INFORME DE COLOMBIA EN VIRTUD DEL PARRAFO 46 DEL "SEGUNDO REPORTE ANUAL DEL GRUPO DE TRABAJO DE COMPOSICION ABIERTA SOBRE EL USO Y LA SEGURIDAD DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS TELECOMUNICACIONES"

Atendiendo a lo solicitado en el párrafo 46 del "Informe del Grupo de Trabajo de Composición Abierta sobre el uso y seguridad de las telecomunicaciones 2021-2025", contenido en el documento 78/265, en relación con el ejercicio de mapeo del panorama de programas e iniciativas de construcción de capacidad, incluidas las opiniones de los Estados, se remite a continuación el punto de vista de Colombia:

NECESIDADES DE CONSTRUCCIÓN DE CAPACIDAD NACIONAL EN MATERIA DE SEGURIDAD DE LAS TICS IDENTIFICADAS POR COLOMBIA

- Mejora de la infraestructura de seguridad. Realizar evaluación y actualización de cada una de las infraestructuras de seguridad con que se cuenta (firewalls, Sistemas de detección de intrusos y medidas de protección de red, entre otros) para garantizar un entorno más seguro.

- Políticas y procedimientos de seguridad. Desarrollo y actualización de las políticas de seguridad, incluyendo protocolos de respuesta a incidentes y uso de la inteligencia artificial.

- Gestión de Riesgos. Implementación de marcos de gestión de riesgos que identifiquen, evalúen y mitiguen las amenazas potenciales de seguridad de las TICS.

- Actualización tecnológica continua. Mantenimiento y actualización periódica de los sistemas de información, hardware y software para mitigar vulnerabilidades conocidas y asegurar los entornos digitales

- Análisis de vulnerabilidades a aplicaciones (código fuente) mediante inteligencia artificial. Fortalecer el equipo humano con el propósito de incrementar capacidades en respuesta a incidentes.

- Fortalecimiento de habilidades técnicas en las capacidades de análisis forense y evidencia digital.

- Apoyo en el desarrollo de mecanismos de asistencia legislativa para la estructuración de lineamientos técnicos y doctrina jurídica sectorial y/o nacional que contribuya a impulsar la generación de normas, afines con los estándares internacionales en materia de aplicación del Derecho Internacional en el ciberespacio.

- Capacitación y colaboración para una mayor comprensión sobre la aplicación del Derecho Internacional y el Derecho Internacional Humanitario en el ciberespacio.

- Fortalecimiento en la comprensión e implementación de las normas voluntarias de comportamiento responsables en el uso y seguridad de las TIC.

- Profundización sobre entendimientos comunes en lo que se refiere a amenazas existentes y potenciales, así como la creación de esquemas de intercambio de información y generación de conocimiento respecto a tales amenazas. Igualmente, fortalecer la inteligencia sobre amenazas latentes a través de las redes, comunidades, agencias y comités del orden nacional e internacional.

- Apoyo en la realización de ejercicios de simulación de ciberataques que impliquen respuesta, recuperación y gestión técnica y de conocimiento para eventos futuros.

- Capacitación de los funcionarios que hacen parte de las instancias con responsabilidad en la seguridad digital, que hacen parte del ecosistema digital nacional y/o sectorial, con el propósito de enfrentar de manera preventiva las amenazas en el ciberespacio y los procesos de recuperación y resiliencia.

- Actualización constante de las herramientas tecnológicas, infraestructura de hardware y adquisición de software que permitan incrementar la capacidad de procesamiento, correlación, búsquedas avanzadas en grandes volúmenes de datos, recolección de información que puede servir como elemento material probatorio en campo y actividades que exigen unas características técnicas superiores a las contenidas en los equipos de cómputo convencionales; atendiendo la rápida obsolescencia de este tipo de recursos.

- Fortalecimiento de plataforma y procesos de criptografía. Se requiere darles mayor importancia a los procedimientos de Criptografía con el fin de garantizar la confidencialidad e integridad de la información que se maneja a nivel nacional.

- Es necesario el apoyo en la definición de rutas claras para la atención y recuperación en caso de la materialización de incidentes de seguridad digital.

- Generar capacidades para impulsar emprendimientos nacionales de base tecnológica relacionados con seguridad digital, el cual responda a los desafíos que se presenten, desde la realidad nacional.

- Es fundamental definir metodologías y apropiar mejores prácticas para realizar el levantamiento del inventario de infraestructuras críticas cibernéticas y de servicios esenciales.

- Desarrollar capacidades de formación especializada, con el fin de aumentar el conocimiento y la conciencia de los riesgos cibernéticos entre los diferentes grupos poblacionales del territorio colombiano.

ALGUNAS INICIATIVAS REGIONALES O GLOBALES DE CONSTRUCCIÓN DE CAPACIDAD EN MATERIA DE SEGURIDAD DE LAS TIC, DE LAS QUE COLOMBIA HA SIDO BENEFICIARIO:

- Acompañamiento metodológico de la Carnegie Mellon University, apoyado por el Departamento de Estado y la Embajada de los Estados Unidos, para la construcción del plan de acción de la Oficina de Respuesta a Incidentes Cibernéticos de Colombia (CSIRT DEFENSA).

- Mediante el acompañamiento del Ministerio de Relaciones Exteriores de Colombia, se realizó la vinculación del CSIRT – Defensa del Ministerio de Defensa Nacional y los CSIRT de las Fuerzas Militares de Colombia en el Programa CSIRT – Américas, que lidera el comité interamericano contra el terrorismo (CICTE) de la Organización de Estados Americanos (OEA). Este programa permite compartir información de indicadores de Compromisos e Inteligencia de Amenazas que busca afectar la región.

- Actualmente desde el Departamento Nacional de Planeación se está trabajando en una iniciativa de Cooperación Técnica Regional No Reembolsable Regional con el Banco Interamericano de Desarrollo (BID), para el "Apoyo al cierre de brechas de las empresas en Latinoamérica en ciberseguridad", que tiene como objetivo apoyar a los países beneficiarios (Colombia, Costa Rica y Panamá) en la creación de políticas públicas para sensibilizar a las empresas en ciberseguridad a partir de la identificación de brechas, exploración de sectores/cadenas, identificación de problemas específicos, y diseño de programas de formación para empresas y particulares que permitan aumentar la oferta de personas con habilidades digitales avanzadas relevantes para la ciberseguridad. El resultado esperado es que las empresas fortalezcan sus capacidades de ciberseguridad para poder insertarse en clústeres y cadenas globales de valor (CGV). Esta cooperación se trabajará de manera articulada con el Ministerio de Tecnologías de la Información y las Comunicaciones y el Departamento Administrativo de la Presidencia de la República, teniendo en cuenta sus competencias con respecto a seguridad y confianza digital. Hasta el momento se ha solicitado a la Agencia Presidencial de Cooperación Internacional de Colombia (APC-Colombia) que se prioricen los recursos de manera oficial ante el BID.

- De igual forma, el Ministerio de Relaciones Exteriores de Colombia ha sido beneficiario de varias iniciativas de construcción de capacidad en ciber diplomacia, en particular, la Escuela de Verano de Tallin sobre ciber diplomacia, liderado por el Gobierno de Estonia; el programa Mujeres en Ciber, a través del cual se ha contribuido enormemente al cierre de la brecha de género en las negociaciones multilaterales sobre ciberseguridad, y que para el caso de

Colombia es patrocinado por el Gobierno de Canadá; y el Programa de Becas cibernéticas ONU-Singapur, dirigida a funcionarios con amplia experiencia y capacidad de decisión en el campo de la ciberseguridad.

- Por último, se destaca la Misión sobre ciberseguridad e inteligencia artificial liderada y organizada por el Gobierno de la República Checa, esta iniciativa bilateral contó con una amplia participación interinstitucional a nivel gubernamental y de sociedad civil de ambos países. En el marco, de la Misión que tuvo lugar del 8 al 14 de octubre, se abordaron, entre otras, temáticas como Legislación, políticas y estrategias en el campo de la ciberseguridad; Cooperación público-privada en el campo de la ciberseguridad; y ciberdelincuencia y herramientas forenses.