Organización de Aviación Civil Internacional

A41-WP/158
EX/72
2/8/22

NOTA DE ESTUDIO

ASAMBLEA — 41º PERÍODO DE SESIONES

COMITÉ EJECUTIVO

Cuestión 14: Seguridad de la aviación — Política

CREACIÓN DE CAPACIDAD E INSTRUCCIÓN EN CIBERSEGURIDAD DESTINADA A LOS ESTADOS

(Nota presentada por Guyana con el apoyo de la Argentina, Bolivia, el Brasil, Colombia, el Ecuador, El Salvador, Guatemala, Panamá, el Perú, la República Dominicana, el Uruguay y Venezuela)

RESUMEN

La ciberseguridad es un fenómeno multidisciplinar que constituye una amenaza para la aviación civil. La OACI ha reconocido esta amenaza a la seguridad de la aviación civil internacional y, para responder a ella, ha formulado su Estrategia de Ciberseguridad y su Plan de Acción de Ciberseguridad. Si bien estas políticas y textos de orientación son útiles para los Estados, es imprescindible que estos se doten de los conocimientos, la capacidad, la instrucción y los recursos necesarios para mitigar eficazmente las ciberamenazas y los ciberriesgos a escala nacional, regional e internacional.

Por ello, en esta nota de estudio se pide que la OACI dedique recursos a la creación de capacidad a fin de que los Estados satisfagan los objetivos de los siete pilares de su Estrategia de Ciberseguridad, que se enumeran a continuación:

a) Cooperación internacional;
b) Gobernanza;
c) Leyes y reglamentos eficaces;
d) Política de ciberseguridad;
e) Intercambio de información;
f) Gestión de incidentes y planificación ante emergencias; y
g) Creación de capacidad, instrucción y cultura de ciberseguridad

Decisión de la Asamblea: Se invita a la Asamblea a:

a) encargar al Consejo que solicite a la Secretaría que dedique recursos a la resiliencia y la creación de capacidad en materia de ciberseguridad destinada a los Estados pequeños. Entre los ámbitos de interés se encuentran la instrucción en materia de conciencia sobre ciberseguridad, la instrucción en gestión de incidentes de ciberseguridad y respuesta ante emergencias, y el programa de instrucción y certificación de instructores/as de ciberseguridad; y
b) pedir que la OACI promueva y cree un mecanismo de cooperación para fomentar los programas de mentoría e intercambio técnico en la esfera de la aviación entre los Estados.

Objetivos estratégicos:	Esta nota de estudio se relaciona con el objetivo estratégico de *Seguridad de la aviación y facilitación*.
Referencias:	Anexo 17 — *Seguridad de la aviación* *Estrategia de Ciberseguridad de la Aviación* *Plan de Acción de Ciberseguridad*

1. INTRODUCCIÓN

1.1 El tráfico de la aviación civil tiene previsiones de crecimiento, al igual que su utilización de la tecnología. Esa mayor utilización de la tecnología conlleva mayores amenazas y riesgos, por lo que la ciberseguridad es una cuestión importante para los Estados, que deben reforzar su resiliencia frente a esta amenaza. La ciberseguridad en la aviación es fundamental, ya que incide en un ámbito amplio que abarca aspectos de seguridad operacional, seguridad de la aviación, navegación aérea, sistemas ICT y operaciones de la aviación general. La Estrategia de Ciberseguridad y el Plan de Acción de Ciberseguridad de la OACI proporcionan la orientación necesaria para que los Estados empiecen a sentar las bases de una infraestructura sólida de ciberseguridad. Sin embargo, para ello se requiere la creación de capacidad, instrucción, una cultura de la ciberseguridad y la colaboración interinstitucional e interregional.

1.2 Para construir una infraestructura sólida de ciberseguridad, los Estados deben seguir los siete pilares de la Estrategia de Ciberseguridad de la Aviación de la OACI y adoptar el Plan de Acción de Ciberseguridad de la Organización, que sienta las bases para que los Estados, las partes interesadas de la industria y la OACI trabajen juntas con el objetivo de desarrollar la capacidad de determinar, prevenir y detectar los ciberataques a la aviación civil, y de darles respuesta y recuperarse de sus efectos, así como de crear un marco de cooperación. El Plan de Acción de Ciberseguridad propone varias medidas y acciones que los Estados deberían adoptar para satisfacer los objetivos de los siete pilares. Entre ellos se cuentan la cooperación internacional entre los Estados, la creación de estructuras de gobernanza, la formulación de leyes y marcos reglamentarios nacionales eficaces, la elaboración de políticas de ciberseguridad, el intercambio de información pertinente entre los Estados, la gestión de incidentes y planificación ante emergencias, y la creación de capacidad, la instrucción y la promoción de una cultura de la ciberseguridad con el fin último de crear resiliencia para hacer frente a este fenómeno mundial.

1.3 La creación de capacidad es esencial para establecer una infraestructura sólida de la ciberseguridad (global). De hecho, constituye la base sobre la que se pueden construir los otros seis pilares. Por este motivo, se alienta a la OACI a fomentar y proporcionar la creación de capacidad necesaria destinada a los Estados, especialmente los pequeños.

2. ANÁLISIS

2.1 Guyana ha emprendido varias iniciativas para luchar contra los ciberataques y aumentar la resiliencia de la ciberseguridad que están en consonancia con los siete pilares de la Estrategia de Ciberseguridad de la Aviación. Este esfuerzo está encabezado por la Autoridad Nacional de Gestión de Datos (NDMA), la entidad designada para el control y la protección de los datos en el país. La NDMA ha empezado a redactar políticas, normas, leyes y reglamentos nacionales de ciberseguridad que se promulgan para su consulta a través de comités interinstitucionales. Se trata de un proceso iterativo que requiere aportaciones de los organismos pertinentes, en especial de los que tienen infraestructuras críticas. Teniendo en cuenta las limitaciones y los retos de los Estados pequeños, es necesario proporcionar orientación e instrucción externas sobre cómo enfrentar la ciberseguridad de manera holística. Si bien la información se comparte a escala nacional entre los organismos y la instrucción se solicita a través del comité interinstitucional, se necesita la creación de capacidad a nivel del Estado.

2.2 La creación de capacidad implica la impartición de la instrucción pertinente al personal de la aviación con el fin de incrementar sus conocimientos, habilidades, aptitudes y capacidades en materia de ciberseguridad. También conlleva la dotación de los recursos humanos y de capital necesarios para construir una infraestructura sólida de ciberseguridad. Se necesita personal cualificado y con experiencia para elaborar la legislación y reglamentación sobre ciberseguridad. Esta capacidad puede desarrollarse mediante la realización de talleres nacionales, regionales e internacionales. También requiere una formación pertinente y adecuada para fortalecer las capacidades de los Estados para gestionar los incidentes de ciberseguridad y

la planificación de la respuesta ante emergencias. Se trata de algo imprescindible, ya que los ciberataques no se pueden detener por completo, pero sí se pueden mitigar con sistemas sólidos. Así pues, los ciberataques no dejarán de producirse, pero es fundamental que los Estados sean capaces de crear una resiliencia que asegure la continuidad de las actividades.

2.3 La realización de sesiones de instrucción, talleres, programas de aprendizaje y de mentoría, etc., son necesarios para crear capacidad en los Estados pequeños. Se pueden ofrecer a los Estados individuales y a la región, según corresponda.

3. CONCLUSIÓN

3.1 En esta nota de estudio se reconoce la necesidad de que los Estados refuercen la creación de capacidad y la resiliencia en materia de ciberseguridad.

— FIN —