PLATAFORMAS INSEGURAS, EL CASO DE IMEICOLOMBIA.COM.CO

Fundación Karisma

Autor:

Stéphane Labarthe

Coordinación editorial:

Nathaly Espitia Díaz

Septiembre de 2016

"En un esfuerzo para que todas las personas tengan acceso al conocimiento, Fundación Karisma está trabajando para que sus documentos sean accesible, es decir, tienen un formato electrónico diseñado para que su contenido pueda ser leído por el mayor número de personas posible, incluidas las que tienenalgun tipo de discapacidad o de dificultada para la lectura y comprensión. Más información sobre el tema: http://www.documentoaccesible.com/#que-es

Consulta este análisis en línea en:
https://karisma.org.co/descargar/plataformas-inseguras-el-caso-de-imeicolombia-com-co/

PLATAFORMAS INSEGURAS,

EL CASO DE IMEICOLOMBIA.COM.CO

Desde hace tiempo el gobierno colombiano, como otros en la región, ha tratado de controlar el problema del robo de celulares con una estrategia que pretende hacer inútil cualquier celular robado o perdido. La idea es que, si le roban el celular, usted pueda bloquearlo de tal forma que quien lo haya robado no pueda revenderlo y usar una nueva tarjeta SIM en dicho celular robado (claro, aún así puede venderse por piezas). Dado que el sistema involucra la creación de bases de datos de suscriptores móviles a nivel nacional y su intercambio, es importante plantearnos ¿cómo se hace?, ¿qué tan seguro es? y ¿cuánto cuidado han puesto en proteger los datos de quienes consultan la plataforma?

Aunque el sistema general contra el hurto de celulares es tan enredado que, por ahora, no hay espacio para explicarlo todo, decidimos empezar revisando el sitio imeicolombia.com.co, que es una parte de este sistema. Y, como ya se había anticipado en su relanzamiento, las conclusiones no son muy alentadoras.[1]

* Este artículo es el primero de una serie que Karisma inicia para acercar a las personas aspectos técnicos de Internet que les permita entender mejor cómo proteger su intimidad en línea y comprender la importancia de la seguridad digital. En esta nueva serie de Fundación Karisma el análisis se envía a las autoridades involucradas antes de la publicación para facilitar el mejoramiento de su gestión y, cuando corresponda, se incluye información que no forma parte de la versión pública.

EL SITIO
IMEICOLOMBIA.COM.CO

Imeicolombia.com.co es un sitio web desarrollado en el marco de la estrategia de gobierno contra el hurto de celulares para permitir a la ciudadanía consultar si el número de identificación de su equipo (International Mobile Station Equipment Identity, IMEI) tiene reporte de hurto y/o extravío, por tanto, aparece inscrito en un registro público —la base de datos negativa— donde están todos los IMEI declarados por las mismas personas como robados o perdidos. Este sitio permite verificar a quien adquiera un teléfono celular que el dispositivo no es producto de un robo. Si el número aparece en el registro, el dispositivo ha sido reportado.

Este sitio ha sido ampliamente promovido por el gobierno. Se ha recomendado en los sitios web de la Comisión de Regulación de Comunicaciones (CRC)[2], del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)[3] e incluso desde la Presidencia de la República[4] y la Policía Nacional[5]. El nuevo Código de Policía hace obligatoria la consulta de la base de datos negativa por parte de las personas usuarias de celulares cuando necesiten comprar, alquilar, usar, distribuir, almacenar o vender un equipo (Artículo 95), además de sancionar a quien no cumpla estas obligaciones.[6]

Aunque el robo de celulares es un tema sensible para el país, dejar desprotegidos los números IMEI que se ingresan en la plataforma para consulta es también preocupante. Por ejemplo, dado que, como veremos, la página no cuenta con seguridad suficiente, los números IMEI consultados que no aparezcan como reportados pueden ser capturados por personas inescrupulosas para ser duplicados y usados en equipos robados. En Colombia hay millones de equipos clonados sin que la persona legítimamente dueña lo sepa.[7] Si se establece que el equipo ha sido clonado, el riesgo de que sea bloqueado persiste aunque quien sea su dueño no sepa nada del asunto. Es como si por la ciudad rodara un carro robado que no nos pertenece, pero que muestra las mismas placas del nuestro. La información que provee imeicolombia.com.co o cualquier otro sitio futuro donde se pueda consultar la base de datos negativa de celulares debe ser protegida, pues, si bandas de ladrones tienen acceso al intercambio de datos que se hace allí, pueden apropiarse de la lista de IMEI legítimos para consulta y clonarlos.

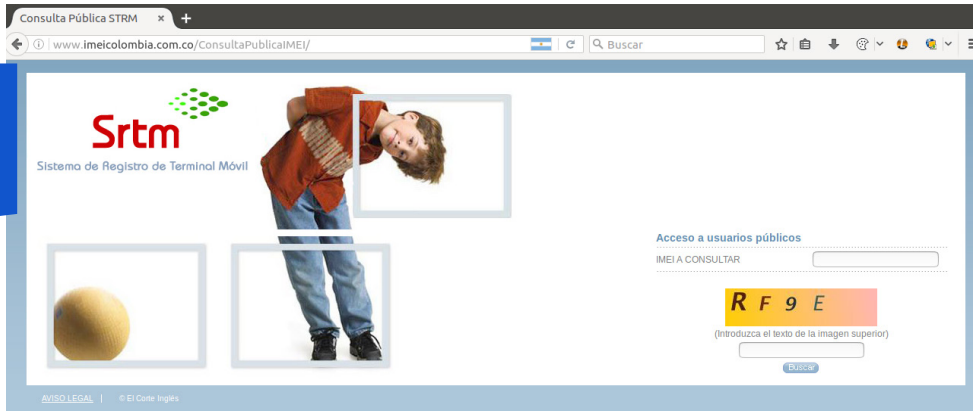
Una mirada superficial del sitio deja muchos interrogantes. Por ejemplo, no es claro quién es su responsable, ni se ofrece a quien lo visita las políticas de privacidad y seguridad de la información. **Pero fuimos más allá y decidimos hacer una investigación y un análisis técnico para mirar mejor los detalles del sitio.**

El análisis puso en evidencia que no solo hace falta información en el sitio web, sino que existen fallas de seguridad. Este documento busca presentar las fallas identificadas y ofrecer algunas recomendaciones con el objetivo de permitir mejorar la transparencia, seguridad y confianza en este proceso y plantear así temas que puedan ser considerados en iniciativas similares que se lleguen a implementar a futuro.

En el anexo se encontrarán los detalles y justificaciones técnicas del análisis. Los métodos y programas usados son todos *libres*[8], por lo cual la experiencia es reproducible e invitamos a cualquier persona a hacerlo. Los datos encontrados son todos públicos, además de que los métodos utilizados son pasivos y no intrusivos: solo se analizaron los flujos de entrada y salida desde nuestro computador (es decir, no hemos utilizado para este análisis ninguna metodología de *hackeo*[9]). Hemos documentado la experiencia paso a paso, pues consideramos importante que cualquier persona pueda cuidar de su propia seguridad digital, tomar este caso como un ejemplo y repetir el método de análisis con otros sitios donde comparte sus datos personales para indagar sobre su fiabilidad.

¿IMEICOLOMBIA.COM.CO ES UN SITIO CONFIABLE?

Al visitar el sitio web www.imeicolombia.com.co se entra a esta página:



Lo primero que llama la atención es que no hay ninguna identificación del Estado o alguna seña institucional que brinde confianza. Solo se encuentra la referencia *"Srtm – Sistema de Registro de Terminal Móvil"* que deja más interrogantes que aclaraciones. Abajo, en letra muy pequeña, se puede leer "©El Corte Inglés", lo que despista todavía más. ¿Qué tiene que ver El Corte Inglés —la tienda española por departamentos— con este sistema?

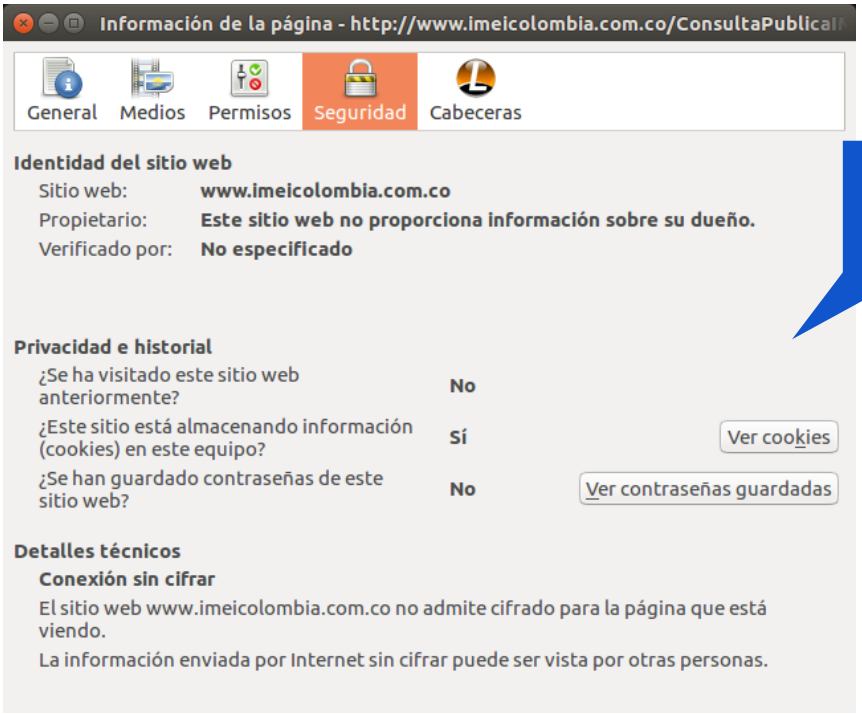
Una persona especialista con conocimientos sobre la regulación del sector podría deducir que probablemente la sucursal informática de El Corte Inglés está encargada por el Estado o los operadores de telecomunicaciones del país de gestionar este sitio web y, quizás, la base de datos correspondiente (lo que parece ser el caso). Pero, ¿cómo podría la persona común llegar a esta conclusión si no hay nada que lo diga expresamente?

La página cuenta con un "Aviso legal" que, sin embargo, no sirve para nada, pues al hacer clic sobre el enlace no aparece ninguna información, no se abre ventana alguna. Para entender por qué la ausencia de acción en este caso, revisamos el "código fuente" de la página[1]. El resultado es que no estamos ante una falla temporal de funcionamiento (por ejemplo, que la página enlazada esté caída), sino que en realidad el enlace está programado para que simplemente la página se desplace hacia arriba y no enlaza a ninguna parte.

Más allá del uso que en este caso concreto se le da al IMEI en el sitio que estamos analizando, hay que tener en cuenta su valor para identificar e individualizar a una persona, especialmente cuando está asociado con otros datos personales. Según un concepto no vinculante de la Delegatura de Protección de Datos referido por funcionarios del Ministerio de las TIC, el IMEI no es considerado un dato personal en Colombia. Al respecto, consideramos que en el contexto de la política de registro de celulares, precisamente, el sistema hace que el IMEI sea un dato que puede individualizar a las personas, por tanto, debe ser considerado un dato personal. A diferencia de la posición del gobierno –que en esto sigue la opinión de Singapur–, Fundación Karisma cree que esta base de datos gestiona datos personales –en consonancia con la situación en Europa y en sintonía con los estándares de la OCDE.

Mientras más información buscamos, más dudas aparecen. ¿Cómo estar seguros de que este sitio es legítimo, que no es un sitio falsificado, destinado, por ejemplo, al *phishing* de los IMEI?

Hicimos otra revisión. Consultamos la información que recibe el navegador web (en este caso utilizamos Firefox), haciendo clic en la "i" de información que aparece al inicio de la barra de dirección, justo antes del "www", y el mensaje que recibimos es "Conexión no segura". Esto está muy lejos de poder tranquilizarnos.



Al buscar más información en el navegador, aparece lo siguiente:

Esto significa que el sitio no admite un protocolo seguro y cifrado como HTTPS; es decir, no permite asegurar una autenticación del sitio (comprobar qué sitio se visita y a quién pertenece) ni ofrece confidencialidad de los datos enviados (este punto se analiza con más detalles a continuación).

Según funcionarios del Ministerio de las TIC, los lineamientos oficiales sobre Gobierno en Línea obligan a las entidades del Estado a implementar el protocolo HTTPS en sus sitios web. Sin embargo, este deber no se extiende explícitamente a terceros particulares en el cumplimiento de obligaciones contractuales con el Estado. A pesar de ello, creemos que se debe exigir al administrador de imeicolombia.com.co el uso HTTPS pues no ser entidad oficial no puede servir de excusa para no emplear medidas técnicas estándar de seguridad. Debe considerarse incluir estas obligaciones en los contratos que se firman con terceros para este tipo de gestiones.

En suma, hasta acá, quien llegue al sitio no tiene ninguna indicación seria sobre la legitimidad del mismo.

Aún nos queda una última posibilidad para obtener información sobre el sitio: el registro del dominio.

En internet, los dominios (en este caso, "imeicolombia.com.co") son registrados oficialmente ante registradores acreditados y, generalmente, se puede obtener cierta información sobre quién hace el registro. En Colombia, los sitios terminados en ".co" (que es al que pertenece el ".com.co") están bajo la responsabilidad del MinTIC, que delegó esta gestión a la empresa .CO Internet SAS, una entidad de carácter privado que, por contrato de concesión con el Estado colombiano, tiene la responsabilidad de administración del dominio.[10]

Para obtener información sobre el dominio "imei.colombia.com.co" se puede revisar el registro del ".co" en este enlace[11] o correr el comando Linux "whois imeicolombia.com.co"[2].

Se usaron los dos métodos y el resultado es muy interesante. Resulta que los registros para imeicolombia.com.co están protegidos. Es decir, que quien controla el sitio optó por usar un servicio de intermediación, en este caso, el de la empresa australiana PrivacyProtect.org, que oculta los datos reales del registro cuando se hace la consulta pública. Como se explica en el sitio de la empresa:

> *Cuando activa Privacy Protection en un nombre de dominio, nosotros reemplazamos todos los detalles de contacto públicos con información alternativa. Así, cuando se hace una consulta WHOIS, se muestran números de teléfono, direcciones físicas y electrónicas alternativas. USTED SIGUE SIENDO EL PROPIETARIO EL DOMINIO Y TIENE COMPLETO CONTROL SOBRE ÉL (Traducción nuestra).*[12]

Dicho de otra manera, quienes tienen el control sobre el dominio "imeicolombia.com.co" quieren proteger su privacidad. Aunque valoramos su intimidad, nos gustaría que también protegieran la nuestra. Indagar cómo se protegen nuestros datos en este sitio web es precisamente uno de los objetivos de este artículo. Hasta ahora, y a pesar de nuestra investigación, no sabemos mucho sobre imeicolombia.com.co y lo que conocemos no nos permite tener nada de confianza.

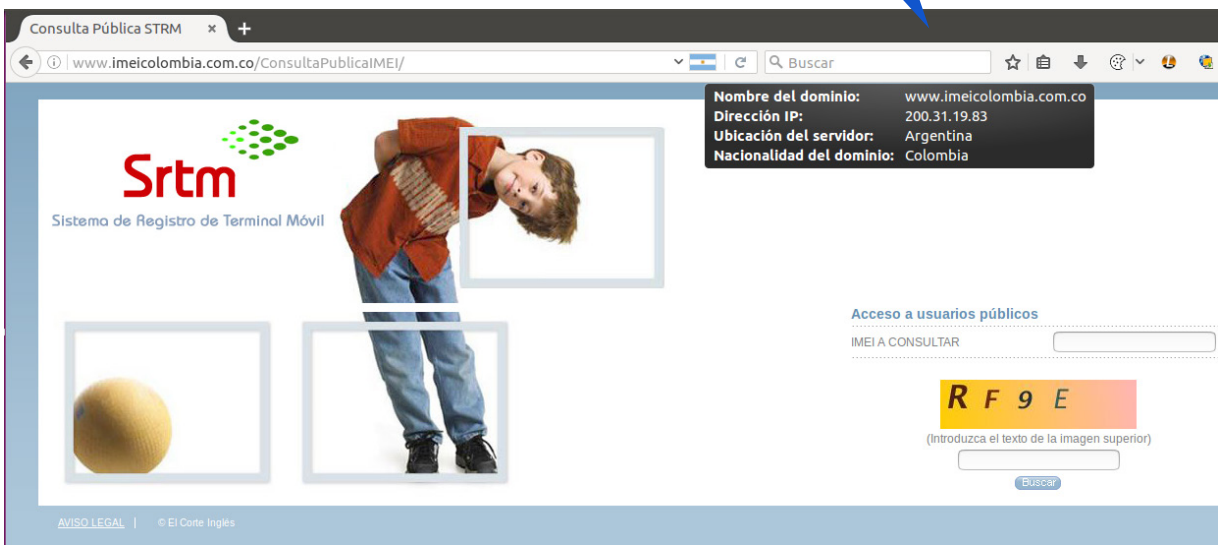
Hablando de confianza, vale la pena indicar que la extensión .com del dominio de este sitio web hace referencia a una actividad comercial. Como no parece que el propósito de este servicio sea comercial, la referencia es al menos inconveniente para generar tranquilidad en el público.

Lo siguiente que se puede hacer es un análisis técnico de los flujos que entran y salen de nuestro computador, para saber cómo y a dónde van nuestros datos cuando completamos el formulario.

¿DÓNDE ESTÁN MIS DATOS?

Para esta parte del análisis usamos varios complementos del navegador Firefox y un programa de análisis de flujo de datos. El primer complemento es la extensión FlagFox, que permite conocer la ubicación del servidor web que alberga el sitio web que visitamos, además de algunos detalles más.[13] Es sencilla de usar y muy práctica.

Para el sitio de imeicolombia.com.co, se observa el ícono de la bandera de Argentina, que supuestamente corresponde a la ubicación del servidor web de "imei.colombia.com.co" y suministra la dirección IP del servidor: 200.31.19.83.



Pero lo que realmente nos interesa es saber a dónde van nuestros datos, en este caso nuestro IMEI o número que identifica nuestro equipo, pues se trata de un dato sensible, que, como explicamos antes, si es duplicado en un terminal robado puede generarnos perjuicios. Para obtener esa información, hicimos una consulta de IMEI llenando el formulario del sitio con un número ficticio. El resultado es el siguiente:

El resultado es el siguiente:

Durante este experimento, simultáneamente analizamos los flujos de datos que salen y entran de nuestro navegador con la extensión Live HTTP Headers[14] y con el programa Wireshark[15].

El resultado nos muestra[3] que los datos del formulario son enviados a un servidor web con dirección IP que es la misma que nos presentó FlagFox, o sea, 200.31.19.83. Para saber hacia dónde van nuestros datos tenemos que determinar a quién pertenece esta dirección IP: ¿al **MinTIC, a la CRC, a los operadores, o a El Corte Inglés?**

La información sobre los flujos de datos que hemos analizado con la extensión y el programa mencionados se puede obtener también en ciertos sitios web que proveen servicios de WHOIS de IP, con la extensión FlagFox ya mencionada o mediante el comando *whois* ejecutado en un terminal Linux. En nuestro caso, usamos el tercer método[4]. El resultado nos muestra que esta IP pertenece a la empresa IMPSAT Colombia, con sede en Bogotá. Sin embargo, las coordenadas del servicio técnico que aparecen en la respuesta muestran una dirección en Argentina, que es el mismo país al que apunta FlagFox.

Entonces, todo parece indicar que el servidor web del sitio —y muy probablemente la base de datos correspondiente— está en un centro de datos de la empresa IMPSAT situado en Argentina. Es también lo que indica cuando consultamos la base *iptonation*[5], que provee correspondencia entre las IP de internet y

los países. Sin embargo, no puede saberse con certeza si la base de datos con los IMEI está en Argentina o Colombia porque la localización de un servidor web con su dirección IP no es completamente confiable, el servidor de base de datos no está obligatoriamente en el mismo datacenter, y además, IMPSAT tiene sucursales y centros de datos en ambos países.

En resumidas cuentas, esta parte de la investigación nos ha llevado a lo siguiente:

- La dirección IP del servidor web del sitio "imeicolombia.com.co", que es también la dirección IP a la que son enviados los IMEI, es la dirección 200.31.19.83.
- El servidor web del sitio "imeicolombia.com.co" está en un centro de datos de la empresa IMPSAT, lo que implica, *a priori*, un segundo nivel de tercerización. Es decir, parece que la gestión del servidor web "imeicolombia.com.co" —y muy probablemente de la base de datos correspondiente— está legalmente a cargo de El Corte Inglés, en su sucursal informática, que a su vez parece que confío su almacenamiento a la empresa IMPSAT.
- El servidor web del sitio "imeicolombia.com.co" esta situado en Argentina y/o en Colombia, en un centro de datos de la empresa IMPSAT, y el contacto técnico para la gestión de este servidor está basado en Argentina.

Quien lea este artículo se preguntará por qué insistimos tanto en la cuestión del país donde está ubicado el servidor web y probablemente la base de datos correspondiente, que incluye la base de datos negativa. (Generalmente, el servidor web y el servidor de base de datos suelen estar en el mismo centro de datos por razones logísticas, de arquitectura técnica y de tiempo de respuesta (y de todas formas los datos pasan por el servidor web). Aunque es discutible, muchas empresas consideran que la ley que se aplica a la gestión de datos personales es la del país donde está ubicada la base de datos. Por tanto, aunque estemos hablando de datos sujetos a la ley colombiana, si están albergados en Argentina, puede que haya dudas sobre qué ley aplicar.

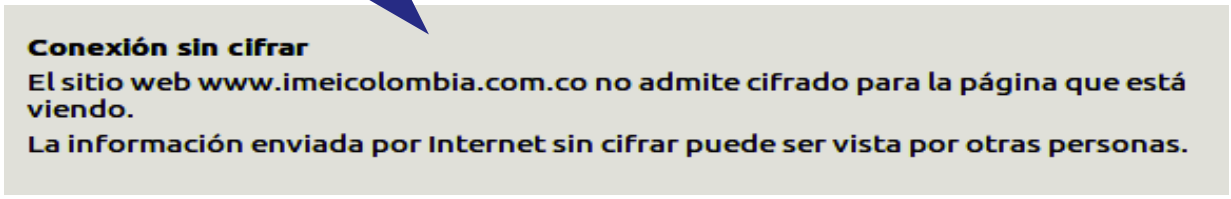
En todo caso, habría que preguntarse si es necesario hacer un análisis más profundo, pues, de acuerdo con la ley colombiana, las transferencias de datos a países que no proporcionen niveles adecuados de protección de datos están prohibidas, con algunas excepciones como la existencia de consentimiento expreso o datos médicos por razones de salud o datos bancarios.[16] Por eso es importante revisar el nivel de protección de datos que ofrece Argentina, particularmente si

el servicio está patrocinado por el Estado colombiano en una estrategia amplia sobre hurto de celulares. Esto resulta aún más relevante si consideramos que el nuevo Código de Policía, en su artículo 95, parágrafo 2, impone a las personas la obligación de consultar esta base de datos para evitar adquirir o alquilar teléfonos celulares; de no hacerlo, se prevén sanciones que incluye multa y destrucción del equipo.

De otra parte, si como ya dijimos El Corte Inglés está adelantando una tarea en nombre del gobierno colombiano, esperamos que tenga disposiciones contractuales que protejan los datos e impongan obligaciones en su administración. Si El Corte Inglés tiene contratos con otras entidades para cumplir su función, se requiere analizar las condiciones en que esas empresas lo hacen.

¿ES WWW.IMEICOLOMBIA.COM.CO UN SITIO SEGURO PARA LOS DATOS QUE TRANSMITIMOS A TRAVÉS DE ÉL?

Como vimos en la primera parte de este análisis, el navegador nos mostró la siguiente alerta de seguridad:



Esto significa que la primera página del sitio usa el protocolo HTTP, que no permite autenticación de la página ni el cifrado de los datos transmitidos.

Para comprobar si también los datos del formulario son enviados de forma insegura, buscamos en las capturas de flujo de datos de nuestro equipo. La (más global) de *Wireshark*[3] como la captura HTTP hecha con *Live HTTP Headers*[6] demuestran que los datos son enviados mediante el protocolo HTTP, que no es seguro.

Una revisión más detallada nos permite establecer que tiene otras características que la hacen vulnerable a ataques de baja complejidad. Esta información forma parte de la versión del artículo que se enviará a las autoridades, pero no la desplegamos acá para evitar ofrecer a posibles criminales la información exacta de tales vulnerabilidades.

LA JOYA DE LA CORONA:
EL ENIGMA DE LA HORA

En resumen, no solo la transferencia es insegura porque no usa el protocolo recomendado para seguridad HTTPS, sino que, además, el servidor es potencialmente vulnerable a ataques de baja complejidad.

Un índice débil para determinar la zona geográfica de un servidor puede ser la hora en que funciona, puesto que nos da la indicación del huso horario. En el caso que examinamos, el servidor mostró un horario de alrededor de las 3:46 con fecha el 15 de junio, que se puede observar, por ejemplo, en sus respuestas HTTP. Esto corresponde a 5 horas más del horario en que el análisis fue realizado.

Frente a esta situación hay dos posibilidades:

- El servidor está situado en Reikiavik, Nuakchott o Dakar[17], lo que sería muy sorprendente respecto a lo visto previamente, además de que plantearía otra serie de preguntas, o

- El servidor no está en la hora correcta, lo que demostraría una falta de rigor en su gestión y plantea también asuntos de seguridad digital. La más simple de todas es que cuando un servidor es atacado lo primero que se hace es mirar los registros o *logs*. Si estos archivos no están en la hora correcta, quien haga el análisis tendrá problemas para establecer la cronología del ataque y documentarlo.

A pesar de los numerosos puntos negativos ya mencionados, se puede establecer al menos un punto positivo del sitio: no encontramos rastros de terceros como empresas de publicidad, *analytics*, etc. Este detalle no es menor, pues significa que se están cuidando de no permitir —o mejor, buscan evitar— el rastreo o *tracking*, por ejemplo, a través de cookies externos. Con esto se estaría evitando el riesgo de transmisión de datos a estas empresas externas.

RECOMENDACIONES PARA LA GESTIÓN DE IMEICOLOMBIA.COM.CO

Con el fin de permitir mayor transparencia, seguridad y confianza a este proceso, presentamos las siguientes recomendaciones:

- Cambiar la presentación gráfica del sitio de modo que se ofrezca claridad sobre el hecho de que es un sitio gestionado por privados en el marco de una campaña de gobierno y en desarrollo de una obligación legal. La página de imeicolombia.com.co no tiene información sobre el responsable del sitio o la justificación del mismo. Sin embargo, si se consulta la normatividad sobre la política contra el hurto de celulares es posible establecer que la página resulta de una obligación legal que se impone a los operadores de telefonía celular y que pueden cumplir contratando a un tercero.
- Reconsiderar la posición oficial sobre la calificación del IMEI como un dato no personal teniendo en cuenta los datos que asocian las bases de datos positivas del sistema de registro de celulares.
- Ser transparente sobre el tipo de gestión de datos que se hace y describir la forma como se protegen. Para esto, es necesario desplegar más información en el sitio, en particular redactar y publicar los textos correspondientes a la parte de "Aviso Legal". Como mínimo, se debe explicar quién

es la entidad responsable del tratamiento, quién gestiona el sitio y quién almacena los datos, con indicación de los países correspondientes. De otra parte, deben desarrollarse las obligaciones legales de la Ley de Protección de Datos colombiana. Esto obligará, al menos, a evaluar si están cumpliendo con la misma.

- Si hay contratos de tercerización de nivel 1 y 2, es necesario asegurarse que cada uno contengan las cláusulas de confidencialidad necesarias.
- Reemplazar el protocolo HTTP, que no es seguro, por el protocolo HTTPS que permitirá una autenticación del sitio web y la confidencialidad de los datos transmitidos.
- Modificar el dominio para que la extensión no sea .com, que hace referencia a un sistema comercial.
- Configurar el servidor web a la hora correcta (*ntpdate*).

El servicio prestado por "imeicolombia.com.co" no es uno cualquiera. El compromiso que el gobierno tiene con la ciudadanía lo obliga a cuidar sus datos, sobre todo, considerando el papel que esta base de datos adquiere de acuerdo con el artículo 95, numeral 1, parágrafo 2 del nuevo Código de Policía.

Antes de publicar este informe se envió a algunas autoridades para solicitar retroalimentación, evidenciar el trabajo que hicimos y dar espacio para hacer correcciones antes de su publicación. Antes de publicar este informe Fundación Karisma sostuvo una reunión con funcionarios de Ministerio de las Tecnologías de la Información y las Comunicaciones (MINTIC) y de la Comisión de Regulación de Comunicaciones (CRC) en la que se explicó el análisis y se comentaron algunos temas presentados por nosotros como problemáticos en el informe. Después de esa reunión, el gobierno indicó que enviaría algunas explicaciones técnicas. A la fecha, no se han recibido estas explicaciones, sin embargo algunos puntos del informe se modificaron y las recomendaciones se ampliaron con base en el diálogo sostenido en esa reunión.

Fundación Karisma reconoce que el propósito de imeicolombia.com.co es positivo y legítimo pero sostiene que la forma como se implementa debe ser cuidadosa y responsable y que, especialmente, siendo parte de una política nacional los estándares de protección a los derechos de suscriptores debe ser cuidadosos (privacidad, libertad de expresión, de movimiento, de asociación, etcétera), sin importar si son adelantados por entes privados o no.

Esperamos que esta investigación sirva para mejorar ese proceso y continuaremos analizando los otros eslabones del sistema teniendo en cuenta que esta es la pieza pública, la que tiene el sitio web a disposición de las personas. Dado que el resto de la arquitectura no es pública, su análisis es más complejo.

NOTAS

[1] Análisis del enlace "Aviso legal"

Mediante un examen del código fuente (HTML y Javascript) de la página (para verlo: Ctrl + U con Firefox), se puede encontrar que es la línea siguiente la que maneja este enlace:

```
<a class="hpie" title="Aviso legal" href="#">AVISO LEGAL</a>
```

Esta línea muestra que el resultado de la acción de hacer clic en "Aviso legal" es solo subir la página hacia arriba (href="#"), lo que no produce nada en nuestro caso porque es una página pequeña. Nada muestra que haya un enlace hacia una página de información. Si lo tuviera, el código HTML sería algo similar a:

```
<a class="hpie" title="Aviso legal" href="InformacionLegal/">AVISO LEGAL</a>
```

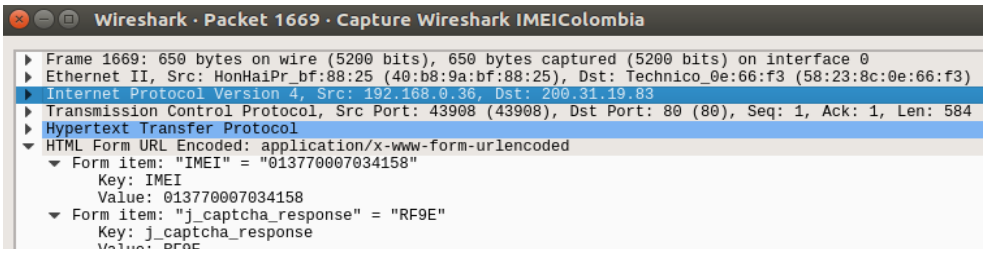
[2] Resultado de una consulta sobre el dominio "imeicolombia.com.co"

La primera parte del resultado del comando "whois imeicolombia.com.co" ejecutada en una terminal Linux, muestra la siguiente información:

Domain Name:	IMEICOLOMBIA.COM.CO
Domain ID:	D26156972-CO
Sponsoring Registrar:	CENTRAL COMERCIALIZADORA DE INTERNET S.A.S
Sponsoring Registrar IANA ID:	88888
Registrar URL (registration services):	http://mi.com.co/
Domain Status:	clientTransferProhibited
Registrant ID:	PP-SP-001
Registrant Name:	Domain Admin
Registrant Organization:	PrivacyProtect.org
Registrant Address1:	ID#10760, PO Box 16
Registrant Address2:	Note - All Postal Mails Rejected, visit Privacyprotect.org
Registrant City:	Nobby Beach
Registrant Postal Code:	QLD 4218
Registrant Country:	Australia
Registrant Country Code:	AU
Registrant Phone Number:	+45.36946676
Registrant Email:	contact@privacyprotect.org
Domain Registration Date:	Wed Dec 14 14:15:50 GMT 2011
Domain Expiration Date:	Tue Dec 13 23:59:59 GMT 2016
Domain Last Updated Date:	Thu Dec 29 09:11:00 GMT 2011

[3] Servidor destinatario del envío del número IMEI

Una búsqueda del IMEI consultado en el formulario (013770007034158), en la captura de flujo que hicimos con el programa WireShark, nos lleva a este extracto de *query* que resalta el envío del IMEI y del *captcha* hacia la dirección IP: 200.13.19.83:



[4] Propietario de la IP 200.13.19.83

La respuesta al comando "whois 200.13.19.83" nos permite obtener estos elementos:

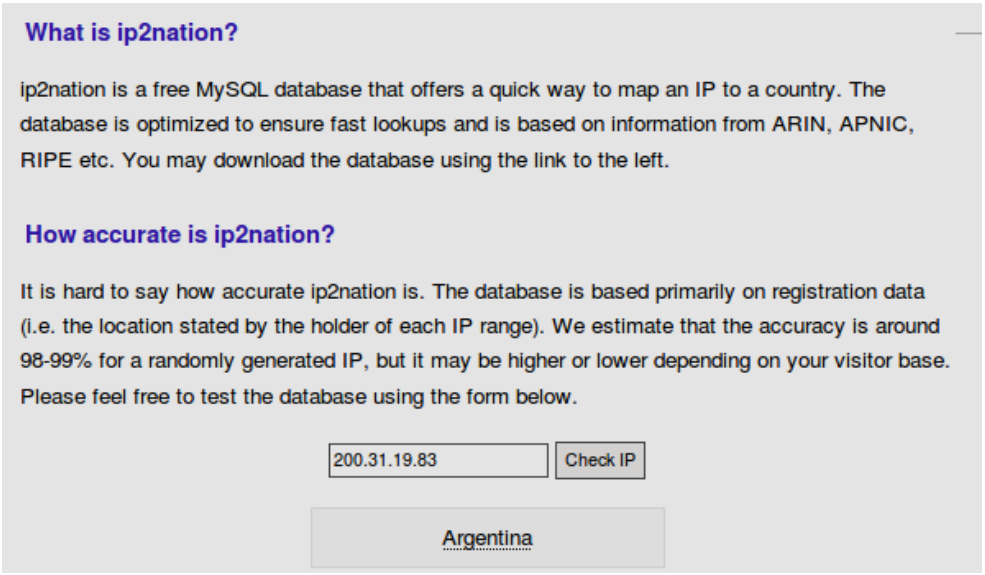
inetnum:	200.31.19.0/25
status:	reallocated
owner:	Impsat Colombia - Datacenter
ownerid:	CO-ICDA-LACNIC z
responsible:	Gloria Cuestas
address:	Diagonal 126, 67-19,
address:	- - Santa Fe de Bogota - DC
country:	CO
phone:	+57 1 6119000 []
owner-c:	IMC
tech-c:	NEA5
abuse-c:	NEA5
created:	20070615
changed:	20070615
inetnum-up:	200.31.16/21
inetnum-up:	200.31.0/19

nic-hdl:	MC
person:	Impsat Colombia
e-mail:	ip-col@GBLX.NET.AR
address:	Diagonal, 126, 67-19
address:	11001000 - Santa Fe de Bogota -
country:	CO
phone:	+57 1 433-5968 []
created:	20081020
changed:	20081020

nic-hdl: NEA5
person: Jorge Lam
e-mail: DL-NP&I-IP-Latam@LEVEL3.COM
address: Alferez Pareja, 256,
address: 1107 - Capital Federal - BA
country: AR
phone: +54 11 51706000 []
created: 20030710
changed: 20130423

Resalta que la empresa Impsat Colombia en Bogotá es la propietaria y que el contacto técnico está en Argentina.

[5] Respuesta a una interrogación de la base *iptonation*



[6] El envío del número IMEI se hace mediante el protocolo HTTP, que no cifra los datos en tránsito.

Esta parte de la captura HTTP, realizada con *Live HTTP Headers*, muestra que el número IMEI es enviado mediante el protocolo HTTP (método POST), que no cifra los datos en tránsito.

http://www.imeicolombia.com.co/ConsultaPublicaIMEI/Consulta

POST /ConsultaPublicaIMEI/Consulta HTTP/1.1
Host: www.imeicolombia.com.co
[...]
Content-Type: application/x-www-form-urlencoded
Content-Length: 45
IMEI=013770007034158&j_captcha_response=T1LQS

1. Castro, F. (2015, 27 de noviembre), Mintic predica pero no aplica. *Las 2 Orillas*. Disponible en http://www.las2orillas.co/mintic-predica-pero-no-aplica/.
2. Rebellón, C. (2012). *Acta de Informe de Gestión de la CRC*. Disponible en https://www.crcom.gov.co/uploads/images/files/2012_11_Informe_Gestion_Carlos_Rebellon.pdf.
3. MinTIC (2011, 11 de mayo). *Ya van 2.8 millones de celulares bloqueados por no estar registrados*. Disponible en http://www.mintic.gov.co/portal/604/w3-article-15241.html.
4. Presidencia de la República. (2015, 20 de agosto). *Nuevas medidas para el fortalecimiento de la lucha contra el hurto de celulares*. Disponible en http://wp.presidencia.gov.co/SitePages/DocumentsPDF/CelularesMedidasContraelRobo-HojadeDatos-VF_20150820.pdf.
5. Policía Nacional. (s.f.). ¿Qué es el número IMEI en mi celular?. Disponible en http://portal.policia.gov.co/es-co/Servicios/Celulares/Paginas/IMEI.aspx.
6. Ley No. 1801 de 2016, artículos 95. Disponible en http://es.presidencia.gov.co/normativa/normativa/LEY%201801%20DEL%2029%20DE%20JULIO%20DE%202016.pdf.
7. El análisis que refleja esta situación puede leerse en CRC. (2016). *Revisión de las condiciones y criterios para la identificación de equipos terminales móviles: etapa de control*. Disponible en https://crcom.gov.co/uploads/images/files/Doc_soporte_Etapa_Control_publicar_180516.pdf.

8. Cuando hablamos de programas libres nos referimos a aquellos que cumplen las 4 libertades del software, a saber: (1) uso, (2) estudio y modificación, (3) redistribución del original, y (4) redistribución de las modificaciones. La disponibilidad de dicho software facilita su utilización por cualquier persona, por tanto, permite la replicación de los análisis que se presentan en este reporte sin que exista una barrera adicional por la disponibilidad de las herramientas utilizadas.
9. *Hackear* es una expresión que identifica una ética que consiste en propiciar el acceso a la tecnología para empoderar a las personas. Luego se entendió como la actividad de encontrar vulnerabilidades en sistemas de información pero con la idea de reportarlas y repararlas. Finalmente, se empezó a usar en el sentido de buscar vulnerabilidades en sistemas de información y aprovecharlas en forma ilícita. Para Karisma, la expresión correcta cuando se *hackea* para hacer daño es la de *crackear* y, por tanto, decir *hackear* en ese sentido es incorrecto. Sin embargo, no es este el uso que se ha popularizado. Para facilitar la comprensión de este documento hemos decidido usar el término *hackear* en el sentido de *crackear*, aunque somos conscientes de que es solo uno de los sentidos de esa palabra.
10. Se puede indagar sobre este organismo en su propia sitio web, especialmente, en http://www.cointernet.com.co/responsabilidad-global/gobernanza.

11. La información descrita en el texto puede consultarse en http://www.whois.co/whois-gui/.
12. When you enable Privacy Protection on a domain name, we replace all your publicly visible contact details with alternate contact information so that when a WHOIS query is performed on the domain, an alternate mailing address, email address and phone number are displayed. YOU RETAIN FULL OWNERSHIP OF THE DOMAIN AND HAVE COMPLETE CONTROL OF IT. *Véase* la sección "Sobre Privacy Protect" en http://privacyprotect.org/about-privacyprotection/.
13. La información sobre FlagFox puede consultarse en el siguiente enlace: https://addons.mozilla.org/en-US/firefox/addon/flagfox/.
14. La información sobre *Live HTTP Headers* se puede consultar en el siguiente enlace: https://addons.mozilla.org/en-US/firefox/addon/live-http-headers/.
15. La información sobre el programa *Wireshark* se puede consultar en el siguiente enlace: https://www.wireshark.org.
16. Ley No. 1581 de 2012. Disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley/_1581/_2012.html#26.
17. Para consultar esta información se puede ingresar al siguiente enlace: http://24timezones.com/reloj_hora_exacta.php.