Organización de Aviación Civil Internacional
Oficina para Norteamérica, Centroamérica y Caribe

NOTA DE ESTUDIO

NACC/DCA/14 — NE/19
15/05/26

Decimocuarta Reunión de Directores/as de Aviación Civil de Norteamérica, Centroamérica y Caribe (NACC/DCA/14)

St. George's, Antigua y Barbuda, 1 al 5 de junio de 2026

Cuestión 6 del Orden del Día: **Servicios de Navegación Aérea (ANS) homogéneos e interoperables que se adecúan al futuro**

FORTALECIMIENTO DE LA CIBERSEGURIDAD EN LA AVIACIÓN CIVIL CENTROAMERICANA

(Presentada por COCESNA)

RESUMEN EJECUTIVO

La ciberseguridad en la aviación civil se ha convertido en un pilar fundamental para garantizar la seguridad operacional y la eficiencia de la navegación aérea. Actualmente, la industria enfrenta un entorno dinámico con amenazas cibernéticas en constante evolución, lo que requiere de un enfoque estratégico y coordinado para proteger infraestructuras críticas.

Esta nota de estudio presenta una evaluación preliminar de la postura de ciberseguridad en la Corporación Centroamericana de Servicios de Navegación Aérea (COCESNA) y la necesidad de implementar un marco normativo basado en normas NIST y las consiguiente medidas y controles para el fortalecimiento a nivel Corporativo y el impacto que estas medidas pueden tener en la seguridad operacional en la Región Centroamericana.

También aborda la necesidad de disponer de mecanismos de cooperación técnica que permitan sostener, con una visión de largo plazo, la implementación Corporativa de un marco normativo de ciberseguridad basado en la normas de OACI, NIST, ISO 27000 Seguridad de la Información e ISO 31000 Gestión de Riesgos, estructurado sobre tres pilares fundamentales: el fortalecimiento de los procesos institucionales, la incorporación de capacidades y controles tecnológicos, y el desarrollo del talento humano mediante formación, especialización y concienciación continua.

Acción:	Bajo la Sección 5
Objetivos Estratégicos:	• Todos los vuelos son seguros y protegidos • Movilidad fluida, accesible y confiable
Referencias:	• Marco Normativo NIST

1. Introducción

1.1. COCESNA recibió una misión de asistencia técnica realizada por la Oficina Regional OACI NACC, la cual se desarrolló en Tegucigalpa, Honduras, del 13 al 17 de octubre de 2025, y tuvo como referencia principal los lineamientos y marcos de la OACI, especialmente el Doc. 9985, el Doc. 10213, los Anexos 17 y 19, así como estándares internacionales como ISO/IEC 27001 e ISO 22301. El plan de trabajo comprendió un taller de capacitación sobre principios, normativas y mejores prácticas de ciberseguridad aplicadas a sistemas CNS/ATM; una visita técnica en sitio a las facilidades CNS/ATM y radar de COCESNA; y una evaluación técnica y operativa basada en revisión documental, entrevistas, observaciones directas y análisis preliminar de los controles existentes, con énfasis en vulnerabilidades, gestión de incidentes, mitigación y alineamiento con el marco global de ciberseguridad de la OACI.

1.2. La evaluación evidenció que COCESNA cuenta con fortalezas importantes, particularmente en la documentación de seguridad ATM, la gestión corporativa del riesgo, la segmentación básica de redes y medidas de control físico y lógico ya implementadas. No obstante, también se identificaron áreas de actuación a fortalecer que de hecho COCESNA ya lo está contemplando proactivamente desde su Plan Estratégico 2026-2030, lo cual fortalecerá la integración completa y sostenible de la ciberseguridad en los servicios de navegación aérea, entre ellas la consolidación de un marco formal de gobernanza con un alcance a nivel Corporativo, fortalezas en la definición de roles y responsabilidades, mayor involucramiento de las áreas operativas y OT en la gestión del riesgo, ampliación y automatización del inventario de activos críticos, fortalecimiento de la gestión de proveedores, mejora en la gestión de monitoreo, vulnerabilidades y de los planes de respuesta a incidentes y continuidad del negocio.

1.3. En conjunto, los resultados muestran una base positiva, pero que, dado que estamos en un entorno altamente evolutivo, dinámico y de grandes retos, esto conlleva a implementar objetivos, estrategias y acciones para una gestión permanente de fortalecimiento de la ciberseguridad como un elemento clave para la seguridad operacional y continuidad en la provisión de los servicios.

1.4. En este contexto, la ciberseguridad ha sido incorporada en el Plan Estratégico de COCESNA (PEC) 2026–2030 mediante objetivos estratégicos, objetivos específicos y planes operativos anuales a desarrollar durante todo el período, en los cuales se establece una serie de actividades orientadas al fortalecimiento progresivo de las capacidades Corporativas. Dichas acciones se estructuran sobre tres pilares fundamentales: el fortalecimiento de los procesos (Marco normativo), la incorporación de tecnología y controles de ciberseguridad, y el desarrollo del talento humano mediante formación, especialización y concienciación continua, con el propósito de consolidar una postura más resiliente, sostenible y alineada con las mejores prácticas internacionales.

2. IMPLEMENTACIÓN DE CIBERSEGURIDAD EN COCESNA

2.1 Como resultado de la misión de asistencia técnica realizada por la Oficina Regional OACI NACC, se recomendó a COCESNA avanzar hacia un enfoque estructurado, Corporativo y basado en riesgo, mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con las normativas NIST, ISO/IEC 27001, ISO 31000, ISO 22301 y el Doc. 9985 de la OACI.

2.2 COCESNA dentro de su Plan Estratégico 2026-2030 ha establecido una serie de iniciativas que se describen a continuación:

a. **Evaluación Integral y Diagnóstico de Controles de Ciberseguridad:** Comprende la realización de una evaluación exhaustiva y diagnóstico de los controles de ciberseguridad basados en la norma NIST. Incluye el desarrollo de instrumentos de evaluación, la ejecución del diagnóstico, el análisis detallado de brechas y la definición de planes de acción de mejora. Adicionalmente, contempla el levantamiento completo del inventario de activos tecnológicos, su clasificación según criticidad y nivel de sensibilidad, así como el registro de servicios clave y sus dependencias en la Base de Datos de Administración de Configuraciones (CMDB). Esta evaluación se realizará de forma cíclica durante todo el período de planificación / ejecución, estableciendo una línea base en el primer año que permitirá medir la evolución del cumplimiento de controles.

b. **Marco de Gobernanza de Ciberseguridad**: Esta iniciativa tiene como propósito establecer y mantener un marco robusto de gobernanza de ciberseguridad Corporativo. Contempla la validación del marco normativo e incluye el desarrollo progresivo de instructivos específicos para entornos de Tecnología de Información (TI) y Tecnología Operacional (OT), asegurando que la Corporación cuente con documentación normativa actualizada y alineada con las mejores prácticas internacionales.

c. **Monitoreo Continuo de Ciberseguridad**: Esta iniciativa se enfoca en implementar soluciones, servicios, sistemas, metodologías y tecnologías que permitan el monitoreo continuo de la postura de ciberseguridad de la Corporación. El componente central es la implementación y operación permanente del Centro de Operaciones de Ciberseguridad (SOC), para lo cual COCESNA ya ha lanzado este servicio en producción a partir del 16 marzo 2026, lo cual es sumamente positivo para fortalecer capacidades de monitoreo y de respuesta especializada externa ante contingencias de ciberseguridad, lo que fortalece la vigilancia ininterrumpida de la infraestructura tecnológica, la detección oportuna de amenazas y la respuesta efectiva ante incidentes de seguridad. Complementariamente, se implementarán de manera progresiva medidas tecnológicas, controles y acciones de mejora identificadas a partir de las evaluaciones de ciberseguridad, fortaleciendo continuamente las capacidades de defensa de la Corporación.

d. **Formación y Concienciación en Ciberseguridad**: Esta iniciativa representa el reconocimiento de COCESNA de que el factor humano constituye un elemento crítico en la postura de ciberseguridad Corporativa, contempla el desarrollo e implementación de programas integrales de formación y concienciación. Incluye la realización de inducciones en ciberseguridad para personal de nuevo ingreso, el levantamiento de necesidades de capacitación y definición de planes formativos, la ejecución de campañas permanentes de sensibilización para mantener al personal actualizado en temas de ciberseguridad, así como la implementación de capacitaciones técnicas básicas para todo el personal corporativo con cursos autoguiados en plataformas e-learning y que fue desarrollado con ICCAE y también capacitaciones especializadas a personal clave. El objetivo es desarrollar una cultura de ciberseguridad robusta en todos los niveles de la Corporación y que reduzca significativamente el riesgo asociado al comportamiento humano.

3. MECANISMOS DE COOPERACIÓN TÉCNICA

3.1 La implementación y sostenibilidad de un marco de ciberseguridad basado en NIST requiere un esfuerzo continuo de carácter técnico, organizacional y financiero. Su desarrollo demanda inversiones recurrentes orientadas al fortalecimiento de los procesos, la actualización y renovación de capacidades tecnológicas, incluyendo la contratación de servicios especializados de monitoreo y respuesta, así como en la capacitación, formación y concienciación permanente del talento humano para mantener una cultura de ciberseguridad.

3.2 En ese contexto, resulta necesario promover mecanismos de cooperación técnica y apoyo financiero que contribuyan a sostener este proceso de fortalecimiento. El acompañamiento técnico, como el brindado mediante misiones de asistencia de la OACI, junto con recursos externos de apoyo, puede facilitar una implementación gradual y sostenible.

3.3 El fortalecimiento de las capacidades de ciberseguridad de COCESNA aportará beneficios directos a la seguridad, resiliencia y continuidad de los servicios de navegación aérea en Centroamérica. Asimismo, la experiencia, lecciones aprendidas y capacidades que se desarrollen a nivel corporativo podrán constituirse en una referencia útil para su posterior adaptación y replicabilidad en las Autoridades de Aviación Civil de la región, favoreciendo un enfoque más armonizado y progresivo de la ciberseguridad aeronáutica regional.

4. CONCLUSIONES

4.1 La evaluación preliminar de la postura de ciberseguridad de COCESNA evidencia avances relevantes, pero también aspectos sobre los que COCESNA proactivamente ya gestiona en su Plan Estratégico 2026-2030, a fin de consolidar un enfoque corporativo, estructurado y sostenible, sustentado en un marco normativo basado en la norma NIST y en mejores prácticas internacionales aplicables a la aviación civil (ISO 27000, ISO 31000 entre otras).

4.2 La incorporación de la ciberseguridad en el Plan Estratégico de COCESNA (PEC) 2026–2030, mediante objetivos estratégicos, objetivos específicos y planes operativos anuales, constituye una base institucional para impulsar un fortalecimiento progresivo y medible en los tres pilares fundamentales: procesos, tecnología y talento humano.

4.3 Dado el carácter continuo y oneroso de la implementación y sostenibilidad de este marco, resulta necesario promover mecanismos de cooperación técnica, asistencia especializada y apoyo financiero que permitan sostener en el tiempo las capacidades institucionales requeridas para su operación y mejora continua.

4.4 El fortalecimiento de COCESNA en materia de ciberseguridad generará beneficios directos para la seguridad, resiliencia y continuidad de los servicios de navegación aérea en Centroamérica, y podrá constituirse, además, en una referencia útil para su adaptación progresiva en las Autoridades de Aviación Civil de la región.

4.5 En ese sentido, la presente iniciativa representa una oportunidad para avanzar hacia un enfoque regional más armonizado de la ciberseguridad aeronáutica, en consonancia con los lineamientos y objetivos promovidos por la OACI para la protección de la aviación civil internacional.

5. ACCIONES SUGERIDAS

5.1 Se invita a la reunión a:

a) Apoyar la implementación de un marco de ciberseguridad basado en la normativa que aplica, OACI, ISO, NIST y normativa complementaria, en atención a las necesidades identificadas y a su importancia para la seguridad operacional de la aviación civil en Centroamérica y de la región CAR.

5.2 Respaldar el cumplimiento de las iniciativas incorporadas en el Plan Estratégico de COCESNA (PEC) 2026–2030 y en los planes operativos anuales, orientadas al fortalecimiento progresivo de los procesos, la tecnología y el talento humano en materia de ciberseguridad.

5.3 Brindar (o gestionar) cooperación técnica y asistencia especializada, incluyendo misiones de apoyo y acompañamiento metodológico, que faciliten una implementación gradual y sostenible del marco de ciberseguridad.

5.4 Gestionar y Promover apoyo financiero que contribuya a sostener las inversiones recurrentes requeridas para servicios especializados, actualización tecnológica y formación continua del personal.

5.5 Apoyar a que las capacidades, experiencias y lecciones aprendidas derivadas del fortalecimiento de COCESNA puedan servir como referencia para su adaptación progresiva en las Autoridades de Aviación Civil de Centroamérica, favoreciendo un enfoque regional más armonizado de la ciberseguridad aeronáutica para toda la región.

— FIN —