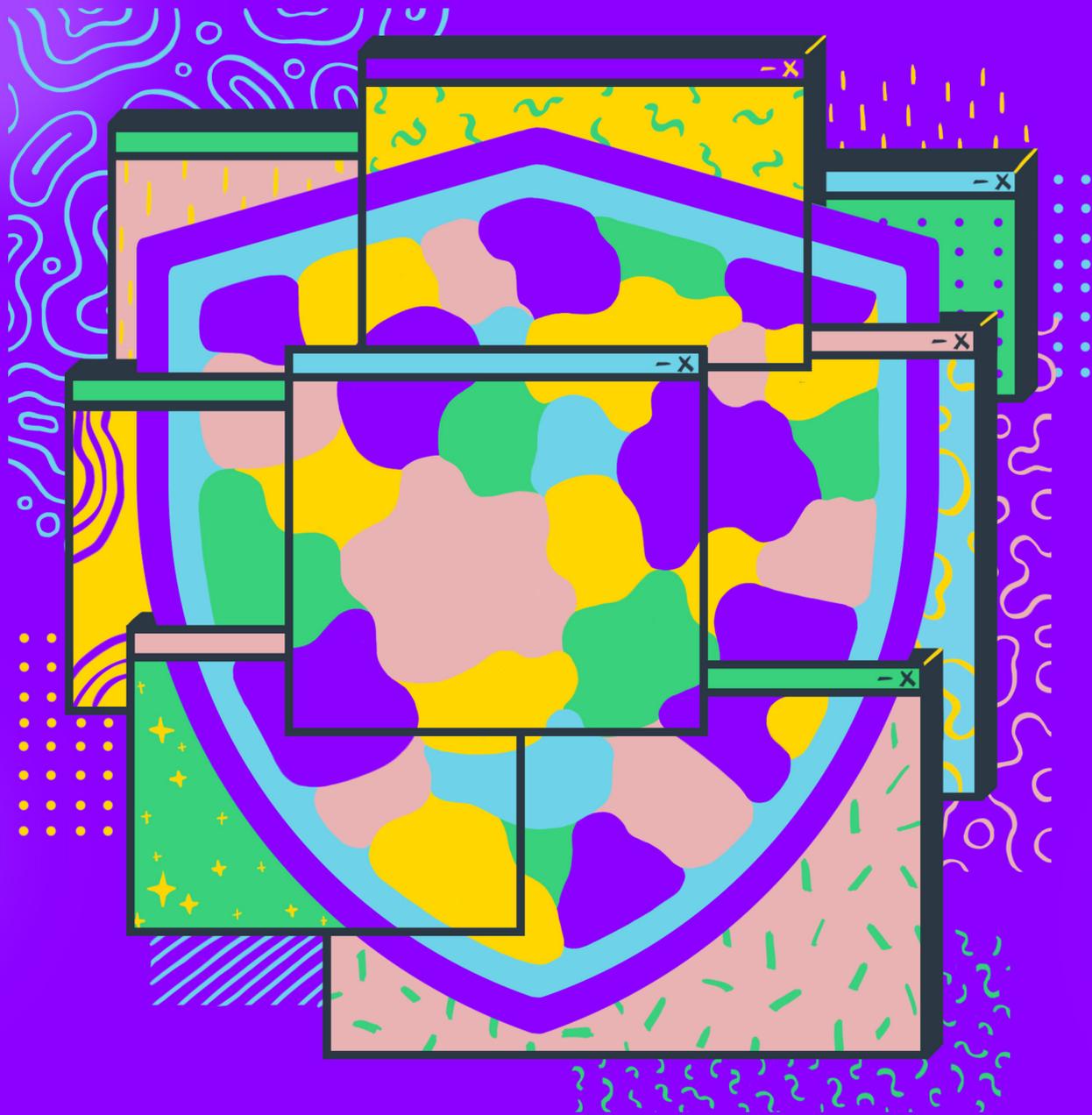


Comunidad de Seguridad Organizacional

Desafíos y oportunidades para el fortalecimiento comunitario



Junio de 2020

Introducción	→ 3
¿Qué es seguridad organizacional?	→ 4
Definiciones	5
Seguridad organizacional eficaz	10
Evaluando los efectos del apoyo en seguridad organizacional	15
El valor de los espacios comunitarios en la seguridad organizacional	→ 17
Formando y fortaleciendo conexiones	19
Aprendizaje y crecimiento	21
Obstáculos a la participación comunitaria	→ 22
Disparidades regionales de poder	23
Falta de confianza	24
Oportunidades	→ 26
Principios para espacios comunitarios inclusivos y resilientes	27

Esta investigación, encargada por Internews, fue realizada por The Engine Room de abril a septiembre de 2019. Esta investigación informó la implementación de oportunidades comunitarias en los espacios comunitarios de la comunidad orgsec.community, y fue parte de un mayor apoyo a la comunidad que también involucró el desarrollo de un marco de Monitoreo y Evaluación.

Líder de proyecto: Paola Mosso
 Líder de investigación: Madeleine Maxwell
 Apoyo en investigación: Paola Mosso
 Editoras: Sara Baker, Laura Guzman, Paola Mosso (versión en español).
 Diseño de reporte: Matildetilde

THE ENGINE ROOM

El texto de este trabajo está licenciado bajo la Licencia Internacional Creative Commons Reconocimiento-CompartirIgual 4.0. Para ver una copia de esta licencia, visita: <http://creativecommons.org/licenses/by-sa/4.0/>
 La ilustración se licencia por separado según las notas al pie.



Introducción



Entre abril y septiembre de 2019, The Engine Room realizó una investigación en conjunto con la comunidad de seguridad organizacional (orgsec). El objetivo de nuestro trabajo en alianza con Internews fue comprender mejor esta comunidad, los desafíos que enfrenta y la oportunidad de desarrollar recursos nuevos y actualizados para apoyarla. Específicamente, esta investigación contribuyó al desarrollo de un marco de Monitoreo y Evaluación (MyE) destinado a los profesionales de la seguridad organizacional y al rediseño de dos de las herramientas de orgsec.community: una [wiki](#) y una lista de distribución de correo electrónico para la comunidad de seguridad organizacional.

Esta investigación buscó abordar las siguientes preguntas:

- 1. ¿Qué es la seguridad organizacional y cómo podemos reflexionar sobre los efectos de esta práctica?**
- 2. ¿Cuál es el valor de los espacios comunitarios para los profesionales de la seguridad organizacional?**
- 3. ¿Qué oportunidades existen para aumentar la utilidad de las herramientas de orgsec.community?**

Esta investigación comunitaria consistió en investigación documental y revisión de publicaciones, participación de eventos importantes de la comunidad, como el Internet Freedom Festival (IFF) en Valencia (2019) y la RightsCon en Túnez (2019), y 16 entrevistas con un grupo diverso de profesionales en seguridad organizacional.

Este informe es un resumen de nuestro aprendizaje e incluye una serie de oportunidades en las que podríamos centrarnos en la siguiente fase de trabajo.

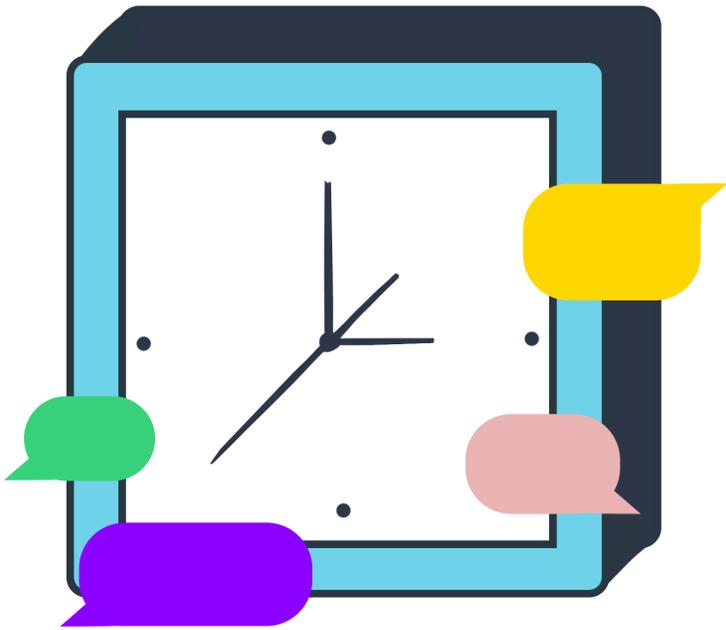


**¿Qué es
seguridad
organizacional?**

Definiciones

En grupos concretos de esta comunidad está surgiendo un consenso acerca de lo que constituye la seguridad y cómo lograrla. Hankey y Clunaigh enfatizaron cómo la definición de seguridad “debería ser personal para cada Defensor de los Derechos Humanos (DDH)”, pero en términos generales, se trata de “posibilitar el trabajo de los DDH”... “frente a fuerzas y actos hostiles”. [1] Hay una tendencia creciente a incidir en favor de compromisos a largo plazo con organizaciones y defensores, considerando la seguridad de una manera ‘integrada’[2] y ‘holística’[3], donde la seguridad digital, física, legal y psicosocial están todas consideradas, y a apartarse del modelo de un único entrenamiento. Dicho esto, en su artículo del 2015 en el International Journal for Human Rights, Bennett et al[4] advierten contra la “sistematización y estandarización en las actividades de protección”, destacando el riesgo de que esto pueda conducir a una “rigidez y exclusividad” que no coincide con los cambios rápidos en los tipos de amenazas que enfrentan los defensores ni con los cambios en la forma en que la sociedad civil protege y promueve los derechos humanos.

A través de nuestra investigación comunitaria, descubrimos descripciones y definiciones dispares de seguridad organizacional, con profesionales que usan y se comunican en diferentes idiomas dependiendo de la geografía, antecedentes y comunidades que apoyan. Las características comunes de la seguridad organizacional que surgieron en la mayoría de nuestras conversaciones incluyeron la naturaleza a largo plazo de la práctica, priorizar el desarrollo de capacidades del equipo de la organización y adoptar un enfoque holístico.



Apoyo a largo plazo

Las personas que trabajan en el área describieron la seguridad organizacional como el trabajo con organizaciones durante meses o años, no como una tarea de horas, días o semanas. En todas nuestras entrevistas, las personas compartieron la opinión de que “el apoyo a largo plazo es la única forma de hacer que [una organización] sea más resistente”, y una de ellas enfatizó que el primer año de la relación podría tener

que ver solamente con la organización “preparándose para hacer este trabajo”. La importancia del seguimiento también se enfatizó en nuestras entrevistas: “Ser capaz de hacer un seguimiento con las organizaciones [es importante]; por lo general el apoyo a las organizaciones termina con la auditoría o las recomendaciones, pero el cambio cultural lleva tiempo y seguimiento”. El cambio hacia compromisos a más largo plazo dentro de la comunidad de seguridad organizacional también fue evidente en el IFF del 2019. Quienes trabajan en seguridad organizacional hablaron de los beneficios de contar con más tiempo para conocer una organización y su contexto; de tener la oportunidad de contactarse con la organización después de realizar recomendaciones para ayudarlos con su implementación, para hacer ajustes cuando el contexto ha cambiado.[5]

**“el cambio cultural
lleva tiempo y
seguimiento”**

Desarrollo de capacidades del equipo

Las personas que trabajan en el área hablaron constantemente sobre la importancia del desarrollo de capacidades entre los múltiples miembros de una organización, siempre que sea posible. Se consideró que esta era la clave del impacto sostenible y del cambio dentro de una organización. En este contexto, el desarrollo de capacidades no se trata solo de buscar cambios en la infraestructura técnica de una organización, sino también a nivel humano. Una persona entrevistada lo resumió como “tanto trabajando directamente y como con el equipo que realizará el trabajo”.

Seguridad holística

Relacionado con este enfoque centrado en las personas está la idea de “acompañar” a las organizaciones como profesionales de la seguridad organizacional, en lugar de apoyarlas o capacitarlas. Este sutil cambio en el lenguaje comunica el papel ideal de una persona que apoya en seguridad organizacional como facilitador, ayudando al equipo de las organizaciones a desarrollar una “comprensión o intuición más profunda sobre cómo gestionar y elaborar estrategias colectivas en torno a los procesos organizacionales centrales”.

La seguridad organizacional fue vista como un enfoque holístico de seguridad por la mayoría de quienes entrevistamos. Una de estas personas definió la seguridad holística como “integrar conciencia y prácticas en torno a la seguridad, ya sea seguridad física, digital y prosperidad, en todos los aspectos de la organización”. Tal enfoque implica considerar a las personas, la capacitación, la estrategia, el proceso, los flujos de trabajo, la seguridad digital, el presupuesto, la política en el contexto del apoyo, lo personal, los viajes: “Todas las cosas con las que lidian las organizaciones”. Esta idea se repite en un artículo publicado en conjunto por dos profesionales de la seguridad organizacional, Slammer y Maya Richman[6]: “Muchas organizaciones con las que trabajo no tienen políticas organizacionales escritas. Esto incluye el código de conducta del equipo, los procesos de resolución de conflictos, las pautas de comunicación y almacenamiento. La seguridad y la protección están ligadas a todo eso.



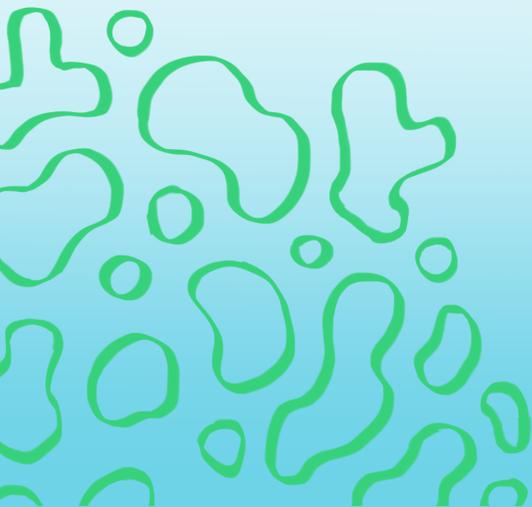
Es más que solo decidir qué datos encriptar o la administración de contraseñas de una organización. Se trata de cuidar cada parte de nuestro trabajo”.

El idioma

Sin embargo, profesionales del área sintieron que el vocabulario y los modelos de apoyo en torno a la seguridad organizacional están dominados por Estados Unidos. Hubo una demanda de un lenguaje y marco con mayor especificidad local: “Tanto en términos de vocabulario como de modelos, está muy dominado por Estados Unidos. Tengo conversaciones con personas que trabajan en seguridad organizacional en Latinoamérica. Dicen: ‘primero necesitamos modelos latinoamericanos’, sienten que estos modelos estadounidenses no se aplican”. Por ejemplo, algunos de nuestros entrevistados rechazaron el lenguaje de “seguridad”, ya que conllevaba connotaciones negativas en un país con una dictadura militar en la memoria reciente. En su lugar estas personas usan un lenguaje de protección y bienestar.



“ primero
necesitamos modelos
latinoamericanos ”



Antecedentes profesionales

Esta comunidad de práctica es extremadamente diversa, tanto en términos de antecedentes y experiencia de quienes trabajan en el área de seguridad organizacional, modalidades de apoyo y de desarrollo de capacidades que ofrecen a las organizaciones de derechos humanos, como en el formato en el que se brinda este apoyo. Entre nuestros entrevistados para esta investigación comunitaria, hablamos con profesionales con trayectorias muy diferentes en este trabajo. Los antecedentes de las personas van desde orígenes en el activismo, en movimientos sociales feministas y en ciencias sociales hasta roles previos en seguridad e informática en el sector privado, pasando por todos los estadios intermedios.

Esta introducción de Aspiration Tech resume esta diversidad de manera más eficaz:

“Las personas que entrenan en materia de seguridad de la información y tecnológica que apoyan a las organizaciones de derechos humanos constituyen un grupo de partes interesadas amplio y multifacético dentro del ecosistema de tecnología de los derechos humanos. Su profesión requiere habilidades interdisciplinarias únicas, desde alfabetización técnica hasta capacitación educativa, conocimiento pedagógico, prácticas de facilitación, habilidades interpersonales bien desarrolladas y una comprensión profunda de los contextos sociales, políticos y económicos.

Apoyan a quienes trabajan en derechos humanos a construir una cultura de seguridad en sus organizaciones y a adquirir el conocimiento y la confianza para tomar el control de la tecnología que deciden usar. Su objetivo es proporcionarles herramientas para funcionar de manera sostenible y prácticas que fortalezcan los derechos y la seguridad de sus partes interesadas”.[7]

Estos sentimientos hicieron eco en el IFF del 2019, donde los profesionales del área destacaron en múltiples sesiones cómo el trabajo de seguridad organizacional a menudo se caracteriza como una práctica “técnica”, pero que en realidad, las habilidades de comunicación y participación son a menudo más importantes.[8]

Seguridad organizacional eficaz

El impacto depende del contexto

Aunque la seguridad organizacional es una práctica diversa y variada, como se destacó anteriormente, Tactical Tech ha señalado que “la comunidad de capacitación en seguridad digital está colaborando, profesionalizando y explorando nuevos enfoques de una manera más sistemática que antes”.[9] Este estudio destacó el entusiasmo entre quienes hacen parte de la comunidad de entrenamiento y desarrollo de capacidades en seguridad digital para

co-desarrollar “un conjunto de conocimientos y estándares profesionales compartidos”, que podría incluir una teoría del cambio para la práctica en su totalidad. También se ha destacado la necesidad de un enfoque colaborativo en el desarrollo de parámetros para evaluar el éxito o impacto, a fin de garantizar que “satisfagan las necesidades prácticas y las preocupaciones esenciales de una comunidad diversa”[10].





Los desafíos en torno al desarrollo de una única teoría del cambio para una práctica tan diversa han sido destacados anteriormente. El “enfoque para el desarrollo de análisis de riesgos y prácticas de seguridad para DDH” depende completamente del contexto. Si bien existen herramientas que se usan comúnmente, que incluyen “mapeo de actividades, mapeo de actores, análisis de incidentes de seguridad y uso de la ‘fórmula de riesgo’ para lograr un análisis de su entorno que sirva de base a planes de seguridad y emergencia” [11], los profesionales usarán estas herramientas de diversas maneras, en distintos momentos y con diferentes niveles de rigor según el contexto. Como destacan los autores:



“La lógica de este enfoque es bastante clara: no existe un único enfoque de seguridad para todas las personas, y ninguna debería prescribir arbitrariamente medidas ‘seguras’, ya que el desarrollo de medidas de seguridad apropiadas requiere una comprensión profunda del conjunto de fuerzas que contribuyen al nivel de riesgo del DDH particular u organización en cuestión”.[12]

Este sentimiento hizo eco en nuestras entrevistas de investigación comunitaria, donde los profesionales hablaron de la necesidad de un enfoque flexible que aborde los matices del problema. Una persona del área describió la diferencia entre la mejor práctica en una organización con “procesos organizacionales establecidos y bien desarrollados con una estructura de gestión clara” y otra organización en la que “no hay capacidad para hacer frente a una evaluación de riesgos”, en cuyo caso, proporcionar “asistencia obvia (como cambiar a software con licencia)” podría ser más apropiado. Otra persona habló sobre la importancia de comprender el contexto histórico. Por ejemplo, en Europa del Este, donde hay un “historial de vigilancia y la aceptación de que esto continuará, lograr que las personas sean más críticas ya es una ventaja”. Otra persona lo resumió claramente: “Hay muchas rutas diferentes para lograr resultados. Lo que funciona con una organización no funciona con otras”.

La naturaleza contexto-dependiente de la práctica de seguridad organizacional también se destacó en las sesiones del IFF en el 2019[13]. Hasta los resultados de una auditoría de seguridad pueden variar, incluso la extensión de un informe. Para algunas organizaciones, un resumen de dos páginas podría ser el mejor enfoque, si se sabe que el personal tiene una capacidad limitada para comprometerse con recomendaciones detalladas. Para otras organizaciones, un informe de 30 páginas sería más apropiado.

La importancia de la participación en las organizaciones de la sociedad civil (OSC)

Si bien reconocemos la naturaleza contexto-dependiente de la seguridad organizacional, a partir de nuestras conversaciones con un grupo diverso de profesionales, la participación y pertenencia a las OSC surgió como un facilitador clave para generar impacto, que era relevante y hacia el que valía la pena luchar en la mayoría, si no en todas las situaciones.

La importancia de la participación y pertenencia a las OSC está relacionada con el enfoque centrado en el desarrollo de capacidades mencionado anteriormente. Garantizar que la organización priorice la seguridad aumenta la probabilidad de lograr un impacto sostenido con una organización. Esto podría manifestarse, por ejemplo, de las siguientes maneras:

→ Cuando uno o dos miembros del equipo ven la seguridad como parte de sus funciones, es relevante preguntarse: “¿Quién es la persona responsable [de la seguridad] en la organización? Tiene que haber alguien, alguien que sienta que “este es mi trabajo”.

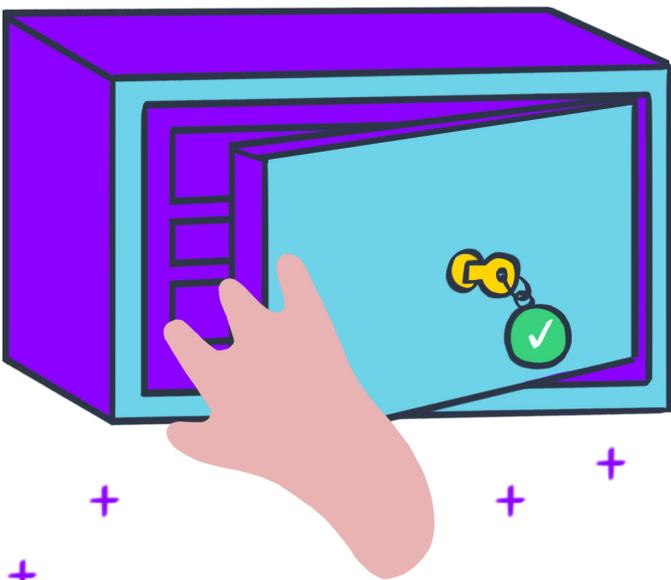
**Tiene que haber alguien,
alguien que sienta que
“este es mi trabajo”**

→ **Buscar que las organizaciones comprendan las razones para priorizar la seguridad:** “El ‘por qué’ es importante... Es poco probable que se mantenga una política que no es tan sencilla de seguir o es incómoda para algunas personas si no está justificada. La seguridad digital puede ser bastante difícil de seguir. Cuanta mayor comprensión tengan nuestros aliados de por qué estamos pidiendo esto y qué puede hacer por ellos, más probabilidades hay de que la adopten”.

+ → **Buscar la participación de quienes ocupan los puestos directivos:** “Conseguir que el director esté comprometido tiene un impacto a largo plazo: (este proceso de seguridad organizacional) se convierte en una prioridad”.

Barreras al apoyo efectivo

Nuestras conversaciones también subrayaron algunas barreras constantes para que los profesionales brinden un apoyo efectivo. Estas barreras incluyen la alta rotación de personal dentro de las OSC y la falta de capacidad o recursos dentro de las OSC para priorizar la seguridad. Se consideró que estas barreras eran más estructurales y estaban fuera del control de los profesionales, y podrían ser áreas prioritarias para que las financiadoras y otras organizaciones intermedias las aborden.



La alta rotación de personal dentro de las OSC plantea un gran desafío para los profesionales. Se invierte tiempo, energía y recursos en desarrollar las capacidades del equipo de una organización, pero cuando alguien se va de la organización, se lleva consigo esa nueva comprensión y habilidades: “Esta es una conversación que hemos tenido con compañeras y compañeros del área : les digo ‘Sé que ya has entrenado a esta organización y a su equipo,

+ ¿por qué no está vigente la política?... Y dicen: ‘Todo el equipo al que se capacitó ha renunciado’ ”. Aunque la idea de encontrar individuos dentro

de las organizaciones que se muestran entusiastas de fortalecer la seguridad de la organización habla de la importancia de la pertenencia a las OSC, este enfoque deja a una organización vulnerable a la pérdida de conocimiento: “la seguridad organizacional depende mucho de un defensor que la promueva dentro de la organización... cuando te vas, y el defensor también, es problemático”.

La falta de capacidades (de tiempo, mentales, energéticas, financieras) de las OSC para involucrarse en el proceso es otro obstáculo para la práctica efectiva de la seguridad organizacional. Especialmente para organizaciones pequeñas o con pocos recursos (que es cada vez más el caso dentro de la sociedad civil), a menudo hay prioridades más urgentes: “Estás luchando una batalla cuesta arriba: la gente está completamente sobreexigida. No disponen de grandes presupuestos. No pueden contratar a un responsable de seguridad de sistemas de información si tienen tres empleados en plantilla. Si hay 30 empleados remunerados, están haciendo el trabajo de 60 personas. Tienen poco tiempo y otras prioridades más apremiantes. Por ejemplo, resolver una propuesta de financiación siempre es prioritario”.

“ Estás luchando una batalla cuesta arriba: la gente está completamente sobreexigida ”

Evaluando los efectos del apoyo en seguridad organizacional

Dados estos hallazgos, hay una serie de consideraciones importantes a tener en cuenta al diseñar un enfoque de monitoreo y evaluación, o evaluación de impacto, dentro de la seguridad organizacional. El enfoque debe abarcar una amplia gama de indicadores para responder a la naturaleza variada y holística del apoyo de la seguridad organizacional; la interfaz debe ser simple para que los profesionales puedan participar de una manera que no los aleje del trabajo en sí; y el enfoque debe tener en cuenta los diversos contextos en los que se lleva a cabo este trabajo.

Aunque se han desarrollado algunas mejores prácticas en la comunidad de seguridad organizacional, no ha habido una evaluación exhaustiva de los métodos del área para determinar su efectividad. Está claro que las organizaciones de derechos humanos necesitan apoyo y que la organización debe ser efectiva en algún nivel, pero hay preguntas sobre el nivel de impacto y cómo aumentar el impacto, especialmente cuando los recursos son limitados. The Engine Room trabajó con Internews y varios profesionales de diversos contextos para diseñar un marco de monitoreo y evaluación que los profesionales de la organización puedan usar para medir el impacto de su trabajo.

“ no ha habido una evaluación exhaustiva de los métodos del área para determinar su efectividad ”



Al desarrollar una comprensión más profunda del impacto de su trabajo, los profesionales pueden enfocarse en lo que funciona en diferentes contextos, refinar los enfoques para aumentar el impacto y convencer a las financiadoras de invertir en la organización. Presentar la evaluación como una parte esencial del proceso de apoyo puede ayudar a las organizaciones a ver el valor de comprender las formas en que

están mejorando y dónde quedan las brechas. Este marco está diseñado para medir los cambios en el conocimiento, la actitud, el comportamiento y la condición de la organización, brindando una imagen clara y completa de los logros y soluciones que los profesionales permiten. Es un modelo de cómo puede ocurrir un cambio.

+



+



+

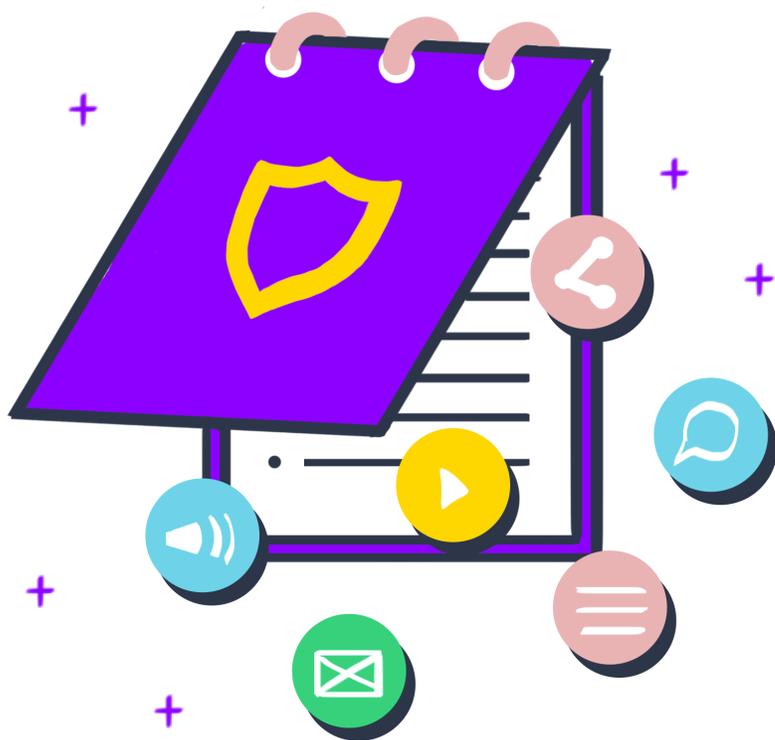


El valor de los espacios comunitarios en la seguridad organizacional

La naturaleza colaborativa de esta comunidad y el afán de encontrar más oportunidades para conectarse y apoyarse mutuamente quedó de manifiesto en publicaciones y eventos comunitarios. Tactical Tech habla de la existencia de un “entusiasta apoyo para el creciente ambiente de colaboración y coordinación entre los miembros de la gran comunidad de capacitación en seguridad digital”. En su investigación[14], descubrieron que los profesionales sentían que el impacto de pertenecer a una comunidad era variado: provoca aparentes mejoras en la calidad del trabajo que realizan al exponerse a nuevos principios, metodologías y enfoques. Los profesionales pueden aprender más rápidamente, lo que constituye por sí misma una forma de reducción de daños, ya que la alternativa es aprender “a través de la prueba y el error”, lo que seguramente tiene un gran costo para las ODH y requiere una gran inversión de tiempo. Conectarse y colaborar también ayuda a los profesionales a sentirse menos aislados.

Existen múltiples redes de profesionales de la seguridad que coordinan esfuerzos colectivos para crear y mejorar metodologías y recursos. La investigación de Aspiration Tech destacó el hecho de que “la creación y el cultivo de espacios en persona y en línea para que los profesionales de seguridad se reúnan e interactúen ha ayudado a construir y fortalecer relaciones de confianza, y ha proporcionado canales mediante los cuales se comparten conocimientos y habilidades, y más importante aún, donde se pueden apoyar unos a otros”[15].

Los profesionales han resaltado la necesidad de espacios dedicados explícitamente al intercambio de conocimientos y habilidades[16], lo que incluye más oportunidades para conectarse y colaborar interdisciplinariamente, entre profesionales de seguridad psicosocial, legal, física y digital[17]. También



se ha destacado la necesidad de mayor uniformidad en la documentación y la notificación de incidentes, amenazas y aprendizajes como una forma de facilitar el intercambio de conocimientos en la comunidad[18].

En la investigación de Aspiration Tech, los profesionales consideraron que las listas de correo entre pares “garantizan un espacio para discusiones remotas y asincrónicas entre personas que viven en geografías muy diferentes”. Los entrevistados señalaron estas listas como sus fuentes preferidas y más confiables de información y aprendizaje entre pares en línea” [19]. También encontraron que los esfuerzos “diseñados, liderados y de propiedad de la comunidad” en torno a la construcción, la colaboración y el aprendizaje comunitarios se consideraron más efectivos que los impuestos desde el exterior, o por las financiadoras.[20]

Nuestras entrevistas con profesionales respaldaron estas ideas y ayudaron a enmarcar el valor de la comunidad en dos grandes categorías: una en torno a aumentar y fortalecer las relaciones y la otra centrada en compartir conocimientos y habilidades.

Formando y fortaleciendo conexiones

Donde existen espacios comunitarios, digitales y físicos, los profesionales pueden:

- **Conectarse entre sí.**
- **Construir y fortalecer relaciones de confianza.**
- **Apoyarse unos a otros y sentirse menos aislados.**
- **Volverse más resiliente como comunidad.**

Estos espacios comunitarios son fundamentales para establecer conexiones, que impactan profundamente en la calidad y la seguridad del trabajo en seguridad organizacional. Por ejemplo, para una persona recién llegada a este espacio, puede ser difícil aprender los matices relacionados con el lenguaje y el contexto en la sociedad civil. Tener acceso a una comunidad puede facilitar y acelerar ese proceso de aprendizaje. Los espacios comunitarios también ofrecen una manera fácil para que los profesionales identifiquen a sus pares. Como dijo una profesional del área: “¿Quiénes son nuestros compañeros? El mundo de los derechos digitales es tan diverso que es difícil saber quiénes son mis pares”.

El ejercicio público de la seguridad organizacional también puede ser peligroso en ciertas regiones, lo que suma un elemento más de complejidad al conectarse y participar en espacios comunitarios: “Nos escondemos de los malos, pero también la una de la otra, por lo que es difícil encontrarnos”. Cada vez más, quienes trabajan en el área de la seguridad organizacional lo hacen independientemente como contratistas o consultores, siendo a menudo el único profesional que ofrece apoyo a determinada organización de la sociedad civil. “Esto causa mucho agotamiento emocional a los profesionales. Cuando te sientes personalmente responsable de muchos grupos diferentes, no puedes renunciar. Es mucha presión sentir que necesitas saber todo para un grupo. Si te equivocas, realmente podrías dañarlos”, dijo otra persona entrevistada. Una red diversa y fuerte también puede aumentar la resistencia de esta comunidad. Como afirmó una profesional: “Tenemos ciertos adversarios, el gobierno, el sector privado, estas personas siempre estarán allí. Serán más poderosos, [tienen] más recursos. ¿Cómo podemos garantizar nuestra continuidad? ¿Cómo podemos resistir estos cambios?”.

“ Nos escondemos de los malos, pero también la una de la otra ”

Aprendizaje y crecimiento

Dentro de los espacios comunitarios, los profesionales también pueden:

- **Compartir conocimientos e información sobre amenazas y habilidades.**
- **Colaborar en forma interdisciplinaria.**
- **Aprender más rápido y mejorar la calidad de su trabajo.**

El valor de una comunidad internacional de seguridad organizacional está en conectar a las personas que trabajan internacionalmente, o en diferentes contextos, para que planteen y debatan diferentes técnicas. “Aprender sobre diferentes perspectivas y experiencias, ¡es invaluable para mí!”. Al compartir conocimientos con otras regiones, las “mejores prácticas”, las inquietudes y la información pueden viajar más rápido, reduciendo esfuerzo desperdiciado en el sector para aprender las mismas lecciones una y otra vez. “Si hubiera un foro en línea, donde poder compartir habilidades, interactuar con otros profesionales de seguridad organizacional para compartir habilidades y desafíos. No sé si existe alguno”. Dado que los profesionales trabajan de forma independiente y no tienen acceso a las oportunidades de desarrollo personal o profesional que puede ofrecer pertenecer a una organización, sus colegas pueden brindarles ese apoyo y permitir que se sientan más seguros con sus métodos. Como dijo un profesional: “Me trae a tierra, ‘esto seguro que no, esto seguro que sí, a moverme de la duda’”.

Como mencionó otro profesional, “siempre he estado solo trabajando con una organización. Una plataforma o lista podría ser una forma de ayudar a encontrar-nos para colaborar en el proceso... podría permitirnos aprender unos de otros. Todos tenemos lagunas. Si pudiera trabajar con otros, [donde los conjuntos de habilidades se complementan entre sí], podríamos mejorar juntos”.



Obstáculos a la participación comunitaria



Durante nuestra investigación comunitaria, se constató la existencia de dos grandes obstáculos para participar en espacios comunitarios. La primera se refería a la distribución desigual de recursos entre las regiones, con una priorización de las perspectivas, marcos y experiencias occidentales no representativa. La segunda fue la falta de confianza.

Disparidades regionales de poder

La distribución desigual de poder y recursos para los profesionales de la seguridad organizacional en diferentes regiones se manifiesta de varias maneras. En la IFF este año, fue patente la disparidad regional en términos de cuán desarrollada está la comunidad de seguridad organizacional[21]. Aunque redes como la Rapid Response Network (Red de Respuesta Rápida) estaba razonablemente desarrollada y contaba con recursos en Europa del Este y en el norte de Latinoamérica, y recién estaba surgiendo en MENA (Medio Oriente y Norte de África). Esta red tiene diversos propósitos: establecer conexiones y colaboraciones con otros profesionales, compartir consejos e información sobre incidentes, discutir nuevas metodologías y técnicas, identificar debilidades en respuesta a amenazas emergentes y mapear actividades en la región. Las regiones donde no se realizan eventos o reuniones de la comunidad local y que carecen de organizaciones que actúen como centros regionales (como por ejemplo, Digital Security Lab en Ucrania) también están en desventaja, sin un fácil acceso al conocimiento, el aprendizaje y

el apoyo que brindan estos espacios.

En nuestras entrevistas con profesionales de América Latina y MENA, priorizar ciertas perspectivas y experiencias sobre otras surgió como otro obstáculo para la participación. Esto se manifiesta principalmente en el idioma y la priorización del inglés. Los recursos a menudo solo están disponibles en inglés; los espacios comunitarios requieren participación o intervención en inglés (la mayoría de las sesiones en IFF este año fueron solo en inglés), y la capacitación y listas de correo administradas por organizaciones occidentales a menudo solo se imparten en inglés. Esto significa que las organizaciones y las personas necesitan poder hablar inglés para establecer conexiones, desarrollarse y crecer.

Además del lenguaje, este desequilibrio de poder también se manifiesta a través de las estructuras y modelos que se enseñan o comparten en espacios comunitarios. Además, existe una disparidad en los tipos de organizaciones que lideran y facilitan iniciativas y espacios comunitarios: “Mucho del material de seguridad digital está dominado internacionalmente por actores estadounidenses y europeos”.

Falta de confianza

La confianza es un componente esencial de cualquier comunidad activa y exitosa. Con los espacios en línea, generar confianza es aún más difícil que hacerlo en persona. Muchos de los profesionales con los que hablamos tienen amigos cercanos en sus redes con quienes comparten preguntas y desafíos. Estas relaciones de confianza son importantes para ellos. “Cuando tienen preguntas o quieren comparar notas, tienen un puñado de personas a las que acuden, y envían correos electrónicos dentro de ese círculo”. Sin embargo, con bastante razón, esta confianza a menudo no se extiende más allá de los grupos de profesionales que se conocen personalmente. Durante nuestra

investigación, **quiénes son parte de una comunidad** y el **liderazgo de ella** surgieron como factores clave que afectan la cantidad de confianza que existe en un espacio comunitario particular.

Membresía comunitaria:

¿Quién es parte de un espacio comunitario?

Quiénes son los integrantes de un espacio comunitario influye en el grado de comodidad que sienten las personas para compartir y participar en ese espacio. Durante una sesión en RightsCon, los profesionales hablaron sobre la lista de correos de orgsec.community y cómo la cantidad de personas en la lista había aumentado rápidamente, pero la gente no sabía quiénes se habían sumado. Esto hizo que las personas se sintieran reticentes a compartir, destacando la importancia de una membresía transparente y/o procesos de inscripción transparentes. Algunas personas que entrevistamos sólo se sentían cómodas y seguras en espacios comunitarios que eran exclusivamente para mujeres y personas no binarias, y otras personas buscaban espacios que compartían sus valores, tal como espacios feministas.

Liderazgo comunitario:

¿Quién lleva el espacio de la comunidad?

El hecho de que las personas del área se sientan cómodas o no de participar en un espacio comunitario en particular también depende de la organización o grupo que dirige el espacio. “La gente tiene que confiar en el grupo que lo hace. Eso no es algo que puedas inventar”. Esto está relacionado con la barrera de disparidad de poder descrita anteriormente. Los espacios y estructuras que reproducen los desequilibrios de poder existentes, con actores estadounidenses o europeos ejerciendo la mayor influencia y control, no son confiables para muchos profesionales. Como dijo una persona del área: “No me entusiasma la idea de que los grupos occidentales gestionen esto globalmente”. Otra persona lo resumió enfáticamente: “Como cualquier iniciativa, necesita un líder o un grupo líder. ¿Lo lidera OTF (Open Tech Fund) o The Engine Room? ¿Por qué lideran los blancos? ¿Por qué es un hombre? No puede ser un esfuerzo individual, no es justo. Repite los mismos patrones. No tengo ningún interés en ser parte de algo que replica [las mismas estructuras de poder] y la participación meramente simbólica de las poblaciones marginadas”.



Oportunidades

Principios para espacios comunitarios inclusivos y resilientes

Al considerar el valor de los espacios comunitarios para los profesionales, así como las barreras que existen para participar en estos espacios, surgen cuatro principios clave que, si se cumplen, podrían ayudar a crear y mantener espacios comunitarios inclusivos y útiles.

1. Para que los espacios comunitarios funcionen, prosperen y creen un valor real para la comunidad, la confianza entre los miembros es esencial.
2. Para evitar perpetuar los desequilibrios de poder y abordar las barreras a la participación que existen, los espacios deben ser inclusivos y priorizar las necesidades de aquellos profesionales que han sido desatendidos por los sistemas de apoyo existentes.
3. Los espacios deben ser justos y respetuosos con la capacidad de los miembros para contribuir a ellos.
4. Para fomentar la confianza y garantizar que se satisfagan las necesidades de la comunidad, los miembros deben estar alineados con los valores que estos espacios encarnan.

El aspecto de estos principios en la práctica variará según la composición y los objetivos de los diferentes espacios comunitarios, pero esperamos que puedan actuar como indicaciones útiles, ya sea que esté comenzando un nuevo espacio comunitario, revisando o refrescando políticas y prácticas, o reflexionando sobre grupos de los que has formado parte en el pasado.

Referencias

- [1] Rethinking Risk and Security of Human Rights Defenders in the Digital Age
<https://academic.oup.com/jhrp/article-abstract/5/3/535/2188773?redirectedFrom=PDF>
- [2] <http://www.integratedsecuritymanual.org/>
- [3] <https://holistic-security.tacticaltech.org/>
- [4] Critical perspectives on the security and protection of human rights defenders.
http://eprints.whiterose.ac.uk/95532/1/Bennett_et_al_2015_IJHR.pdf
- [5] Chilled digital security, IFF 2019
https://docs.google.com/document/d/1W_O3SWdly5OemlEvhAnkZxMJsrDpt2A3SlSUuHD0wMs/edit#
- [6] <https://medium.com/read-write-participate/a-slow-and-faraway-conversation-between-slammer-musuta-and-maya-richman-d47311ec65fd>
- [7] Forging Careers in Human Rights Information Security Today
<https://aspirationtech.org/files/AspirationHRTechPractitionerSustainabilityReport.pdf>
- [8] https://docs.google.com/document/d/1W_O3SWdly5OemlEvhAnkZxMJsrDpt2A3SlSUuHD0wMs/edit#
- [9] Digital Security Trainers' Practices and Observations
https://secresearch.tacticaltech.org/media/pages/pdfs/original/TrainersPractices_Observations.pdf

- [10] Training Digital Security Trainers: A Preliminary Review of Methods, Needs and Challenges
https://internews.org/sites/default/files/resources/InternewsWPDigitalSecurity_2013-11-29.pdf
- [11] Rethinking Risk and Security of Human Rights Defenders in the Digital Age
<https://academic.oup.com/jhrp/article-abstract/5/3/535/2188773?redirectedFrom=PDF>
- [12] Rethinking Risk and Security of Human Rights Defenders in the Digital Age
<https://academic.oup.com/jhrp/article-abstract/5/3/535/2188773?redirectedFrom=PDF>
- [13] 5 day non-technical SAFETAG training, IFF 2019
https://docs.google.com/document/d/1W_O3SWdly5OemlEvhAnkZxMJsrDpt2A3SlSUuHD0wMs/edit#heading=h.1998sx2tnjw0
- [14] Digital Security Trainers' Practices and Observations
https://secresearch.tacticaltech.org/media/pages/pdfs/original/TrainersPractices_Observations.pdf
- [15] Forging Careers in Human Rights Information Security Today
<https://aspirationtech.org/files/AspirationHRTechPractitionerSustainabilityReport.pdf>
- [16] Forging Careers in Human Rights Information Security Today
<https://aspirationtech.org/files/AspirationHRTechPractitionerSustainabilityReport.pdf>

[17] What Next? The Quest to Protect Journalists and Human Rights Defenders in a Digital World

<https://freedomhouse.org/sites/default/files/What%27s%20Next%20-%20The%20Quest%20to%20Protect%20Journalists%20and%20Human%20Rights%20Defenders%20in%20a%20Digital%20World.pdf>

[18] Training Digital Security Trainers: A Preliminary Review of Methods, Needs and Challenges

https://internews.org/sites/default/files/resources/InternewsWPDigitalSecurity_2013-11-29.pdf

[19] Forging Careers in Human Rights Information Security Today

<https://aspirationtech.org/files/AspirationHRTechPractitionerSustainabilityReport.pdf>

[20] Forging Careers in Human Rights Information Security Today

<https://aspirationtech.org/files/AspirationHRTechPractitionerSustainabilityReport.pdf>

[21] Regional networks, IFF 2019

https://docs.google.com/document/d/1W_O3SWdlY5OemlEvhAnkZxMJsrDpt2A3SlSUuHD0wMs/edit#