Organización de Aviación Civil Internacional

A41-WP/488[1]
EX/235
2/8/22

NOTA DE ESTUDIO

ASAMBLEA — 41º PERÍODO DE SESIONES

COMITÉ EJECUTIVO

Cuestión 15: Programa de Auditoria – Enfoque de Observación Continua

FORTALECIMIENTO DE LOS EQUIPOS DE AUDITORES DE LA USAP-CMA PARA LA EVALUACIÓN E IMPLEMENTACIÓN DE LOS REQUERIMIENTOS EN CIBERSEGURIDAD SOLICITADOS EN EL ANEXO 17

[Nota presentada por Venezuela (República Bolivariana de) y apoyada por Bolivia (Estado Plurinacional de), Costa Rica, Panamá, Perú y Uruguay][2]

RESUMEN

En el marco del Programa Universal de Auditorías de la Seguridad de la Aviación (USAP), los Estados actualmente disponen de lineamientos que permiten la evaluación del desempeño del sistema de supervisión estatal de la seguridad de la aviación en general, lo que ha permitido el desarrollo de recomendaciones para su mejora, bajo los principios comunes en materia de seguridad de la aviación. Dicha evaluación es llevada a cabo por un equipo de auditores, quienes cumplen con el propósito de que tales actividades contemplen los elementos críticos del sistema de vigilancia de la seguridad de la aviación, las disposiciones y el nivel de cumplimiento de las normas del Anexo 17 – *Seguridad*; en el cual se establece el desarrollo y puesta en práctica de medidas para la protección de los sistemas de tecnología de la información y las comunicaciones, así como datos críticos que se empleen para los fines de la aviación civil. En este sentido, es necesario el fortalecimiento del equipo auditor (USAP) a través del desarrollo de material orientativo o instrucción que les permita la evaluación e implementación de los requerimientos en ciberseguridad solicitados en el Anexo 17.

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

a) tonar nota de la información presentada en esta Nota de Estudio, y
b) solicitar al Consejo, desarrolle herramientas o material de instrucción para que el equipo de auditores USAP sea orientado y formado integralmente en materia de ciberseguridad, con la finalidad de que los grupos designados realicen una evaluación objetiva y técnica de las preguntas del protocolo (PQs), de acuerdo a lo especializado del tema de la ciberseguridad en la aviación civil.

Objetivos estratégicos:	Esta nota de estudio se relaciona con el Objetivo estratégico *Seguridad y Facilitación*
Repercusiones financieras:	Se propone que las actividades mencionadas en esta nota se lleven a cabo con los recursos disponibles en el presupuesto del programa regular del actual trienio y/o con contribuciones extrapresupuestarias.
Referencias:	Método recomendado 4.9.1 del Anexo 17 y Protocolo USAP-CMA.

[1] La versión en español fue proporcionada por Venezuela (República Bolivariana de).
[2] Estados miembros de la Región Sudamérica (SAM) y la Comisión Latinoamericana de Aviación Civil (CLAC).

1. INTRODUCCIÓN

1.1 El Programa Universal de Auditorías de la Seguridad de la Aviación (USAP), permite a los Estados disponer de lineamientos que ayudan en la evaluación del desempeño del sistema de supervisión estatal de la seguridad de la aviación en general, lo que ha permitido el desarrollo de recomendaciones específicas para su mejora, bajo los principios comunes en materia de seguridad de la aviación. De acuerdo al Protocolo USAP, Programa universal de auditoría de la seguridad de la aviación (USAP-CMA), actualmente se disponen de Preguntas de Protocolo (PQs) específicas (1345, 1350, 1355, 1360 y 3278) que se relacionan con la evaluación de aspectos generales o básicos relacionados con el desarrollo y puesta en práctica de medidas para la protección de los sistemas de tecnología de la información y las comunicaciones, así como datos críticos que se empleen para los fines de la aviación civil.

1.2 Dicha evaluación es llevada a cabo por un equipo de auditores USAP quienes cumplen con el propósito de que tales inspecciones contemplen los elementos críticos del sistema de vigilancia de la seguridad de la aviación, las disposiciones y el nivel de cumplimiento de las normas del Anexo 17 – *Seguridad*, en el cual se incluye el compromiso de cada Estado en la designación de responsabilidades, establecimientos de criterios nacionales para la protección de los sistemas asociados a las operaciones aeronáuticas a través de la aplicación de medidas de protección, la identificación de sistemas críticos, observación continua, detección, análisis, y respuestas a los ciberataques, así como la evaluación de las actividades de control de la calidad realizadas por el Estado conforme a la aplicación de evaluaciones de riesgo.

2. ANÁLISIS

2.1 De acuerdo a la importancia que reviste la conducción de las actividades bajo el USAP-CMA, en materia de ciberseguridad es importante que el equipo auditor (USAP) pueda disponer de material orientativo que les permita la evaluación objetiva y técnica de la aplicación de las normas internacionales, estrategias y mejores prácticas, desarrolladas e implementadas por los Estados para la identificación y protección de los sistemas críticos de tecnología de la información y las comunicaciones contra cualquier interferencia que puedan atentar contra la seguridad operacional, la integridad y el funcionamiento del sistema de aviación civil.

2.2 Actualmente, a nivel global se disponen de marcos referenciales y prácticas existentes que han permitido a diferentes organizaciones gestionar de forma eficiente y reducir el riesgo de ciberseguridad, tales como: las normas que forman la serie ISO/IEC-27000 orientadas al establecimiento de buenas prácticas en relación con diferentes aspectos vinculados a la gestión de la seguridad de la información, la mejora continua y la mitigación de riesgos; la guía de Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT), la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT), entre otros estándares, directrices y mejores prácticas a nivel internacional.

2.3 Dichos documentos referenciales, representan un avance significativo de cooperación e integración global en ciberseguridad, permitiendo disponer de líneas de acción y referencias aplicables, comunes en todos los sectores de infraestructuras críticas, específicamente en términos de estándares de la industria, directrices y prácticas que posibilitan la aplicación de la ciberseguridad y la evaluación no solo a nivel organizacional o documental, sino también a nivel de operación y de implementación.

2.4 En este sentido, se propone el desarrollo de material o textos de orientación estandarizados, que permita el establecimiento de un marco referencial para aprovechar las mejores prácticas y metodologías de la industria y la experiencia de los Estados, con el fin de establecer un enfoque armonizado, sin ser necesariamente un documento estático, sino un texto de orientación que permita al grupo de auditores USAP evaluar técnica y objetivamente el nivel de cumplimiento de las normas con base a las especificaciones y necesidades de cada Estado, según se presentan en las PQs 1345, 1350, 1355, 1360 y 3278.

2.5 El apéndice de esta nota de estudio se presenta un modelo de contenido sugerido en áreas de conocimiento y guías de orientación, propuesta basada en la integración de los criterios de diferentes estándares, directrices y prácticas existentes para la gestión de la seguridad de la información, mejora continua y la mitigación en organizaciones de infraestructura crítica a nivel internacional. En el mismo se destacan:

a) las áreas de conocimiento y experiencia potencialmente necesaria para la evaluación de las medidas implementadas por los Estados en materia de ciberseguridad (según las PQs), y

b) el contenido sugerido para el desarrollo del texto o material orientativo que permita al equipo auditor USAP la evaluación e implementación de los requerimientos en ciberseguridad solicitados en el Anexo 17.

3. CONCLUSIÓN

3.1 Es vital que los equipos de auditores asignados para la implementación del USAP-CMA, dispongan de las herramientas y conocimientos que les permitan evaluar de manera precisa y objetiva el cumplimiento de los Estados en el diseño, desarrollo e implementación de las tareas de protección en materia de ciberseguridad para la aviación civil, en acuerdo a los requerimientos que son solicitados en las Normas y Métodos Recomendados del Anexo 17 – *Seguridad*.

— — — — — — — — —

APÉNDICE

CONTENIDO SUGERIDO EN ÁREAS DE CONOCIMIENTO Y GUÍAS DE ORIENTACIÓN

a) Áreas de conocimiento y experiencia necesaria para la evaluación de las medidas implementadas por los Estados en materia de ciberseguridad

Conocimientos sobre procedimientos y técnicas para la gestión de activos y procesos críticos; identificación y valoración de activos tecnológicos, informáticos o de información asociados a la aviación; políticas, procedimientos y medidas de seguridad de la información; gestión de riesgos e incidentes; gestión de controles o salvaguardas que permitan la mitigación de hallazgos de ciberseguridad; auditoría forense, de redes, de código, vulnerabilidades, físicas, análisis web, otras.

Capacidad técnica para la evaluación de medidas de protección en la aplicación de pruebas, como por ejemplo: levantamiento, clasificación e identificación de activos, escaneo de servicios, análisis y validación de vulnerabilidades; pruebas de comprobación del funcionamiento del sistema de alimentación eléctrica, equipos, recursos o sistemas dependientes, ante la caída del sistema eléctrico; pruebas en equipos de administración de sistemas de información y plataforma tecnológica; pruebas de hardware, software operativo, infraestructura y/o aplicativos; pruebas de desempeño de la plataforma tecnológica (bajo ambiente de interrupción total); prueba de respaldo del servicio de Internet (desconexión del canal principal, verificación de conexión del canal secundario, balanceo de carga, etc.); pruebas de recuperación de información, entre otras.

b) Contenido sugerido para el desarrollo del texto o material orientativo que permita la evaluación e implementación de los requerimientos en ciberseguridad solicitados en el Anexo 17

1. Guía de procesos críticos comunes en la industria de la aviación civil relacionados con aerolíneas (gestión de pasajeros, equipaje, carga, asistencia en tierra, despacho de vuelo, mantenimiento aeronáutico, entre otros): procesos críticos en aeropuertos (seguridad aeroportuaria, operaciones e infraestructura aeroportuaria, gestión y emergencias aeroportuarias, entre otros); procesos críticos en la gestión del tránsito aéreo (comunicaciones de voz, mensajería aeronáutica y datos radar, navegación aérea, entre otros).

2. Metodología de evaluación de riesgo estandarizada para el sector de la aviación que considere el establecimiento del contexto, políticas y responsabilidades, identificación de procesos operativos, identificación y valoración de activos, identificación de vulnerabilidades, identificación y probabilidad de ocurrencia de amenazas y estimación del impacto (consecuencias).

3. Guía de controles o salvaguardas que considere la gestión de dispositivos hardware en la red, la gestión de software autorizado y no autorizado, la configuración base para dispositivos móviles, portátiles, de escritorio, servidores, proceso continuo de identificación y remediación de vulnerabilidades, procesos y herramientas para la identificación, prevención y corrección del uso y configuración de privilegios administrativos (redes/aplicaciones), el mantenimiento, monitorización y análisis resultados de auditorías, procedimientos de protección del correo electrónico y del navegador, gestión de puertos, protocolos y servicios en los dispositivos en red; procedimientos basados en metodologías y herramientas adecuadas para el respaldo de información crítica y pruebas de recuperación; procedimientos para configuraciones seguras de dispositivos de red (firewalls, routers y switches); defensa perimetral; procedimientos y herramientas de protección de datos para prevenir la fuga de información, mitigar incidentes, y asegurar la confidencialidad e integridad de la información sensible; procedimientos de gestión y respuesta a incidentes, entre otros controles.

— FIN —