ICAO UNITING AVIATION

Estrategia sobre ciberseguridad de la aviación

La visión de una estrategia mundial de la ciberseguridad de la aviación

Mayda Ávila

- Especialista Regional en Comunicaciones, Navegación y Vigilancia
- Oficina Regional para Norteamérica, Centroamérica y Caribe de la Organización de Aviación Civil Internacional

Introducción

- Tecnología y ciber-sistemas se han convertido en esenciales para la sociedad moderna, volviéndose componentes de muchas actividades dependientes de tecnologías de la información. Junto con beneficio de las ciber tecnologías surgen las inseguridades, afectando todos los sistemas e infraestructuras. Las ciber amenazas y los ciber ataques tienen un componente y un efecto transnacional ya que los sistemas mundiales están interconectados. Además la complejidad de acción tiene implicaciones para varios actores a nivel nacional, regional e internacional.

Antecedente

- La Resolución A39-19 de la Asamblea instruyó a la OACI a desarrollar un plan de trabajo integras de ciberseguridad y una estructura de gobernanza.
- El Grupo de estudio de la Secretaría sobre ciberseguridad (SSGC) desarrolló una Estrategia de ciberseguridad respaldado por la 40a Asamblea de la OACI (Resolución A40-10 – Abordar la ciberseguridad en la aviación civil, que sustituye a la Resolución A39-19).
- La OACI desarrolló la Estrategia de Ciberseguridad respaldada por su 40a Asamblea.

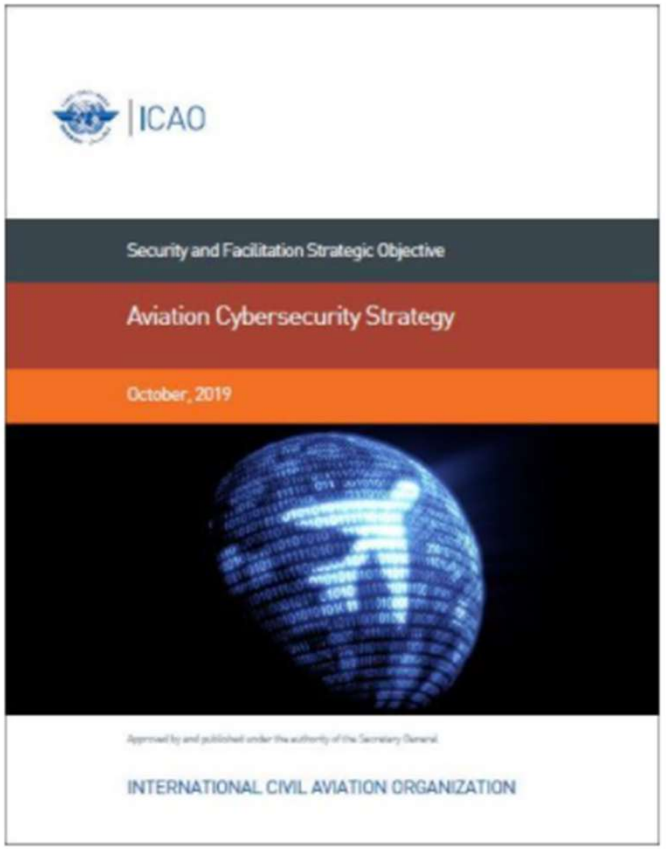
Grupos de trabajo sobre ciberseguridad de la OACI

- ***Grupo de estudio de la Secretaría sobre ciberseguridad (SSGC) de la OACI:***
  - **SSGC está organizado como un grupo plenario apoyado por un Subgrupo (Subgrupo de investigación sobre aspectos legales) y tres Grupos de trabajo (Grupo de trabajo sobre aerolíneas y aeródromos, Grupo de trabajo sobre sistemas de navegación aérea y Grupo de trabajo sobre ciberseguridad para la seguridad operacional de vuelo).**

https://www.icao.int/cybersecurity/Pages/Working-Groups.aspx

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

- ISe 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.

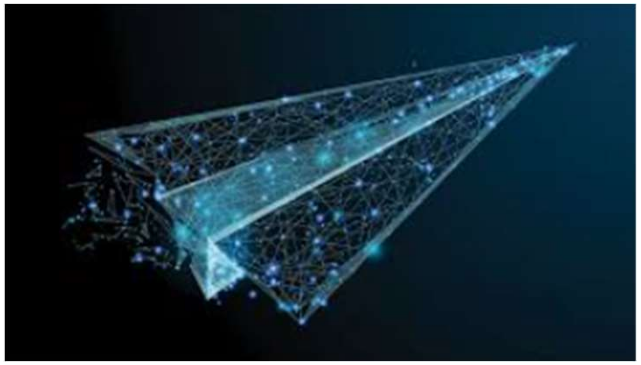
Compartición de información

- 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

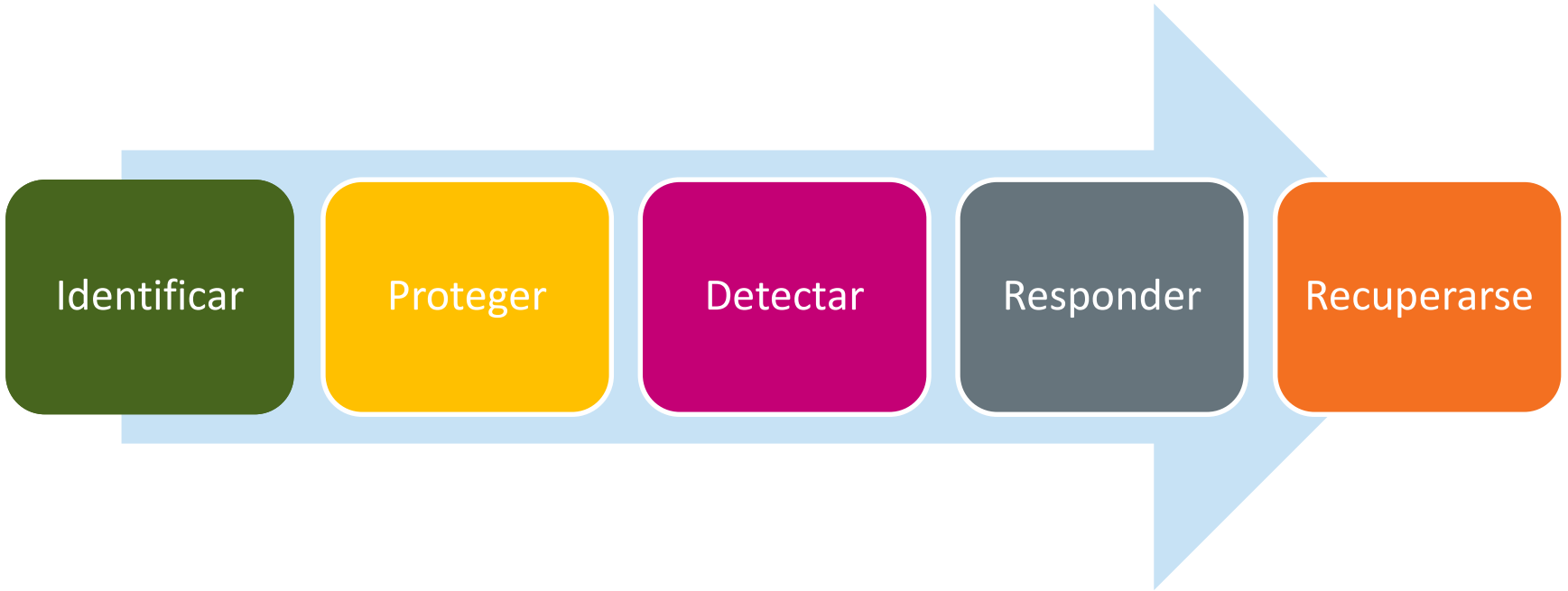
- Hay una necesidad, en línea con mecanismos existentes sobre gestión de incidentes, de tener planes apropiados y escalables que proporcionen continuidad del transporte aéreo durante ciber incidentes.
- Los ejercicios de ciberseguridad son herramientas útiles para probar ciber resiliencia existente e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

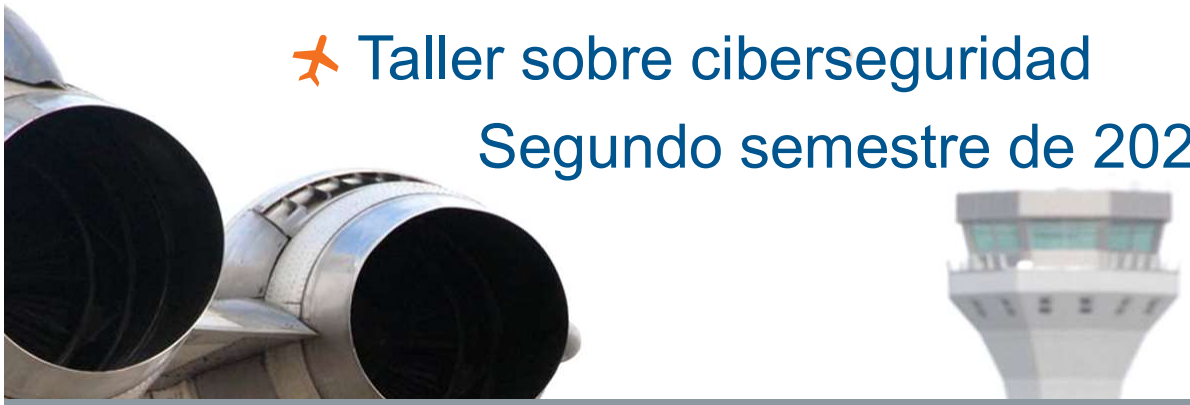
Próximos eventos

- Webinario sobre el Manual Políticas de Ciberseguridad OACI/CANSO/AIRBUS:

  Febrero de 2021

- Taller sobre ciberseguridad

  Segundo semestre de 2021, La Habana, Cuba




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!