Fundación Karisma

DECLARACIÓN DE KARISMA PARA LA QUINTA SESIÓN SUSTANTIVA DE OEWG-ONU
26 de julio de 2023

Señor presidente, agradezco su labor y la de su equipo dirigiendo este Grupo de Trabajo de Composición Abierta y la oportunidad de participar en la conversación del día de hoy. Soy parte de Fundación Karisma[1], una organización de la sociedad civil colombiana que trabaja en derechos digitales y cuenta con un laboratorio de seguridad digital y privacidad[2] especializado en atención a la sociedad civil.

Al igual que varias delegaciones ya lo han hecho, celebramos las menciones a la participación sistemática y sustancial de las múltiples partes interesadas en el segundo informe de reporte anual. Al respecto quisiera señalar dos puntos concretos en los que sería importante sopesar la necesidad de fortalecer la participación de las partes interesadas.

En primer lugar, en la sección sobre amenazas existentes y potenciación es necesario tener en cuenta que la ciberseguridad debe tener como objetivo no la protección de sistemas informáticos por sí mismos, sino de los sistemas e infraestructuras como medios que hacen posible la realización de los derechos de la ciudadanía. En ese sentido, se debe tener en cuenta los aportes que pueden hacer las organizaciones de la sociedad civil incluyendo está perspectiva respecto a las amenazas que afectan de mayor manera a la ciudadanía y porque pueden poner en la mesa casos y argumentos que usualmente no presentarían otros interesados.

De igual forma, la academia, los expertos en ciberseguridad y los privados tienen un rol esencial cuando hablamos de entender cómo las nuevas tecnologías pueden generar riesgos a la ciberseguridad de los Estados y las personas, y para definir cómo regular de forma adecuada a la naturaleza técnica y cambiante de las tecnologías.

En resumen, es fundamental que todas las partes interesadas tengan la posibilidad de aportar y recibir información respecto a las amenazas existentes y potenciales a la ciberseguridad. En el caso de que el repositorio de riesgos de ciberseguridad llegara a ser acordado por los Estados, la forma de garantizar que el mismo sea lo más completo posible es, de nuevo, recibiendo los aportes de todas las partes interesadas.

El segundo tema tratado en el segundo informe anual respecto del que quisiera hacer una mención es el referente a las medidas de construcción de confianza y, de forma concreta, respecto de la propuesta de establecer un Directorio de Puntos de Contacto. Al respecto, señor presidente, debe evaluarse si estos puntos de contacto incluirán CERTs, CSIRTs y otros mecanismos de respuesta a incidentes de otros sectores, como los gremiales, académicos o de la sociedad civil, de modo que ellos también puedan intercambiar información según lo definan las delegaciones.

---

[1] Página web Fundación Karisma: https://www.karisma.org.co
[2] Página web del K + LAB:https://web.karisma.org.co/klab/

Fundación Karisma

De la misma forma, no debemos olvidar que las partes interesadas también pueden tener un rol en la creación de capacidades al interior de los Estados ya sea en el diseño o implementación de políticas de ciberseguridad, la capacitación de la ciudadanía en temas de ciberseguridad, la creación de capacidades para atender incidentes, la definición de infraestructura crítica o la divulgación responsable de vulnerabilidades, tal como lo explicamos en nuestras intervenciones anteriores.

En conclusión, señor presidente, esperamos que la participación de las múltiples partes interesadas continúe siendo sistemática y sustancial no solo al interior de OEWG, sino en los mecanismos que aquí sean aprobados. Debe tenerse en cuenta que una política de ciberseguridad que incluye a todas las partes interesadas suele ser más efectiva y realista que las que no, ya que las múltiples perspectivas permiten abordar los problemas que afectan a un mayor número de personas y empresas y, además, son de más fácil ejecución pues se ajustan a las exigencias técnicas y jurídicas preexistentes.

Muchas gracias.