

Opinión de México sobre las capacidades necesarias para participar en el directorio global de puntos de contacto (PoCs) sobre ciberseguridad, en el marco del Grupo de Trabajo de Composición Abierta (GTCA 2021-2025)

México participa en redes de respuesta a incidentes cibernéticos, a través de la designación puntos de contacto nacionales en los siguientes mecanismos de comunicación y cooperación:

- **Red CSIRTAméricas en el marco de la Organización de los Estados Americanos (OEA).** Participación de entidades operativas.
- **Directorio Regional de Puntos de Contacto para el portal de CBMs del Comité Interamericano contra el Terrorismo (CICTE) de la OEA.** Participación de entidades operativas y un punto de contacto diplomático.
- **Red 24/7 de Interpol.** Participación de entidades operativas.
- **Red 24/7 del Consejo de Europa-Convenio de Budapest.** Participación de entidades operativas.

Con base en dicha experiencia, y considerando las experiencias compartidas por las agencias de operación de respuesta ante incidentes cibernéticos del Gobierno de México, se han identificado los siguientes elementos que podrían ser útiles en cuanto al desarrollo y fortalecimiento de capacidades para la operacionalización del Directorio Global de Puntos de Contacto (PoC):

- **Papeles claros:** a fin de facilitar la identificación de capacidades nacionales, será importante trabajar en la definición de los papeles, responsabilidades y expectativas del Directorio Global de Puntos de Contacto, a fin de que los PoC designados tengan claridad frente a la gestión de incidentes.
- **Capacidades Técnicas Avanzadas:** es importante reconocer la brecha digital y necesidades diferenciadas entre los Estados Miembros. El intercambio de experiencias, el fomento a la asistencia técnica, e incluso la transferencia de tecnología, contribuirá significativamente a la construcción de capacidades en cuanto a la detección, análisis, mitigación y recuperación ante incidentes cibernéticos.
- **Comunicación Efectiva y Colaboración:** como punto de partida, se considera esencial la identificación y establecimiento de un canal de comunicación efectivo, en tanto el éxito del Directorio Global de PoCs, dependerá en buena medida de la rapidez y eficacia con la que sus miembros sean capaces de establecer canales seguros y confiables para el intercambio de información sobre amenazas, así como la colaboración en la respuesta y mitigación de estas.
- **Respuesta 24/7:** será importante definir si se espera que el punto de contacto operativo/técnico tenga una capacidad de respuesta 24/7. De ser el caso, será deseable que el establecimiento de procedimientos de escalado y comunicación efectivos para situaciones fuera del horario “regular”.
- **Creación de capacidades:** será ideal que los puntos de contacto tengan acceso a iniciativas formales de creación de capacidades, de manera sistemática, con base en los principios de cooperación internacional contenidos en el Anexo C del segundo informe anual sobre los progresos

realizados del GTCA 2021-2025. Asimismo, será deseable la participación en ejercicios de tipo "table-top" y simulacros de respuesta.

- Como resultado de la participación en las redes de respuesta a incidentes cibernéticos, las entidades nacionales de México han llevado a cabo el establecimiento de colaboraciones estratégicas centradas en la capacitación en Gestión de Incidentes de Seguridad Informática, con el objetivo principal de fortalecer sus capacidades técnicas y operativas, logrando mejorar significativamente la preparación y respuesta ante incidentes de seguridad informática, lo cual ha contribuido de manera significativa a la seguridad digital del país.
- **Gestión de Crisis y Recuperación:** será deseable el desarrollo y revisión constante de planes de gestión de crisis y recuperación ante incidentes graves, tanto a nivel nacional, regional e internacional.
- **Adhesión a estándares internacionales y marcos regulatorios relevantes en materia de ciberseguridad:** una base optima de estandarización de procesos a nivel regional ha sido por ejemplo la implementación del marco NIST de ciberseguridad, con el que a nivel regional se encuentran ya familiarizados los PoCs.

oOo

[COURTESY TRANSLATION]

Mexico's views on the capacities required to participate in the PoC directory on cybersecurity, within the framework of the Open Ended Working Group (OEWG 2021-2025)

Mexico participates in networks for responding to cyber incidents, through the designation of national points of contact in the following communication and cooperation mechanisms:

- **CSIRT Americas Network within the framework of the Organization of American States (OAS).** Participation of operational entities.
- **Regional Directory of Points of Contact for the CBMs portal of the Inter-American Committee against Terrorism (CICTE) of the OAS.** Participation of operational entities and a diplomatic point of contact.
- **INTERPOL 24/7 Network.** Participation of operational entities.
- **24/7 Network - Council of Europe-Budapest Convention.** Participation of operational entities.

Based on this experience, and considering the shared experiences of Mexican Government cyber incident response agencies, the following elements have been identified that could be useful for the development and strengthening of capabilities for the operationalization of the global Points of Contact (PoC) directory:

- **Defined roles:** to facilitate the identification of national capabilities, it will be important to work on defining the roles, responsibilities, and expectations of the Global Directory of Points of Contact, so that the designated PoCs have clarity on incident management.
- **Advanced technical capacities:** is important to recognize the digital gap and the differentiated needs of Member States. The exchange of experiences, the promotion of technical assistance, and even the transfer of technology, will contribute significantly to capacity building in terms of detection, analysis, mitigation, and recovery from cyber incidents.
- **Effective communication and collaboration:** the identification and establishment of an effective communication channel is considered essential as a starting point, since the success of the Global PoC Directory will depend -to a large extent- on the speed and efficiency with which its members are able to establish secure and reliable channels for the exchange of information on threats, as well as collaboration in the response and mitigation of these threats.
- **24/7 response:** it will be important to define whether the operational/technical contact point is expected to have a 24/7 response capacity. If so, it will be desirable to establish effective escalation and communication procedures for situations outside of "regular" hours.
- **Capacity building:** it will be ideal for points of contact to have access to formal capacity-building initiatives, systematically, based on the principles of international cooperation contained in Annex C of the second annual

progress report of the OEWG 2021-2025. Likewise, participation in "table-top" exercises and response drills will be desirable.

- As a result of their participation in cyber incident response networks, Mexican national entities have carried out the establishment of strategic collaborations focused on training in Computer Security Incident Management, with the main goal of strengthening their technical and operational capabilities, achieving a significant improvement in preparedness and response to computer security incidents, which has contributed significantly to the country's digital security.
- **Crisis management and recovery:** the development and constant review of Cyber Crisis Management Plan for serious incidents, at the national, regional, and international levels, will be desirable.
- **Adherence to international standards and relevant regulatory frameworks in cybersecurity:** an optimal basis for standardizing processes at the regional level has been, for example, the implementation of the NIST Cybersecurity Framework, which PoCs are already familiar at the regional level.

oOo