Hackers y Gorras 2

Resumen, análisis y perspectivas de las conversaciones informales con la comunidad de *infosec*

Por Beatriz Busaniche
Fundación Vía Libre[1]
www.vialibre.org.ar

Metodología

Este documento fue elaborado a partir de conversaciones informales sostenidas durante una reunión de trabajo realizada en diciembre de 2018 bajo la premisa de la charla informal sobre una agenda temática semi estructurada. La modalidad metodológica más aproximada es la del *focus group*, sin embargo, no se aplicó la técnica de forma sistemática.

Hallazgos de nuestra investigación con la comunidad de infosec

A lo largo de nuestro primer informe[2] sobre la relación de la comunidad de *infosec* con las leyes vigentes que afectan su actividad y los organismos que se ocupan de la aplicación de las mencionadas leyes, encontramos algunos lineamientos que nos permiten detectar áreas clave de trabajo a futuro para fortalecer las capacidades de la comunidad de practicantes y con ella, mejorar considerablemente las estrategias de seguridad informática en Argentina y la región.

Entendemos que el fortalecimiento de la comunidad en Argentina implica un fortalecimiento a nivel regional por la magnitud e influencia que la comunidad de *infosec* de nuestro país tiene en la región, especialmente por el impacto de diversas iniciativas locales que han cobrado suficiente visibilidad y magnitud como para ser la referencia indiscutida en la región. Un ejemplo de esto es la celebración anual de la reunión de *hackers* más grande de la región: Ekoparty, un evento al que concurren practicantes de todo el continente y donde se amplía la discusión sobre la práctica y la actualidad del campo de la seguridad informática.

Un hallazgo fundamental de nuestra investigación es que la comunidad de *infosec* considera que los legisladores tienen magros o nulos conocimientos sobre el campo que regulan cuando abordan temas que se vinculan con la seguridad informática y con la informática en general. A los ojos de la comunidad, los legisladores carecen también de buen asesoramiento en la materia.

En el marco de las conversaciones informales que mantuvimos con la comunidad, detectamos además que hay una mirada muy crítica sobre las políticas de ciberseguridad adoptadas por organismos públicos, e incluso una mirada sumamente desconfiada de la capacidad del Estado en la materia. Especialmente, la definición de ciberseguridad aparece como un campo controvertido ya que se incluye en ese término acciones tan diversas como un ataque de *fishing*, el tráfico de pornografía infantil o el *grooming* así como una amenaza a un funcionario público en cualquier red social.

Por otro lado, aparece con claridad el hecho de que no solo no hay un concepto operativo de trabajo apropiado y una planificación consecuente, sino que las acciones que se toman son puramente punitivas y absolutamente ineficaces para proteger a la ciudadanía y defender la infraestructura informática en Argentina ante un eventual ataque.

Un antecedente mencionado con regularidad en las reuniones de la comunidad tiene que ver con la adopción de regulaciones que poco y nada contribuyen a fortalecer a la comunidad de *infosec* en Argentina y que en algunos casos contribuyen al deterioro de sus condiciones de trabajo.

2 Véase Hackers y Gorras 1.

Por ejemplo, es citado con frecuencia el caso de la ley de delitos informáticos aprobada en Argentina en 2008, que modifica el código penal de la siguiente forma:

> Será reprimido con prisión de quince días a un año, … el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños. [3]

Desde el inicio del debate sobre esa reforma legal en 2006, en el que Fundación Vía Libre participó intensamente, venimos reiterando que la prohibición de circulación de software y cualquier otro sistema de este tipo por su capacidad de causar daños y la acción concreta de hacer el daño es contrario a la práctica de la seguridad, ya que las mismas herramientas que se usan para atacar un sistema son las apropiadas para defenderlo. Sin embargo, la capacidad de incidencia en la materia ha sido prácticamente nula.

Otro tema sobre el que se trabajó más recientemente tiene que ver con la adhesión por parte de Argentina al Convenio de Ciberseguridad de Budapest. Este convenio es apenas conocido por la comunidad de *infosec*, pese a que se trata de un documento relativamente antiguo para el campo al que Argentina adhirió con muy pocas reservas.

Otro de los temas que emerge entre las preocupaciones de la comunidad de *infosec* tiene que ver con las regulaciones de propiedad intelectual y las diversas iniciativas abiertas al debate que incluyen la ampliación de los tipos penales relacionados, especialmente los que tienen que ver con la ingeniería reversa y con la posibilidad de realizar investigación sobre sistemas con gestión digital de derechos o DRM por su sigla en inglés (Digital Rights Management).

Claramente, a la gran preocupación sobre la falta de un correcto asesoramiento de los legisladores se suma la tendencia a replicar modelos extranjeros con sus propias flaquezas y problemas. Por ejemplo, la tendencia a adoptar medidas vinculadas con la vigilancia en redes sociales, la incorporación de puertas traseras en determinados programas, entre otros tópicos aparecen en la conversación informal con la comunidad de *infosec*.

Sin lugar a dudas, una de las principales causales de preocupación es la incertidumbre a la hora del reporte de vulnerabilidades. Los antecedentes locales de persecuciones, imputaciones e incluso allanamientos al domicilio de miembros de la comunidad de *infosec* locales por haber reportado vulnerabilidades a empresas, desincentivan la práctica y generan un precedente serio en el país.[4]

A esto se suma otro aspecto crítico: que casi cualquier cosa es considerada cibercrimen o ciberdelito porque ocurre en internet. Por ejemplo, en los documentos de trabajo de la Organización de los Estados Americanos (OEA), que ha fijado los lineamientos sobre Ciberseguridad en toda la región, aparece una mezcla irrisoria de acciones tan dispares como el discurso de odio o una amenaza en redes sociales hasta el reporte de vulnerabilidades de infraestructura crítica. Si todo eso es metido en la misma bolsa y las políticas públicas no son claras al respecto, entonces la estrategia de ciberseguridad de un país está condenada al fracaso.

Otra coincidencia relevante de la comunidad es que a lo largo de los años, pese al prestigio que detenta, al nivel de los especialistas locales, a la capacidad de la comunidad local, nunca fue

3 Véase Ley de Delitos Infomáticos. Modificación del Art. 183 del Código Penal http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

4 El caso de Joaquín Sorianelo, acusado por supuestos delitos informáticos y allanado por haber reportado vulnerabilidades en su sistema a la firma MSA S.A., proveedora de los sistemas de voto electrónico en la Ciudad Autónoma de Buenos Aires es el más destacado y mencionado, más no el único.

convocada a realizar ningún aporte a la hora de regular sobre ciberseguridad en Argentina. A esto se suma la imagen distorsionada de una comunidad de *hackers* rica en experiencia y conocimientos pero que muchas veces es visualizada desde los medios de comunicación como una banda de delincuentes o, en el mejor de los casos, de un grupo de impresentables. La capacidad instalada de la comunidad de *infosec* no merece ese desdén bajo ninguna circunstancia.

Todos recuerdan y destacan como un hito fundamental el aporte de esta comunidad a la discusión sobre la reforma electoral para introducir voto electrónico en 2016 en Diputados y Senado de la Nación. Sin embargo, en ese caso, fue la propia comunidad la que se movilizó para incidir en ese debate por la importancia crucial del mismo. Además, muchos observaron ese debate como un antes y un después del potencial involucramiento de esta comunidad en temas de política pública que se vinculan con sus competencias.

Finalmente, es importante destacar la buena voluntad de la comunidad a la hora de involucrarse en la definición de políticas públicas para fortalecer la seguridad informática. Saben que sin la participación de la comunidad de práctica en la toma de decisiones estratégicas, poco se podrá hacer en un abordaje de la seguridad de la información como sistema.

Desconocen cuál puede ser el mecanismo, pero saben también que no se puede poner la mirada solo en los potenciales atacantes, sino que es menester establecer estrategias y políticas públicas que obliguen a las empresas y organizaciones que administran infraestructura crítica a tomar recaudos serios a la hora de proteger la información que detentan. Esto es especialmente claro a la hora de evaluar cuál es la responsabilidad de aquellos que manejan no solo información de los ciudadanos (como pueden ser los organismos públicos) sino de todos aquellos integrantes del sector privado que administran infraestructura crítica por concesión (como pueden ser los concesionarios de servicios públicos).

La ausencia de una política de seguridad de la información en estos sectores, la falta de respuesta apropiada a reportes de vulnerabilidades o la pérdida de datos e información de los ciudadanos no puede ser minimizada a la hora de distribuir responsabilidades sobre la seguridad de la información.

La agenda de ciberseguridad en la región

En la región, el principal organismo que trabaja en la agenda de Ciberseguridad es la Organización de los Estados Americanos (OEA), que desde hace varios años realiza recomendaciones a sus países miembros sobre estrategias de seguridad de la información.

Sin embargo, a la hora de revisar los reportes de la OEA encontramos que bajo la agenda de la Cyberseguridad se encuentran iniciativas tan diversas como la búsqueda de niños, niñas y adolescentes perdidos utilizando el error 404[5] hasta estudios y perfiles de cibercriminalidad.[6] Son numerosas las publicaciones de OEA para el período 2015-2018 y están disponibles en la sección Cyber del sitio web del organismo.[7]

El programa de Seguridad Cibernética de la OEA (tal como se autodenomina en el sitio web del organismo) trabaja desde comienzos de la década de los 2000 con el objetivo de prestar asistencia a

5 Véase https://www.sites.oas.org/cyber/Documents/2016%20-%20Presentacio%CC%81n%20No%20Encontrado-Daniel%20Monastersky.pdf (Visitado el 27 de diciembre de 2018)

6 Véase otro ejemplo en https://www.sites.oas.org/cyber/Documents/2016%20-%20Tendencias%20y%20oportunidades%20en%20ciberseguridad-Alberto%20Bohorquez.pdf

7 Véase https://www.sites.oas.org/cyber/EN/Pages/Documents.aspx

los países miembros para fortalecer su capacidad técnica y sus políticas de seguridad informática para garantizar un "ciberespacio seguro y resiliente".[8]

Entre sus objetivos se incluye la incorporación de múltiples actores involucrados, incluyendo la sociedad civil y los usuarios finales de las tecnologías como parte clave de los procesos de ciberseguridad. Hasta donde logramos indagar, esta incorporación no solo no ha ocurrido, sino que no se han considerado prácticamente los aportes de la comunidad de *infosec*.

Tras muchos años de iniciada esta agenda, lo cierto es que la sociedad civil, los usuarios finales y la comunidad de *infosec* están ausentes de los debates que han redundado, al menos en una primera aproximación, en meras modificaciones legislativas de corte punitivista, en la creación de nuevos tipos penales y en muchos casos en la incorporación de aspectos que poco tienen que ver con lo que podríamos entender como ciberseguridad, como por ejemplo, el *bullying*, el acoso en línea, las amenazas y el *grooming*.

Argentina y la ciberseguridad. Un asunto pendiente

Hasta finales de 2015, el organismo líder a cargo de la denominada "ciberseguridad" en Argentina era el Programa Nacional de Infraestructuras Críticas y de Información y Ciberseguridad (ICIC) bajo la órbita de la Oficina Nacional de Tecnología de la Información (ONTI) dependiente de la Jefatura de Gabinete de Ministros. Dentro de este ámbito se creó el primer CERT (Equipo de respuesta a emergencias informáticas) a nivel nacional en 1994 y en 2011 se designó como parte de la ONTI. A partir del cambio de gobierno y con la gestión del Presidente Mauricio Macri, todas estas funciones pasaron a la órbita del Ministerio de Modernización que fue posteriormente disuelto y reconvertido en Secretaría de Gobierno de Modernización bajo la órbita de la Jefatura de Gabinete.[9]

En relación a delitos informáticos, el área de investigación de los mismos está a cargo de la División de Delitos Tecnológicos de la Policía Federal Argentina.

Un factor importante a destacar es que ni las empresas del sector privado ni las oficinas públicas están obligadas por ley a proporcionar información vinculada a incidentes sufridos en relación a la seguridad de su información a las autoridades nacionales. En la sección Argentina del informe regional por países de OEA, las autoridades indicaron que, si bien la ley de 2008 ha permitido tipificar ciertas prácticas como delitos, los obstáculos principales que enfrentan tienen que ver con la naturaleza de muchos de ellos que no tienen fronteras y están en "constante evolución", posición ciertamente discutible toda vez que los delitos son conductas no deseadas en una sociedad y su definición no debería estar atada al uso de una determinada tecnología que puede evolucionar o sofisticarse. Sin más, una estafa es una estafa, ya sea cometida en una esquina de la ciudad como a través de un correo electrónico. Esta explicación del gobierno argentino habla más de la baja calidad legislativa que de la problemática en sí misma de los delitos tipificados.

A su vez, el reporte de OEA detalla iniciativas gubernamentales para crear conciencia respecto de los desafíos de la seguridad cibernética así como la creación de una iniciativa llamada "Internet sano" destinado a promover el uso responsable de TICs e internet. Otro programa mencionado tiene que ver con la iniciativa "Con vos en la web", una campaña de protección de datos para niños, niñas

8 Tal como consta en el perfil de la iniciativa, véase https://www.sites.oas.org/cyber/es/paginas/contacts.aspx

9 Véase https://www.argentina.gob.ar/modernizacion/infraestructuras-criticas-de-informacion-y-ciberseguridad (Visitado el 27 de diciembre de 2018)

y adolescentes diseñada por la ahora disuelta y reestructurada Dirección Nacional de Protección de Datos Personales.

En el reporte de OEA se indica, además, que no hay un registro detallado ni cifras disponibles de incidentes y delitos informáticos u otras actividades informáticas maliciosas, sin embargo destacan un supuesto incremento de "suplantación de identidad", fraudes por medio de redes sociales, correo electrónico o banca en línea mediante el uso de ingeniería social o *keyloggers*. Es elocuente que bajo la figura de la ciberseguridad se mezclan demasiadas cuestiones de muy diverso tipo, variedad e impacto. El gobierno reconoce como limitantes e impedimentos: "La falta constante de concientización entre las partes interesadas en todos los niveles, problemas y cuestiones relacionados con la privacidad, y financiación insuficiente."[10] Vale mencionar que las cuestiones vinculadas con la privacidad jamás deberían ser consideradas una limitante a la investigación de delitos sino parte del sistema de derechos y garantías constitucionales que el Estado y los organismos públicos tienen obligación de respetar y proteger.

Desde aquel entonces y en el marco de la nueva gestión a cargo del Poder Ejecutivo Nacional desde diciembre de 2015, la estrategia de ciberseguridad no ha cambiado.

Sin embargo, siempre se mencionan los "ciberdelitos" en proyectos legislativos como las modificaciones a la ley de inteligencia, en la adhesión a la Convención de Budapest y en el diseño de las diversas regulaciones vinculadas con la cartera de seguridad y en el marco de la investigación de delitos complejos.

A la fecha, la estrategia de "ciberseguridad" en Argentina no ha evolucionado y adolece de los mismos problemas históricos que la caracterizaron a lo largo de las últimas décadas: no se piensa la seguridad como sistema; no se realiza una tarea clara que distinga cuestiones menores como puede ser un mensaje amenazante o sospechoso en una red social de un potencial sistema de seguridad de infraestructuras críticas; no se obliga a las empresas a mantener políticas claras de seguridad ni se les exigen reportes de incidentes; no se promueve la búsqueda y reporte de vulnerabilidades como una buena práctica ni se trabaja de manera fluida con la rica y sólida comunidad de práctica de *infosec* en el país.

¿Por qué es necesario desarrollar una agenda de *infosec* y Derechos Humanos en articulación con la comunidad local?

Los puntos de intersección entre la comunidad de *infosec*, las políticas de ciberseguridad y los Derechos Humanos son muchos y no siempre son explorados de manera apropiada. En este breve informe queremos destacar algunos ejes clave en esas intersecciones.

Derechos Electorales

En el marco de los derechos civiles y políticos, los derechos al voto secreto, íntegro, igual, auditable y transparente forman parte de los principios fundamentales que las Constituciones de cualquier

10 Véase https://www.sites.oas.org/cyber/Documents/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf pag. 35 y 36 (Visitado el 27 de diciembre de 2018)

país democrático deben asegurar. Desde finales de la década del 90 del siglo pasado, las iniciativas de “modernización” de los sistemas electorales han llevado a los diversos países a incursionar en experiencias de voto electrónico e informatización de diversas áreas de los procesos electorales. Desde aquel primer utopismo acrítico, que dio sustento a numerosas iniciativas legislativas de adopción de tecnologías electorales, al presente de críticas y retrocesos de esos procesos, han pasado numerosas experiencias en las cuales la comunidad de *infosec* ha sido y es protagonista.

En Argentina, la comunidad de *infosec* ha sido clave para llamar la atención pública sobre las vulnerabilidades y problemas asociados a la incorporación de computadoras en la intermediación entre el ciudadano votante y la expresión de su voluntad política. Tanto en la experiencia de la Ciudad Autónoma de Buenos Aires en 2015, en la cual la comunidad tuvo virtualmente su bautismo político -que concluyó con allanamientos y amenazas de toda índole a varios integrantes de la comunidad-, hasta la participación activa en el debate parlamentario en el Congreso Nacional en 2016, con la consecuente suspensión de la reforma electoral que el poder ejecutivo impulsaba para las elecciones nacionales de 2017. Fue la academia, la Sociedad Civil y la comunidad de *infosec* local la responsable principal de haber detectado y difundido vulnerabilidades graves que hubieran puesto en serio riesgo los derechos electorales de la ciudadanía argentina.

Derecho a la integridad y la seguridad pública

Contrariamente a la imagen negativa que se ha construido de la figura del *hacker*, nada más alejado de la realidad de la comunidad de *infosec* en Argentina y la región. La integridad de infraestructuras críticas es un tema de preocupación constante para la comunidad y la posibilidad de contribuir en esas áreas es fundamental.

Mientras no haya una delimitación clara de los alcances del problema y se siga pensando que la ciberseguridad es una mezcla de temas de muy diversa índole como el *grooming*, los insultos en redes sociales o el *hacktivismo* en línea, en lugar de pensar que las amenazas a la ciberseguridad deben considerar seriamente una estrategia de protección de las infraestructuras críticas como los servicios públicos, las oficinas de gobierno que administran datos sensibles de la ciudadanía, poco se podrá hacer para proteger la integridad de la información y la seguridad pública.

Derecho a la intimidad de las personas

La incorporación de cada vez más dispositivos de la denominada internet de las cosas (IoT, por sus siglas en inglés) a la vida cotidiana supone riesgos a la seguridad y la privacidad de las personas en el ámbito doméstico. Sin una comunidad de seguridad sólida y capaz de reportar vulnerabilidades, cada vez más empresas integrarán sus aplicaciones a nuestros teléfonos y tendrán puertas abiertas a nuestros domicilios desde las cuales obtendrán datos personales, conversaciones, hábitos de vida, juegos, etc.

Una vigorosa comunidad de *infosec* puede contribuir a reportar estos problemas y elevar la vara de las exigencias a estas empresas que venden electrodomésticos y otro tipo de dispositivos sin recaudos suficientes o con vulnerabilidades múltiples.

A su vez, es indispensable contar con una mirada crítica sobre las diversas aplicaciones que los gobiernos proponen en la interacción con la ciudadanía para controlar el uso y potencial abuso de los datos personales.

Los ciudadanos tenemos derecho a saber cómo funcionan y cuáles son los datos obtenidos en cada una de nuestras interacciones con las aplicaciones de la gestión pública de todo nivel, por lo que deben ser auditables y pasibles de investigación por parte de la comunidad. En este caso, es clave también una política abierta y transparente de incentivo al reporte de vulnerabilidades.

Derecho de acceso a la información

Cuando una oficina pública o una empresa de servicios públicos tiene un problema de seguridad y un incidente serio de pérdida de control sobre los datos, es fundamental exigir la publicación de la misma e informar de manera apropiada a las personas que puedan verse afectadas por este tipo de incidentes. Se debe promover el acceso a la información de este tipo de situaciones a fin de que la ciudadanía pueda tomar los recaudos del caso. Se debe exigir a las oficinas públicas a cargo de datos personales de la ciudadanía que informen de manera apropiada todo incidente de seguridad y las medidas de mitigación adoptadas. Se debe promover además una política de reporte de vulnerabilidades apropiada.

Libertad de Expresión y *hacktivismo*

Finalmente, pero no menos importante, la comunidad informática tiene larga trayectoria en activismo de todo tipo y este campo debe ser respetado y protegido con todas las garantías de la libertad de expresión y el derecho a la protesta social. No se debe confundir una actividad de *hacktivismo* con un delito informático. Acciones tales como la intervención de un sitio web con un mensaje político o de protesta deben ser analizadas dentro del derecho fundamental a la expresión y la protesta social y no confundir las acciones políticas de una comunidad con las acciones de delincuentes informáticos.

Asimismo, en aras de proteger el derecho a la libertad de expresión y el *hacktivismo*, se debe reivindicar y proteger especialmente el derecho al anonimato en la red, al uso de seudónimos y al reporte anónimo de vulnerabilidades para proteger a la comunidad de práctica de la seguridad de sistemas de información y su rol clave en una sociedad cada vez más mediada por dispositivos digitales.

Tampoco deben ser incorporadas en el campo punitivo acciones menores que bien pueden dirimirse en otras esferas: el discurso de odio, el insulto y otras expresiones que pueden bordear los límites de la libertad de expresión pero que deben ser tratados de forma apropiada y no necesariamente represivas. Se debe tender a una reducción y no un incremento de los denominados delitos de expresión.

Además, es fundamental que nunca una publicación de una vulnerabilidad detectada configure un delito si se han seguido los pasos apropiados y las buenas prácticas para la protección de la seguridad pública y los derechos fundamentales, especialmente cuando la publicación de tal información está protegida por el interés público.[11]
Acciones futuras

11 El ejemplo paradigmático es la difusión de las notorias vulnerabilidades del sistema de votación electrónica de la firma MSA S.A. utilizado en la Ciudad Autónoma de Buenos Aires en julio de 2015 en la elección para Jefe de Gobierno y legisladores de la Ciudad. Tras una ardua investigación judicial que incluyó el allanamiento del domicilio de una de las personas que reportaron las vulnerabilidades, la justicia dictamino que reportar la vulnerabilidad no era delito y que la seguridad del sistema electoral era vaga. Véase el caso de Joaquín Sorianello, entrevistado en el marco de esta investigación.

Fruto de esta investigación desarrollada por Fundación Vía Libre en cooperación con un sector importante de la comunidad de *infosec* de Argentina se pueden delinear algunas acciones a seguir para el año 2019 en adelante.

- Conformar un comité de trabajo permanente entre la comunidad de *infosec* y la Fundación Vía Libre para mantener el hilo de trabajo abierto en esta investigación, revisar estado del arte en materia legislativa y diseñar estrategias de incidencia pública.
- Promover el diálogo permanente con asesores de tomadores de decisiones, incluyendo legisladores de nivel nacional así como funcionarios de las áreas vinculadas para potenciar las posibilidades de establecer una agenda común de trabajo.
- Diseñar y poner en marcha un sistema de reporte de vulnerabilidades que permita proteger a los investigadores de *infosec* y cumplir con la responsabilidad pública de informar sobre incidentes reales y potenciales que puedan afectar a la ciudadanía.
- Crear conciencia sobre la necesidad de fomentar y no combatir la tarea de la comunidad de seguridad informática promoviendo una mirada realista de su rol y actividades, diferenciando y descartando los mitos del *hacker malo* instalados en la prensa y en el imaginario colectivo.
- Incidir positivamente en la agenda de ciberseguridad para proteger los Derechos Humanos.

Reconocimientos

Este trabajo no hubiera sido posible sin las contribuciones de un gran número de individuos y organizaciones. Debemos agradecer a los organizadores y al personal de la Ekoparty, y en particular a Federico Kirschbaum, Francisco Amato y Paola Mastrángelo; los expertos en seguridad de la información que nos brindaron su tiempo y paciencia para discutir esta investigación, incluidos Iván Arce, Javier Blanco, Fabián Cuchietti, Martín Doyhenard, María José Erquiaga, Johanna Caterina Faliero, Roberto Fresca, Sebastián García, Alfredo Ortega, Alfredo Rezinovsky, Juliano Rizzo, Javier Smaldone, Alberto Soliño, Joaquín Sorianello, Nicolás Waisman y otros que prefirieron permanecer en el anonimato; Alexia Halvorsen, que realizó el trabajo de campo en Ekoparty; Alejo Di Risio y Matías Blanco a cargo de la captura y edición de los materiales audiovisuales y AccessNow, por su generoso apoyo a este trabajo.

Equipo de trabajo de Fundación Vía Libre a cargo de este proyecto

Beatriz Busaniche - Dirección General de Proyecto

Carolina Martinez Elebi – Logística, coordinación, reportes.

Enrique A. Chaparro – Asesoramiento en Infosec – Diseño y análisis de los datos

Alexia Halvorsen – Asistente en el campo – Aplicación y seguimiento de encuestas

Alejo Di Risio y Matías Blanco – Producción Audiovisual

Elena Maule – Administración