Publicado en América Latina el 25/08/2023

# [Los autos eléctricos y el futuro de la seguridad digital](http://www.notasdeprensa.es)

## Para DigiCert el impacto de las prácticas de seguridad débiles y la falta de implementación de las mejores prácticas de confianza digital para las estaciones de carga de vehículos eléctricos puede tener graves consecuencias

 Durante el transcurso de 2022 se matricularon en América Latina 143.281 vehículos eléctricos e híbridos, lo que representa un crecimiento del 21,7% respecto a 2021 cuando se matricularon 117.742 nuevas unidades. A pesar de ocurrir lentamente, la adopción de automóviles eléctricos viene ocurriendo en Brasil.  Así como las bolsas de aire protegen a los ocupantes del vehículo, la confianza digital juega un papel vital en la protección de los vehículos eléctricos (EV) y sus usuarios durante las operaciones de carga. A medida que esta clase de vehículos se vuelven cada vez más populares, no se puede pasar por alto la importancia de la confianza digital en el proceso de carga. "Si bien los vehículos de combustión tradicionales dependen de interacciones físicas con las bombas de gasolina, la llegada de los vehículos eléctricos requiere la implementación de confianza digital para garantizar el intercambio seguro de datos entre los vehículos eléctricos y los equipos de suministro de vehículos eléctricos (EVSE). Sin embargo, es crucial reconocer que los EVSE, a pesar de su papel indispensable en el transporte sostenible, son susceptibles a riesgos de ciberseguridad que exigen medidas de protección sólidas", explica Dean Coclin, director senior de desarrollo empresarial de DigiCert.  Sin medidas de seguridad adecuadas, los EVSE están expuestos a diversas vulnerabilidades, entre ellas: Interrupción operativa: los piratas informáticos pueden alterar la infraestructura de carga, inutilizar los EVSE y causar molestias a los propietarios de vehículos eléctricos. Esto puede tener un impacto significativo en los sistemas de transporte y obstaculizar la adopción de la movilidad eléctrica. Violación y compromiso de datos: violar la seguridad de las estaciones de carga puede provocar el robo o comprometer datos confidenciales, incluida la información de pago de los clientes. Estos datos pueden explotarse para fraude financiero, robo de identidad u otros fines maliciosos, dañando la confianza entre los usuarios de vehículos eléctricos y los proveedores de infraestructura de carga. Desconfianza reputacional: las violaciones de seguridad pueden empañar la reputación de los proveedores de infraestructura de carga de vehículos eléctricos, lo que lleva a una pérdida de confianza por parte de los clientes. Esto puede tener implicaciones a largo plazo para la adopción y el éxito de los vehículos eléctricos. Los peligros de una política de seguridad débilEl impacto de las prácticas de seguridad débiles y la falta de implementación de las mejores prácticas de confianza digital para las estaciones de carga de vehículos eléctricos puede tener graves consecuencias: Incomodidades e insatisfacción del usuario: las estaciones de carga no seguras pueden experimentar interrupciones o mal funcionamiento frecuentes, lo que incomoda a los propietarios de vehículos eléctricos que dependen de ellas. Esto puede generar insatisfacción y frustración entre los usuarios, obstaculizando el crecimiento del mercado de vehículos eléctricos. Pérdidas financieras y responsabilidad: las filtraciones de datos y la información de pago comprometida pueden provocar pérdidas financieras tanto para los propietarios de vehículos eléctricos como para los operadores de estaciones de carga. Además, unas medidas de seguridad inadecuadas pueden exponer a los operadores de estaciones de carga a responsabilidades legales y reglamentarias. Crecimiento atrofiado del mercado de vehículos eléctricos: la falta de confianza en la seguridad de la infraestructura de carga puede disuadir a los posibles compradores de vehículos eléctricos de adoptar la movilidad eléctrica. Una confianza digital sólida es crucial para fomentar la confianza y fomentar la adopción generalizada de vehículos eléctricos. "La implementación de un enfoque de bricolaje para la confianza digital en las estaciones de carga de vehículos eléctricos plantea desafíos importantes en términos de tiempo y costo. La instalación de sistemas de autenticación seguros y confiables puede llevar mucho tiempo y requerir coordinación con múltiples partes interesadas. Además, la inversión inicial en sistemas sólidos, las medidas de ciberseguridad y las actualizaciones de la infraestructura, junto con el mantenimiento y las actualizaciones continuas, pueden generar costos sustanciales para garantizar la integridad y confiabilidad de las estaciones de carga", agregó Dean Coclin. Proteger y ayudar a los EV/EVSEEs importante proteger las estaciones de carga de vehículos eléctricos con una gestión de certificados que ofrezca capacidades seguras de conexión y carga, garantizando confianza y confiabilidad en la infraestructura de carga de vehículos eléctricos. IoT Trust Manager ofrece confianza digital a las estaciones de carga de vehículos eléctricos con: Seguridad y escalabilidad: IoT Trust Manager autentica de forma segura los vehículos eléctricos y los EVSE, protegiéndolos contra posibles amenazas cibernéticas. Se escala fácilmente, lo que permite acelerar el tiempo de comercialización sin comprometer la seguridad. Flexibilidad y eficiencia de implementación: la solución permite el aprovisionamiento y la implementación de certificados de manera rápida y flexible a través de una infraestructura global. Esto garantiza la compatibilidad con todos los tipos de certificados, lo que facilita la implementación. Compatibilidad y preparación para el futuro: IoT Trust Manager se adhiere a los estándares internacionales, lo que garantiza la compatibilidad con futuros desarrollos en tecnología e infraestructura de vehículos eléctricos. Esta preparación para el futuro ayuda a las estaciones de carga a adelantarse a las cambiantes amenazas a la ciberseguridad. El futuro del transporte limpioLa confianza digital es un componente crucial en el funcionamiento de las estaciones de carga de vehículos eléctricos. Al implementar medidas de seguridad sólidas, los EVSE pueden proteger contra vulnerabilidades, prevenir interrupciones, salvaguardar los datos de los clientes y generar confianza entre los usuarios de vehículos eléctricos. "Fortalecer la confianza digital no sólo es esencial para el éxito de las estaciones de carga individuales, sino también para una adopción más amplia de la movilidad eléctrica. Adoptar  soluciones seguras y escalables para impulsar el futuro del transporte limpio: eso es confianza digital para el mundo real", concluyó Coclin.

**Datos de contacto:**

DigiCert Latam

3125893314

Nota de prensa publicada en: [https://www.mexicopress.com.mx/los-autos-electricos-y-el-futuro-de-la](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Internacional Inteligencia Artificial y Robótica Movilidad y Transporte Industria Automotriz



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)