Lazos que unen

Seguridad organizacional para la sociedad civil

Resumen Ejecutivo

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.

Resumen Ejecutivo

La tecnología nos dota de superpoderes, pero también es nuestro talón de Aquiles.

En un momento de retracción del espacio cívico a nivel mundial[1], los ataques y las amenazas digitales van en aumento. Para que el espacio cívico funcione correctamente, una defensa y preparación efectivas son cada vez más críticas, especialmente para organizaciones y comunidades que procuran que quienes ejercen el poder rindan cuentas.

Conceptualmente, asegurar digitalmente a las organizaciones se puede comparar con acondicionar una oficina contra incendios, ya que existen múltiples niveles que necesitan preparación:

- **Infraestructura:** los edificios se diseñan teniendo en cuenta las medidas de protección contra incendios, desde el revestimiento de las paredes hasta la construcción de salidas de incendios accesibles. Del mismo modo, las organizaciones al momento de establecer y mantener su infraestructura operativa deberían pensar en su seguridad.

- **Niveles de respuesta:** en caso de incendio, hay múltiples opciones disponibles, desde llamar al operador si se trata de una gran emergencia hasta usar un extintor de incendios. También son diversos los factores desencadenantes que provocan una respuesta: alarmas de humo, sistemas de rociadores o la alarma de incendio activada manualmente. Para las organizaciones, los diferentes niveles de amenazas a la seguridad digital justifican respuestas diversas y distintos tipos de conocimientos especializados.

- **Cultura y conocimiento:** las respuestas frente a incendios difieren de un país a otro. Recomendaciones como "encender los rociadores" en un país donde no se usa ese sistema, no son útiles, al igual que consejos de seguridad digital tales como "usar un iPhone" en un país donde los teléfonos Android son la norma no son útiles. Fortalecer el conocimiento y desarrollar una cultura que priorice la seguridad toma tiempo y requiere repetición y mantenimiento.

---

[1] 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/.

Las sociedades de todo el mundo reconocen que en cada uno de estos niveles la protección contra incendios es crucial y salva vidas. Esto no sucede aún en lo que respecta a la seguridad digital: a pesar de nuestra creciente dependencia de las tecnologías digitales, el ecosistema de apoyo de la seguridad digital no ha evolucionado para satisfacer las realidades y necesidades de la sociedad civil. El ecosistema de apoyo sigue dominado por proveedores de soporte que, desconociendo el contexto, a menudo se enfocan en soluciones técnicas de nicho, ignoran las necesidades de infraestructura a largo plazo y no abordan adecuadamente las prácticas culturales que deben desarrollarse. Se necesita una inversión sólida a largo plazo en cada uno de estos niveles para generar un ecosistema saludable en general.

Históricamente, la filantropía y el ecosistema de seguridad digital se han centrado en los aspectos más visibles y con recompensa inmediata del soporte : crear nuevas herramientas y aplicaciones y proporcionar soporte técnico a corto plazo. Esto ha causado que los elementos de infraestructura necesarios para una sociedad civil fuerte, incluida la seguridad organizacional, no cuenten con recursos suficientes y permanezcan subdesarrollados. Sin organizaciones seguras, la sociedad civil no podrá servir de manera eficaz al interés público a largo plazo.

El ecosistema de apoyo de la seguridad digital es multifacético, cada parte es apoyada y vigilada por diferentes actores que trabajan en pos de objetivos complementarios, pero diferentes:

- Infraestructura física: Estados, empresas o comunidades construyen una infraestructura física resistente para proporcionar acceso a Internet. (Compárese con: *construir una infraestructura resistente de acceso al agua para que los edificios puedan usarla para combatir incendios*)

- Normas técnicas: los organismos de normalización garantizan que el modo en que funciona Internet incorpora medidas de protección de la privacidad. (Compárese con: *desarrollar estándares de construcción con garantía de calidad aprobados institucionalmente)*.

- Marcos legales y política: los abogados y los responsables de la formulación de políticas se aseguran de que los marcos legales y las políticas respeten los derechos humanos en la esfera digital. (Compárese con: a*segurar respuestas legales apropiadas contra los pirómanos, o pólizas de seguro contra incendios accidentales*).

- Desarrollo técnico: desarrollo de software que permita prácticas digitales seguras. (Compárese con: *desarrollar productos innovadores que sean resistentes al fuego*).

Las organizaciones de la sociedad civil interactúan con los elementos mencionados y tienen necesidades especiales propias de su función de exigir que quienes detentan el poder rindan cuentas, y a menudo son el primer blanco de ataque. Este informe se enfoca en el ecosistema de apoyo de la seguridad digital

desde la perspectiva de las organizaciones de la sociedad civil, y propone medidas que los patrocinadores y miembros del ecosistema de apoyo de la seguridad digital podrían adoptar para satisfacer mejor las necesidades de estas organizaciones.

En el año 2018, la sociedad civil depende casi por completo de la tecnología para operar, desde tareas como la gestión de la información hasta la comunicación básica. Nuestra infraestructura digital nos conecta a una escala más amplia que nunca antes, pero abre nuevas vulnerabilidades que a menudo permanecen invisibles hasta que son usadas en nuestra contra. Al mismo tiempo, muchas organizaciones de la sociedad civil enfrentan severas limitaciones de recursos que les obligan a elegir entre el trabajo orientado a concretar su misión y las inversiones en su propia seguridad, a menudo en detrimento de ambos objetivos. En gran medida la clave para corregir esta situación radica en la filantropía: para garantizar que existan incentivos destinados a fomentar mejores prácticas de seguridad y para brindar soporte al ecosistema de apoyo de seguridad digital en todos los niveles.

En pocas palabras: ignorar la seguridad digital socava la misión de cualquier organización de la sociedad civil en la actualidad.

Para que las organizaciones de la sociedad civil continúen operando de manera eficiente optimizando sus recursos, debemos comenzar a desarrollar prácticas saludables que aborden la seguridad digital en todos sus niveles, desde el uso y desarrollo de herramientas tecnológicas seguras y fáciles de usar, hasta el almacenamiento seguro de datos y, sobre todo, el desarrollo de una cultura organizacional que integre y valore la seguridad digital. Para que eso suceda, necesitamos que el ecosistema de apoyo de seguridad digital evolucione, aprenda de los errores del pasado y satisfaga las necesidades de la sociedad civil.

Aspectos fundamentales

Contexto

La mejor manera de comprender la seguridad digital es en el marco del entorno político y social circundante, y del rol que desempeña en el tejido y la infraestructura de una organización. Comprender estos cuatro puntos es clave para entender las siguientes recomendaciones.

- **La seguridad es multidimensional:** en particular para las organizaciones de la sociedad civil que trabajan en condiciones estresantes y de riesgo, la seguridad y protección comprenden numerosas dimensiones: física, sicosocial y organizacional. Para que las medidas de apoyo tengan éxito, deben ser integrales, reconocer y abordar la seguridad como un complejo problema social, político y técnico.

- **La seguridad digital se penaliza cada vez más:** especialmente en países políticamente restrictivos, tomar medidas para protegerse digitalmente se considera un acto político. Como ejemplos cabe mencionar los instructores de seguridad digital que están siendo encarcelados en Turquía; la encriptación que ha sido declarada ilegal en Pakistán; y el anonimato en línea que ha sido considerado inconstitucional en Venezuela.

- **La seguridad es contextual:** los consejos que tienen como destinataria a una organización determinada pueden ser totalmente irrelevantes, inútiles o, en el peor de los casos, perjudiciales para otra. El contexto cambia la forma en que las organizaciones utilizan e implementan las tecnologías, y por tanto, afecta cuáles son las prácticas de seguridad relevantes para las diferentes comunidades.

· **La seguridad digital es una serie de prácticas, no un ejercicio aislado:** las prácticas saludables de seguridad digital son comportamientos constantes que deben actualizarse a medida que los entornos políticos y técnicos se modifican. Dominar la seguridad digital significa establecer prácticas con el objetivo de aprender, evolucionar y actualizar el comportamiento individual.

Recomendaciones

Estas recomendaciones provienen de entrevistas con expertos en seguridad digital, proveedores de soporte en dicha materia y destinatarios del apoyo de seguridad digital, centrado especialmente 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 The Engine Room como organización que brinda apoyo a la sociedad civil ha tenido que enfrentar a lo largo del tiempo en materia de seguridad digital.

Fortalecimiento del ecosistema de apoyo de seguridad digital

Las siguientes recomendaciones comprenden medidas tendientes a favorecer el ecosistema de apoyo de seguridad digital en su totalidad.

· **Financie el estudio de los ataques digitales experimentados por organizaciones de la sociedad civil:** una investigación sistemática de los ataques que han tenido como blanco la sociedad civil a nivel mundial podría revelar patrones en los tipos de ataques y aumentar la capacidad de la comunidad para responder con precisión ante estas amenazas. Por ejemplo: investigar el spyware (programa espía) enviado por correo electrónico a grupos de la sociedad civil a escala global y sistemática.

· **Apoye las actividades de promoción destinadas a los directivos de las organizaciones** acerca de la importancia y pertinencia de la seguridad digital para su organización: los entrevistados destacaron la existencia de una brecha generacional en las actitudes hacia la seguridad digital, así como la falta de materiales accesibles de promoción de la seguridad digital orientados al sector de mayor edad dentro de la sociedad civil, quienes a menudo ocupan puestos directivos encargados de supervisar los presupuestos y decidir las prioridades. Comprender la seguridad digital es particularmente importante para las autoridades a cargo de la toma de decisiones y que pueden ser neófitas en algunos de estos temas. Para que las organizaciones de la sociedad civil den prioridad a la seguridad digital, la promoción debe ocurrir en todos los niveles de la estructura y jerarquía organizacional.

· **Apoye la elaboración de materiales accesibles y relevantes para la comunidad que aborden el tema de la seguridad digital:** estos deben ser desarrollados por organizaciones o comunidades que también sean destinatarias de dichos materiales. Esto permitiría que los creadores de recursos identifiquen de manera realista tanto la necesidad de materiales como la capacidad existente, y garantizaría la posibilidad de compartir estos recursos con las organizaciones integrantes de sus redes.

· **Apoye la gestión comunitaria de las redes de proveedores de apoyo de seguridad digital:** aunque las redes de proveedores de apoyo de seguridad digital técnica se están expandiendo, corren el riesgo de no llegar a su potencial público objetivo y no documentar sus aprendizajes de una manera que contribuya al conocimiento compartido. Esto podría mitigarse alentando a las redes de proveedores técnicos a invertir en la gestión comunitaria. Los responsables de la gestión de la comunidad desempeñarían un rol operativo / de soporte en la red, centrándose en la elaboración de documentación, la construcción de

procesos simplificados para la provisión de soporte y el intercambio de aprendizajes con otras comunidades relevantes.

· **Priorice por igual las solicitudes de apoyo de seguridad** del personal, los beneficiarios y los voluntarios. De ejemplo de conducta saludable tomándose la seguridad en serio para poner de manifiesto que la seguridad es una prioridad para una organización. Cuando sea posible hacerlo de manera responsable, comparta que esto se ha convertido en una prioridad (por ejemplo, ante el consejo directivo de una organización, mediante una declaración pública, en una reunión de personal).

· **Anime a integrantes de comunidades subrepresentadas** a que participen en la provisión de apoyo de seguridad digital. En la actualidad, existe una gran brecha de capacidad, con una gran escasez de miembros de las comunidades afectadas capaces de entender los problemas de seguridad digital y su contexto, y con relaciones sólidas dentro de esas comunidades. A largo plazo, abordar esta brecha de capacidad es una parte fundamental de un ecosistema de apoyo de seguridad digital saludable.

· **Construir redes entre "técnicos por accidente" en las organizaciones beneficiarias:** estas son las personas que, a menudo sin una formación técnica formal, terminan siendo responsables de la seguridad de la organización. Este rol puede ser desafiante y estresante, y a menudo terminan trabajando solos. Establezca conexiones entre los técnicos por accidente de las organizaciones beneficiarias para brindarles un grupo de apoyo e inspiración.

Para filantropía

· **Recompense a las organizaciones que hacen grandes progresos en su propia seguridad,** aumentando su financiación básica a lo largo del tiempo. Esto transmite al resto de las organizaciones el mensaje de que priorizar la seguridad organizacional es una parte importante de su crecimiento y contribuye al desarrollo a largo plazo de las capacidades de más personas con raíces dentro del movimiento con habilidades relacionadas con la seguridad organizacional.

· **Reste respaldo a guías y sitios web que ofrecen recursos generalizados**. Hemos escuchado muchas veces que los recursos "multiuso" no satisfacen las necesidades de ningún grupo en particular, y son muchos quienes consideran que no son lo bastante precisos para sus contextos. En cambio, identifique los principales grupos y comunidades que necesitan recursos, y las instituciones con mejores posibilidades de comprender sus necesidades y diseñar recursos en consecuencia.

· **Apoye proyectos que vinculen la investigación de ataques a la sociedad civil, litigios estratégicos, desarrollo técnico y soporte centrado en el usuario.** La seguridad digital no es un mecanismo de soporte independiente, y para tener éxito necesita asociarse con otras bases institucionales clave.

· **Considere la seguridad organizacional como parte del soporte operativo:** para algunos, la seguridad de una organización se enmarca dentro de su equipo de operaciones, abarca desde garantizar que los correos electrónicos se alojen de forma segura, hasta ejecutar el software financiero y el presupuesto. Pero los entrevistados sugirieron que existen mayores dificultades para encontrar respaldo básico que incluya un presupuesto destinado a la seguridad organizacional que fondos para el financiamiento de proyectos individuales.