

Hackers y Gorras 1

Percepciones de la comunidad de seguridad informática sobre la ley y su aplicación en Argentina.

Enrique A. Chaparro

Asistencia, logística y trabajo de campo por

Beatriz Busaniche

&

Carolina Martínez-Elebi

Versión original en Inglés.

Traducción al Español por Beatriz Busaniche



Fundación
Vía Libre

Hackers & Gorras 1

Percepción de la comunidad de seguridad informática sobre la ley y su aplicación en Argentina.

Enrique A. Chaparro

Asistencia, logística y trabajo de campo
Beatriz Busaniche &
Carolina Martínez Elebi
Traducción al español
Beatriz Busaniche

Fundación Vía Libre
Buenos Aires, 2018



Copyright © 2018 Enrique A. Chaparro & Fundación Vía Libre.
This text can be freely reproduced and distributed under the
Terms and Conditions of the *Creative Commons Attribution -
NoDerivatives 4.0 International* licence. As partial exception to
the *NoDerivatives* clause, bona fide translations are expressly
allowed.

Esta investigación

El objetivo de este estudio es llevar adelante un análisis cuantitativo de las percepciones de la comunidad de seguridad informática sobre ciertos aspectos de la ley y la observancia de la misma directamente relacionadas con la disciplina. En este marco, preferimos el término “Seguridad de la información” (*Infosec* en breve) porque tiene un significado más abarcativo que el de “seguridad informática” y además porque parece ser el término preferido por la comunidad involucrada.

Por largo tiempo han existido fricciones entre sectores de la comunidad de *infosec* y las agencias de observancia de la ley. Los legisladores, a menudo bajo la presión de la opinión pública, tienden a establecer regulaciones para prevenir o minimizar “*ciberamenazas*” reales o imaginarias. A su vez, la comunidad encuentra que buena parte de esas regulaciones son rara vez útiles para nada más que imponer obstáculos a lo largo de investigaciones completamente legítimas. El estereotipo de *hacker* que aparece a menudo en los medios de comunicación, cubierto con un buzo con capucha y tecleando en la oscuridad, ha hecho un verdadero daño.¹

¿Cómo ven los practicantes de la *infosec* su interacción con la ley penal y las leyes de propiedad intelectual? ¿Cuán conflictiva es la relación? ¿Cuánto saben sobre los aspectos de la ley que afectan su trabajo? ¿Qué áreas de la actividad están más afectadas por las eventuales regulaciones inadecuadas?

1 Por otra parte, el autor principal de este documento ha trabajado por más de treinta años en el área de *infosec* y no recuerda a nadie trabajando detrás de una computadora usando tal atuendo absurdo.

¿Qué piensan los *hackers*² de los legisladores y tomadores de decisiones de políticas públicas? Todas estas preguntas merecen una respuesta, pero hasta donde sabemos, nunca se había hecho en Argentina un estudio sistemático de las percepciones de la comunidad de *infosec* sobre aspectos legales.

Argentina tiene una comunidad de *infosec* vibrante y es el hogar de un buen número de expertos y empresas de seguridad con altos niveles de reconocimiento.³

Es, entonces, un campo excelente para medir las percepciones de la comunidad frente a la ley y las agencias de observancia de la ley.

Ekoparty, la conferencia más grande de seguridad informática en América latina y del mundo hispanohablante, provee un terreno fértil para la realización de nuestro trabajo de campo: por el número de asistentes, por la especificidad de sus intereses, nos ofrece una muestra excelente de la comunidad de *infosec* en toda su diversidad.

La edición 2018 tuvo lugar en la Ciudad Autónoma de Buenos Aires entre el 26 y el 28 de Septiembre. El número de asistentes alcanzó las 1933 personas. Alrededor de 1500 cuestionarios fueron distribuidos aleatoriamente entre los asistentes, de los cuales recibimos 257 respuestas para esta investigación.⁴

Demografía

La primera parte del cuestionario contiene preguntas destinadas a establecer un perfil demográfico de la muestra:

-
- 2 El mismo término *hacker* es controversial. Originalmente define a una persona que disfruta explorando los detalles de un sistema programable y buscando la forma de ampliar sus capacidades (véase e.g. G. Malkin & T. LaQuey Parker. *Internet Users' Glossary*. RFC 1392, January 1993, page 20; and G. Malkin. id-, RFC 1983, August 1996, page 22.) El uso peyorativo del término en los medios de comunicación ha causado que el público en general comience a usarlo con un significado diferente.
 - 3 Véase e.g. Penroth, Nicole. "Famed for Tango and Hackers". *The New York Times*, 1 December 2015, page B1.
 - 4 Desde ese número, 256 fueron procesadas y una desechada por razones técnicas. El hecho de que el número efectivo de respuestas utilizadas en nuestro trabajo fuera 2⁸, o 0xFF, es pura coincidencia.

- **Grupos etéreos:** Se pidió a los encuestados que indicaran su segmento de edad marcando uno de los cinco grupos desiguales: <18, 19 → 25, 26 → 35, 36 → 45 y > 45. El resultado muestra una distribución gaussiana típica centrada en el grupo medio: 10, 62, 112, 62, 10.
- **Género:** es un hecho bien conocido que existe una profunda brecha de género en las ocupaciones generalmente relacionadas con la computación⁵, y esa brecha se profundiza en el campo de la *infosec*. Nuestra encuesta refleja esas desigualdades. De las 254 personas que respondieron la pregunta sobre género, 218 (85.4% de la muestra) se identificaron como masculinos. Treinta y tres encuestadas se identificaron como femeninas, lo que representa un 13.0% de la muestra. Esa cifra es consistente con, y ligeramente más alta que los promedios globales y más alta que el promedio latinoamericano mostrado por otras encuestas de mujeres en *infosec*.⁶ Cuatro encuestados (1.6%) establecieron su género como otro/no-binario.⁷[3]
- **Relación con *infosec*:** la comunidad de *infosec* está muy lejos del estereotipo de un grupo de genios desarrapados e impresentables en un sótano. Gente de los más diversos perfiles trabaja en seguridad informática o tiene un interés académico en el campo. Y ese grupo se ve incrementado por personas que, aunque no tengan dedicación a tiempo completo a la *infosec*, tienen un interés profundo y práctico en el campo. Todos estos perfiles, de acuerdo con la información suministrada por los encuestados en las respuestas a Q4 definen lo que de aquí en más daremos en

5 Catherine Ashcraft, Brad McLain, and Elizabeth Eger. *Women in Tech: The Facts — 2016 Update*. Boulder, CO : National Center for Women & Information Technology, 2017.

6 Jason Reed, Yiru Zhong, Lynn Terwoerds, and Joyce Brocaglia. *The 2017 Global Information Security Workforce Study: Women in Cybersecurity*. White paper. Santa Clara, CA : Frost & Sullivan, 2017.

7 El estudio de la distribución de género en el campo de la *infosec* está más allá de los objetivos de esta investigación. Sin embargo, es interesante observar que tres cuartas partes de los encuestados autoidentificados como otro género no binario pertenecen al subconjunto "núcleo" o "core".

llamar la comunidad “amplia” o “extendida”. Definimos además otros dos subconjuntos:

- El subconjunto "núcleo" (Core), compuesto por todos los individuos en la muestra que tienen el trabajo en *infosec* como fuente principal de ingresos ($n = 110$) más los individuos del campo académico cuyas respuestas mostraron participación práctica en temas *infosec*⁸ ($n=16$); y
- El subconjunto "periférico", compuesto por todos los individuos restantes en la muestra ($n = 130$). Cinco encuestados que no respondieron Q4 fueron incluidos en este grupo.

Observaciones metodológicas

La encuesta se realizó utilizando cuestionarios anónimos. Las preguntas eran auto-explicativas, pero se brindó asistencia para resolver dudas en el stand de Fundación Vía Libre en Ekoparty. Proporcionar información demográfica no era obligatorio, pero fue enfáticamente alentado desde nuestro equipo de Vía Libre. Ninguna persona encuestada se negó a entregar esa información.

Noventa y seis encuestados (37.5% de la muestra) aceptaron nuestra invitación a informar un correo electrónico de contacto por si hacían falta comunicaciones futuras por alguna eventual aclaración.

Después de traducir los valores textuales en variables numéricas y procesarlos, se realizaron pruebas estadísticas regulares para una muestra de este tamaño con un nivel de confianza esperado del 90%.

A menos que se indique lo contrario en el texto, la muestra de la comunidad amplia o extendida es estadísticamente relevante: con un nivel de confianza del 90%, los márgenes de error son generalmente mejores que el 5,4% (podrían ser bastante mejores para proporciones de población sesgadas, como en el caso de la Q14).

⁸ Por ejemplo, por respuestas no negativas a Q8 y 11.

Los resultados

Conocimiento sobre la ley aplicable

Se pidió a los encuestados que realizaran una autoevaluación de su conocimiento sobre los aspectos que vinculan la *infosec* con el marco de la regulación penal [Q5] y de propiedad intelectual [Q6] en una escala de cinco puntos que van desde "nada" hasta "en detalle". Las respuestas válidas fueron 255 para la pregunta sobre derecho penal y 251 para la propiedad intelectual.

La tabla 1 a continuación muestra la fracción de los encuestados para cada clase y el gráfico 1 los números absolutos con respecto al conocimiento autoevaluado de la ley penal. La mediana de las respuestas fue 2 (poco conocimiento) y el modo 3 (algo de conocimiento).

	Comunidad Amplia	Núcleo	Periférica
Nada	25.9	7.1	44.2
Poco	29.8	30.2	29.5
Algo	30.6	36.5	24.8
Mucho	10.2	19.8	0.8
En detalle	3.5	6.3	0,8

Tabla 1: Conocimiento del código penal (porcentajes)

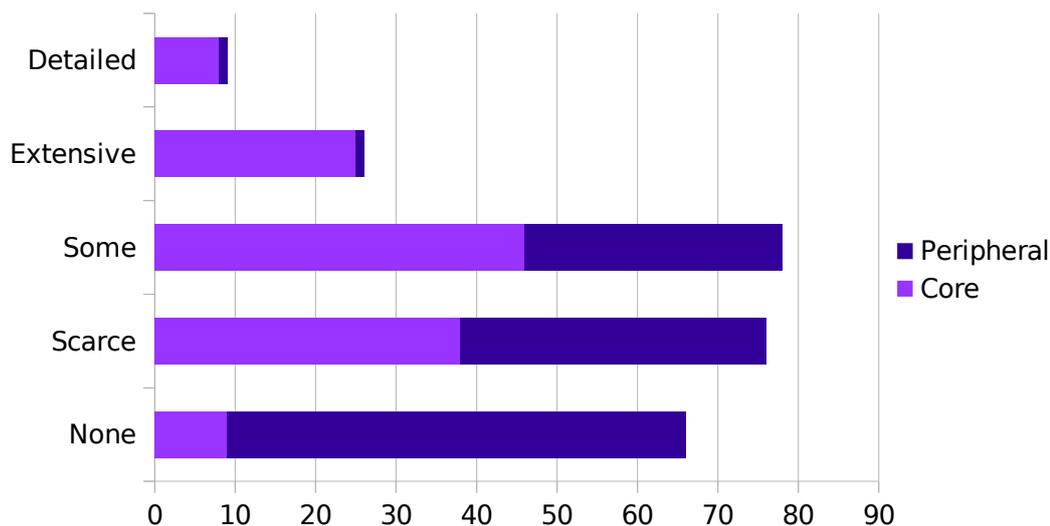


Gráfico 1: Conocimiento del Código Penal (número de encuestados)

En términos generales, más del 55% de los miembros de la comunidad "amplia" reconocen un conocimiento muy limitado de los aspectos del derecho penal relacionados con la seguridad de la información. Aquellos que evalúan sus conocimientos como extensos o detallados son menos de una séptima parte de la muestra. El nivel de familiaridad con el derecho penal aparece más alto en el grupo "núcleo", donde el subconjunto más grande pertenece a la categoría "algo" y el segundo más grande a la categoría "poco", mientras que las categorías de "nada" y "poco", en ese orden, son las más pobladas para el subconjunto "periférico". Sin embargo, las cifras obtenidas deben ser, en cualquier caso, un motivo de preocupación.

Se realizó una prueba de validación simple en [Q15]. Les pedimos a los encuestados que respondieran una pregunta sobre el marco legal que, en nuestra opinión, debería ser respondida correctamente por cualquier profesional *infosec* con "algo" o un nivel más alto de conocimiento:

¿La siguiente afirmación es verdadera o falsa?: "Enviar a alguien una muestra de malware para estudio puede constituir un delito bajo determinadas legislaciones o acuerdos internacionales".

Basado en las autoevaluaciones de [Q5], es esperable un nivel de respuestas correctas en torno al 44 por ciento (para el conjunto completo), el 62 por ciento (para el subconjunto "núcleo") y el 26 por ciento (para el subconjunto "periférico"). El supuesto se mostró correcto para el conjunto mayor: el 45.9 por ciento de los 246 encuestados dio la respuesta correcta. Las respuestas correctas fueron algo menos de lo esperado para el subconjunto "núcleo" con un 55,3 por ciento, mientras que el subconjunto "periférico" obtuvo mejores resultados de lo previsto, con un 36,6 por ciento. Podría plantearse entonces que el nivel de conocimiento dentro del subconjunto "núcleo" puede ser más bajo de lo que sugieren los valores autoevaluados. Esta inferencia también está respaldada por otros cruces de datos: se debe esperar que un encuestado con "extenso" o mejor conocimiento del derecho penal también tenga una "idea aproximada" o mejor sobre el Arreglo de Wassenaar⁹ [Q13b] debido a los delitos penales vinculados con la violación de los controles de exportación. Sin embargo, mientras 35 encuestados entran en la primera clase, solo 10 coinciden en ambas condiciones.

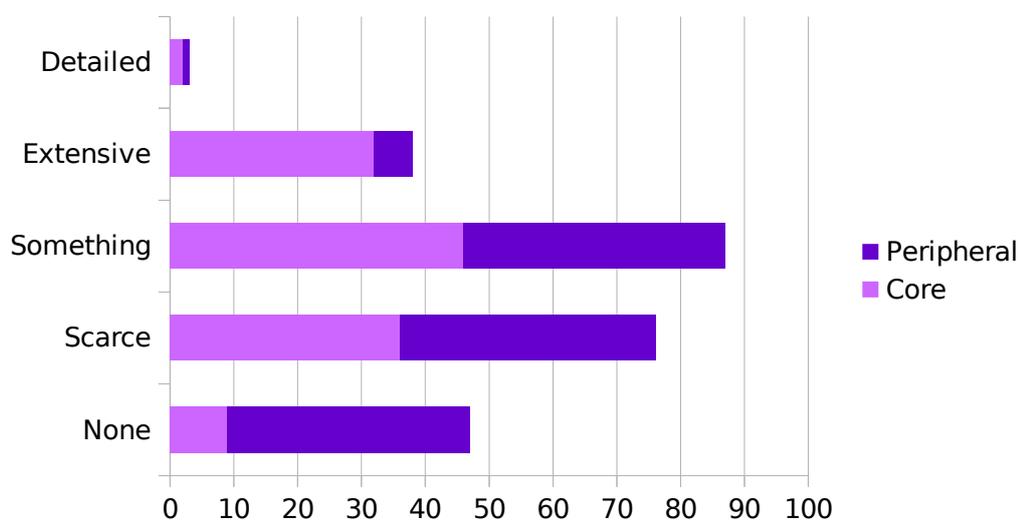
La Tabla 2 a continuación muestra la fracción de los encuestados para cada clase, y en el cuadro 2, los números absolutos con respecto al conocimiento autoevaluado de la ley de propiedad intelectual. La mediana de las respuestas fue de 2.5 (a medio camino entre "poco" y "algo") y el modo 3 (algo de conocimiento).

9 El Acuerdo de Wassenaar sobre controles de exportación para armas convencionales y bienes y tecnologías de doble uso es un régimen multilateral de control de exportaciones con 42 estados participantes, aplicable a las transferencias de armas convencionales y bienes y tecnologías de doble uso, establecido el 12 de julio de 1996 en Wassenaar, Países Bajos. Las enmiendas de diciembre de 2013 fueron ampliamente criticadas por los investigadores de seguridad, ya que se consideró que la inclusión de una serie de herramientas infosec en las listas de "doble uso" limitaba la capacidad de identificar y corregir vulnerabilidades de seguridad.

	Comunidad Amplia	Núcleo	Periférica
Nada	18,7	7,2	30,2
Poco	30,3	28,8	31,7
Algo	34,7	36,8	32,5
Mucho	15,1	25,6	4,8
En detalle	1,2	1,6	0,8

Tabla 2: Conocimiento de la Ley de Propiedad Intelectual (porcentajes)

La ley de propiedad intelectual incluye, pero no se limita a, la ley de protección de derechos de autor, patentes, marcas registradas y diseños de circuitos integrados (también conocida como "trabajo de máscara"). Los encuestados evaluaron su conocimiento de ese marco legal un poco más alto que el mismo para el derecho penal, pero aún así sigue siendo todavía bajo. Casi la mitad del conjunto completo reportó un conocimiento muy limitado (36 por ciento del subconjunto "núcleo", 61.9 por ciento del subconjunto "periférico"). Los resultados parecen contraintuitivos, ya que el derecho de propiedad intelectual es mucho más amplio y complejo.



Cuadro 2: Conocimiento de la Ley de Propiedad Intelectual (número de encuestados)

La ley como un obstáculo

Se preguntó a los encuestados si su trabajo de seguridad informática había sido afectado alguna vez por la ley penal o las regulaciones de propiedad intelectual. [Q7]. Las respuestas válidas fueron sí, no y no sé, y se recibieron 252 respuestas. La Tabla 3 muestra los números de las respuestas y sus porcentajes.

	Comunidad Amplia	Núcleo	Periférica
Si	41 (16.3)	30 (24.0)	11 (8.7)
No	169 (67.1)	76 (60.8)	93 (73.2)
No Sé	42 (16.7)	19 (15.2)	23 (18.1)

Tabla 3: Afectados por las leyes penales o de propiedad intelectual (número absoluto y porcentaje - Los porcentajes pueden no dar 100% debido al redondeo)

Incluso si "afectado" no significa necesariamente que los demandados o sus empleadores fueran imputados o procesados, un asunto que se planteó específicamente en otro lugar (véase las referencias a [Q8] a continuación), el número de respuestas afirmativas es muy importante. Si las cifras para el grupo núcleo se extrapolan para excluir las respuestas que no se conocen, encontramos que el trabajo del 28.3 por ciento de los profesionales que tienen la *infosec* como principal fuente de ingresos u otra forma de participación importante en la disciplina se ha visto afectada al menos una vez por cuestiones legales. Eso corresponde a dos de cada siete encuestados en el subconjunto.¹⁰

Como era de esperar, el subconjunto "periférico" ha experimentado menos fricción con el sistema legal, un hecho que se explica por las características definidas para ese subconjunto como se detalla en la sección Demografía más arriba.

La siguiente pregunta, [Q8] estaba más enfocada. Se preguntó a los encuestados si ellos o sus empleadores alguna vez habían

¹⁰ Tenga en cuenta, sin embargo, que debido a las limitaciones en el tamaño de la muestra de este subconjunto, existe un margen de error (razonable) de $\pm 5\%$ a un nivel de confianza del 90%.

sido objeto de acciones legales debido a las actividades de *infosec*. Las respuestas posibles fueron las mismas que en la pregunta anterior y se recibieron 255 respuestas. La tabla 4 muestra el número de respuestas y sus porcentajes.

	Comunidad Amplia	Núcleo	Periférica
Si	26 (10.2)	21 (16.7)	5 (3.9)
No	157 (69.4)	81 (64.3)	96 (74.4)
No sé	52 (20.4)	24 (19.0)	28 (21.7)

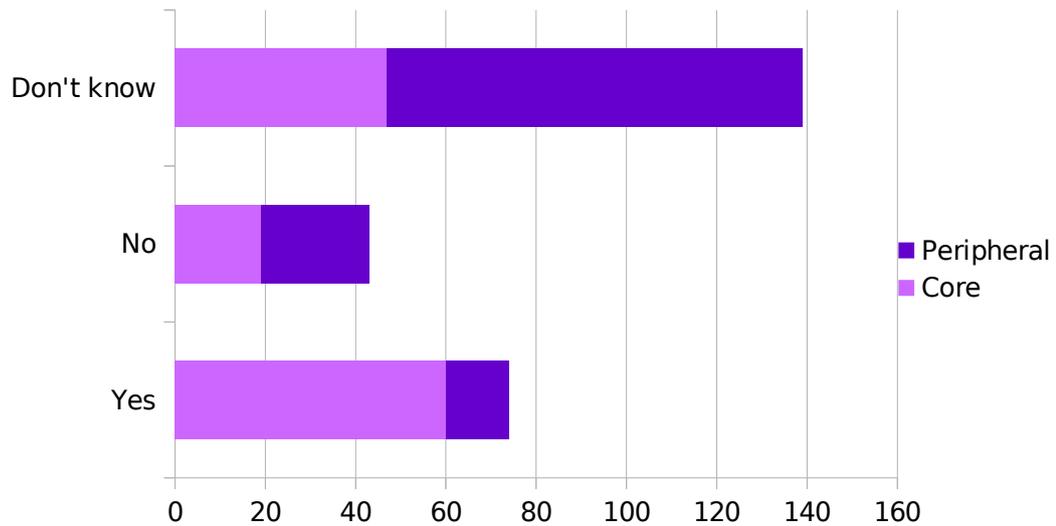
Tabla 4: Objeto de las acciones legales (números absolutos y porcentajes - los porcentajes pueden no sumar 100 debido al redondeo)

Nuevamente, como se esperaba, el porcentaje de personas afectadas por acciones legales en el subconjunto "periférico" es muy bajo, pero no despreciable. Aparece un indicador fuerte en el subconjunto "principal": poco más de dos tercios de las personas cuyo trabajo se vio afectado al menos una vez debido a la aplicación de alguna ley penal o de propiedad intelectual fueron imputadas o procesadas (véase la nota al pie número 9). Este dato puede indicar una falta de recursos adecuados, procedimientos o conocimientos suficientes como para prevenir este tipo de escalada.

Se solicitó a los encuestados su opinión sobre la siguiente pregunta [Q9]: ¿Considera que la ley actual es perjudicial para las actividades legítimas de *infosec*? Las posibles respuestas fueron sí, no y no sé, y se recibieron 256 respuestas. La Tabla 5 más abajo muestra la fracción de encuestados para cada tipo y el cuadro 5 los números absolutos.

	Comunidad Amplia	Núcleo	Periférica
Si	28,9	47,6	10,8
No	16,8	15,1	18,5
No sé	54,3	37,3	70,8

Tabla 5: Ley vigente en detrimento de actividades legítimas (porcentajes).



Cuadro 5: Ley vigente en detrimento de actividades legítimas (Números absolutos).

Las cifras para “no sé” correlacionan de manera razonable en todos los casos con la suma de aquellos ubicados en los dos niveles más bajos de conocimiento de la ley en la sección sobre conocimiento de la ley aplicable más arriba. Existe una diferencia notable entre las percepciones de los subconjuntos “núcleo” y “periférico”.

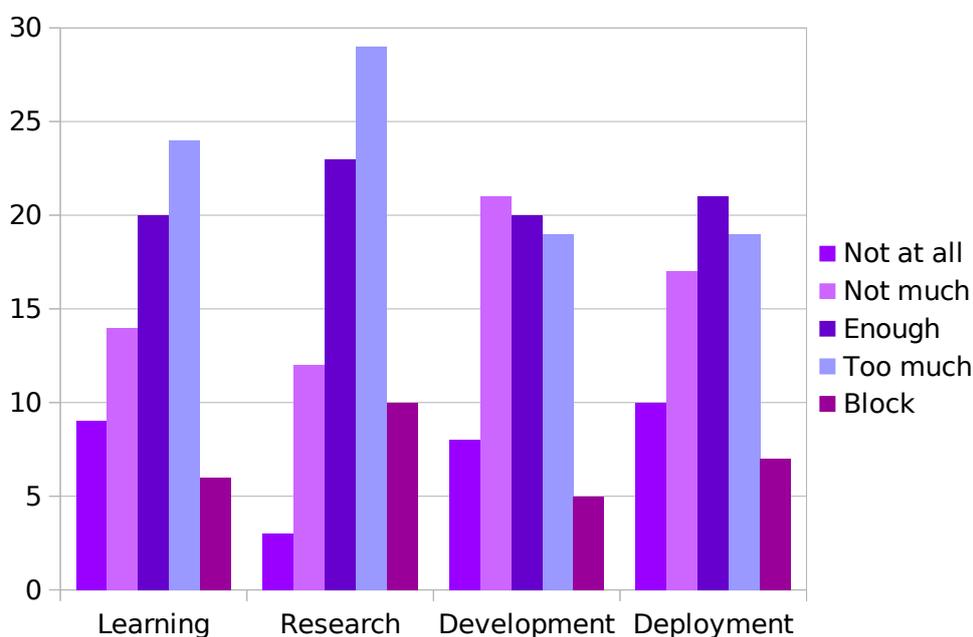
Los miembros de la primera consideran que la ley actual es un obstáculo para el desarrollo de actividades *infosec* legítimas: cuando las cifras se extrapolan para eliminar las respuestas indecisas, tres cuartas partes del grupo están de acuerdo con la respuesta de “sí”. La amplia mayoría del segundo subconjunto no pudo dar una respuesta decisiva y casi dos tercios del resto creen que la ley actual no representa una amenaza significativa para las actividades legítimas de *infosec*.

A los encuestados que respondieron afirmativamente a la pregunta anterior se les pidió que clasificaran [Q10a a Q10d] el nivel de daño creado por leyes inadecuadas en varias áreas de actividad utilizando una escala de cinco puntos que va desde “nada” hasta “las impide”. Las preguntas 10a y 10c fueron respondidas por 73 personas, mientras que el conjunto completo de 74 respondió las preguntas 10b y 10d. *Las áreas fueron*

Aprendizaje, Investigación, Desarrollo de productos de infosec y Despliegue de medidas de seguridad. Dado que muy pocos encuestados del subconjunto "periférico" respondieron que sí en la Q9, la tabla 6 y el cuadro 6 a continuación muestran los porcentajes y las cantidades para el conjunto completo ("amplio").

	Aprendizaje	Investigación	Desarrollo	Despliegue
Nada	12,3	3,9	11	13,5
Un poco	19,2	15,6	28,8	23
Bastante	27,4	29,9	27,4	28,4
Mucho	32,9	37,7	26	25,7
Las impide	8,2	13	6,8	9,5

Tabla 6: Actividades afectadas por el marco legal vigente (porcentajes).



Cuadro 6: Actividades afectadas por el marco legal vigente (número de encuestados)

La investigación aparece como el esfuerzo más afectado: más del 50 por ciento de los encuestados cree que el marco legal actual obstaculiza o bloquea seriamente las actividades en esta

categoría. Además, el número de participantes que consideran que esta categoría no está afectada es notablemente el más bajo entre todas las áreas: menos del 4 por ciento. Los encuestados también muestran niveles significativos de preocupación por los obstáculos planteados por la regulación en las áreas de Aprendizaje, Desarrollo de productos e Implementación, todos clasificados aproximadamente en escalas similares.

Asesoramiento legal

Se preguntó a los encuestados si ellos o sus empleadores habían recurrido a contratar asesoría legal por cuestiones de derecho penal o de propiedad intelectual [Q11]. Las respuestas válidas fueron sí, no y no sé y se recibieron 245 respuestas. La Tabla 7 muestra el número de respuestas y sus porcentajes para cada categoría.

	Comunidad Amplia	Núcleo	Periférica
Si	65 (26.5 %)	50 (40.0)	15 (12.5)
No	132 (53.9 %)	54 (43.2)	78 (62.5)
No Sé	48 (19.6 %)	21 (16.8)	27 (25.0)

Tabla 7: Asesoría legal contratada (números absolutos y porcentaje).

La comparación de estas respuestas con las de la pregunta 7 (ver tabla 3) puede mostrar que una serie de profesionales y empresas de seguridad de la información mantienen de manera preventiva un asesoramiento legal para reducir los riesgos asociados a las potenciales infracciones de la normativa. Si las cifras se ajustan para descartar respuestas indecisas, la proporción de practicantes que pertenecen al subconjunto "núcleo" o cuyos empleadores hayan contratado abogados es aproximadamente igual a la fracción que no lo hace.

A los participantes que respondieron afirmativamente a la pregunta 11 se les pidió información adicional sobre las

intervenciones de los asesores legales [Q12a a 12d].

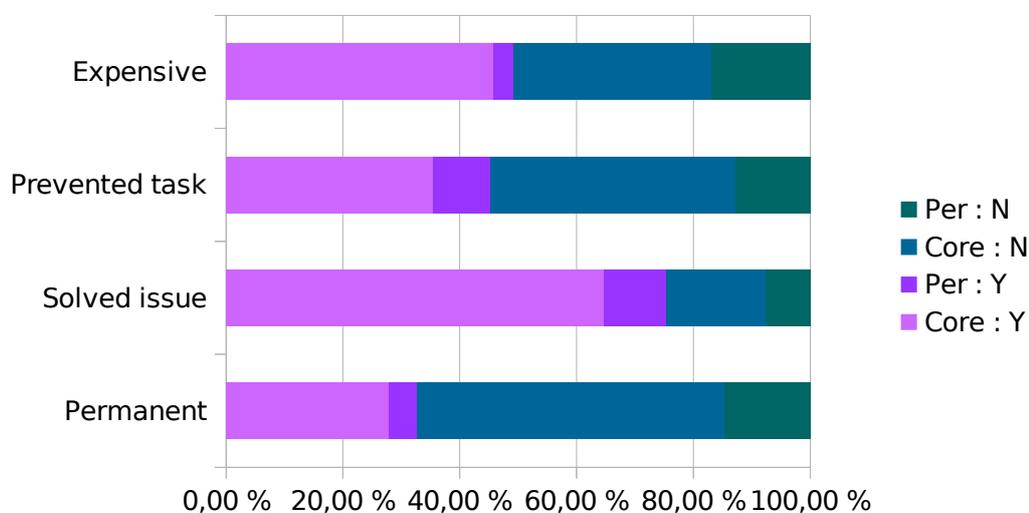
Específicamente,

- a) Si el abogado es contratado de manera permanente o caso por caso. Las respuestas válidas fueron permanentes, puntual y no sé, y se recibieron 88 respuestas.
- b) Si el abogado fue útil para resolver el problema (s). Las respuestas válidas fueron sí, no y no sé y se recibieron 100 respuestas.
- c) Si la ejecución de una tarea programada se volvió imposible como consecuencia de la intervención del abogado. Las respuestas válidas fueron las mismas que en b) arriba y se recibieron 98 respuestas.
- d) Si la asesoría legal implicaba un costo significativo para los encuestados (o sus empleadores). Las respuestas válidas fueron las mismas que en b) arriba y se recibieron 97 respuestas.

Más de dos tercios de las respuestas fueron proporcionadas por los encuestados en el subconjunto "núcleo": 70 por ciento para la pregunta 12a, 67 por ciento para 12b, c y d. Además, la mayoría de las respuestas del subconjunto "periférico" eran indecisas. La tabla 8 muestra el número de respuestas para cada pregunta y categoría. El cuadro 7 muestra los porcentajes para cada categoría y respuesta, una vez que se ajusta eliminando las respuestas indecisas.

	Comunidad Amplia	Núcleo	Periférica
12a. Base asesoría contratada			
Permanente	20	17	3
Puntual	41	32	9
No Sé	27	13	14
12b. El abogado fue útil para resolver el problema			
Si	49	42	7
No	16	11	5
No sé	35	14	21
12c. Tareas impedidas de realizar			
Si	28	22	6
No	34	26	8
No sé	36	18	18
12d. Implicó costo significativo			
Si	29	27	2
No	30	20	10
No sé	38	20	18

Tabla 8: Detalles sobre asesoría legal (número de respuestas)



Cuadro 7: Detalles del asesor legal, ajustado (porcentajes).

Así, las respuestas ajustadas señalan que:

- a) El asesoramiento legal se contrata preferentemente caso por caso y por un asunto puntual ($67.2 \pm 5.7\%$).¹¹
- b) La intervención del asesor legal contribuyó al resultado satisfactorio del problema en la mayoría de los casos ($75.4 \pm 6.4\%$.)
- c) En un número significativo de casos ($45.8 \pm 3.9\%$) la solución del problema legal impidió el desempeño de una tarea programada.
- d) El asesoramiento legal podría considerarse un costo significativo para cerca de la mitad de la comunidad de *infosec*.¹²

Regulaciones Multilaterales

Se pidió a los encuestados que realizaran una autoevaluación sobre su conocimiento de dos tratados internacionales relevantes: el Convenio de Budapest¹³ y el Arreglo de Wassenaar¹⁴ [Q13a y b]. El Convenio es un marco regulatorio para la armonización de medidas legislativas sobre el llamado "delito cibernético", es decir, delitos cometidos a través del uso de dispositivos digitales electrónicos, redes de comunicación digital o programas informáticos como medios principales de ejecución. También es un marco para la cooperación entre los estados miembros para la investigación, el enjuiciamiento y el castigo de tales delitos. En cada pregunta, a los encuestados se les preguntó: "¿Conoce el alcance de este acuerdo internacional?" Sobre la base de una escala de 4 puntos: no, lo oí nombrar, tenga una idea aproximada y sí. Las respuestas fueron 247 para las preguntas 13a y 245 para 13b. La tabla 9 muestra el número de respuestas para cada categoría.

11 Márgenes de error calculados al nivel de confianza del 90%.

12 La muestra es demasiado pequeña para hacer una afirmación con un nivel razonable de confianza.

13 Convenio sobre el delito informático del Consejo de Europa, ETS Nº 185, Budapest, 23/11/2001. La Convención está abierta a la adhesión de Estados no miembros. La adhesión de Argentina al tratado fue promulgada en noviembre de 2017.

14 Véase nota al pie [9].

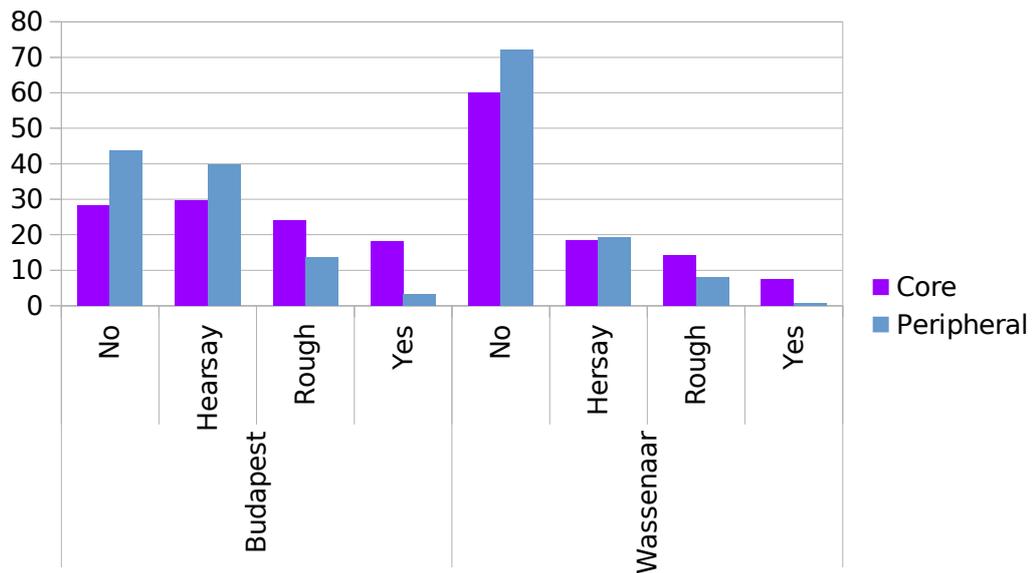
	Comunidad Amplia	Núcleo	Periférica
Conversión de Budapest			
No	89	34	55
De oídas	86	36	50
Leve idea	46	29	17
Si	26	22	4
Arreglo de Wassenaar			
No	162	72	90
De oídas	46	22	24
Leve idea	27	17	10
Si	10	9	1

Tabla 9: Conocimiento de los acuerdos internacionales (número de respuestas)

En términos generales, las cifras muestran que ambos marcos multilaterales clave son muy poco conocidos. Los porcentajes relativos para cada respuesta y subconjunto de encuestados se muestran en el cuadro 8. El subconjunto "periférico" tiene en promedio menos conocimiento en este campo que el subconjunto "núcleo", como se ve en la tabla 10.

	Núcleo	Periférica
Budapest	58.9 %	73.4 %
Wassenaar	78.3 %	91.2 %

Tabla 10: Suma de las dos categorías más bajas (porcentajes)



Cuadro 8: Conocimiento de acuerdos internacionales (porcentaje)

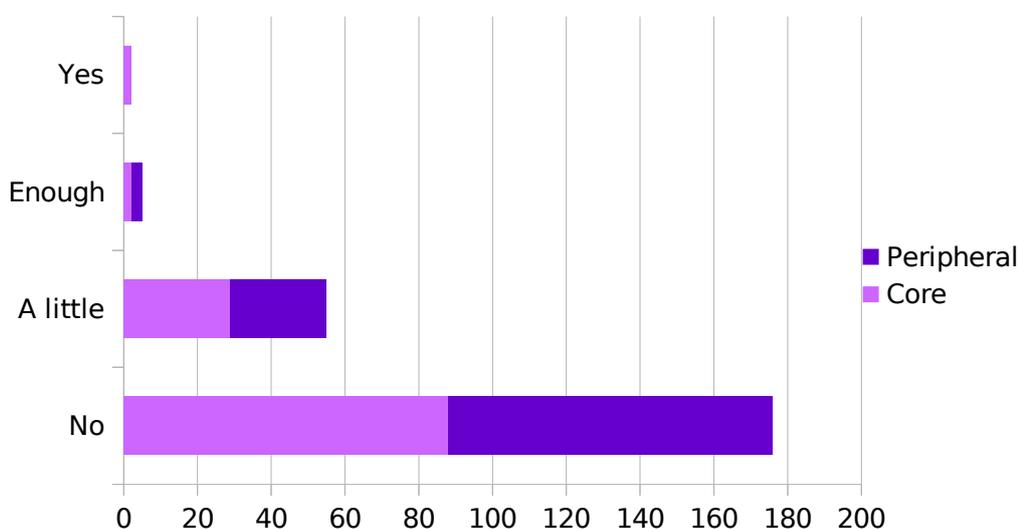
Legisladores

Se les preguntó a los encuestados su opinión sobre la comprensión de los legisladores sobre temas de seguridad de la información. La pregunta fue "¿Los legisladores entienden las cuestiones de infosec, o están correctamente asesorados sobre ellas?" Y las respuestas válidas fueron no, un poco, bastante y sí. Recibimos 238 respuestas; la mediana y el modo fueron iguales a 1. El consenso parece ser que los legisladores no están bien informados ni bien asesorados al respecto, como lo muestran tabla 11 y cuadro 9.

	Comunidad Amplia	Núcleo	Periférica
No	73,9	72,7	75,2
Un poco	23,1	24	22,2
Bastante	2,1	1,7	2,6
Si	0,8	1,7	0

Tabla 11: ¿Los legisladores están bien informados sobre infosec? (porcentaje de respuestas)

No hay diferencias relevantes entre los subconjuntos, un hecho que no sorprende considerando que, de acuerdo con la información recopilada durante las encuestas cualitativas realizadas en paralelo con este informe, los contactos formales entre la comunidad de *infosec* y los legisladores tienden a ser muy raros.



Cuadro 9: ¿Los legisladores están bien informados sobre infosec? (Número de encuestados)

Conclusiones y trabajo futuro

Conclusiones

Sobre la base de las respuestas recogidas, es posible concluir con una confianza estadística razonable que:

1. El conocimiento sobre las leyes y regulaciones fundamentales que afectan el campo es deficiente en una fracción relevante de la comunidad *infosec*. Existen suficientes razones para creer que la autopercepción de la comunidad acerca de tal conocimiento está un tanto sesgada hacia creer que tienen mayores habilidades en esa área de las que realmente poseen.
2. Profesionales de seguridad de la información a tiempo completo parecen tener menos conocimientos de los que creen sobre el campo.
3. Aproximadamente uno de cada cinco profesionales de la información o sus empleadores ha sido objeto de acciones legales debido a su oficio. La correlación con la aparición de problemas legales menos engorrosos puede indicar una preparación inadecuada.
4. La comunidad tiende a creer que el marco regulatorio actual es perjudicial para el desempeño de actividades legítimas de *infosec*. La investigación es considerada el campo de actividad más amenazado.
5. Aproximadamente uno de cada dos profesionales de *infosec* o sus empleadores ha contratado asesoría legal debido a cuestiones de derecho penal o de propiedad intelectual. El asesor legal es más a menudo contratado de manera puntual, caso por caso. Dicho abogado ha ayudado a resolver satisfactoriamente el problema tres cuartas partes del tiempo, pero en algunos casos los profesionales o sus empleadores se vieron obligados a detener las tareas planificadas para lograr un resultado satisfactorio en el

proceso legal. El costo de contratar y mantener un asesor legal es considerado como alto por aproximadamente la mitad de la comunidad.

6. Los acuerdos internacionales clave que afectan la actividad *infosec* son muy poco comprendidos por la comunidad. El Arreglo de Wassenaar es muy poco conocido.
7. Existe un consenso en la comunidad sobre la total falta de comprensión de los legisladores o sobre el asesoramiento inadecuado que tienen sobre temas de seguridad de la información.

Trabajo futuro

Para nosotros en Vía Libre, la investigación sobre la comunidad de seguridad de la información excede en gran medida el interés sociológico o antropológico. La nuestra es fundamentalmente una organización de cabildeo que realiza trabajo político no partidario en la poco explorada zona en la cual las tecnologías interactúan con las libertades y derechos fundamentales. Este trabajo debe ser considerado como un primer paso hacia el objetivo de lograr mejores estrategias y políticas públicas para el campo de la seguridad informática, de modo tal que las acciones de los estados y el sector privado en la adopción de políticas y regulaciones para proteger sus legítimos intereses no colisione con los objetivos de proteger los Derechos Humanos y el fomento y avance de la investigación en el entorno digital.

En consecuencia, detectamos un buen número de cosas por hacer:

- Se puede extraer más información útil del conjunto de datos disponibles, que podrían aportar al estudio del comportamiento de ciertas variables en correspondencia con los datos demográficos.
- La conformación de un espacio informal para la discusión de temas de política relacionados con *infosec* parece ser un paso necesario, alentando la participación de las partes interesadas relevantes en el campo. Ese espacio también

podría ser útil para diseñar estrategias para una relación más cercana con los responsables políticos.

- La investigación sobre las relaciones entre la comunidad infosec y la legislación y las agencias de aplicación de la ley no estará completa si el otro lado de las ecuaciones no se investiga también. Se debe concebir y llevar a cabo un proceso para estudiar "el otro lado".
- Este tipo de encuesta se debe ajustar en base a las lecciones aprendidas¹⁵ durante este estudio y repetido si es posible, puliendo los temas actuales y posiblemente agregando otros nuevos.
- Otras tareas complementarias se llevaron a cabo en paralelo con este estudio, incluida una serie de entrevistas grabadas en video y una reunión relajada pero rica en ideas con algunos de los interesados más relevantes de la comunidad infosec. Los materiales resultantes deben procesarse y consolidarse con una revisión mejorada de este estudio.

¹⁵ Por ejemplo, será útil agregar más estructuras de control en los cuestionarios para verificar las autoevaluaciones. En esta encuesta, usamos Q15 como un código de corrección para un posible sesgo en las respuestas a Q5 (conocimiento del derecho penal).

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 encuestados anónimos de nuestra encuesta; 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, una leona que realizó el trabajo de campo para esta encuesta; y AccessNow, por su generoso apoyo a este trabajo.