Lazos que unen

Seguridad organizacional para la sociedad civil

Preparado por The Engine Room, para la Fundación Ford
Marzo del 2018

THE ENGINE ROOM

Este informe de investigación, encargado por la Fundación Ford, fue realizado por The Engine Room de enero a diciembre del 2017. El contenido de este informe no refleja la opinión oficial de la Fundación Ford, y la responsabilidad por la información y puntos de vista expresados en el informe radica completamente en The Engine Room.

Responsables de publicación y editores de contenidos: Michael Brennan, Jean Cook, Ryan Gerety, Jenny Toomey.

Investigadora principal: Zara Rahman (The Engine Room),
Investigadora asistente: Paola Verhaert (The Engine Room).
Investigación y contenido: Nicole Anand, Alix Dunn, Laura Guzman, Anca Matioc, Maya Richman, (The Engine Room).
Ilustraciones: Jason Li, http://hongkonggong.com/
Diseño del informe: Adjoa Opoku, http://adjoaopoku.com/

The Engine Room solicita que el reconocimiento y citas de esta publicación sean referenciadas como: The Engine Room: Fortalecimiento del ecosistema de apoyo de seguridad digital, marzo del 2018. Este informe está disponible en https://theengineroom.org.

Contenido

Introducción

A medida que el uso de las tecnologías digitales se ha extendido en la sociedad civil, ha traído consigo nuevas oportunidades para que los grupos amplifiquen su trabajo a mayor escala y velocidad. Pero también ha supuesto nuevos escenarios de riesgos y vulnerabilidades. Para la sociedad civil, la respuesta ante dichos riesgos puede encontrarse en el **ecosistema de apoyo de seguridad digital**, un ecosistema en expansión compuesto por organizaciones, individuos, colectivos y grupos de múltiples partes interesadas que buscan brindar apoyo de seguridad a la sociedad civil.

Este informe adopta una comprensión amplia de la seguridad digital, abarcando no solo las intervenciones centradas en la seguridad y aquellas tradicionalmente entendidas bajo la etiqueta de seguridad digital, sino también áreas de debilidad o vulnerabilidad para la sociedad civil en el uso de tecnologías digitales e infraestructura técnica a nivel institucional.

Tradicionalmente, el soporte de seguridad digital ha sido proporcionado a través de capacitaciones, a menudo enfocadas en herramientas. Esto no ha funcionado: el contexto social cambia rápidamente y, con él, la idoneidad de ciertas herramientas. En este informe, miramos más allá de los enfoques centrados en herramientas para la seguridad digital, para considerar de manera más amplia áreas de vulnerabilidad para la sociedad civil y cómo pueden abordarse. Adoptamos un enfoque amplio de lo que se entiende como **apoyo de seguridad digital**, considerando aspectos como soporte emocional e intervenciones sociales, así como recursos técnicos.

Teniendo en cuenta el énfasis de la Fundación Ford en el fortalecimiento de las instituciones, en esta discusión y análisis examinamos el modo de **construir un ecosistema de apoyo de seguridad digital saludable para la sociedad civil a largo plazo**, e intervenciones que construyan instituciones en lugar de capacidades individuales. Las tecnologías digitales nos conectan, lo que significa que una debilidad en un punto de la red puede generar riesgos para otra parte, como correos electrónicos enviados con virus o bases de datos de contactos filtradas por una persona con los datos personales de otra. Para las instituciones y organizaciones, este efecto en cadena debería tener un gran impacto en la forma en que se implementan las intervenciones de apoyo de seguridad digital.

Como describimos en el informe, la seguridad digital está profundamente entrelazada con otras formas de seguridad, como la física y la sicológica. Pero la sociedad civil está actualmente menos acostumbrada a darse cuenta y saber cómo responder a las amenazas a la seguridad digital. La seguridad digital puede ser mucho menos tangible y visible que otros tipos de seguridad. Aquí resumimos por qué es importante. Destacamos las diferentes necesidades organizacionales en torno a la seguridad digital y proponemos enfoques para satisfacer esas necesidades.

El ecosistema de seguridad digital se compone de muchas partes: en este informe nos centramos en las necesidades de las organizaciones de la sociedad civil. En el siguiente diagrama, mostramos una visión (no exhaustiva) de cómo estas necesidades se cruzan con otras partes clave del ecosistema.

Para comprender qué elementos deben estar presentes dentro de un ecosistema de apoyo de seguridad digital saludable, nos enfocamos en identificar las **necesidades organizacionales de la sociedad civil** a partir de ese ecosistema de soporte. Al entender primero las necesidades, podemos evaluar los posibles enfoques y, en la última sección, sugerir recomendaciones para los financiadores.

Creemos que, sobre todo, un ecosistema de apoyo de seguridad digital saludable puede satisfacer esas necesidades de manera receptiva y puede ayudar a las organizaciones de la sociedad civil a construir prácticas de seguridad digital saludables a lo largo del tiempo.

Resumen

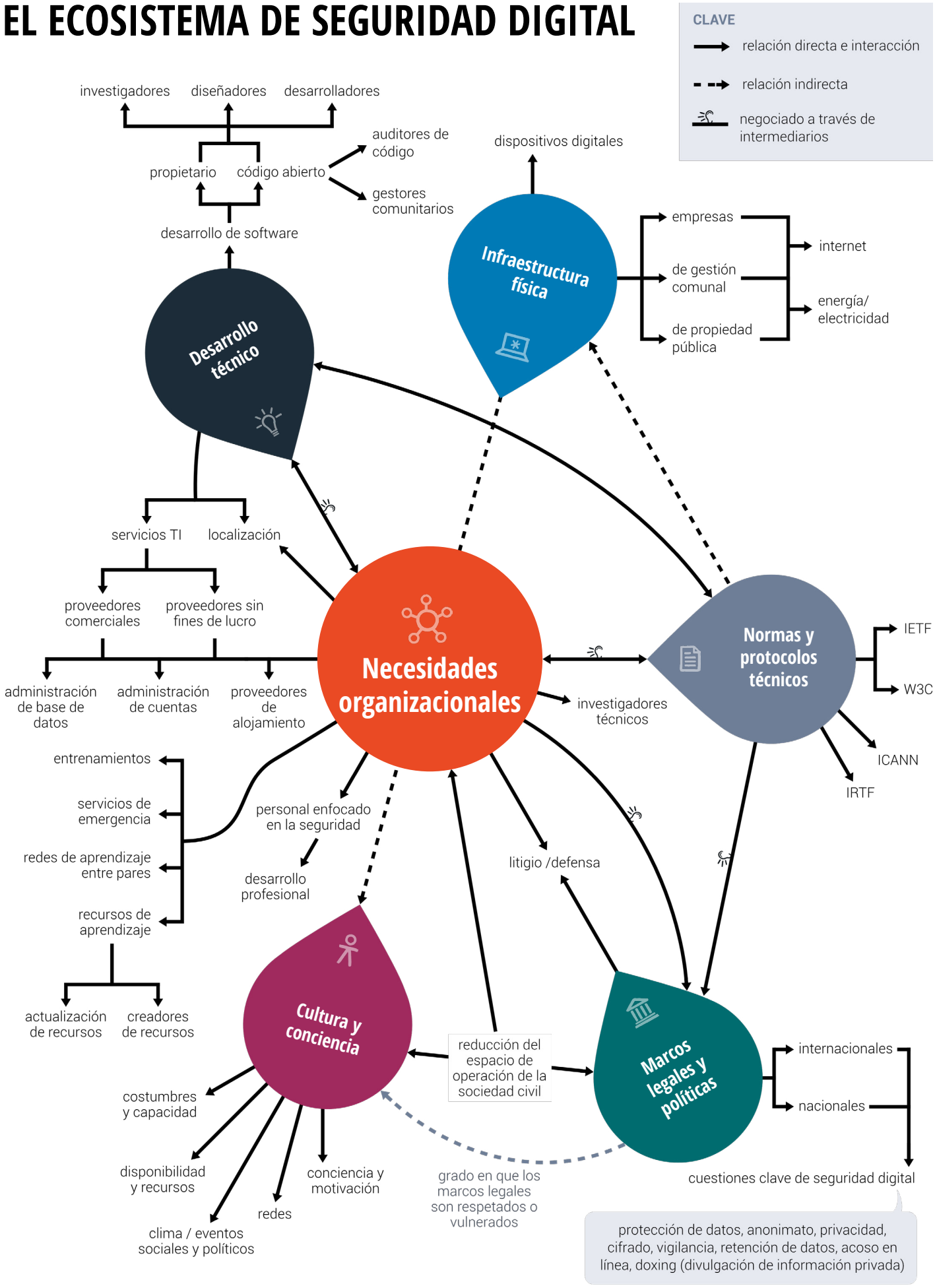
Sección 1 – La naturaleza contextual de la seguridad presenta información contextual para ubicar el resto del informe. Aquí, discutimos los conceptos básicos de la seguridad digital, consideramos los contextos políticos y echamos un vistazo breve a los enfoques actuales y pasados para la provisión de apoyo de seguridad digital. Esta sección enmarca el resto del informe y proporciona una introducción al pensamiento sobre el papel de la seguridad digital dentro de un amplio contexto social y político.

Sección 2 – Viajes organizacionales presenta un marco para comprender el recorrido que atraviesa una organización (un beneficiario) en el desarrollo de sus procesos de seguridad digital. Este marco se describe en un diagrama en la página 17 e introduce tres arquetipos organizacionales. De organizaciones en etapa de "desconocimiento, para quienes la seguridad digital no es en absoluto una prioridad; a organizaciones en "aprendizaje", que comienzan a darse cuenta de por qué la seguridad digital es importante; a organizaciones con "dominio", que han desarrollado formas de implementar y poner en funcionamiento la seguridad digital dentro de su institución.

Las ideas en la Sección 2 se centran en estos tres arquetipos, con el objetivo de enfatizar cómo se requieren diferentes tipos de apoyo de seguridad digital para las organizaciones que se encuentran en diferentes etapas de este ciclo. Tenga en cuenta también que esto es más un "ciclo" que un "proceso" único: las organizaciones continúan en este ciclo mientras desarrollan capacidades en las diferentes prácticas de seguridad digital.

Sección 3 - Recomendaciones abreva en los conocimientos resultado de esta investigación, y está particularmente fundamentada por la experiencia de The Engine Room en este campo.

EL ECOSISTEMA DE SEGURIDAD DIGITAL



Publicado por primera vez en marzo del 2018. Creado por The Engine Room con el apoyo de la Fundación Ford, ilustrado por Jason Li.

1. La naturaleza contextual de la seguridad

Las percepciones de seguridad y las necesarias reacciones son altamente contextuales. Con esto en mente, este informe se enfoca en un contexto: el de Estados Unidos entre enero y setiembre del 2017. La mayoría de nuestros informantes y entrevistados conocen bien el contexto de EE.UU. También hablamos con expertos en seguridad digital que trabajan en un contexto internacional, y todos se refirieron al menos una vez a materiales de seguridad digital creados en o para el contexto de EE. UU.

The Engine Room ha trabajado en y con la comunidad de seguridad digital de los EE. UU. y de varias comunidades internacionales. A lo largo de este informe, nuestro objetivo es enriquecer las opiniones y experiencias de los grupos subrepresentados en estas comunidades, al tiempo que reconocemos las voces más tradicionales en el espacio de la seguridad digital.

1.1 ENTENDIENDO LA SEGURIDAD DIGITAL

Para ayudar a los lectores a entender cómo vemos el papel de la seguridad digital en la creación de instituciones, desarrollamos esta metáfora visual, que incluye descripciones en los recuadros amarillos de similitudes entre "seguridad contra incendios" y "seguridad digital".

Muchas vulnerabilidades están integradas en la infraestructura de una organización: son difíciles de ver y demoran en resolverse. Sin embargo, muchas organizaciones priorizan las soluciones rápidas que no tienen un impacto duradero porque son más visibles y proporcionan una gratificación más instantánea.

ESTUDIO DE CASO

SOLUCIONES RÁPIDAS E INADECUADAS

Aprendizaje clave: aquellas que son percibidas como "soluciones rápidas" para la seguridad digital a menudo tienen prioridad, a pesar de que pueden no ser tan útiles a largo plazo.

Una organización llevó a cabo una campaña de crowdfunding en su comunidad bajo el marco de "ayudar al personal a aumentar su seguridad digital". Usaron el dinero para comprar nuevos iPhones para el personal, pero no cubrieron cuestiones clave de seguridad, como:

- Políticas para poner cuentas de trabajo en teléfonos personales
- Guía de gestión de dispositivos móviles
- Desarrollo y/o aplicación de algún tipo de política de seguridad

Comprar nuevos iPhones para el personal es un resultado tangible y de rápida consecución de la recaudación de dinero. Pero sin un enfoque de seguridad a más largo plazo, los nuevos dispositivos pueden no contribuir en última instancia a una práctica de seguridad digital más saludable dentro de la propia organización.

Las vulnerabilidades institucionales en el espacio digital pueden derivarse de la forma en que el sitio web de una organización se configuró inicialmente -quizás sin utilizar el software más actualizado- o se relaciona con las prácticas operacionales diarias de una organización, tales como el pago de sueldos, u

Proteger digitalmente a su organización es como preparar su oficina para un incendio

Detector de humo
sistemas de detección + indicadores de estado visuales /auditivos

Charlas de bomberos en escuelas
Los expertos externos enseñan métodos y mejores prácticas relacionadas con pequeñas emergencias, **pero no** cómo combatir personalmente un incendio de gran escala

Rociadores
sistemas de respuesta ante emergencias manuales o automatizados

Salida en caso de incendio
señalizada permanentemente funciona como recordatorio continuo

Revestimiento ignífugo
materiales resistentes y medidas de protección incorporadas al edificio

Simulacros de incendio
entrenamiento periódico en respuesta ante emergencias

Oficial a cargo de la prevención de incendios
persona designada que realiza el mantenimiento diario y sirve de contacto durante las emergencias

Extintores
herramientas personales que cualquiera puede usar destinadas a solucionar emergencias menores

Pautas de sentido común / normas culturales
no sobrecargue los enchufes eléctricos, no deje el gas encendido, tenga cuidado con las velas

Investigador de incendios provocados
análisis forense de desastres

Nota: Usted no llama al cuerpo de bomberos directamente, ellos acuden mediante el operador

Código de incendios
¡Las leyes, políticas y reglas institucionales pueden cambiar con el tiempo!, y dependen del país donde se lleva a cabo la operación

Operador 911/999
agente externo al que se recu en caso de emergencia + tejido emocionalmente atento + intermediario que se conecta con la persona correcta

La seguridad digital a menudo se entiende como una acción **personal**, pero para que las prácticas saludables de seguridad digital sean efectivas, deben **compartirse**. Al igual que la seguridad contra incendios, la seguridad digital puede concebirse en diferentes niveles:

- Dentro de la infraestructura institucional: garantizando la seguridad de su infraestructura operativa, desde el alojamiento del correo electrónico hasta el software de finanzas.
- Comprensión de los diferentes niveles de respuesta: distintos niveles de amenazas a la seguridad digital requieren convocar a diferentes expertos (externos o internos).
- Cultura y conocimiento: Fomentar capacitación continua en torno a la seguridad digital, para desarrollar una cultura que priorice la seguridad.

Publicado por primera vez en marzo del 2018. Creado por The Engine Room con el apoyo de la Fundación Ford, ilustrado por Jason Li.

otras transacciones financieras. Solucionar estas vulnerabilidades a menudo requiere tanto un cambio técnico como uno de comportamiento en los hábitos del personal, lo cual demanda mucho más tiempo para implementar y acostumbrarse.

Esto se puede observar en una mayor demanda entre las organizaciones de entrenamientos de uno o dos días en lugar de asumir compromisos presupuestarios a largo plazo para la implementación metódica de nuevas políticas. Las organizaciones también pueden priorizar probar una nueva herramienta tecnológica en lugar de invertir en impulsar la infraestructura técnica. Muchos entrevistados destacaron tanto la preferencia de la sociedad civil como la de los financiadores por las soluciones rápidas y "brillantes".

DILEMMA

LAS POLÍTICAS DE SEGURIDAD DIGITAL

Comprender el rol de la seguridad digital dentro de una organización puede hacer una diferencia en cómo se la percibe.

La seguridad digital como intervención técnica

Para algunos proveedores de soporte, el trabajo de apoyo de seguridad digital era percibido como "apolítico", y centrado principalmente en intervenciones técnicas para apoyar varias misiones políticas en lugar de políticas en sí mismas. Los proveedores de soporte que trabajan con comunidades con las que no están familiarizados o que desempeñan un rol puramente técnico en, por ejemplo, realizar análisis de instancias potenciales de malware, perciben su rol como algo separado de cualquier tipo de política, y puramente como una intervención técnica.

VS.

La seguridad digital es parte de una lucha política por la justicia

Para otros entrevistados, la seguridad digital es intrínsecamente un acto político, basado en la creencia de que "la vigilancia es un deseo de controlar poblaciones pobres de color". Las personas con las que hablamos que comparten este punto de vista destacaron que la privacidad y la seguridad significan cosas muy diferentes para las poblaciones que se encuentran desde su nacimiento bajo diferentes niveles de vigilancia. En los Estados Unidos, esto incluye a las comunidades pobres, las que dependen del apoyo del estado y las personas que son objeto de excesiva persecución por fuerzas estatales (como las poblaciones afronorteamericanas), por nombrar solo algunas.[1] Para estos entrevistados, partir de este punto resulta en un enfoque para la seguridad digital centrado en la justicia.

Nuestra Opinión:
Creemos que particularmente en los Estados Unidos, centrarse en lo racial es esencial para comprender las amenazas a la seguridad y los desafíos que enfrentan las comunidades de color en particular. La seguridad digital, al igual que cualquier otro tipo de seguridad, cambia según la posición social y política de la persona o comunidad bajo amenaza. Particularmente en los Estados Unidos, las comunidades de color están sujetas a niveles y tipos de vigilancia muy diferentes que las comunidades predominantemente blancas, y esto debe tenerse en cuenta al diseñar las intervenciones de apoyo de seguridad.

La aplicación de una lente de justicia racial para el diseño de la asistencia técnica garantiza que estas necesidades y modelos de amenazas asimétricas sean reconocidas adecuadamente y se planifiquen de manera proactiva. Este es solo un ejemplo de cómo contar con proveedores de apoyo de seguridad que estén íntimamente familiarizados con el contexto de aquellos a los que intentan apoyar, puede marcar una gran diferencia en la efectividad del soporte en última instancia.

ESTUDIO DE CASO

POLÍTICAS TECNOLÓGICAS QUE CAMBIAN RÁPIDAMENTE

Aprendizaje clave: cuando la aplicación de mensajería WhatsApp cambió sus políticas de seguridad, los usuarios quedaron confundidos por los mensajes contradictorios provenientes de los medios, y de WhatsApp, sobre la idoneidad de la aplicación para sus necesidades.

En febrero del 2016, mil millones de personas estaban usando WhatsApp.[3] A mediados del 2016, la aplicación de mensajería implementó el cifrado de extremo a extremo predeterminado para la totalidad de usuarios en todos los dispositivos. Esta decisión fue un paso importante hacia la normalización del cifrado de extremo a extremo como estándar para las aplicaciones de mensajería[4], pero no incluyó el cifrado de extremo a extremo para la mensajería grupal, lo que generó confusión entre los usuarios. Sin embargo, es importante tener en cuenta que las necesidades de privacidad y seguridad de los usuarios van más allá del cifrado de contenido de extremo a extremo. Esto quedó demostrado cuando WhatsApp anunció en agosto del 2016 que compartiría los números de teléfono de los usuarios y la hora de la última conexión, con Facebook, que adquirió WhatsApp en el 2014[5].

La forma en que las políticas de la compañía cambiaron rápidamente en torno a la administración de contactos y el cifrado de WhatsApp supuso que las personas que querían practicar una buena seguridad digital recibían mensajes diversos acerca de su idoneidad. Para los lectores del periódico The Guardian en el Reino Unido, esto se confundió aún más con informes que afirmaban que había una "puerta trasera" en WhatsApp (un término que el periodista posteriormente corrigió sustituyéndolo por "vulnerabilidad"), que fueron fuertemente criticados por un grupo de importantes investigadores de seguridad.[6]

Los cambios de política y los desarrollos técnicos pueden generar mensajes confusos para los usuarios de ciertas herramientas o prácticas, incluso para aquellos que desean mejorar sus prácticas de seguridad digital.

1.2 CONTEXTOS CAMBIANTES

Aprender y dominar la seguridad digital requiere un aprendizaje constante en lugar de esfuerzos puntuales, porque el ecosistema de seguridad digital (y el propio modelo de amenaza) puede cambiar rápidamente.

Como Martin Shelton escribe: "la tecnología digital no muere, simplemente envejece muy, muy rápido". Incluso los recursos de seguridad digital más ricos se vuelven rápidamente obsoletos".[2]

La falta de recursos de las organizaciones guiadas por su misión para el aprendizaje continuo significa que muchas se apoyan en intermediarios de confianza para actualizarse sobre lo que los nuevos desarrollos significan para su trabajo.[7] Estos intermediarios son normalmente instituciones o individuos con tiempo y recursos para monitorear los últimos desarrollos, comprender sus implicaciones para la sociedad civil y 'traducirlos' a un formato que tenga sentido para la sociedad civil.

Los entrevistados sugirieron que otra consecuencia de este panorama cambiante era que los receptores de intervenciones de apoyo únicas se sentían confundidos o abrumados por los consejos cambiantes que recibían.

Las mejores prácticas recomendadas para la seguridad digital cambian rápidamente como resultado de cambios políticos, cambios legales o una mayor conciencia de las vulnerabilidades técnicas.

Muchos de los entrevistados que trabajan en la provisión de apoyo en los Estados Unidos mencionaron un aumento definitivo en el interés por impulsar las prácticas de seguridad digital después de las elecciones presidenciales de EE. UU. del 2016. Para describirlo en términos usados en el mundo de la seguridad digital,

esto se debió a que los **modelos de amenaza** de las personas cambiaron: las posibles formas en que su seguridad y protección podrían verse comprometidas o atacadas, cambiaron como resultado del cambio de contexto político.

Sin embargo, las opiniones de los entrevistados se dividieron en gran medida en torno a si este interés inicial se tradujo en un cambio a largo plazo en el comportamiento o en la forma en que se recibió su consejo.

Los fondos receptivos, como el Fondo de seguridad digital de Ford, fueron calificados como muy útiles para permitir que las organizaciones respondan de manera ágil y flexible en contextos que cambian rápidamente.

Esto también habla de la necesidad de que el apoyo de seguridad digital se centre en brindar soporte a la adopción del pensamiento crítico y la autoevaluación, en lugar de recomendar herramientas particulares que pueden envejecer rápidamente.

1.3 POLÍTICAS Y CRIMINALIZACIÓN DE LA SEGURIDAD DIGITAL

En un momento de reducción del espacio cívico en los Estados Unidos, y de hecho en todo el mundo[8], y de hecho en todo el mundo, las medidas de seguridad digital son cada vez más importantes para las organizaciones que buscan que quienes detentan el poder rindan cuentas. Pero especialmente en los últimos tiempos, el apoyo de seguridad digital se ha convertido en un objetivo para los gobiernos que quieren tomar medidas enérgicas contra la sociedad civil.

El caso de los 10 de Estambul es un acontecimiento extremadamente preocupante en términos de cómo los gobiernos y otros perciben la seguridad digital. Politiza en un grado preocupante la cuestión de protegerse a sí mismo al utilizar las tecnologías digitales, especialmente para quienes trabajan en la sociedad civil.

La selección como blanco, detención y arresto de *instructores de seguridad digital* explícitamente por su trabajo marca un claro cambio en la manera en que los gobiernos represivos han tratado el apoyo de seguridad digital. El caso de los diez defensores de los derechos humanos en Turquía todavía está en curso, y si este caso significa que los talleres de seguridad digital se convertirán más en un objetivo explícito, o si se trata de un evento único, aún está por verse.

ESTUDIO DE CASO

LOS 10 DE ESTAMBUL

Aprendizaje clave: la seguridad digital está siendo cada vez más criminalizada y politizada por los estados represivos. Esto presenta una tendencia preocupante para el futuro.

El 5 de julio del 2017, se realizó en Turquía un allanamiento en un taller de seguridad digital para defensoras de los derechos de las mujeres, y ocho participantes y dos entrenadores fueron detenidos, entre ellos el director de Amnistía Internacional en Turquía; un ciudadano alemán, Peter Steudtner, y un ciudadano sueco, Ali Gharavi. Hasta donde tenemos conocimiento, esta es la primera vez que un taller de seguridad digital ha sido atacado de manera tan explícita por las fuerzas del orden público en cualquier parte del mundo. Después de 113 días de prisión, los diez fueron puestos en libertad en espera de juicio; a dos de los participantes se les prohibió viajar y los entrenadores de seguridad digital pudieron abandonar el país.[9]

El apoyo de seguridad digital debe ser planeado cuidadosamente para el contexto en el que se implementará.

Por ejemplo, particularmente en países políticamente restrictivos como Turquía, está claro que la provisión de seguridad digital debe planificarse cuidadosamente. Esto podría significar apoyar a los activistas para que viajen fuera de su país de origen para recibir capacitación (un enfoque común en los esfuerzos para apoyar a los activistas sirios, que viajan a Turquía, o entre los activistas turcos, que podrían viajar a Georgia). También podría implicar tomar más precauciones al viajar a ciertos países.

Ejemplos: Si bien los talleres de seguridad digital en sí mismos no habían sido antes convertidos en objetivos, los gobiernos de todo el mundo han revelado su falta de comprensión de la seguridad digital y la administración de datos a través de políticas legales y declaraciones:

Comprender mal el papel del cifrado: Altos funcionarios de gobierno han demostrado que no entienden cómo funciona el "cifrado", lo que demuestra que carecen de una comprensión sólida de los aspectos técnicos, pero tal vez más problemático aún, que tampoco entienden que el cifrado es importante para muchos aspectos de la vida cotidiana. Contrariamente a algunas de las citas a continuación, todos dependemos del cifrado, por ejemplo, para interactuar de forma segura con su banco en línea y para asegurarse de que los extraños no puedan ver sus contraseñas cuando las escribe.

• En julio del 2017, la Ministra del Interior del Reino Unido, Amber Rudd, calificó al "supuesto" cifrado de extremo a extremo como un "problema" porque los funcionarios no pueden acceder al contenido de los mensajes enviados a través de plataformas que usan el cifrado. Solicitó que las empresas de tecnología trabajen más estrechamente con las autoridades, de modo que puedan acceder a más información cuando sea necesario.[10]

• En julio del 2017, el primer ministro australiano Malcolm Turnbull pidió la prohibición del cifrado de extremo a extremo, afirmando que "las leyes de las matemáticas son muy encomiables, pero la única ley que se aplica en Australia es la ley de Australia".[11]

• En agosto del 2016, el entonces Ministro del Interior de Francia, Bernard Cazeneuve, declaró que "el cifrado de mensajes, ampliamente utilizado por los extremistas islámicos para planear ataques, debe combatirse a nivel internacional".[12]

• En febrero del 2016, después del ataque de San Bernardino en California, el FBI instó a Apple a ayudar a "desbloquear" un iPhone utilizado por uno de los dos atacantes. Apple rechazó la solicitud de crear una "puerta trasera" para evitar sus propias salvaguardas, aunque el FBI posteriormente afirmó que habían desbloqueado con éxito el teléfono sin la cooperación de Apple.[13]

No ver la importancia de invertir en seguridad digital: como se analiza en este informe, la seguridad digital es contextual y un aspecto fundamental para la capacidad de una organización para cumplir su misión. Para los gobiernos, depender de voluntarios sin supervisión sería una manera increíblemente arriesgada de reforzar su propia seguridad digital (y potencialmente pondría en riesgo sus propios sistemas).

• En octubre del 2016, el Ministerio del Interior de Alemania dio a conocer planes para establecer un "cuerpo de ciberbomberos voluntarios" ("Cyber Feuerwehr") y pedir a las empresas locales que presten sus expertos en TI hasta 20 días al año como parte de una brigada voluntaria de ciberbomberos.[14]

La seguridad digital es parte de un contexto de seguridad integral, que también incluye la seguridad física, la seguridad sicosocial y la continuidad operacional. Centrarse exclusivamente en la seguridad digital puede ignorar el cuadro completo y dar como resultado consejos de seguridad redundantes o dañinos.

Para muchas organizaciones basadas en una misión, especialmente para aquellas que trabajan en entornos de alto riesgo, la seguridad digital simplemente forma parte de sus necesidades de seguridad, según las definieron Alice Nah et al.[15] Los enfoques sicosociales consideran los factores sicológicos junto con el entorno social de las personas y consideran cómo se cruzan para afectar el bienestar físico y mental de las personas.

La facilidad y comodidad de uso también son importantes. El asesoramiento de seguridad digital que se centra en los aspectos técnicos pero ignora el componente de usabilidad puede ser inútil. Como lo resume Jessy Irwin,[16] existe un equilibrio entre la seguridad y la conveniencia, y señala que muchas de las opciones más seguras que existen se quedan cortas en cuanto a la conveniencia.

Para evaluar y comprender adecuadamente esas necesidades, las preocupaciones de seguridad física y sicosocial deben tomarse en consideración juntas, en esencia, se debe adoptar un enfoque holístico.[17]

1.4 APRENDIENDO DEL PASADO

Como la comunidad de soporte ha aprendido de las actividades desarrolladas en el pasado, las mejores prácticas en torno al apoyo de seguridad digital han evolucionado con el tiempo.

A medida que el uso de las tecnologías digitales ha aumentado, las intervenciones y prácticas de seguridad digital han evolucionado. El campo todavía es relativamente nuevo, pero ya hay lecciones que podemos aprender de lo que ha funcionado en el

pasado y lo que no, y asegurarnos de que ese aprendizaje nos sirve de base a medida que crece la comunidad de apoyo de seguridad digital.

La siguiente tabla resume las tendencias de cómo estas prácticas han cambiado con el tiempo, según nuestras entrevistas y análisis.

Sin embargo, vale la pena señalar que los diferentes proveedores de apoyo de seguridad digital podrían estar en desacuerdo con este análisis, especialmente en la elección de herramientas de software.

Tema	Enfoque antiguo	Enfoque actual
Enfoque	No causar daño	Reducción de daños[18]
Herramientas de Software	Solo software libre y de código abierto	Supeditado al contexto y la capacidad de los usuarios, lo que podría resultar en la elección de una opción propietaria
Frecuencia	Entrenamientos puntuales, a menudo a cargo de entrenadores no familiarizados con el contexto o la cultura[19]	Intervenciones a largo plazo para aumentar la capacidad de la comunidad en cuestión.
Soluciones sugeridas	Una fórmula universal, que usa recursos "globales".	Priorizar diferentes contextos exige soluciones diferentes.

DILEMMA

ESCOGER SU SOFTWARE

El apoyo de seguridad digital va de la mano con el software libre y de código abierto (FOSS por su sigla en inglés)

Para los seguidores de este punto de vista, recomendar cualquier solución de software que no sea FOSS se considera irresponsable. Los proveedores de apoyo de seguridad digital que promueven únicamente soluciones FOSS creen que cualquier otra cosa a la larga es perjudicial. Las ganancias a corto plazo en cuanto a facilidad de uso y conveniencia se contrarrestan, de muchas maneras, con las pérdidas de control y privacidad, y para algunos, el uso de la solución propietaria es en sí misma un paso en falso en materia de seguridad digital. Por ejemplo, cualquier software que almacene sus datos en 'la nube' podría, en el peor de los casos, estar disponible para las autoridades y poner en riesgo a la organización y, potencialmente, a las personas reflejadas en esos datos.

VS.

El apoyo de seguridad digital debe basarse en las prácticas existentes. Si esto significa recomendar soluciones de software propietario, entonces esa es la medida a adoptar más responsable.

En cierto modo, este enfoque equilibra la tensión existente entre tener más control sobre su tecnología, con la posibilidad de carecer de la capacidad interna para ejercer ese control, o corregir los errores que la acompañan. Las soluciones propietarias a menudo son más fáciles de configurar y de usar.

Nuestra opinión:
Adoptamos un enfoque pragmático para las soluciones de software, y señalamos que, siempre que sea posible, las opciones de código abierto son, a la larga, la mejor opción para las organizaciones que luchan por la justicia social. Las decisiones técnicas son políticas, y la usabilidad de las herramientas de código abierto no mejorará a menos que más personas dediquen recursos para usar y mejorar esa experiencia. Dicho esto, también hemos visto casos en los que los capacitadores de seguridad digital han recomendado soluciones de código abierto a organizaciones que, cuando fallan o no se utilizan exactamente conforme a lo previsto, en última instancia las ponen en mayor riesgo.[20] Con esto en mente, fomentamos una evaluación caso por caso de las herramientas de software, teniendo en cuenta el entorno de trabajo actual de la organización, su capacidad interna y sus objetivos políticos. En última instancia, las organizaciones deben estar facultadas para tomar la mejor decisión para ellos, por lo que nos esforzamos por proporcionarles información bien equilibrada y apoyarlos en lo que decidan hacer.

DESTACADO

PROVEEDORES COMERCIALES

Los proveedores comerciales están llenando un vacío en el espacio de seguridad digital y servicios tecnológicos. Algunos se centran explícitamente en la prestación de servicios a organizaciones sin fines de lucro, pero la mayoría tiene un mandato más amplio, que atiende a una variedad de clientes.

El rol de los proveedores comerciales en el ecosistema

Los entrevistados sugirieron varias funciones que los proveedores comerciales podrían desempeñar:

Proporcionar apoyo directo a través de contratos pagados: las opiniones se dividieron en gran parte sobre si los proveedores comerciales proporcionaban apoyo de seguridad digital útil para el sector sin fines de lucro. En términos generales, las organizaciones con identidades políticas más fuertes -para quienes sus socios, sus políticas y sus elecciones técnicas forman parte de su identidad y, por lo tanto, de su trabajo- rechazaron a los proveedores comerciales por no entender el contexto en el que estaban trabajando. Para otros, sin embargo, los proveedores comerciales estaban llenando un vacío en el ecosistema de apoyo.

> *Advertencia:* los entrevistados generalmente estuvieron de acuerdo en que la calidad del apoyo brindado por los proveedores comerciales a clientes sin fines de lucro fue menor de lo esperado. Un entrevistado especuló que esto se debía a que los clientes sin fines de lucro se contaban entre los clientes más pequeños y de pagos más bajos, y como resultado, tenían una menor prioridad para el proveedor.

Proporcionar experiencia voluntaria: otros, especialmente aquellos con experiencia en el sector privado, señalaron que las habilidades aprendidas por los trabajadores técnicos en el sector privado eran mucho más avanzadas que las de aquellos que trabajan exclusivamente en organizaciones sin fines de lucro. Las oportunidades para el avance técnico fueron más pronunciadas; había más oportunidades para aprender de sus compañeros y trabajar en equipos técnicos, en lugar de ser el único asesor técnico; y el sector privado atrajo a trabajadores inteligentes y calificados.

También señalaron, sin embargo, que las organizaciones sin fines de lucro probablemente nunca podrían competir en términos de salario y beneficios ofrecidos por el sector privado, y como tal, sugirieron que la forma más realista de aprovechar esa experiencia era mediante la creación de **vías voluntarias** para que las personas que trabajan en el sector privado puedan colaborar.

ESTUDIO DE CASO

ORGANIZACIONES SIN FINES DE LUCRO QUE USAN HERRAMIENTAS PROPIETARIAS

Aprendizaje clave: aunque esta es una opinión potencialmente impopular entre algunos expertos en seguridad digital, algunas herramientas propietarias pueden ser más utilizables y accesibles para organizaciones sin fines de lucro, ya sea porque las versiones de código abierto requieren más habilidades técnicas para configurarlas, no son amigables con el usuario, o por otras razones.

No podemos comentar sobre el estado de seguridad de esta herramienta específica, pero un entrevistado nos dijo que Salesforce CRM, que ofrece una versión sin fines de lucro al 76% del costo comercial, ha contribuido enormemente tanto con su trabajo como con el de muchas organizaciones afines del sector. Confían en el equipo de seguridad que protege a Salesforce, e indicaron que nunca había sido hackeado, considerándolo tan "seguro como puede ser".

"Todos estamos en Salesforce CRM ... crearon una versión específica para uso sin fines de lucro. Ha sido el desarrollo más impactante en el sector. Es la cuarta empresa más grande del mundo: nunca ha sido hackeada, es tan segura como es posible serlo".

La comprensión de las amenazas a la seguridad en todo el mundo están limitadas por puntos ciegos creados como resultado de que los investigadores se focalizan en áreas específicas y de campañas de concientización estrechamente definidas.

Esto significa que los análisis globales centrados en áreas afectadas por problemas tales como la alta incidencia de malware no siempre representan la imagen global con precisión. Una variedad de factores contribuyen a esto, como la disponibilidad de recursos de financiación para la investigación en áreas geográficas particulares, combinado con una mayor alfabetización entre la sociedad civil en esas áreas, lo que significa que es más probable que señalen amenazas particularmente preocupantes; o una atención creciente debida a eventos políticos, o una mayor conciencia o capacidad de respuesta ante amenazas a la seguridad en ciertas regiones si se perciben como incidentes de "mayor visibilidad" en todo el mundo.

ESTUDIO DE CASO

INVESTIGACIÓN CIRCUNSCRIPTA A ZONAS PRIORITARIAS

Aprendizaje clave: la comprensión actual de las amenazas técnicas está impulsada por la inversión destinada a investigar y entender la seguridad digital en áreas geográficas específicas, en lugar de ser un indicador de las zonas con una mayor frecuencia de incidentes.

Un entrevistado que trabajó anteriormente como investigador de seguridad destacó que las áreas de interés para la investigación "crean una narrativa" que producirá más en la misma línea de trabajo. Por ejemplo, los entrevistados sugirieron que debido a que hay más recursos dedicados a comprender las amenazas digitales que enfrentan México o Siria, las personas que trabajan en esas zonas se vuelven más conscientes de las amenazas que podrían enfrentar. En consecuencia, acumulan más capacidad para reconocer esas amenazas, fortaleciendo una vez más esta narrativa.

Incluso cuando se ha brindado apoyo de seguridad digital, a menudo es incompleto. En muchos casos, los mecanismos de monitoreo y evaluación no están incluidos o no brindan información útil para permitir la iteración y la mejora.

En el pasado, las métricas relacionadas con el apoyo de seguridad digital se han centrado en datos de fácil recopilación, como el número de visitas a un recurso en línea o el número de asistentes a una capacitación de seguridad digital en particular. Ninguno de estos puntos de datos indica la forma en que se recibió el apoyo y el impacto que tuvo a largo plazo.

1.5 REPENSANDO LA "EXPERIENCIA"

Cuando alguien se siente amenazado, las reacciones iniciales se centran en el miedo, por lo que es clave tener a alguien que al responder brinde apoyo emocional, en la forma de escuchar, de comprender cuál es el problema y qué tipo de respuestas podrían ser apropiadas. Pero bajo el modelo actual, los expertos técnicos a menudo son el primer puerto de escala para las personas que necesitan apoyo de seguridad digital. Esto tiene una serie de consecuencias perjudiciales:

Cuando alguien se siente amenazado, las reacciones iniciales se centran en el miedo, por lo que es clave tener a alguien que al responder brinde apoyo emocional, en la forma de escuchar, de comprender cuál es el problema y qué tipo de respuestas podrían ser apropiadas. Pero bajo el modelo actual, los expertos técnicos a menudo son el primer puerto de escala para las personas que necesitan apoyo de seguridad digital. Esto tiene una serie de consecuencias perjudiciales:

- Combina la demanda de apoyo emocional y técnico cuando se es víctima de un ataque.

- Significa que todas las solicitudes de apoyo de seguridad digital van a personas técnicamente capacitadas, incluso las que no requieren soporte técnico, lo que puede obstaculizar la coordinación y la provisión de apoyo adecuado.

- Disminuye las posibilidades de que personas sin capacitación técnica se sientan capaces de asumir funciones clave con respecto a la seguridad digital, manteniendo así el statu quo relativamente homogéneo en el espacio de seguridad digital.

• Devalúa la contribución de los expertos no técnicos que trabajan en el gran ecosistema de seguridad digital, y reduce la eficacia del ecosistema en su conjunto, creando cuellos de botella en torno a los expertos técnicos.

DESTACADO

EL MODELO DEL HÉROE

Durante nuestras entrevistas, pedimos recomendaciones acerca de con qué otras personas deberíamos hablar. Muchos entrevistados nos recomendaron hablar con las mismas personas, que claramente juegan un papel clave dentro de la comunidad de provisión de soporte y que tienen redes amplias.

El número de veces que se nos recomendó a estas personas sugiere que es probable que reciban muchas solicitudes de apoyo y, de manera más amplia, que este enfoque de la provisión de apoyo no podría potenciarse.

Un entrevistado describió esta estructura como el "modelo del héroe", en el que determinadas personas son consideradas "héroes". Esto dificulta que los recién llegados se unan a estos proveedores de soporte y crea cuellos de botella en torno a la cantidad de asistencia que pueden brindar. Algunas de las personas recomendadas identificaron explícitamente que necesitan más apoyo de los administradores de la comunidad o de personas que podrían clasificar las solicitudes, lo que sugiere que el modelo del héroe no funciona para nadie.

A partir del 2017 ha salido a la luz una consecuencia particularmente grave del modelo del héroe: la del abuso de poder. Una concentración de poder sin controles de rendición de cuentas ni equilibrios no es saludable en ninguna comunidad, y las denuncias sobre presuntas agresiones sexuales que han surgido en los últimos meses demuestran ese punto, con devastadoras consecuencias.[21]

ESTUDIO DE CASO

APOYO DE SEGURIDAD BASADO EN EL CONTEXTO

Aprendizaje clave: los proveedores de apoyo de seguridad digital capaces de comprender los problemas de las comunidades a las que buscan apoyar son buscados y percibidos como mejor capacitados para brindar el apoyo de seguridad digital apropiado.

El Proteus Fund es un financiador intermediario con sede en los Estados Unidos que canaliza de manera estratégica fondos de fundaciones y donantes individuales para apoyar el trabajo de promoción progresista.

El Security & Rights Collaborative (SRC) es una iniciativa del Proteus Fund que recauda dinero y otorga fondos para fomentar a organizaciones musulmanas, árabes y del sur de Asia (MASA), coordina los esfuerzos de políticas y promoción en los EE. UU., y proporciona apoyo estratégico y asistencia técnica para el resto del área de MASA. En el 2016 y 2017, el SRC solicitó apoyo de seguridad digital para sus beneficiarios, y describió cómo priorizaron la búsqueda de un proveedor de soporte que pudiera ser "alguien de la misma comunidad porque podían conectarse más, hay una experiencia compartida", particularmente con respecto a entender la intersección de ataques físicos con ataques digitales para los organizadores y las comunidades de MASA. Querían "no solo un experto en seguridad digital, sino alguien que fuera capaz de interactuar realmente con nuestros beneficiarios", y terminaron eligiendo un grupo sudasiático - norteamericano de derechos humanos para liderar un proyecto sobre seguridad y protección digital.

Múltiples entrevistados nos hablaron acerca de la necesidad de contar con proveedores de apoyo que tuvieran suficiente experiencia técnica y confianza para hablar con las personas cuando necesitaban apoyo de seguridad digital o se sentían amenazadas. Muchos tuvieron experiencias personales o de segunda mano en las que entraron en contacto directamente con personas que priorizaron las soluciones técnicas sobre las emocionales y sufrieron los consiguientes efectos negativos en su motivación y bienestar.

Algunos calificaron estos roles como "traductores" o "guardianes tecnológicos", mientras que otros los describieron como "facilitadores" que podían entender las necesidades y facilitar la relación entre un proveedor de soporte más técnico y un destinatario. Otros incluso describieron el papel simplemente como un "intermediario" entre los desarrolladores de herramientas y los usuarios finales, que puede agregar patrones y descubrir los principales puntos débiles.

La falta de diversidad en la comunidad de apoyo de seguridad digital significa que las herramientas, recursos y espacios se crean predominantemente para ciertos tipos de usuarios, y no para otros. Esto va en detrimento de su uso y efectividad.

Los entrevistados citaron algunos obstáculos para proporcionar recursos útiles para las comunidades con las que trabajaron: "hay tantas comunidades donde no hay herramientas en el idioma local, o no hay herramientas apropiadas para el contexto, como herramientas que necesitan una fuerte conexión a Internet para funcionar, o herramientas a las que solo se puede acceder desde una computadora de escritorio".

Otros mencionaron que los casos de uso más notables planteados provienen de una comunidad relativamente homogénea, blanca y dominada por hombres, lo que significa que los problemas que se trabajan podrían no ser los problemas de seguridad digital más apremiantes, sino aquellos que afectan a las personas presentes en la comunidad de seguridad digital. La comunidad de apoyo se describió como un "círculo interno" de personas que "tienen tiempo para asistir a conferencias, viajar internacionalmente y crear recursos", lo que dificulta que los recién llegados, especialmente los menos dotados de recursos, se unan.

2. Viajes organizacionales

Para evaluar y comprender adecuadamente el **ecosistema de apoyo de seguridad digital,** buscamos primero comprender, desde una perspectiva organizacional e institucional, las **necesidades de la sociedad civil** de este sistema de apoyo.

Priorizamos un enfoque de primero-el-problema, buscando identificar las necesidades y los comportamientos a su alrededor. En respuesta a esto, identificamos aquí tres arquetipos organizacionales típicos, clasificándolos en términos de la prioridad que otorgan a la **promoción de prácticas saludables de seguridad digital:**

- Desconocimiento: donde la seguridad digital no es una prioridad
- Aprendizaje: donde la seguridad digital se ha identificado como una prioridad creciente
- Dominio: donde la seguridad digital es una alta prioridad

La seguridad digital es multifacética, lo que significa que una organización podría pasar del "Desconocimiento" al "Aprendizaje" y al "Dominio" en lo que respecta a una práctica en particular, pero ser catalogada en el "Desconocimiento" en otra práctica.

Ejemplo: una organización de la sociedad civil se da cuenta de que alguien está intentando acceder a su sitio en Wordpress, que tiene cientos de usuarios con varios niveles de permisos de usuario.

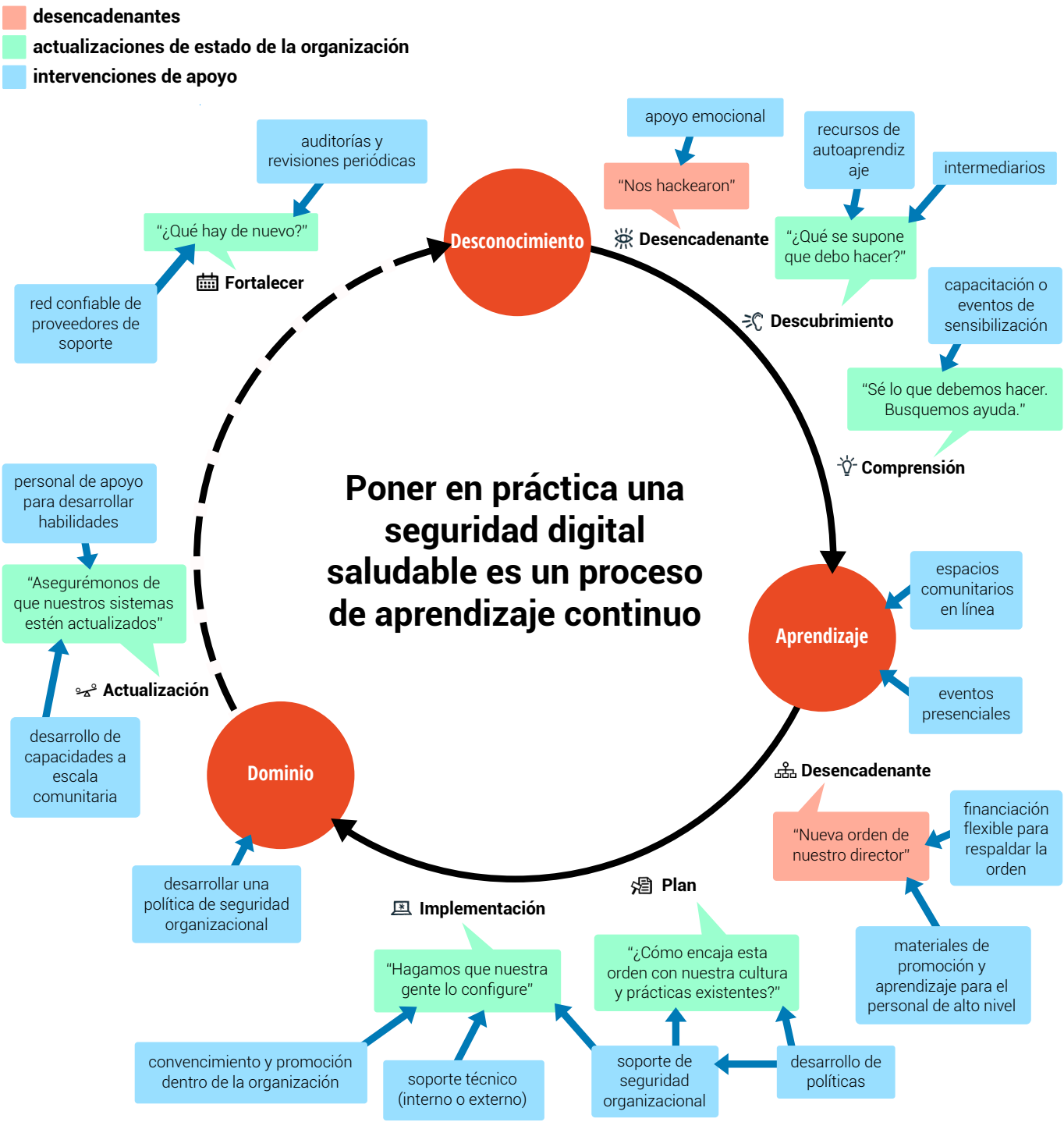
- [DESCONOCIMIENTO] En el pasado, dieron la bienvenida a cualquiera que quisiera contribuir a su sitio, y tener una cuenta de Wordpress es parte del proceso de incorporación.
- [APRENDIZAJE] Se dan cuenta de que tener tantas cuentas significa que su sistema tiene más vulnerabilidades de las necesarias. No están seguros de qué cuentas aún están activas y quién realmente necesita ciertos permisos de usuario, por lo que llevan a cabo una auditoría para comprender el estado actual.
- [DOMINIO] Establecen una política para definir qué clase de usuarios necesitan qué tipo de permisos. Explican esto a todos en la organización, junto con los motivos para adoptar esta política, y todos están de acuerdo en implementarla. A partir de ahora, a los usuarios nuevos se les asigna el nivel más bajo de permisos necesario, revisan las cuentas de los usuarios cada pocos meses y eliminan regularmente las cuentas inactivas.

De esta manera, se han movido a lo largo del ciclo de práctica de la seguridad digital saludable en un aspecto particular, pero hay muchos más comportamientos para alentar y apoyar.

Ejemplo: una organización de la sociedad civil descubre que una organización similar ha sido recientemente objeto de un ataque de phishing: se envió un correo electrónico a varios miembros de la organización, simulando ser una compañía con la que interactuaban regularmente. No están seguros de si este fue un ataque dirigido, pero de todos modos, les preocupa que podrían ser objeto del mismo tipo de ataque.

- [DESCONOCIMIENTO] En el pasado, los miembros del personal cliqueaban en enlaces de compañías externas sin verificar la legitimidad de ese enlace, o del remitente.

CICLOS DE SEGURIDAD DIGITAL PARA ORGANIZACIONES



La seguridad digital es multifacética, lo que significa que una organización podría pasar del **Desconocimiento** al **Aprendizaje** y al **Dominio** en lo que respecta a una práctica en particular, pero ser catalogada en el **Desconocimiento** en otra práctica.

• [APRENDIZAJE] Se dan cuenta de que esto podría ponerlos en riesgo (y a las comunidades con las que trabajan, ya que tienen información confidencial sobre esas comunidades en sus computadoras de trabajo). Como primer paso, solicitan a todos que reenvíen correos electrónicos que mencionen esta empresa a un investigador de malware con quien están trabajando, y realizan capacitaciones de sensibilización para ayudar al personal a detectar factores desencadenantes que pueden indicar ataques de phishing en lugar de correos electrónicos del remitente real.

• [DOMINIO] La detección de ataques de phishing se convierte en parte del proceso de incorporación regular para los nuevos miembros del personal; todos los miembros del personal saben a quién remitir los ataques sospechosos y cómo detectar correos electrónicos de phishing, y publican una guía paso a paso para cualquier persona que necesite información de actualización, también documentan y muestran su proceso para inspirar a otras organizaciones similares a hacer lo mismo.

Ejemplo: una organización de la sociedad civil tiene datos personales sobre el estado inmigratorio de las personas con las que trabaja, y el contexto político cambia drásticamente con respecto a la inmigración. Esto significa que la información que guardan es repentinamente muy sensible y podría poner a muchas personas en riesgo si de alguna manera se hiciera pública, y que ahora tienen más adversarios que potencialmente buscan obtener esta información.

• [DESCONOCIMIENTO] Anteriormente entendían que esta información podría ser delicada, pero decidieron que la recopilación de datos sobre el estado migratorio les proporcionaba una mejor capacidad para comprender a sus comunidades y poder satisfacer sus necesidades. Lo almacenaron en un disco duro compartido, pero a medida que la organización creció, cada vez más personas terminaban necesitando acceso y hacían copias en sus propias computadoras para facilitar el acceso.

• [APRENDIZAJE] Se dan cuenta de que en el clima actual, incluso la posesión de esta información es peligrosa. Se ponen en contacto con un especialista en desidentificación que es recomendado por uno de los miembros de su personal, que examina un subconjunto de los datos y les aconseja que eliminen la mayoría de los elementos, excepto los que realmente necesitan. Piden a todos los miembros del personal que eliminen todos los datos de sus propias computadoras, explicando por qué es tan importante. Siguen los consejos del especialista y guardan los datos restantes en dos discos duros que cifran con contraseñas que solo un par de personas de la organización conocen.

• [DOMINIO] A partir de ahora, practican la "minimización de datos", recolectando solo los datos que realmente necesitan. Para acceder a la base de datos, el personal tiene que pedirle a una de tres personas que ingrese la contraseña, y la base de datos está muy reducida en comparación con la versión original. Rutinariamente cambian la contraseña, y ambos discos duros se mantienen en instalaciones físicamente seguras.

2.1 ORGANIZACIONES EN ETAPA DE DESCONOCIMIENTO

Historia: una organización en etapa de **desconocimiento** *arquetípica carece de personal de tecnología básica dentro de su plantilla. Su personal no se considera lo suficientemente "capacitado en tecnología" como para abordar cuestiones de seguridad digital, y tienen poco o ningún conocimiento de la misma, y no tienen un presupuesto dedicado a la seguridad digital. Cuando se trata de tecnología, sus prioridades son la comodidad y / la experiencia previa, es decir, herramientas con las que las personas ya están familiarizadas. Tienden a utilizar soluciones tecnológicas listas para usar, y como ejemplo, es posible que no hayan activado la Autenticación de dos factores, si no viene de forma automática.*

Controlando la seguridad digital

El mayor obstáculo para la construcción de mejores prácticas de seguridad digital entre la sociedad civil fue la falta general de comprensión de lo que implica la seguridad digital.

Las consecuencias de esta brecha en la comprensión son de gran alcance e incluyen:

• En general relegar la seguridad digital dentro de las prioridades de la organización (presupuesto, personal, implementación de políticas), a menudo sin darse cuenta de cómo la seguridad digital interviene y afecta la implementación de otras prioridades centrales.

• Prácticas de tecnología digital inseguras dentro de las organizaciones (por ejemplo, compartir contraseñas, almacenar datos confidenciales en lugares de fácil acceso o no actualizar el software regularmente).

• Los socios o proveedores comerciales contratados para proporcionar soporte técnico no son los más apropiados, lo que puede llevar a un asesoramiento inadecuado o a prácticas de seguridad insostenibles.

• Falta de apoyo para las personas que buscan impulsar las prácticas de seguridad digital dentro de una organización, ya sea que se trate de oportunidades de desarrollo profesional para los responsables de la seguridad digital o de la creación involuntaria de barreras para que esas personas implementen mejores prácticas de seguridad digital dentro de una organización.

Muchos entrevistados nos dijeron que la seguridad digital se ha percibido tradicionalmente como un acto e intervención puramente técnica, con muchos recursos o herramientas vistos como inaccesibles u hostiles para quienes carecen de formación técnica. Los entrevistados identificaron la tecnología y la seguridad como "intimidantes y fuera de su ámbito", mientras que los expertos en seguridad digital técnica fueron descritos como "poco accesibles".

Este enfoque también prevaleció en cómo son percibidas las comunidades de seguridad digital. Esto crea una barrera para los recién llegados que buscan unirse y aprender de las comunidades enfocadas en la seguridad digital.

Para las organizaciones basadas en una misión y que están en la categoría de desconocimiento, gastar dinero en seguridad digital es una prioridad menor. Otras prioridades más visibles la preceden (como destinar fondos a las comunidades afectadas o al personal). Esto afecta el impacto que los financiadores pueden tener cuando pretenden que sus beneficiarios gasten dinero en seguridad digital, pero no destinan fondos de manera explícita. Si después de la concientización no se fomenta el apoyo, contemplar la seguridad digital puede parecer un ejercicio de rellenado de casilleros para el beneficiario.

El fortalecimiento de la seguridad digital de una institución a menudo puede ser mucho menos tangible y visible que el respaldo de otros tipos de seguridad (por ejemplo, la seguridad física) o la dirección de recursos hacia las comunidades afectadas.

Pasando del desconocimiento al aprendizaje

En términos generales, tiende a haber un disparador particular que estimula esta transición. Podría ser cualquiera de los siguientes:

• Experimentar un ataque o violación de seguridad digital de primera mano: la motivación comienza desde un lugar de miedo

• Aprendizaje de compañeros que experimentan fallas de seguridad digital

• Cambios dramáticos en el contexto político, resultan en cambios dramáticos en la forma en que una organización percibe su propia posición.

ATAQUES QUE ENFRENTAN LAS ORGANIZACIONES SIN FINES DE LUCRO

Los entrevistados describieron haber sido testigos de primera o segunda mano de diversos tipos de amenazas que enfrentan las organizaciones sin fines de lucro, entre ellas:

• *Crypto-ransomware,* donde los archivos son encriptados y solo se liberan tras el pago a través de un determinado software malicioso (conocido como malware). Si esto sucede, la persona bajo ataque ve un mensaje pidiendo que se pague un rescate para recuperar el acceso a su computadora y archivos.

• Violaciones de datos, generales o específicas en momentos particularmente oportunos, como durante las semanas previas a un gran evento comunitario.

• Incursiones físicas en las oficinas

• Amenazas legales: usar instrumentos legales particulares para cerrar las organizaciones o señalar a las autoridades que una organización puede estar excediendo su estatus de "no cabildeo" (es decir, organizaciones regidas por la sección 501 (c) 3 del Código de Rentas Internas de Estados Unidos)

• Correos de phishing (suplantación de identidad)[22]

• Malware dirigido

• Virus generales: en una encuesta realizada en todo el campo por Idealware con Immigration Advocates Network en junio del 2016 sobre las necesidades tecnológicas de los grupos de derechos de inmigración, el 20% de los participantes dijo que las computadoras de su organización habían sido infectadas con virus el año anteriors.[23]

Tipos de apoyo útiles

Cuando las personas o las organizaciones pasan del "Desconocimiento" al "Aprendizaje" (sobre todo si la motivación es el miedo o el riesgo de ataque), los expertos que pueden brindar apoyo emocional son más útiles como primer recurso que los expertos técnicos.

ESTUDIO DE CASO

COMPRENSIÓN DE LAS NECESIDADES EMOCIONALES

Aprendizaje clave: para abordar las amenazas a la seguridad digital el apoyo emocional puede ser tan valioso y necesario como las intervenciones técnicas.

Las personas dentro de la red de Global Voices a veces se comunican con el personal central después de experimentar fallas de seguridad digital o amenazas. Su Director de Defensa, después de haber tratado con varias personas que requirieron apoyo, compartió un aprendizaje clave:

"Hemos aprendido que cuando las personas se acercan necesitan que las escuchen, que no les pidan que hagan algo técnico".

Los gestores comunitarios y encargados de brindar primeros auxilios que puedan satisfacer con éxito las necesidades son particularmente necesarios en esta etapa, por varias razones:

• Para ofrecer una experiencia más acogedora para las personas y organizaciones que están pasando del "Desconocimiento" al "Aprendizaje".

• Para reducir la cantidad de trabajo que recae en los expertos técnicos, y permitirles trabajar en los casos en los que su experiencia técnica particular es más relevante.

• Para hacer que la provisión de soporte sea más amplia y accesible para los recién llegados, y aumentar la probabilidad de que los recién llegados ingresen al espacio de provisión.

ESTUDIO DE CASO

SECURITY WITHOUT BORDERS

Aprendizaje clave: la gestión comunitaria dedicada es una parte clave del desarrollo de comunidades saludables, y llevar a cabo una buena gestión comunitaria requiere un conjunto diferente de habilidades para aportar experiencia técnica a la propia comunidad.

Security Without Borders se creó en el 2016,[24] y fue citado por muchos como un recurso enormemente útil. Es un colectivo abierto de hackers y profesionales de la seguridad que brindan asistencia técnica a la sociedad civil y activistas que se dedican a la protección de los derechos humanos fundamentales. Fue fundado con el objetivo de permitir que los profesionales de la seguridad (del sector privado) colaboraran con la sociedad civil.[25] Uno de los miembros del equipo central nos dijo:

"Hubo mucha disfunción al principio, con cientos de personas que querían hacer cosas. Tomó un tiempo superar esa fase, y ahora tenemos un núcleo de personas comprometidas a quedarse... Hay una prioridad mayor: descubrir cómo tratar con las personas. No hemos encontrado una buena manera de administrarnos a nosotros mismos y a los demás. Lo hacemos en nuestro tiempo libre y ninguno de nosotros es un buen gestor de la comunidad".

Su diagnóstico: **tener un gestor comunitario** aumentaría enormemente su efectividad como red, ayudándoles a:

- Diseñar procesos efectivos para la admisión.
- Tener llamadas iniciales de selección para entender cuáles son las necesidades de las personas y el tipo de experiencia o apoyo de seguridad que necesitan.
- Organizar a las personas que quieran aportar su experiencia e idear algo ligero pero útil para que contribuyan con su experiencia.

En nuestra fase de entrevistas, se destacó más claramente el enfoque de centrarse únicamente en expertos técnicos, muchos entrevistados recomendaron a los mismos expertos (en gran parte técnicos) como proveedores de apoyo de seguridad digital útil, o como expertos con los que deberíamos hablar.

Para que los recursos de seguridad digital sean efectivos en la transición del "Desconocimiento" al "Aprendizaje", deben ser prácticos, procesables y alcanzables. Muchos recursos existentes en torno a la seguridad digital están escritos para audiencias en gran parte "generales", y en su intento de atraer a todos, terminan por no atraer a nadie.

Las críticas particulares planteadas mencionaron que algunos recursos describen las tareas y el apoyo de seguridad digital como "fáciles" o "simples", lo que hace que las personas que luchan con esas tareas sientan que no están lo suficientemente calificadas como para seguir adelante.

Los recursos dirigidos explícitamente a los principiantes existen, y muchos de ellos parecen haber sido creados hace relativamente poco tiempo (en el último año más o menos). Ejemplos notables incluyen Signal for Beginners de Martin Shelton,[26] o más recientemente, Recursos Net Alert del Citizen Lab, con "consejos fáciles para mantener sus cuentas seguras",[27] o su Agenda de seguridad, que anima a las personas a "mejorar su seguridad en línea con el asesoramiento de expertos".[28]

La provisión de recursos y apoyo de seguridad digital actualmente no reconoce diferencias generacionales en las necesidades y enfoques, y tiende a dirigirse a audiencias más jóvenes. Esto crea una barrera para las personas en posiciones de liderazgo en organizaciones que provienen de generaciones anteriores, y que tienen pocas opciones disponibles diseñadas explícitamente para su experiencia.

En muchas organizaciones, las personas en puestos de liderazgo son personas mayores con más experiencia en el sector y posiblemente (aunque no siempre) menos experiencia en tecnología que sus colegas más jóvenes. Para los paladines internos que buscan aumentar la seguridad digital en las prioridades de una organización, convencer a quienes están en los niveles

más altos de toma de decisiones de la organización puede ser una gran barrera.[29]

La confianza es la clave. La construcción de un ecosistema de apoyo saludable requiere que las organizaciones de la sociedad civil establezcan relaciones con los proveedores de apoyo como una práctica continua. Esto se debe a que, para muchos grupos (en particular para las comunidades guiadas por una misión o vulnerables), la provisión de apoyo de seguridad digital depende de las relaciones de confianza existentes.

Como nos dijo Bex Hurwitz de Research Action Design, el primer puerto de escala para las organizaciones que necesitan cualquier tipo de apoyo, especialmente el relacionado con la seguridad, es gente de confianza. Como resultado, algunos proveedores de soporte incorporan esto de manera explícita a la forma en que brindan apoyo, asegurándose de "seguir avanzando a un ritmo en el que podamos mantener y generar confianza en el tiempo".

Los entrevistados notaron reticencia entre las comunidades con las que trabajaron para acercarse a organizaciones que se consideran enfocadas en seguridad digital, diciendo que "es poco probable que la gente decida no escatimar esfuerzos para encontrar recursos, o para contactarse con personas dedicadas específicamente a la seguridad digital".

Fortalecer las capacidades de provisión de apoyo de seguridad digital en las comunidades que trabajan en la primera línea requiere brindar apoyo para su bienestar a lo largo del tiempo, así como fortalecer sus conocimientos técnicos. Para que las personas se sientan cómodas aprendiendo sobre la seguridad digital, necesitan que se atiendan sus necesidades generales de recursos humanos, como los ingresos financieros regulares y los derechos laborales generales.

2.2 APRENDIZAJE

Historia: dentro de una organización típica en la etapa de "aprendizaje", al menos un miembro del personal es consciente de la importancia de la seguridad digital y está buscando formas de impulsarla dentro de la organización. Su prioridad es la defensa interna y el fomento del conocimiento y las habilidades propias. Podría haber recibido uno o dos entrenamientos, y sentirse un poco abrumado con consejos e inseguro sobre el modo de implementarlos. Usa recursos existentes / en línea para aprender más sobre seguridad digital.

El desencadenante para pasar del "Desconocimiento" al "Aprendizaje" a menudo es convencer al personal directivo de la importancia de la seguridad digital y

ESTUDIO DE CASO

— IMPULSAR LA CAPACIDAD TÉCNICA Y LOS RECURSOS HUMANOS

Aprendizaje clave: las prácticas saludables de seguridad digital y las contribuciones de la comunidad se pueden potenciar teniendo en cuenta el bienestar general, a través del apoyo en el aspecto operativo y de recursos humanos.

Wellstone es una progresista organización de defensa que capacita a organizadores comunitarios, activistas estudiantiles, personal de campaña, candidatos progresistas y funcionarios electos. A través de su programa de Tecnología del Movimiento, Wellstone también trabaja con asociaciones afiliadas para capacitar a sus miembros o a su personal en seguridad digital.

Priorizan tanto el aumento de la capacidad técnica como el apoyo de recursos humanos, centrándose en la logística y la atención comunitaria. Su enfoque en la columna vertebral operacional de la creación de redes y comunidades les permite garantizar que su personal y los capacitadores adjuntos puedan percibir sus remuneraciones a tiempo, y recibir apoyo sobre la logística para llevar a cabo una capacitación, así como otros recursos humanos que les permite permanecer en la comunidad.

También es de destacar que Wellstone fue uno de los pocos proveedores de seguridad con los que hablamos que brinda apoyo financiero para que las personas asistan a sus capacitaciones y desarrollen sus habilidades. Por lo general, tener la oportunidad de asistir a un entrenamiento, o una capacitación de entrenadores, se presenta como una oportunidad no remunerada para mejorar las habilidades.

lograr su colaboración; obtener recursos de un proyecto para trabajar en el tema; u otro factor externo como la presión de grupo o del financiador. En esta etapa, los recursos de autoaprendizaje son útiles, como lo son los eventos presenciales, la documentación de pares sobre cómo abordaron los problemas de seguridad digital y demás.

Intervenciones de apoyo

La forma típica en que se producen los recursos y las guías en torno a la seguridad digital a menudo no refleja la velocidad con la que su contenido puede cambiar. Sin una comunidad dedicada a mantenerlos actualizados, los recursos estáticos se vuelven obsoletos rápidamente. Como resultado, puede ser difícil para los usuarios saber si los recursos existentes todavía son aplicables.

Producir nuevos recursos sin un plan continuo a largo plazo para las actualizaciones y estructuras de propiedad y responsabilidad claramente establecidas, no contribuye a un ecosistema de apoyo saludable.

Por lo general, los recursos se han producido como archivos PDF estáticos o, más recientemente, como sitios web o artículos. Debido a la naturaleza cambiante del espacio de seguridad digital, el contenido requiere actualizaciones periódicas y una forma de marcar contenido inadecuado. Sin embargo, rara vez está etiquetado explícitamente con su última fecha de actualización.

Los entrevistados con los que hablamos citaron los recursos de soporte de seguridad digital más populares como Security in a Box[30] (SIAB), de Tactical Technology Collective y Frontline Defenders, y Surveillance Self-Defense[31] (SSD) de Electronic Frontier Foundation. En el caso de SIAB, sin embargo, algunos entrevistados mencionaron que desconocían si el contenido se mantenía actualizado y de ser así quién se encargaba de hacerlo (como una métrica, al momento de escribir este informe en enero del 2018, la última publicación del blog es de abril del 2016) o que enviaron un correo electrónico a la dirección de contacto provista para notificarles sobre consejos desactualizados y no recibieron respuesta.

Muchas de estas preocupaciones podrían abordarse con un plan integral de comunicaciones que acompañe al recurso en sí. Como descubrimos a través de nuestra investigación documental, los sitios web que comparten recursos a menudo no se mantienen actualizados ni comparten información que aumentaría enormemente su usabilidad, como la "fecha de la última actualización". A partir del 2017, las mejores prácticas para compartir recursos incluyen contemplar una "Fecha de caducidad" para el recurso en sí;[32] y tener un proceso claro y activamente mantenido para reportar errores en el contenido.

También vale la pena señalar que, aunque estas guías están escritas para una audiencia general, los entrevistados de fuera de los Estados Unidos y Europa mencionaron que gran parte de los consejos dados no eran relevantes en sus contextos, así como algunos de los proveedores de apoyo que trabajan explícitamente con organizaciones de la sociedad civil de primera línea. Muchos de los recursos existentes no son específicos sobre su público objetivo, pero hacen una serie de suposiciones que excluyen a comunidades particulares. Un entrevistado nos dijo:

"En realidad, no hay nada en la seguridad digital tradicional para muchos de los grupos con los que trabajo. He realizado entrenamientos en los Estados Unidos, y hay muy poco que pueda decirles sobre seguridad digital a las mujeres trans de color que hacen trabajo sexual: la seguridad física debe prepararse desde el principio, y no está en la seguridad digital tradicional ".

Algunos grupos han realizado esfuerzos para satisfacer estas necesidades más acordes con cada contexto específico, tales como:

- Ciberseguridad para la violencia doméstica de Hackblossomal, al estilo Hágalo Ud. mismo.[33]
- Cibermujeres, una guía de autodefensa digital para mujeres defensoras de derechos humanos que trabajan en entornos de alto riesgo.[34]
- Cómo cifrar y eliminar rápidamente y en forma segura sus datos para los activistas que trabajan en la región del Golfo.[35]

(Nota: lo anterior es una lista no exhaustiva de consejos de seguridad digital específicos para un contexto determinado, destinados a ilustrar el concepto en lugar de proporcionar todos los recursos posibles).

Además, están surgiendo algunos recursos que están diseñados de una manera más interactiva, lo que permite a los espectadores recibir consejos adaptados a sus contextos específicos, como Security Planner del Citizen Lab.[36] Al momento de escribir en enero del 2018, el Planner está disponible únicamente en inglés y están previstas versiones en español y en

francés. También sigue la buena práctica mencionada anteriormente de señalar claramente la fecha de la última actualización.

CASE STUDY

PRODUCIR RECURSOS DE FORMAS MÁS DINÁMICAS Y FÁCILES DE ACTUALIZAR

Aprendizaje clave: los recursos de seguridad digital necesitan actualizarse regularmente; por lo que producirlos en formatos que sean fáciles de actualizar y compartir (como sitios web, en lugar de archivos PDF) es un buen principio de diseño.

Un entrevistado nos contó cómo al principio comenzaron a producir recursos de seguridad digital como archivos PDF para distribuirlos en la comunidad. En un momento dado, un traductor se puso en contacto para decirles que habían completado una traducción de uno de los recursos. Sin embargo, la guía que se había traducido tenía cuatro años y estaba completamente desactualizada.

La imposibilidad de marcar el contenido como desactualizado (especialmente para archivos PDF que podrían enviarse por correo electrónico como archivos adjuntos, independientemente del sitio web en el que están alojados), significaba que se habían desperdiciado recursos al traducir la guía. Después de este incidente, el entrevistado ahora prefiere crear recursos como páginas web y enlazar a los usuarios de modo que si las cosas cambian, la página se puede actualizar y los usuarios verán la versión más actualizada.

No es útil conocer los riesgos y amenazas que se enfrentan sin tener la facultad o capacidad para implementar soluciones contra esas amenazas. El solo hecho de tomar conciencia de los riesgos puede provocar más temor y / o impedir que las personas se relacionen con datos y tecnología en lo absoluto.

Los entrevistados describieron cómo recibir apoyo de seguridad digital sin pensar en la capacidad o conocimiento existente puede "asustar a las personas y convertirlas en miedosas". Otro describió cómo vieron a las organizaciones de la sociedad civil ser alentadas por financiadores a asistir a webinars y capacitaciones, a pesar del hecho de que no tenían capacidad para asistir a un gran número de eventos puntuales o para implementar ninguna de las prácticas recomendadas.

Las organizaciones que pretenden potenciar sus propias capacidades en materia de seguridad digital necesitan ser capaces de invertir en su infraestructura operativa. De lo contrario, no serán capaces de invertir en las soluciones que podrían encontrar. Esto podría resolverse con apoyo explícito mediante subvenciones.

Las organizaciones que reciben soporte básico en la etapa de 'aprendizaje' pueden tener demandas adicionales relacionadas con su infraestructura técnica o de seguridad digital, que a menudo pueden no ajustarse a los presupuestos de los proyectos. Sin fondos básicos para invertir en estas soluciones, tendrán dificultades para poder implementar el apoyo de seguridad digital y desarrollar una cultura organizacional orientada a la seguridad digital.

Por ejemplo, según un estudio realizado por Idealware y la Red de Defensores de la Inmigración sobre las necesidades tecnológicas de los grupos de derechos de inmigración, el 26% del personal comparte una computadora y casi el 52% no respalda los archivos regularmente.[37]

Seguridad digital, trabajando juntos

Debido a la naturaleza interconectada de las tecnologías digitales, las prácticas de seguridad digital deben enmarcarse como acciones colectivas a lo largo del tiempo para ser efectivas. Las acciones individuales no son suficientes.

Los recursos existentes y los consejos de seguridad digital a menudo brindan apoyo que solo es útil si quienes lo rodean también practican el mismo comportamiento, centrándose en el individuo y no en el grupo.

Ejemplos de este asesoramiento centrado en el individuo son, por ejemplo:

- Configurar PGP, *pero si usted es el único que lo usa, PGP no será útil para usted ni para quienes lo rodean.*

• Descargar Signal, *de manera similar, si ninguno de sus contactos está en Signal, puede usarlo pero sus conversaciones no serán cifradas.*

• Encriptar su disco duro: *si muchas personas tienen acceso a la misma información y ninguna de ellas encripta su disco duro, un disco duro encriptado no asegurará la información en última instancia.*

Para que las intervenciones de apoyo a la seguridad digital formen parte de un desarrollo institucional saludable, deben enmarcarse no como intervenciones aisladas, sino como parte de un enfoque de seguridad organizacional.

Como Becky Kazansky escribe acerca de su trabajo con los enfoques de seguridad digital para defensoras de los derechos humanos, "alentar el énfasis en el individuo como el lugar primario de responsabilidad para la protección contra el daño tuvo el efecto conveniente de desviar la atención de sus causas".[38] A diferencia de promover acciones individuales, adoptar un enfoque de seguridad organizacional reconoce la naturaleza colectiva de la seguridad digital y se basa en la cultura, el contexto, los hábitos y las prácticas existentes para desarrollar la capacidad de organización a largo plazo. También tiene en cuenta el contexto y permite a las personas diseñar intervenciones que conecten prácticas de seguridad saludables con la misión de la organización.[39]

Pasando del "Aprendizaje" al "Dominio"

Existe una gran falta de apoyo institucional para las personas de comunidades subrepresentadas que brindan apoyo de seguridad digital a sus comunidades y organizaciones. La falta de apoyo les dificulta involucrarse con la más amplia comunidad de seguridad digital, y como resultado, la comunidad no valora ni aprecia su trabajo y experiencia.

Proporcionar apoyo institucional y oportunidades de desarrollo profesional para las personas que operan fuera del ámbito de los proveedores de apoyo de seguridad digital más visibles les permitirá tanto crecer en su capacidad de brindar apoyo, como en la diversificación de la comunidad de seguridad digital en su conjunto.

ESTUDIO DE CASO

IMPULSAR LA SEGURIDAD ORGANIZACIONAL

Aprendizaje clave: Proporcionar espacio dentro de la comunidad para las personas responsables de impulsar la seguridad digital de las organizaciones es una buena manera de facilitar el aprendizaje más allá de las fronteras y las organizaciones, y proporcionar apoyo de pares para personas que a menudo están trabajando solas.

Orgsec.community[40] es una comunidad de práctica que trabaja para fortalecer la conciencia, la capacidad y la confianza de los defensores de los derechos humanos y las organizaciones de la sociedad civil a fin de impedir amenazas a la seguridad. La primera convocatoria de 15 profesionales tuvo lugar a principios del 2016, y desde entonces la red ha crecido hasta incluir a más de 100 miembros de todo el mundo.

El apoyo de seguridad organizacional comprende un proceso complejo, evolutivo y multifacético que conduce a las organizaciones a través de una serie de fases: descubrimiento, estrategia, implementación y construcción de confianza, acompañadas por un profesional de la organización a lo largo de una serie de meses o, en algunos casos, de años de apoyo.

Ahora, es una lista de correos a la que se accede solo por invitación que actúa como un grupo de debate para compartir experiencias y crear enfoques estandarizados y accesibles para la seguridad organizacional. Comparten recursos, desafíos, mejores prácticas y aprendizajes de sus diversos enfoques y trabajo continuo.

Las organizaciones que han pasado por un ciclo de aprendizaje de seguridad digital también podrían pensar en fomentar una mejora en la salud a largo plazo de las comunidades de las que forman parte. Esto podría significar:

• Tomarse el tiempo para documentar el proceso que atravesaron

• Apoyar activamente o asesorar a organizaciones similares que tienen habilidades de seguridad digital menos avanzadas

• Compartir aprendizajes en espacios comunitarios para crear conciencia sobre las necesidades de seguridad digital, actividad destinada a organizaciones similares y otras

• Proporcionar espacios para que las personas de comunidades subrepresentadas aprendan más sobre la seguridad digital y se inicien en el ámbito de los proveedores de apoyo.

2.3 DOMINIO

Historia: con una organización típica que se encuentra en la etapa de "dominio", hay un compromiso de la dirigencia sobre la importancia de la seguridad digital y un presupuesto apropiado dedicado a garantizar que la organización tenga sistemas seguros y soporte tecnológico. Para algunas organizaciones, esto podría significar tener alguien en el personal que sea responsable por la seguridad digital de la organización, y que se han desarrollado (y seguido) políticas relacionadas con la administración de datos, con personal dispuesto a sacrificar de alguna manera facilidad de uso por razones de seguridad. Este tipo de organización está dispuesta a invertir fondos (como en proveedores comerciales) si esa es la mejor opción, y se esfuerza por tomar decisiones intencionales en torno a las herramientas y sistemas tecnológicos.

Aprendizaje continuo

Poner en práctica e implementar prácticas saludables de seguridad digital puede significar cosas muy diferentes para distintas organizaciones. Generalmente, será una serie cíclica de prácticas en lugar de una acción única. Como resultado, las organizaciones en esta etapa deben dedicar recursos continuos a la seguridad digital y ser conscientes de que siempre hay más para aprender.

Un buen consejo para una organización puede ser inútil para otra. Esto hace que la calidad del soporte dependa en gran medida del contexto.

Ver metáfora visual. Si el edificio en el que se encuentra no tiene instalado un sistema de rociadores, recibir el consejo de "encender los rociadores" en caso de emergencia no tiene sentido. En cambio, para que sea

ESTUDIO DE CASO

AMENAZAS A LA SEGURIDAD DIGITAL EN NEPAL

Aprendizaje clave: Comprender el contexto cultural y social puede cambiar drásticamente los consejos de seguridad digital que se ofrecen frente a las amenazas.

El informe de Citizen Lab, Targeted Threats,[41] analizó las amenazas de seguridad digital que enfrentan varias organizaciones. A continuación, describen una intervención de apoyo de seguridad digital llevada a cabo por organizaciones en el Tíbet:

"Por ejemplo, algunos grupos tibetanos han estado promoviendo una campaña en favor de "No usar archivos adjuntos" que alienta a los usuarios a optar por plataformas alternativas basadas en la nube como Google Drive para compartir documentos en lugar de hacerlo como archivos adjuntos del correo electrónico. La campaña utiliza una mezcla de humor y referencias a la cultura tibetana y es un buen ejemplo de educación del usuario que está conectada a un modelo de amenaza específico y contexto local... en base a lo que hemos visto, la campaña podría ser efectiva contra algunas de las actuales amenazas contra la comunidad tibetana. Más del 80% del malware que nos enviaron los grupos del Tíbet utilizó un archivo adjunto de correo electrónico malicioso. Además, para dos de los grupos del Tíbet en nuestro estudio, simplemente no abrir archivos adjuntos mitigaría más del 95% de las amenazas de malware dirigidas que usan el correo electrónico como vector".

Para estos grupos tibetanos, ajustar sus prácticas para responder a su amenaza más destacada, la de los ataques de phishing transmitidos a través de archivos adjuntos de correo electrónico, sería una forma efectiva de adoptar prácticas saludables de seguridad digital. Sin embargo, para que la comunidad de soporte de seguridad digital lo sepa, necesitarían comprender el contexto en el que operan estos grupos y cómo fomentar estos comportamientos de una manera culturalmente apropiada, como parece hacer la campaña "No usar archivos adjuntos".

útil y operativo el asesoramiento debe diseñarse para el contexto en el que se encuentra la persona.

Se considera que existe falta de disponibilidad de fondos para el mantenimiento y el apoyo a largo plazo. Como resultado, las organizaciones lanzarán nuevas intervenciones en lugar de las actuales, a pesar de que las intervenciones continuas suelen ser más útiles.

Un entrevistado nos dijo que el aprendizaje clave para apoyar a las organizaciones a implementar prácticas de seguridad digital es hacer que la seguridad digital "sea tan prioritaria como los presupuestos, la financiación y las cuestiones de personal".

Esta percepción también fue planteada por aquellos que trabajan en áreas de infraestructura técnica, quienes mencionaron que les resultó difícil recaudar fondos. A su vez, la falta de recursos dificultó que estos grupos pudieran brindar apoyo a los grupos de la sociedad civil que dependen de ellos.

3. RECOMENDACIONES

Las recomendaciones de esta sección se centran en lo que los financiadores podrían hacer para apoyar y fomentar el desarrollo de un ecosistema de apoyo de seguridad digital saludable.

Estas recomendaciones provienen de entrevistas con proveedores de apoyo de seguridad digital, expertos en seguridad digital y destinatarios de apoyo de seguridad digital, con un enfoque particular en los Estados Unidos. Todas las recomendaciones son respuestas a problemas planteados sistemática y reiteradamente por los entrevistados, sugerencias directas de varios entrevistados o el resultado de los desafíos que a lo largo de los últimos seis años The Engine Room como organización que brinda apoyo a la sociedad civil ha tenido que enfrentar.

3.1 RECOMENDACIONES PARA PATROCINADORES

Este informe busca dar una idea de cuáles son las brechas actuales entre el apoyo de seguridad digital y las necesidades de la sociedad civil con el objetivo de orientar mejores prácticas filantrópicas en todos los ámbitos.

La seguridad digital debe ser priorizada por la filantropía de modo ostensible, a fin de que la sociedad civil continúe aumentando su dependencia de la tecnología de una manera que no constituya un riesgo para sí ni para aquellos a quienes intenta apoyar.

Desarrollar la seguridad digital como un tema central dentro del ámbito de la concesión de subvenciones

Como la seguridad digital sigue siendo una preocupación fundamental recopilar de manera proactiva la información de los beneficiarios (en particular los de alto riesgo, para quienes la seguridad digital aún no está en su radar) enviaría una señal de que los patrocinadores en todos los niveles toman en serio la seguridad.

La Guía de Seguridad Digital y Subvenciones[42] es un excelente ejemplo de lo que es posible cuando los financiadores en las etapas más avanzadas del abordaje de un problema producen ideas prácticas para otras fundaciones. También es un buen ejemplo de una organización que comparte las lecciones aprendidas a lo largo del ciclo "desconocimiento -> aprendizaje -> dominio", definiendo un camino potencial de evolución para que otros financiadores lo vean.

Se podría hacer más para alentar la adopción y el uso de la guía entre otros financiadores, como seminarios web con redes o grupos de patrocinadores, como el que se realizó para la Iniciativa de Transparencia y Responsabilidad, o mayor desarrollo de materiales prácticos de la guía para que otros patrocinadores los utilicen.

Brindar más apoyo a los actuales beneficiarios

Las siguientes sugerencias están dirigidas a potenciar y apoyar a las organizaciones que invierten en sus organizaciones para contribuir al aprendizaje de toda la comunidad.

- **Recompense a las organizaciones que hacen grandes avances en seguridad** y continúan invirtiendo en su crecimiento, aumentando su financiación básica a lo largo del tiempo. Desarrolle

mecanismos para señalar cuáles son estas organizaciones.

• **Apóyelas en la implementación de mejores mecanismos de monitoreo y evaluación para los proveedores de apoyo de seguridad digital** más allá de simplemente contar el número de personas que asisten a un evento, o el número de descargas de una guía en particular.

• **Aliente a estas organizaciones a documentar el proceso** de cómo han aumentado su capacidad de seguridad organizacional, proporcionando ejemplos para otras organizaciones pares y contribuyendo al conocimiento y al desarrollo de capacidades a escala comunitaria.

• **Priorice de forma activa el apoyo de seguridad:** incluya la seguridad dentro de la esfera básica del soporte cuando trabaje con organizaciones en la elaboración de presupuestos generales de soporte.

Informing investments in the digital security support space

Como se menciona en este informe, los tipos de apoyo han evolucionado con el tiempo. La filantropía podría aprender de estas evoluciones y como resultado ajustar los tipos de intervenciones que reciben apoyo.

• **Reducir el financiamiento para guías y sitios web de recursos generalizados:** como se describe en este informe, los recursos "multiuso" no satisfacen las necesidades de ningún grupo en particular, y muchos los consideran no lo bastante específicos para sus contextos. En su lugar, identifique los principales grupos y comunidades que necesitan recursos, y las instituciones con mejores posibilidades para comprender sus necesidades y diseñar recursos en consecuencia.

• **Financie proyectos que vinculen la investigación con ataques a la sociedad civil, litigios estratégicos, desarrollo técnico y apoyo centrado en el usuario:** la seguridad digital no es un mecanismo de apoyo independiente y debe asociarse con otras bases institucionales clave para tener éxito.

• **Respalde una mejor experiencia de usuario de herramientas que respetan la privacidad:** una barrera importante para la adopción de herramientas de código abierto es el hecho de que no se perciben como fáciles de usar. Si bien el apoyo de seguridad digital debe centrarse en procesos en lugar de herramientas, es posible respaldar el ecosistema asegurando que existan herramientas disponibles que se mantienen y auditan periódicamente y han construido activamente una experiencia de usuario fluida y accesible.

Como se menciona en el informe, invertir en la oferta de capacitación tradicional en seguridad del usuario final es insuficiente para respaldar los logros de seguridad de las organizaciones de cambio social. Los entrenamientos pueden funcionar como una intervención de sensibilización, pero en términos de apoyo práctico, a menudo se quedan cortos. En particular, las capacitaciones pueden ser una pérdida de tiempo y recursos para las organizaciones si:

• no son parte de una estrategia más amplia de apoyo y cambio

• se limitan a intervenciones altamente técnicas

• no abordan las necesidades de usabilidad y tecnología de las organizaciones de cambio social

• no se conectan a las necesidades culturales, políticas y sociales

• dejan al participante abrumado, solo dentro de su organización, o inseguro de cómo las modificaciones en la conducta del usuario final sirven para que el individuo se conecte a las soluciones de la organización

Como respuesta a eso, alentamos las capacitaciones solo si son parte de un mecanismo de apoyo a largo plazo y de una estrategia ecosistémica.

Coordinación entre financiadores

Los entrevistados mencionaron que recibir información conflictiva o superpuesta de los financiadores respecto a la seguridad digital es una barrera para saber qué hacer a continuación.

• **Fomentar una mejor coordinación entre quienes financian** el apoyo brindado a los beneficiarios y los consejos que ofrecen. Los entrevistados mencionaron la falta de coordinación entre los financiadores, lo que ocasionó que los beneficiarios recibieran consejos contradictorios, o que a veces se les animara a ir a múltiples capacitaciones en un breve período de tiempo, pero sin apoyo para la implementación de medidas.

• **Sincronice los esfuerzos con otras fundaciones (más allá de los Jefes de Información) para investigar y prevenir ataques y capacitar al personal,** de la misma manera que el personal recibe cada vez más apoyo para comprender la gestión financiera, las comunicaciones y la estrategia. Más allá de recopilar una base de datos de ataques por fundación, también puede haber espacio para hacer lo mismo para una red más amplia de patrocinadores, permitiendo un análisis más completo del espacio de la sociedad civil y, en consecuencia, estrategias de respuesta mejor fundamentadas.

CONCLUSIÓN

Este informe se centra en la comprensión de la seguridad digital desde una perspectiva organizacional, y sugiere formas en que el ecosistema de apoyo de seguridad digital podría evolucionar para satisfacer las necesidades de la sociedad civil. La confianza de la sociedad civil en las tecnologías digitales está creciendo, y nuestro enfoque hacia la seguridad digital necesita crecer en paralelo. Está claro que la seguridad digital es contextual: un enfoque genérico, o un conjunto de consejos, no es válido para todos. La cultura, las costumbres y el comportamiento afectan la forma en que se proporciona y recibe el apoyo de seguridad digital.

Sobre todo, a partir de este trabajo queda claro que el ecosistema de apoyo necesita crecer y valorar diferentes tipos de experiencia. Esta experiencia debe pasar por un proceso de selección a cargo de personas con el conocimiento contextual y técnico requerido para saber a quién recomendar, asegurándose de que diferentes tipos de expertos puedan conectarse allí donde sean más útiles. Necesitamos mejores formas de entender el impacto del apoyo de seguridad digital; más personas que se sientan cómodas hablando de seguridad digital y enfoques basados en el contexto para impulsar la seguridad digital.

Para que las organizaciones de la sociedad civil continúen funcionando de manera eficiente optimizando sus recursos, debemos comenzar a desarrollar comportamientos saludables en torno a la seguridad digital en todos los niveles, desde el uso y desarrollo de herramientas de tecnología segura y fácil de usar, hasta el almacenamiento seguro de datos y, sobre todo, el desarrollo de una cultura organizacional que integre la seguridad digital. Para que eso suceda, necesitamos que el ecosistema de apoyo de seguridad digital evolucione, aprenda de los errores del pasado y esté cada vez más integrado por las comunidades a las que apunta.

METODOLOGÍA

Este informe se basa en una revisión del actual ecosistema de seguridad digital, literatura y recursos relevantes, y entrevistas con destinatarios y proveedores de apoyo de seguridad digital (incluyendo personas que trabajan como expertos en seguridad digital, capacitadores, proveedores y financiadores de TI (comerciales)) La investigación se complementó con investigación documental durante todo el proceso.

Los entrevistados fueron identificados a través de las redes de The Engine Room, recomendaciones de entrevistados y sobre la base de la investigación documental. La mayoría (23) de los entrevistados trabaja en los Estados Unidos, mientras que el grupo restante de entrevistados (12) trabaja a nivel internacional. Las entrevistas se realizaron en inglés, de junio a agosto del 2017. Se realizaron un total de 35 entrevistas semiestructuradas, y se complementaron con la observación de talleres y capacitaciones de seguridad digital; asistencia a varios eventos donde se discutió el apoyo de seguridad digital y conversaciones informales con una amplia gama de personas.

Este informe tiene como objetivo identificar las brechas y necesidades en el actual ecosistema de apoyo de seguridad digital en los Estados Unidos. Los resultados se basan en una pequeña muestra de entrevistados y, por lo tanto, no son exhaustivos. Sin embargo, esperamos que el informe pueda contribuir a una mejor comprensión de las necesidades actuales de seguridad digital de la sociedad civil en los Estados Unidos.

RECONOCIMIENTOS

Ofrecemos nuestro sincero agradecimiento a todas aquellas personas que generosamente aportaron su tiempo y sabiduría durante este proyecto; aquellos con quienes llevamos a cabo entrevistas oficiales, los que contribuyeron al cuerpo de investigación que leímos, valoramos y desarrollamos, y con quienes hablamos en conversaciones informales.

Las personas que fueron entrevistadas para Lazos que unen, y dieron su consentimiento para ser incluidas en esta lista son: Micah Anderson; Sarah Aoun; Jack Aponte; Matthew Burnett; Michael Carbone; Claire Downing; Ryan Gerety; Daniel Kahn Gillmor; Claudio Guarnieri; guido; Bex Hurwitz; Lisa Jervis; Dragana Kaurin; Dia Kayalli; Noah Kelley; Mark Kiggundu; Tania Lee; Josh Levy; Rickke Mananzala; Jordan McCarthy; Matt Mitchell; Azeenarh Mohammed; Ken Montenegro; Joshua Peskay; Lisa Rau; Aliya Rahman; Jonah Silas; y Dan Staples.

El equipo de Internet Freedom de la Fundación Ford ofreció un valioso apoyo y orientación durante todo el proceso, y agradecemos la oportunidad de haber trabajado en este proyecto. Cualquier error es exclusiva responsabilidad de los autores.

NOTAS

[1] Para más información sobre el rol que la raza, la sexualidad y el género juegan en la vigilancia, vea: Rachel E. Dubrofsky and Shoshana Amielle Magnet (eds.) Feminist Surveillance Studies. Duke University Press, 2015: https://www.dukeupress.edu/feminist-surveillance-studies.

[2] Martin Shelton, Current Digital Security Resources, 19 de diciembre del 2016: https://medium.com/@mshelton/current-digital-security-resources-5c88ba40ce5c.

[3] Activate, 2016 Tech and Media Outlook, 2016: http://www.slideshare.net/ActivateInc/activate-tech-and-media-outlook-2016/2-Over_the_next_ five_years.

[4] ICRC, The Engine Room and Block Party, Humanitarian Futures for Messaging Apps, enero del 2017, p. 20: https://www.icrc.org/en/publication/humanitarian-futures-messaging-apps.

[5] ICRC, The Engine Room and Block Party, Humanitarian Futures for Messaging Apps, enero del 2017, p. 20: https://www.icrc.org/en/publication/humanitarian-futures-messaging-apps.

[6] Natasha Lomas, "Security researchers call for Guardian to retract false WhatsApp "backdoor" story", TechCrunch, 20 de enero del 2017: https://techcrunch.com/2017/01/20/security-researchers-call-for-guardian-to-retract-false-whatsapp-backdoor-story/.

[7] Un informe publicado por Citizen Lab en el 2014 identificó la necesidad de mantenerse al día con los nuevos desarrollos técnicos y los riesgos específicos del contexto como "desafiantes y lentos" para las organizaciones de la sociedad civil con las que trabajaron. Citizen Lab, Communities @ Risk: Targeted Digital Threats Against Civil Society, 11 de noviembre del 2014, p. 122: https://targetedthreats.net.

[8] Ver por ejemplo: Camila Bustos, "El cierre de los espacios cívicos: ¿Qué está pasando y qué podemos hacer?", Dejusticia, 17 de abril del 2017: https://www.dejusticia.org/column/el-cierre-de-los-espacios-civicos-que-esta-pasando-y-que-podemos-hacer/.

[9] https://es.globalvoices.org/2017/10/27/tras-113-dias-detenidos-liberan-a-defensores-de-derechos-a-la-espera-de-juicio/

[10] Matt Burgess, "The 'real people' using encryption for privacy protection", Wired, 1 de agosto del 2017: http://www.wired.co.uk/article/uk-encryption-whatsapp-amber-rudd.

[11] Jeremy Malcolm, "Australian PM Calls for End-to-End Encryption Ban, Says the Laws of Mathematics Don't Apply Down Under", Electronic Frontier Foundation, 14 de julio del 2017: https://www.eff.org/deeplinks/2017/07/australian-pm-calls-end-end-encryption-ban-says-laws-mathematics-dont-apply-down.

[12] Reuters, "France says fight against messaging encryption needs worldwide initiative", Reuters, 11 de agosto del 2016: http://www.reuters.com/article/us-france-internet-encryption-idUSKCN10M1KB.

[13] Eric Luchtblau and Katie Benner, "Apple Fights Order to Unlock San Bernardino Gunman's iPhone", New York Time, 17 de febrero del 2016: https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html.

[14] Kai Biermann, "Innenministerium sucht freiwillige Cyberfeuerwehr", Zeit Online, 6 de octubre del 2016: http://www.zeit.de/digital/datenschutz/2016-10/bsi-cyberangriff-it-sicherheit-feuerwehr-cyberwehr.

[15] See "For some HRDs, technology is not the root of their risk." Nah, Alice M., et al., "A Research Agenda for the Protection of Human Rights Defenders." Journal of Human Rights Practice, 2013, p. 415.

[16] https://theoutline.com/post/2489/two-passwords-are-always-better-than-one

[17] Tactical Tech, Holistic Security: https://holistic-security.tacticaltech.org/.

[18] El Compañero de educación en seguridad de la Electronic Frontier Foundation toma un enfoque explícito de reducción de daños y proporciona un resumen útil de algunos principios clave:https://sec.eff.org/articles/harm-reduction

[19] Para más información sobre diferentes tipos de entrenamientos, vea Waters, Carol. "Digital Security Trainers: Practices and Observations." Publicación. Tactical Technology Collective, 2015. Web. 14 de junio del 2017.

[20] Para más información, vea "Digital Security Concerns" en: The Engine Room, Technology Tools for Human Rights, setiembre del 2016, p. 10: https://www.theengineroom.org/wp-content/uploads/2017/01/technology-tools-in-human-rights_lower-quality.pdf.

NOTAS (CONT.)

[21] Advertencia de activación para descripciones detalladas de agresión sexual: https://www.theverge.com/2017/10/13/16473996/morgan-marquis-boire-citizen-lab-sexual-assault. https://citizenlab.ca/2017/10/open-letter-sexual-assault/

[22] Descrito en mayor detalle en el informe Targeted Threats del Citizen Lab. Citizen Lab, Communities @ Risk: Targeted Digital Threats Against Civil Society, 11 de noviembre del 2014: https://targetedthreats.net.

[23] Immigration Advocates Network and Idealware, Technology Needs Among Immigrant Rights and Immigration Legal Services Organizations: A Survey of the Field, agosto del 2016: https://www.immigrationadvocates.org/link.cfm?25937.

[24] Media.ccc.de, Hacking the World (33c3), 28 de diciembre del 2016: https://www.youtube.com/watch?v=K-F860QYZzUE.

[25] Security Without Borders, Transmission 1, 13 de mayo del 2017: https://securitywithoutborders.org/blog/2017/05/13/transmission-1.html.

[26] Martin Shelton, Signal for Beginners, 18 de noviembre del 2016: https://medium.com/@mshelton/signal-for-beginners-c6b44f76a1f0#.3bocimnxj.

[27] Net Alert: https://netalert.me/.

[28] https://securityplanner.org/#/

[29] Ver "Barriers to sustained learning and implementation", Waters, Carol. "Digital Security Trainers: Practices and Observations." Publication. Tactical Technology Collective, 2015. Web. 14 de junio del 2017

[30] Tactical Tech and Front Line Defenders, Security-in-A-Box - Herramientas y tácticas de seguridad digital: https://securityinabox.org/es/.

[31] Electronic Frontier Foundation, Surveillance Self-Defense: https://ssd.eff.org/es (En castellano)

[32] Matt Mitchell, Digital Security training resources for digital security trainers, Winter 2017 Edition, 19 de noviembre del 2016: https://medium.com/@geminiimatt/security-training-resources-for-security-trainers-winter-2016-edition-4d10670ef8d3.

[33] Hackblossom, DIY Cybersecurity for Domestic Violence: https://hackblossom.org/domestic-violence/.

[34] https://cyber-women.com/es/#acerca (En castellano)

[35] https://bahrainwatch.org/amanatech/en/advice/how-to-store-and-wipe-your-data-securely

[36] https://securityplanner.org/#/

[37] Immigration Advocates Network and Idealware, Technology Needs Among Immigrant Rights and Immigration Legal Services Organizations: A Survey of the Field, agosto del 2016, p. 8: https://www.immigrationadvocates.org/link.cfm?25937.

[38] Kazansky, Becky. "FCJ-195 Privacy, Responsibility, and Human Rights Activism." The Fibreculture Journal, 26, 2015: Entanglements–Activism and Technology (2015).

[39] Para más información sobre la seguridad digital como un conjunto de prácticas, ver Kazansky, Becky. "Digital Security in Context: Learning How Human Rights Defenders Adopt Digital Security Practices." Publication. Tactical Technology Collective, 2015. Web. 14 de junio del 2017.

[40] Orgsec community: https://Orgsec.community.

[41] Citizen Lab, Communities @ Risk: Targeted Digital Threats Against Civil Society: https://targetedthreats.net/.

[42] Michael Brennan, Elizabeth Eagen, Bryan Nuñez, John Scott-Railton and Eric Sears, Digital Security & Grantcraft Guide: an Introduction Guide for Funders, marzo del 2017: https://www.fordfoundation.org/library/reports-and-studies/digital-security-grantcraft-guide/.


THE
ENGINE
ROOM