Sistema de información automotriz basado en un esquema de seguridad y protección jurídica

Diana Carolina Carrión Martínez, *Estudiante Maestría, INAOE,* Alejandro Medina Santiago, *Investigador, INAOE,* Ignacio Algredo Badillo, *Investigador, INAOE*

***Abstract*—En México los accidentes automovilísticos con daños materiales y/o humanos requieren realizar una investigación pericial ya que es obligatoría por ley, con el objetivo de descubrir lo sucedido y las causas del mismo. Sin embargo, existen ocasiones donde las pruebas son insuficientes para comprender lo sucedido o bien éstas han sido alteradas. El presente trabajo propone un dispositivo electrónico utilizando un sistema embebido basado en microcontroladores, eligiendolo por su capacidad de programación empleando un lenguaje de alto nivel, para realizar una tarea específica así como obtener una mayor eficiencia de sus componentes; guarda los datos generados por los sensores que se encuentran integrados dentro de los automóviles. Se agrega un esquema de seguridad para evitar que los datos sean alterados por algún elemento externo antes, durante o después de que el accidente automovilístico se produzca. El esquema propuesto ocupa blockchain, funciones hash, cifrado AES aunado a un esquema jurídico; el primero y segundo para asegurar la integridad durante todo el proceso jurídico mientras que el tercero para dar privacidad a los datos mientras son transferidos del automóvil a la máquina donde se examinan. Asimismo se propone un protocolo jurídico, planteando el manejo de las llaves de descifrado para o dentro del sistema jurídico mexicano disponiendo del mismo para tal propósito; en el manejo correcto de evidencias de los datos generados por el automóvil, empleados o usados para evidencia válida en caso de accidente automovilístico.**

***Index Terms*—Sistemas embebidos, AES, Funciones Hash, Protocolo Jurídico, Esquema de Seguridad, IoT**

I. Introducción

En el año 2017 en México se registraron un total de 367,789 accidentes automovilísticos solo considerando zonas urbanas y suburbanas [1]; cuando en éstos existen consecuencias con daños, tanto materiales como humanos, citando al capítulo VI artículo 183 del reglamento de Tránsito en Carreteras Federales [2], se realizará una investigación de los hechos por parte de la autoridad correspondiente. Sin embargo existen panoramas donde el automóvil queda dañado a un nivel que hace difícil el comprender lo que realmente ocurrió en la escena y/o los hechos en ella son ambiguos, dificultando el aclarar los hechos. De igual manera hay otro problema, la manipulación de la escena del crimen, incluyendo los indicios que se encuentran en esta, ya sea de forma natural, interviniendo elementos como la lluvia, animales y demás; o de forma artificial, siendo manipulado por alguna persona con la intención de obtener algún beneficio, afectando la declaración final del investigador y el veredicto que se dará.

La era tecnológica en la cual se encuentra la sociedad ha permitido el usar la ciencia en casi cualquier sitio para resolver problemas y automatizar procesos gracias a la gran aceptación que esta ha tenido, se persigue de forma constante el mejorar y hacer las tareas de forma más eficaz, produciendo tecnologías cada vez más eficientes, rápidas, fáciles de usar, atractivas, visionarias, etc. Para obtener una mayor cantidad de beneficios se requiere tener un mejor control sobre el intercambio de información que se da entre los sistemas, por lo que existe la intención de que cada vez más dispositivos se encuentren conectados a la red, generando e intercambiando de forma constante datos. Esto representa un gran desafío tanto de logística como de seguridad, puesto que dichos dispositivos contienen información privada, si los mismos que la crean y distribuyen no poseen un sistema de seguridad apropiado, el robo de información es probable .

Actualmente existen diferentes formas de proteger la información que se encuentra en formato digital, el tipo de protección que se dará dependerá de la necesidad que se tenga o lo que se desee hacer con la información; un ejemplo de método de protección para la información es el de un algoritmo que la modifica de un formato legible a un formato codificado, con el fín de que sea difícil el comprender y de esta forma darle confidencialidad al mensaje, cuando se desee regresar el mensaje a su estado original es necesario poseer una “llave” o clave que es usada junto con operaciones matemáticas para la alteración del texto de un formato legible a ilegible y viceversa. Estas operaciones se llaman algoritmos de cifrado y se enfocan en el área que el autor requiera, como ejemplo el asegurar la protección de la información con un algoritmo más robusto y complejo sacrificando el tiempo ejecución así como los recursos a usar.

Otros procedimientos que sirven para la protección de la información son las marcas de agua digitales, se emplean para ocultar información dentro de un objeto digital, introduciendo una cadena de bits en el mensaje que se enviará sin que afecte de forma visible o detectable al objeto, ocupando este método se busca que el mensaje pase desapercibido. El tipo de algoritmo utilizado para comprobar la integridad de los datos son las funciones hash, cuando un mensaje es introducido se hace uso de un algoritmo, el cual transforma dicho mensaje en una cadena de bits incomprensible que, a diferencia de los algoritmos anteriormente mencionados, la cadena de caracteres, resultado de la operación matemática realizada tendrá siempre la misma longitud. Si el contenido del mensaje cambia en lo más mínimo el resultado de la transformación cambia de igual manera de forma que resulte sencillo el notar la alteración en el mensaje. La función hash se creó con la particularidad de que una vez alterados los datos estos no volverán a formar el mensaje original, a lo anterior se

le conoce como picar y mezclar; gracias a las características de este algoritmo se usa para la autenticación de los datos, al comparar la cadena de datos que resulta de la operación, a la cual se le conoce como digesto, antes de realizar alguna acción en la cual el mensaje se pudo haber modificado con la generada despues de dicho acontecimiento.

La necesidad de proteger la información existe para todos los dispositivos que la generan puesto que el no hacerlo puede llegar a perjudicar los mismos. Una de las áreas a las cuales no se le ha puesto la suficiente atención a la protección de los datos es en el sector automotriz donde, para mejorar el control y modernizar sus productos las empresas automotrices agregan sensores, los cuales ayudan al conductor a tener una mejor experiencia, así como un sistema más intuitivo; mientras que del lado del software apoya mejorando la conducción. Contribuyendo a generar una gran cantidad de datos, que podrían servir para mejorar la experiencia de los usuarios de los automóviles o para realizar acciones malintencionadas.

Anteriormente se han creado sistemas como [3], [4] y [5] que ayudan a esclarecer los accidentes automovilísticos, estos han llegado a ser desde simples cámaras de video hasta sistemas avanzados que ayudan a determinar la situación del vehículo, llevando un seguimiento de lo que sucede alrededor haciendo uso de los distintos dispositivos con los que cuenta. En otros países ya se ha implementado sistemas de caja negra en los automóviles al darse cuenta de la creciente necesidad de dicho dispositivo ayudando en la investigación, asimismo proporcionando información sobre lo sucedido durante el accidente. Aunque existe el debate sobre si estos objetos violan los derechos de privacidad de los individuos a consecuencia de que los investigadores pueden descargar los datos contenidos en la caja negra sin necesidad de autorización previa del dueño, siendo que las leyes que deberían regular esto no son claras al respecto, aumentando la polémica con respecto a este aspecto; en la siguiente sección se describirá la situación jurídica actual con respecto al tratamiento de datos informáticos.

Se describira, en la sección III, el sistema propuesto buscando ayudar en la investigación de accidentes relacionados con vehículos, así como proporcionar una herramienta que apoye los procesos de averiguación. Proponiendo un sistema sencillo, útil y que cuente con la información necesaria para lograr tal tarea de forma satisfactoria. El sistema contendrá datos en forma de texto plano, obtenidos a partir de los sensores ya existentes dentro del automóvil, lo cual evitará el tener que agregar dispositivos y/o sistemas extras. Los datos al ser obtenidos por los sensores del mismo automóvil aportará conocimiento sobre su funcionamiento interno y si existieron problemas en este antes o durante el accidente.

II. Situación Jurídica

El 17 de Junio del año 2016 se llegó a un acuerdo general por parte de la Consejo de la Judicatura Federal, por el que se expide el Protocolo de actuación para la obtención y tratamiento de los recursos informáticos y/o evidencias digitales. Donde se manifiestan los deberes y compromisos que el poder judicial tiene para con los nuevos recursos tecnológicos y la protección que se debe dar por parte del poder judicial. Se consideran las obligaciones ya presentes en la constitución, las cuales son: la normatividad y los criterios para modernizar los sistemas y procedimientos administrativos internos, conformidad con el artículo 81, fracción XVIII, de la Ley Orgánica del Poder Judicial de la Federación; con el auge de las tecnologías de la información, es necesario proporcionar métodos y procedimientos que aseguren la detección, recolección, manejo, autentificación, análisis, procesamiento y resguardo de los recursos informáticos y/o evidencias digitales. La obtención de la información (elementos de prueba) constituye una de las facetas útiles dentro del éxito de una investigación, aspecto que demanda de los encargados de la recolección, preservación, análisis y presentación de las evidencias, una eficaz labor que garantice la autenticidad e integridad de estas, a fin de ser utilizadas posteriormente como parte de los diversos procedimientos que se tramitan en el Consejo de la Judicatura Federal y/o en su caso, ante las autoridades ministeriales o judiciales correspondientes, entre otras. Por lo anterior se acuerda un protocolo de actuación para la obtención y tratamiento de los recursos informáticos y/o evidencias digitales el cual toca los tópicos de: *I. Procedencia, II. Inspección, detección, aseguramiento y documentación, III. Recolección, IV. Registro, V. Embalaje, VI. Traslado y entrega para análisis, VII. Desembalaje, VIII. Análisis e informes, IX. Almacenamiento en el lugar de resguardo, X. Traslado para la presentación de los recursos informáticos y/o evidencia digital como Material probatorio, XI. Destino final.*

III. Sistema propuesto

El objetivo de este trabajo es presentar un protocolo jurídico, implementar un esquema de seguridad y desarrollar un dispositivo electrónico. El primero utiliza artículos y acuerdos para dar relevancia a los datos digitales obtenidos a través del dispositivo electrónico, y que sean considerados como evidencia probatoria sin que su ambiente sea un inconveniente para ello. El esquema de seguridad sirve para dar confidencialidad a los datos, así como para certificarlos durante todo el proceso como auténticos e íntegros, en caso contrario existe una forma de comprobar que tal alteración se ha llevado a cabo, esto al comparar las cadenas picadillos creadas a partir de la función hash y blockchain con los datos almacenados; por último, el dispositivo electrónico se ocupa de recopilar, guardar, procesar y enviar la información obtenida de los sensores del automóviles al dispositivo donde el investigador custodiará los datos.

Se expondrán los elementos que intervienen:

- Peritos, expertos en determinada materia, proporcionan información confiable y objetiva, producto de la aplicación del método científico y de técnicas especializadas; [6]
- Investigador, alguien que lleva adelante un proyecto orientado a la búsqueda de conocimiento y al esclarecimiento de hechos y de relaciones; [7]
- Evidencia, prueba determinante; [8]
- Juez de control, Órgano Jurisdiccional del Distrito Federal que interviene desde el principio del procedimiento y hasta el dictado del auto de apertura a juicio; [9]

- Llave de descifrado, porción de información que es utilizada para convertir un mensaje legible a una forma ilegible y viceversa; [10]
- Automóvil, vehículo autopropulsado destinado al transporte de personas o mercancías sin necesidad de carriles; [11]
- Bases de datos, conjunto de datos pertenecientes a un mismo contexto y almacenados; [12]
- Dispositivo, pieza o conjunto de piezas o elementos preparados para realizar una función determinada; [13]
- Sensores, aquello que tiene una propiedad sensible a una magnitud del medio, y al variar esta magnitud también varía con cierta intensidad la propiedad; [14]
- Repositorio, espacio centralizado donde se almacena, organiza, mantiene y difunde información digital; [15]
- Sistema embebido, sistema de computación diseñado para realizar una o algunas pocas funciones dedicadas. [16]

A. Metodología Jurídico

La metodología que se siguió para la parte jurídica, actuando los peritos, la evidencia digital, el juez de control y la llave de descifrado; en la cual se siguen los siguientes pasos durante su realización: a) revisar las leyes actuales concernientes a las evidencias digitales, b) examinar los procedimientos en caso de accidentes automovilísticos, c) analizar los sensores que proporcionan datos relevantes para la investigación y d) proponer una metodología jurídica que dé relevancia a la evidencia digital. Se revisan las leyes actuales que atañen a las evidencias digitales, así como el tratamiento que estas reciben desde la escena del crimen hasta su disposición, tales como [17], [18], [19], el artículo 251 del código nacional de procedimientos penales, donde se indica que es necesaria la autorización de un juez de control para descifrar la información que se encuentre dentro del dispositivo electrónico [20] y el artículo 9 de la Ley Modelo sobre el Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional [21], donde se estipula que toda información presentada en forma de mensaje de datos gozará de la debida fuerza probatoria. De igual forma se revisa cómo se tratan las evidencias y el procedimiento legal que se gestiona en caso de un accidente automovilístico con daños materiales y/o humanos, el cual se encuentra estipulado en el Manual para el manejo de la evidencia digital así como en Lineamientos para la obtención y tratamiento de los recursos informáticos y/o evidencias digitales, el último estipulado por el Poder Judicial de la Federación Consejo de la Judicatura Federal [22].

A continuación se hace una investigación, para conocer los sensores que se encuentran dentro del automóvil y proporcionan datos relevantes que ayudan a aclarar los hechos ocurridos antes, durante y después del accidente, así como las condiciones en las cuales se encontraba el automóvil, para esto se consulta a un perito judicial automotriz, así como a un experto automotriz. Una vez realizadas las correspondientes entrevistas se indaga sobre los sensores más comunes que se encuentran en las distintas marcas de automóviles. Se explica más acerca de los sensores en la sección de dispositivo electrónico.

La propuesta metodológica jurídica, apoya en dar relevancia a los datos aportados por los sensores, proporcionando les una base legal que los considere como un indicio fiable así como una pieza clave para el comprender los hechos ocurridos que afectaron al automóvil y/o que resultaron en el accidente automovilístico; para lograr esto se hace uso de las leyes existentes y procedimientos establecidos para la manipulación de la evidencia digital cuando existe la necesidad de una investigación o se ha pedido una por cualquiera de las partes involucradas.

La metodología indica que las empresas automotrices creen las llaves y las guarden; en caso de que exista un accidente de tráfico y las respectivas sean requeridas por el juez de control necesitara una orden judicial donde solicitará la llave antes mencionada a la empresa correspondiente y en cuanto ingrese dentro de la investigación será tratada como evidencia, por lo que tendrá su propia cadena de custodia teniendo, de esta forma, que seguir los lineamientos que se marcan para evitar su extravío o que se cree una copia no autorizada de la misma.

Cumplido la llave su objetivo, el cual es el descifrado de los datos, se buscará su pronta eliminación siguiendo los protocolos establecidos para lograr tal propósito; así como los procedimientos adecuados establecidos para tal finalidad. Se tendrá un programa que se emplea tanto para el descifrado de los datos como para la verificación de los mismos ocupando blockchain, funciones hash y el descifrador AES, dicho programa no guarda las llaves ni las claves se ocupan para realizar las tareas anteriores esto con la finalidad de evitar cualquier filtración de información importante que pueda llegar a afectar casos parecidos.

Las llaves se dejan al cuidado de las empresas y decidiendo estás como guardar las mismas, aunque se espera que se almacenen en una sola sede central y en ellas se salvaguarden dichas llaves, evitando que la información se filtre o extravíe. Se llevará un mejor control de las llaves y la información durante la investigación judicial gracias a que las primeras entran en la cadena de custodia desde que son entregadas al juez de control por lo que se tiene una estricta vigilancia sobre ellas desde que entran en la carpeta de investigación hasta que las mismas son desechadas.

Con respecto a la asignación de las llaves a los automóviles, las empresas decidirán cómo y de qué forma. La metodología jurídica antes descrita se representa en la figura **??**.

B. Esquema de Seguridad

En esta parte se consideran los actores que vienen siendo el automóvil, los peritos, los investigadores, las bases de datos, el dispositivo y los sensores.

Asimismo existen los procesos de almacenamiento seguro y recepción. En el *proceso de almacenamiento seguro* los datos son extraídos de los sensores dentro del automóvil y almacenados por el dispositivo electrónico. A partir de aquí el sistema: a) genera una cadena de caracteres única ocupando blockchain, b) cifra los datos ocupando AES y c) produce una cadena de caracteres única a toda la base de datos ocupando SHA-2. En el *proceso de recepción* los datos enviados del dispositivo electrónico dentro del automóvil se

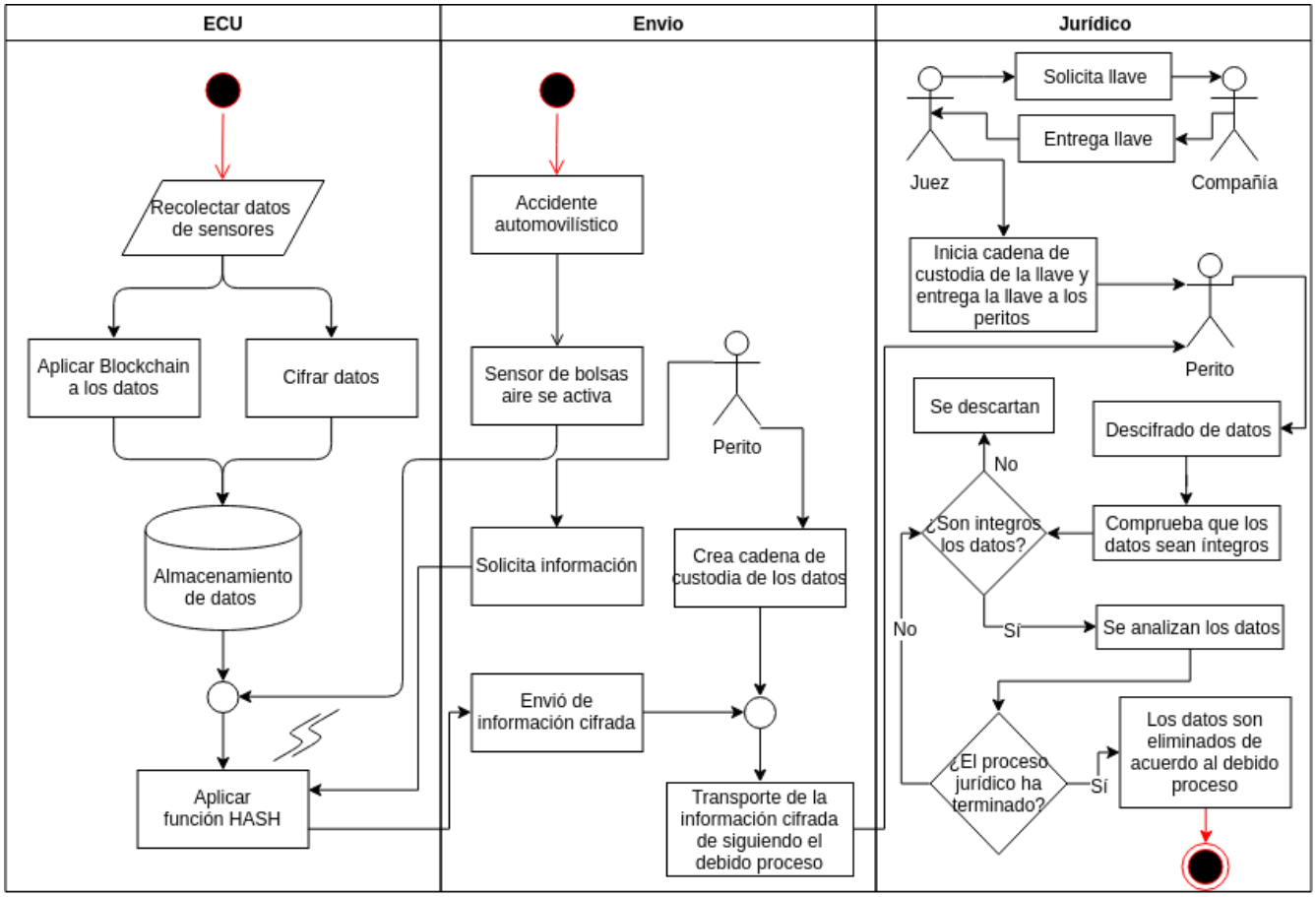

Fig. 1: Diagrama de flujo del sistema propuesto

reciben y almacenan dentro de un dispositivo digital en el cual el perito o investigador observa los datos obtenidos. En esta parte se: a) comprueba que la base de datos no ha sido alterada comparando la cadena de caracteres que procede desde la extracción, con la que se genera en el sistema del perito: b) descifra la información utilizando la llave obtenida del proceso jurídico y: c) comprueba la autenticidad de los datos comprobando la última cadena de caracteres de cada base de datos con la cadena generada por el sistema del investigador ocupando la llave obtenida por el proceso jurídico.

Se va a detallar el proceso de almacenamiento seguro a continuación:

En la parte de seguridad se busca que los datos extraídos de los sensores se ocupen para ayudar a esclarecer los hechos ocurridos en un accidente, sean confiables y ante cualquier intento de manipulación, exista una forma de advertir así como de comprobar que tales alteraciones se han realizado. Para esto, lo primero que se realizó fue encontrar una forma comprobar que los datos no han sido alterados durante el proceso de investigación, por lo tal es necesario tener una forma de comprobar que la modificación no ha ocurrido o que estos se hayan corrompido, puesto que si existe una mínima modificación de los mismos pueden ser descartados como evidencia al haber sesgo en la información; a continuación se necesita proteger los datos, evitando el que se puedan comprender el contenido que se encuentra guardado en el dispositivo electrónico otorgandole confidencialidad; posteriormente se perseguirá la integridad de la base de datos complera, esto con el propósito de, si existe alteración alguna, por cualquier medio o circunstancia se corrobore la misma.

La integridad de los datos es importante, ya que con la misma se puede comprobar que durante todo el proceso los datos han sido los mismos, haciéndolos legítimos. Para lograr dicho se ha elegido el blockchain [23] puesto que es un registro único, consensuado y distribuido en varios bloques, y gracias a que cada bloque contiene una cadena de caracteres particular conseguido después de ejecutar el blockchain, es factible el comprobar la integridad de los datos de forma sencilla, donde el proceso opera detectando si los datos han sido modificados, al agregar una cadena de caracteres al final de cada línea. El blockchain funciona de la siguiente manera: las cadenas de caracteres anteriormente mencionadas se cuentan de igual manera y al llegar a los 128 bits se extrae la función picadillo de las mismas, para esto se necesitan lo siguiente: la función picadillo anterior, la cadena anteriormente mencionada, una clave y la fecha junto con la hora en que se realizó dicha acción. Esto se repite hasta que todos los bloques de 128 bits cuentan con su cadena de caracteres resultante de la función picadillo. Una vez realizado la comprobación de la integridad se continua con la protección.

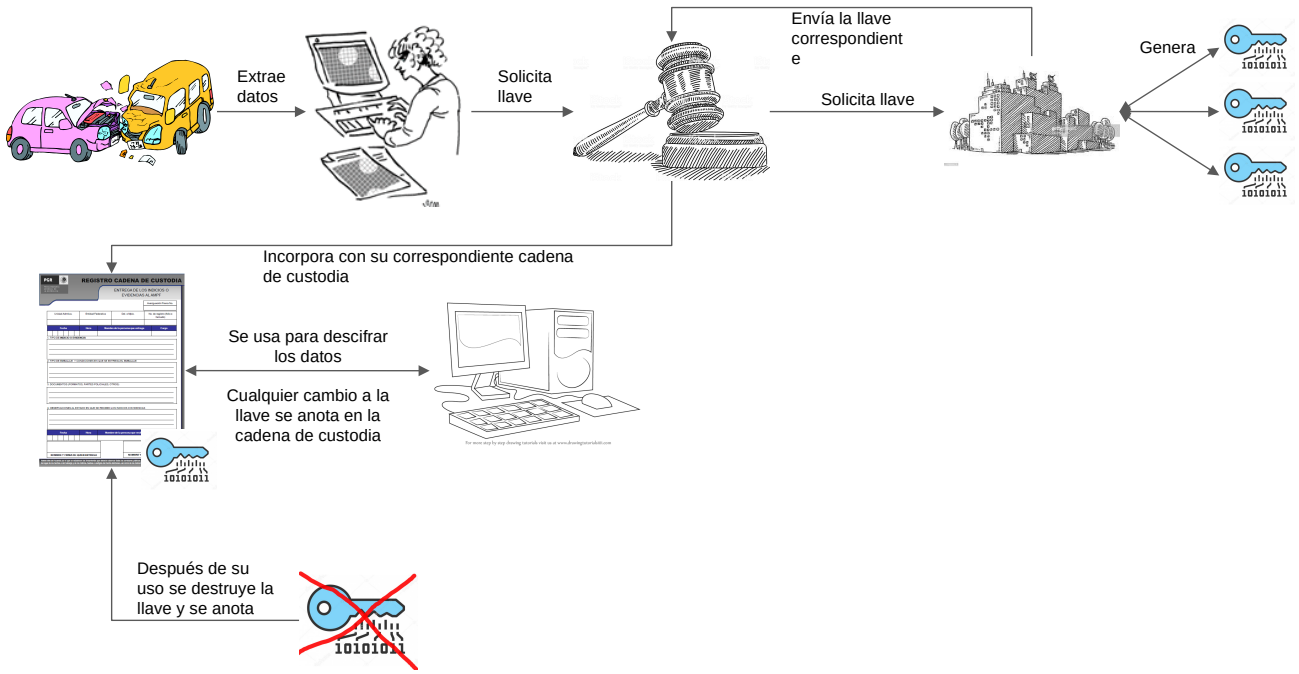

Fig. 2: Diagrama de flujo del protocolo jurídico

Para la confidencialidad de los datos se resolvió el cifrarlos, ya que dicho método transforma las cadenas de caracteres en un texto incomprensible así como el mensaje creado dificulta el que se pueda adivinar o, por medio de fuerza bruta, descifrar el texto original a menos que se tenga la llave de descifrado. Existen distintos tipos de cifrados, entre los cuales se encuentran los asimétricos y simétricos; se decidió ocupar el tipo de cifrado simétrico por la rapidez y simplicidad al momento de realizar los cálculos en comparación con el cifrado asimétrico. Una vez seleccionado el tipo de cifrado a usar se investigó entre los existentes decidiendo por el AES esto debido a que actualmente se encuentra entre los más seguros, conocidos y utilizados, al cual hasta el momento en que se escribe este artículo, los ataques a este cifrado no han tenido éxito y solo existen propuestas de ataque que podrían llegar a vulnerarlo aprovechando el sistema matemático ordenado en el que se basa.

El cifrado AES [24] funciona dentro del dispositivo de la siguiente manera, se cuentan los datos de los sensores que entran, cuando estos alcanzan el tamaño de requerido en bits comienza el cifrado de los datos haciendo uso de rondas donde en cada una de estas, un byte es reemplazado por otro. Los bits de ciertas columnas son rotadas de manera cíclica con otros bits de otras columnas para luego ser mezcladas y por último cada byte es combinado con la clave del round, esto se hace un determinado número de veces, definido por el tamaño de los bloques, lo que finalmente nos el mensaje cifrado.

Posteriormente estos datos se convierten en un archivo, a dicho archivo se le genera su código hash. El hash previo de la cadena anterior se guarda en un archivo en conjunto con el de los bloques de datos; ayudando a agregar otra capa de seguridad, la cual sirve para verificar que el archivo general no se modificó durante el traslado de un dispositivo a otro, puesto que el hash que se genera después de cifrar los datos y antes de enviarlos, lo que permite que al dispositivo recibirlos este pueda hacer el digesto del archivo y corroborar que estos no estén alterados por cualquier razón. La función hash elegida para realizar dicha tarea es el SHA-2 [25], puesto que, aunque actualmente ya existe el SHA-3, el SHA-2 todavía sigue vigente y hasta el momento no existen ataques que puedan dañar la seguridad del digesto.

Ahora se detallará el proceso de recepción; una vez obtenidos los datos, se comprueba que éstos sean auténticos al comparar la cadena hash incluida en el archivo con la generada por el sistema del perito utilizando la base de datos adquirida; seguidamente se descifrara dicha con la llave de descifrado, obtenida a través del proceso jurídico antes mencionado y el descifrador del AES. Una vez los datos se encuentren en forma de texto plano comprensible será posible comprobar si estos han sido modificados desde que salieron del dispositivo gracias a la cadena de caracteres del valor hash que se le incrustó a cada línea de datos con la generada por el sistema utilizando la clave obtenida. Puede comprobar que estos son integros al checar la última cadena hash creada, puesto que si ésta varía significa que los datos, ya sea por algún elemento externo o por corrupción, han sido alterados. En la figura 3 se observa el diagrama de flujo del Esquema de Seguridad que ya se ha explicado, en la figura 4 se detalla mas profundamente el proceso de almacenamiento seguro, mientras que en la figura 5 es el proceso de recepción lo que se expone.

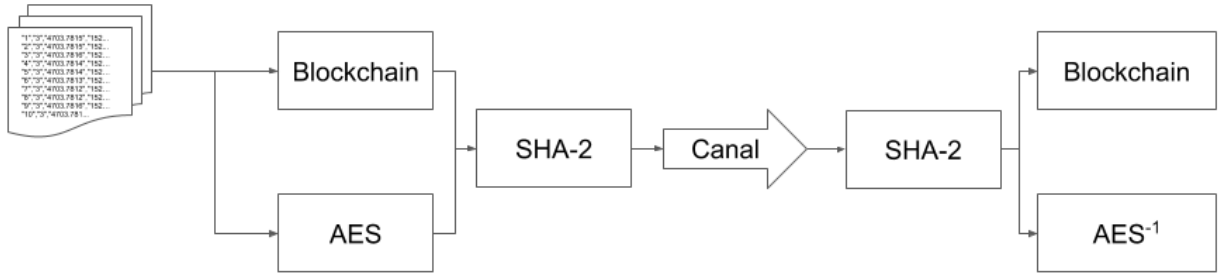

Fig. 3: Diagrama de flujo del Esquema de Seguridad

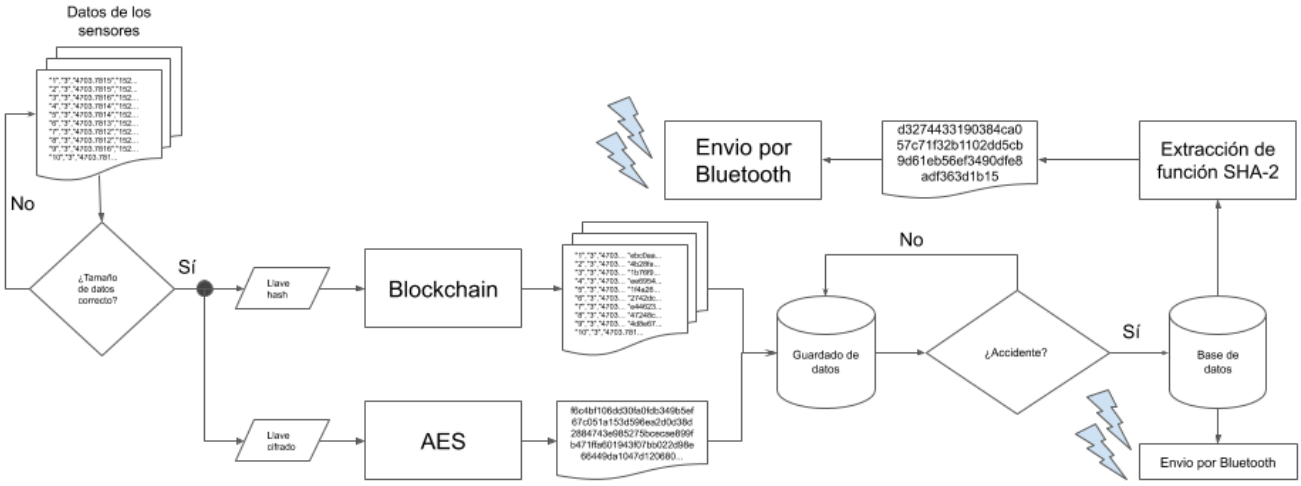

Fig. 4: Diagrama de flujo del proceso de almacenamiento seguro

C. Dispositivo electrónico

Los actores considerados para esta sección son el dispositivo electrónico, el repositorio, el automóvil, los sistemas embebidos y los sensores. En tanto los pasos a seguir son: a) examinar y escoger los sensores, b) extraer los datos de los sensores y crear un repositorio con estos, c) analizar la información de los sensores, d) analizar las necesidades para con los datos y su tratamiento, e) seleccionar los dispositivos a usar y f) armar el dispositivo.

Se procede a examinar los sensores que contiene el automóvil con la finalidad de ubicar aquellos que podrían servir en una investigación judicial o para las aseguradoras. Con el objetivo de lograr esto, se entrevistó a peritos vehiculares así como a expertos en el área automotriz con la meta de conocer los sensores que tomarían más relevancia en caso de accidente y de estos, cuáles son los más comunes que se encuentran en los automóviles; ya elegidos los sensores se extraen los datos y se crea un repositorio con el propósito de tener una gran cantidad de información para realizar experimentos y comprobar resultados. Entre los sensores elegidos para crear dicho repositorio están considerados los sensores de seguridad, algunos de los cuales son los siguientes: Radar telemétrico (el cual sirve para la prevención de colisión), sensor de ocupación de asiento (cuando hay un choque, éste indica dónde se activan las bolsas de aire), sensor de inclinación de ruedas (indica la posición en la que se encuentran las ruedas), sensor de inclinación (ayuda a la regulación de los faros), sensor de aceleración (detectan la aceleración en curvas así como para activar sistemas de protección de los pasajeros), sensor de vuelco (se activa cuando un ángulo varía respecto su posición de montaje), sensor de velocidad de giro de las ruedas (ABS), entre otros.

También se consideraron otros sensores como el sensor de posición del pedal, esto para saber qué tanto el conductor estaba apretando el acelerador o el freno o si en todo caso los estaba apretando; el sensor de presión de aceite y combustible, sensor de presión del líquido de freno, y demás. El repositorio sirve para analizar los datos, realizar los algoritmos que aseguran la información, así como tener al alcance diferentes datos de diferentes sensores de diferentes modelos de automóviles, lo cual ayuda a tener mayor rango para confirmar el correcto funcionamiento del software y hardware.

Con los datos extraídos que los sensores generan, analizando y comprendiendo la misma se descifra como los sensores representan, en texto plano, la información que les corresponde registrar, por ejemplo el sensor de posición nos da los sigu-

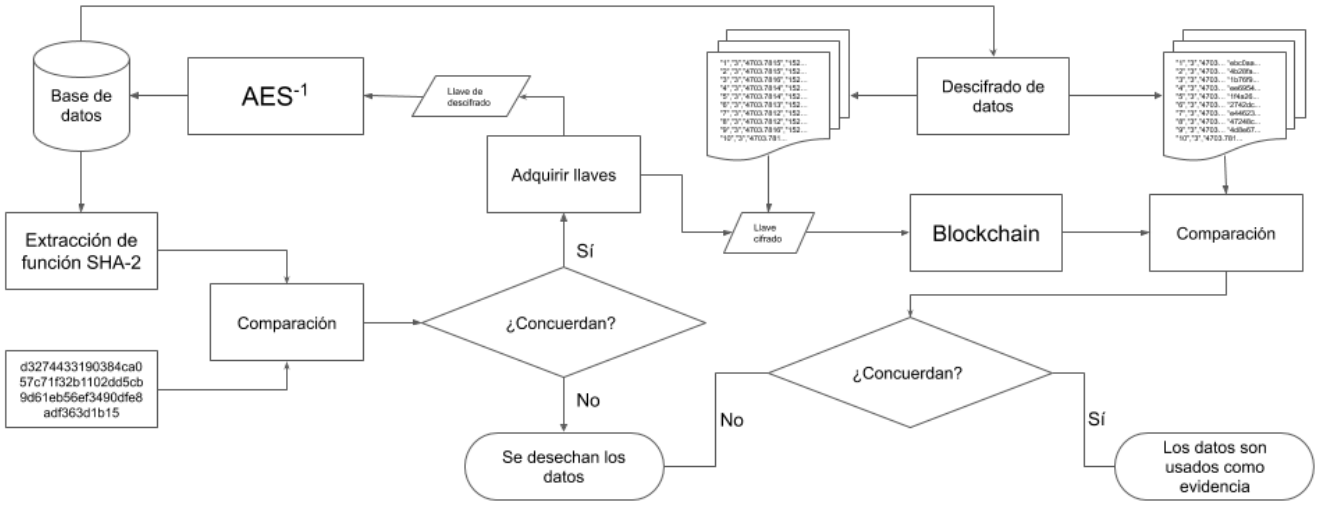

Fig. 5: Diagrama de flujo del proceso de recepción

ientes datos: ”1”,”3”,”4703.7815”,”1527.4713”,”359.9”,”2017-01-19 16:19:04.742113”, donde el primer dato es el id de posición; el segundo es el id del viaje; el tercero es la latitud; el cuarto la longitud; el quinto la altitud y el último la fecha y hora.

Se advierte de la necesidad de almacenar los datos dentro del dispositivo electrónico, así como procesarlos usando un esquema de seguridad, el cual ya se ha mencionado anteriormente, con la finalidad de protegerlos de algún daño a nivel software o si existe alguno identificar tal, y enviarlos de un dispositivo a otro usando algún medio de transmisión; de igual manera se busca que éste sea económico, tenga la suficiente memoria para almacenar el código necesario para realizar las funciones anteriormente nombradas, así como para almacenar los datos extraídos de los sensores del automóvil y una velocidad de procesamiento aceptable tomando en consideración el uso que se la va a dar. Con todo lo anteriormente mencionado, se desarrolla el dispositivo electrónico deseado.

Para logralo, sin recurrir a placas armadas, se analizó las opciones existentes en el mercado y las características con las que cada una cuenta, considerando como prioridad la velocidad del procesamiento de los datos con las que estas cuentan, lo que terminó con la elección de un sistema embebido, puesto que dispone de las entradas necesarias para soportar los módulos que se ocuparan, así como la capacidad de memoria necesaria para almacenar el código que se implementa y la velocidad de procesamiento con la cuenta es aceptable para lo que se pretenden realizar. En la tabla I se hará una comparación del ATmega2560 contra el sistema embebido Nano, la cual fue considerada como una placa a ocupar, explicando el porque de que el ATmega2560 fuera elegido.

Como se puede observar el voltaje que utilizan ambas es el mismo, pero mientras el número de pines en el ATmega2560 es mayor son los necesarios para conectar los módulos que se ocupan. La velocidad de reloj es la misma en ambos sistemas embebidos, sin embargo la Memoria Flash y la SRAM son mayores en el ATmega2560 ayudando a la velocidad de procesamiento de los datos; siendo éstas las principales razones para dicha elección.

	ATmega2560	Nano
Voltaje	5V	5V
Pines	54 D, 16 A	14 D, 8 A
Memoria Flash	256 KB	16 KB
SRAM	8 KB	1 KB
EEPROM	4 KB	512 bytes
Clock Speed	16 MHz	16 MHz

TABLE I: Comparación de las características de los arduinos ATmega2560 y Nano

Para la parte del envío de datos de un dispositivo a otro se analizaron las opciones de envío de forma alámbrica e inalámbrica optando por esta última; llegando a esta resolución cuando se vieron los pro y contras de cada una de las opciones. Mientras que la alámbrica podría dar más seguridad, al necesitar de conectarse directamente al dispositivo para sustraer la información, evitando el enviarlos de forma indiscriminada a los dispositivos cercanos como lo hace la comunicación inalámbrica, la misma es una desventaja considerable, puesto que en caso de un accidente catastrófico el conectarse al dispositivo sería casi imposible o, si este se encuentra en lugares de difícil acceso causaría retrasos en la investigación o incluso el no obtener la misma, ya que el conectarse ocupando algún medio físico sería casi imposible, sino hasta que se recupere el dispositivo; por lo cual se decidió que el envío de los datos de forma inalámbrica sería la mejor opción.

Ya resuelto que la forma de envío de datos se realiza por medios inalámbricos se procedió a elegir el tipo a usar. Las opciones que se discutieron fueron Wi-Fi y Bluetooth, quedando la última como la seleccionada por las razones se enlistan a continuación.

- En el caso de Wi-Fi el consumo de energía es elevado comparado con el Bluetooth, lo cual ayuda en dicho trabajo que busca reducir en lo posible dicha características para que se pueda utilizar en otras funciones.

- El rango de envío de datos está limitado a unos 30 m alrededor del dispositivo, en el caso de Bluetooth; dicho tamaño de área es aceptable en caso de necesitar extraer la información de un área poco accesible.

Decidido el método de transmisión a continuación se decide el tipo de módulo que se ocupara para dicha tarea, siendo el Bluetooth BLE SH-HC-08 y como su nombre lo indica es un Bluetooth Low Energy o Bluetooth de baja energía, que contiene el nuevo protocolo v4, dicho está pensando en disminuir todo lo posible la necesidad de energía de los dispositivos que lo usan.

Detallado lo anterior así como los sensores que se van a utilizar, se procede a ocuparse de los datos con la finalidad de prepararlos para la siguiente fase. En la figura 6 se observa el diagrama del sistema embebido, mostrando el dispositivo electrónico finalizado, los módulos que se van a emplear son: el módulo SDCard, el cual almacena la información y el módulo Bluetooth el cual se encarga de enviar la información cuando la misma es requerida. El módulo Bluetooth se encontrara en modo stand-by, es decir, sin enviar una señal como comunicarse con otro dispositivo, si no hasta que el accidente automovilístico ocurra, momento en el que el sistema embebido y la programación dentro de él lo active y el mismo comience a enviar una señal a la espera de una contestación para conectarse al dispositivo que contenga la clave correcta.

IV. Conclusiones

El sistema judicial actual en México se encuentra atrasado con respecto a incorporar a las leyes para las tecnologías de la información así como el asistirse con éstas, lo que genera una carencia a la hora utilizar y juzgar las mismas. Esto provoca que en caso de cometerse un delito donde se encuentren involucrados recursos tecnológicos, se dé un veredicto incorrecto o que el proceso se alargue más de lo necesario, existiendo la posibilidad de probar o ayudar a demostrar la inocencia o culpabilidad de una persona haciendo uso de los recursos obtenidos. Y al no existir una legislación que respalde dicha evidencia durante los procedimientos legales y jurídicos la misma es descartada. Por ello es necesario comprender el cómo funciona la tecnología y los avances que ofrece, de esta forma se dará un uso más efectivo de ella. Se tiene la intención de que el dispositivo propuesto ayude no sólo como evidencia válida durante investigaciones judiciales, sino también como un método de prevención, al comprender lo sucedido, el saber cómo, dónde y por qué ocurrió tal incidente. Se espera que este dispositivo no solo ayude a la justicia mexicana sino también a las personas.

References

[1] INEGI. (2018) Accidentes de tránsito terrestre en zonas urbanas y suburbanas. [Online]. Available: https://www.inegi.org.mx/sistemas/olap/proyectos/bd/continuas/transporte/accidentes.asp

[2] R. de Tránsito en Carreteras y Puentes de Jurisdicción Federal, "Artículo 183," 11 2012.

[3] H. Mansor, K. Markantonakis, R. N. Akram, K. Mayes, and I. Gurulian, "Log your car: The non-invasive vehicle forensics," in *2016 IEEE Trustcom/BigDataSE/ISPA*, Aug 2016, pp. 974–982.

[4] X. Yi, A. Bouguettaya, D. Georgakopoulos, A. Song, and J. Willemson, "Privacy protection for wireless medical sensor data," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 3, pp. 369–380, May 2016.

[5] R. S. S. k. B. A. U. V. C. V. Roja, R. Revathi, "Intelligent safety using smart blackbox," *SSRG International Journal of Electronics and Communication Engineering*, vol. 5, March 2015.

[6] P. R. Guerra, *El Ministerio Publico y su vinculo con los servicios periciales*, 1st ed. "", 11 2017, ch. 14, pp. 2–77.

[7] anonimo, "Investigador," 2019, Última actualización 20 jul 2019 a las 12:56. [Online]. Available: https://es.wikipedia.org/wiki/Investigador

[8] J. Martínez, "Evidencia," 2017, diccionario Social — Enciclopedia Jurídica Online. [Online]. Available: https://diccionario.leyderecho.org/evidencia/

[9] D. G. de Servicios Legales, "Glosario," 2019, gobierno de la Ciudad de México. [Online]. Available: https://data.consejeria.cdmx.gob.mx/index.php/dgsl/glosario/Glosario-Consejera-1/J/JUEZ-DE-CONTROL-31/

[10] G. J. Simmons, "A survey of information authentication," *Proceedings of the IEEE*, vol. 76, no. 5, pp. 603–620, May 1988.

[11] R. A. Española, *Automóvil*, 23rd ed., ser. 15. Felipe IV, 4 - 28014 Madrid: Real Academia Española, 7 2018, vol. 1, edición del Tricentenario.

[12] J. D. Ullman, *A first course in database systems*. Upper Saddle River, N.J: Prentice Hall, 1997.

[13] J. P. P. y María Merino, "DefiniciÓn de dispositivo," 2014. [Online]. Available: https://definicion.de/dispositivo/

[14] S. Bennett and I. of Electrical Engineers, *A History of Control Engineering, 1930-1955*, ser. Control, Robotics and Sensors Series. P. Peregrinus, 1993. [Online]. Available: https://books.google.com.mx/books?id=VD_b81J3yFoC

[15] M. R. Domínguez López, *Los derechos de autor y el uso de los repositorios institucionales en México*. México: UNAM, 5 2014, p. 60, consultado el 23 de enero de 2017.

[16] M. Barr, "Embedded systems glossary," 4 2007.

[17] B. J. BECERRA, "El proceso civil en méxico," *México: Porrúa SA*, 2006.

[18] J. O. Favela, *Derecho procesal civil*. Oxford University Press, 2013.

[19] M. A. D. de Léon, *Las pruebas en el derecho procesal del trabajo*. Textos universitarios, 1981.

[20] C. N. de Procedimientos Penales, "Artículo 251," 7 2014.

[21] L. M. sobre el Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, "Artículo 9," 12 1996.

[22] P. J. D. L. F. C. D. L. J. Federal, *Lineamientos Para La Obtención Y Tratamiento De Los Recursos Informáticos Y/O Evidencias Digitales*. México: Poder Judicial De La Federación Consejo De La Judicatura Federal, 6 2016, p. 11.

[23] L. FORTNEY, "Blockchain explained," 2019, last accessed 21 September 2019. [Online]. Available: https://www.investopedia.com/terms/b/blockchain.asp

[24] U. S. N. I. of Standards and T. (NIST), "Announcing the advanced encryption standard (aes)," 11 2001, federal Information Processing Standards Publication 197.

[25] P. C. v. O. Alfred J. Menezes and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 8 2001, vol. 5.

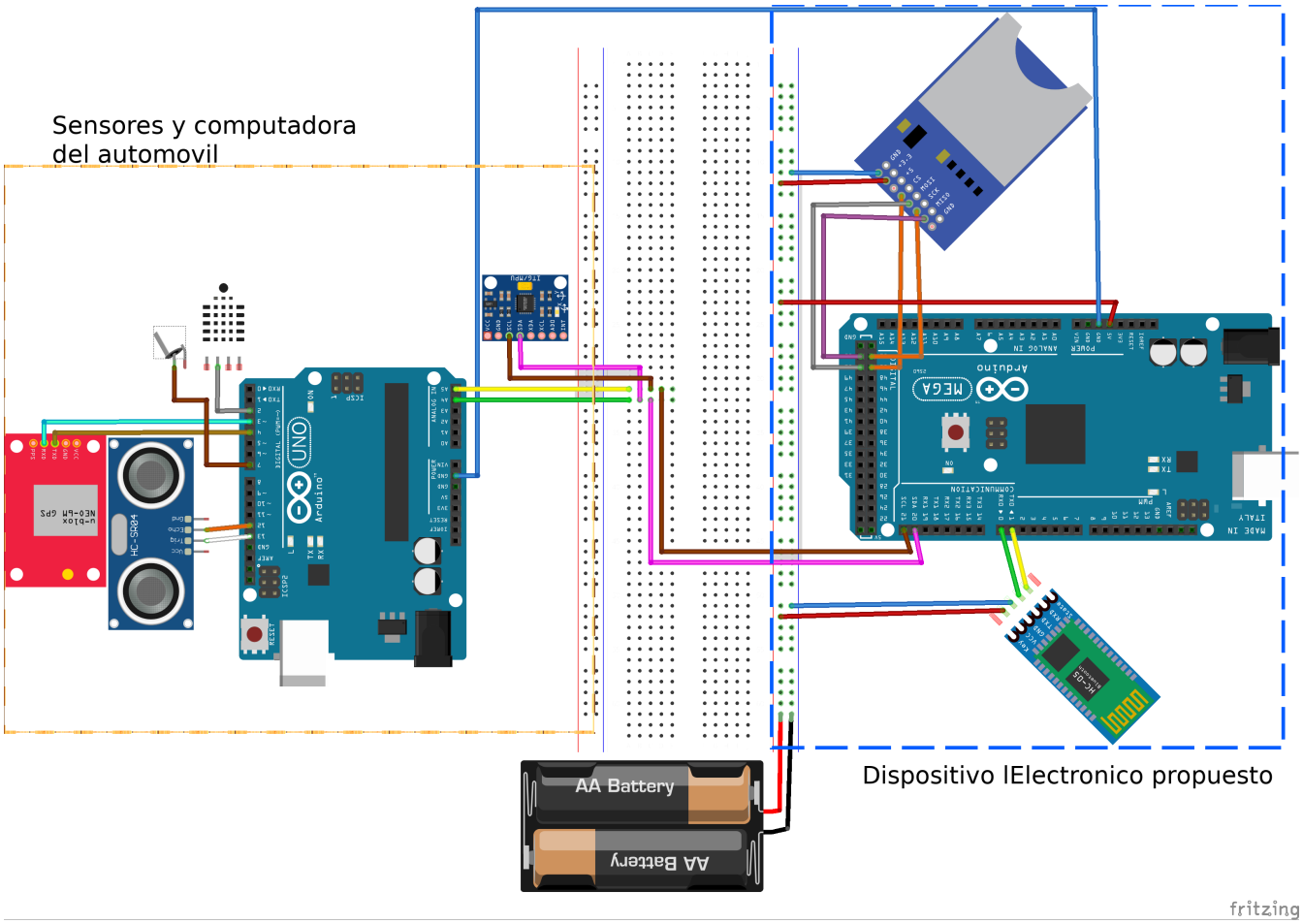

Fig. 6: Diagrama del protoboard del dispositivo electrónico