Fundación Karisma

DECLARACIÓN DE KARISMA PARA LA TERCERA SESIÓN SUSTANTIVA DE OEWG-ONU.
Julio 27 de 2022.

Le agradezco, señor presidente, su trabajo durante esta sesión y la oportunidad de participar en la conversación del Grupo de Trabajo de Composición Abierta. Soy la directora de la Fundación Karisma[1], una organización de la sociedad civil colombiana que ha trabajado y participado en debates sobre seguridad digital desde hace seis años y cuenta con un laboratorio de seguridad digital y privacidad, K+Lab[2], especializado en atender a la sociedad civil.

El K+Lab ofrece talleres de seguridad digital para población civil -periodistas, defensores de derechos humanos y activistas-. También realiza auditorías para organizaciones de la sociedad civil basadas en análisis de riesgo, cuyo objetivo es crear planes de mejoramiento de sus políticas y prácticas, y hace investigaciones e incidencia en temas relacionados a la ciberseguridad; entre otras acciones.

Desde el K+Lab, hacemos parte de redes con organizaciones similares entre las que se incluyen el CiviCERT[3], el Observatorio Latinoamericano de Amenazas Digitales (OLAD) y la comunidad de seguridad digital en América Latina (COSIC-LAT). Karisma, además, ha publicado una guía[4] y construído un curso[5] sobre políticas de seguridad digital con enfoque de derechos humanos para construir capacidad de forma que las organizaciones de sociedad civil puedan participar en las discusiones de diseño y creación de política pública sobre seguridad y tecnología.

En relación con la discusión que ocupa a este grupo en primer lugar afirmamos que apoyamos el enfoque de género que se quiere imprimir a los documentos. En concreto, presentaremos cinco puntos en donde creemos que la sociedad civil puede aportar su capacidad, en cada caso resaltamos las lecciones que pueden servir para avanzar en los propósitos de paz y seguridad mundiales.

---

[1] https://www.karisma.org.co, Carolina Botero (carobotero@karisma.org.co),
[2] https://web.karisma.org.co/klab/
[3] https://www.civicert.org/
[4] https://web.karisma.org.co/guia-de-viaje-al-mundo-digital-politicas-de-ciberseguridad-para-personas-defensoras-de-los-derechos-humanos/
[5] https://web.karisma.org.co/taller-online-politicas-de-ciberseguridad-con-enfoque-en-derechos-humanos/

Fundación
Karisma

1. **La participación de los diferentes actores y partes interesadas, en especial de la sociedad civil, en las discusiones de política pública en materia de seguridad digital es esencial para cubrir temas de derechos humanos y dar una amplia visión a la regulación.** La participación de la sociedad civil ha servido para ampliar la perspectiva de este campo y permitir una transición desde la visión militarista hacia una donde el centro es la persona y se apuesta por el respeto a los derechos humanos.
   Así, desde 2014 Karisma ha participado activamente en las discusiones de política pública de ciberseguridad apoyando el plan estratégico nacional colombiano. En este marco presentamos comentarios[6] de diferente tipo, uno de esos reclamaba la idea de que la construcción de confianza es un elemento central de la seguridad digital y por tanto se cuestionaba que el CERT nacional estuviera en el Ministerio de Defensa, para ilustrar el problema se explicaba por ejemplo que el reporte de vulnerabilidades a una entidad que dependía del ente con capacidad ofensiva no era un antecedente positivo. En 2022 se dieron a conocer las nuevas regulaciones en materia de ciberseguridad en las que el CERT nacional pasó al Ministerio de las TIC[7]. Con esta disposición se consolidó la naturaleza civil del CERT nacional.

2. **La coordinación nacional para la divulgación y respuesta de vulnerabilidades tiene un papel importante en la protección de actividades críticas, productos y servicios**. La detección de vulnerabilidades a tiempo es fundamental en la construcción de confianza y las y los investigadores independientes de seguridad que las reportan son actores claves en este proceso. El reporte de vulnerabilidades requiere la creación y despliegue de coordinadores nacionales para gestión de vulnerabilidades que frecuentemente están dentro de la estructura estatal. Estos organismos deben trabajar activamente en la protección de los investigadores de seguridad digital, en ejercicios que estimulen la presentación de estos ejercicios, en acciones de respuesta eficaces y en mecanismos de compromiso y supervisión para evitar que sus funciones se mezclen con las ofensivas del Estado.
   La sociedad civil tiene importantes investigaciones y experiencias que pueden apoyar el desarrollo de acciones en este campo.

---

[6] "La política nacional de seguridad digital: cómo hacerlo mediocremente y con poca reflexión" incluye una relación de los diferentes argumentos entre los que se destaca las preocupaciones por que el Ministerio de Defensa tiene facultades ofensivas y puede abusar en forma oportunista la información de vulnerabilidades. Uno de los análisis realizados pueden consultarse en https://web.karisma.org.co/la-politica-nacional-de-seguridad-digital-como-hacerlo-mediocremente-y-con-poca-reflexion/

[7] Desde los borradores socializados por el Ministerio TIC se hizo ese importante ajuste en donde el Estado colombiano reconoce que este importante actor del sector de ciberseguridad debe salir del ministerio de defensa, como quedó reflejado en los comentarios que hicimos al borrador correspondiente. Disponible en https://docs.google.com/document/d/1JRBZd7OzQJ2PzzVAwl08_WIuMsaGF1ZjqH7bCiG2HXU/edit

Fundación Karisma

Por ejemplo, con el propósito de explicar de forma práctica la importancia de quienes investigan en seguridad digital y la utilidad de dar respuesta efectiva a los reportes de vulnerabilidades, Karisma adelanta desde 2016 un proyecto de incidencia en el que analiza sitios web y aplicaciones del Estado colombiano en búsqueda de problemas de privacidad y vulnerabilidades. Usando metodologías no intrusivas de análisis, eventualmente encontramos vulnerabilidades que reportamos a través del Ministerio TIC y las entidades responsables se enteran y proceden en consecuencia.

Con base en esta experiencia, Karisma y el Ministerio TIC creamos una ruta de reporte y respuesta a vulnerabilidades "de facto" al interior del Estado, este proyecto ha ido cambiando la cultura de temor de las entidades públicas a este tipo de reportes y ha conseguido proteger los datos de millones de personas. El caso más importante fue el informe que hicimos de los problemas en el sitio de la Unidad de Protección de Víctimas[8].

Este proceso llevó a la elaboración y publicación del informe de investigación "Estudio sobre rutas de divulgación en seguridad digital"[9]. En este informe se da una serie de recomendaciones para que el Estado colombiano pueda crear este la ruta de reporte y respuesta a vulnerabilidades nacional que permita a cualquiera reportar vulnerabilidades de forma segura y efectiva. Los primeros pasos para desarrollar esta ruta fueron recogidos en la política nacional de ciberseguridad colombiana Conpes 3995 de 2020[10] que deberá ser desarrollada en los próximos años. Esta experiencia fue reconocida por la OCDE como una buena práctica en su investigación para el desarrollo de recomendaciones en este campo[11].

3. **El debate de esta semana adelantado por el Grupo de Trabajo de Composición Abierta sobre la inclusión o no del ransomware como una amenaza supone reflexionar sobre la relación que existe entre algunos de estos ataques con motivaciones políticas y sobre la creciente industria del software espía que vende legalmente y se usa también con motivaciones políticas incluso por los Estados.** Se trata del uso oportunista de vulnerabilidades y engaños para desplegar malware, mantener un acceso remoto a los dispositivos y a la información presente

---

[8] https://web.karisma.org.co/wp-content/uploads/download-manager-files/INFORME%20CONJUNTO.pdf

[9] Estudio sobre rutas de divulgación en seguridad digital, Karisma. Disponile en: https://web.karisma.org.co/wp-content/uploads/download-manager-files/RutasDeDivulgacion.pdf

[10] Conpes 3995 de 2020. Disponible en https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

[11] Encouraging Vulnerability Treatment: How policy makers can help address digital security vulnerabilities, OCDE. Disponible en https://one.oecd.org/document/DSTI/CDEP/SDE(2020)3/FINAL/en/pdf

en estos. Visto de esta forma se trata sin duda de un tema de seguridad digital, son acciones ofensivas que no solo deben leerse como un problema de seguridad nacional, sino que afectan directamente a las personas y el ejercicio de sus derechos.
La sociedad civil ha denunciado cómo este tipo de armas se usan contra poblaciones vulnerables, son desplegadas en conflictos armados -pero no solamente- contra periodistas, activistas medioambientales y defensores de derechos humanos[12] y como tal deben ser parte del análisis para la respuesta estatal.
El marco jurídico de derecho internacional humanitario y de derechos humanos existente permite la elaboración de políticas y la implementación de prácticas en este campo, en ese sentido desde Karisma apoyamos la declaración realizada por el representante de Suiza, la cual ha sido ampliamente respaldada por otros países durante las presentes discusiones. Esperamos también que se incorporen las conclusiones y recomendaciones de los investigadores del mundo académico y de las organizaciones de la sociedad civil[13] que piden evaluaciones de impacto sobre los derechos humanos -incluyendo principios de derechos humanos como los de necesidad y proporcionalidad- y la regulación del mercado de productos y servicios. Los efectos indeseados de esta industria en crecimiento preocupan por su poder intrusivo y destructivo en la vida de las personas a quienes se les implanta este tipo de software en sus dispositivos, y la afectación que tendrá en la paz y seguridad mundial. El mercado que se desarrolla genera inestabilidad y produce incentivos que difícilmente se podrán controlar sin acuerdos internacionales y decisiones que limiten su uso por los Estados.

4. **La criptografía es necesaria para la protección del derecho a la privacidad,la libertad de expresión y una herramienta básica de seguridad digital, por tanto, las regulaciones que socavan el cifrado son una amenaza.** Los procesos de capacitación e investigación que adelanta la sociedad civil incluyen procesos de alfabetización de seguridad digital a todos los niveles de la sociedad, donde se resaltan principios básicos como la comprensión del funcionamiento de la

[12] https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus
https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens
[13] Karisma adelantó una investigación sobre el marco jurídico para el uso de herramientas de hackeo por parte del Estado “Cuando el estado hackea” que puede consultarse en https://web.karisma.org.co/cuando-el-estado-hackea-3/
Más recientemente se puede ver en cartas como https://web.karisma.org.co/al-descubierto-la-sociedad-civil-repudia-el-uso-de-pegasus-para-espiar-a-periodistas-y-activistas-en-el-salvador/

criptografía y sus usos para los hacedores de política pública. Se requiere construir una cultura de seguridad digital que sitúe los derechos humanos en el centro del debate, que hable de la gestión responsable de las evaluaciones de riesgo y que se base en la cooperación entre múltiples partes interesadas.

5. **La cooperación entre múltiples partes interesadas con los organismos nacionales responsables de la seguridad digital es una herramienta clave para garantizar la confianza**. No solo los CERT y CSIRT requieren de suficiente financiación, recursos y experiencia, que pueden ser escasos y difíciles de retener especialmente para países en desarrollo, además deben impulsar la cooperación de no solo con el sector privado -que está a cargo de la infraestructura clave de comunicaciones e información- también con otros actores que pueden resultar más inusuales para los gobiernos locales.
   Consideramos que en las acciones de cooperación que se discuten en esta sesión deben incluir expresamente a la sociedad civil, actor clave si se quiere asegurar que las actividades y estrategias que se desarrollen en ciberseguridad tengan un impacto en toda la población, especialmente la más vulnerable y sobre todo en procesos en los que se busca mantener la paz y la seguridad internacional. Es la sociedad civil la que tiene la capacidad de proporcionar los matices y especificidades en sociedades diversas y así construir la confianza necesaria.
   En una relación más amplia de cooperación la sociedad civil puede proporcionar datos y experiencias de sectores menos estudiados para la ciberseguridad.
   El análisis de casi cualquier plan nacional de seguridad digital -especialmente en el sur global- muestra diagnósticos usualmente vinculados con el sector financiero y público, no hay mucha evidencia sobre otros sectores y en consecuencia es muy difícil que éstos desarrollen enfoques diversos. Si el diagnóstico se hace con datos y experiencias similares las estrategias asumen una uniformidad poco realista. En la nueva generación de acciones y construcción de confianza en ciberseguridad se debe trabajar poniendo en el centro a las personas y la diversidad de la sociedad, eso tendrá especial impacto en procesos internacionales de conservación de paz y seguridad.