INTERVENCIONES DE EL SALVADOR EN LA SEGUNDA SESIÓN SUSTANTIVA DEL GRUPO DE TRABAJO DE COMPOSICIÓN ABIERTA SOBRE LA SEGURIDAD Y LA UTILIZACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES PARA EL PERÍODO 2021-2025

1. Seguir estudiando, con miras a promover el entendimiento común, **las amenazas actuales y potenciales en la esfera de la seguridad de la información**, incluida la seguridad de los datos, y las posibles medidas de cooperación para prevenir y contrarrestar esas amenazas.

INTERVENCIÓN
Señor Presidente,

Nuestra delegación le agradece la convocatoria a este segundo período de sesiones del Grupo de Trabajo de Composición Abierta sobre la seguridad y la utilización de las tecnologías de la información y comunicaciones. Respecto del punto de agenda en discusión El Salvador propone las siguientes medidas preventivas y de respuesta ante las amenazas ya identificadas en el primer periodo de sesiones.

1. En el sector público con miras a reducir las amenazas causadas por el ransomware y para promover la seguridad de los datos, se sugieren las capacitaciones en ciberseguridad a los funcionarios a todo nivel para practicar el uso seguro de TICs particularmente dentro de los sistemas institucionales. Entendemos que estas amenazas comprometen información y datos sensibles, por lo que mayor conocimiento de cómo se vulneran los sistemas internos puede ser clave para prevenir estas vulneraciones y para hacer un uso más responsable de los sistemas de la información y las telecomunicaciones.
2. A nivel general, se sugiere se lleven a cabo campañas de educación en temas de ciberseguridad, ahondado en los riesgos asociados a los usos de tecnologías de la información y la comunicación para fomentar un uso responsable que permita el pleno goce de los derechos ciudadanos en el mundo digital. El objetivo es promover buenos hábitos y responsabilidad en el uso de las TICs.
3. Respecto de la protección de infraestructura crítica, incluida la infraestructura de información crítica contra amenazas existentes y potenciales, se propone el desarrollo de normativas que permitan inicialmente clasificar activos estratégicos nacionales, para luego formular estrategias de protección. En esa línea es básico continuar trabajando en como compartir las mejores prácticas para proteger la infraestructura crítica a todos los niveles. El objetivo final es crear un esquema de ciberseguridad resiliente que permita la protección de la infraestructura crítica y activos estratégicos nacionales.

4. El establecimiento y fortalecimiento de los equipos nacionales de respuesta a incidentes en el ciberespacio es un componente central para compartir información de amenazas e incidentes en tiempo real. A nivel regional la Organización de Estados Americanos ha ofrecido asistencia técnica para el establecimiento de los centros de respuesta a incidentes de seguridad informática. El Salvador es uno de los beneficiarios de esta asistencia técnica personalizada que fortalecerá la institucionalidad nacional en los temas de ciberseguridad.
5. Como último punto se reconoce la importancia de continuar estas discusiones sobre amenazas potenciales, dado que entendemos que los avances en las tecnologías emergentes son de rápido desarrollo.