguridad vial, lo que amplifica su importancia.

5. Recomendaciones

Hasta ahora las buenas prácticas ofrecidas han sido para ciberataques concretos pero existen ciertas recomendaciones que se pueden tener en cuenta en todo momento para mantener nuestros datos protegidos. Algunas de estas recomendaciones son:

- No sincronices dispositivos si no es necesario. Desactiva conexiones como Bluetooth o Wi-Fi cuando no las estés utilizando (HackerCar, 2025a). En caso de querer conectar los dispositivos, evitar conectarlos a sistemas desconocidos pues pueden traer otros riesgos como la infección por malware (La Sexta, 2024). Otra de las acciones que se puede llevar a cabo es limitar el número de personas conectadas a dichos dispositivos (González de la Mora, 2024).
- Borra los datos del coche antes de dejarlo estacionado. Esto es especialmente importante si has conectado tu móvil y almacenado información personal. En estos casos, hay que tener siempre en mente que los datos compartidos por la conexión pueden ser almacenados automáticamente (La Sexta, 2024).

  Siguiendo esta línea es importante mencionar los coches de alquiler puesto que si se conecta al móvil, los datos compartidos pueden quedar almacenados y ser visibles para otros usuarios (La Sexta, 2024).

  Esto también se aplica a la venta de vehículos. Es importante eliminar todos los datos personales almacenados en el coche antes de su entrega al nuevo propietario (LaSexta, 2024).
- Limita los datos que compartes. Evita compartir datos sensibles o no necesarios (HackerCar, 2025a; González de la Mora, 2024). Esto también es esencial en casos de conexión con móviles de empresa debido a la protección y confidencialidad de la información almacenada en estos dispositivos (HackerCar, 2025a).
- Mantén actualizado el software del vehículo (González de la Mora, 2024). Los fabricantes lanzan actualizaciones de seguridad periódicamente, y

mantener tu coche actualizado te protege contra las últimas amenazas. Es importante que se mantenga tanto el móvil como el sistema del coche actualizados puesto que generalmente las nuevas versiones incluyen parches de seguridad (HackerCar, 2025a).

- Protege tus dispositivos con claves de seguridad y sistemas de seguridad adicionales como antivirus (HackerCar, 2025a).

- Si se sospecha de intrusión, es importante que se contacte con el concesionario o directamente con el fabricante (González de la Mora, 2024). En estos casos, esta misma fuente recomienda que se sigan estos pasos: primero "desactivar las funcionalidades conectadas del vehículo". Seguidamente se debe desconectar los dispositivos, apagar las conexiones y cerrar cualquier sesión abierta.

También se recomiendan acciones más conocidas como cambios de contraseña o búsqueda de actividades inusuales (González de la Mora, 2024).

- Por último, se recomienda si es posible, contratar un seguro completo con cobertura por ciberataques (González de la Mora, 2024)

6. La IA en los coches

Es bien sabido que la IA puede mejorar y facilitar desde tareas simples hasta operaciones más complejas. En el campo de la ciberseguridad, la IA puede ser utilizada para aumentar la seguridad de los dispositivos. No obstante, todo lo bueno tiene una parte negativa. En este caso, es que la IA también puede ser utilizada como arma de ataque (INCIBE, 2019).

En este sentido, teniendo en cuenta que los coches inteligentes están introduciendo cada vez más IA en sus sistemas (González de la Mora, 2024), es de suponer que esta IA tendrá tanto un rol defensivo como uno atacante. En otras palabras, la IA podría ser utilizada como una herramienta con el objetivo de hackear los coches inteligentes y poder robar los datos almacenados en este y aquellos compartidos con otros dispositivos. Sin embargo, por su parte contraria, la IA también podría ser utilizada para reforzar los mecanismos de seguridad tanto de coches como de otros dispositivos.

7. Conclusiones

Teniendo todo en cuenta, creo que es más que evidente que algo que considerábamos impenetrable como puede ser nuestro coche, es también vulnerable al lado oscuro de las nuevas tecnologías. Es por ello, que es importante que se tengan presente los riesgos asociados a conectar nuestros dispositivos con el coche y que tengamos toda la información disponible para aprender a reducir la posibilidad de ser víctimas de un ciberataque en este contexto.

Asimismo, es necesario que las empresas dedicadas al sector automovilístico sean conscientes de esta problemática y tomen las medidas necesarias para mantener a salvo a sus usuarios. A este respecto, hay que destacar que cada vez se invierte más en la ciberseguridad de los vehículos (INCIBE, 2019) y de hecho nuevos "sistemas de detección de intrusiones, o el cifrado de datos y protecciones contra la eventual manipulación del software del vehículo" (González de la Mora, 2024) están siendo incorporados. No obstante, aún sigue siendo una cuestión poco explorada y desarrollada.

Dicho esto, se puede concluir que la ciberseguridad en los coches es un tema poco conocido y considerado de poca importancia pero que en nuestro día a día supone un riesgo elevado para nuestros datos más sensibles. A pesar de que cada vez se están tomando más medidas para reducir dichos riesgos, el camino por delante es aún lo suficientemente largo y potencialmente peligroso como para convertirse en una de las prioridades del momento.

8. Bibliografía

BBC Mundo. (2015, 24 de julio). *El "hackeo" de un Jeep hace que llamen a revisión 1,4 millones de autos*. BBC News Mundo. https://www.bbc.com/mundo/noticias/2015/07/150723_fiat_chrysler_hackeo_revision_cch

Coches.net. (2025). *Coches conectados y ciberseguridad*. Coches.net. Recuperado de https://www.coches.net/blog-profesionales/coches-conectados-y-ciberseguridad/

Eleconomista. *(2025, 25 de marzo)*. Los ciberataques contra la automoción y la movilidad inteligente crecen un 39 %. *Eleconomista.* *https://www.eleconomista.es/tecnologia/noticias/13246428/03/25/los-ciberataques-contra-la-automocion-y-la-movilidad-inteligente-crecen-un-39.html*

González de la Mora, B. (2024, 30 de septiembre). *¿Cómo proteger tu coche conectado de los ciberataques?* RACC. https://www.racc.es/blog/coche/proteger-tu-coche-conectado-de-los-ciberataques/

HackerCar. (2025a). *¿Por qué es importante tener cuidado con el móvil que conectas al vehículo?* HackerCar. https://hackercar.com/por-que-es-importante-tener-cuidado-con-el-movil-que-conectas-al-vehiculo/

HackerCar. (2025b). *Cómo proteger a los vehículos con sistema de acceso y arranque manos libres: estas son las recomendaciones de un cuerpo policial.* HackerCar. https://hackercar.com/como-proteger-a-los-vehiculos-con-sistema-de-acceso-y-arranque-manos-libres-estas-son-las-recomendaciones-de-un-cuerpo-policial/

INCIBE. (2019, 28 de noviembre). *Los coches inteligentes: ¿preparados ante amenazas?* INCIBE-CERT. https://www.incibe.es/incibe-cert/blog/los-coches-inteligentes-preparados-amenazas

La Sexta. (2024, 28 de junio). *Mucho cuidado al utilizar tu teléfono móvil en un coche de alquiler*. TecnoXplora / La Sexta. https://www.lasexta.com/tecnologia-tecnoxplora/internet/mucho-cuidado-utilizar-telefono-movil-coche-alquiler_20240628667ec65d0de31e0001f09472.html

Sanz Bartolomé, E. (2024, 11 de abril). *¿Qué es el sistema keyless y cómo se utiliza para robar un coche en segundos?* El País. https://motor.elpais.com/tecnologia/que-es-el-sistema-keyless-y-como-se-utiliza-para-robar-un-coche-en-segundos/