Organización de Aviación Civil Internacional

NOTA DE ESTUDIO

A41-WP/395[1]
TE/149
2/8/22

ASAMBLEA — 41º PERÍODO DE SESIONES

COMISIÓN TÉCNICA

Cuestión 30: Seguridad operacional de la aviación y navegación aérea – Políticas
30.3: Resultados pertinentes del Componente de Seguridad Operacional de la Conferencia de Alto Nivel sobre la COVID-19 (HLCC 2021)

SEGURIDAD OPERACIONAL CENTRADA EN LA RED (SAFETY NETWORK)

(Nota presentada por Chile con el apoyo de 20 Estados miembros de la CLAC[2], Guyana y Surinam)

RESUMEN

Esta nota de estudio presenta un nivel de entendimiento que facilita la decisión sobre el riesgo y propone una forma para acelerar las sugerencias del Anexo 19 y Doc 9859 respecto a la implementación y consolidación de la supervisión de la seguridad operacional del Estado (SSO). Los conceptos de dirección y control en la toma de decisiones de los entes ejecutivos relacionados con la gestión del riesgo operacional (Aeronáutico), demanda información de calidad y oportuna para accionar (decisión) en la complejidad del Sistema Aeronáutico de un Estado (SAN). En la cadena de valor; los sistemas de información, la colección de datos y la consolidación de éstos en una estructura de conocimiento, proporciona a la Autoridad de seguridad operacional, un nivel de entendimiento que facilita la decisión sobre los riesgos en el SAN. Esta cadena del valor que conecta a los entes de un SAN es conocida como la red de trabajo (network) y, cuando esta red es un componente preponderante en el diseño de intercambio de datos de carácter más específicos, se denomina: trabajo centrado en la red (network centric).

La complejidad del SAN y la adopción de las SARPS exige a los Estados cambios radicales en sus normativas, organizaciones, funciones y cultura, proceso que no es simple y, además, lento. Estas barreras de carácter estructural afectan el accionar eficaz de la AAC respecto a la gestión del riesgo operacional, induciendo un proceso de toma de decisiones reactivo y anulando el accionar proactivo.

Adicionalmente, la estructura de datos es otro componente que está sujeta a la modernización; cambio que, de realizarse de manera sincrónica y secuencialmente respecto a la actualización de la estructura orgánica-funcional y cultural, induce una demora adicional en la implantación del SSP. Sin embargo, el desarrollo asincrónico entre la adaptación normativa y el diseño de las estructuras de datos puede agilizar la capacidad de supervisión del Estado de la seguridad operacional (SSO). El concepto clave para acelerar la SSO es priorizar la implantación del dominio de la información (estructura de datos), mientras se consolida el marco normativo.

[1] La versión en español fue proporcionada por Chile.

[2] Argentina, Aruba (Reino de los Países Bajos), Belice, Bolivia (Estado Plurinacional de), Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Honduras, Jamaica, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay y Venezuela (República Bolivariana de).

Decisión de la Asamblea: Se invita a la Asamblea a solicitar a la OACI que: a) considere esta propuesta como sugerencia en la implantación de la SSO; b) difunda la experiencia (ante la existencia) del diseño centrado en la red de trabajo, específicamente, para el propósito de la gestión del riesgo operacional del Estado (SRM); c) identifique e incluya las ventajas del dominio de la información y el accionar basado en red, como parte de las prioridades para lograr agilidad en el ciclo de toma de decisiones del riesgo operacional de un Estado; y d) promueva la capacitación de herramientas que facilitan la implantación de SDCPS en los Estados.	
Objetivos estratégicos:	Esta nota de estudio se relaciona con los objetivos estratégicos Seguridad Operacional y Desarrollo económico del transporte aéreo
Repercusiones financieras:	*Para la comunidad de la aviación:* Se prevén repercusiones financieras si se establecen ciertos dominios descritos en la presente nota. *Para la OACI:* no determinados.
Referencias:	Anexo19, *Gestión de la seguridad operacional* *Plan global para la seguridad operacional de la aviación* (Doc10004) *Manual de gestión de la seguridad operacional* (Doc 9859) Literatura referencias en los pies de página

1. INTRODUCCIÓN

1.1 La capacidad de supervisión de la seguridad operacional del Estado (SSO) se funda en el concepto del SSP planteado en el Anexo 19, pero es también, una nueva aproximación para cada país porque redunda en la gestión del cambio. El nuevo paradigma se sustenta en la complementariedad de una triada entre las funciones de vigilancia, gestión de la seguridad operacional (SMS) y un sistema de recopilación y procesamiento de datos de seguridad operacional (SDCPS). Esta triada debería facilitar la implementación eficaz de la gestión del riesgo operacional (safety), no obstante, es un gran desafío debido a la naturaleza constitucional de cada uno de los Estados en particular. El desarrollo e incorporación de las SARPS asociadas a la seguridad operacional en el SAN está afectado por las barreras propias de la burocracia estatal, siendo, el cambio y/o adaptación orgánica y legal lo más difícil de superar. Adicionalmente, el *Plan Global para la Seguridad Operacional de la Aviación* (GASP, Doc 10004) considera el SSP (como programa) en el desafío de progresivo de cero víctimas fatales en 2030, luego, el imperativo del GASP exige innovar en la implantación del SSP.

1.2 El SDCPS como elemento en la SSO es un factor determinante en la gestión del riesgo de seguridad operacional, es decir, en la triada: Vigilancia, SMS y SDCPS, este último es esencial para un proceso eficaz de la gestión del riesgo operacional estatal (SRM). Aun cuando la incorporación de un SDCPS es una tarea difícil de realizar por ser oneroso y complejo (hardware/software, redes, sistema de comunicaciones, etc.), la experiencia en el ámbito gerencial y militar ha evidenciado que la brecha del diseño del sistema de información es uno de los procesos más rápidos de resolver, es decir, existe ventaja respecto a la variable temporal. Hoy se reconoce la contribución a la gestión del cambio que ofrece el **dominio de la información** cuando esta cumple con: precisión, relevancia y oportunidad[3]. Adicionalmente, está comprobado el efecto multiplicador (sinergia) del uso de la red como elemento esencial en la conducción de operaciones. Entonces el diseño de una red de trabajo de seguridad operacional (safety network), se presenta como una solución conveniente y factible para acelerar la capacidad de SSO de la AAC.

[3] Monografía “Sistema de Observación y Prospectiva Tecnológica”, http://www.060.es

1.3 El planteamiento de esta nota reafirma que como paso inicial en la implantación de SSP, la red proporcionará un estado situacional del riesgo operacional del SAN en menor tiempo de aquel que se necesita para actualizar la norma, orgánica y funciones. La pregunta es: ¿cómo lograr expedición en la inclusión de la red de trabajo de seguridad operacional (safety network)? Esta propuesta plantea que debería realizarse mediante **desarrollo modular y bajo un diseño de prototipos y/o aplicaciones.**

2. PROPUESTA PARA LA RED DE TRABAJO DE SEGURIDAD OPERACIONAL (SAFETY NETWORK)

2.1 Las tecnologías de la información produjeron, producen y seguirán sorprendiendo por la influencia de los cambios a que se somete. El gran dilema que se presenta en esta vorágine evolutiva es: ¿cómo la organización aeronáutica podría incorporar un SDCPS coherente y adaptable a los cambios en las tecnologías de la información (ITs)? La respuesta a este continuo cambio es un diseño que sea flexible y permita la actualización tecnológica, cómo también, de los procesos considerados. La simulación es una herramienta útil para resolver las brechas que el dinamismo de las ITs, pero esta conlleva el uso de herramientas que a veces demoran la implantación del SDCPS. Otra forma de realizarlo es mediante el diseño por prototipos y la experiencia de Chile, demuestra que esta es la forma que ofrece mayor flexibilidad porque permite una construcción más real y ajustada a los requerimientos del usuario. Respecto a la metodología, la propuesta debería ser de carácter inductivo (bottom up) y, dentro de este proceso existen dos ejes de desarrollo: horizontal y vertical. En ambos ejes el diseño del intercambio de datos (transaccionalidad) debería ser mediante el desarrollo de **módulos prototipos**[4] que permitan el análisis y evaluación de la utilidad de la información generada (output) para la toma de decisiones.

2.2 El eje horizontal es el intercambio de datos e información entre los proveedores de servicios aéreos (PSA) que interactúan directamente en las operaciones aéreas, esto es: módulos de datos (prototipos) de las áreas que, en su accionar interactúan directamente con las operaciones aéreas, por ejemplo: la transacción de datos entre operaciones-servicios de tránsito aéreo (OPS-ATS); entre operaciones-aeródromos (OPS-AGA); entre OPS-ATS-AGA. Cada una de estas relaciones es un módulo de intercambio de información y en primera instancia, se sugiere el uso de reportes obligatorios establecidos en los SMS, por contener estos, datos desde el origen de los sucesos. En el marco de la asincronía, no es imperativo que todos los PSA tenga sus SMS aceptados por el Estado, pero si es mandatorio que adopten la cultura del reporte obligatorio y voluntario.

2.3 En el eje vertical están los requerimientos de datos que agilizan el análisis y conclusión de la información. La intención de este eje es entregar a los diferentes niveles de conducción la posibilidad de accionar en su ámbito (OPS, ATS, AGA, etc.), pero sin coartar la transaccionalidad vertical de la información. Se entiende como niveles de conducción a los siguientes estamentos de decisión:

a) Ejecutivo: nivel que se desenvuelve directamente en la operación aérea y es la fuente que provee la información base. Es también el nivel que puede accionar con inmediatez ante la aparición de un suceso que sea causal de un riesgo de alta clasificación (HRC).

b) Operacional: nivel que captura información y analiza la relación entre los estamentos ejecutivos para identificar nuevos peligros y/o desviaciones respecto a los indicadores establecidos en el programa de seguridad operacional del Estado. Este nivel debería accionar con flexibilidad para evaluar el desempeño (SMS) de los PSA y supervisar como estos aceptan y adoptan las directrices asociadas a la mitigación del riesgo.

[4] De esta manera es posible mantener una actualización.

c) Estratégico: último nivel que está recibiendo la información para los fines de la gestión del riesgo operacional del Estado (SRM). Es también el nivel que puede controlar la coexistencia de las directivas ejecutivas provenientes de OACI, por ejemplo, GASP, NASP, resoluciones, circulares, etc. Todas ellas en el marco de la seguridad operacional.

2.4 Esta iteración horizontal y vertical es la característica principal del diseño centrado en red y es también, el efecto multiplicador a capacidad cognitiva para un reconocimiento situacional del riesgo del Estado, facilitando una toma de decisiones oportuna y eficaz. Al mismo tiempo fortalece la relación entre Estado y PSA, dando espacio a soluciones de interés común respecto a las brechas del SAN. La implantación bajo el enfoque de diseño por prototipos proporciona flexibilidad, para los ajustes propios de la multiplicidad de las transacciones de información. Es esta última característica la que impone agilidad a la SSO y fortalece el SSP.

3. LA EXPERIENCIA DE LA IMPLANTACIÓN DE UNA RED DE TRABAJO DE SEGURIDAD OPERACIONAL

3.1 Se mencionan las siguientes consideraciones en la implantación de un SDCPS:

a) la complejidad del SAN demanda accionar de manera eficaz, luego, la ventaja del diseño en red puede colaborar en la consolidación de la SSO y el SSP;

b) la implantación de un SDCPS debería plantearse como es un proyecto de corto plazo, siendo la mayor restricción, la definición de los datos para la información que permita el reconocimiento de la situación del riesgo operacional del Estado;

c) la interacción debe ser en el eje horizontal (funciones) y en el eje vertical (niveles de conducción), no coartando el intercambio de información, como tampoco, las acciones en favor de la mitigación del riesgo en los respectivos ámbitos de acción; y

d) la incorporación de un SDCPS basados en el diseño de red, podría ser oneroso si se opta por una metodología deductiva (top Down), luego, se sugiere el desarrollo mediante la implementación de módulos prototipos y/o aplicaciones.

3.2 La OACI, mediante las SARPS, señala que el Estado debería desarrollar una capacidad de gestión del riesgo de seguridad operacional (SRM) eficaz. Este proceso de implantación es dependiente de la libertad de acción de los Estados (normativa), como también, del presupuesto asignado, luego es materia de ley, es decir: presupuesto y personas.

— FIN —