In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Introducción a la Política de Ciberseguridad para la ATM

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Agenda

- **Introducción**
  - Beneficios de la política de ciberseguridad
  - Documentación
  - ***Evolución de la Ciberseguridad en la OACI***
- **Introducción del modelo de política de Ciberseguridad para la gestión del tráfico aéreo**
  - Revisión del modelo de política de seguridad
    - Objetivos
    - Contenido
- **Ejemplo de caso de utilización.**

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Introducción

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Beneficios de la Política de Ciberseguridad

Cómo una buena política de seguridad protege y defiende

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

¿Hemos tenido suerte hasta ahora...?

- Ha habido incidentes de seguridad que han afectado a la aviación, pero ningún evento cibernético verdaderamente perturbador.
- ¿Es porque somos "buenos", o porque hemos tenido "suerte“?

Lo “Bueno”

- Tenemos una cultura de cuidado y atención para apoyar la seguridad.
- Nuestros sistemas suelen funcionar en un entorno aislado (pero esto está cambiando...)
- Nuestros procesos y procedimientos son naturalmente defensivos y cautelosos
- Tenemos listas de comprobación de listas de comprobación

¿Y sí ...?

- ... nuestro enfoque de seguridad puede ser utilizado para distraer de otras amenazas
- ... los sistemas en los que confiamos implícitamente han sido alterados
- ... nuestra precaución nos impide actuar con rapidez cuando lo necesitamos
- ... nuestras listas de control y procedimientos nos hacen predecibles para un atacante
- ... un proveedor en el que confiamos se ve comprometido

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

ESTUDIO DE CASO: Ataque "SUNBURST" de SolarWinds

- ***Probablemente el ataque más publicitado en lo que va de 2021***

A finales de 2020, SolarWinds descubrió que se había insertado un código malicioso en su producto de monitorización Orion.

El código malicioso se distribuyó a los clientes alrededor de marzo de 2020.

Los atacantes accedieron por primera vez a los sistemas internos de SolarWinds en septiembre de 2019.

Información extraída de Microsoft Security's Deep Dive into Solorigate/SUNBURST

Paso 4 - Compromiso
El código fue diseñado para proporcionar un punto de entrada en las organizaciones de usuarios finales. **Incluso en entornos aislados.**

Paso 3 - Despliegue
Los atacantes desplegaron 4.000 líneas de código malicioso, empaquetadas como parte genuina de Orion

Paso 2 - Investigación
Los atacantes se dedicaron a investigar las protecciones que tenía SolarWinds y a encontrar la manera de utilizarlas de forma maliciosa.

Paso 1 - Acceso no autorizado
Los atacantes encontraron de forma encubierta una forma de entrar en los sistemas de SolarWinds y establecieron una capacidad persistente.

Fuente:
https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

¿POR QUÉ UTILIZAR LA "POLÍTICA" COMO CONTROL DE SEGURIDAD?

¿Pero la seguridad no consiste en protecciones técnicas, cortafuegos y mantener 10.000 contraseñas únicas?

Estas protecciones técnicas tienen que basarse en una base sólida:

Gestión del riesgo
Los negocios consisten en gestionar el riesgo, por lo que se trata de gestionar la seguridad de una manera que resulte familiar y bien entendida.

Regulación
Aka Governance: supervisión independiente para ayudar a mantener los comportamientos correctos.

Mantenimiento
Protección contra los ataques a la cadena de suministro a través de los socios de mantenimiento

Seguridad de las comunicaciones
Protección contra la suplantación de identidad y la influencia de atacantes anónimos

Control de acceso
Tanto físico como lógico, uso del mínimo privilegio, etc.

Manejo de incidentes
Considere que un incidente podría ser un atacante inteligente en lugar de un evento estadístico.
Piense en la continuidad del negocio, tal vez en la degradación gradual del servicio.
Considere también la recuperación de desastres: cómo reconstruir desde la nada.

Nuevos sistemas
Diseñar la seguridad básica y asegurarse de que las cadenas de suministro son fiables y no se ven comprometidas

Seguridad operacional
Incorporar una buena ciberseguridad a los procesos operativos

Cumplimiento
Mantener los paquetes de pruebas: una parte fundamental de la auditoría

Gestión de activos
Saber qué tiene y a qué vulnerabilidades puede estar expuesto

La política es la base de una buena protección técnica

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

¿Hay algún ejemplo de "buena" política?

Por supuesto!! La "Plantilla de política de Ciberseguridad para la gestión del tráfico aéreo"

Desarrollada en colaboración entre ICAO NACC, CANSO and Airbus

In cooperation with

ICAO canso AIRBUS

CONTEXTO

Gestión de riesgos:

- Tener en cuenta la seguridad en toda la gestión de riesgos
- Disponer de un proceso metódico para tomar decisiones justificadas
- Integrar la seguridad en todo el ciclo de vida

Gestión de activos:

- Conozca lo que tiene
- Controle el acceso y sea proporcional a las TI/OT/IACS/Comunicaciones
- Reconocer el valor de los datos y de los activos físicos

Cadena de suministro:

- Trazar un mapa de toda la cadena de extremo a extremo
- Empiece por los eslabones adyacentes y trabaje hacia fuera
- Mitigar mediante la gestión de riesgos

Respuesta a los incidentes:

- Preparar y tener en cuenta a los atacantes informados
- Definir las prioridades en función de los escenarios
- Compartir información con los socios

OBJECTIVOS

Gestión de riesgos y gobernanza

• Gestión	Sección 7
• Regulación	Sección 8
• Cumplimiento	Sección 20

Proteger los activos

Gestión de activos	Sección 10
Seguridad operativa	Sección 13
Control de acceso	Sección 11
Seguridad de las comunicaciones	Sección 14

Cadena de suministro

Mantenimiento	Sección 15
Adquisición	Sección 15
Relaciones	Sección 16

Cuando las cosas van mal...

Gestión de incidentes	Sección 17
BC / DR	Sección 18
Hablar en voz alta	Sección 18

In cooperation with

ICAO

canso

AIRBUS

¿CUÁLES SON LOS BENEFICIOS?

Al repasar cómo los requisitos de la plantilla de ciberpolítica de la ATM protegen contra un ataque como el de SolarWinds Orion...

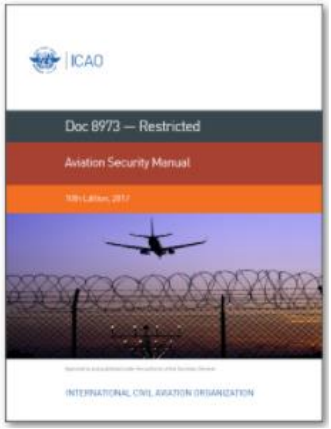
In cooperation with

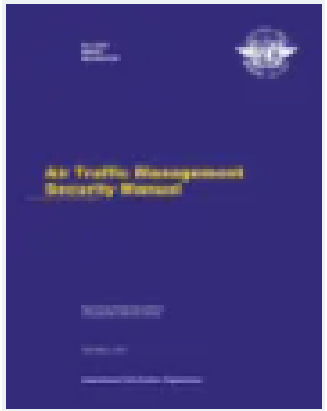
ICAO

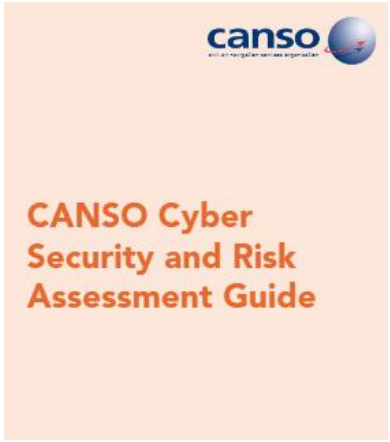
canso
civil air navigation services organisation

AIRBUS

Documentos







In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Documentación

- *Resolución A40-10: Abordar la Ciberseguridad en la aviación civil*
- *Plantilla de política de Ciberseguridad para la gestión del tráfico aéreo.*
- *Manual de gestión de la seguridad (SMM) (Doc 9859).*
- *Declaración del contexto de riesgo global de la seguridad de la aviación de la OACI (Doc 10108)*
- *Manual de Seguridad de la Aviación (Doc 8973)*
- *Anexo 17: Disposiciones de seguridad*

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Documentación

- *Manual de seguridad para la gestión del tráfico aéreo (Doc 9985)*
- *Anexo 19; Gestión de la seguridad.*
- *Estrategia de Ciberseguridad de la aviación de la OACI*
- *Norma de Excelencia en Ciberseguridad de CANSO*
- *La serie ISO/IEC 27000 comprende normas de seguridad de la información*
- *Plan de Acción de Ciberseguridad de la OACI*

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

La serie ISO/IEC 27000 incluye normas de seguridad de la información

- Información sobre las mejores prácticas para mejorar la seguridad de la información
- ISO/IEC 27000 Sistemas de gestión de la seguridad de la información Descripción general y vocabulario
- ISO/IEC 27001 Sistemas de gestión de la seguridad de la información Requisitos
- ISO/IEC 27002 Código de prácticas para la gestión de la seguridad de la información
- ISO/IEC 27003 Guía de implementación de sistemas de gestión de la seguridad de la información
- ISO/IEC 27004 Gestión de la seguridad de la información Medición
- ISO/IEC 27005 Gestión de riesgos de la seguridad de la información
- ISO/IEC 27006 Requisitos para los organismos de auditoría y certificación de los sistemas de gestión de la seguridad de la información
- ISO/IEC 27010 Tecnología de la información -- Técnicas de seguridad -- Gestión de la seguridad de la información para las comunicaciones intersectoriales e interorganizacionales.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

La serie ISO/IEC 27000 incluye normas de seguridad de la información

- Información sobre las mejores prácticas para mejorar la seguridad de la información
  - ISO/IEC 27011 Directrices de gestión de la seguridad de la información para organizaciones de telecomunicaciones basadas en la norma ISO/IEC 27002
  - ISO/IEC 27031 Directrices para la preparación de las tecnologías de la información y las comunicaciones para la continuidad de las actividades
  - ISO/IEC 27033-1 Visión general y conceptos de seguridad de redes
  - ISO/IEC 27033-3:2010 Seguridad de la red - Parte 3: Escenarios de red de referencia - Amenazas, técnicas de diseño y cuestiones de control
  - ISO/IEC 27035 Gestión de incidentes de seguridad
  - ISO 27799 Gestión de la seguridad de la información en el ámbito de la salud utilizando la norma ISO/IEC 27002

La Ciberseguridad debe interactuar con otras disciplinas (seguridad, eficiencia) de forma similar a lo que ocurre actualmente con la seguridad "tradicional" de la aviación para garantizar la evaluación precisa de la exposición a las amenazas de Ciberseguridad y asegurar el desarrollo de estrategias de ciberprotección eficaces y eficientes basadas en el riesgo.

La Ciberseguridad debe tender puentes entre la seguridad y la protección de la aviación, ya que la naturaleza multidisciplinar de la Ciberseguridad debe beneficiarse de la seguridad y la protección.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Evolución de la Ciberseguridad en la OACI

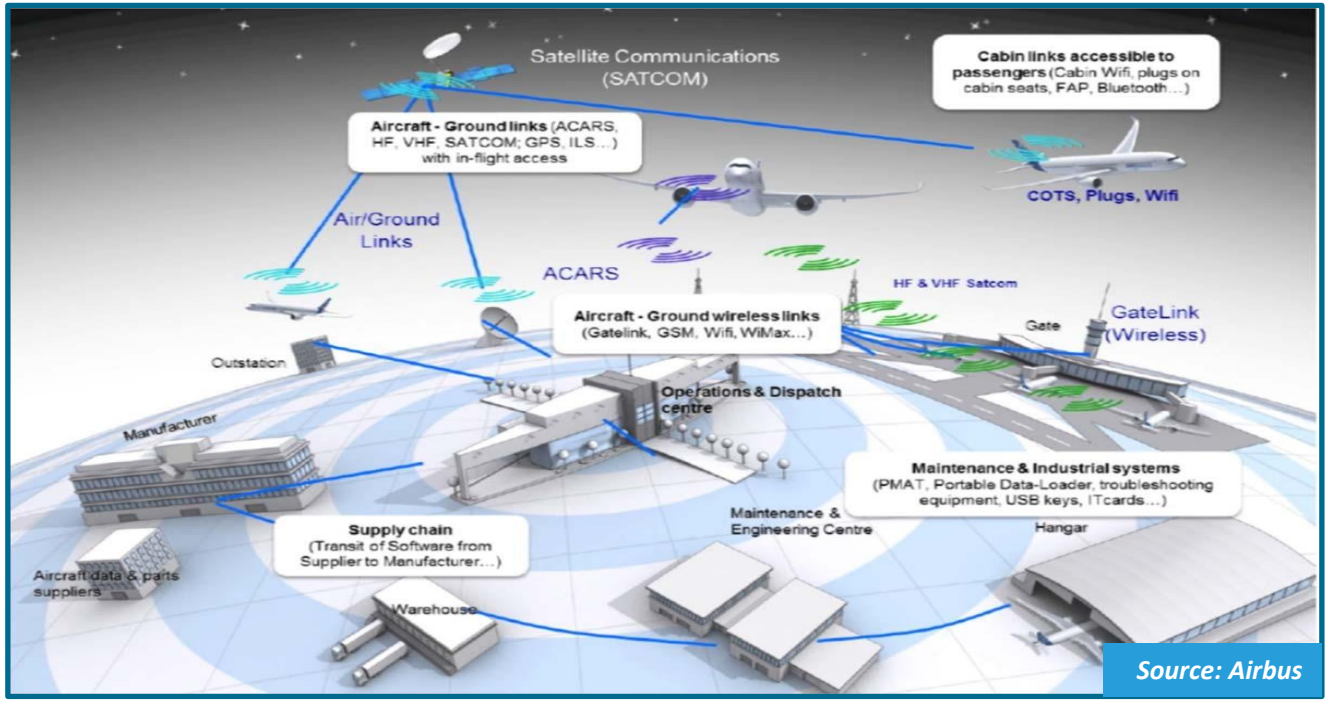
In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

¿Por qué la ciberseguridad en la aviación civil?



Source: Airbus

La interconexión e interoperabilidad de los sistemas digitales entre las partes interesadas de la aviación amplía el panorama de las ciberamenazas

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Cronología de la Ciberseguridad de la OACI

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

La labor de la OACI en materia de ciberseguridad

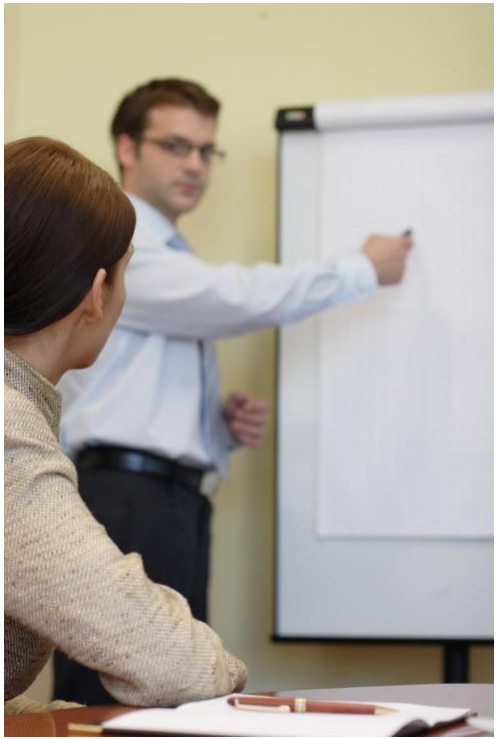
- **Instrumentos jurídicos:**
  - El Convenio de Pekín y el Protocolo de Pekín de 2010
- **Resoluciones de la Asamblea:**
  - Resoluciones A39-19 y A40-10 sobre ciberseguridad
- **Normas y prácticas recomendadas:**
  - Anexo 17 - Seguridad: Norma 4.9.1 y Práctica recomendada 4.9.2
- **Material de orientación:**
  - Procedimientos para los servicios de navegación aérea - PANS
  - Doc 8973 - Manual de seguridad de la aviación
  - Doc 9985 - Manual de Seguridad ATM
  - Estrategia de ciberseguridad de la aviación
  - Plan de Acción de Ciberseguridad
- **Formación**
  - Hoja de ruta de formación en ciberseguridad
  - Cursos de formación

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Entrenamiento

- **Cursos de formación en desarrollo:**
  - ✓ Fundamentos de la ciberseguridad en la aviación Liderazgo y gestión técnica
    - ✓ Desarrollado en colaboración con la OACI y la Embry-Riddle Universidad Aeronáutica
    - ✓ Dos cursos: Liderazgo y Gestión Técnica
  - ✓ Gestión de la seguridad ATM
    - ✓ Desarrollado en asociación entre la OACI y EuroControl
    - ✓ Cubre la seguridad tradicional ATM, así como la cibernética.



In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Grupos de expertos de la OACI que abordan la ciberseguridad en su trabajo

- **Grupo de Estudio de la Secretaría sobre Ciberseguridad – SSGC**
  - ✓ Subgrupo de Investigación sobre Aspectos Jurídicos
  - ✓ Grupo de trabajo sobre líneas aéreas y aeródromos
  - ✓ Grupo de Trabajo sobre Sistemas de Navegación Aérea
  - ✓ Grupo de Trabajo sobre Ciberseguridad para la Seguridad de Vuelo
- **Grupo de Estudio del Marco de Confianza – TFSG**
  - ✓ Grupo de trabajo sobre necesidades operativas de reciprocidad de confianza
  - ✓ Grupo de trabajo sobre identidad digital
  - ✓ Grupo de trabajo de la red interoperable de aviación global resistente

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

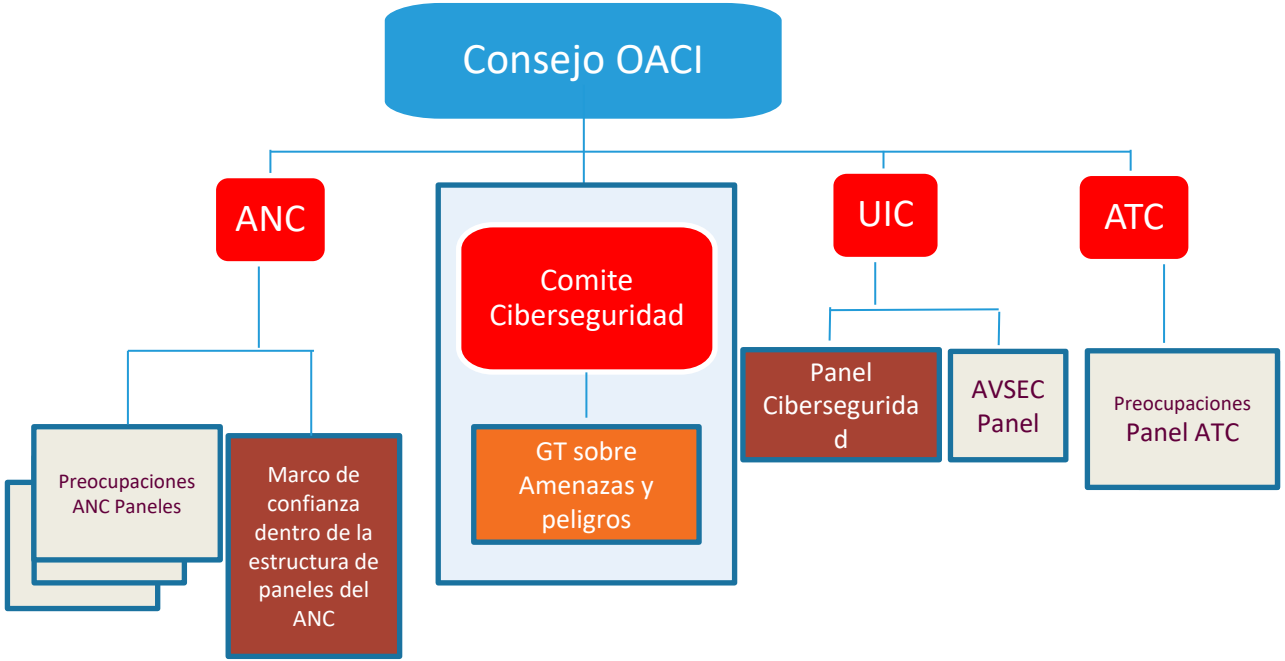
Estudio de viabilidad del mecanismo para abordar la ciberseguridad en la OACI

- Los trabajos comenzaron en 2018.
- Primer borrador presentado al Consejo en 2020.
- Pequeño grupo de trabajo (SWG)
  - Establecido el 30 de octubre de 2020
  - Se reunió 15 veces en menos de dos meses
  - Desarrolló 3 opciones, las evaluó y recomendó una opción preferida para la consideración del Consejo

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Decisión del Consejo sobre el mecanismo para abordar la ciberseguridad en la OACI



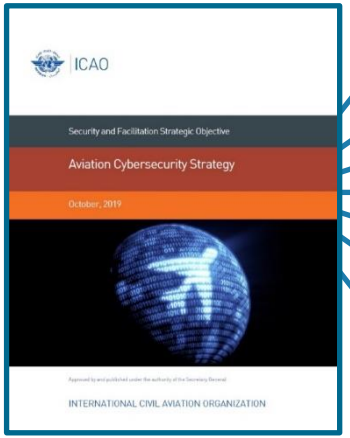
In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Estrategia de ciberseguridad en la aviación



- Cooperación Internacional
- Gobernanza
- Efectiva legislación y regulación
- Politica de ciberseguridad
- Compartir Información
- Gestión de incidentes y planificación de emergencias
- Creación de capacidades, formación y cultura de ciberseguridad

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Plan de acción de Ciberseguridad

- Publicado en noviembre 2020.
- **TLP verde.**
- **Proporciona la base para** OACI, Estados y partes interesadas para trabajar juntos, y propone una **serie de principios, formas de medición y acciones** para alcanzar los objetivos de los siete pilares de la Estrategia de Ciberseguridad.
- **Desarrolla los siete pilares** de la Estrategia de Ciberseguridad de la Aviación en **29 acciones prioritarias,** que se desglosan a su vez en **54 tareas** que deben ser aplicadas por la OACI, los Estados y las partes interesadas.

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Plan de Acción de Ciberseguridad (Ejemplo)

Resultado prioritario	Pilar 3: DESARROLLO DE LEGISLACIÓN Y REGLAMENTACIÓN EFICAZ
Acciones con prioridad	• Garantizar la existencia de una normativa y una legislación adecuadas en materia de ciberseguridad; • Desarrollar directrices apropiadas para los Estados y la industria en la aplicación de las disposiciones relacionadas con la ciberseguridad; • Garantizar que los instrumentos jurídicos internacionales proporcionen medidas adecuadas para la prevención, la reacción oportuna y el enjuiciamiento de los ciberincidentes.

Actiones

Acción #	Por	Seguimiento de la estrategia de ciberseguridad	Trazabilidad en el Plan de Acción	Medidas/tareas específicas	Indicadores	Madurez	Objetivo
CyAP 3.1	Estados Miembros	3.3	8.4	Estados Miembros ratificar los instrumentos de Pekín.	Número de Estados que han ratificado los instrumentos de Pekín	Bajo	En proceso
CyAP 3.2	OACI	3.3	8.3	Análisis de los instrumentos de derecho aéreo internacional	Informe y plan de actualización	N/A	2020
CyAP 3.3	OACI and Estados Miembros	3.3	8.2	Análisis de la legislación internacional y nacional existente en el ámbito de la ciberseguridad e identificación de las lagunas, incluido el derecho penal.	Promover la ratificación de instrumentos para incriminar los actos cibernéticos ilícitos.	Medio	2022 - 2023
CyAP 3.4	OACI, Estados Miembros y la Industria	3.3	8.1	Revisar las normas de seguridad existentes de la OACI para identificar la necesidad de posibles actualizaciones de ciberseguridad	Análisis de las lagunas normativas	Alta	2021
CyAP 3.5	OACI	3.2	5.4	Crear, revisar y modificar el material de orientación relacionado con la aplicación de los	Material de orientación sobre ciberseguridad aceptado y acordado	Alta	2021-2022

In cooperation with

ICAO

canso
civil air navigation services organisation

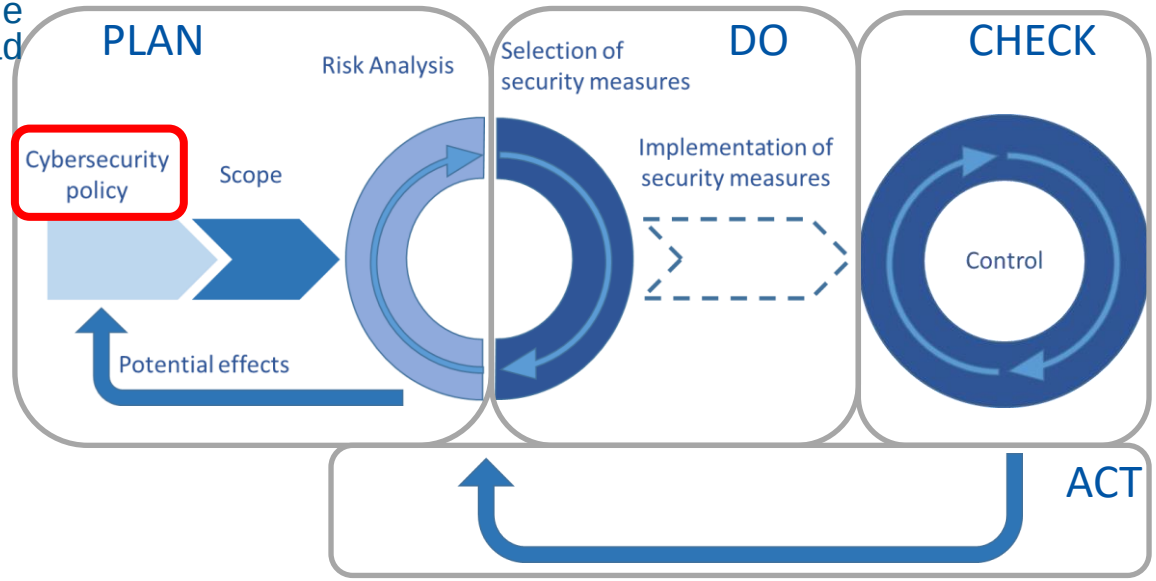
AIRBUS

Introducción del modelo de política de Ciberseguridad para la gestión del tráfico aéreo

Enfoque del Sistema de Gestión de información de seguridad (ISMS)

El ISMS proporciona un enfoque sistemático para pruebas de la seguridad de la información de las organizaciones.

- Con los objetivos de:
  - Cumplir con las limitaciones de seguridad
  - Proporcionar resiliencia
  - Asegurar confiabilidad
  - Apoyar el modelo de negocios ATM



In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Política de Ciberseguridad para iniciar ISMS

Requisito ATMSP-001-01

Basado en la política de seguridad, un sistema de gestión de seguridad de la información debería ser definido, implementado y mantenido basado en un enfoque de gestión de riesgos.

Las normas ISO27001 e ISO27002 proporcionan un proceso aprobado y mejores prácticas para los beneficios ISMS a partir de los principios de la gestión de seguridad de las aeronaves de Airbus.

➔ Adicionalmente: Alcanzar una madurez permite reducir muchos cambios al sistema y a los sistemas de información bajo las limitaciones de la regulación de la seguridad operacional (dirigido a costos)

Objetivos de la política de Ciberseguridad

- Se enfoca en 2 objetivos clave
  - Seguridad operacional
  - Continuidad del negocio
- Con base principios clave del ISO27001 y IEC62443 (sistemas industriales)
- Beneficios de los principios del sistema de la gestión de seguridad de las aeronaves de Airbus

➔ Para proporcionar seguridad de principio a fin: “seguridad bajo diseño de la tierra al cielo”

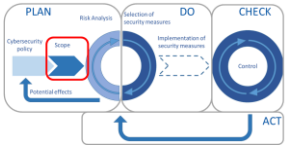
In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Enfoque y objetivos



- Atender ATM en su totalidad:
  - Actores, empleados/as, socios/as y proveedores
  - Servicios y sistemas relacionados con la información
  - Infraestructuras (IT, OT, IACS)
- Con el objetivo de proporcionar resiliencia
  - Basado en criticidad sobre seguridad y operatividad

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Infraestructuras (IT, OT, IACS)

Infraestructura IT	Infraestructura OT y IACS
Infraestructura IT son los componentes requeridos para operar y gestionar entornos TI empresarial, hardware, software, componentes de redes de trabajo, un sistema operativo (OS) y almacenamiento de datos.	Tecnología operacional (OT) y los Componentes del Esquema de Certificación de Ciberseguridad; Automatización industrial y sistemas de control (IACS). Elemento crítico para ciberseguridad

Gestión de riesgo de Ciberseguridad

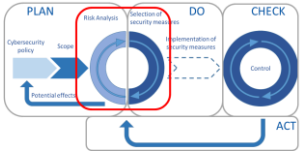
Requisito ATMSP-002-01:

La seguridad ATM debería ser dirigida a la inteligencia, basada en la amenaza y gestionada al riesgo.

Requisito ATMSP-003-01:

La gestión del riesgo en la seguridad de la información debería ser considerada como parte integral del proceso general del ciclo de vida del sistema.

Gestión de riesgo de ciberseguridad



Requisito ATMSP-004-01:

Todos los activos ATM (datos, sistemas, personal...) debería tener propiedad definida.

Requisito ATMSP-005-01:

Defensa profunda de principios como se define en 5 – Objetivo de la arquitectura de seguridad, debe ser parte de la gestión de la información de seguridad.

Gestión de riesgo de ciberseguridad

Requisito ATMSP-006-01:

El enfoque basado en el Riesgo de seguridad ATM debe implementar medidas se seguridad técnica y operacional (políticas y procesos) para reducir el riesgo aun nivel aceptable sobre:

- (Intencional) ciberataque exitoso,
- Error humano,
- Accidente o incidente,
- Imparto por desastre natural.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Gestión de riesgo de Ciberseguridad

Requisito ATMSP-007-01:

La organización encargada de la seguridad física o información ATM debe asegurar tratamiento eficiente y coordinado del riesgo de seguridad.

Requisito ATMSP-008-01:

Los riesgos de seguridad de la información ATM deben ser revisados y monitoreados de manera regular.

Gestión de riesgo de ciberseguridad

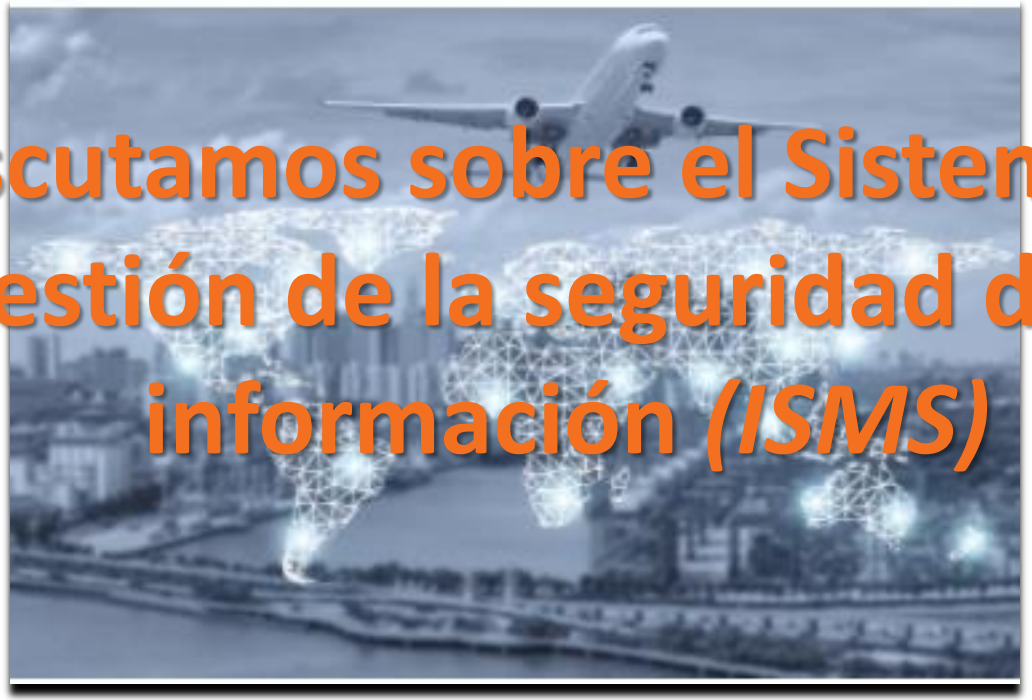
- Reducir el riesgo a un nivel aceptable
  - Basado en criticidad sobre seguridad operacional y operatividad
- Probabilidad basada en la resiliencia de los sistemas al ataque
  - Principios de arquitectura
  - Ningún punto de vulnerabilidad común

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS



Discutamos sobre el Sistema de gestión de la seguridad de la información *(ISMS)*

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Seguridad de la gobernanza y organización

Requisito ATMSP-009-01:

La AAC debe designar una Autoridad apropiada (AA) responsable de toda la seguridad ATM.

Requisito ATMSP-010-01:

El responsable de seguridad ATM designado por la AAC debe definir un mínimo de:

- Roles y responsabilidades para la gestión del riesgo de seguridad ATM;
- Procesar la gestión del riesgo;
- Procesos para incidentes, crisis y gestión de la continuidad del negocio.

Requisito ATMSP-011-01:

Las habilidades y competencias del personal designado a los roles y responsabilidades de seguridad ATM deben permanecer actualizadas.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Seguridad de la gobernanza y organización

- Pensar la Ciberseguridad con una perspectiva de largo plazo
  - Política de Ciberseguridad puesta en marcha y aplicable
  - La Ciberseguridad identificada como como interés central de la organización (en cuanto a seguridad operacional)
- Definir roles y responsabilidades
  - Nominación formal
  - Descripción detallada de las responsabilidades


Riesgo de seguridad

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Política a detalle

- Recursos humanos
- Gestión de activos
- Control de acceso
- Seguridad física y del entorno
- Seguridad de operación
- Seguridad de comunicación
- Sistema de adquisición, desarrollo y mantenimiento
- Proveedores y socios
- Gestión del incidente de seguridad
- Continuidad del negocio
- Datos personales
- Cumplimiento

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Recursos humanos

- Revisión de antecedentes antes de la contratación
- Cultura de la seguridad y capacitación durante el empleo
- Recordatorios de bajas y compromisos después del empleo

Recursos Humanos

Requisito ATMSP-012-01:

El personal debe ser parte de la seguridad ATM durante todas las fases de empleo:

- Antes del empleo: a través de medidas como revisión de antecedentes de conformidad con las regulaciones locales;
- Durante el empleo: al desarrollar una cultura de la seguridad a través de capacitación regular y levantando conciencia; y
- Después del empleo: al asegurar el respeto del proceso de baja y recordando al personal el compromiso de no-divulgación.

Recursos Humanos

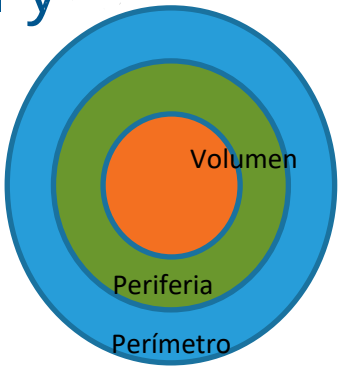
Requisito ATMSP-013-01:

El personal de seguridad deber asegurar que todos los individuos con acceso a las instalaciones ATM, áreas controladas y datos sensibles ATM no constituyan un riesgo inaceptable (como en el Capítulo 7 de Gestión de riesgos).

Revisión de antecedentes de seguridad

Gestión de Activos

- Establecer y mantener un inventario de activos
- Incluir criticidad (sobre seguridad operacional y operatividad) en la categorización de activos
- Asegurar consistencia entre
  - Acceso lógico y físico
  - Acceso y zonificación



In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Gestión de Activos

Requisito ATMSP-014-01:

Un inventario de activos ATM debe ser desarrollado y mantenido actualizado.

Requisito ATMSP-015-01:

ATM debe clasificar (categorizar) sus activo de acuerdo a su criticidad a fin de implementar medios adecuados de protección.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Gestión de activos

Requisito ATMSP-016-01:

Los datos ATM deben ser clasificados por defecto con un nivel adecuado de clasificación.

Información adicional: por favor refiérase a la regulación nacional aplicable

Requisito ATMSP-017-01:

Los datos ATM deben ser protegidos durante almacenamiento, procesamiento e intercambio, en línea con su perfil de sensibilidad.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Hablemos sobre activos de Ciberseguridad

Zonificación lógica

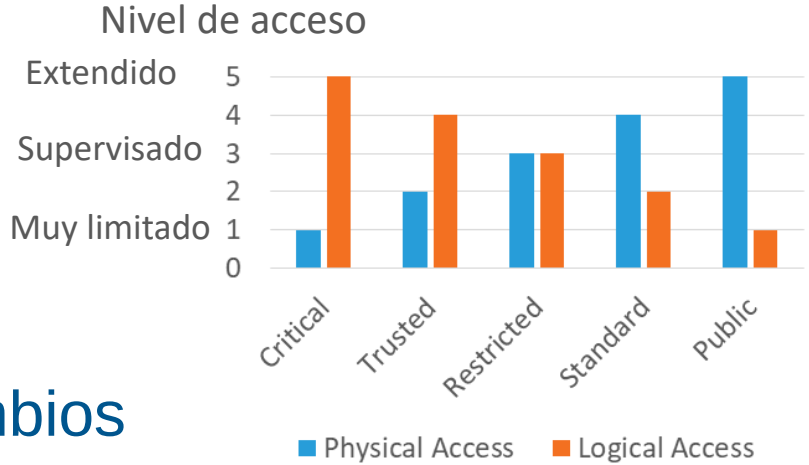
- La zonificación en un enfoque de diseño lógico utilizado para controlar y restringir el acceso y flujos de comunicación de datos solamente a aquellos componentes y usuarios de conformidad con la política de seguridad.

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Control de acceso y seguridad física y del entorno

- Poner atención en el balance entre el control de acceso físico y lógico
- Asegurar consistencia de las Zonas lógicas y físicas
- Monitorear y adaptarse a los cambios
  - Revisiones y monitoreo regulares
  - Eliminación y desmantelamiento



Control de acceso y seguridad física y del entorno

Requisito ATMSP-018-01:

Acceso a cualquier activo ATM debe ser permitido sobre:

La verificación de ausencia de riesgo inaceptable (como en el Capítulo 7 de la Gestión de riesgos); con base en la necesidad de saber).

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Control de acceso y seguridad física y del entorno

Requisito ATMSP-019-01:

La seguridad física ATM debe salvaguardar TI, OT, IACS e infraestructura CNS/ATM, contra interferencia ilítica y acceso no autorizado.

Requisito ATMSP-020-01:

La seguridad física ATM debe identificar zonas que alberguen activos CNS/ATM de acuerdo con su criticidad en cuanto a seguridad operacional y operatividad.

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Control de acceso y seguridad física y del entorno

Requisito ATMSP-021-01:

Medidas de seguridad física ATM deben proteger la CNS/ATM de interrupciones intencionales o ilícitas de los servicios y operaciones.

Requisito ATMSP-022-01:

La seguridad física ATM debe proteger flujos entrantes y salientes de zonas de almacenaje y centros de datos.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Zonas de Ciberseguridad

Seguridad de la Operación

- Operar la seguridad desde la zona de confianza
- La eficiencia de las medidas de seguridad basada en la fortaleza de los procesos de seguridad
- Aplicar el proceso de gestión de vulnerabilidad (incluyendo monitoreo, calificación y mitigación)

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Seguridad de la Operación

Requisito ATMSP-023-01:

La organización de la Ciberseguridad ATM debe asegurar la coordinación de operaciones de seguridad, monitoreo y mejora continua del procesamiento de información.

Requisito ATMSP-024-01:

Las operaciones de Ciberseguridad ATM deben incluir TI, OT, IACS e infraestructura CNS/ATM en el ámbito de las operaciones de seguridad.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Seguridad de la operación

Requisito ATMSP-025-01:

Las operaciones de Ciberseguridad ATM deben mantener la efectividad de las medidas de seguridad a través de su ciclo de vida.

Requisito ATMSP-026-01:

La Ciberseguridad ATM deber ser operada desde zonas dedicadas habiendo designado un perímetro de seguridad físico y lógico.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Seguridad de la Operación

Requisito ATMSP-027-01:

La Ciberseguridad ATM debe prevenir la explotación de vulnerabilidades técnicas en la infraestructura TI, OT, IACS y CNS/ATM.

Requisito ATMSP-028-01:

La Ciberseguridad ATM debe prohibir el uso de aparatos móviles personales para las actividades CNS/ATM.

Seguridad de la Operación

Requisito ATMSP-029-01:

La Ciberseguridad ATM deber asegurar que los aparatos móviles profesionales no constituyan un riesgo inaceptable a la seguridad (como en el Capítulo 7 de la Gestión de riesgos).

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Gestión de la Ciberseguridad

Seguridad de la Comunicación

- Mantener el control en las conexiones y conectividad
- Asegurar consistencia de zonas lógicas y físicas (activos)
- Implementar defensa a fondo basado en la criticidad de activos de seguridad operacional y operatividad

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Seguridad de la Comunicación

Requisito ATMSP-030-01:

La Ciberseguridad ATM debe mantener y actualizar el mapeo de redes y sus interconexiones.

Requisito ATMSP-031-01:

Las redes ATM deben ser lógica y físicamente segregadas basadas en su criticidad de seguridad operacional y operatividad.

Seguridad de la Comunicación

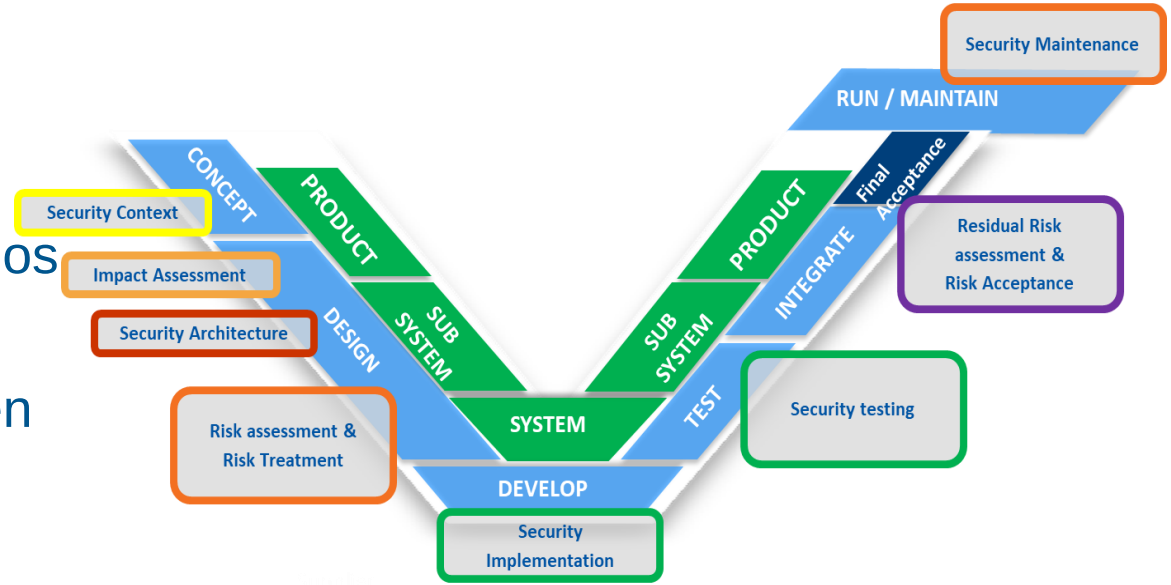
Requisito ATMSP-032-01:

La Ciberseguridad ATM debe asegurar que las tecnologías inalámbricas y el acceso a internet no constituyan un riesgo inaceptable a la seguridad operacional y a la seguridad de la aviación (como en el Capítulo 7 de la Gestión de riesgos).

Segregación de redes

Adquisición de sistemas, desarrollo y mantenimiento

- Integrar la seguridad al desarrollo de ciclo de vida
- Basado en gestión de riesgos
- Gestión de vulnerabilidad en todo momento



In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Adquisición de sistemas, desarrollo y mantenimiento

Requisito ATMSP-033-01:

La Ciberseguridad ATM debe asegurar que la seguridad de la información sea una parte integral de sistemas de información CNS/ATM a través de su ciclo de vida completo.

Información adicional: Esto también incluye los requisitos de sistemas de información que proporcionan servicios ATM en redes públicas.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Adquisición de sistemas, desarrollo y mantenimiento

Requisito ATMSP-034-01:

La Ciberseguridad ATM que los sistemas de información CNS/ATM estén diseñados sobre los siguientes principios (lista no exhaustiva):

- Ningún punto de vulnerabilidad único ni común;
- Definición e implementación de reglas de códigos de seguridad;
- Gestión de la vulnerabilidad en software y hardware COTS;
- Implementación de normas industriales y recomendaciones (NIST, OWASP, …).

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Cuando desarrollas proyectos….

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Proveedores y socios (S & P)

- Defina sus expectativas de seguridad: requisitos de seguridad de S & P
- Ingrese a la madurez de seguridad de los S & P
- Monitorear y dar seguimiento a S & P
- Incluir adquisiciones en el equipo de seguridad

Proveedores y socios

Requisitos de seguridad

Autoevaluación de seguridad

Seguridad contractual

Supplier Marketing

Supplier Selection

Supplier onboarding

Evaluación de capacidades de seguridad

Supplier design

Seguimiento de seguridad

Tests

Supplier development

Organización de seguridad del proyecto

Supplier delivery

Seguridad del cambio y mantenimiento

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Proveedores y socios

Requisito ATMSP-035-01:

La Ciberseguridad ATM debe proporcionar seguridad a socios de principio a fin en la cadena de suministro en el enfoque del sistema de gestión de la Ciberseguridad CNS/ATM.

Requisito ATMSP-036-01:

La Ciberseguridad ATM debe asegurar que relaciones con entidades externas no constituyan un riesgo inaceptable (como en el Capítulo 7 de la Gestión de riesgos).

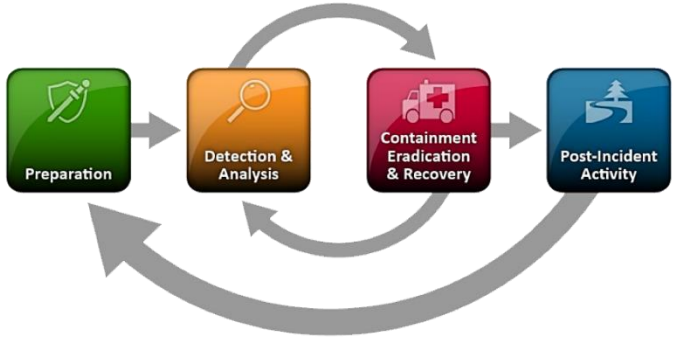
Hablando sobre proveedores….

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Gestión de incidentes de seguridad

- Esté preparado: con capacitación, exámenes regulares, juego serio, …
- Defina reglas de comunicación e identifique tomadores de decisión clave (proceso escalado)
- Conecte incidentes con crisis y Gestión de la continuidad del negocio
- Asegúrese de recopilar registros de manera coherente entre seguridad, protección y operatividad (centrado en activos críticos)
- Asegurar consistencia en la detección de incidentes con riesgos para mejorar la prioridad y exactitud del incidente



In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Gestión de incidentes de seguridad

Requisito ATMSP-037-01:

La Ciberseguridad ATM debe asegurar un enfoque consistente y efectivo de la gestión de incidentes de seguridad CNS/ATM, incluyendo comunicación en eventos y debilidades de seguridad.

Requisito ATMSP-038-01:

La seguridad operacional y continuidad del negocio deben ser las prioridades principales ATM de la gestión de incidentes de seguridad.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Incidentes y procedimientos de Ciberseguridad…

Continuidad del negocio

- Identificar los criterios desencadenantes
  - De la continuidad del negocio a la recuperación de desastres
  - De la continuidad del negocio a la crisis
- Reconsiderar la continuidad del negocio, incluyendo actos maliciosos y la seguridad de la cadena de suministro
  - Revisar sitios alternativos basados en la criticidad y la seguridad
  - Considerar la seguridad en la reubicación a sitios de negocio alternativos
  - Incluir la seguridad en pruebas de procedimientos de cambio y recuperación

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Continuidad del negocio

Requisito ATMSP-039-01:

La continuidad del negocio ATM debe ser diseñado conforme con los resultados de la Gestión de riesgos.

Requisito ATMSP-040-01:

La Ciberseguridad ATM debe establecer una estrategia consistente, efectiva y común para gestionar la seguridad de la aviación y la seguridad operacional CNS/ATM a través de la integración de todas las partes interesadas con esfuerzos comunes, compartición de información, para completar sus objetivos operacionales.

Plan de continuidad del negocio (BCP)

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

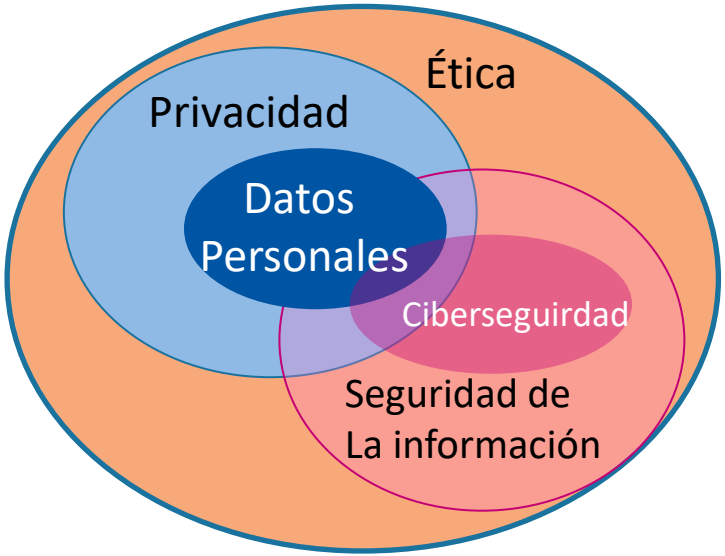
Datos personales

Requisito ATMSP-041-01:

La Ciberseguridad ATM debe asegurar la privacidad y protección de la información personalmente identificable de acuerdo con las regulaciones aplicables.

Datos personales

- Establecer y mantener un inventario de procesamiento de datos personales y realizar evaluaciones del impacto de privacidad
- Nominar el DPO y estableces gobernanza de dados personales (política y procedimientos)
- Poner atención a aspectos legales del intercambio de datos con EUA y (Acta de privacidad) y la UE (GPDR)
- Implementar recolección minimizado de datos y evitar interconexión de datos
- Verificar la duración del almacenamiento de datos e implementar la depuración de datos



In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Cumplimiento

- Realizar auditorías de terceras partes y proporcionar una declaración formal
- Revisión de cumplimiento a la regulación
- Verificar consistencia en la gobernanza y la organización
- Evaluar eficiencia controles de seguridad
- Realizar examentes de intrusión
- Apoyar la mejora continua

Regulations
- Law
- External requirements / Standards

Governance & Organization
- Policies
- Processes
- Roles and Responsibilities

Implementation
- Cyber Security: Architecture & Configuration (Best practices)
  - Equipments & softwares
  - Accounts network, ...
- Physical Security: Protection & Detection
  - Physical controls and detection
  - Video Protection and CCTV

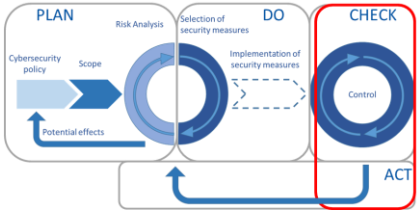
Cumplimiento

Requisito ATMSP-042-01:

Los sistemas de información CNS/ATM deben recibir calificación de validación de seguridad reconocida antes de entrar en servicio en cumplimiento con el estándar del proceso ED 205 para aspectos de seguridad en tierra sobre certificación/declaración de la gestión de tránsito aéreo / servicios de navegación aérea (ATM/ANS).

Información adicional: el proceso reconocido de acreditación será definido a nivel nacional y aplicable en infraestructuras críticas.

Cumplimiento



Requisito ATMSP-043-01:

La validación de los sistemas de seguridad de la información CNS/ATM debe ser controlada de manera regular.

Requisito ATMSP-044-01:

La Ciberseguridad ATM debe asegurar que cualquier desviación, detectada a través del proceso de validación, no constituye un riesgo aceptable (como en el Capítulo 7 de la Gestión de riesgos).

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Requisitos externos.....

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Usar ejemplos de caso y actividades iniciales de Ciberseguridad

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Orden del día

- Inicie su Sistema de gestión de seguridad ATM
- Política de compromiso de Ciberseguridad
- Actividades esperadas
- Ejemplo de caso: Sistema de comunicación
  - Descripción
  - Arquitectura
  - Identificación de impacto funcional
  - Muestras de trazabilidad y justificación con la política de seguridad
- Conclusión
- Preguntas y respuestas

In cooperation with

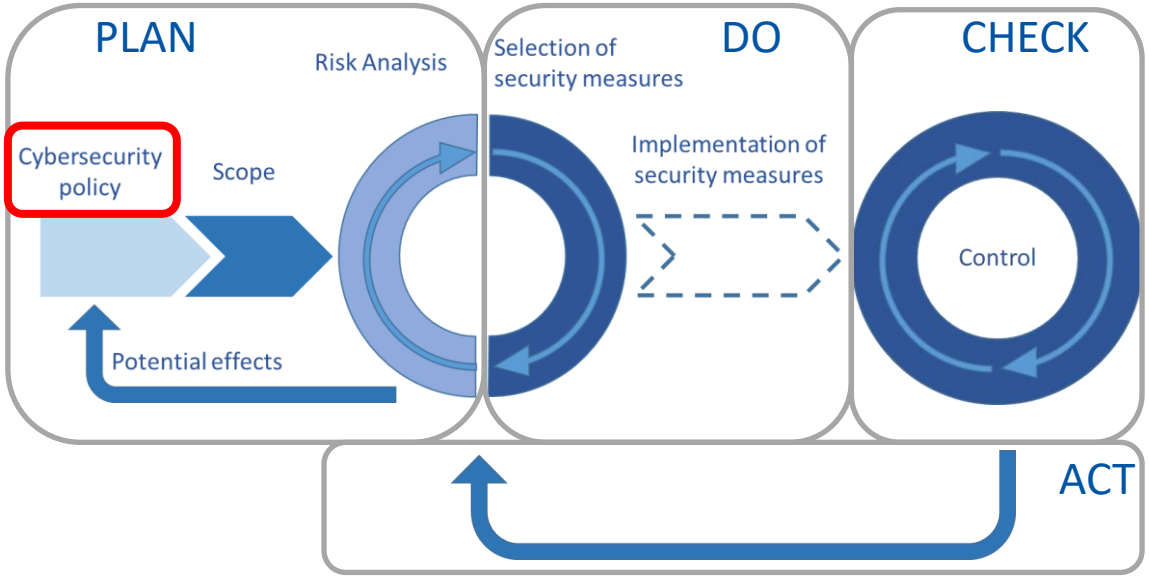
ICAO

canso
civil air navigation services organisation

AIRBUS

Inicie su Sistema de gestión de seguridad ATM

- Personalizar esta política de Ciberseguridad a su propio contexto
- Revisar cumplimiento con la regulación
- Hacerlo aplicable y comunicable



In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Política de compromiso de Ciberseguridad

- Empoderar la organización
  - Nominar personas clave
  - Asignar roles y responsabilidades
- Liderar la implementación del ISMS (comunicación transversal)

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Actividades esperadas

- Implementar una línea base de seguridad, basado en estándares y mejores prácticas (ISO 27002, NIST, IEC 62443) e iniciar la implementación.
- Empezar a trabajar utilizando un método basado en procesos
- Introducir ISMS en los procesos de la organización
- Evaluar riesgos y realizar decisiones de mitigación de riesgos
- Seguimiento a la implementación de mitigación de riesgos hasta su aceptación
- Monitoreo de riesgos y establecer un análisis de amenazas de inteligencia
- Revisar la efectividad (Auditoría y pruebas de penetración)
- Repetición de lo antes mencionado

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Ejemplo de caso: Sistema de comunicación

- El sistema a cargo de todas las comunicaciones entre el controlador y la aeronave (voz y datos)
- Gestiona las frecuencias y habilita a los pilotos
  - Para estar consciente de otras aeronaves en la misma zona
  - Reunir y gestionar instrucciones de ruta
- Cambiado de una base de circuitos a software y voz sobre IP

In cooperation with

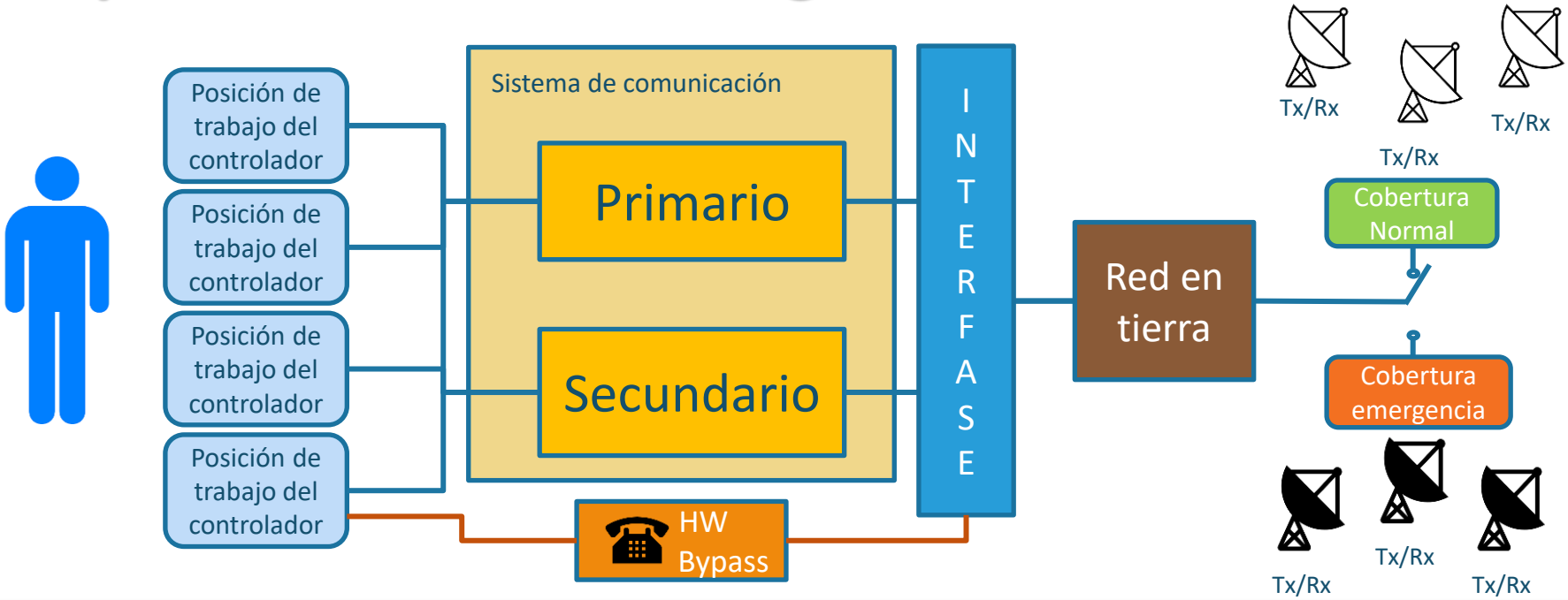
ICAO | canso civil air navigation services organisation | AIRBUS

Impacto funcional de Ciberseguridad

Evaluación de **consecuencias**:

Fase	Descripción del impacto	Nivel de impacto (seguridad operacional)
Tierra / Taxi	Pérdida de transmisión de datos: **sobre carga del controlador, limitación de capacidad en despegue y aterrizaje**	Más que peligroso
	Pérdida de comunicación: Atrasos, AoG	Menos a mayor
Ascenso / Aproximación	Pérdida de comunicación: Cierre de la posición del controlador / **Clausura de zona ATC / Procedimiento de « Cielo despejado »**	De peligroso a catastrófico
Crucero	Pérdida de comunicación: **Limitación de alta capacidad**	De peligroso a catastrófico

Arquitectura del sistema global de comunicación



Identificación de eventos temidos

Personal y usuarios

Posición de trabajo del controlador

Posición de trabajo del controlador

Posición de trabajo del controlador

Posición de trabajo del controlador

Sistema de comunicación

Primario

Secundario

HW Bypass

INTERFASE

Red en tierra

Cobertura normal

Cobertura emergencia

Tx/Rx

Tx/Rx

Tx/Rx

Tx/Rx

Tx/Rx

Tx/Rx

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Personal y usuarios

Requisito ATMSP-012-01:

El personal debe ser parte de la seguridad ATM durante todas las fases de contratación:

- Entres del empleo: a graves de revisiones de antecedentes de conformidad con regulaciones locales;
- **Durante el empleo: al desarrollar una cultura de la seguridad a través de capacitación regular y levantamiento de conciencia; y**
- Después del empleo: al asegurar el respeto del proceso de baja y recordando al personal el compromiso de no-divulgación.

Requisito ATMSP-013-01:

El personal de seguridad deber asegurar que todos los individuos con acceso a las instalaciones ATM, áreas controladas y datos sensibles ATM no constituyan un riesgo inaceptable (como en el Capítulo de la Gestión de riesgos).

Personal y usuarios

- Extender la verificación de antecedentes a todos los empleados, incluidos los que se encuentran fuera de las zonas del aeropuerto
- Definir un plan de capacitación de seguridad
- Establecer conexiones con autoridades
- Implementar el desmantelamiento estricto de las cuentas y los derechos de los usuarios.

Identificación de eventos temidos

Personal y usuarios

Posición de trabajo del controlador

Posición de trabajo del controlador

Posición de trabajo del controlador

Posición de trabajo del controlador

Zonificación

Sistema de comunicación

Primario

Secundario

HW Bypass

INTERFASE

Red en tierra

Tx/Rx

Tx/Rx

Tx/Rx

Cobertura normal

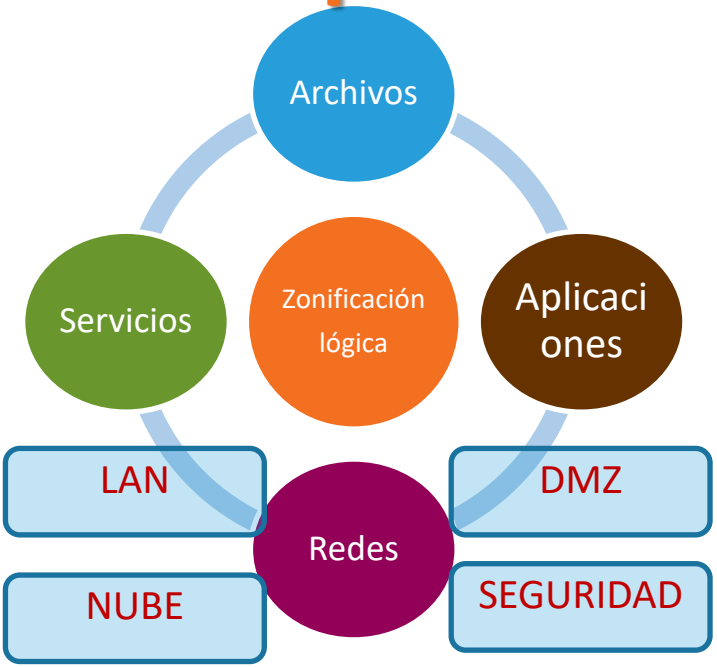
Cobertura emergencia

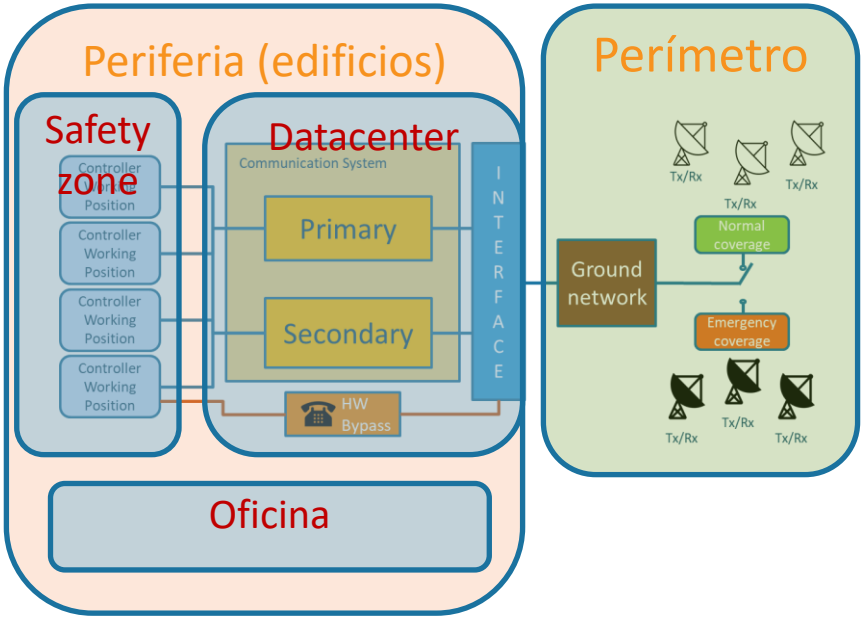
Tx/Rx

Tx/Rx

Tx/Rx

Verifique la coherencia de la zonificación





Control de acceso y seguridad física y del entorno

Requisito ATMSP-019-01:

La seguridad física ATM debe salvaguardar TI, OT, IACS e infraestructura CNS/ATM, contra interferencia ilícita y acceso no autorizado.

Requisito ATMSP-020-01:

La seguridad física ATM debe identificar zonas que alberguen activos CNS/ATM de acuerdo con su criticidad en cuanto a seguridad operacional y operatividad.

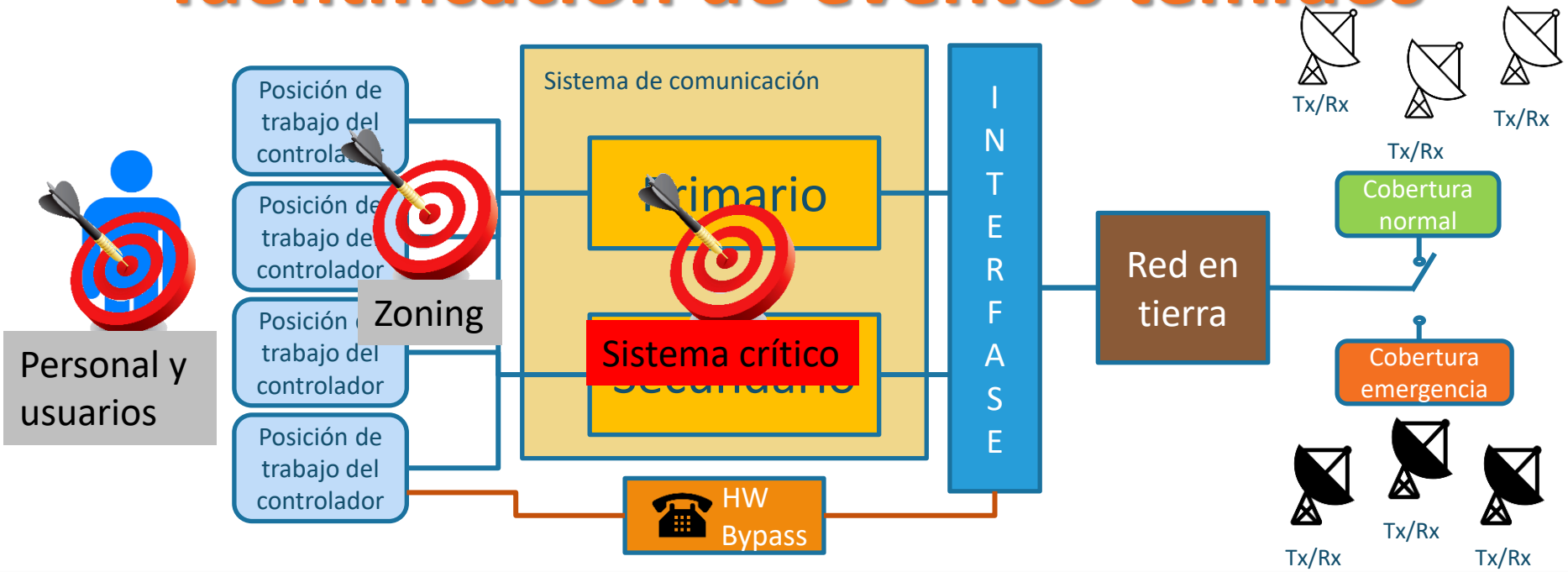
Control de acceso y seguridad física y del entorno

Requisito ATMSP-018-01:

Ingresar a cualquier activo ATM debe ser permitido bajo:

- Verificación de ausencia de riesgo inaceptable (como en el Capítulo 7 de Gestión de riesgos; en una base de necesidad de conocer).

Identificación de eventos temidos

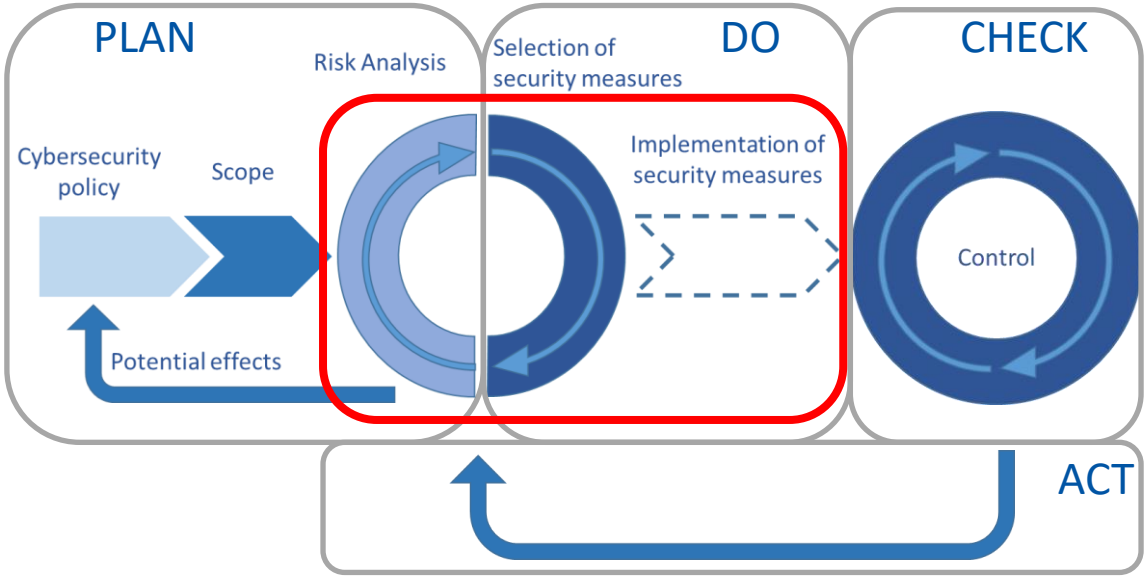


In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Gestión de riesgos en sistemas críticos

- Implementar mejores prácticas de seguridad (ISO 27002, NIST)
- Identificar, evaluar y reducir riesgos inaceptables
- **SOLAMENTE** aceptar riesgos residuales cuando se implementa el plan de mitigación



In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

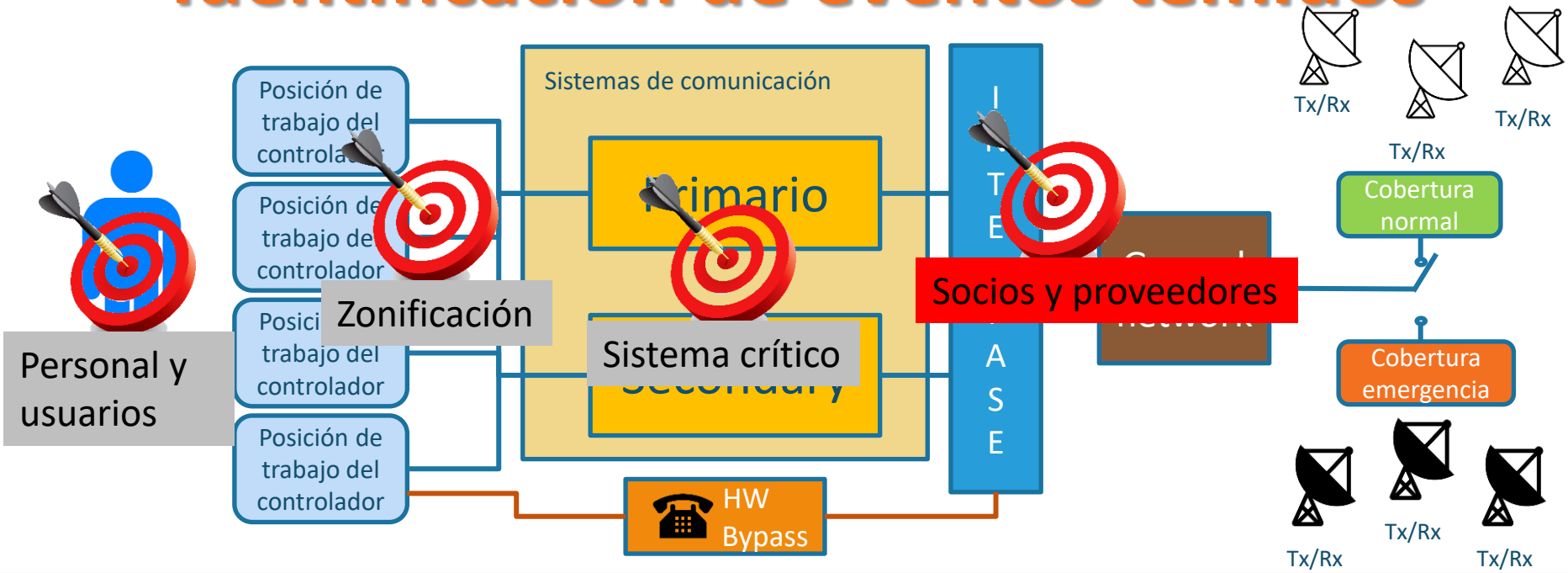
Gestión de riesgos de Ciberseguridad

Requisito ATMSP-006-01:

El enfoque basado en el Riesgo de seguridad ATM debe implementar medidas se seguridad técnica y operacional (políticas y procesos) para reducir el riesgo aun nivel aceptable sobre:

- (Intencional) ciberataque exitoso,
- Error humano,
- Accidente o incidente,
- Imparto por desastre natural.

Identificación de eventos temidos



In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Proveedores y socios

Requisito ATMSP-035-01:

La Ciberseguridad ATM debe proporcionar seguridad a socios de principio a fin en la cadena de suministro en el enfoque del sistema de gestión de la Ciberseguridad CNS/ATM.

Requisito ATMSP-036-01:

La Ciberseguridad ATM debe asegurar que relaciones con entidades externas no constituyan un riesgo inaceptable (como en el Capítulo 7 de la Gestión de riesgos).

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Proveedores y socios

- Asegúrese de incluir a **TODOS** sus proveedores y socios en el proceso de gestión de riesgos de Ciberseguridad
- Defina objetivos de seguridad a ser alcanzado en un proyecto, personas, entregables, interconexiones…
- Asegurar un estricto seguimiento al proceso de seguridad

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

¿Qué es lo que tiene?

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Conclusión

- **“El arte supremo de la guerra es someter al enemigo sin luchar.”** Sun Tzu – el arte de la guerra
- Gestione los riesgos y establezca controles de seguridad para disuadir y prevenir ciberataques.
- Esté preparado/a para reaccionar en caso de que se materialice el riesgo de seguridad cibernética.:
  - Plan de continuidad del negocio
  - Gestión de incidentes y crisis

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Gracias por su atención

Preguntas y respuestas

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!