GRUPO DE REVISIÓN DE LA IMPLEMENTACIÓN DE CUMBRES (GRIC)
Grupo Técnico Ad Hoc para el Programa Regional para la Transformación Digital
Primera Reunión
13 de diciembre de 2023

OEA/Ser.E
GRIC/CA-IX/GT-DIG/inf3/24
18 enero 2024
Original: español

CONTRIBUCIONES DE LA SOCIEDAD CIVIL Y ACTORES SOCIALES

Ciberseguridad

28.

El papel esencial de los ecosistemas digitales dinámicos y resilientes es apoyar las economías digitales pujantes, mejorar la preparación para futuros eventos de salud, climáticos y desastres naturales, promover la inclusión digital de todos los pueblos, fomentar y promover el respeto por los derechos humanos y las libertades fundamentales, aumentar la innovación, la competitividad, la inversión, optimizar la prestación de servicios públicos, fortalecer el gobierno, la transformación y la confianza digital de la región, mediante el aprovechamiento de las tecnologías emergentes y digitales, son algunas de las oportunidades que aún tenemos pendientes. La transformación digital implica el acceso digital como derecho humano, con una red de internet abierta, interoperable y segura, y con un acceso amplio a las tecnologías digitales, donde se asegure la inclusión digital de todos los miembros de la sociedad.

Recomendamos la creación de una plataforma conjunta de los países para generar y gestionar informes enfocados en la protección, manejo y mejores prácticas de la ciberseguridad.

La posibilidad de incentivar y abrir los espacios para una escucha activa y participación permanente, permitirá visionar acciones a corto y mediano plazo, logrando que puedan diseñar una lista de criterios de posibles riesgos, las acciones preventivas y primeras respuestas a futuros ataques, acordes al avance constante de la tecnología.

29.

Los Estados Miembros tienen el objetivo de promover el desarrollo digital especializado en materia de ciberseguridad para la región, con enfoque en fortalecer las capacidades de identificación y gestión de riesgos de ciberseguridad en las diferentes partes interesadas e incentivar comportamientos y prácticas adecuadas en el ámbito digital por parte de toda la sociedad.

Promover compromisos regulares en los que las organizaciones de ciberseguridad se conecten para revisar las últimas tendencias y métodos para mantenerse seguros, lo que permitirá a los ciudadanos y a las empresas mantenerse actualizados sobre el conocimiento y los procesos de recuperación de las tendencias de ciberseguridad. Sugerimos la creación de un “Ciber Seguro”, que pueda proteger a los Estados miembros, empresas, sociedad civil de las pérdidas por los Ciberataques.

30.

Los Estados Miembros deben de fomentar la discusión de estándares y el intercambio de las mejores prácticas en las áreas de ciberseguridad para la protección de los usuarios, consumidores, y de la ciudadanía en general, sobre prevención del ciberdelito, de conformidad con las disposiciones de instrumentos internacionales y regionales, como el convenio sobre la ciberdelincuencia del consejo de Europa (Convenio de Budapest) cuando corresponda, con participación del sector privado, sector académico y otras partes interesadas. Los estándares deben de ser incluidos en todos los convenios e instrumentos internacionales, académicos y comerciales. Se debe de ofrecer la estandarización del protocolo mínimo de ciberseguridad orientado a la protección de las empresas basadas en la nube. Fomentar la adopción y las mejores prácticas basadas en los estándares mínimos. Promover la colaboración entre las empresas privadas y organizaciones gubernamentales para apoyarse mutuamente en caso de que haya evidencia de una amenaza de ciberseguridad.

31.

Los Estados Miembros acordaron promover y fortalecer la cooperación internacional entre los Estados para prevenir, enjuiciar, investigar y juzgar eficazmente los delitos cibernéticos, el uso ilícito de datos pertenecientes a instituciones gubernamentales, privadas y personas; y otras actividades delictivas fomentadas por el uso indebido de las tecnologías de la información y la comunicación, como la trata de personas, el tráfico ilícito de migrantes, la explotación sexual infantil y otras formas de violencia sexual, el tráfico ilícito de drogas y armas, así como el lavado de activos, entre otros, en un marco de respeto a los derechos humanos y con perspectiva de género.

Los Estados Miembros tienen el compromiso de la revisión de las leyes vigentes para castigar los delitos de ciberataques, cometidos por adultos contra niñas, niños, adolescentes, personas con discapacidad, adultos mayores, así como los cometidos mediante la contratación de terceros para generar un terrorismo psicológico, persecución real y suplantación de identidad en contra de personas que ejercen sus derechos políticos; especialmente aquellos en los que la víctima es un menor o considerado un grupo en vulnerabilidad.

Hay una ausencia de soluciones de datos abiertos que permita compartir información sobre ciberdelincuencia, trata humana, migrantes desaparecidos entre los Estados Miembros.

Dado que Estados Unidos y Canadá son pioneros en tecnología, es importante que apoyen a otros Estados Miembros menos desplegados en la materia a desarrollar protocolos para garantizar que los servicios de Información Tecnológica y comunicación estén protegidos, especialmente aquellos que prestan servicios en la atención médica, defensa de los derechos humanos, ambientalistas al igual aquellas organizaciones que brindan servicios básicos a la población.

32.

Impulsar la asistencia técnica, programas, proyectos y la transferencia de capacidades y experiencias para prevenir los ciberdelitos en tecnología de la información y comunicación entre los estados, de acuerdo con su respectivo ordenamiento jurídico internacional. Previo a la aprobación es necesario un acuerdo sobre Ciberdelito y tecnología aprobado que vaya de la mano con el cumplimiento a la normativa sobre el ordenamiento jurídico internacional, CDI y la Declaración universal de DDHH.

33.

Apoyar debates en el marco de la naciones unidas y otros foros globales y regionales sobre las amenazas existentes y emergentes, el desarrollo e implementación del marco del comportamiento responsable por parte del Estado Miembro en el ciberespacio, incluyendo el respeto por el derecho internacional en las a las actividades del ciberespacio, las medidas de fomento de la confianza, el desarrollo de capacidades y el diálogo institucional para promover el uso responsable de las TIC por parte de los Estados Miembros, la paz y estabilidad internacional.

La transformación digital debe reconocer el derecho a la identidad, se requiere que todos los ciudadanos tengan acceso a sus documentos de identidad y ciudadanía y que estos no se limiten por razones políticas, sociales, culturales, ideológicas o económicas, que la diáspora o exilio tenga derecho a voto (e-democracy).

Los debates o encuentros debieran tener varios enfoques:

Autofinanciamiento por cada Estado, rectificación del acuerdo por Estado Miembro e incorporación en el marco legal en cada país de lo ya aprobado; la conclusión de la auditoria del avance y verificación de resultados para optar a financiamiento de asistencia técnica para su autosostenibilidad. Esto se debe dar en un contexto de ciberseguridad.

El requerimiento principal para participar en el siguiente evento internacional y ser parte de la plataforma internacional para su certificación CICTE, es obteniendo la certificación de legitimad de proceso electoral del Estado Miembro ante el Consejo Permanente de la OEA.

34.

Fortalecer las articulaciones con el sector privado, el sector académico, la sociedad civil y otras partes interesadas para promover la responsabilidad compartida, cooperación y desarrollar acciones coordinadas en materia de seguridad y confianza digital frente a los riesgos en el entorno digital. La transformación digital como un contexto de importante dinamismo requiere el seguimiento permanente de los compromisos asumidos en la Novena Cumbre de las Américas, es por esta razón que los actores y organizaciones de la sociedad civil proponen la creación del Observatorio de Transformación Digital de las Américas.

Se debe fomentar la colaboración entre agencias privadas y gubernamentales para garantizar la legitimidad de los procesos electorales (antes, durante y despues) protegiendo la integridad de los datos finales en cualquier elección que se realice dentro de los Estados Miembros.

Dentro de la transformación digital uno de los puntos a poner énfasis es la identificación de las infraestructuras críticas, especialmente aquellas que abastecen de servicios básicos a los ciudadanos, no por su concepto si no por su ubicación, categorizando su grado de impacto en el caso de un ciberataque logrando con ello una métrica de probabilidad, así también poder realizar un análisis de acciones contra las mismas lograrán una mejor protección y cuidado por parte de los Estados Miembros. La protección de las infraestructuras críticas en la era digital es un desafío constante, y la colaboración entre gobiernos, empresas privadas, la academia y otros actores relevantes, es fundamental para abordar estas amenazas de manera efectiva. Desarrollar un protocolo de emergencia cada doce meses como respuesta de emergencia a nivel nacional a la guerra y los ataques cibernéticos.

La colaboración de la empresa privada, organizaciones gubernamentales, academia y sociedad civil es primordial en proteger los espacios cibernéticos dentro de los países democráticos.