



ASAMBLEA — 42º PERÍODO DE SESIONES

COMITÉ EJECUTIVO

Cuestión 13: Seguridad de la aviación — Política

PLANES DE CONTINGENCIA Y EJERCICIOS CIBERNÉTICOS COMO MEDIO PARA
REFORZAR LA RESILIENCIA ANTE LAS AMENAZAS CIBERNÉTICAS

(Nota presentada por el Brasil)

RESUMEN

Esta nota de estudio hace hincapié en la necesidad de disponer de planes de contingencia para los sistemas críticos utilizados por la aviación civil, tal como se describe en el Plan de Acción de Ciberseguridad de la OACI correspondiente al pilar 6 de la Estrategia de Ciberseguridad de la Aviación de la OACI, así como la mejora de los planes derivados de ejercicios de entrenamiento con simulacros de ciberataques que se ajustan a las características reales de los sistemas y en hechos ya observados que podrían provocar dichos ataques. como se describe en el Plan de Acción de Ciberseguridad de la OACI correspondiente al pilar 7 de la Estrategia. Destaca la evolución de los ciberataques en la aviación civil, así como la importancia de los ejercicios correspondientes y los planes de contingencia.

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

- fomentar los planes de gestión de incidentes cibernéticos vinculados con la infraestructura crítica de la aviación; y
- organizar simulacros cibernéticos frecuentes, con la participación de partes interesadas gubernamentales y privadas.

<i>Objetivos estratégicos:</i>	Esta nota de estudio se relaciona con el Objetivo estratégico Todos los vuelos son seguros y protegidos.
<i>Repercusiones financieras:</i>	No tiene.
<i>Referencias:</i>	Pilar 6 (Gestión de incidentes y planificación de emergencias) y pilar 7 (Creación de capacidad, instrucción y cultura de ciberseguridad) de la Estrategia de Ciberseguridad de la Aviación de la OACI.

1. INTRODUCCIÓN

1.1 Las amenazas cibernéticas suponen un desafío importante y creciente para el sector de la aviación civil, un sistema global intrínsecamente interconectado donde las vulnerabilidades pueden contribuir a la rápida propagación de programas maliciosos, repercutiendo de forma generalizada y mundial. Si bien los avances tecnológicos han aportado numerosos beneficios a la aviación, también han generado amenazas cibernéticas variables debido a la gran dependencia de las infraestructuras digitales. Reconociendo la urgente necesidad de ciberprotección y resiliencia para los sistemas críticos de aviación, la Estrategia de Ciberseguridad de la Aviación de la OACI contiene principios, medidas y acciones basadas en siete pilares fundamentales.

1.2 Por tanto, esta nota de estudio describe algunas de las medidas tomadas por el Brasil para lograr una mayor resiliencia cibernética en situaciones en las que los pilares 6 (Gestión de incidentes y planificación de emergencias) y 7 (Creación de capacidad, instrucción y cultura de ciberseguridad) de la Estrategia de Ciberseguridad de la Aviación de la OACI pueden servir para la protección cibernética de activos importantes utilizados en el control del tránsito aéreo. Al integrar estos dos pilares, la aviación civil puede dotarse de una defensa integral y adaptable, no solo reaccionando a las amenazas, sino previniendo y mitigando activamente su impacto, garantizando la seguridad operacional y la fiabilidad constantes de los viajes aéreos.

1.3 El pilar 6 ofrece procedimientos de recuperación sólidos, con planes de contingencia claros y probados para iniciar de inmediato los procedimientos para restaurar los sistemas y datos comprometidos, con una interrupción mínima del control del tránsito aéreo, las operaciones en tierra y los servicios para el público pasajero. Esto incluye copias de seguridad, sistemas alternativos y pasos detallados para la recuperación.

1.4 El pilar 7 se refiere a la concienciación y la formación de todas las partes implicadas en el control del tránsito aéreo, capacitando a todas las personas, desde controladores/as hasta el personal de mantenimiento en tierra, sobre cómo responder a un incidente cibernético y su papel para disponer de un entorno seguro y protegido. Una sólida cultura de ciberseguridad significa que cada cual asume que es una primera línea de defensa potencial. Del mismo modo, el aprendizaje y la adaptación constantes son importantes, en el entendido de que las amenazas cibernéticas están en constante evolución y hay que adaptarse a las nuevas estrategias y tecnologías de ciberseguridad, lo que supone no caer nunca en la complacencia y esforzarse siempre por mejorar.

1.5 Estos principios son esenciales para estrechar la colaboración entre las autoridades de ciberseguridad de la aviación civil y otras partes interesadas para responder a los ciberataques, en un entorno firme en que los planes de contingencia permitan responder a toda actividad dañina. La coordinación entre todas las partes debería plasmarse en el documento, enumerando todos los mecanismos que estarán disponibles para restablecer las operaciones ordinarias una vez un sistema se ha visto comprometido, destacando los requisitos básicos para aplicar medidas de respuesta, a favor de un sistema de aviación mundial más seguro y resiliente.

2. ANÁLISIS

2.1 A diario, los medios de comunicación informan sobre intentos de ciberataque, algunos de los cuales culminan con éxito y otros que ni siquiera se notifican porque pudieron contenerse gracias a las diversas medidas de protección que las empresas y organizaciones implementan para hacer frente a estos ataques cotidianos. La situación no es diferente en el sector de la aviación. Quienes atacan buscan principalmente vulnerabilidades en sistemas no actualizados para intentar infiltrarse, sustraer información y modificarlos, normalmente con el objetivo de lucrarse.

2.2 El Brasil, a través de DECEA, ha elaborado medidas para que el sistema de control del espacio aéreo brasileño sea más resiliente en el contexto de las amenazas cibernéticas, que crecen cada día. Así, corroborando el planteamiento de la OACI sobre el tema e incorporando dos de los pilares citados en la estrategia de ciberseguridad de la Organización, DECEA promueve ejercicios para capacitar a los equipos de respuesta a incidentes de las agencias de control del espacio aéreo. Además de contribuir a la capacitación del equipo, estos ejercicios también sirven para detectar brechas de ciberseguridad causadas por combinaciones de sistemas y aplicaciones previstos para satisfacer las demandas de las operaciones de control de tránsito aéreo. Los resultados de estos ejercicios de capacitación se recopilan en informes destinados a los equipos responsables de mejorar los sistemas y el plan de contingencia.

2.3 En relación con los ejercicios, cada situación simulada va acompañada de detalles aportados por especialistas en el mantenimiento de cada sistema para que las situaciones sean fiables y se basen en hechos reales. Así, las actividades se acercan más a una situación real y permiten una evaluación más precisa para extraer mejoras efectivas para las medidas adoptadas, para cada sistema (brechas detectadas) y para el propio plan.

2.4 Otro pilar de la estrategia de ciberseguridad de la OACI, referido a la gestión de incidentes y planes de emergencia, sirve como referencia para elaborar planes de contingencia vinculados a cada sistema crítico que se utiliza en el control del espacio aéreo brasileño. Se explica qué información es necesaria para tratar de restablecer las funcionalidades que ofrece cada sistema en los diferentes niveles de control del tránsito aéreo, así como las diversas entidades involucradas en las respuestas con la debida coordinación para minimizar la indisponibilidad y el impacto causado a quienes usan el transporte aéreo.

2.5 Los planes de contingencia se atienen a la normativa internacional, como ISO/CEI 27031, y se ajustan a las especificidades de cada ubicación. Esto permite agregar detalles de las funcionalidades de los sistemas en cada ubicación para conservarlas incluso en caso de ataque cibernético y de forma que el entorno se mantenga resiliente y controlado.

2.6 Es importante aclarar que DECEA también participa en el ejercicio nacional de ciberseguridad brasileño, bajo la responsabilidad del Ministerio de Defensa, que tiene como objetivo proteger los sistemas críticos del país. En este ejercicio nacional, DECEA aporta la experiencia obtenida en sus unidades de control del espacio aéreo a la seguridad del transporte aéreo y recibe información de otras áreas que también tienen sistemas críticos y requieren medidas de protección y resiliencia. Las actividades realizadas en este importante ejercicio nacional ayudan a corroborar y mejorar los planes de contingencia, que deben actualizarse constantemente ante las nuevas amenazas diarias.

2.7 El Brasil hace un llamado a los Estados miembros de la OACI y a la industria de la aviación para que respalden y organicen ejercicios de ciberseguridad con participación del personal experto de la administración y de la industria, para intercambiar las mejores prácticas y experiencia en formación de especialistas en cibernética para responder a ataques cibernéticos y elaborar planes de contingencia cibernética más fiables para proteger la infraestructura y los sistemas críticos de la aviación.

3. CONCLUSIÓN

3.1 Las amenazas cibernéticas son un desafío omnipresente, y el sector de la aviación civil, con su intrincada red mundial, también es vulnerable. La actitud proactiva del Brasil, como lo demuestran las iniciativas de DECEA, concuerda con la Estrategia de Ciberseguridad de la Aviación de la OACI, en particular sus pilares 6 y 7. Hacer hincapié en planes de contingencia sólidos, ajustados a normas internacionales tales como ISO/CEI 27031 y adaptados a las especificidades locales, junto con ejercicios cibernéticos periódicos y realistas, mejora significativamente la resiliencia cibernética. Esta labor no solo

capacita a los equipos de respuesta a incidentes y detecta vulnerabilidades, sino que también fomenta una sólida cultura de la ciberseguridad entre todas las partes interesadas. Al compartir su experiencia y colaborar en ejercicios nacionales e internacionales, el Brasil insiste en que es acuciante adaptarse constantemente y actuar de forma mancomunada para salvaguardar el sistema de la aviación mundial ante los riesgos cibernéticos que van surgiendo.

— FIN —