In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

CONSIDERACIONES SOBRE CIBERSEGURIDAD PARA LA AVIACIÓN

Mayda Ávila S.
Especialista Regional en Comunicaciones, Navegación y Vigilancia
Oficina Regional para Norteamérica, Centroamérica y el Caribe (NACC) de la
Organización de Aviación Civil Internacional

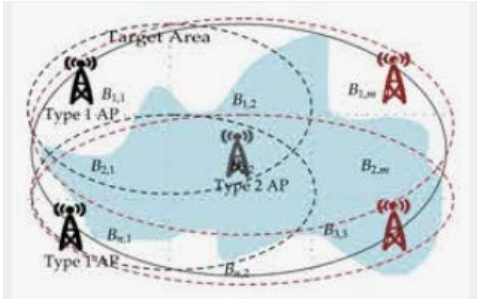
In cooperation with

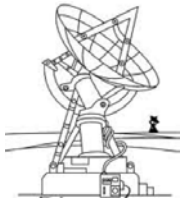
ICAO

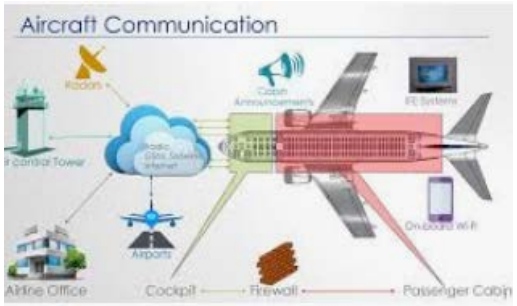
canso
civil air navigation services organisation

AIRBUS

Nuestro sector, incluye usuarios del espacio aéreo, proveedores de navegación aérea, explotadores de aeropuertos, autoridades de aviación civil y fabricantes de equipo ha sido objetivo de ciber-ataques por muchas razones, pero especialmente por ganancia financiera y robo de propiedad intelectual, así como para reducir la seguridad de las operaciones aeronáuticas.







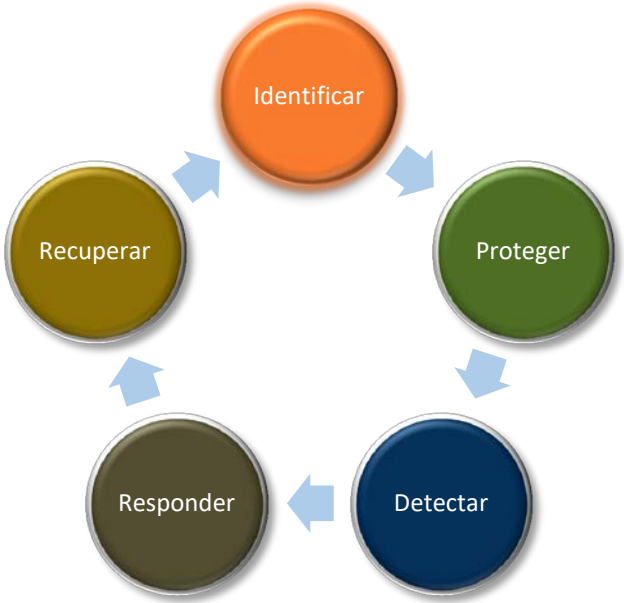
In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Mejores prácticas en ciberseguridad



- Estándar de Excelencia en ciberseguridad de CANSO.
- Unión Internacional de Telecomunicaciones (ITU):
  - Guía de la estrategia nacional sobre ciberseguridad.
- Marco de referencia del Instituto nacional de normas y tecnología (NIST) de los Estados Unidos.

In cooperation with

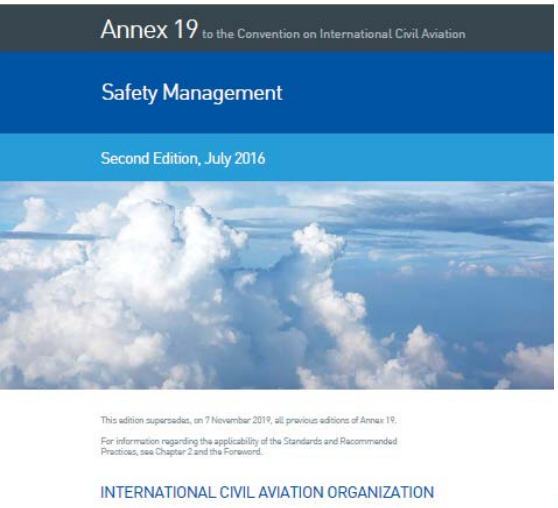
ICAO

canso
civil air navigation services organisation

AIRBUS

Identificar

- Identificar vulnerabilidades y riesgos de su organización.
- La organización identifica los riesgos en cuanto a ciberseguridad de su organización.
- ANSP deberían conducir una evaluación de riesgos para determinar sus riesgos y vulnerabilidades del negocio.
- Recolección de datos, información de seguridad, análisis de información e intercambio de información.
- La gestión de riesgos debería ser un proceso importante dentro de cualquier organización



Risk Management

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Proteger

- Proteger los elementos críticos de su organización.
- Identificar qué elementos requieren protección de otros que no pueden ser protegidos.
- La protección incluye muchos tipos de barreras, hardware, software, y también personas.

Proteger a fondo es un principio básico para definir la arquitectura de su estrategia de ciberseguridad.

Ninguna actividad tecnológica o de seguridad es perfecta, la presencia de diferentes capas de defensa incrementarán la dificultad para los ciber-atacantes y reducirán las oportunidades de tener un ataque exitoso.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

El proceso de identificación de activos, clasificación e implementación de medidas de protección es por lo tanto un elemento esencial de un programa de ciberseguridad.

Un programa de gestión de activos eficaz ayudará a mejorar la ciberseguridad a través del descubrimiento y análisis apropiado de activos. Estos incluyen datos, sistemas/equipos, instalaciones y personas.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Detectar

- Tenga por seguro que su organización enfrentara un evento de ciberseguridad.
- Detectar a tiempo y entender el impacto potencial del evento.
- Detectar e identificar actividad anómala.
- Desarrollar procedimientos y acciones para detección.
- Ser proactivo.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Responder

- Ha detectado un ciberataque.
  ¿Qué es lo que hará?

- Los procesos y procedimientos de respuesta se ejecutan y mantienen para asegurar respuestas puntuales a eventos detectados de ciberseguridad.

- La respuesta incluye programación (Plan de respuesta) y mitigación.

Recuperación

- Plan de recuperación en marcha.
- Los procesos y procedimientos de recuperación son ejecutados y mantenidos para asegurar una restauración a tiempo de los sistemas o activos afectados por los eventos de ciberseguridad.
- Una recuperación puedes ser pequeña como de un solo incidente de malware hasta un escenario de recuperación ante un desastre.
- Planear todos los procedimientos, mitigaciones y recursos requeridos son clave para construir una solución de recuperación sólida independientemente de la escala del incidente.

Deben ponerse en operación medidas efectivas para medir los diferentes procesos.

“Recuerde que lo que no se mide no puede ser mejorado”

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

El elemento humano de la ciberseguridad

- *El internet de las cosas.*
- *Hacer de su gente parte esencial de una estrategia de ciberseguridad de cualquier organización.*
- *Crear una cultura de la ciberseguridad.*
- *Hablar el mismo lenguaje sobre ciberseguridad.*

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

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.*

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Actividades bajo las Oficinas Regionales de la OACI

- Capacitación con el apoyo de Eurocontrol en la gestión de bases de datos y direccionamiento AMHS.
- Capacitación por la industria en la gestión y configuración de bases de datos de sistema ATC.
- Gestión de frecuencias aeronáuticas a nivel regional para asegurar que están protegidas para servicios actuales y futuros.
- Fortalecimiento de redes de comunicación regionales a través de nuevos proyectos que incrementan la seguridad.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

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.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

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

“Reunirse es un comienzo, mantenerse juntos es un progreso, trabajar juntos es un éxito.”

Henry Ford

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

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)

THANK YOU!