CIBERSEGURIDAD GESTIÓN DE INFORMACIÓN AERONÁUTICA

Mayda Ávila

Especialista Regional en Comunicaciones, Navegación y Vigilancia

Sexta Reunión del Grupo de Tarea para la Implementación de la Gestión de la Información Aeronáutica (AIM/TF/6) del Grupo de Trabajo de Norteamérica, Centroamérica y Caribe (NACC/WG/AIM/TF)

Diciembre 08, 2020

Introducción

- Tecnología y ciber-sistemas se han convertido en esenciales para la sociedad moderna.
- Las ciber amenazas y los ciber ataques tienen un componente y un efecto transnacional ya que los sistemas mundiales están interconectados.

Ciberseguridad

- ***Conjunto de tecnologías, controles, medidas, procesos y prácticas diseñados para proteger la confidencialidad, integridad, disponibilidad y protección general de sistemas, redes, programas, dispositivos, información y datos contra ataques o daños y acceso, uso y/o explotación no autorizados.***

Antecedente

- Durante la 41 Asamblea de la OACI en Octubre 2022, la Resolución A41-19: Formas de abordar la ciberseguridad en la aviación civil, invito a los Estados a tener en cuenta lo siguiente:
  - el sistema de aviación mundial es un sistema altamente complejo e integrado que comprende sistemas que son críticos para la seguridad y protección de las operaciones de aviación civil.
  - que el sector de la aviación depende cada vez más de la confiabilidad, integridad y disponibilidad de sistemas, datos e información.

- Recomendó a los Estados a:
  - Implantar la Estrategia de Ciberseguridad de la Aviación de la OACI, y utilizar el Plan de Acción de Ciberseguridad de la OACI como herramienta para apoyar la implementación de la Estrategia de Ciberseguridad de la Aviación;
  - designar la autoridad competente en materia de ciberseguridad de la aviación y definir la interacción entre dicha autoridad y los organismos nacionales interesados;
  - definir las responsabilidades de los organismos nacionales y las partes interesadas de la industria con respecto a la ciberseguridad en la aviación civil;
  - elaborar e implementar un marco sólido de gestión de riesgos de ciberseguridad que se base en prácticas pertinentes de gestión de riesgos de seguridad de la aviación y seguridad operacional, y adoptar un enfoque basado en los riesgos para proteger los sistemas, información y datos críticos de la aviación civil de las ciberamenazas.

- Establecer políticas e instrumentos y destinar recursos para garantizar que los sistemas de aviación críticos tengan una arquitectura diseñada para ser segura.
- fomentar la coordinación entre gobierno e industria con respecto a las estrategias, políticas y planes de ciberseguridad de la aviación.
- formar y participar en asociaciones y mecanismos entre gobierno e industria, a nivel nacional e internacional, para compartir sistemáticamente la información sobre ciberamenazas, incidentes, tendencias y acciones de mitigación;
- diseñar y aplicar una sólida cultura de ciberseguridad en todo el sector de la aviación civil;
- alentar a los Estados a que sigan aportando su contribución a la OACI en la elaboración y aplicación de normas, estrategias y mejores prácticas internacionales para hacer que progresen la ciberseguridad y la ciber resiliencia de la aviación; y
- colaborar continuamente en el desarrollo del marco de ciberseguridad de la OACI adoptando un enfoque horizontal, intersectorial y funcional que integre la seguridad operacional de la aviación, la seguridad de la aviación, la facilitación, la navegación aérea, las comunicaciones, la vigilancia, la gestión del tránsito aéreo, las operaciones de aeronaves, la aeronavegabilidad y demás disciplinas pertinentes

GESTIÓN DE INFORMACIÓN AERONÁUTICA

- Es un área de navegación aérea que habilita las operaciones de control de tráfico aéreo, entre otras y es necesario que se implementen mecanismos de protección que aseguren la validación y seguridad de los datos en toda su cadena de suministro.

Estrategia de ciberseguridad de la OACI

- El sector de la aviación civil es cada vez más dependiente de la disponibilidad de la información y de los sistemas tecnológicos de comunicación, así como de la integridad de la confidencialidad de datos. La amenaza planteada por un posible incidente cibernético en la aviación civil está continuamente evolucionando, con actores amenazantes enfocando sus intenciones maliciosas, interrupciones de la continuidad del negocio y el robo de información por motivos políticos, financieros o de otro tipo.
- https://www.icao.int/cybersecurity/Documents/AVIATION%20CYBERSECURITY%20STRATEGY.SP.pdf

Estrategia de ciberseguridad de la OACI

- El objetivo de la estrategia será alcanzado mediante una serie de principios, medidas y acciones contenidas en un marco de referencia construido sobre siete pilares :
  1. Cooperación internacional
  2. Gobernanza
  3. Legislación efectiva y regulaciones
  4. Política de ciberseguridad
  5. Compartición de información
  6. Gestión de incidentes y planeación de emergencia
  7. Construcción de capacidad, capacitación y cultura de la ciberseguridad

Cooperación internacional

- La ciberseguridad requiere cooperación a nivel nacional e internacional para mejorarse y con el objetivo de proteges al sector de la aviación civil de todas las amenazas cibernéticas a la seguridad operacional y la seguridad de la aviación.
- La ciberseguridad de la aviación requiere armonización global.
- La OACI es un foro apropiado para involucrar a los Estados en abordar la ciberseguridad de la aviación civil internacional.

Gobernanza

- Se les exhorta a os Estados miembros de la OACI a apoyar y contruir sobre la Estrategia de ciberseguridad de la aviación.
- Se exhorta a los Estados a desarrollar clara gobernanza nacional y responsabilidad para la ciberseguridad de la aviación civil.
- Se exhorta a los Estados miembros a incluir la ciberseguridad en sus programas nacionales de seguridad operacional y de seguridad de la aviación.

Legislación efectiva y regulación

- Legislación y regulación internacional, regional y nacional sobre ciberseguridad para la aviación civil
- Los Estados miembros deber asegurar la formulación y aplicación de legislación y regulación apropiadas, de acuerdo con las disposiciones de la OACI, previamente a la implementación de políticas nacionales de ciberseguridad para la aviación civil
- Instrumentos legales internacionales relevantes deben ser analizado para identificar disposiciones legales clave existentes o faltantes en el derecho aeronáutico para la prevención, enjuiciamiento y reacción puntual a ciber incidentes.
- Se exhorta a los Estados a considerar si su legislación nacional requiere una actualización o la adopción de una nueva legislación nacional para la ciberseguridad.

Política sobre ciberseguridad

- La ciberseguridad debe ser incluida en los sistemas de vigilancia de la seguridad de la aviación y la seguridad operacional de los Estados como parte de un marco de referencia integral sobre gestión de riesgo.
- Crear material para evaluar las amenazas de ciberseguridad y análisis de riesgos.
- Las políticas de ciberseguridad deben considerar el ciclo de vida completo del sistema de aviación.

Compartición de información

- Compartir información para permitir la prevención, detección temprana y mitigación de eventos relevantes de ciberseguridad antes de que se encaminen a efectos mayores sobre la seguridad operacional o la seguridad de la aviación.

- La compartición de información en aspectos como las vulnerabilidades, amenazas, eventos y mejores prácticas, a través de relaciones establecidas y confiables para reducir el impacto de ataques en curso.

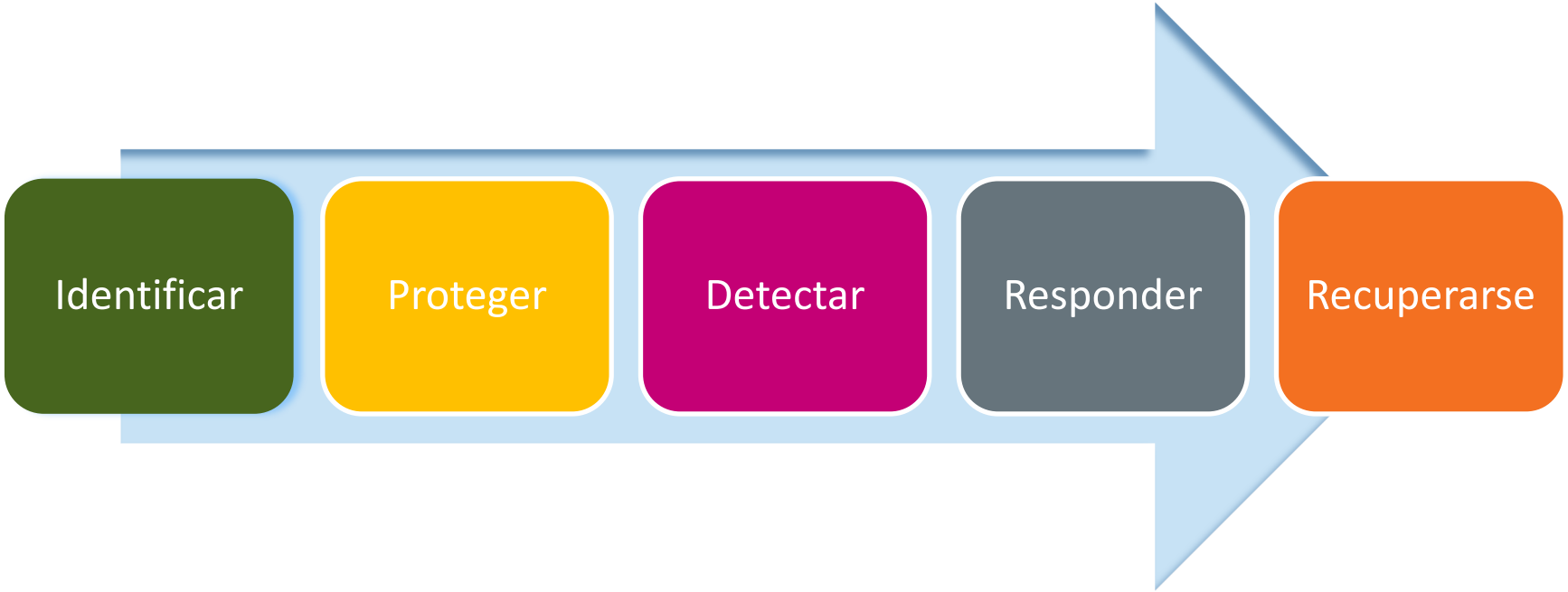
Gestión de incidentes y planeación de emergencia

- Hay una necesidad, en línea con mecanismos existentes sobre gestión de incidentes, de tener planes apropiados y escalables que proporcionen continuidad del transporte aéreo durante ciber incidentes.
- Los ejercicios de ciberseguridad son herramientas útiles para probar ciber resiliencia existente e identificas mejoras, y son por consiguiente ampliamente recomendados.

CONSTRUCCIÓN DE CAPACIDAD, CAPACITACIÓN Y CULTURA DE LA CIBERSEGURIDAD

- El elemento humano es el núcleo de la ciberseguridad.
- Para mejorar la cultura de la ciberseguridad.
- Estrategia para desarrollar recursos humanos para la ciberseguridad.

Mejores prácticas en ciberseguridad



El elemento humano de la ciberseguridad

- *Un incidente puede ser debido a una entidad externa o interna.*
- *Eventos internos pueden ser intencionales o debido a un error humano.*
- *Elementos como una adecuada capacitación debe ser parte de una estrategia de ciberseguridad.*
- *La seguridad de la información no es solo una cuestión de tecnología, también de las personas.*

Conclusiones

- La estrategia incluye identificación de todas las partes interesadas, entender y gestionar todas las operaciones de aviación, implementar procedimientos efectivos en todos los enfoques de ciberseguridad y proporcionar recursos adecuados para apoyar el proceso.
- El enfoque de ciberseguridad debe ser una orientación para políticas y directivos, gobernanza que proviene de los niveles altos de la organización.
- Debes establecerse responsabilidades en todo el proceso de ciberseguridad.
- Capacitación y conocimiento adecuados del personal deben ser establecidos.
- La gestión del riesgo y un proceso de medida/mejora para asegurar controles de seguridad como una forma de medir mejor y gestionar el riesgo.
- Lenguaje común en los que se pueda hablar sobre riesgo cibernético y cómo medirlo.

Documentos

- Anexos de la OACI
- OACI Documento 8973 – Manual de la seguridad de la aviación
- OACI Documento 9985 – Manual de seguridad ATM
- Estrategia sobre ciberseguridad de la aviación de la OACI
- OACI Documento 9849- Manual GNSS
- Guía sobre la Estrategia Nacional de Ciberseguridad ITU
- CANSO Estándar de excelencia sobre ciberseguridad
- Serie de normas ISO 27000
  - ISO/IEC 27001 Gestión de la información sobre seguridad
  - ISO/IEC 27002:2013- Tecnología de la información — Técnicas de seguridad — Código de práctica para controles de seguridad de la información.
- OACI: https://www.icao.int/cybersecurity/Pages/default.aspx
- FAA: https://www.faa.gov/air_traffic/technology/cas/
- EUROCONTROL : https://www.eurocontrol.int/cybersecurity
- NIST: https://www.nist.gov/cyberframework/framework


MONTRÉAL
(HEADQUARTERS)
PARIS
(EUROPEAN AND
NORTH ATLANTIC)
BEIJING
(ASIA-PACIFIC
SUB-OFFICE)
CAIRO
(MIDDLE EAST)
MEXICO CITY
(NORTH AMERICA AND CARIBBEAN)
DAKAR
(WESTERN AFRICA)
BANGKOK
(ASIA-PACIFIC)
NAIROBI
(EASTERN AFRICA)
LIMA
(SOUTH AMERICA)
ICAO

THANK YOU!