Organización de Aviación Civil Internacional
Grupo Regional de Planificación y Ejecución CAR/SAM (GREPECAS)

NOTA DE ESTUDIO

GREPECAS/23 — NE/5.7
14/01/26

Quinta Reunión Conjunta GREPECAS–RASG-PA (GREPECAS-RASG-PA/5) y Vigésima tercera Reunión del Grupo Regional de Planificación y Ejecución del Caribe y Sudamérica (GREPECAS/23)

Fase Virtual (Asincrónica, 19 de enero al 17 de febrero de 2026)
Fase Presencial (Ciudad de México, México del 4 al 6 de marzo de 2026)

Cuestión 5 del Orden del Día: **Resultados de la Asamblea 42; Cuestiones relativas a las iniciativas de navegación aérea**

MEJORA DE LA CIBER RESILIENCIA: EL PAPEL DE LOS PLANES DE CONTINGENCIA Y LOS CIBEREJERCICIOS

(Presentada por Brasil)

RESUMEN EJECUTIVO

Esta NE aborda la necesidad crítica de establecer planes de contingencia robustos para los sistemas de aviación civil, en alineación con el Pilar 6 (Gestión de Incidentes y Planificación de Emergencias) de la Estrategia de Ciberseguridad de la Aviación de la OACI. Asimismo, explora la mejora continua de estos protocolos a través de ejercicios de simulación de ciberataques, tal como lo promueve el Pilar 7 (Creación de Capacidad, Instrucción y Cultura de Ciberseguridad). Mediante el uso de simulaciones basadas en vulnerabilidades de sistemas del mundo real y en hechos ya observados, las organizaciones pueden fortalecer significativamente su postura defensiva. La NE destaca la evolución de las ciberamenazas dentro del sector de la aviación y subraya la sinergia fundamental entre los ejercicios prácticos y la planificación de contingencias como motores esenciales para la resiliencia cibernética institucional.

Acción:	Se invita la Reunión a: a) Promover el desarrollo de planes robustos de gestión de incidentes cibernéticos, específicamente adaptados a la infraestructura aeronáutica crítica; y b) Considerar la realización de simulaciones cibernéticas periódicas, con participación integrada de socios gubernamentales y de la industria en la Región CAR/SAM.
Metas Estratégicas 2026-2050:	• Todos los vuelos son seguros y protegidos • La Aviación es sostenible en términos medioambientales • La Aviación brinda movilidad fluida, accesible y confiable para todo el mundo • Ningún país se queda atrás • Marco jurídico integral • Desarrollo económico
Referencias:	• 42ª Asamblea de la OACI - WP/240 (Brasil).

	● 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 En respuesta a los riesgos emergentes y reconociendo el imperativo de una mayor protección de los activos críticos de la aviación, la Estrategia de Ciberseguridad de la Aviación de la OACI establece principios y acciones estructurados en siete pilares fundamentales, con el objetivo de armonizar los esfuerzos de resiliencia entre los actores de la aviación civil internacional. Si bien la modernización tecnológica en el espacio aéreo de América del Sur y el Caribe ha mejorado la eficiencia operativa, simultáneamente ha ampliado la superficie de ataque debido a una profunda dependencia de las infraestructuras digitales. Esta expansión es crítica dado que las ciberamenazas representan un desafío creciente para el ecosistema de la aviación civil, incluso dentro de las Regiones CAR/SAM, donde el alto grado de integración sistémica implica que las vulnerabilidades localizadas pueden facilitar la rápida propagación de malware con consecuencias transfronterizas.

1.2 Esta nota de estudio describe las iniciativas estratégicas emprendidas por Brasil para reforzar la resiliencia cibernética, centrándose específicamente en la integración del Pilar 6 (Gestión de Incidentes y Planificación de Emergencias) y el Pilar 7 (Creación de Capacidad, Instrucción y Cultura de Ciberseguridad) de la Estrategia de Ciberseguridad de la Aviación de la OACI. Al armonizar estos dos pilares, el sector de la aviación civil brasileña establece una estrategia de defensa integral y adaptativa para los activos críticos del control de tránsito aéreo. Este enfoque trasciende las medidas reactivas, permitiendo una postura proactiva que prioriza la prevención y mitigación de amenazas, salvaguardando así la seguridad operacional (safety), la seguridad de la aviación (security) y la confiabilidad operativa duradera del transporte aéreo en las regiones CAR/SAM.

1.3 Garantizar la mínima interrupción del control de tránsito aéreo, las operaciones en tierra y los servicios a los pasajeros es el objetivo principal de las medidas establecidas bajo el Pilar 6. Esto se logra mediante procedimientos de recuperación robustos y la implementación de planes de contingencia claros y validados, diseñados para la restauración inmediata de los sistemas y datos comprometidos. Para este enfoque, resultan esenciales la disponibilidad de sistemas alternos, el mantenimiento de copias de seguridad (backups) seguras y la ejecución de protocolos de recuperación detallados paso a paso.

1.4 Una cultura de ciberseguridad robusta es fundamental para el Pilar 7, garantizando que cada individuo —desde los controladores de tránsito aéreo hasta el personal de mantenimiento en tierra— reconozca su posición como una primera línea de defensa vital. Al abordar la concientización y la instrucción de todas las partes interesadas dentro del entorno del control de tránsito aéreo, este pilar busca estimular la capacitación del personal para que comprenda sus funciones específicas en la respuesta a incidentes y el mantenimiento de un entorno operativo seguro. Asimismo, enfatiza la necesidad del aprendizaje continuo y la adaptación frente a un panorama de amenazas en constante evolución. Este compromiso garantiza que la preparación organizacional permanezca proactiva en lugar de complaciente, lo que requiere una mejora constante y la integración de tecnologías y estrategias de ciberseguridad actualizadas.

1.5 Para contribuir a un ecosistema de aviación global más seguro y resiliente, es esencial mejorar la colaboración entre las autoridades de ciberseguridad de la aviación civil y otras partes interesadas a través de estos principios. De este modo, se establece un entorno robusto donde los planes de contingencia sirven como el medio para hacer frente a acciones maliciosas y responder a los ciberataques. Estos planes deben abordar la coordinación entre todos los actores, destacando los requisitos críticos para implementar

acciones de respuesta y detallando los mecanismos disponibles para restaurar la normalidad de las operaciones tras la vulneración de un sistema.

2. Discussión

2.1 En consonancia con la estrategia de ciberseguridad de la OACI y sus pilares específicos, el DECEA ha venido realizando ejercicios de capacitación para equipos de respuesta a incidentes, con el fin de fortalecer la resiliencia del sistema brasileño de control del espacio aéreo frente al aumento de las amenazas cibernéticas. Estos ejercicios cumplen un doble propósito: proporcionan capacitación esencial al personal de las unidades de control del espacio aéreo y facilitan la identificación de brechas de ciberseguridad derivadas de la compleja integración de los sistemas y aplicaciones de control del tránsito aéreo. Los resultados de estas simulaciones se documentan meticulosamente en informes, que posteriormente son utilizados por los equipos responsables de perfeccionar la seguridad de los sistemas y actualizar los planes de contingencia. Mediante estas acciones, Brasil continúa reflejando las mejores prácticas internacionales en el mantenimiento de un entorno operacional seguro.

2.2 Para garantizar una evaluación más precisa y extraer mejoras efectivas para los planes de contingencia y las brechas específicas de los sistemas, cada situación simulada está diseñada para reflejar sucesos del mundo real, replicando así fielmente los escenarios actuales. Esta fiabilidad se obtiene y mantiene mediante la participación de expertos en mantenimiento de sistemas, quienes aportan los detalles técnicos necesarios para fundamentar cada ejercicio en la realidad. Como resultado, las acciones de instrucción permiten una evaluación precisa de las medidas de respuesta adoptadas, facilitando un diagnóstico exacto del entorno y permitiendo la identificación de los refinamientos necesarios para cada sistema individual, así como la obtención de mejoras efectivas para los planes de contingencia.

2.3 De conformidad con estándares internacionales como la norma ISO/IEC 27031, los planes de contingencia se desarrollan y ajustan cuidadosamente para abordar las especificidades locales. Esta integración de los estándares globales con los requisitos únicos de cada emplazamiento permite agregar detalles funcionales específicos dentro de sus respectivos planes. En consecuencia, incluso durante un ciberataque, se preservan las funcionalidades críticas y se mantiene un entorno controlado, garantizando una continuidad operativa mínima.

2.4 Minimizar la indisponibilidad de los sistemas y el impacto resultante en los usuarios del transporte aéreo es el objetivo principal de las acciones de coordinación y respuesta descritas en los planes. La documentación detalla toda la información requerida para dirigir el restablecimiento de las funcionalidades del sistema en los diferentes niveles del control de tránsito aéreo. Estos planes de contingencia, asociados a cada sistema crítico de la red de control del espacio aéreo brasileño, se fundamentan en el pilar de ciberseguridad de la OACI relativo a la gestión de incidentes y la planificación de emergencias. Al identificar a los diversos actores involucrados y su coordinación necesaria, el documento proporciona una base integral para mantener la continuidad operativa.

2.5 Al participar en el ejercicio nacional de ciberseguridad de Brasil, el DECEA garantiza que sus planes de contingencia se actualicen constantemente para hacer frente a las amenazas emergentes diarias mediante un intercambio vital de conocimientos intersectoriales. Esta participación de alto nivel permite que el DECEA aporte conocimientos especializados en control del espacio aéreo a la seguridad nacional, al tiempo que integra perspectivas críticas de resiliencia provenientes de otros sectores estratégicos para el perfeccionamiento de las medidas de seguridad de la aviación. Basándose en este modelo exitoso de protección de infraestructuras críticas, Brasil insta a los Estados miembros de las Regiones CAR/SAM de la OACI y a la industria de la aviación a organizar ejercicios colaborativos similares que reúnan a expertos del gobierno y de la industria. Al utilizar estas plataformas para compartir mejores prácticas, instruir a especialistas en respuesta a incidentes y desarrollar planes de contingencia más fiables, la comunidad internacional puede fortalecer eficazmente la postura de seguridad colectiva del sector de la aviación global.

3. Conclusión

3.1 La postura proactiva de Brasil para salvaguardar su espacio aéreo queda demostrada por las iniciativas del DECEA, las cuales se alinean directamente con los Pilares 6 y 7 de la Estrategia de Ciberseguridad de la Aviación de la OACI. Reconociendo que la compleja red global de la aviación civil sigue siendo vulnerable al desafío omnipresente de las ciberamenazas, estos esfuerzos priorizan el desarrollo de planes de contingencia robustos. Al adherirse a estándares internacionales como la norma ISO/IEC 27031 y adaptarlos a las especificidades locales, el sector garantiza que la resiliencia se construya sobre una base que combina tanto las mejores prácticas globales como las necesidades operativas específicas.

3.2 El fortalecimiento de la resiliencia cibernética se impulsa, además, mediante ejercicios cibernéticos periódicos y realistas que fomentan una sólida cultura de ciberseguridad entre todas las partes interesadas, al tiempo que permiten identificar vulnerabilidades e instruir a los equipos de respuesta a incidentes. A través del intercambio de conocimientos y la colaboración activa en ejercicios tanto nacionales como internacionales, Brasil subraya la necesidad crítica de una acción colectiva. Este compromiso con la adaptación continua garantiza que el ecosistema de la aviación global esté mejor protegido contra la naturaleza persistente y evolutiva de los riesgos cibernéticos.

4. Acciones sugeridas

4.1 Se invita la Reunión a:

a) Promover el desarrollo de planes robustos de gestión de incidentes cibernéticos, específicamente adaptados a la infraestructura aeronáutica crítica; y

b) Considerar la realización de simulaciones cibernéticas periódicas, con participación integrada de socios gubernamentales y de la industria en la Región CAR/SAM.

— FIN —