OEA
Parlamentos
LABORATORIO DE CIBERSEGURIDAD

LOS 10 PRINCIPIOS RECTORES DE LA CIBERSEGURIDAD CIUDADANA

Los principios rectores para la Ciberseguridad Ciudadana son el resultado de un esfuerzo co-creativo entre legisladoras y legisladores, asesores parlamentarios, expertos del sector privado en los campos de la ciberseguridad y la transformación digital, así como, de académicos y líderes de sociedad civil, quienes bajo la coordinación del Laboratorio en materia de Ciberseguridad para los Poderes Legislativos, identificaron 10 lineamientos básicos para que todo Estado impulse la creación de políticas públicas, legislaciones, marcos normativos y reglamentos que le ofrezcan a las y los ciudadanos una mejor protección en su interacción con las actuales infraestructuras tecnológicas, como son la Internet, las redes sociales y los sistemas y/o plataformas de la información y de la comunicación.

El principal objetivo de estos principios rectores es dotar de una herramienta coherente, rigurosa y estructurada, que les permita a los Estados garantizar una eficaz inclusión, alfabetización y universalización digital, así como, proveer a las personas de la mayor protección posible ante las graves amenazas y efectos dañinos que existen en el ciberespacio.

Los 10 principios rectores de la Ciberseguridad Ciudadana son:

1. RESGUARDAR Y PROTEGER LOS DERECHOS Y LIBERTADES INDIVIDUALES:

Los Estados deben garantizar el derecho a la conexión, inclusión e igualdad en el acceso a la internet.

2. PRESERVAR LA SOBERANIA EN LA DEMOCRACIA DIGITAL:

Corresponde al Estado establecer la normativa necesaria a fin de garantizar la soberanía digital, así como, impulsar incentivos para que los proveedores de plataformas digitales y servicios tecnológicos garanticen el ejercicio de una ciudadanía digital plena, donde existan las condiciones para gestionar el anonimato, el equilibrio en la contratación de servicios, los derechos a la propiedad y los alcances de la localización.

3. CONSAGRAR LA LIBERTAD DE EXPRESION Y LA PRIVACIDAD POR DEFECTO EN EL CIBERESPACIO:

Corresponde al Estado fomentar y potenciar acciones, normas y procedimientos que, por una parte, garanticen la libertad de expresión y la privacidad por defecto y, por otra, impidan el acoso, las amenazas y los ataques al honor y dignidad de las personas, y que, en caso de conflicto entre unas y otras, provea mecanismos de solución que sean efectivos, razonables y proporcionales.

4. IMPULSAR UNA CULTURA DE LA CIBERSEGURIDAD:

El Estado debe comprometerse en activar iniciativas, tanto en el ámbito público como en el privado, que permitan la sensibilización y concientización en el uso responsable y seguro del ciberespacio, privilegiando la socialización e inclusión, y atendiendo aquellos factores que contribuyan a atender los problemas derivados de la brecha digital.

5. CONSTRUIR UN ENTORNO CIBERSEGURO:

Todo Estado debe procurarle al ciudadano un ecosistema digital participativo y resiliente en su conjunto, donde la máxima sea usar la tecnología para preservar la libertad.

6. ASEGURAR LA PRIVACIDAD DE LOS DATOS:

Los Estados deben velar por la protección de los datos personales y la privacidad, así como, delimitar de manera rigurosa la responsabilidad de quienes brindan servicios tecnológicos, con el fin de incrementar su función social y garantizar el bienestar de los ciudadanos en el uso de las tecnologías de información y comunicación. Particularmente, debe garantizarse el ejercicio de una supervisión oportuna por parte de padres, tutores y representantes en pro del bienestar de los niños, niñas y adolescentes.

7. ESTABLECER LA RESPONSABILIDAD COMPARTIDA:

El Estado debe identificar el alcance de las responsabilidades de los usuarios en el uso de las tecnologías de la información y comunicación, así como las responsabilidades de los proveedores e intermediarios de los servicios tecnológicos. Reconocer la existencia de una responsabilidad compartida de usuarios y proveedores permitirá que se acepte o rechace fácilmente una aplicación y/o servicio tecnológico, que se garantice la usabilidad como diseño y que los datos sean utilizados únicamente cuando sea justificado.

8. FORTALECER EL DESARROLLO DE APTITUDES Y HABILIDADES:

Los Estados deben contemplar acciones que fortalezcan el desarrollo de aptitudes y habilidades técnicas y jurídicas necesarias para que los ciudadanos sepan gestionar sus datos, conozcan sus derechos, sean conscientes de las condiciones que han aceptado, sepan detectar y prevenir incidentes y amenazas en el ciberespacio, y que dichas acciones garanticen que un ciudadano pueda realizar reclamos efectivos contra intermediarios y proveedores de servicio en su propio país.

9. INCORPORAR LA EDUCACION PARA LA VIDA EN EL CIBERESPACIO:

Cada Estado debe asegurar un conocimiento abierto y asequible a la ciencia, la tecnología, la innovación y especialmente a la ciberseguridad, con una visión puesta al servicio del desarrollo humano, digital, económico y social. Para ello, es fundamental optimizar las políticas públicas y las legislaciones con el fin de fortalecer las instituciones estatales y privadas a cargo de la educación y formación de talento humano, así como definir partidas presupuestales suficientes para la investigación, el desarrollo y la innovación (I+D+i).

10. INVOLUCRAR A LA CIUDADANIA EN LOS PROCESO DE CREACION DE MARCOS NORMATIVOS QUE IMPULSEN LA INNOVACION Y LA TRANSFORMACION DIGITAL:

Corresponde a los Estados el reconocimiento de la importancia de que el ciudadano se involucre activamente en los procesos de transformación digital en su conjunto. La seguridad del ciudadano debe constituir la esencia de la innovación para lograr un ciberespacio seguro que procure un mejor nivel de vida individual y social.