Cuestión 7 del Orden del Día:

IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE CIBERSEGURIDAD EN LA AVIACIÓN, MEDIANTE LA CREACIÓN DE UNA GUÍA METODOLÓGICA

(Nota presentada por Chile)

RESUMEN

Esta nota de estudio propone la implementación de un Sistema de Gestión de Ciberseguridad en la Aviación, mediante una guía metodológica. Para la elaboración de esta Guía fueron consideradas las últimas Notas de Estudio presentadas por Chile en materias de Ciberseguridad: "Documento técnico de ciberseguridad para la aviación", presentada en la reunión RAAC 17 del año 2023 y la Nota de Estudio sobre "Gestión del riesgo e inventario de ciber-activos de información en los Servicios de Navegación Aérea". presentada en la Conferencia de Navegación Aérea AN Conf/14 del año 2024.

En el contexto global actual, la aviación se enfrenta a desafíos cada vez más complejos en términos de ciberseguridad. La creciente dependencia de la tecnología digital para operaciones críticas, como la navegación aérea, el control del tránsito, la gestión de flotas y los sistemas aeroportuarios, ha expuesto al sector a nuevas amenazas cibernéticas que podrían comprometer la seguridad, la continuidad del servicio y la confianza de los usuarios.

El objetivo del Sistema de Gestión de Ciberseguridad en la Aviación es, a través de una guía metodológica, establecer un marco de trabajo estratégico para las Organizaciones de aviación, tanto públicas como privadas, en el fortalecimiento de sus capacidades de prevención, detección, respuesta y recuperación ante incidentes cibernéticos.

La guía debe proporciona un enfoque estructurado para identificar riesgos clave, implementar medidas de seguridad efectivas y fomentar una cultura colaborativa de ciberseguridad.

Referencias:
AN Conf/14, Recomendación 4.2/1
Conclusión RAAC 17/05
Norma ISO 27001:2022
Norma ISO 27002:2022
Norma ISO 27035-1:2016
Norma ISO 27032:2012

Objetivos Estratégicos de la OACI:	• *Seguridad de la aviación* • *Seguridad operacional*

1. Introducción

1.1 En la era digital, la aviación civil enfrenta nuevos desafíos derivados de la creciente dependencia de tecnologías de la información y comunicación. La digitalización ha mejorado la eficiencia, la seguridad operacional y la experiencia del pasajero, pero también ha introducido riesgos cibernéticos que podrían comprometer la seguridad, continuidad y confiabilidad de las operaciones aéreas.

1.2 Dado el carácter crítico de la aviación, las amenazas cibernéticas pueden tener un impacto significativo, afectando desde los sistemas de navegación aérea y el control del tránsito aéreo hasta las operaciones en aeropuertos y las comunicaciones con aeronaves. Esto hace fundamental la implementación de medidas de ciberseguridad robustas y actualizadas que protejan la infraestructura, los sistemas y los datos en el ecosistema de la aviación.

1.3 La guía debe tener como objetivo, proporcionar un marco integral para la implementación de un *Sistema de Gestión de Ciberseguridad para la aviación*, alineada con las mejores prácticas internacionales y estándares de seguridad reconocidos.

1.4 Con una visión estratégica a largo plazo, esta guía abordará aspectos esenciales como:

- La identificación y evaluación de vulnerabilidades específicas del sector.
- El desarrollo de programas de capacitación y concienciación para el personal.
- La promoción de la colaboración entre actores clave de la industria.
- La implementación de tecnologías avanzadas de seguridad, como la inteligencia artificial y el análisis predictivo, y
- La creación de protocolos de respuesta a incidentes cibernéticos y mecanismos de colaboración, entre otros.

1.5 Como estrategia complementaria se deben impartir lineamientos, directrices y medidas, con el fin de establecer un piso mínimo que permita la evaluación e implementación de medidas y controles, para la protección frente a amenazas que puedan afectar a los activos críticos y que impulsen aspectos relevantes para la ciberseguridad, tales como:

- Designación de un encargado de ciberseguridad de alto nivel en cada servicio.
- Aplicación y actualización de normativa técnica sobre ciberseguridad.
- Medidas internas de ciberseguridad.
- Revisión detallada de redes, sistemas y plataformas digitales de funcionamiento crítico.
- Vigilancia y análisis del funcionamiento de la infraestructura tecnológica de los órganos de la Administración del Estado.
- Reporte obligatorio de incidentes de ciberseguridad
- Respuesta a incidentes de ciberseguridad por los órganos de la Administración del Estado.

2. Discusión

2.1 El aspecto técnico de la ciberseguridad en la aviación se centra en implementar soluciones avanzadas que protejan sistemas críticos frente a amenazas emergentes. Esto incluye:

- Análisis de vulnerabilidades: Identificar brechas en sistemas como la gestión del tráfico aéreo (ATM), la conectividad a bordo, y los sistemas aeroportuarios.

- Arquitectura segura: Diseñar infraestructuras robustas que segmenten redes y utilicen sistemas redundantes para garantizar la continuidad del servicio.
- Uso de tecnologías emergentes: Implementar inteligencia artificial y aprendizaje automático para la detección proactiva de anomalías, así como blockchain para asegurar datos sensibles y transacciones.
- Cifrado y autenticación: Asegurar la transmisión de datos entre aeronaves, sistemas de tierra y satélites mediante protocolos avanzados de cifrado y autenticación multifactor.

2.2 Pruebas de penetración regulares: Simular ataques para evaluar la eficacia de las defensas implementadas y mejorar continuamente la seguridad. El cumplimiento normativo es esencial para garantizar un enfoque unificado y coordinado en la ciberseguridad de la aviación. Algunas consideraciones clave incluyen:

- Normas internacionales: Alinearse con las directrices de la Organización de Aviación Civil Internacional (OACI) en su "Marco Global de Seguridad Cibernética".
- Legislación nacional: Adoptar las regulaciones específicas de cada país, como las directrices de la Agencia Europea de Seguridad Aérea (EASA) o la Administración Federal de Aviación (FAA).
- Certificaciones obligatorias: Asegurar que las empresas del sector obtengan certificaciones como ISO/IEC 27001 y estándares específicos de la aviación como RTCA DO-326A.
- Evaluaciones periódicas de cumplimiento: Realizar auditorías regulares para verificar que los sistemas cumplen con las normativas y estándares vigentes.
- Colaboración entre reguladores: Facilitar acuerdos entre países para compartir información y adoptar mejores prácticas globales.

2.3 Dado que la aviación es una industria global, la cooperación entre países, organizaciones y actores privados es fundamental. Algunos puntos clave son:

- Intercambio de inteligencia cibernética: Crear redes internacionales para compartir información en tiempo real sobre amenazas emergentes.
- Programas conjuntos de investigación y desarrollo: Invertir colectivamente en soluciones innovadoras para la detección y mitigación de ataques.
- Simulacros y ejercicios multinacionales: Organizar entrenamientos internacionales que simulen incidentes cibernéticos complejos, evaluando la respuesta coordinada entre países.
- Organizaciones de cooperación: Impulsar el rol de entidades como ICAO, EASA, IATA y CANSO para establecer estándares globales y garantizar su implementación efectiva.
- Asistencia técnica a regiones vulnerables: Apoyar a países en desarrollo en la creación de capacidades locales para prevenir y responder a ciberamenazas.

2.4 La identificación y evaluación de vulnerabilidades son pasos esenciales en cualquier estrategia de ciberseguridad, particularmente en el sector de la aviación, donde los sistemas críticos están cada vez más interconectados y expuestos a amenazas cibernéticas. Estas vulnerabilidades abarcan tanto los aspectos técnicos como operativos, e incluyen componentes físicos, digitales y humanos.

La aviación presenta un ecosistema complejo con múltiples puntos de entrada para posibles ataques. Entre las áreas clave a evaluar se encuentran:

- Comunicación no cifrada entre aeronaves y controladores.
- Sistemas de radar y navegación expuestos a interferencias o ataques de suplantación de señales (spoofing).
- Dependencia de sistemas heredados que no cumplen con los estándares de seguridad modernos.

- Segmentación insuficiente entre las redes de pasajeros y los sistemas críticos de vuelo.
- Acceso remoto no autorizado a través de interfaces mal configuradas.
- Sistemas de gestión de equipaje vulnerables a ataques que alteren la clasificación o rastreo.
- Dependencia de sistemas IoT (Internet de las Cosas) mal protegidos, como cámaras de seguridad o sensores de acceso.
- Proveedores que no cumplen con estándares de ciberseguridad.
- Actualizaciones de software o firmware que introducen código malicioso.
- Cifrado avanzado
- Formación y concienciación**:**
- Planes de contingencia y respuesta

2.5 Metodológica para la implementación "*Sistema de Gestión de Ciberseguridad para la aviación"* (SGCA)

2.5.1 El objetivo de la Guía debe abarcar de manera detallada el desarrollo de cada uno de los requisitos técnicos, asociados a las distintas etapas deben componer un Sistema de Gestión de Ciberseguridad en la Aviación (SGCA), para verificar el cumplimiento asociados a las normativas y directrices aplicables en la materia, tales como ISO27001:2022, Anexo 17 y 19 de la OACI, ISO31000, CISSP, definiendo un instrumento de basado en un marco de trabajo que recoge las mejores prácticas de dichos lineamientos, contemplando los activos de información que permiten la operación aeronáutica. En este mismo contexto, para la aplicación del marco aludido, se distinguen 3 niveles básicos de activos de información:

- La Información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.)
- Los Equipos/Sistemas/infraestructura que soportan esta información.
- Las Personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.

2.5.2 La guía debe entregar lineamientos para la presentación de los requisitos técnicos del SGCA. Sin embargo, no debe constituirse en un manual de gestión de proyectos. Por esta razón, el desarrollo de algunos requisitos pudiera requerir del uso de otras herramientas de gestión y, en general, el empleo de conocimientos, capacidades y habilidades que se suponen existentes en cada uno de los organismos involucrados en la aeronáutica, sin perjuicio de que exista asistencia, control y evaluación de resultados por parte de una Red de especialistas con vasta experiencia en la implementación del mencionado instrumento.

2.5.3 Este nuevo Sistema constituye una herramienta para el ordenamiento de la gestión de cada organización o empresa aérea desde el punto de vista del aporte efectivo de la tecnología a sus procesos o cadena de valor, identificando, en primera instancia sus activos de información críticos vinculados a sus procesos de negocio y de soporte, seguidamente, que se logre identificar y gestionar los riesgos asociados a los mencionados activos, contemplando planes de contingencia y de recuperación frente a desastres relacionados con la ciberseguridad y actividades afines, que permitan establecer una continuidad operacional de sus procesos relevantes a nivel organizacional, de modo de asegurar la provisión de los productos y servicios que deben ser brindados a sus clientes, usuarios o beneficiarios.

2.5.4 El Sistema de Gestión de Ciberseguridad en la Aviación permite identificar amenazas y vulnerabilidades que afectan a los activos de información vinculados a cada proceso de provisión de la organización. El énfasis está en desarrollar un plan para el tratamiento de riesgos, cautelando debidamente

los siguientes activos de información: Equipos, infraestructura física y tecnológica, software, bases datos, personas e información propiamente tal en sus múltiples formatos (papel, digital, audio, video, etc.).

2.5.5 A través de SGCA, las empresas y organizaciones involucradas en asuntos aeronáuticos deberán elaborar un levantamiento pormenorizado de estos activos en dos planes: el Plan de Continuidad del Negocio y el Plan de Recuperación frente a Desastres. En toda organización moderna, donde un gran porcentaje de sus procesos contemplan elementos tecnológicos, los planes mencionados se transforman en elementos fundamentales para cumplir los objetivos principales de gestión de ciberseguridad (lograr que todos los activos de información institucional estén protegidos desde las perspectivas de Confiabilidad, Integridad y Disponibilidad).

2.6 Propuesta de Etapas de Implementación

A. Etapa 1

- Diagnosticar la situación de ciberseguridad de la organización, poniendo énfasis en identificar adecuadamente los activos de información vinculados a sus procesos de provisión, así como las amenazas, vulnerabilidades y los riesgos e impacto asociados a tales activos.
- Determinar las brechas a ser abordadas en el Plan General de ciberseguridad organizacional.

B. Etapa 2

- Definir el Plan General de Ciberseguridad, para los periodos aplicables contemplando la realidad organizacional y priorización de brechas, considerando los resultados del diagnóstico y brechas detectadas en la Etapa I, y que comprenda la coordinación de todas las áreas vinculadas y los métodos para la implementación de los controles de mitigación. Este plan debe estar aprobado por la Autoridad Superior de la organización y debe incluir: el tratamiento y monitoreo para todos los riesgos críticos identificados; la identificación de los productos y/o medidas necesarias para el debido tratamiento de los riesgos y el cierre de cada una de las brechas detectadas; los responsables por cada medida o actividad aplicable y finalmente la definición del porcentaje de cumplimiento que se espera alcanzar durante el periodo definido para cada control de mitigación, en términos de aceptabilidad.
- Elaborar el Programa de Trabajo Anual para implementar el plan de ciberseguridad de la definida, que incluya hitos, cronograma, plazos y responsables, y las acciones orientadas a difusión/capacitación/sensibilización a todos los empleados del programa de trabajo y sus actividades.

C. Etapa 3

- Implementar el programa de trabajo anual definido en la etapa anterior, de acuerdo con lo establecido en el plan general de ciberseguridad y el porcentaje de cumplimiento de al respecto.
- Registrar y controlar los resultados de la implementación del programa de trabajo anual considerando actividades, dificultades, grado de avance en el cierre de las brechas, holguras detectadas, implementación del plan de mitigación de riesgos asociados a cada proyecto o iniciativa, las acciones de difusión/ sensibilización/ capacitación y las modificaciones realizadas según lo programado.

D. Etapa 4

- Evaluar los resultados de la implementación del Plan General de Ciberseguridad y Programa de Trabajo Anual, y formular recomendaciones de mejora.
- Difundir a los empleados los resultados de la evaluación del Plan y Programa de Trabajo Anual.
- Diseñar el Programa de Seguimiento a partir de las recomendaciones formuladas.
- Mantener el grado de desarrollo del sistema de acuerdo a cada una de las Etapas.
- Implementar los compromisos establecidos en el Programa de Seguimiento, considerando plazos y responsables para superar las brechas aún existentes y debilidades detectadas.

2.7 Conclusión

2.7.1 La identificación y evaluación de vulnerabilidades específicas del sector de la aviación son pasos fundamentales para construir un ecosistema seguro y resiliente. Este proceso debe ser continuo, dinámico y adaptativo, teniendo en cuenta tanto las amenazas actuales como los riesgos emergentes. Con un enfoque preventivo y el uso de herramientas avanzadas, es posible reducir significativamente la superficie de ataque y garantizar la seguridad de las operaciones en la aviación global.

2.7.2 En consecuencia, mientras la industria de la aviación navega por un panorama digital cada vez más complejo, la ciberseguridad se erige como una prioridad esencial. La colaboración, la inversión en tecnologías (no tan solo relacionadas con TI) y la inversión en capacitación/concientización son fundamentales para enfrentar estar preparados de la mejor forma frente a las amenazas cada vez más evolutivas.

3. **Acción sugerida**

3.1 Se invita a la reunión a:

3.1.1 Analizar la Nota de Estudio, para la *Implementación de un Sistema Gestión de Ciberseguridad en la aviación*, elaborada por Chile,

3.1.2 Determinar la pertinencia de la creación de una Guía Metodológica y una implementación regional y armonizada del SGCA.

3.1.3 En caso de determinar positivamente la pertinencia de una implementación regional, evaluar la creación de una Red de colaboración en la materia, liderada por la Secretaría de la SAMRO, que facilite la implementación y el asesoramiento en la materia a los Estados.

- FIN -