PROPUESTA DE COOPERACIÓN HEMISFÉRICA EN CIBERDEFENSA EN EL MARCO DE XIV CONFERENCIA DE MINISTROS DE DEFENSA DE LAS ÁMERICAS (CMDA)

MINISTERIO DE DEFENSA DE LA REPÚBLICA FEDERATIVA DE BRASIL

22 DE NOVIEMBRE DE 2019

El Ministerio de Defensa de la República Federativa de Brasil ha decidido levantar una propuesta de "Cooperación Hemisférica en Ciberdefensa" para promover un ciberespacio internacional seguro y confiable, en apoyo a los intereses nacionales y con la finalidad de fomentar una colaboración y cooperación más estrecha entre los países miembros de la CMDA.

Esta propuesta reconoce las oportunidades y riesgos que la globalización tecnológica crea y los beneficios de la colaboración mutua para lograr estándares globales, expandir el sistema jurídico internacional y desarrollar y promover mejores prácticas en materias de Ciberdefensa.

1. Validar definiciones, grados de alerta y de impacto

- Se pretende adoptar una taxonomía común a nivel internacional, de manera de facilitar el intercambio de información ante ciber amenazas. El objetivo es unificar lenguaje y definiciones, adoptando y/o definiendo normas y estándares en materias de ciber incidentes.

2. Establecer un protocolo de intercambio de información

- La mayoría de los países de la OTAN y sus socios, así como varios países de la región (algunos participantes del Foro Iberoamericano de Defensa Cibernética) y sus respectivas instituciones civiles y militares, ya están usando la plataforma MISP (https://www.misp-project.org/), la cual es una plataforma que permite el Intercambio de información ante ciber amenazas, definiendo un protocolo para ello. Se busca que los países se sumen a esta iniciativa de forma de unificar protocolos a nivel internacional.

- La uniformidad conceptual ayudará a acortar y facilitar cualquier posible informe y divulgación de ciber incidentes, mejores prácticas y más medidas de contingencia; así como de utilidad al intercambiar información para diferentes propósitos, por ejemplo, cursos, entrenamiento, ejercicios, simulaciones, etc.

- MISP podría ser un instrumento valioso para la adopción de acciones preventivas y reactivas ante ciber incidentes.

3. Protección de Infraestructuras Críticas

- Se pretende establecer protocolos de acción preventiva sobre amenazas a los sistemas de información de las Infraestructuras Críticas.

- Crear protocolos para intercambiar información y producir las alarmas necesarias ante la detección de conductas anómalas en la operación, así como los intentos de intrusión a los controladores de los activos protegidos.

Por último, se hace presente que las ciber amenazas no respetan los límites físicos y pueden tener efectos de defensa, lo que hace que la acción de colaboración internacional sea de gran valor en el escenario en cuestión.