<Análisis del sitio Internet **www.dian.gov.co** y de su **app>**

Versión pública

Noviembre 2018

<KTRL+INFORME>

<K+ LAB>

Fundación Karisma

Fundación Karisma

<K+LAB>
SEGURIDAD DIGITAL Y PRIVACIDAD

Bogotá, Colombia

2018

En un esfuerzo para que todas las personas tengan acceso al conocimiento, Fundación Karisma está trabajando para que sus documentos sean accesibles, eso quiere decir que su formato incluye metadatos y otros elementos que lo hacen compatible con herramientas como lectores de pantallas o pantalla braille. El propósito del diseño accesible es que todas las personas puedan leer, incluidas aquellas que tienen algún tipo de discapacidad visual o de dificultad para la lectura y comprensión.

Más información sobre documentos accesibles en: http://www.documentoaccesible.com/#que-es

Consulta este documento en línea en el sitio web Karisma en:
https://karisma.org.co/descargar/analisis-del-sitio-internet-www-dian-gov-co-y-de-su-app/

Informe de

Fundación Karisma

Coordinación editorial

Pilar Sáenz

Diego Mora Bello

Diseño

Daniela Moreno

Análisis del sitio Internet www.dian.gov.co y de su app

Versión pública

Este informe se basa en investigaciones que se hicieron en agosto y septiembre del 2017, y en una verificación de Enero del 2018.

En Febrero del 2018 una versión completa de este informe se envió a la DIAN y al MINTIC y se generaron intercambios.

En mayo 2018, se presentó una parte de estos análisis en una conferencia internacional (*DiY Kit: How to analyze privacy and security on smartphone apps*, RightsCon 2018, Toronto).

En noviembre 2018, dándonos cuenta que la gran mayoría de las recomendaciones importantes todavía no habían sido tomadas en cuenta por parte de la DIAN, decidimos publicar este informe. Sin embargo, quitamos ciertas partes sensibles (vulnerabilidades de ciertos servidores y eventual informaciones inapropiadas en el sitio) que aun aparecen indicadas como título pero que no tienen el texto desarrollado.

Finalmente, actualizamos la Tabla sintética de recomendaciones, añadiendo una columna que da cuenta del estado de la implementación de cambios.

Tabla de contenido

Resumen Ejecutivo

La Fundación Karisma, fundada en 2003 y localizada en Bogotá (Colombia), busca responder a las oportunidades y amenazas que surgen en el contexto de la "tecnología para el desarrollo" para el ejercicio de los derechos humanos, desde perspectivas que promuevan la libertad de expresión y las equidades de género y social. Karisma trabaja desde el activismo con múltiples miradas —legales y tecnológicas— en coaliciones con socios locales, regionales e internacionales.

En el marco de un nuevo proyecto, la organización analiza sitios web y aplicaciones para teléfonos inteligentes y tabletas del Gobierno colombiano con el objetivo de contribuir a mejorar su información, su seguridad digital y su privacidad, para el beneficio de la ciudadanía y de las entidades responsables de estos sitios. Nos parece que estos análisis también pueden ayudar a la entidad a cumplir de mejor manera la Ley de protección de datos (Ley 1581 del 2012) y a incorporar los últimos lineamientos del Gobierno en materia de seguridad digital, la política nacional de seguridad digital en particular.

En un primer ejercicio, analizamos la página imeicolombia.com.co y, tras la socialización de nuestro análisis, se generaron cambios importantes en su implementación, lo que nos demostró que es un ejercicio valioso y que puede llevar a mejoras importantes[1]. Hicimos también un segundo ejercicio con el sitio web de la Unidad para la Atención y Reparación Integral a las Víctimas, el cual fue presentado junto con la entidad y el Mintic en el IV foro de seguridad digital en Bogotá, como un "caso de éxito de colaboración entre la sociedad civil y Gobierno"[2].

En el presente informe, hemos analizado de forma no intrusiva —desde el exterior— el sitio web de la DIAN, http://www.dian.gov.co/, que además de información de consulta, también ofrece servicios extensamente usados por los ciudadanos colombianos, extranjeros residentes y empresas. El informe presenta también el análisis de la aplicación de la DIAN para teléfonos inteligentes y tabletas, que provee un servicio de CHAT y de localización de los puntos de atención cercanos.

Este ejercicio busca ayudar a mejorar los aspectos mencionados y en particular la seguridad digital del sitio web y de la aplicación.

Cabe mencionar que antes de comenzar el análisis que estamos presentando, enviamos un correo electrónico a la DIAN con el fin de informarles sobre la exploración que íbamos a hacer y así actuar con total transparencia. Cuando decidimos extender el análisis a la aplicación de la DIAN, enviamos otro correo electrónico (Anexo 1). Además, en los formularios en línea que se completaron para hacer el análisis, también mencionamos la Fundación Karisma y el análisis que estábamos realizando cuando ellos lo permitían[3].

---

[1] *Véase* Fundación Karisma (2017, 24 de marzo). *Análisis de «imeicolombia.com.co»: cronología de un diálogo con el Gobierno*. Disponible en https://karisma.org.co/analisis-de-imeicolombia-com-co-cronologia-de-un-dialogo-con-el-gobierno/.

[2] https://seguridaddigitalcolombia.com/site/index.php/es/#agenda/program

[3] Ciertos formularios solo permiten entrar un número (NIT, Cédula, RUT, etc.). Por lo tanto, en estos no se podía hacer referencia a la Fundación Karisma o a nuestro análisis.

Queremos resaltar que el análisis que se presenta a continuación se realizó “desde el exterior”, y que no fuimos más allá del “primer nivel” en los formularios que revisamos. Utilizamos solo métodos y análisis a veces técnicos pero siempre pasivos, no intrusivos, documentados y reproductibles. Para decirlo en términos sencillos, miramos la casa desde el exterior pero no entramos en ella.

El informe cuenta con tres ejes principales: cumplimiento con los requisitos de la ley de protección de datos (información legal, transparencia y contratos), seguridad digital del sitio web; y privacidad y *tracking*.

Al final, se ofrecen una serie de recomendaciones que van desde la más urgentes y prioritarias a las importantes pero menos prioritarias. El informe va acompañado de 22 anexos que incluyen información complementaria o técnica, donde se detallan o apoyan los argumentos y constataciones del informe.

Cabe mencionar que el análisis puso en evidencia varios puntos positivos en el sitio de la DIAN: una buena implementación del protocolo seguro HTTPS en la mayoría de las páginas y formularios, una información legal bastante completa, un sitio principal albergado en Colombia, etc.

Sin embargo, el análisis también arrojó algunos puntos para mejorar. Algunos prioritarios, que recomendamos evaluar y solucionar a la mayor brevedad posible. Estos tienen que ver principalmente con: 1. la seguridad del sitio y de la aplicación para teléfonos inteligentes y tabletas; 2. el servidor web de [...] 3. el protocolo HTTPS no se implementa en ciertas partes del sitio donde se piden datos personales a los usuarios (CHAT y escuelavirtual); 4. la aplicación para teléfonos y tabletas “DIAN” sufre vulnerabilidades de seguridad y transmite los datos de los usuarios a Google; 5. hay una recomendación importante vinculada con la neutralidad tecnológica (definido en la ley 1341 del 2009) y la compatibilidad con los sistemas de todos los usuarios. El proceso de firma digital del sitio Internet no es compatible con otros sistemas operativos distintos a Windows (Mac y Linux por ejemplo). También se resaltan problemas menores pero que no deben ser ignorados para un sitio en Internet tan sensible e importante como el de la DIAN. Por ejemplo, la información del sitio no cuenta con todos los requisitos de la ley de protección de datos “Habeas Data”, hay una difusión publica de hojas de vida de empleados de la DIAN que podría ser un error y el uso de la herramienta de medida y estadísticas de Google (analytics) genera un rastreo detallado de la actividad de los usuarios en el sitio de la DIAN.

El informe provee, por lo tanto, una serie de recomendaciones que hemos resumido en la “tabla sintética de recomendaciones” (parte 7). Esperamos que estas recomendaciones sean evaluadas y que la DIAN pueda resolver los problemas que identificamos. Insistimos en el hecho que ciertos problemas son importantes y deben ser resueltos a la mayor brevedad.

Si bien, la metodología que usamos es muy limitada, ya que sólo usamos métodos no intrusivos y analizamos sólo la información pública del sitio y de la aplicación, creemos que es necesario que la institución utilice estos hallazgos para plantear un plan de mejora. Suponemos que desde la DIAN, con el apoyo de MinTIC, y otras instancias estatales, se puede realizar una exploración más profunda, con base en una auditoría externa, para detectar y mejorar otros puntos que no hemos logrado identificar debido a las limitaciones de nuestro análisis.

Nuestro principal objetivo al dar a conocer este informe a la entidad es que se resuelvan estos problemas de la manera más rápida y eficiente posible. Reiteramos que nuestra intención es contribuir a mejorar la seguridad digital, la protección de datos y la privacidad en el uso que se hace de Internet en Colombia. En el proceso, buscamos también mantener un diálogo franco que permita resolver los problemas identificados como sucedió con los dos primeros análisis de este tipo que hemos hecho y ya hemos mencionado.

1. Presentación general del sitio Internet www.dian.gov.co

www.dian.gov.co es el sitio Internet de la DIAN, la *Dirección de Impuestos y Aduanas Nacionales*, que es una unidad administrativa especial (UAE) del Estado colombiano[4]. El sitio provee información y servicios en línea a los ciudadanos y las empresas, que incluyen:

- solicitud de inscripción y obtención de copia del RUT;
- declaración de actividad económicas y de rentas;
- otros servicios relacionados con los impuestos (consulta estado RUT, solicitud de devolución o compensación;
- servicios vinculados con operaciones aduaneras (ingreso, salida o tránsito de mercancías) ;
- un CHAT en línea;
- un servicio de formación en línea ("Escuela Virtual");
- un servicio de denuncias en línea, vinculado con la *Agencia del Inspector General de Tributos, Rentas y Contribuciones Parafiscales*[5].

[4]Decreto 2117 de 1992, Art. 2: "La Dirección de Impuestos y Aduanas Nacionales, es una Unidad Administrativa Especial, constituida como una entidad de carácter técnico, adscrita al Ministerio de Hacienda y Crédito Público, la cual cuenta con regímenes especiales en materia de administración de personal, nomenclatura, clasificación, carrera administrativa especial, salarios, prestaciones, régimen disciplinario, presupuesto y contratación administrativa, de acuerdo con los regímenes que regulaban las entidades que por este decreto se fusionan y de conformidad con lo previsto en las disposiciones finales del presente Decreto."

[5]Sitio Internet de la Agencia ITRC : http://www.itrc.gov.co/itrc/

El sitio web provee servicios al público que pueden involucrar una cantidad importante de datos personales incluyendo datos sensibles y financieros. Además se dirige potencialmente a toda la población del país.

Por lo tanto, el nivel de sensibilidad de los datos que se transfieren a través del sitio web de la DIAN y el alto número de potenciales personas usuarias (los ciudadanos de Colombia y residentes extranjeros en el país) obliga a tener fuertes consideraciones en términos de transparencia, seguridad, privacidad y protección de datos. Esto nos permite asignarle una alta relevancia a los problemas identificados en este informe.

Explicación inicial: sobre el uso de HTTPS en lugar de HTTP

En las siguientes partes de este informe insistimos varias veces sobre el hecho de que el protocolo[6] HTTP (*Hyper Text Transfer Protocol*), usado en el sitio web de la DIAN, no es seguro. En su lugar, debe usarse e implementarse correctamente el protocolo HTTPS[7] (*Hyper Text Transfer Protocol Secure*). ¿Por qué?

El protocolo HTTP no permite asegurar:

- La **autenticación** del sitio web, es decir, no permite garantizar que el sitio web es de quien dice ser.
- La **confidencialidad** de los datos que se intercambian entre el computador de la persona usuaria y el sitio web (el servidor), puesto que los datos se envían a través de un canal no cifrado.

Cuando no se autentica el sitio web, se corre un mayor riesgo de que una persona entre a un sitio falso con apariencia del verdadero, concebido con el fin de robar datos personales o contraseñas. Esto se llama *phishing* y su uso está ampliamente documentado en la historia de la seguridad digital.

El riesgo de no contar con una garantía de confidencialidad mediante un cifrado en la transmisión de datos es que todos los intermediarios entre el computador de la persona y el sitio web (servidor) pueden potencialmente acceder a esos datos. Esto incluye, por ejemplo, desde el punto WiFi[8] o la red interna de una empresa hasta los operadores de comunicación y todos los intermediarios técnicos.

En cambio, la alternativa segura, es decir, el protocolo HTTPS en cuanto sea bien implementado, permite (gracias al cifrado) asegurar la autenticación del sitio y la confidencialidad de los datos enviados y recibidos.

[6]De acuerdo a un artículo de Wikipedia, un protocolo de comunicaciones en informática y telecomunicaciones «es un sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para transmitir información [...] ».

[7]Técnicamente, consiste en un protocolo HTTP encapsulado en una capa SSL o TLS.

[8]Además, el punto WIFI puede ser falso. Por ejemplo, alguien se puede sentar en un establecimiento de *McDonald's* o un lugar cercano y crear desde su computador un punto WiFi abierto llamado «Wifi McDonalds». Es probable que muchas personas creen que la conexión es del establecimiento y se conecten. Quien creo esa conexión fraudulenta, entonces, podrá interceptar todos los datos enviados y recibidos que no estén cifrados.

2. Cumplimiento de los requisitos de la ley de protección de datos: información, confianza y transparencia

2.1. Identificación del sitio y política de privacidad

El sitio web es bien identificado como un sitio web de la DIAN y del Gobierno colombiano en su cabecera:

Y en su pie de página, el sitio Internet provee un enlace (en letra pequeña…) hacía las "***Políticas de privacidad y términos de uso***" **y una "*Política Facebook*"**:

La página correspondiente al primer enlace[9] contiene una sección relacionada a la privacidad y la confidencialidad de los datos personales que es la siguiente:

> *Se encuentra sujeta a confidencialidad y protección de datos toda aquella información personal que el usuario ingresa libre y voluntariamente al Sitio Web de la DIAN, así como aquella de obligatorio ingreso, tal como: nombre de usuario, número de identificación y palabra clave o password. El usuario podrá corregir o actualizar esta información en cualquier momento.*
>
> *La DIAN se reserva el derecho de modificar las normas de confidencialidad y protección de datos con el fin de adaptarlas a nuevos requerimientos legislativos, jurisprudenciales, técnicos o todos aquellos que le permitan brindar mejores y más oportunos servicios y contenidos informativos.*
>
> *La información proporcionada por el usuario al registrarse en portal de la DIAN está resguardada tecnológicamente. El usuario es el único responsable de mantener su palabra clave o password y la información de su cuenta. Para disminuir los riesgos, la DIAN recomienda al usuario salir de su cuenta y cerrar la ventana de su navegador cuando finalice su actividad, más aún si comparte su*

[9]Disponible aquí : http://www.dian.gov.co/dian/12SobreD.nsf/pages/Politicas_Privacidad?OpenDocument

computadora con alguien o utiliza una computadora en un lugar público que preste servicios de acceso a Internet.

Si bien el portal de la DIAN posee un sistema de protección tecnológico que va desde sus servidores hasta la salida a Internet, ninguna transmisión por Internet puede garantizar su seguridad al 100%. La DIAN no puede garantizar que la información ingresada a su Sitio Web o transmitida utilizando su servicio sea completamente segura, con lo cual el usuario asume su propio riesgo.

La DIAN no compartirá ni revelará la información confidencial del usuario con terceros, excepto cuando se tenga la autorización expresa del usuario titular de la misma o cuando ha sido requerida por orden judicial o administrativa en los términos definidos por la ley.

Si el usuario ingresa al Sitio Web de la DIAN significa que ha leído, entendido y aceptado los términos antes expuestos. Si no está de acuerdo con ellos, tiene la opción de no ingresar al Sitio Web de la DIAN.

Si bien es un punto positivo que el sitio cuente con una **política de privacidad,** que da consejos a los usuarios sobre el uso de las claves y provee ciertas garantías importantes en cuanto a la transmisión de informaciones confidenciales del usuario, no hace referencia a la Ley de protección de datos ("Habeas data") ni a las obligaciones de la DIAN como responsable de tratamiento de datos. En particular, no hay mención explícita sobre la finalidad del tratamiento y si hay un encargado distinto a la DIAN. Tampoco se informa a las personas que son titulares de los datos (los usuarios del sitio) sobre sus derechos y, en particular, los de acceso y rectificación.[10] Por esto, en términos legales es una información que se debería completar con fin de cumplir completamente con las disposiciones de la ley colombiana de protección de datos.

El sitio web cuenta también con una **política Facebook**. Esta tiene que ver más con el respeto que se tiene que dar en los comentarios ya que la página no maneja directamente datos personales. Sin embargo, es positivo que cuenta con esta parte :

la DIAN, como administrador, se reserva el derecho a eliminar, sin derecho a réplica, cualquier aportación que:
[...]
• Incorpore datos de terceros sin su autorización.

La DIAN cuenta también con unas páginas en otras redes sociales : YouTube, Twitter y Soundcloud. Ellos aparecen vía botones clásicos abajo de la página de inicio:

Cabe mencionar que que el enlace "Google +" no funciona y apunta hacia la página *Twitter* de la DIAN.

[10] *Ley de protección de datos personas*, Ley 1581 del 2012, artículos 8 y 12.

En cualquier caso, se podría fácilmente generalizar la “Política Facebook” hacia una “Política de redes sociales” ya que estos mismos principios se pueden aplicar en estas distintas redes.

Recomendación sobre información legal

Es positivo que exista una política de privacidad y una política Facebook. Sin embargo, es necesario hacer referencia a la Ley de protección de datos colombiana e incluir sus obligaciones informativas, en particular los derechos de los usuarios (acceso y rectificación). Para darle más visibilidad se aconseja incluir un enlace visible al final de cada formulario que recoja datos personales. Además, se aconseja extender la política de Facebook hacía una política de redes sociales de la DIAN, que se aplique a las distintas redes sociales en las que la DIAN administra un perfil.

2.2. Validación de la identidad de la página y uso del HTTPS

Cuando uno llega a la página de inicio de la DIAN, se encuentra la siguiente URL: «http://www.dian.gov.co».

Esto significa que el sitio usa el protocolo HTTP, el cual como ya lo hemos mencionado no permite validar la identidad de la página.

Sin embargo, como veremos después, la mayoría de páginas del sitio que contienen un formulario donde se solicitan datos se encuentran en el subdominio «muisca.dian.gov.co» y usan el protocolo HTTPS. En estas se puede tener un segundo nivel de verificación sobre la identidad del sitio, examinando el certificado criptográfico de la página (o exportando el certificado, ver anexo 2):

La imágen nos muestra que es un certificado emitido por la empresa GeoTrust para la Dirección de Impuestos y Aduana Nacionales de BOGOTÁ DC. La parte siguiente del nombre común del certificado (« EV SSL CA – G4 ») nos indica[11] que se trata de un certificado SSL de la autoridad de certificación G4 de Geotrust obtenido por un proceso de tipo “Extended Validation” lo que da un nivel de garantía alto sobre la verificación de la identidad del sitio y de su titular[12].

[11]Leer explicaciones sobre las nomenclaturas y procesos usadas por la empresa de certificación Geotrust, aquí:
https://www.geotrust.com/resources/extended-validation-ssl/ y
https://www.geotrust.com/resources/root-certificates/

[12]El certificado de tipo Extended Validation (EV) da más garantías e información sobre la organización que adquirió el dominio, como se explica en un artículo en Wikipedia: «Un certificado de validación ampliada (EV, por sus siglas en inglés) es un certificado utilizado para sitios web HTTPS y software que demuestra la entidad legal que controla el sitio web o el paquete de software. La obtención de un certificado EV requiere la verificación de la identidad de la entidad solicitante por una autoridad de certificación (CA,

Recomendación sobre la autenticación del sitio

Se recomienda implementar el protocolo HTTPS no sólo en las páginas que contengan formularios con datos personales sino también en las otras páginas del sitio y en particular en la página de inicio, con fin de permitir una validación de la identidad del sitio, su autenticación.

2.3. Análisis del dominio y del *hosting*: servidores con direcciones IP propias y en Colombia

El whois en el dominio "dian.gov.co" muestra que la DIAN registro directamente y a su nombre este dominio ante la empresa ".CO INTERNET S.A.S." que tiene a su cargo el dominio ".co" (Anexo 3).

Una búsqueda de las direcciones IP de los servidores web del sitio y sus principales servicios en línea da lo siguiente :

- 190.24.148.167 para http://www.dian.gov.co/;
- 190.24.148.130 para el subdominio muisca.dian.gov.co, IP (servicios en línea relacionado con los impuestos) ;
- 190.24.148.145 para el subdominio importacionescarga.dian.gov.co (parte aduanera) ;
- 190.24.148.147 para el subdominio certificadosdeorigen.dian.gov.co;
- 190.24.148.137, para el subdominio escuelavirtual.dian.gov.co.

Todas estas direcciones IP pertenecen a la DIAN y están situadas en Colombia y un *who is* en cada una da el mismo resultado (Anexo 4).

No hay recomendación en esta parte.

2.4. Tercerización del servicio de chat y de su *hosting*

El sitio de la DIAN cuenta con un servicio de chat en línea ubicado en el dominio externo: «asistenciachat.com».

A través de un análisis de las *cookies* y de las capturas de flujo HTTP, también aparece que el servicio de chat usa la URL: «atencionvirtual.com » (anexo 5).

Un *whois* en estos dos dominios no nos permite saber directamente a quien pertenecen estos dominios ya que la entidad eligió una opción para que esta información no sea pública (anexo 6), aunque sea probablemente a una entidad externa. Esto explicaría también que los servidores web correspondiente sean albergados en la empresa EPM Telecomunicaciones, lo que se puede ver después de buscar las direcciones IP correspondientes y haciendo un whois en estas direcciones (anexo 8).

por sus siglas en inglés). Los navegadores web muestran la identidad legal verificada de forma destacada en su interfaz de usuario, ya sea antes o en lugar del nombre de dominio».

Sin embargo, los servidores de dominios (Name Server) asociado al dominio “atencionvirtual.com” dejan aparecer las URL siguientes: BIRLOCHA.EPM.NET.CO y LAUTA.EPM.NET.CO. Estas pertenecen a la empresa EPM Telecomunicaciones.

Es una práctica usual que se tercericen servicios como el de chat. Sin embargo, la sensibilidad de la información y su vulnerabilidad obliga al Estado a tener especial cuidado con este tipo de contrataciones. Es una buena práctica en este tipo de contratos incluir, como mínimo, cláusulas y acuerdos de confidencialidad específicos sobre el manejo de la información, la forma como debe darse la transferencia de datos, la seguridad que requiere esta información y prohibiciones para la reutilización de datos. Considerando este punto, ofrecemos la siguiente recomendación.

Recomendación sobre tercerización de servicio de chat

Es importante que los contratos con la empresa de chat y la empresa que alberga el servicio (EPM Telecomunicaciones) incluyeran cláusulas y garantías en términos de seguridad y confidencialidad, y que fuera expreso en considerar posibles auditorías por parte del Estado. Además, teniendo en cuenta la sensibilidad de los datos manejados, se podría contemplar la migración del servicio de chat a sistemas internos.

2.5. ¿ Posible información inapropiada en las páginas webs del sitio de la DIAN?

[...]

3. Seguridad digital del sitio web de la DIAN

3.1. Del buen uso del protocolo HTTPS en (casi todos) los formularios internos

Nota inicial: El análisis de los formularios y de los espacios virtuales del sitio no pudo ser completado dado que el uso de datos ficticios en los formularios no permite ir a las etapas siguientes de cada formulario.

El sitio web de la DIAN cuenta con muchos formularios en línea. Encontramos los siguientes que cuentan todos con una URL de tipo HTTPS:

1. Inscripción en el RUT:
https://muisca.dian.gov.co/WebRutMuisca/DefInscripcionRutPortal.faces
2. Nuevos usuarios:
https://muisca.dian.gov.co/WebArquitectura/DefNuevosUsuarios.faces
3. inicio de sesión para usuarios registrados:
https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces
4. Recuperación Clave de Accesos:
https://muisca.dian.gov.co/WebArquitectura/DefPasswordRecuperacion.faces
5. Consulta Estado RUT:
https://muisca.dian.gov.co/WebRutMuisca/DefConsultaEstadoRUT.faces
6. Gestión Aduanera:
Importación: https://importacionescarga.dian.gov.co/WebArquitectura/DefLogin.faces
7. Consulta de Inconsistencia:
https://muisca.dian.gov.co/WebGestionmasiva/DefSelPublicacionesExterna.faces
8. Consulta de planillas radicadas:
https://certificadosdeorigen.dian.gov.co/autocalificacion/Admonform03/scripts_php/consulta.php
9. Actualice su actividad económica:
https://muisca.dian.gov.co/WebRutMuisca/DefActualizarActividadesCIIU.faces

Aquí, se encuentran por ejemplo copias de pantalla del formulario de los formularios 3 y del inicio del formulario 1 :

Iniciar sesión

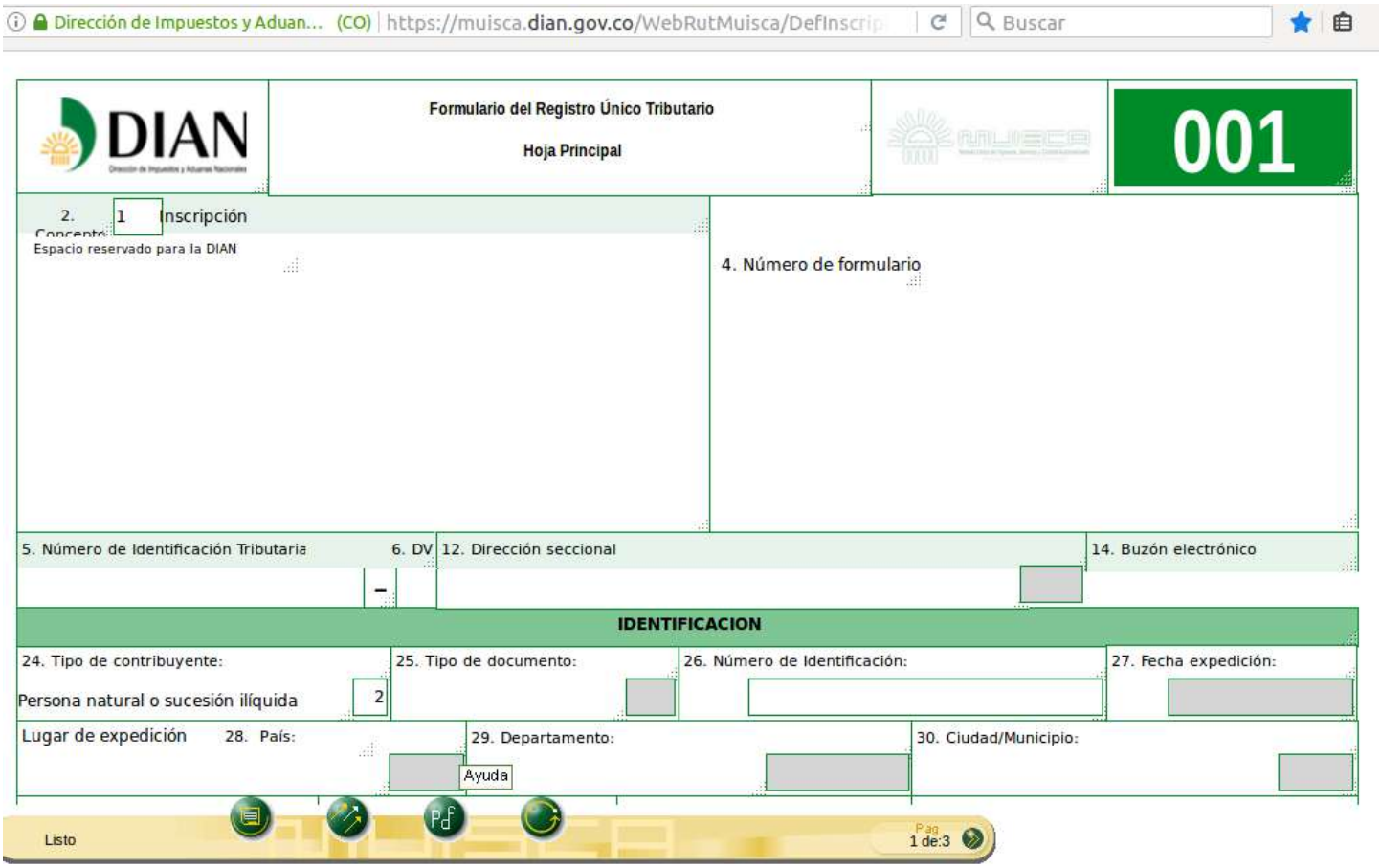
SERVICIOS EN LÍNEA MUISCA

Para ingresar suministre los siguientes datos

Ingresa a nombre de:	NIT
Número de documento de la organización:	
Tipo de documento del usuario:	Cédula de ciudadanía
Número de documento:	
Contraseña	

Activar teclado virtual No

Ingresar



Los análisis que hicimos de estos formulario, tanto al nivel del código fuente (Anexo 9) como analizando los flujos de datos generados por un envío (Anexo 10), mostraron que los datos se envían con el protocolo HTTPS y el método POST, lo que permite asegurar la confidencialidad de los datos transmitidos.

3.2. Implementación del HTTPS en las páginas mencionadas

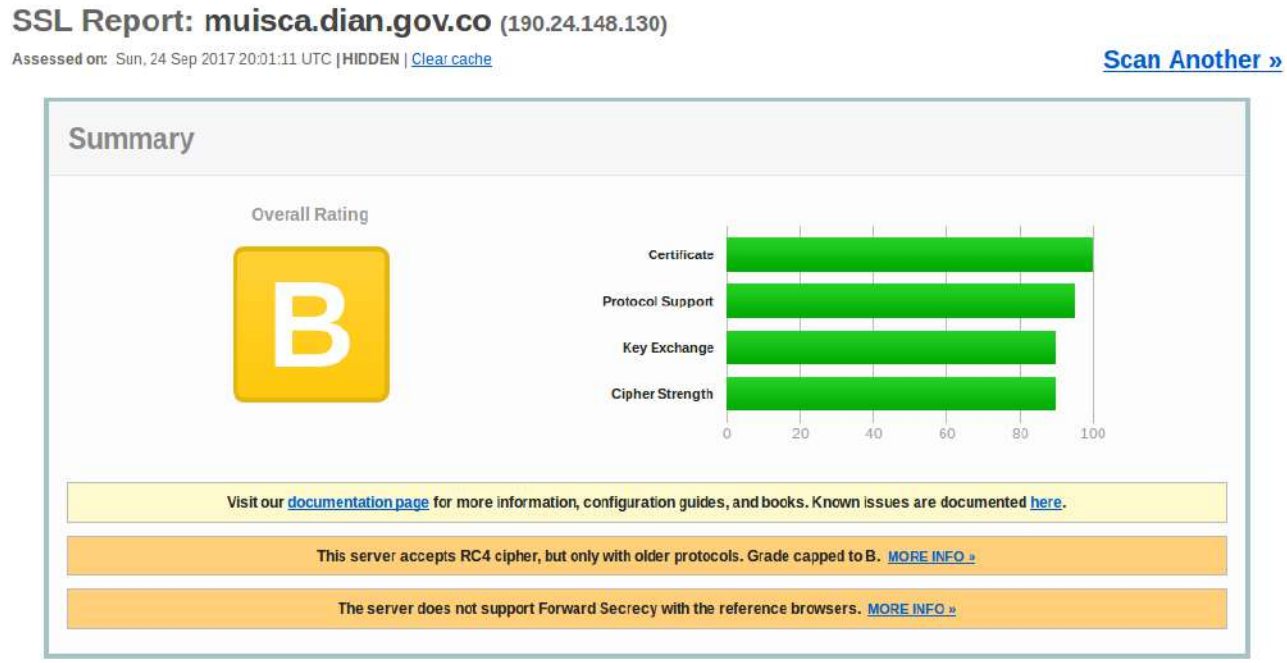
Como ya lo hemos dicho, implementar el HTTPS es necesario para la seguridad de las páginas webs y en particular las que manejan datos personales. Sin embargo, no es suficiente. Hace falta tener certificados de calidad y una buena implementación para evitar vulnerabilidades residuales.

En el examen "manual" del certificado y de la implementación no encontramos puntos negativos o "debilidades" sino al contrario puntos positivos como la "*Extended Validation*" que como ya mencionamos da garantías más fuertes sobre la identidad del propietario del dominio.

Entonces, completamos este primer análisis por un análisis automatizado en los dominios "muisca.dian.gov.co" que contienen la mayoría de los formularios y

"importacionescarga.dian.gov.co", mediante el servicio en línea https://www.ssllabs.com/, reconocido dentro de los expertos en seguridad digital.

El resultado fue lo mismo para ambos y fue bueno, ya que la nota global fue un "B" (van de A para una implementación perfecta hasta E para una implementación mala):



Sin embargo, resaltan dos puntos que se pueden mejorar:

- el servidor acepta el sistema de cifrado de flujo RC4 en ciertos casos
- el servidor no soporta *Forward Secrecy*.

Recomendación para la implementación del HTTPS

Globalmente el HTTPS (SSL/TLS) está bien implementado. Para perfeccionarlo, recomendamos resolver los dos problemas identificados en el test de ssllabs (RC4 y Forward Secrecy)[13].

3.3. Uso del HTTP y problemas de confidencialidad en los formularios de "escuelavirtual" y externos (CHAT y denuncias)

Como lo acabamos de mencionar, la gran mayoría de las páginas del sitio web de la DIAN con formulario usan el protocolo HTTPS. **Sin embargo, encontramos un sub-dominio interno y dos**

[13]Para buenas prácticas en la implementación, podemos recomendar la página github del mismo sitio: https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices

dominios externos vinculados con el sitio web en los cuales no es el caso y los datos se transmiten con el protocolo HTTP.

Se trata de :

1. el formulario de login del subdominio "escuelavirtual.dian.gov.co";
2. el formulario de CHAT;
3. el formulario de Denuncias: http://www.123contactform.com/form-522398/Itrc-Formulario

Para el último formulario, no hicimos un análisis profundo porque pertenece a otro sitio que depende a otro ente público: la Agencia del Inspector General de Tributos, rentas y contribuciones parafiscales (ITRC). Sin embargo, nos parece necesario señalar que los datos son enviados sin seguridad[14] hacía un servidor basado en Estados Unidos.

Para el primero, **el formulario de conexión del servicio de Escuela Virtual** del sitio de la DIAN, la página tiene una URL principal de tipo "http", lo que genera una alerta en nuestro navegador:

[14]En el codigo fuente de la página, la parte correspondiente al envío de datos muestra una transmisión con HTTP/POST:
<form role="form" aria-label="itrc formulario" class="form js-form" action="http://www.123contactform.com/form-522398/Itrc-Formulario" id="mainform123" method="post" name="mainform123" enctype="multipart/form-data" novalidate>

Un análisis del código fuente confirma que este formulario de conexión envía los datos (usuario y contraseña) con el protocolo HTTP (Anexo 11).

El formulario de CHAT está situado, como ya lo hemos mencionado, en una URL externa y el servicio es probablemente tercerizado.

Un análisis de los flujos HTTP generados por el envío de los datos permite ir más allá del examen del código fuente y muestra lo siguiente (Anexo 12):

- El envío de los datos del formulario se hace con el protocolo HTTP y el método POST;
- En la página precedente se había transmitido el número de cédula en la URL y con el protocolo HTTP (método GET);
- La respuesta del servidor web es muy interesante. Hace una redirección hacía una nueva URL que contiene los datos del formulario en parámetro. A partir de este momento los datos se transmiten con el método GET, lo que es muy problemático como se detalla más adelante.

Estos dos últimos puntos generan otros problemas que se detallan en la parte 5.2. y se repiten en la parte "CHAT" de la aplicación de la DIAN (ver parte 6).

Recomendación para el subdominio "escuelavirtual.dian.gov.co" y el servicio de CHAT

La transmisión de los datos se debe hacer con protocolo HTTP y con el método POST únicamente.

3.4. Seguridad de las *cookies* internas

Un análisis de las *cookies* instaladas en el sitio de la DIAN muestran la presencia de varias *cookies* de sesión con una finalidad probablemente técnica (Anexo 13). Esta puede estar vinculada con la seguridad, porque a veces sirven para mantener una conexión, una vez se ha ingresado con usuario y contraseña. En ciertos casos, robar una *cookie* puede permitir robar la sesión de la persona y conectarse en su espacio sin haber pasado por la etapa de autenticación. Por esto, es importante protegerlas de un robo en su transporte o en su almacenamiento[15].

Hay dos atributos que permiten esto:

- el atributo "Secure" que permite garantizar que una *cookie* solo se puede transmitir con el protocolo HTTPS[16] ;
- el atributo "HTTPOnly" que permite garantizar que la *cookie* solo pueda ser accedida por el protocolo HTTP y no de otra manera (por una función javascript por ejemplo).

En análisis efectuado, se puede observar que ninguna de estas *cookies* tienen el atributo "HTTPOnly" o "Secure".

[15]Por una función javascript o un ataque de tipo XSS por ejemplo.

[16]Definido así en la RFC 6265 : "If the cookie's secure-only-flag is true, then the request-uri's scheme must denote a "secure" protocol (as defined by the user agent)."

Recomendación para la seguridad de las cookies internas

Analizar cuales son las cookies internas sensibles y ponerles el flag “HttpOnly” y “Secure” (para este último, una vez generalizado el uso del protocolo HTTP en el sitio).

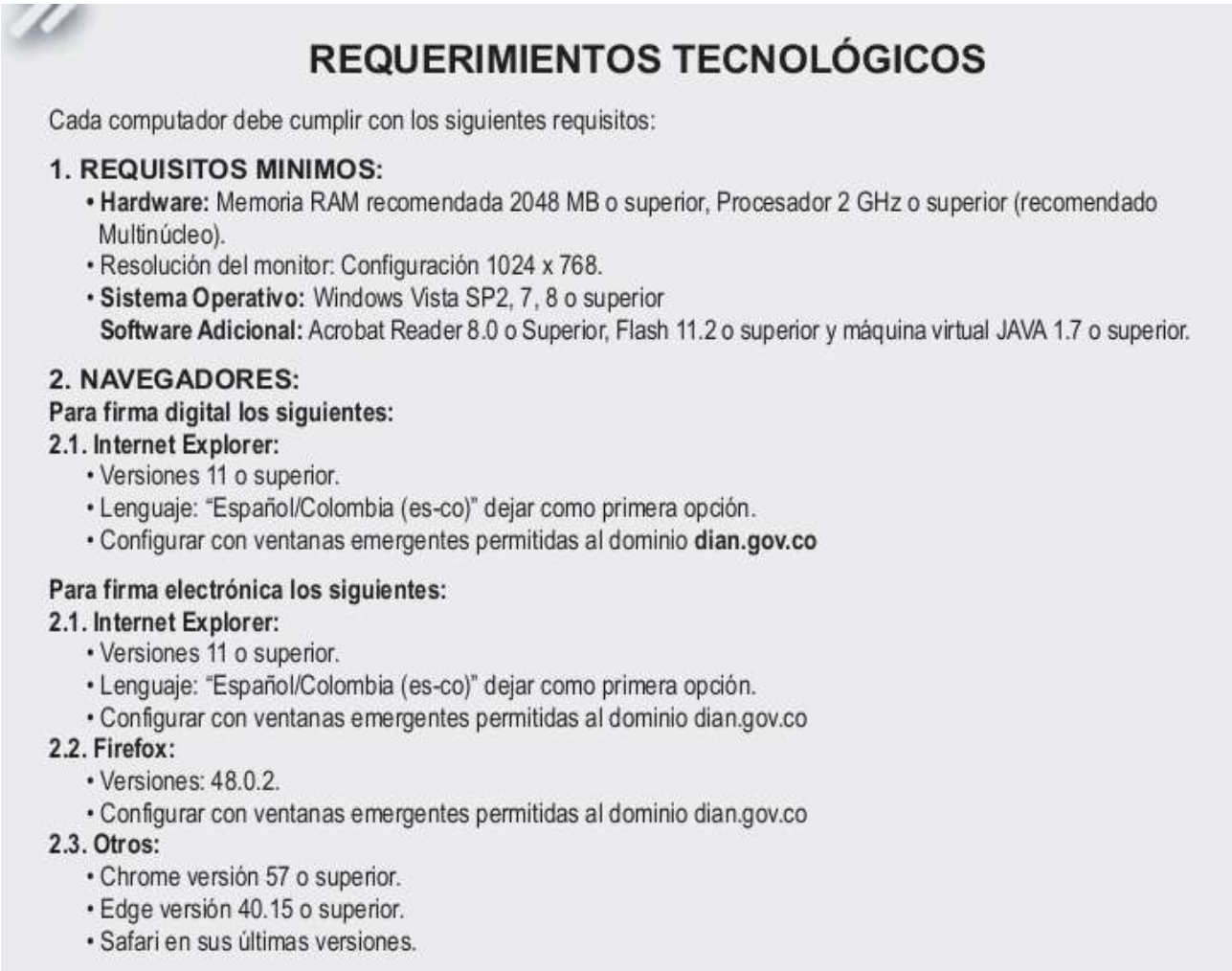
3.5. Actualizaciones de los servidores y vulnerabilidades

[...]

4. Incompatibilidad del sitio (firma digital) con otros sistemas operativos diferentes a Windows

Para dar más seguridad a ciertas operaciones, el sitio provee un mecanismo de firma digital basado en la tecnología de la máquina virtual Java y en una aplicación de la DIAN. **Desafortunadamente, este sistema de firma digital funciona solo con sistemas Windows**.

En un documento disponible en el sitio[17] y que describe los requerimientos tecnológicos, se indica que soló los sistemas operativos de la familia Windows son aceptados:



REQUERIMIENTOS TECNOLÓGICOS

Cada computador debe cumplir con los siguientes requisitos:

1. REQUISITOS MINIMOS:

- **Hardware:** Memoria RAM recomendada 2048 MB o superior, Procesador 2 GHz o superior (recomendado Multinúcleo).
- Resolución del monitor: Configuración 1024 x 768.
- **Sistema Operativo:** Windows Vista SP2, 7, 8 o superior

Software Adicional: Acrobat Reader 8.0 o Superior, Flash 11.2 o superior y máquina virtual JAVA 1.7 o superior.

2. NAVEGADORES:

Para firma digital los siguientes:

2.1. Internet Explorer:

- Versiones 11 o superior.
- Lenguaje: "Español/Colombia (es-co)" dejar como primera opción.
- Configurar con ventanas emergentes permitidas al dominio **dian.gov.co**

Para firma electrónica los siguientes:

2.1. Internet Explorer:

- Versiones 11 o superior.
- Lenguaje: "Español/Colombia (es-co)" dejar como primera opción.
- Configurar con ventanas emergentes permitidas al dominio dian.gov.co

2.2. Firefox:

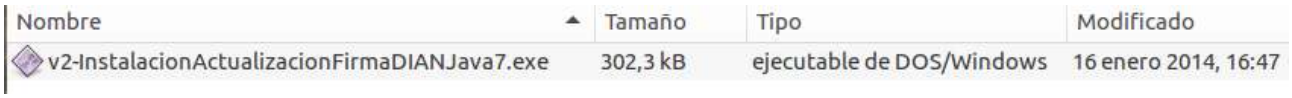
- Versiones: 48.0.2.
- Configurar con ventanas emergentes permitidas al dominio dian.gov.co

2.3. Otros:

- Chrome versión 57 o superior.
- Edge versión 40.15 o superior.
- Safari en sus últimas versiones.

[17] Hay varios versiones de este documento PDF en el sitio de la DIAN (...), pero la última versión parece ser esta: http://www.dian.gov.co/descargas/DianVirtual/Documentos/Requerimientos_tecnologicos_V5.pdf

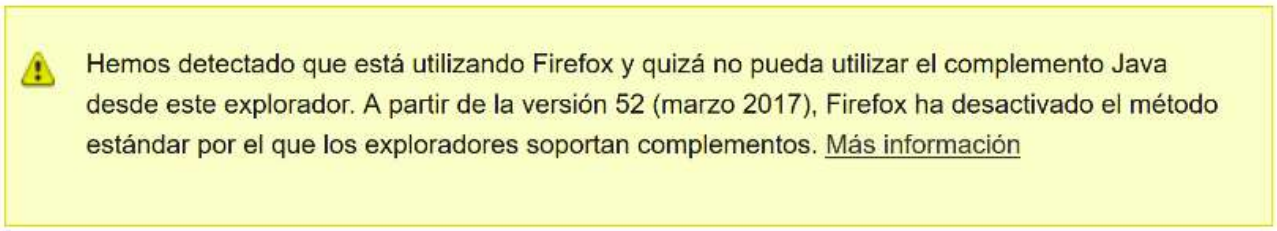
Esto tiene repercusiones también cuando uno quiere instalar el sistema de firma digital, se debe instalar Java y descargar un instalador. Desafortunadamente el instalador solo existe de la forma siguiente :



Nombre	Tamaño	Tipo	Modificado
v2-InstalacionActualizacionFirmaDIANJava7.exe	302,3 kB	ejecutable de DOS/Windows	16 enero 2014, 16:47

El cual es un archivo de instalación de tipo ejecutable (".exe") que solo funciona con Windows.

Además, así teniendo una sistema Windows, hay otros problemas de compatibilidad. Por ejemplo, la necesidad de usar Java crea problema de compatibilidad con el navegador Mozilla Firefox, que es muy común:



Por fin, aún teniendo un sistema Windows compatible y un navegador Internet Explorer o Chrome, hay problemas con la última versión de maquina virtual de Java. Por esto la DIAN hizo un "INSTRUCTIVO PARA RESOLVER INCONVENIENTES CON LA ULTIMA VERSIÓN DE MAQUINA VIRTUAL DE JAVA"[18] que explica parámetros que hay que modificar para lograr hacer funcionar el sistema de firma digital.

Además de constituir un prejuicio para las personas que tienen computadores con sistemas operativos distintos de Windows (Mac OS o Linux por ejemplo) o otros navegadores que Chrome o Internet Explorer, va en contra del principio de neutralidad tecnológica, definido en la Ley 1341 del 2009[19], *por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.*

Recomendación para la compatibilidad del sistema de firma digital / electrónica

Se recomienda que el sistema sea compatible con sistemas operativos distintos de Windows (como Mac OS o Linux) y con los principales navegadores.

[18]http://www.dian.gov.co/descargas/Novedades/2015/v5-instructivoJVM7-45.pdf

[19]Artículo 2: Neutralidad Tecnológica. El Estado garantizará la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, que permitan fomentar la eficiente prestación de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones y garantizar la libre y leal competencia, y que su adopción sea armónica con el desarrollo ambiental sostenible.

5. Análisis del *tracking* y de las *cookies*: Google estaba aquí.

5.1. *Tracking* por las *cookies*

El análisis de las cookies instaladas en nuestro navegador desde el sitio Internet de la DIAN muestra que se pueden clasificar en dos categorías:

- Cookies de sesión que parecen tener una finalidad "técnica";
- **Cookies generados por el servicio *Google Analytics*[20]**, que pueden tener una duración de vida de hasta dos años (la cookie "_utm").

El uso del servicio Google Analytics por el sitio, tanto en las partes informativas públicos, como en la zona de servicios en línea (subdominio *muisca.dian.gov.co*) se confirmó mediante el análisis del código fuente de las páginas correspondientes (Anexo 14).

Aunque esta herramienta es muy usada en la web, su uso en TODO el sitio tiene un impacto frente a la privacidad de los usuarios del sitio. Pues genera envíos de datos regulares a Google, que puede así perfilar el visitante. De hecho estos envíos de datos aparecen en la captura HTTP realizada mediante la extensión *Live HTTP Headers*[21] (Anexo 15).

También puede ser relevante mencionar que en otros países como Francia, se considera que las cookies de Google Analytics no cumplen los criterios de privacidad para el seguimiento de estadísticas webs[22] y necesitan por lo tanto un acuerdo del usuario (de la misma manera que las cookies de tracking publicitario[23]).

Un problema de su uso en sitios como el de la DIAN es que los datos recogidos por todos los servicios de Google (incluyendo los de Google Analytics, de hecho es la contraprestación que se da para no tener que pagar el servicio, es decir, al final realmente no es gratis) son combinados para su uso en el negocio publicitario. Esto queda claramente explicado en los términos y condiciones de los servicios de Google.[24] De hecho, por el tipo de efectos que tiene en servicios como los que ofrece el

[20] El servicio Google Analytics (https://www.google.com/intl/es/analytics/) es la herramienta de analítica web de Google. Permite tener estadísticas de las visitas del sitio Internet e incluso hacer la conexión con las publicidades de Google (por ejemplo conocer el porcentaje de visitantes que vienen en el sitio después de haber sido expuestos a una publicidad Google). Es el servicio de este tipo más usado en la web.

[21] https://addons.mozilla.org/en-US/firefox/addon/live-http-headers/

[22] Definidos en la recomendación "cookies" de la CNIL (***Délibération n° 2013-378 du 5 décembre 2013 portant adoption d'une recommandation relative aux cookies et aux autres traceurs visés par l'article 32-II de la loi du 6 janvier 1978***) en su artículo 6.

[23] "*Si vous utilisez Google Analytics ou Universal Analytics, il faut mettre à jour votre page web afin de bloquer les cookies tant que vous n'avez pas obtenu le consentement utilisateur.*" (traducción : Si esta usando Google Analytics o Universal Analytics, tiene que actualizar su página web con el fin de bloquear las cookies mientras no hayan recibido el acuerdo del usuario.) ; Fuente : https://www.cnil.fr/fr/solutions-pour-la-mesure-daudience

[24] Extracto de la política de privacidad de Google: «Utilizamos la información que recogemos **de todos nuestros servicios** para proporcionarlos, mantenerlos, protegerlos y mejorarlos, para desarrollar otros nuevos y para proteger a Google y a nuestros usuarios. **También utilizamos estos datos para ofrecerte**

sitio web de la DIAN, grupos de activistas y autoridades europeas de protección de datos lo han denunciado.[25]

Recomendación sobre rastreo (*tracking*) y privacidad

Teniendo en cuenta la sensibilidad y el carácter estatal del sitio de la DIAN, el uso de *Google Analytics* puede tener consecuencias negativas para la privacidad de las millones de personas que usan sus servicios en línea. Aunque las herramientas de análisis de estadísticas como la de *Google Analytics* son una necesidad para muchas organizaciones, es importante revisar las consecuencias derivadas de su uso y evaluar posibles alternativas. Nos permitimos recomendar el uso de una herramienta equivalente que se alberga internamente, como *Piwik*.[26] Soluciones de este tipo respetan la privacidad de las personas que visitan el sitio.

5.2. Cuando se envía a Google datos personales con los formularios

La consecuencia de la transmisión de datos en la URL (método GET) analizado en la parte 3.3 del informe (servicio de CHAT) es que los terceros llamados desde la página pueden recibir esta información. Es un poco técnico pero es una consecuencia del Referer del protocolo HTTP. El anexo 16 lo muestra de manera concreta: se transmite a Google el número de cédula entrada en el primer formulario.

Se trata aquí de una transmisión de datos personales completos a la empresa Google Inc. que no es un tercero autorizado para recibirlas. El análisis de la aplicación en la parte 6 muestra que el problema se extiende a los datos completos del segundo formulario.

Además, vale la pena reflexionar que con esta mala práctica se transfieren datos sensibles a una empresa ubicada en los Estados Unidos. Si bien la SIC reconoce a Estados Unidos como un país con protección adecuada, esta decisión ha sido criticada desde la sociedad civil y la academia.

contenido personalizado como, por ejemplo, resultados de búsqueda y anuncios más relevantes». Disponible en https://www.google.com/intl/es/policies/privacy/.

[25] Article 29 Data Protection Working Party. (2014, 23 de septiembre). *Carta a Google Inc. sobre su política de privacidad*. Disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140923_letter_on_google_privacy_policy.pdf.

[26] La herramienta Piwik está disponible en https://piwik.org/.

6. Bonus: análisis de ciertos aspectos de seguridad de la App de la DIAN

Este es el primer análisis de una aplicación para teléfonos inteligentes y tabletas que realizamos. No se trata de un análisis completo sino de un análisis de los flujos de datos generados por la parte "chat" de la aplicación de la DIAN.

6.1. Presentación de la aplicación

La aplicación de la DIAN es una aplicación desarrollada por la empresa colombiana Kubo SAS[27] para teléfonos inteligentes y tabletas:

[27]Sitio web de la empresa: http://kubo.co/

Esta aplicación provee tres servicios:

1. Presentación de los puntos de atención de la DIAN en un mapa, en función de la localización de la persona;
2. Llamadas a líneas de atención;
3. Servicio de chat para atención en línea.

La aplicación no permite conectarse al sistema de la DIAN o hacer diligencias en línea como si lo permite el sitio web. Sus funciones son más reducidas y sólo analizamos aquí los flujos de datos generado por el tercer servicio (el de chat) ya que es el servicio que involucra la transmisión de más datos personales (dos formularios, más los intercambios de mensajes). Además, el análisis del servicio de chat en el sitio web había resaltado varios problemas y queríamos verificar si ellos se extendían en la aplicación. La conclusión es que sí.

Presentación rápida de la metodología usada

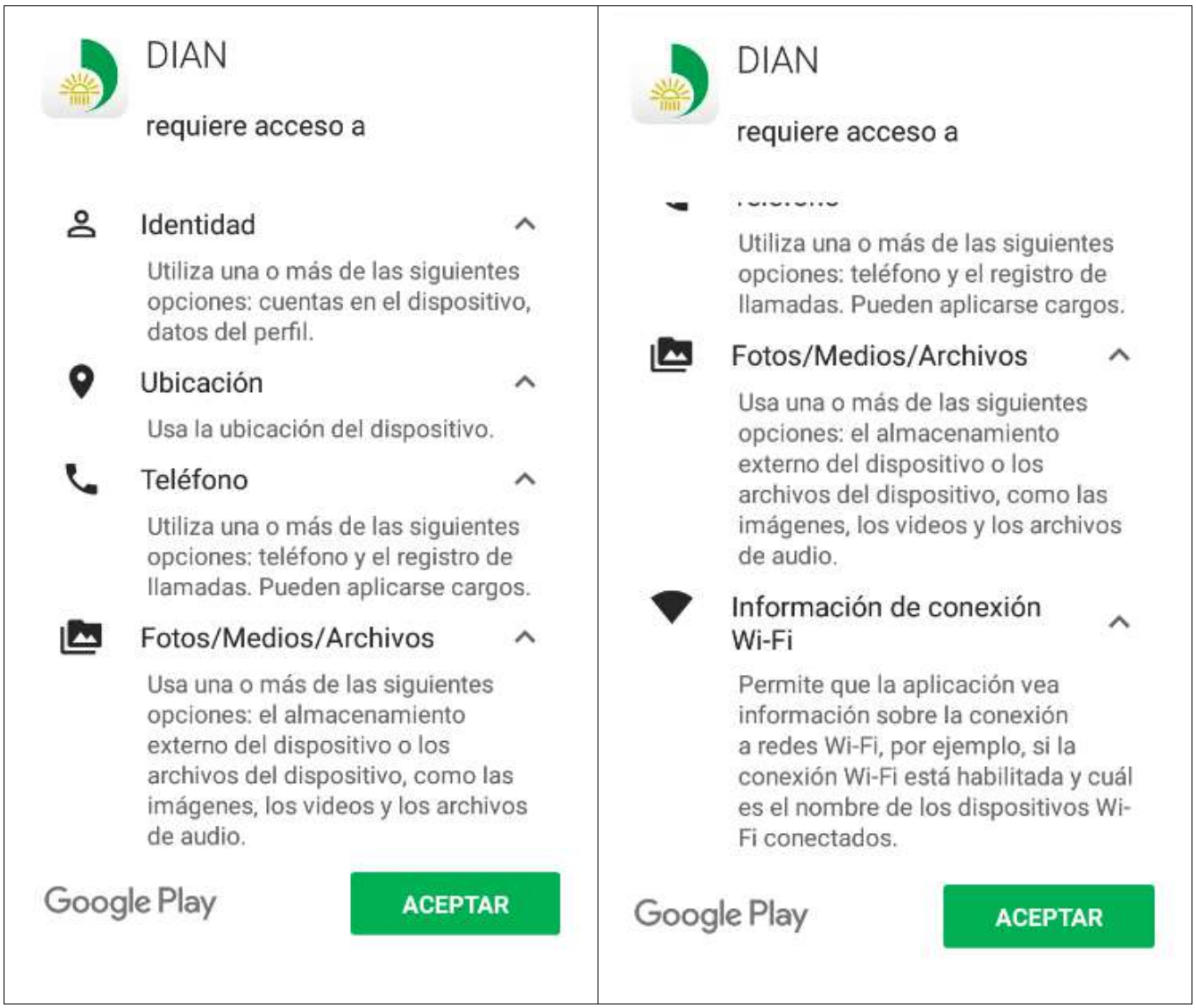
Un teléfono inteligente o una tableta, no es como en un computador. No se puede acceder fácilmente a las "capas bajas" del sistema operativo sin intervenir el dispositivo (hacer lo que se llama un "root" o un "jailbreak"). Esto es algo que no quisimos hacer. Para poder acceder al flujo de datos, analizarlo, poder verificar si se usan canales seguros o no, utilizamos como estrategia el análisis del flujo entrante y saliente del teléfono inteligente usando un dispositivo como intermediario. En concreto utilizamos la siguiente configuración:

- Un computador con dos tarjetas WiFi: una conectada a Internet y una configurada como punto de acceso.
- Un teléfono inteligente con sistema operativo Android conectado de forma previa al punto de acceso, en el cual instalamos la aplicación de la DIAN.
- El programa Wireshark, ejecutado en el computador para grabar y analizar los flujos de datos entre el teléfono inteligente y el punto de acceso.

Así pudimos analizar los datos que entran y que salen de nuestro teléfono mientras usamos la aplicación de la DIAN, en particular cuando llenamos y enviamos los datos en el formulario de CHAT. No usamos herramientas de tipo "proxy SSL". Por lo tanto la limitación de esta metodología es que no podemos observar el contenido de los flujos cifrados (HTTPS por ej.).

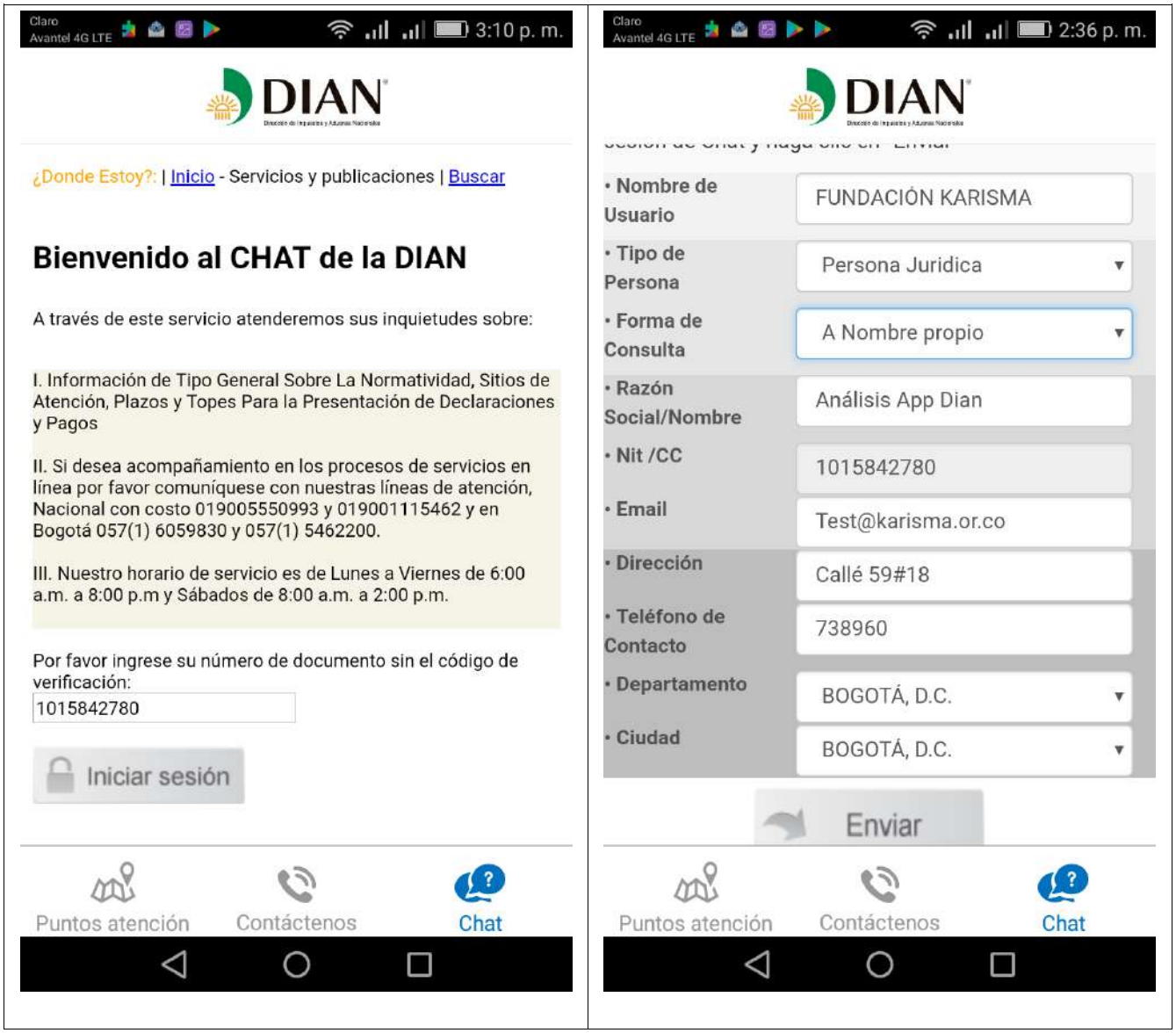
6.2. Las autorizaciones pedidas por la aplicación

Las copias de pantallas muestran las autorizaciones pedidas por la aplicación de la DIAN. De manera general, parecen coherentes con las finalidades de la aplicación.



6.3. Los formularios de datos del servicio de chat

Los formularios relacionados con el servicio de chat de la aplicación son bastante parecidos a los del sitio web, los llenamos de la siguiente manera, antes de analizar los flujos generados por su envío:



Aquí, a la izquierda, el primer formulario (número de cédula) y a la derecha el segundo formulario con datos personales completos (incluyendo nombre, razón social, número de cédula, correo electrónico, teléfono, dirección).

6.4. Seguridad del envío de los datos personales

Cuando hicimos el análisis de la captura de flujo hecha con el programa WireShark, constatamos que:

- El número de documento del primer formulario se transmite con el protocolo HTTP (que no es seguro como ya lo hemos explicado) y con el método POST. Además estos datos se vuelven a transmitir con el método GET (Anexo 17), lo que puede traer otros problemas como se detalla en la parte siguiente.
- Los datos completos que aparecen en el segundo formulario (incluyendo nombre, cédula, dirección, Email, teléfono) se envían con el protocolo HTTP y el método POST (Anexo 18). Además, igual que en el previo envío, hay una solicitud HTTP con el método GET que transmite todos los datos del formulario en parámetros de la URL. Esto es aún más problemático como lo explicamos más adelante.

Por lo tanto, el envío de datos por la aplicación no se hace de manera segura, usando un canal cifrado sino con el protocolo HTTP que no permite garantizar la confidencialidad de los datos transmitidos, como ya lo hemos explicado. Además, un error adicional que tiene consecuencias problemáticas es el uso del método GET para transmitir datos personales así aparecen en las URL.

6.5. Dominios con los cuales de comunica la aplicación

Como lo demuestran los Anexos , la aplicación se comunica principalmente con los servidores webs siguientes (igual que el la parte chat del sitio web) :

- www.asistenciachat.com, con dirección IP 201.232.123.67, ubicado en Colombia ;
- www.atencionvirtual.com, con dirección IP 200.13.225.137, ubicado en Colombia (Ver Anexo 7).

Además de estos, hemos encontrado que la aplicación generó solicitudes hacia los servidores webs siguientes:

- www.dian.kubo.co, con dirección IP 192.185.21.145, ubicado en Texas, Estados Unidos (Anexo 19);
- www.ajax.googleapis.com, con dirección IP 216.58.222.234, de la empresa Google Inc., basada en Estados Unidos (Anexo 20).

Nuestro análisis permito demostrar que la aplicación genera comunicaciones hacía estos cuatro dominios. Esto es importante. En particular, la siguiente parte muestra como la combinación de lo que explicamos en la sección 6.4. y la forma de comunicación entre la aplicación y el dominio "ajax.googleapis.com" genera una fuga de datos hacia Google.

En cuanto al subdominio "dian.kubo.co", toca resaltar que este es un subdominio del desarollador de la aplicación, la empresa Kubo, ya mencionada.

Además, pueden haber otros dominios y terceros asociados que la limitación de nuestra metodología (ver más arriba) no nos permite alcanzar. Por ejemplo, la captura de Wireshark muestra que en el momento de uso de la aplicación hay resoluciones de dominio con el protocolo DNS hacia "ssl.googleanalytics.com", el servicio *analytics* de Google. Pero como las comunicaciones con este

servicio están cifradas, no logramos ver su contenido y detectar si fueron iniciadas por la aplicación de la DIAN o por otro servicio del teléfono.

6.6. Cuando la aplicación transmite los datos completos del formulario a Google

En la parte 6.4. hemos explicado que los datos del segundo formulario se transmiten en las propias URL (uso del método GET). En la parte 6.5. analizamos cómo la aplicación se comunica con servidores webs de al menos cuatro dominios distintos, de los cuales uno es de la empresa Google (dominio "ajax.googleapis.com").

La consecuencia de estos dos hechos es que esta URL, con todos los datos personales que contiene, se transmite a los servidores de Google[28]. Aunque es un tema técnico, es una consecuencia de la presencia del «Referer» en el protocolo HTTP. Lo mostramos de manera concreta y detallada en el Anexo 21.

Se trata aquí de una transmisión de datos personales completos (incluyendo nombre, razón social, número de cédula, correo electrónico, teléfono, dirección) a la empresa Google Inc. que no es un tercero autorizado para recibirlas.

Además, vale la pena reflexionar que con esta mala práctica se transfieren datos sensibles a una empresa ubicada en los Estados Unidos.

6.7. Cuando la aplicación transmite los datos de localización hacia un subdominio externo

La aplicación de la DIAN se comunica con un subdominio del desarrollador de la aplicación: "dian.kubo.co". Un análisis de los intercambios entre la aplicación y este dominio muestran que corresponden al servicio de localización de puntos cercanos: la aplicación envía la localización del usuario y el servidor le responde los puntos de atención de la DIAN más cercanos (ver Anexo 22).

Hecha de esta manera, esta transmisión es problemática por varias razones (ver Anexo 22):

- Se hace con un subdominio del servidor web del desarollador, que la DIAN no controla y que está situado en Estados Unidos.
- Transmite la localización del usuario con el protocolo HTTP que no es seguro.
- Usa el método GET (transmisión en la URL) que como ya lo hemos visto presenta riesgos de fuga de los datos a otros terceros.

[28]Hacía el servicio de "hosted librarys" de Google (https://developers.google.com/speed/libraries/) en el dominio "ajax.googleapis.com".

Recomendaciones para la seguridad de la aplicación

1. Utilizar unicamente el protocolo HTTPS y el método POST para transmitir los datos personales.
2. Asegurarse que terceros no autorizados no sean destinatarios de datos personales manejados por la aplicación.
3. Albergar el servicio de localización de puntos de atención cercanos en el servidor web de la DIAN y no en “kubo.co”.

7. Tabla sintética de recomendaciones

Categoría	Constatación	Recomendación	Lo que se hizo
Seguridad de los formularios de CHAT y de conexión a la Escuela Virtual	Las páginas de la conexión a la Escuela Virtual y del servicio (externo) de CHAT usan el protocolo HTTP. Además para el servicio de CHAT los datos se transmiten en la URL por el método GET.	Para todos los formularios, implementar el protocolo HTTPS. Además los datos correspondientes deben siempre ser transmitidos con el método POST.	No se hizo Los formularios de la Escuela virtual y del CHAT siguen usando HTTP.
Seguridad de los servidores webs	[...]	[...]	No se hizo
Neutralidad tecnológica y compatibilidad	El sistema de firma digital no es compatible con sistemas operativos distintos de Windows y con las últimas versiones del navegador Mozilla Firefox.	Se recomienda que el sistema sea compatible con sistemas operativos distintos de Windows (como Mac OS o Linux) y con los principales navegadores.	Ya no se ven referencias en la página de inicio del sitio al sistema de firma electrónica
Seguridad de la App para smartphones y tabletas	La App de la DIAN transmite los datos completos de los formularios por el protocolo HTTP y a veces con el método GET. Además de la falta de confidencialidad, la consecuencia es que estos datos personales son enviados a Google (por el Referer). Finalmente, la localización del usuario es enviada con el protocolo HTTP y el método GET hacia un subdominio del desarollador (dian.kubo.co).	Utilizar únicamente el protocolo HTTPS y el método POST para transmitir los datos personales. Asegurarse que terceros no autorizados no sean destinatarios de datos personales manejados por la aplicación. Albergar el servicio de localización de puntos de atención cercanos en el servidor web de la DIAN y no en “kubo.co”.	En el análisis de seguimiento que se hizo en mayo 2018, se pudo verificar que se había cumplido con estas recomendaciones con excepción del uso del HTTPS. Sin embargo, en el momento de la publicación de este informe , noviembre 2018, la App no se puede descargar en la tienda de Google pero si en la de Apple (en su versión original). Sin embargo, los servicios que ofrece la App están desactivados.
Seguridad (tercerización de servicios hosting y chat)	Los servidores servicios de CHAT y de *hosting* del mismo CHAT parecen tercerizados con empresas externas.	Es importante que los contratos con la empresa de chat y la empresa que alberga el servicio (EPM Telecomunicaciones) incluyan cláusulas y garantías en términos de seguridad y confidencialidad, y que fuera expreso en considerar	No tenemos información respecto a los contratos. El servicio de CHAT no se ha migrado internamente.

		posibles auditorías por parte del Estado. Además, teniendo en cuenta la sensibilidad de los datos manejados, se podría contemplar la migración del servicio de chat a sistemas internos.	
Seguridad (Autenticación del sitio y HTTPS)	Las páginas que no tienen formularios (la de inicio por ejemplo) usan el protocolo HTTP, que no garantiza la autenticación del sitio.	Se recomienda implementar el protocolo HTTPS no sólo en las páginas que contengan formularios con datos personales sino también en las otras páginas del sitio y en particular en la página de inicio, con fin de permitir una validación de la identidad del sitio, su autenticación.	El protocolo HTTPS se implementó en la página de inicio y en la mayoría de las páginas. Sin embargo, quedan páginas (incluso con formularios) usando el protocolo HTTP.
Privacidad (difusión de documentos inapropiados en el sitio de la DIAN)	[...]	[...]	Los documentos siguen en línea y no sabemos si la DIAN evaluó la pertinencia de su presencia en su sitio.
Seguridad (Implementación del protocolo HTTPS)	El HTTPS esta globalmente bien implementado en las páginas que lo usan. Sin embargo, un test con ssllabs mostró mejoras posibles.	Mejorar la implementación del HTTPS (SSL/TLS), en particular en los dos aspectos identificados (RC4 y Forward Secrecy).	No se mejoró la implementación e incluso se añadió una vulnerabilidad ; por lo cual la nota de ssllabs pasó de B a F.
Información legal y transparencia	El sitio web contiene una política de privacidad y también una política Facebook. La primera es incompleta y la segunda debería extenderse a las otras redes sociales en las que la DIAN maneja una cuenta.	Es necesario hacer referencia a la Ley de protección de datos colombianas e incluir sus obligaciones informativas, en particular los derechos de los usuarios (acceso y rectificación, Ley 1581 del 2012, artículos 8 y 12). Para darle más visibilidad se aconseja incluir un vínculo visible al final de cada formulario que recoja datos personales. Además, se aconseja extender la política Facebook hacía una política de redes sociales de la DIAN que se aplicara a las distintas redes sociales en las que la DIAN administra un perfil.	La política de privacidad de la DIAN no ha cambiado.
Privacidad y tracking (uso de un analytics en las	Quienes visitan las páginas del sitio web es víctima de rastreo (*tracking*) por parte de Google (*Analytics*).	Analizar el impacto del uso de Google analytics en las distintas partes del sitio. Se podría reemplazarlo por una	Todavía se usa la herramienta Google analytics en el sitio. No sabemos de una

páginas públicas del sitio)		herramienta de *analytics* que no sea intrusiva y que pueda ser instalada localmente, como Piwik.	eventual análisis de impacto al respecto.

8. ANEXOS – Referencias técnicas

[1] Emails enviados a la DIAN para informarla de nuestros análisis

-------- Mensaje reenviado --------
Asunto: *Análisis preliminar del sitio www.dian.gov.co*
Fecha: ***Sun, 3 Sep 2017 18:49:40 -0500***
De: *Stéphane LABARTHE - Karisma <stephane@karisma.org.co>*
Organización: *Fundación Karisma*
A: *asistencia@dian.gov.co*
CC: *Carolina Botero <carobotero@karisma.org.co>, Maria del Pilar Saenz <mpsaenz@karisma.org.co>, Juan Diego Castañeda <juancastaneda@karisma.org.co>*

Buenas tardes,

La Fundación Karisma es una organización de la sociedad civil, fundada en 2003 y localizada en Bogotá, que busca responder a las oportunidades y amenazas que surgen en el contexto de la "tecnología para el desarrollo" para el ejercicio de los derechos humanos. Karisma trabaja desde el activismo con múltiples miradas —legales y tecnológicas— en coaliciones con socios locales, regionales e internacionales.

Desde hace un año estamos adelantando un análisis piloto evaluando aspectos de seguridad y privacidad de algunas páginas web asociadas con trámites y servicios del Gobierno colombiano. En este momento estamos haciendo un análisis preliminar del sitio www.dian.gov.co.

Parte de nuestra evaluación incluye el análisis de los formularios que recopilan información personal, y por esto, queremos comunicarles que encontrarán registros a nombre de Karisma, asociados al correo test@karisma.org.co. Estos datos no son reales y no deben ser tomados en cuenta para ningún trámite.

Si tienen alguna duda o inquietud sobre el tema pueden comunicarse con nosotros respondiendo este correo. Estaremos atentos a contestar cualquier pregunta.

Atentamente,

Fundación Karisma.

-------- **Mensaje reenviado** --------
Asunto: Análisis preliminar del sitio www.dian.gov.co
Fecha: **Mon, 18 Sep 2017 16:52:19 -0500**
De: Stéphane LABARTHE - Karisma <stephane@karisma.org.co>
Organización: Fundación Karisma
A: asistencia@dian.gov.co
Carolina Botero <carobotero@karisma.org.co>, Maria del Pilar Saenz
CC: <mpsaenz@karisma.org.co>, Juan Diego Castañeda
<juancastaneda@karisma.org.co>

Buenas tardes,

Un complemento para informarles que nos dimos cuenta que la DIAN también tiene una aplicación para tabletas y smartphones.

La incluimos en nuestros análisis.

Cordialmente,

Fundación Karisma.

[este segundo email incluía también el primero, como transferido]

[2] Certificado criptográfico asociado al dominio "muisca.dian.gov.co" (y a otros subdominios)

muisca.dian.gov.co
Identidad: muisca.dian.gov.co
Verificado por: GeoTrust EV SSL CA - G4
Caduca: 13/05/18

Nombre del asunto
1.3.6.1.4.1.311.60.2.1.3: #1302434F
2.5.4.15: #1311476F7665726E6D656E7420456E74697479
serialNumber (Número de serie): Government Entity
C (País): CO
ST (Estado / provincia): Cundinamarca
L (Localidad): Bogota
O (Organización): Dirección de Impuestos y Aduanas Nacionales
OU (Unidad organizativa): BOGOTA DC
CN (Nombre común): muisca.dian.gov.co
Nombre del emisor
C (País): US

O (Organización): GeoTrust Inc.
CN (Nombre común): GeoTrust EV SSL CA - G4
Certificado emitido
Versión: 3
Número de serie: 58 01 66 08 C7 89 21 D6 E5 0D C1 A4 80 59 6C 76
No es válido antes de: 2016-05-13
No es válido después de: 2018-05-13
Huellas de certificados
SHA1: AF 85 FF 45 3F D4 8C 99 8A 1B CB 1B 78 90 2B 02 AB 98 97 58
MD5: 4D 25 3D 4C A3 F6 2C A7 DF 04 AE 16 5B C7 5A 3A
Información de la clave pública
Clave del algoritmo: RSA
Parámetros de la clave: 05 00
Tamaño de la clave: 2048
Huella de la clave SHA1: 53 DB 62 40 D8 6A 3F 92 25 BB 32 9F 3C 60 49 40 00 BA 70 B6
Clave pública: 30 82 01 0A 02 82 01 01 00 A3 52 A8 D3 C2 E4 8B 3E 00 5C A7 B7 3B 94 B4 C4 F4 41 BC 0A 5C FB 89 59 20 EA 8D 96 7E 93 E0 8D 5A AD 71 19 98 37 B3 B8 59 E1 71 6A 5B 84 BA E1 D5 90 C0 BF 12 32 07 05 C6 40 6F 54 EF 19 DD 24 85 80 68 0E 67 E4 4A 23 E6 00 2C 94 80 75 42 9E 43 46 E5 BF 51 EA 13 49 A4 05 99 01 DA 31 67 B1 F6 C2 D2 8D 9C 97 4C 6A 37 26 5A 5F D8 8B 54 DB 5D 9A FF 13 0A E8 28 3A D7 BF E6 B7 DE C8 32 87 78 D5 24 69 BD BF 55 B0 8B F1 BB D8 DE 73 15 CD 1A 74 35 E8 F3 22 2A 51 C4 2D 3B BC 2A CF E2 A5 4F 18 88 CE 28 60 4F E6 8C B4 5F 8B 79 2D F8 C7 34 D3 6B E0 3C E5 70 FD 18 FE FE C7 AE CA C9 FC 20 58 72 74 4F CE C4 AD A3 32 57 A2 5B 4B 2F 2E EA D5 C1 1D 9C 97 42 11 23 78 90 3F 23 65 DC 23 54 F9 EB A0 E0 CE 43 83 5F 7C 5D 63 41 B2 C1 C0 4A 6D BD 48 CF E8 BB 3A 7B 95 83 13 A3 7C 4F 9F 02 03 01 00 01
Nombres alternativos del asunto
DNS: mail.dian.gov.co
DNS: importacionescarga.dian.gov.co
DNS: importaciones.dian.gov.co
DNS: legacy.dian.gov.co
DNS: agendamientodigiturno.dian.gov.co
DNS: devolucion.dian.gov.co
DNS: ada.dian.gov.co
DNS: ar.dian.gov.co
DNS: salidademercancias.dian.gov.co
DNS: dian.gov.co
DNS: registrosyautorizaciones.dian.gov.co
DNS: autodiscover.dian.gov.co
DNS: certificadosdeorigen.dian.gov.co
DNS: transitoaduanero.dian.gov.co
DNS: muisca.dian.gov.co
Crítico: No
Restricciones básicas
Autoridad de certificación: No
Longitud máxima de la ruta: Sin límite
Crítico: No
Uso de la clave
Usos: Firma digital□Cifrado de la clave
Crítico: Sí
Extensión
Identificador: 2.5.29.31
Valor: 30 22 30 20 A0 1E A0 1C 86 1A 68 74 74 70 3A 2F 2F 67 6D 2E 73 79 6D 63 62 2E 63 6F 6D 2F 67 6D 2E 63 72 6C
Crítico: No

Extensión
Identificador: 2.5.29.32
Valor: 30 81 9E 30 81 92 06 09 2B 06 01 04 01 F0 22 01 06 30 81 84 30 3F 06 08 2B 06 01 05 05 07 02 01 16 33 68 74 74 70 73 3A 2F 2F 77 77 77 2E 67 65 6F 74 72 75 73 74 2E 63 6F 6D 2F 72 65 73 6F 75 72 63 65 73 2F 72 65 70 6F 73 69 74 6F 72 79 2F 6C 65 67 61 6C 30 41 06 08 2B 06 01 05 05 07 02 02 30 35 0C 33 68 74 74 70 73 3A 2F 2F 77 77 77 2E 67 65 6F 74 72 75 73 74 2E 63 6F 6D 2F 72 65 73 6F 75 72 63 65 73 2F 72 65 70 6F 73 69 74 6F 72 79 2F 6C 65 67 61 6C 30 07 06 05 67 81 0C 01 01
Crítico: No
Uso extendido de la clave
Propósitos permitidos: Autenticación del servidor Autenticación del cliente
Crítico: No
Extensión
Identificador: 2.5.29.35
Valor: 30 16 80 14 DE CF 5C 50 B7 AE 02 1F 15 17 AA 16 E8 0D B5 28 9D 6A 5A F3
Crítico: No
Extensión
Identificador: 1.3.6.1.5.5.7.1.1
Valor: 30 49 30 1F 06 08 2B 06 01 05 05 07 30 01 86 13 68 74 74 70 3A 2F 2F 67 6D 2E 73 79 6D 63 64 2E 63 6F 6D 30 26 06 08 2B 06 01 05 05 07 30 02 86 1A 68 74 74 70 3A 2F 2F 67 6D 2E 73 79 6D 63 62 2E 63 6F 6D 2F 67 6D 2E 63 72 74
Crítico: No
Extensión
Identificador: 1.3.6.1.4.1.11129.2.4.2
Valor: 04 82 01 6D 01 6B 00 77 00 DD EB 1D 2B 7A 0D 4F A6 20 8B 81 AD 81 68 70 7E 2E 8E 9D 01 D5 5C 88 8D 3D 11 C4 CD B6 EC BE CC 00 00 01 54 AA FD 38 40 00 00 04 03 00 48 30 46 02 21 00 DA F6 0F 09 0F 71 3B 1C 01 E6 F8 67 F9 34 D0 AE E0 EF D6 76 F4 32 81 61 0E 78 56 D0 17 2B 12 CB 02 21 00 B7 96 C6 37 99 10 EA 67 20 44 38 1F 05 47 99 55 55 A5 D6 16 57 23 2B 10 C2 B1 A0 7F F0 68 07 DC 00 77 00 A4 B9 09 90 B4 18 58 14 87 BB 13 A2 CC 67 70 0A 3C 35 98 04 F9 1B DF B8 E3 77 CD 0E C8 0D DC 10 00 00 01 54 AA FD 38 77 00 00 04 03 00 48 30 46 02 21 00 85 61 4E 93 B5 77 E8 A6 94 11 BD 51 D8 A8 10 15 7D E9 34 01 36 AF 3B 18 11 12 3A 7F 69 6C E8 AC 02 21 00 D8 F3 36 53 C6 9E BE 2F EC 8E 39 1B 72 F6 59 EB 26 9B 30 65 41 F2 32 09 03 31 51 DE 7B 1A 0A BD 00 77 00 68 F6 98 F8 1F 64 82 BE 3A 8C EE B9 28 1D 4C FC 71 51 5D 67 93 D4 44 D1 0A 67 AC BB 4F 4F FB C4 00 00 01 54 AA FD 38 5D 00 00 04 03 00 48 30 46 02 21 00 AB 10 94 A8 1B CA 1D 36 81 12 CB 83 E6 BB DF 94 5B 2A 97 37 15 DE 32 CF 89 81 AD EA 9F 57 95 E5 02 21 00 D8 F2 9E 76 C4 FB 3B 06 1E D2 B7 62 5A 8C B8 24 24 FA 68 58 05 24 50 D5 46 2E 75 7F 96 FF 67 6C
Crítico: No
Firma
Algoritmo de firma: 1.2.840.113549.1.1.11
Parámetros de la firma: 05 00
Firma: 59 78 23 24 DF 3A F8 DF FA 21 72 46 DA 73 9D 75 8D EF 67 4E D4 A4 8D 71 2B 75 50 E4 B4 A3 27 6F AC 70 DC 50 E1 4C 17 DB FE B4 89 BE 63 54 7E DD CD 2B 01 88 D0 FD 22 F8 75 B6 97 72 83 95 D0 45 F0 4E 28 25 19 21 34 68 BB 40 A4 3D A9 0B 9E 97 67 33 37 E8 D3 8D BA 38 55 56 C6 FA 61 BD FA 1B 01 40 BC B5 D3 7D 11 81 01 AC C6 6D 35 FF 34 70 2B 34 65 3E 6A 26 5C A6 CA 24 E5 79 C7 64 63 47 5B DE 84 75 13 8A 71 37 05 6C 2A AF D9 E4 76 52 CB D0 87 F4 FA 83 BF BA 2F 73 58 B0 2A 25 F3 A3 5C 5C C8 89 98 D4 A6 C3 5E 80 2A B7 0D 4D C2 63 41 CB FB FD 89 E0 D0 27 67 F5 A7 59 99 C5 30 62 92 07 94 96 CA FF F3 E5 E3 D0 43 01 B4 78 20 53 F2 FC 8F 52 96 EF 87 CF 24 A0 C3 67 B6 5B 4C B3 77 7D 85 99 73 AA F7 82 A8 30 9B 31 5C A3 03 E0 E9 61 D4 3D 46 68 EE 51 31 EA 45 E3 49 31 B3 17

[3] Resultado de un *who is* en el dominio "dian.gov.co"

El siguiente resultado ha sido obtenido mediante el comando "whois dian.gov.co" ejecutado en un terminal LINUX :

Domain Name: DIAN.GOV.CO
Domain ID: D605803-CO
Sponsoring Registrar: .CO INTERNET S.A.S.
Sponsoring Registrar IANA ID: 111111
Registrar URL (registration services): www.cointernet.com.co
Domain Status: clientTransferProhibited
Registrant ID: 3666-REG
Registrant Name: ***Direccion de Impuestos y Aduanas Nacionales DIAN***
Registrant Organization: ***Direccion de Impuestos y Aduanas Nacionales DIAN***
Registrant Address1: ***CRA 8 # 6 C 38 Piso 5***
Registrant City: ***BOGOTA***
Registrant State/Province: Bogota
Registrant Postal Code: 111711
Registrant Country: Colombia
Registrant Country Code: CO
Registrant Phone Number: +1.6079867
Registrant Email: hmesal@dian.gov.co
Administrative Contact ID: 3666-REG
Administrative Contact Name: Direccion de Impuestos y Aduanas Nacionales DIAN
Administrative Contact Organization: Direccion de Impuestos y Aduanas Nacionales DIAN
Administrative Contact Address1: CRA 8 # 6 C 38 Piso 5
Administrative Contact City: BOGOTA
Administrative Contact State/Province: Bogota
Administrative Contact Postal Code: 111711
Administrative Contact Country: Colombia
Administrative Contact Country Code: CO
Administrative Contact Phone Number: +1.6079867
Administrative Contact Email: hmesal@dian.gov.co
Billing Contact ID: 3666-REG
Billing Contact Name: Direccion de Impuestos y Aduanas Nacionales DIAN
Billing Contact Organization: Direccion de Impuestos y Aduanas Nacionales DIAN
Billing Contact Address1: CRA 8 # 6 C 38 Piso 5
Billing Contact City: BOGOTA
Billing Contact State/Province: Bogota
Billing Contact Postal Code: 111711
Billing Contact Country: Colombia
Billing Contact Country Code: CO
Billing Contact Phone Number: +1.6079867
Billing Contact Email: hmesal@dian.gov.co
Technical Contact ID: 3666-REG
Technical Contact Name: Direccion de Impuestos y Aduanas Nacionales DIAN
Technical Contact Organization: Direccion de Impuestos y Aduanas Nacionales DIAN
Technical Contact Address1: CRA 8 # 6 C 38 Piso 5
Technical Contact City: BOGOTA
Technical Contact State/Province: Bogota
Technical Contact Postal Code: 111711
Technical Contact Country: Colombia

Technical Contact Country Code: CO
Technical Contact Phone Number: +1.6079867
Technical Contact Email: hmesal@dian.gov.co
Name Server: NS1-AUTH.ETB.NET.CO
Name Server: NS2-AUTH.ETB.NET.CO
Name Server: FW.DIAN.GOV.CO
Created by Registrar: NEULEVELCSR
Last Updated by Registrar: .CO INTERNET S.A.S.
Domain Registration Date: Thu Jun 18 00:00:00 GMT 1998
Domain Expiration Date: Fri Dec 31 23:59:59 GMT 2021
Domain Last Updated Date: Sun Jan 01 16:37:09 GMT 2017
DNSSEC: false

[4] Determinación de las direcciones IP de los servidores webs y *who is* en estas

(obtenido mediante los comandos nslookup y *whois* en un terminal LINUX)

Usando el comando nslookup en un terminal Linux se puede primero preguntar los servidores de dominio y obtener las direcciones IP de los servidores :

nslookup www.dian.gov.co
Server: 127.0.1.1
Address: 127.0.1.1#53

Non-authoritative answer:
Name: www.dian.gov.co
Address: ***190.24.148.167***

nslookup muisca.dian.gov.co
Server: 127.0.1.1
Address: 127.0.1.1#53

Non-authoritative answer:
Name: muisca.dian.gov.co
Address: ***190.24.148.130***

nslookup importacionescarga.dian.gov.co
Server: 127.0.1.1
Address: 127.0.1.1#53

Non-authoritative answer:
Name: importacionescarga.dian.gov.co
Address: ***190.24.148.145***

nslookup certificadosdeorigen.dian.gov.co
Server: 127.0.1.1
Address: 127.0.1.1#53

Non-authoritative answer:
Name: certificadosdeorigen.dian.gov.co
Address: ***190.24.148.147***

nslookup escuelavirtual.dian.gov.co
Server: 127.0.1.1
Address: 127.0.1.1#53

Non-authoritative answer:
escuelavirtual.dian.gov.co canonical name = escuela.dian.gov.co.
Name: escuela.dian.gov.co
Address: ***190.24.148.137***

Después el comando whois ejecutado en un terminal Linux nos permite saber a quien pertenece esta gama de direcciones IP, la DIAN:

***whois* 190.24.148.167**

inetnum: 190.24.148/24
status: reallocated
owner: DIAN
ownerid: CO-DIAN1-LACNIC
responsible: Freddy Barrios
address: Calle 25, 12, 15
address: 9999 - Bogotá - CU
country: CO
phone: +57 1 6079999 [1530]
owner-c: FRB5
tech-c: FRB5
abuse-c: FRB5
created: 20070504
changed: 20070504
inetnum-up: 190.24/16

nic-hdl: FRB5
person: Freddy Barrios
e-mail: lacnic_etb@HOTMAIL.COM
address: Calle 25, 15, 30
address: 9999 - Bogotá - CU
country: CO
phone: +57 1 6079999 [1530]
created: 20070504
changed: 20070504

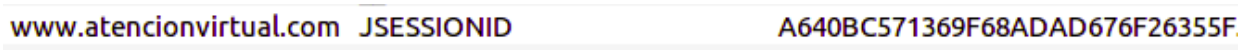
[5] El dominio atencionvirtual.com aparece vinculado con el servicio de chat de la DIAN

La url de las páginas del servicio de chat empiezan por "http://www.asistenciachat.com/".
Sin embargo, el dominio "atencionvirtual.com" aparece escondido en varias partes:

- en el código fuente de la página del segundo formulario de chat :

<iframe id="fram" frameborder="0" width="100%" height="900px" src="http://www.atencionvirtual.com/website/dianchat/?usr=1015842780&origen=Internet"></iframe>

- en las cookies que se instalan cuando uno se conecta al servicio de chat :



- en el análisis de los flujos HTTP :

http://www.atencionvirtual.com/website/dianchat/?usr=1015842780&origen=Internet
GET /website/dianchat/?usr=1015842780&origen=Internet HTTP/1.1
Host: www.atencionvirtual.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: es-MX,es-ES;q=0.9,es;q=0.7,es-AR;q=0.6,es-CL;q=0.4,en-US;q=0.3,en;q=0.1
Accept-Encoding: gzip, deflate
Referer: http://www.asistenciachat.com/chat_dian/chat_dian.aspx
Connection: keep-alive
Upgrade-Insecure-Requests: 1

[6] Los dominios "asistenciachat.com" y "atencionvirtual.com" no dejan ver directamente a quien pertenecen en un whois :

Unos *whois* en un Terminal Linux en estos dos dominios dan respectivamente estas respuestas :

Domain Name: ASISTENCIACHAT.COM
Registry Domain ID: 1766174554_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.enom.com
Registrar URL: http://www.enom.com
Updated Date: 2017-03-02T17:41:02Z
Creation Date: 2012-12-13T21:59:16Z
Registry Expiry Date: 2017-12-13T21:59:16Z
Registrar: eNom, Inc.
Registrar IANA ID: 48
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: DNS1.NAME-SERVICES.COM
Name Server: DNS2.NAME-SERVICES.COM
Name Server: DNS3.NAME-SERVICES.COM
Name Server: DNS4.NAME-SERVICES.COM
Name Server: DNS5.NAME-SERVICES.COM
DNSSEC: unsigned

Domain Name: ATENCIONVIRTUAL.COM
Registry Domain ID: 1741160637_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2015-07-21T19:33:10Z
Creation Date: 2012-08-28T15:05:34Z

Registry Expiry Date: 2018-08-28T15:05:34Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: 480-624-2505
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: BIRLOCHA.EPM.NET.CO
Name Server: LAUTA.EPM.NET.CO
DNSSEC: unsigned

No dejan aparecer explícitamente a quien pertenece (el *Registrant ID*).
Sin embargo los servidores de dominios (*Name Server*) asociado al dominio "atencionvirtual.com" muestra las siguiente URL: BIRLOCHA.EPM.NET.CO y LAUTA.EPM.NET.CO.

[7] [...]

[8] Direcciones IP y *hosting* de los servidores webs del servicio de chat

Para cada uno de los dominios "atencionvirtual.com" y "asistenciachat.com", buscamos la dirección IP del servidor web vía el comando nslookup ejecutado en un terminal Linux e hicimos un whois. En ambos casos, llegamos al mismo resultado : **los servidores webs están albergados en un centro de la empresa colombiana EPM Telecomunicaciones**.

nslookup www.atencionvirtual.com

Server: 127.0.1.1
Address: 127.0.1.1#53
Non-authoritative answer:
Name: atencionvirtual.com
Address: 200.13.225.137

whois 200.13.225.137

inetnum: 200.13.224/19
status: allocated
aut-num: N/A
owner: EPM Telecomunicaciones S.A. E.S.P.
ownerid: CO-EPME1-LACNIC
responsible: Administrador EPMNET
address: Carrera 77 39b-16, -, -
address: 940 - Medellin - CO
country: CO
phone: +57 4 4152280 []
owner-c: YGO2
tech-c: YGO2
abuse-c: YGO2

inetrev: 200.13.224/19
nserver: LAUTA.UNE.NET.CO
nsstat: 20170916 AA
nslastaa: 20170916
nserver: BIRLOCHA.UNE.NET.CO
nsstat: 20170916 AA
nslastaa: 20170916
nserver: NSBOG01.UNE.NET.CO
nsstat: 20170916 AA
nslastaa: 20170916
created: 20000705
changed: 20010926

nic-hdl: YGO2
person: Juan Molina
e-mail: adminternet@UNE.NET.CO
address: Cra. 16 Nro. 11A Sur 100, 100, --
address: NA - Medellin - An
country: CO
phone: +57 4 5150505 [0]
created: 20030120
changed: 20110928

nslookup www.asistenciachat.com

Server: 127.0.1.1
Address: 127.0.1.1#53
Non-authoritative answer:
Name: asistenciachat.com
Address: 201.232.123.67

whois 201.232.123.67

inetnum: 201.232.0/17
status: allocated
aut-num: N/A
owner: EPM Telecomunicaciones S.A. E.S.P.
ownerid: CO-EPME1-LACNIC
responsible: Administrador EPMNET
address: Carrera 77 39b-16, -, -
address: 940 - Medellin - CO
country: CO
phone: +57 4 4152280 []
owner-c: YGO2
tech-c: YGO2
abuse-c: YGO2
inetrev: 201.232.0/17
nserver: LAUTA.UNE.NET.CO
nsstat: 20170915 AA
nslastaa: 20170915
nserver: BIRLOCHA.UNE.NET.CO
nsstat: 20170915 AA
nslastaa: 20170915
nserver: NSBOG01.UNE.NET.CO

nsstat: 20170915 AA
nslastaa: 20170915
created: 20050524
changed: 20050524

nic-hdl: YGO2
person: Juan Molina
e-mail: adminternet@UNE.NET.CO
address: Cra. 16 Nro. 11A Sur 100, 100, --
address: NA - Medellin - An
country: CO
phone: +57 4 5150505 [0]
created: 20030120
changed: 20110928

[9] Envío de datos mediante el protocolo HTTPS (análisis de código fuente HTML)

Se busco en cada una de las páginas mencionadas la parte del código fuente que corresponde al envío de los datos. Ponemos aquí la URL y después el extracto del código fuente HTML correspondiente al envío de datos del formulario de login.

- **Inscripción en el RUT**
  https://muisca.dian.gov.co/WebRutMuisca/DefInscripcionRutPortal.faces
  *<form id="vistaInscripcionRut:frmInscripcionRut" **method="post"** **action="/WebRutMuisca/DefInscripcionRutPortal.faces"** enctype="application/x-www-form-urlencoded">*
  y en el paso siguiente (formulario completo) : <form action="" name="formVisorFormulario">

- **Nuevos usuarios**
  https://muisca.dian.gov.co/WebArquitectura/DefNuevosUsuarios.faces
  *<form id="vistaHabilitarNuevosUsuarios:frmActivarCuentaUsuario" **method="post"***
  *action="/WebArquitectura/**DefNuevosUsuarios**.faces" enctype="application/x-www-form-urlencoded">*

- **Inicio de sesión para usuarios registrados**
  https://muisca.dian.gov.co/WebArquitectura/DefLogin.faces
  *<form id="vistaLogin:frmLogin" **method="post"** action="/WebArquitectura/**DefLogin**.faces"*
  enctype="application/x-www-form-urlencoded">

- **Recuperación Clave de Accesos**
  https://muisca.dian.gov.co/WebArquitectura/DefPasswordRecuperacion.faces
  *<form id="vistaRecuperacion:frmRecuperacion" **method="post"***
  action="/WebArquitectura/DefPasswordRecuperacion.faces" enctype="application/x-www-form-urlencoded">

- **Consulta Estado RUT**
  https://muisca.dian.gov.co/WebRutMuisca/DefConsultaEstadoRUT.faces
  *<form id="vistaConsultaEstadoRUT:formConsultaEstadoRUT" **method="post"***
  action="/WebRutMuisca/DefConsultaEstadoRUT.faces" enctype="application/x-www-f orm-urlencoded">

- **Gestion Aduanera / Importación** :
  https://importacionescarga.dian.gov.co/WebArquitectura/DefLogin.faces
  *<form id="vistaLogin:frmLogin" **method="post"***
  action="/WebArquitectura/DefLogin.faces;jsessionid=FCC079C3B2FB0BA87E81596E0273235E"
  enctype="application/x-www-form-urlencoded">

- **Consulta de Inconsistencia**
  https://muisca.dian.gov.co/WebGestionmasiva/DefSelPublicacionesExterna.faces
  *<form id="vistaSelPublicacionesExterna:formSelPublicacionesExterna" **method="post"***
  action="/WebGestionmasiva/DefSelPublicacionesExterna.faces" enctype="application/x- www-form-urlencoded">

- **Consulta de planillas radicadas**
  https://certificadosdeorigen.dian.gov.co/autocalificacion/Admonform03/scripts_php/consulta.php
  <form id="planilla" name="planilla.php" method="post">

- **Actualice su actividad económica**
  https://muisca.dian.gov.co/WebRutMuisca/DefActualizarActividadesCIIU.faces
  <form id="vistaActualizacionActividadesCIIU:frmActualizacionActividadesCIIU" method="post"
  action="/WebRutMuisca/DefActualizarActividadesCIIU.faces" enctype="application/x-www-form-urlencoded">

Se puede observar que en todos estos casos el envío se hace hacía la misma URL en general completada por algo (despues de "action=", "/WebRutMuisca/DefInscripcionRutPortal.faces" por ejemplo) y con el método POST. Por lo tanto, esto confirma que se usa el protocolo HTTPS para el envío de los datos correspondientes.

[10] Envío de datos mediante el protocolo HTTPS (análisis de flujo)

Aquí, ponemos extractos de capturas HTTP realizadas con la extensión del navegador Firefox *LiveHTTP Headers* en algunos de los formularios mencionados. Todas demuestran una transmisión de datos por el protocolo HTTPS y con el método POST.

https://muisca.dian.gov.co/WebArquitectura/DefNuevosUsuarios.faces

POST /WebArquitectura/DefNuevosUsuarios.faces HTTP/1.1
Host: muisca.dian.gov.co
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: es-MX,es-ES;q=0.9,es;q=0.7,es-AR;q=0.6,es-CL;q=0.4,en-US;q=0.3,en;q=0.1
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 5639
Referer: https://muisca.dian.gov.co/WebArquitectura/DefNuevosUsuarios.faces
Cookie: _ga=GA1.3.1189505068.1505077245; _gid=GA1.3.1088223913.1505077245;
__utma=133095963.1189505068.1505077245.1505077246.1505077246.1;
__utmb=133095963.4.10.1505077246; __utmc=133095963;
__utmz=133095963.1505077246.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
TS0167de4d=01615e36451d20d200cb5fedd9d7c1b2ba4355bbe2969037f7c89c251e3cc145b6d79b369
9be17195c77af9d150f0d9e653805be84a61017efe3099be5a7aeb214539241a0;
JSESSIONID=9170B6C77024ECAF2403B8FBF9CDFD2C; DIAN-
MUISCA=N_1_393939_15e6da7433a_N_61736446313233_;
TS0167de4d_31=0184d7998b1d949fdac51a5c518dd6e894141c3543661bc662db1a5e96a523de67d22
aae3b83b824c1ef802b38e60a49f76928eb235c16e708ba3cd139deb767d56892c8d93c2f96342bf26f00c
ef7e6acc960d895146bd83968714939da8fea967a1d069a3565f8b9c5cfa66fdcd0260e42c2f507;
__utma=64759731.217077313.1505078236.1505078236.1505078236.1;
__utmb=64759731.7.10.1505078236; __utmc=64759731;
__utmz=64759731.1505078236.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
TS0167de4d_77=2332_84516cce81adcaca_rsb_0_rs_%2FWebRutMuisca%2FDefInscripcionRutPortal.
faces_rs_2_rs_0
Connection: keep-alive
Upgrade-Insecure-Requests: 1
vistaHabilitarNuevosUsuarios%3AfrmActivarCuentaUsuario%3AmodoPresentacionSeleccionBO=pantall
a&vistaHabilitarNuevosUsuarios%3AfrmActivarCuentaUsuario%3AsiguienteURL=&vistaHabilitarNuevos
Usuarios%3AfrmActivarCuentaUsuario%3AmodoPresentacionFormBO=pantalla&vistaHabilitarNuevosU
suarios%3AfrmActivarCuentaUsuario%3AmodoOperacionFormBO=&vistaHabilitarNuevosUsuarios%3Af
rmActivarCuentaUsuario%3AhddSiguienteURL=&vistaHabilitarNuevosUsuarios%3AfrmActivarCuentaUs
uario%3Aselect**TipoDocumento=22**&vistaHabilitarNuevosUsuarios%3AfrmActivarCuentaUsuario%3Atx
t**NumeroDocumento=123456**&vistaHabilitarNuevosUsuarios%3AfrmActivarCuentaUsuario%3Atxt**Fech
aExpedicion=01012017**&vistaHabilitarNuevosUsuarios%

**https://importacionescarga.dian.gov.co/WebArquitectura/DefLogin.faces;jsessionid=898197742A70
69A2C8F51EE8A08A325E**

POST /WebArquitectura/DefLogin.faces;jsessionid=898197742A7069A2C8F51EE8A08A325E
HTTP/1.1
Host: importacionescarga.dian.gov.co
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: es-MX,es-ES;q=0.9,es;q=0.7,es-AR;q=0.6,es-CL;q=0.4,en-US;q=0.3,en;q=0.1
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 5835
Referer: https://importacionescarga.dian.gov.co/WebArquitectura/DefLogin.faces
Cookie: _ga=GA1.3.1189505068.1505077245; _gid=GA1.3.1088223913.1505077245;
__utma=133095963.1189505068.1505077245.1505077246.1505080482.2; __utmc=133095963;
__utmz=133095963.1505077246.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
JSESSIONID=898197742A7069A2C8F51EE8A08A325E; DIAN-
MUISCA=N_1_393939_15e6dc9fc5f_N_61736446313233_;
__utma=175849402.1084967609.1505080512.1505080512.1505080512.1; __utmc=175849402;
__utmz=175849402.1505080512.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)

Connection: keep-alive
Upgrade-Insecure-Requests: 1
vistaLogin%3AfrmLogin%3AhddCadena=&vistaLogin%3AfrmLogin%3AhddCodigoOrg=&vistaLogin%3AfrmLogin%3AhddCodigoUsuario=&vistaLogin%3AfrmLogin%3AhddTokTareaNeg=&vistaLogin%3AfrmLogin%3AselNit=0&vistaLogin%3AfrmLogin%3AtxtNit=123456789&vistaLogin%3AfrmLogin%3AselTipoDoc=22&vistaLogin%3AfrmLogin%3AtxtUsuario=123456&vistaLogin%3AfrmLogin%3AtxtCadena=azerty78&vistaLogin%3AfrmLogin%3A_id18.x=57&vistaLogin%3AfrmLogin

https://muisca.dian.gov.co/WebArquitectura/DefNuevosUsuarios.faces

POST /WebArquitectura/DefNuevosUsuarios.faces HTTP/1.1
Host: muisca.dian.gov.co
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: es-MX,es-ES;q=0.9,es;q=0.7,es-AR;q=0.6,es-CL;q=0.4,en-US;q=0.3,en;q=0.1
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 5639
Referer: https://muisca.dian.gov.co/WebArquitectura/DefNuevosUsuarios.faces
Cookie: _ga=GA1.3.1189505068.1505077245; _gid=GA1.3.1088223913.1505077245; __utma=133095963.1189505068.1505077245.1505077246.1505077246.1; __utmb=133095963.4.10.1505077246; __utmc=133095963; __utmz=133095963.1505077246.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); TS0167de4d=01615e36451d20d200cb5fedd9d7c1b2ba4355bbe2969037f7c89c251e3cc145b6d79b3699be17195c77af9d150f0d9e653805be84a61017efe3099be5a7aeb214539241a0; JSESSIONID=9170B6C77024ECAF2403B8FBF9CDFD2C; DIAN-MUISCA=N_1_393939_15e6da7433a_N_61736446313233_; TS0167de4d_31=0184d7998b1d949fdac51a5c518dd6e894141c3543661bc662db1a5e96a523de67d22aae3b83b824c1ef802b38e60a49f76928eb235c16e708ba3cd139deb767d56892c8d93c2f96342bf26f00cef7e6acc960d895146bd83968714939da8fea967a1d069a3565f8b9c5cfa66fdcd0260e42c2f507; __utma=64759731.217077313.1505078236.1505078236.1505078236.1; __utmb=64759731.7.10.1505078236; __utmc=64759731; __utmz=64759731.1505078236.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); TS0167de4d_77=2332_84516cce81adcaca_rsb_0_rs_%2FWebRutMuisca%2FDefInscripcionRutPortal.faces_rs_2_rs_0
Connection: keep-alive
Upgrade-Insecure-Requests: 1
vistaHabilitarNuevosUsuarios%3AfrmActivarCuentaUsuario%3AmodoPresentacionSeleccionBO=pantalla&vistaHabilitarNuevosUsuarios%3AfrmActivarCuentaUsuario%3AsiguienteURL=&vistaHabilitarNuevosUsuarios%3AfrmActivarCuentaUsuario%3AmodoPresentacionFormBO=pantalla&vistaHabilitarNuevosUsuarios%3AfrmActivarCuentaUsuario%3AmodoOperacionFormBO=&vistaHabilitarNuevosUsuarios%3AfrmActivarCuentaUsuario%3AhddSiguienteURL=&vistaHabilitarNuevosUsuarios%3AfrmActivarCuentaUsuario%3AselectTipoDocumento=22&vistaHabilitarNuevosUsuarios%3AfrmActivarCuentaUsuario%3AtxtNumeroDocumento=123456&vistaHabilitarNuevosUsuarios%3AfrmActivarCuentaUsuario%3AtxtFechaExpedicion=01012017&vistaHabilitarNuevosUsuarios%3AfrmActivarCuentaUsuario%

[11] El formulario de login del subdominio “escuelavirtual.gov.co” enviá los datos con HTTP

El siguiente extracto del código fuente HTML de la página correspondiente al formulario de login muestra que los datos se envían con el protocolo HTTP y el método POST :

Entre aquí usando su nombre de usuario y contraseña
(Las 'Cookies' deben estar habilitadas en su navegador)
<form action="http://escuelavirtual.dian.gov.co/moodle/login/index.php" method="post" id="login" >

[12] El formulario de CHAT enviá los datos con HTTP/POST y después con HTTP/GET

Aquí están la solicitud HTTP que corresponde al envió de datos del segundo formulario del CHAT y la respuesta del servidor.

http://www.atencionvirtual.com/website/dianchat/account.jsp

POST /website/dianchat/account.jsp HTTP/1.1
Host: www.atencionvirtual.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: es-MX,es-ES;q=0.9,es;q=0.7,es-AR;q=0.6,es-CL;q=0.4,en-US;q=0.3,en;q=0.1
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 953
Referer: http://www.atencionvirtual.com/website/dianchat/?usr=1015842780&origen=Internet
Cookie: autHorval=1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
aicAuthLogin=KARISMA&TipoPersona=Persona+Juridica&FormaConsulta=Persona+Natural&**RazonSocial=FUNDACION+KARISMA**+%28**test+sitio+Internet**%29&aic**Documento=1015842780**&aicEsc**Contact=test%40karisma.org.co**&**Direccion=Calle+59%2318**&**Tel=7389860**&c**mbMake=BOGOT**%C3%81%2C+**D.C**.&**cmbModel=+BOGOT**%C3%81%2C+D.C.&origen=&aicAuthAction=login&aicEscAction=escalate&aicEscEndpoint=chat&aicTenant=DianChat&aicAuthLevel=guest&aicLanguage=es&aicEscTranscriptRequest=on&aicEscStartURL=http%3A%2F%2Fwww.dian.gov.co&aicEscEmailTo=dian%40dian.gov.co&aicEscQuestion=.+Identificaci%C3%B3n%3A+1015842780+-
++Origen+%3E%3E+Internet+Nombre+Persona+%3E%3E+KARISMA+Tipo+Persona+%3E%3E+Persona+Juridica+Forma+Consulta+%3E%3E+Persona+Natural+Raz%C3%B3n+Social%2FNombre+%3E%3E+FUNDACION+KARISMA+%28test+sitio+Internet%29+Email+%3E%3E+test%40karisma.org.co+Direccion+%3E%3E+Calle+59%2318+Telefono+de+Contacto+%3E%3E+7389860+Departamento+%3E%3E+BOGOT%C3%81%2C+D.C.+Ciudad+%3E%3E++BOGOT%C3%81%2C+D.C.: undefined

HTTP/1.1 302 Moved Temporarily
Cache-Control: no-cache
Pragma: no-cache
Content-Length: 0
Content-Type: text/html;charset=utf-8
Location:
http://www.atencionvirtual.com/website/dianchat/escalate.jsp;jsessionid=A640BC571369F68ADAD676F26355FB62?aicEscTranscriptRequest=on&aicEscAction=escalate&aicEscEndpoint=chat&aicEsc**EmailTo=dian%40dian.gov.co**&aicEscStartURL=http%3a%2f%2fwww.dian.gov.co&aicEsc**Contact=test%40karisma.org.co**&aicEscQuestion=.+Identificaci%c3%b3n%3a+1015842780+-++Origen+%3e%3e+Internet+Nombre+Persona+%3e%3e+**KARISMA**+Tipo+Persona+%3e%3e+Persona+Juridica+Forma+Consulta+%3e%3e+Persona+Natural+Raz%c3%b3n+Social%2fNombre+%3e%3e+**FUNDACION+KARISMA+(test+sitio+Internet)**+**Email+%3e%3e+test%40karisma.org.co**+**Direccion+%3e%3e+Calle+59%2318+Telefono+de+Contacto+%3e%3e+7389860+Departamento+%3e%3e+BOGOT%c3%81%2c+D.C.+Ciudad+%3e%3e++BOGOT%c3%81%2c+D.C.**
Server: Microsoft-IIS/7.0
Set-Cookie: JSESSIONID=A640BC571369F68ADAD676F26355FB62; Path=/website
Set-Cookie:
AVAYA_IC_WEBADMIN_COOKIE=0e160d120033202b3e20247470355d54005a5a060a0253323d2e245b5e51; Domain=.atencionvirtual.com; Path=/
X-Powered-By: ASP.NET
X-Frame-Options: NONE
Date: Sat, 16 Sep 2017 17:29:16 GMT

Se pueden observar lo siguiente:

- el envió de los datos del formulario se hace con el protocolo HTTP y el método POST ;
- en la página precedente (ver cabecera Referer: http://www.atencionvirtual.com/website/dianchat/?usr=1015842780&origen=Internet) se había transmitido el número de cédula en la URL y con el protocolo HTTP (mÉtodo GET) ;
- la respuesta del servidor web es muy interesante. Hace una redirección (“HTTP/1.1 302 Moved Temporarily”) hacía una nueva URL que contiene los datos del formulario en parámetro. A partir de este momento los datos se van a transmitir con el método GET, lo que es una mala práctica, como se detalla más adelante.

Un detalle que se puede observar, la instalación de la cookie “**AVAYA_IC_WEBADMIN_COOKIE**” indica que la solución para el CHAT es muy probablemente de tipo AVAYA.

[13] *Cookies* instaladas en el sitio www.dian.gov.co

Después del experimento de navegación en sitio “www.dian.gov.co” se encontró (usando la extensión de Firefox *Cookie Manager +*) que las siguientes cookies habían sido instaladas en nuestro computador :

Domain	Name	Content	Expires	Created	HTT...	Secure
muisca.dian....	TS0167de4d	01615e3645303bb0c77a8f2a7973e34c953f9f...	Al final de la sesión	10 de septiembre de 2017 ...	No	No
muisca.dian....	TS0167de4d_31	0184d7998ba5d90191d9f3039ca81e60d58fd...	Al final de la sesión	10 de septiembre de 2017 ...	No	No
~~.dian.gov.co~~	~~__utmt~~	~~1~~	~~10 de septiembre de 2017 ...~~	~~10 de septiembre de 2017 ...~~	~~No~~	~~No~~
~~.dian.gov.co~~	~~_gat~~	~~1~~	~~10 de septiembre de 2017 ...~~	~~10 de septiembre de 2017 ...~~	~~No~~	~~No~~
.dian.gov.co	__utmc	133095963	Al final de la sesión	10 de septiembre de 2017 ...	No	No
~~.dian.gov.co~~	~~__utmb~~	~~133095963.1.10.1505080482~~	~~10 de septiembre de 2017 ...~~	~~10 de septiembre de 2017 ...~~	~~No~~	~~No~~
.dian.gov.co	__utma	133095963.1189505068.1505077245.150507...	10 de septiembre de 2019 ...	10 de septiembre de 2017 ...	No	No
.dian.gov.co	__utmz	133095963.1505077246.1.1.utmcsr=(direct)|...	12 de marzo de 2018 04:54...	10 de septiembre de 2017 ...	No	No
.importacion...	__utmc	175849402	Al final de la sesión	10 de septiembre de 2017 ...	No	No
~~.importacion...~~	~~__utmb~~	~~175849402.1.10.1505080512~~	~~10 de septiembre de 2017 ...~~	~~10 de septiembre de 2017 ...~~	~~No~~	~~No~~
.importacion...	__utma	175849402.1084967609.1505080512.150508...	10 de septiembre de 2019 ...	10 de septiembre de 2017 ...	No	No
.importacion...	__utmz	175849402.1505080512.1.1.utmcsr=(direct)|...	12 de marzo de 2018 04:55...	10 de septiembre de 2017 ...	No	No
muisca.dian....	TS0167de4d_77	2332_84516cce81adcaca_rsb_0_rs_%2FWeb...	Al final de la sesión	10 de septiembre de 2017 ...	No	No
.muisca.dian...	__utmc	64759731	Al final de la sesión	10 de septiembre de 2017 ...	No	No
~~.muisca.dian...~~	~~__utmb~~	~~64759731.10.10.1505078236~~	~~10 de septiembre de 2017 ...~~	~~10 de septiembre de 2017 ...~~	~~No~~	~~No~~
.muisca.dian...	__utmz	64759731.1505078236.1.1.utmcsr=(direct)|u...	12 de marzo de 2018 04:46...	10 de septiembre de 2017 ...	No	No
.muisca.dian...	__utma	64759731.217077313.1505078236.15050782...	10 de septiembre de 2019 ...	10 de septiembre de 2017 ...	No	No
importacion...	JSESSIONID	898197742A7069A2C8F51EE8A08A325E	Al final de la sesión	10 de septiembre de 2017 ...	No	No
muisca.dian....	JSESSIONID	9170B6C77024ECAF2403B8FBF9CDFD2C	Al final de la sesión	10 de septiembre de 2017 ...	No	No
.dian.gov.co	_gid	GA1.3.1088223913.1505077245	11 de septiembre de 2017 ...	10 de septiembre de 2017 ...	No	No
.dian.gov.co	_ga	GA1.3.1189505068.1505077245	10 de septiembre de 2019 ...	10 de septiembre de 2017 ...	No	No
muisca.dian....	DIAN-MUISCA	N_1_393939_15e6dbeecc2_N_617364463132...	Al final de la sesión	10 de septiembre de 2017 ...	No	No

Se trata por la mayoría de ellas, de cookies de sesión con una finalidad probablemente técnica, que puede ser vinculada con la seguridad. Se puede observar en las dos últimas columnas que ninguna de ellas tiene el atributo "HTTPOnly" o "Secure".

Hay también otras *cookies* que tienen un nombre que empieza por "_utm" o por "_g" y que tienen larga duración de vida. Estas son las *cookies* del servicio *Google Analytics*. En particular, la *cookie* "_utma" contiene un número único que permite a Google identificar las personas (los "usuarios")[29].

[14] El análisis del código fuente deja aparecer a *Google Analytics*

En el código fuente de la primera página del sitio, se puede encontrar la parte siguiente, que es el script (javascript) de *Google Analytics* :

```
<script type="text/javascript">

  var _gaq = _gaq || [];
  _gaq.push(['_setAccount', 'UA-29697470-1']);
  _gaq.push(['_trackPageview']);

  (function() {
```

[29] "*Used to distinguish users and sessions.*" Para la fuente de esta citación y más detalles sobre las cookies de Google Analytics, ver: https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage

```
  var ga = document.createElement('script'); ga.type = 'text/javascript'; ga.async = true;
  ga.src = ('https:' == document.location.protocol ? 'https://ssl' : 'http://www') + '.google-analytics.com/ga.js';
  var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(ga, s);
 })();
```

En la página de inscripción a los servicios en línea, se encuentra también un javascript de Google Analytics :

```
<script type="text/javascript">

 var _gaq = _gaq || [];
 _gaq.push(['_setAccount', 'UA-29697470-1']);
 _gaq.push(['_trackPageview']);

 (function() {
  var ga = document.createElement('script'); ga.type = 'text/javascript'; ga.async = true;
  ga.src = ('https:' == document.location.protocol ? 'https://ssl' : 'http://www') + '.google-analytics.com/ga.js';
  var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(ga, s);
 })();
```

Estas funciones javascript están llamando otra función llamada “ga.js” y situada en los servidores de Google.

[15] Ejemplo de datos enviados a los servidores de Google

En estos tres extractos de *request* enviados a los servidores de *Google Analytics*, se puede observar que se transmite en parámetros de la URL el contenido de las cookies - en particular “_utma” que contiene el número de identificación con el cual Google nos puede perfilar - la URL de la página en la que estamos (en el primer caso la de definición de un nuevo usuario, en el segundo el cambio de password y en el tercero la inscripción al RUT):

https://ssl.googleanalytics.com/__utm.gif?
utmwv=5.2.5&utms=1&utmn=962382270&utmhn=muisca.dian.gov.co&utmcs=windows-1252&utmsr=1366x768&utmsc=24-bit&utmul=es-es&utmje=0&utmfl=11.2%20r202&utmdt=Direcci%C3%B3n%20de%20Impuestos%20y%20Aduanas%20Nacionales%20de%20Colombia&utmhid=25350478&utmr=http%3A%2F%2F**www.dian.gov.co%2F&utmp=%2FWebArquitectura%2FDefNuevosUsuarios.faces**&utmac=UA-29697470-1&utmcc=**__utma**%3D**64759731.641747317.1472345712.1472345712.1472345712.1**%3B%2B__utmz%3D64759731.1472345712.1.1.utmcsr%3Ddian.gov.co%7Cutmccn%3D(referral)%7Cutmcmd%3Dreferral%7Cutmcct%3D%2F%3B&utmu=q~

https://ssl.googleanalytics.com/__utm.gif?
utmwv=5.2.5&utms=3&utmn=539312189&utmhn=**muisca.dian.gov.co**&utmcs=windows-1252&utmsr=1366x768&utmsc=24-bit&utmul=es-es&utmje=0&utmfl=11.2%20r202&utmdt=Direcci%C3%B3n%20de%20Impuestos%20y%20Aduanas%20Nacionales%20de%20Colombia&utmhid=150472314&utmr=0&utmp=%2FWebArquitectura%2F**DefPas**

swordRecuperacion.faces&utmac=UA-29697470-1&utmcc=__**utma**%3D**64759731.641747317.1472345712.1472345712.1472345712.1**%3B%2B__utmz%3D64759731.1472345712.1.1.utmcsr%3Ddian.gov.co%7Cutmccn%3D(referral)%7Cutmcmd%3Dreferral%7Cutmcct%3D%2F%3B&utmu=q~

https://ssl.googleanalytics.com/__utm.gif?utmwv=5.2.5&utms=4&utmn=1032937431&utmhn=**muisca.dian.gov.co**&utmcs=windows-1252&utmsr=1366x768&utmsc=24-bit&utmul=es-es&utmje=0&utmfl=11.2%20r202&utmdt=Direcci%C3%B3n%20de%20Impuestos%20y%20Aduanas%20Nacionales%20de%20Colombia&utmhid=1606491581&utmr=0&utmp=%2FWebRutMuisca%2FDefl**nscripcionRutPortal**.faces&utmac=UA-29697470-1&utmcc=__**utma**%3D**64759731.641747317.1472345712.1472345712.1472345712**.1%3B%2B__utmz%3D64759731.1472345712.1.1.utmcsr%3Ddian.gov.co%7Cutmccn%3D(referral)%7Cutmcmd%3Dreferral%7Cutmcct%3D%2F%3B&utmu=q~

[16] Transmisión a Google del número de cédula ingresado en el primer formulario del servicio de CHAT

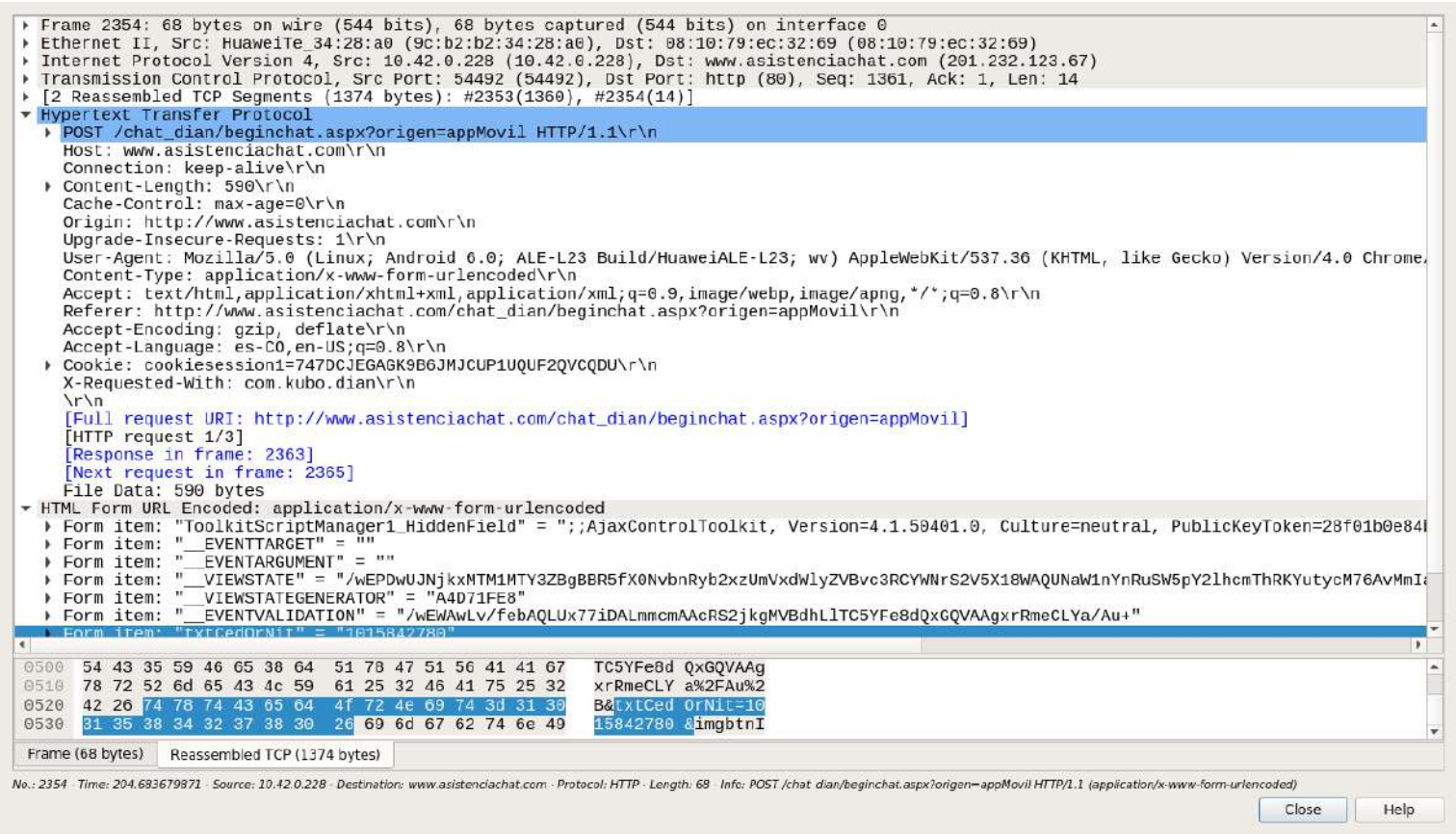
La siguiente solicitud hacía el servidor web de Google de dominio “ajax.googleapis.com”, iniciado desde la página www.atencionvirtual.com transmite el número de cédula entrado en el primero formulario.

https://ajax.googleapis.com/ajax/libs/jquery/1.11.1/jquery.min.js

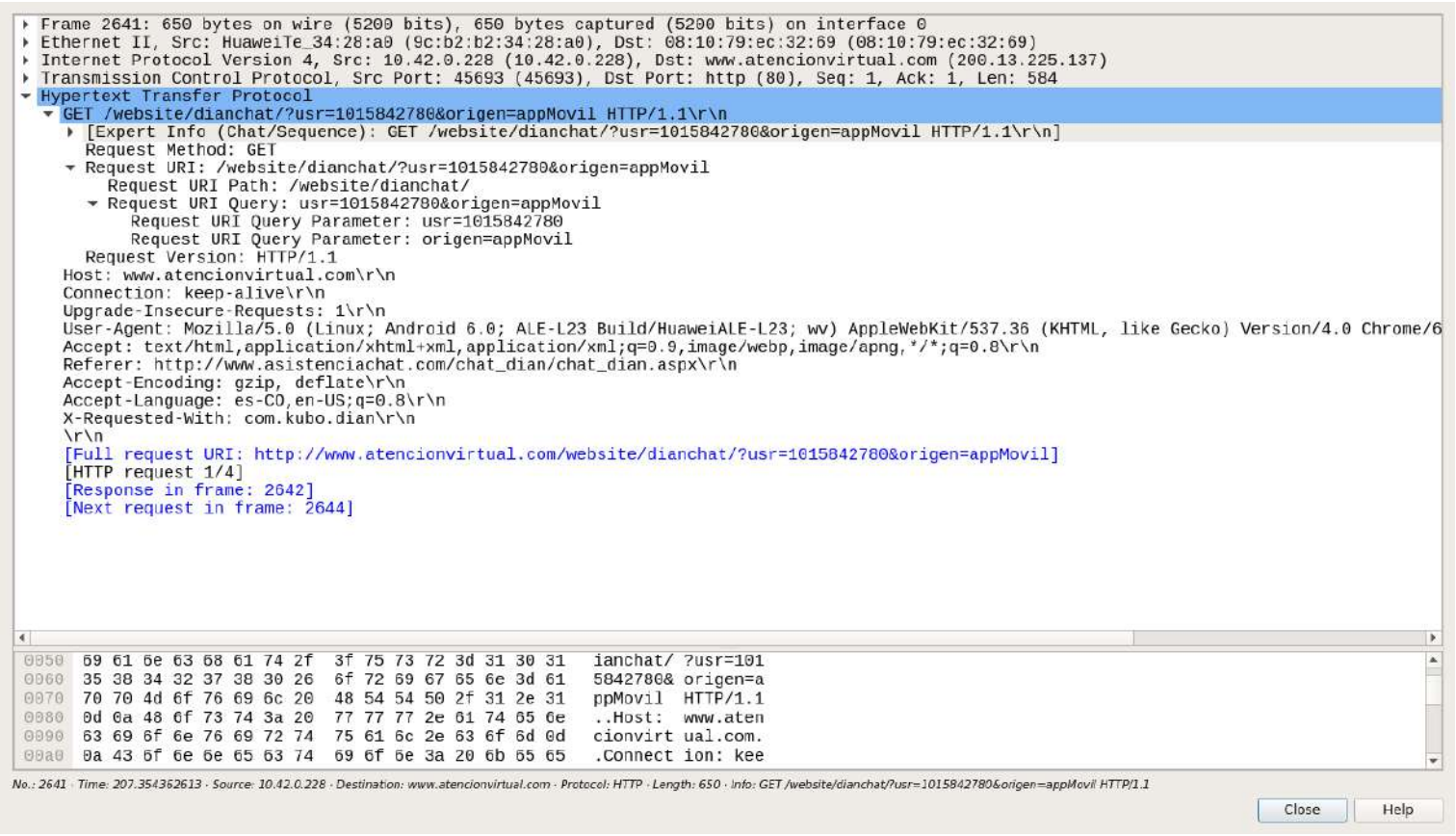
GET /ajax/libs/jquery/1.11.1/jquery.min.js HTTP/1.1
Host: ajax.googleapis.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: */*
Accept-Language: es-MX,es-ES;q=0.9,es;q=0.7,es-AR;q=0.6,es-CL;q=0.4,en-US;q=0.3,en;q=0.1
Accept-Encoding: gzip, deflate, br
Referer: http://www.atencionvirtual.com/website/dianchat/?usr=1015842780&origen=Internet
Connection: keep-alive

[17] Envío del número de cédula del formulario por la Aplicación

Una búsqueda del número de cédula que entramos en el formulario (1015842780) en la captura hecha con Wireshark nos lleva a este paquete :



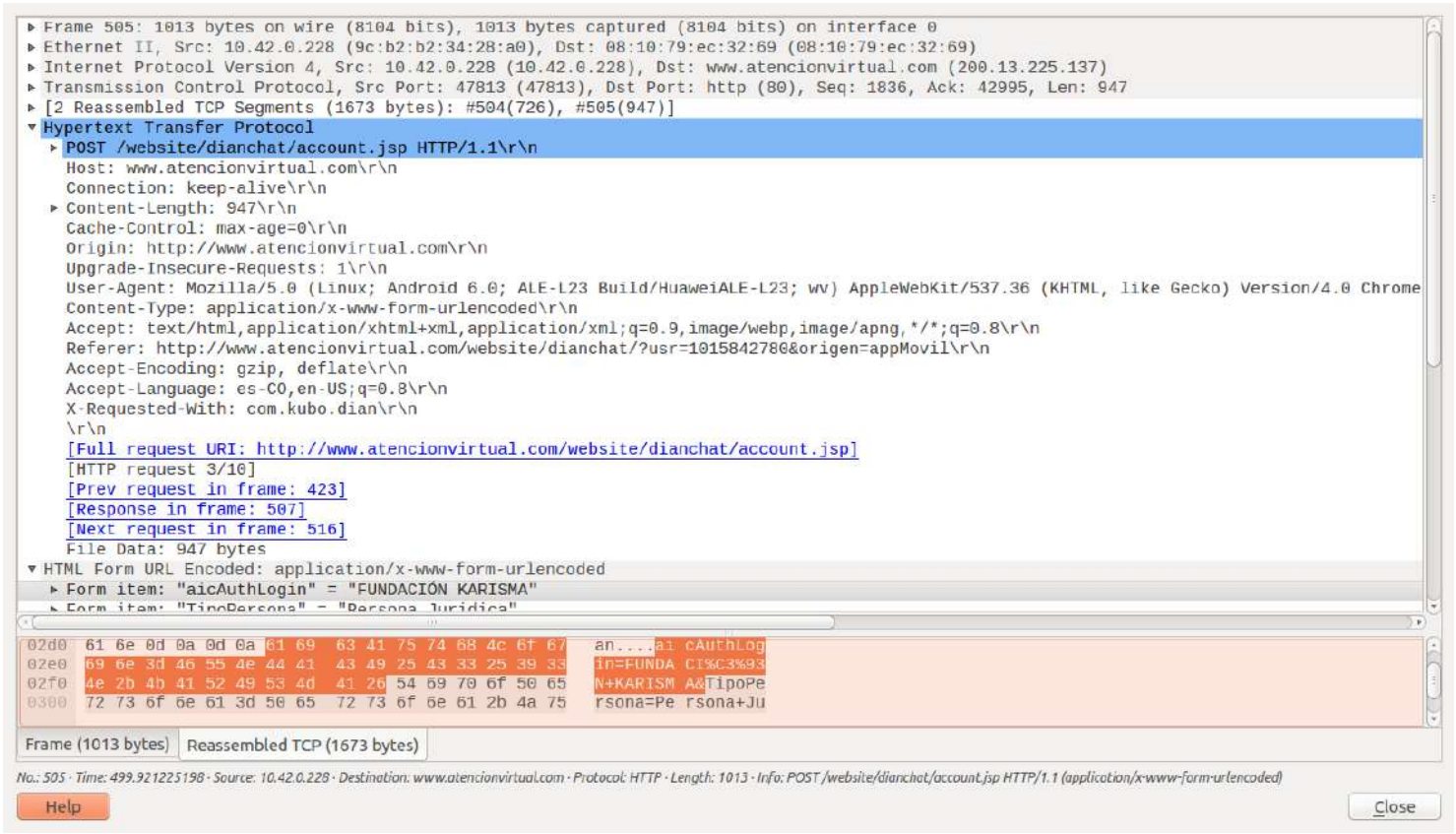
Se puede observar una solicitud con el protocolo HTTP y el método POST que envía el dato del formulario ("txtCed OrNit=1015842780") hacía el servidor "www.asistenciachat.com", con dirección IP 201.232.123.67.

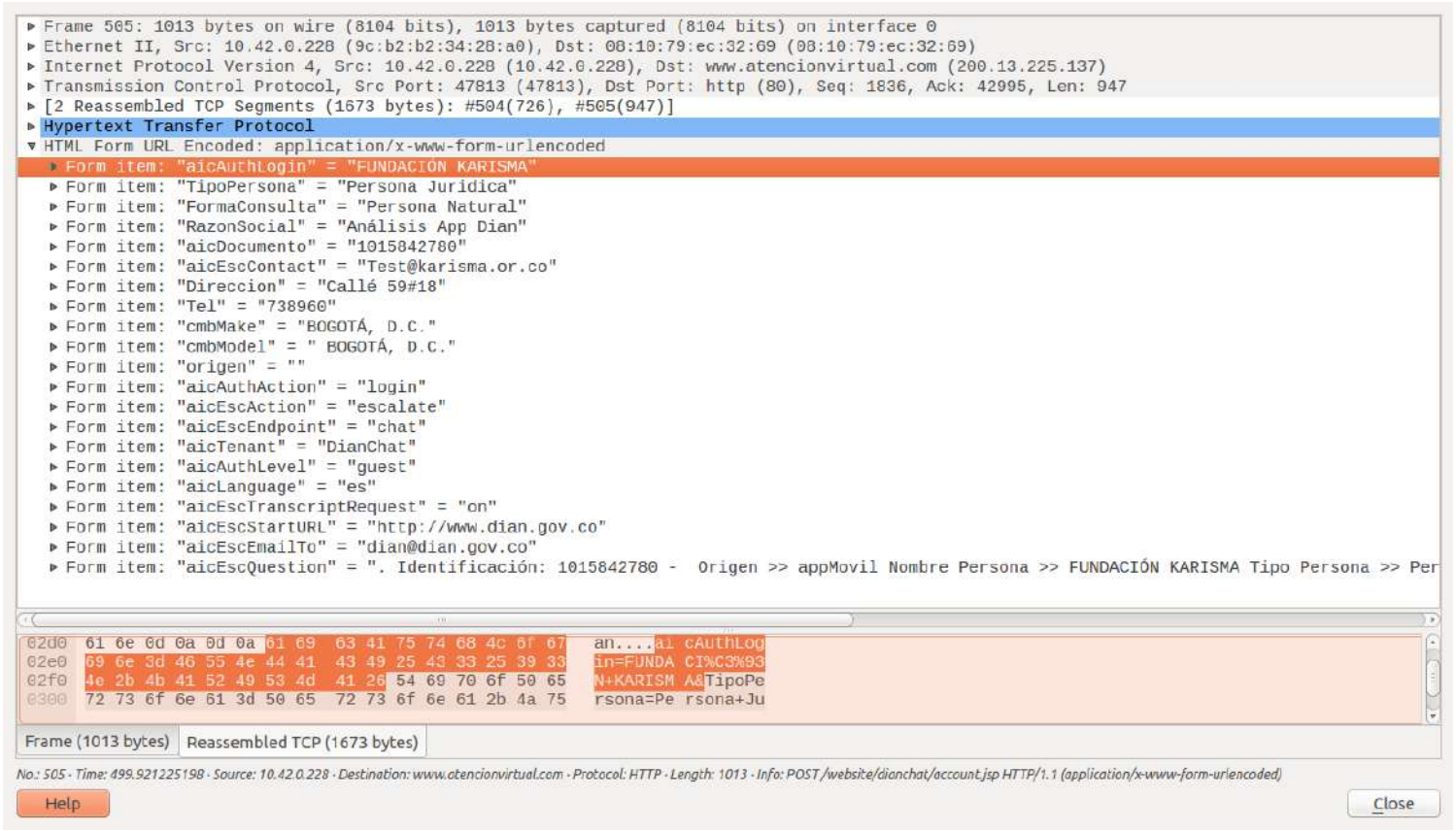


Pero la búsqueda de "1015842780" también nos conduce a otra solicitud similar pero con el método GET y hacía el servidor "www.atencionvirtual.com", con dirección IP 200.13.225.137.

[18] Envío de los datos completos del segundo formulario por la Aplicación

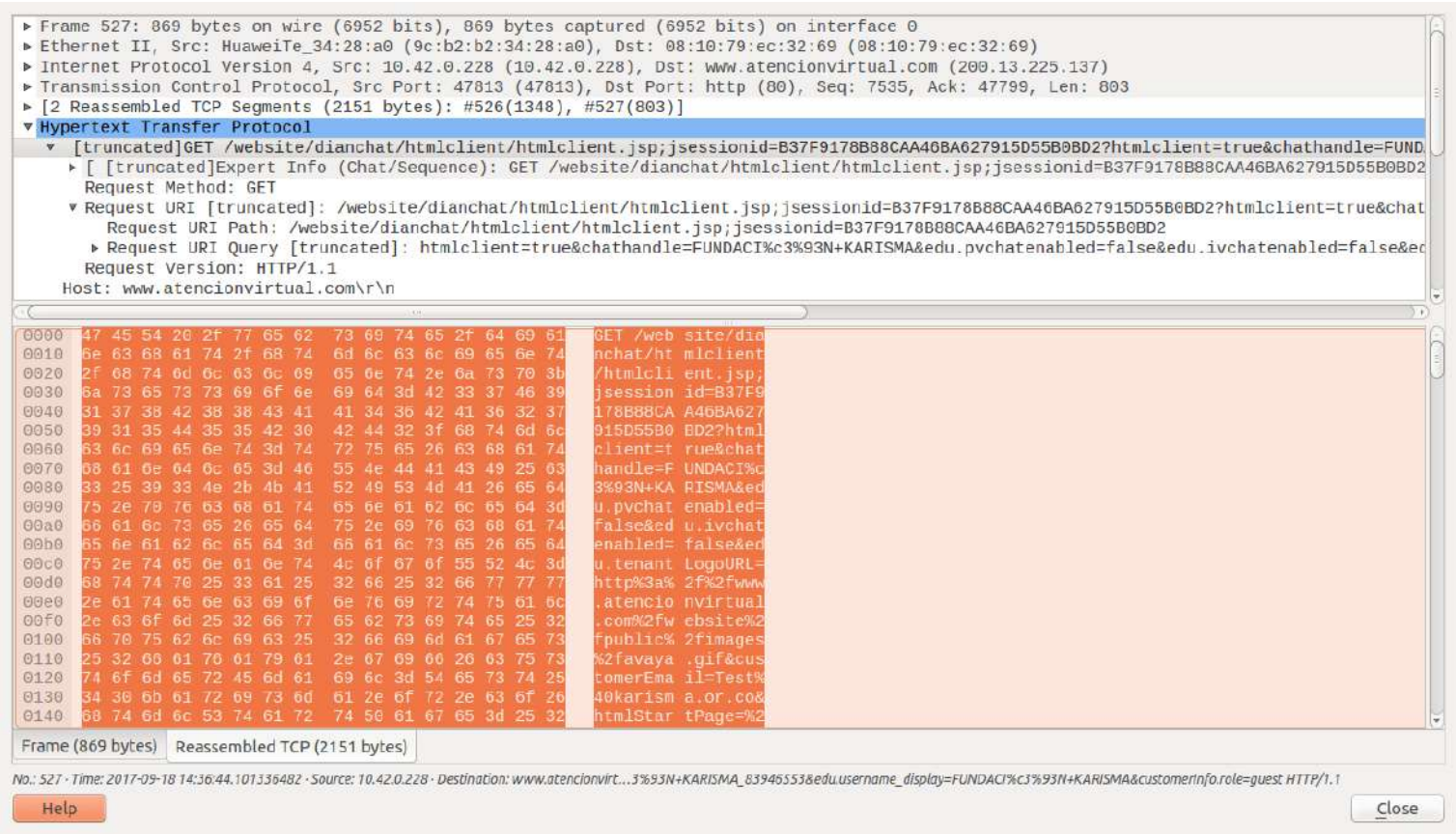
Una búsqueda de los otros datos que entramos en el segundo formulario (por ejemplo “Karisma”) en la captura hecha con *Wireshark* nos lleva a este paquete:





Se puede observar una solicitud con el protocolo HTTP y el método POST que envía los datos del segundo formulario hacía el servidor "www.atencionvirtual.com", con dirección IP 200.13.225.137.

Además la misma búsqueda nos lleva también a otro paquete (527) de datos:



Este muestra el envío de todos los datos del segundo formulario del CHAT con el método GET y hacía el servidor "www.atencionvirtual.com", con dirección IP 200.13.225.137.

[19] La Aplicación de la DIAN se comunica con "dian.kubo.co"

La siguiente solicitud muestra una comunicación con el protocolo HTTP hacía el servidor web del dominio "dian.kubo.co", con dirección IP 192.185.21.145. Kubo es la empresa colombiana que desarrollo la aplicación.

Pero un *whois* en la dirección IP muestra que esta pertenece a la empresa WEBSITEWELCOME, basada en Texas en Estados Unidos.

whois 192.185.21.145

NetRange: 192.185.0.0 - 192.185.255.255
CIDR: 192.185.0.0/16
NetName: HGBLOCK-10
NetHandle: NET-192-185-0-0-1
Parent: NET192 (NET-192-0-0-0-0)
NetType: Direct Allocation
OriginAS:
Organization: WEBSITEWELCOME.COM (BO)
RegDate: 2013-07-22
Updated: 2013-07-22
Ref: https://whois.arin.net/rest/net/NET-192-185-0-0-1

OrgName: **WEBSITEWELCOME.COM**
OrgId: BO
Address: 5005 Mitchelldale
Address: Suite #100
City: **Houston**
StateProv: **TX**
PostalCode: **77092**
Country: **US**
RegDate: 2011-02-16
Updated: 2016-06-10
Ref: https://whois.arin.net/rest/org/BO

ReferralServer: rwhois://rwhois.websitewelcome.com:4321

OrgAbuseHandle: IPADM551-ARIN
OrgAbuseName: IP Admin
OrgAbusePhone: +1-866-964-2867
OrgAbuseEmail: ipadmin@websitewelcome.com
OrgAbuseRef: https://whois.arin.net/rest/poc/IPADM551-ARIN

OrgNOCHandle: IPADM551-ARIN
OrgNOCName: IP Admin
OrgNOCPhone: +1-866-964-2867
OrgNOCEmail: ipadmin@websitewelcome.com
OrgNOCRef: https://whois.arin.net/rest/poc/IPADM551-ARIN

OrgTechHandle: IPADM551-ARIN
OrgTechName: IP Admin
OrgTechPhone: +1-866-964-2867
OrgTechEmail: ipadmin@websitewelcome.com
OrgTechRef: https://whois.arin.net/rest/poc/IPADM551-ARIN

[20] La Aplicación se comunica con "ajax.googleapis.com"

La siguiente solicitud muestra una comunicación con el protocolo HTTP hacía el servidor web del dominio "ajax.googleapis.com", con dirección IP 216.58.222.234. El hecho de que esta solicitud tiene como origen la aplicación de la DIAN se manifesta en la cabecera Referer que empieza por "http://www.atencionvirtual.com/".

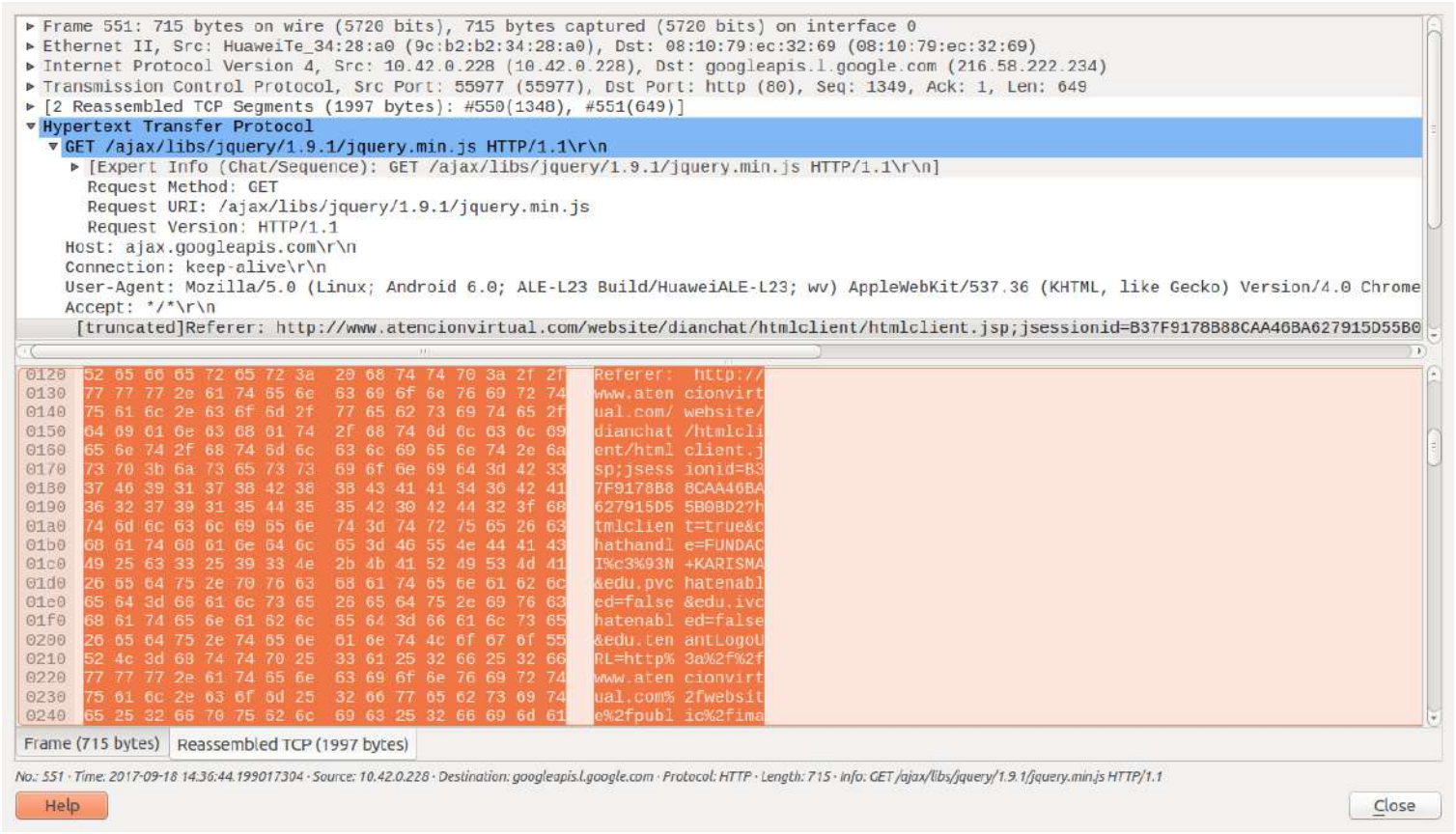
La diferencia entre el dominio solicitado ("ajax.googleapis.com") y con el cual se contacta efectivamente ("googleapis.l.google.com") se explica por el hecho de que el segundo es un alias del primero. Esto se puede observar haciendo una pregunta de los servidores de dominio con nslookup de esta manera :

nslookup ajax.googleapis.com
Server: 127.0.1.1
Address: 127.0.1.1#53

Non-authoritative answer:
ajax.googleapis.com canonical name = googleapis.l.google.com.
Name: googleapis.l.google.com
Address: 216.58.222.202
Name: googleapis.l.google.com
Address: 216.58.222.234

Un *whois* en esta dirección IP muestra que pertenece a Google Inc., en Estados Unidos.

[21] Transmisión, por Referer, de los datos del segundo formulario de CHAT a Google



Se puede observar que la cabecera Referer del protocolo HTTP es la URL del previo Anexo en el cual todos los datos del segundo formulario eran transmitidos en parámetros de la URL (método GET). En esta solicitud se llama una API de Google en la dirección "ajax.googleapis.com". **De paso se le envían a los servidores de Google todo estos datos por el intermedio del Referer.**

La URL completa transmitida a Google vía el Referer es la siguiente :

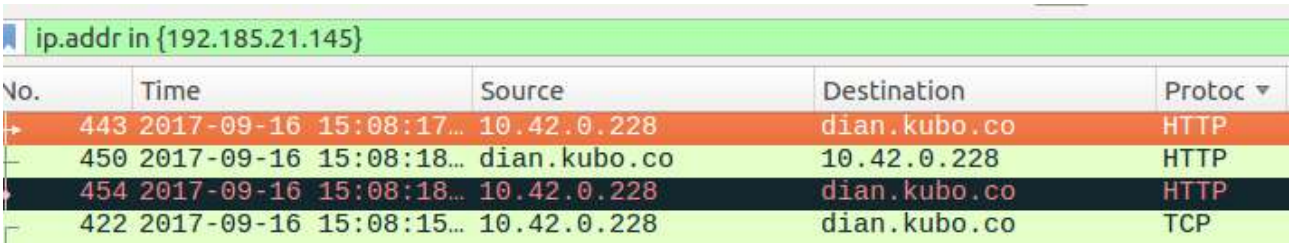
```
http://www.atencionvirtual.com/website/dianchat/htmlclient/htmlclient.jsp;jse
ssionid=B37F9178B88CAA46BA627915D55B0BD2?htmlclient=true&chathandle=FUNDACI%c
3%93N+KARISMA&edu.pvchatenabled=false&edu.ivchatenabled=false&edu.tenantLogoU
RL=http%3a%2f%2fwww.atencionvirtual.com%2fwebsite%2fpublic%2fimages%2favaya.g
if&customerEmail=Test%40karisma.or.co&htmlStartPage=%2fdianchat%2fhtmlclient%
2fhtmlclient.jsp&aicTenant=DianChat&aicLanguage=es&edu.tenant_key=97&tenant=D
ianChat&edu.callbacktype=Immediate&customerInfo.displayName=FUNDACI%c3%93N+KA
RISMA&languagecode=es&edu.language=es&customerInfo.tenant=DianChat&email.smtp
host=10.1.1.96&DomainBaseURL=http%3a%2f%2fwww.atencionvirtual.com%2fwebsite%2
fdianchat&ivchatHome=http%3a%2f%2fwww.atencionvirtual.com%2fwebsite%2fdiancha
t&customerInfo.login=FUNDACI%c3%93N+KARISMA&edu.requestedmedia=chat&customerI
nfo.is_deleted=0&edu.question=.+Identificaci%c3%b3n%3a+1015842780+-
++Origen+%3e%3e+appMovil+Nombre+Persona+%3e%3e+FUNDACI%c3%93N+KARISMA+Tipo+Pe
rsona+%3e%3e+Persona+Juridica+Forma+Consulta+%3e%3e+Persona+Natural+Raz%c3%b3
n+Social%2fNombre+%3e%3e+An%c3%a1lisis+App+Dian+Email+%3e%3e+Test%40karisma.o
r.co+Direccion+%3e%3e+Call%c3%a9+59%2318+Telefono+de+Contacto+%3e%3e+738960+D
epartamento+%3e%3e+BOGOT%c3%81%2c+D.C.+Ciudad+%3e%3e++BOGOT%c3%81%2c+D.C.&cus
tomerInfo.location=Other&edu.username=guest_FUNDACI%c3%93N+KARISMA_83946553&e
du.languagecode=es&email.from=dianchat%40dian.gov.co&edu.tenantName=DianChat&
language=es&customerInfo.mangledName=guest_FUNDACI%c3%93N+KARISMA_83946553&ed
u.username_display=FUNDACI%c3%93N+KARISMA&customerInfo.role=guest
```

Algunos caracteres especiales son codificados (ASCII, hexadecimal) pero después de decodificarlo, da lo siguiente y aparecen los datos entrados en el formulario.

```
http://www.atencionvirtual.com/website/dianchat/htmlclient/htmlclient.jsp;jse
ssionid=B37F9178B88CAA46BA627915D55B0BD2?htmlclient=true&chathandle=FUNDACIÓN
+KARISMA&edu.pvchatenabled=false&edu.ivchatenabled=false&edu.tenantLogoURL=ht
tp://www.atencionvirtual.com/website/public/images/avaya.gif&customerEmail=Te
st@karisma.or.co&htmlStartPage=/dianchat/htmlclient/htmlclient.jsp&aicTenant=
DianChat&aicLanguage=es&edu.tenant_key=97&tenant=DianChat&edu.callbacktype=Im
mediate&customerInfo.displayName=FUNDACIÓN+KARISMA&languagecode=es&edu.langua
ge=es&customerInfo.tenant=DianChat&email.smtphost=10.1.1.96&DomainBaseURL=htt
p://www.atencionvirtual.com/website/dianchat&ivchatHome=http://www.atencionvi
rtual.com/website/dianchat&customerInfo.login=FUNDACIÓN+KARISMA&edu.requested
media=chat&customerInfo.is_deleted=0&edu.question=.+Identificación:+101584278
0+-
++Origen+>>+appMovil+Nombre+Persona+>>+FUNDACIÓN+KARISMA+Tipo+Persona+>>+Pers
ona+Juridica+Forma+Consulta+>>+Persona+Natural+Razón+Social/Nombre+>>+Análisi
s+App+Dian+Email+>>+Test@karisma.or.co+Direccion+>>+Call%c3%a9+59%2318+Telefo
no+de+Contacto+>>+738960+Departamento+>>+BOGOTÁ+D.C.+Ciudad+>>++BOGOTÁ+D.C.&c
ustomerInfo.location=Other&edu.username=guest_FUNDACIÓN+KARISMA_83946553&edu.
languagecode=es&email.from=dianchat@dian.gov.co&edu.tenantName=DianChat&langu
age=es&customerInfo.mangledName=guest_FUNDACIÓN+KARISMA_83946553&edu.username
_display=FUNDACIÓN+KARISMA&customerInfo.role=guest
```

[22] La aplicación se comunica con el subdominio dian.kubo.co

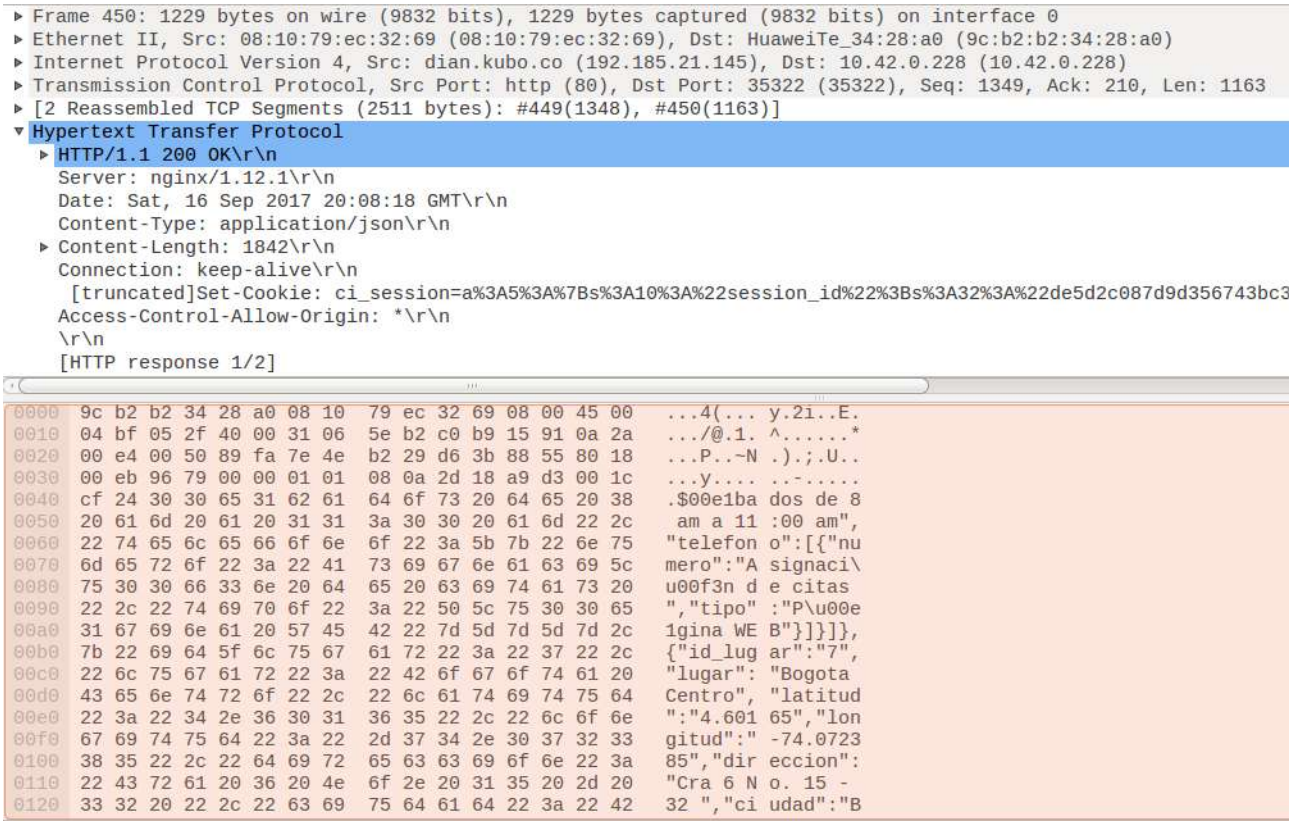
En nuestro experimento, la aplicación tuvo tres intercambios con el protocolo HTTP y otros con TCP, como se puede ver en estos extractos de captura WireShark :



En la primera, se puede observar el envío de los datos de localización con el protocolo HTTP y el método GET :

```
▸ Frame 443: 275 bytes on wire (2200 bits), 275 bytes captured (2200 bits) on interface 0
▸ Ethernet II, Src: HuaweiTe_34:28:a0 (9c:b2:b2:34:28:a0), Dst: 08:10:79:ec:32:69 (08:10:79:ec:32:69)
▸ Internet Protocol Version 4, Src: 10.42.0.228 (10.42.0.228), Dst: dian.kubo.co (192.185.21.145)
▸ Transmission Control Protocol, Src Port: 35322 (35322), Dst Port: http (80), Seq: 1, Ack: 1, Len: 209
▾ Hypertext Transfer Protocol
  ▸ GET /servicio/puntosCercanos/4.6305528/-74.0683867 HTTP/1.1\r\n
    User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0; ALE-L23 Build/HuaweiALE-L23)\r\n
    Host: dian.kubo.co\r\n
    Connection: Keep-Alive\r\n
    Accept-Encoding: gzip\r\n
    \r\n
    [Full request URI: http://dian.kubo.co/servicio/puntosCercanos/4.6305528/-74.0683867]
    [HTTP request 1/2]
    [Response in frame: 450]
    [Next request in frame: 454]
```

En la respuesta aparecen una lista de localizaciones, con longitud, latitud y dirección. Parecen corresponder a la lista de las oficinas de la DIAN más cerca.



Además se puede observar que el servidor web transmite se instala una cookie denominada “ci_session” que contiene un id de tracking, una dirección IP y un user agent.

```
▸ Frame 450: 1229 bytes on wire (9832 bits), 1229 bytes captured (9832 bits) on interface 0
▸ Ethernet II, Src: 08:10:79:ec:32:69 (08:10:79:ec:32:69), Dst: HuaweiTe_34:28:a0 (9c:b2:b2:34:28:a0)
▸ Internet Protocol Version 4, Src: dian.kubo.co (192.185.21.145), Dst: 10.42.0.228 (10.42.0.228)
▸ Transmission Control Protocol, Src Port: http (80), Dst Port: 35322 (35322), Seq: 1349, Ack: 210, Len: 1163
▸ [2 Reassembled TCP Segments (2511 bytes): #449(1348), #450(1163)]
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Server: nginx/1.12.1\r\n
    Date: Sat, 16 Sep 2017 20:08:18 GMT\r\n
    Content-Type: application/json\r\n
  ▸ Content-Length: 1842\r\n
    Connection: keep-alive\r\n
    [truncated]Set-Cookie: ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22de5d2c087d9d356743bc3
    Access-Control-Allow-Origin: *\r\n
    \r\n
    [HTTP response 1/2]
```

```
0090  65 70 2d 61 6c 69 76 65  0d 0a 53 65 74 2d 43 6f   ep-alive ..Set-Co
00a0  6f 6b 69 65 3a 20 63 69  5f 73 65 73 73 69 6f 6e   okie: ci _session
00b0  3d 61 25 33 41 35 25 33  41 25 37 42 73 25 33 41   =a%3A5%3 A%7Bs%3A
00c0  31 30 25 33 41 25 32 32  73 65 73 73 69 6f 6e 5f   10%3A%22 session_
00d0  69 64 25 32 32 25 33 42  73 25 33 41 33 32 25 33   id%22%3B s%3A32%3
00e0  41 25 32 32 64 65 35 64  32 63 30 38 37 64 39 64   A%22de5d 2c087d9d
00f0  33 35 36 37 34 33 62 63  33 30 66 66 36 37 65 35   356743bc 30ff67e5
0100  34 30 39 33 25 32 32 25  33 42 73 25 33 41 31 30   4093%22% 3Bs%3A10
0110  25 33 41 25 32 32 69 70  5f 61 64 64 72 65 73 73   %3A%22ip _address
0120  25 32 32 25 33 42 73 25  33 41 31 35 25 33 41 25   %22%3Bs% 3A15%3A%
0130  32 32 32 30 30 2e 31 31  38 2e 31 37 32 2e 32 32   22200.11 8.172.22
0140  34 25 32 32 25 33 42 73  25 33 41 31 30 25 33 41   4%22%3Bs %3A10%3A
0150  25 32 32 75 73 65 72 5f  61 67 65 6e 74 25 32 32   %22user_ agent%22
0160  25 33 42 73 25 33 41 36  35 25 33 41 25 32 32 44   %3Bs%3A6 5%3A%22D
0170  61 6c 76 69 6b 25 32 46  32 2e 31 2e 30 2b 25 32   alvik%2F 2.1.0+%2
0180  38 4c 69 6e 75 78 25 33  42 2b 55 25 33 42 2b 41   8Linux%3 B+U%3B+A
0190  6e 64 72 6f 69 64 2b 36  2e 30 25 33 42 2b 41 4c   ndroid+6 .0%3B+AL
01a0  45 2d 4c 32 33 2b 42 75  69 6c 64 25 32 46 48 75   E-L23+Bu ild%2FHu
01b0  61 77 65 69 41 4c 45 2d  4c 32 33 25 32 39 25 32   aweiALE- L23%29%2
```

<Análisis del sitio Internet **www.dian.gov.co** y de su **app>**

Versión pública
Noviembre 2018

<K+ LAB> | <KTRL+INFORME>

karisma.org.co
Twitter: **@Karisma**
Facebook: **@fundacionkarismaa**