
ORGANIZACIÓN DE
AVIACIÓN CIVIL
INTERNACIONAL

Ciberseguridad en los servicios de navegación aérea

Amenazas, Estándares, Resiliencia

Informe Técnico y Operativo para los proveedores de servicios de navegación aérea

Mayda Alicia Ávila
Oficial Regional de Comunicaciones, Navegación y Vigilancia (CNS)
Oficina Regional de la Organización de Aviación Civil Internacional de América del Norte, Centroamérica y el Caribe

Por qué los Servicios de Navegación Aérea son un objetivo

- La digitalización y la interconexión en la gestión del tráfico aéreo han ampliado la exposición de los servicios de navegación aérea al riesgo cibernético.
- Los impactos van desde retrasos menores hasta una pérdida catastrófica de seguridad, protección y continuidad del servicio.
- La suposición largamente sostenida de redes aisladas y especializadas ya no se sostiene mientras los sistemas de nueva generación se interconectan. La aviación ha visto incidentes, pero ningún evento cibernético realmente disruptivo, un récord que puede deber tanto a la suerte como al diseño.

Normas y resoluciones

- La respuesta de la OACI se ha desarrollado durante más de dos décadas: Manual de Seguridad ATM Doc 9985 (2013), luego el primer estándar de ciberseguridad en el Anexo 17 (2016).

- La Resolución de la Asamblea A39-19 reconoció la ciberseguridad como núcleo de la aviación civil. La A40-19 presentó la Estrategia de Ciberseguridad de la Aviación y instó a la adopción del Convenio y Protocolo de Pekín.

- La A41-19 insta a los Estados a implementar el Plan de Acción de Ciberseguridad y designar una autoridad competente en ciberseguridad.

Asamblea de la OACI	Resolución	Año	Título / Importancia principal
39.ª Asamblea	**A39-19**	2016	**Abordando la ciberseguridad en la aviación civil** — Primera Resolución de la Asamblea de la OACI dedicada específicamente a la ciberseguridad, estableciéndola como una **prioridad mundial para la aviación civil**.
40.ª Asamblea	**A40-10**	2019	**Abordando la ciberseguridad en la aviación civil** — Sustituyó a la A39-19. Fortaleció el marco mundial y exhortó a la implementación de la **Estrategia de Ciberseguridad de la Aviación de la OACI** y al desarrollo del **Plan de Acción de Ciberseguridad (CyAP)**.
41.ª Asamblea	**A41-19**	2022	**Abordando la ciberseguridad en la aviación civil** — Sustituyó a la A40-10. Reforzó la **gobernanza, la cooperación, la gestión de riesgos, la cultura de ciberseguridad**, la implementación de la Estrategia/CyAP y la adopción de los **instrumentos jurídicos de Beijing**.
42.ª Asamblea	**A42-19**	2025	**Abordando la ciberseguridad en la aviación civil — Resolución vigente/más reciente**, que sustituye a la A41-19. Continúa el enfoque holístico de la OACI, vinculando la ciberseguridad con la **seguridad operacional (safety), la seguridad de la aviación (security) y la eficiencia**, y hace énfasis en la **gobernanza, la cooperación internacional y la implementación**.

La Estrategia de Ciberseguridad de la OACI

Cooperación internacional

- Los Estados, los ANSP y la industria deben compartir información, armonizar la regulación y coordinar la respuesta.
- La coordinación civil-militar y los marcos de confianza son esenciales.

Política de gobernanza y ciberseguridad

- Los Estados deben asignar una responsabilidad clara sobre la ciberseguridad de la aviación a través de una autoridad nacional competente.
- La ciberseguridad debe integrarse en los programas de seguridad y protección, gestionando el riesgo a lo largo de todo el ciclo de vida del sistema.

Legislación, regulación e intercambio de información

- Adoptar leyes que permitan la disuasión, investigación y enjuiciamiento de ciberataques; utilizar plataformas de confianza y el Protocolo de Semáforo para la divulgación.
- Gestión de incidentes y fortalecimiento de capacidades: planes de contingencia escalables, ejercicios cibernéticos en vivo, formación y una cultura de ciberseguridad sustentan la ejecución a través del Plan de Acción en Ciberseguridad.

Anexo 17 y Documento 9985

Standard 4.9.1

- Las entidades bajo el programa nacional de seguridad de la aviación civil deben identificar sistemas y datos críticos de TIC y protegerlos en base a la gestión de riesgos.
- La Práctica Recomendada 4.9.2 aborda la confidencialidad, integridad y disponibilidad a través de la seguridad desde el diseño, la seguridad de la cadena de suministro, la separación de redes y el acceso remoto controlado.
- El Doc 9985 extiende esto a las instalaciones ATS y a la infraestructura CNS — personas, procedimientos, información, instalaciones y equipos.

Los Estándares

- ISO/IEC 27001 establece los requisitos para un sistema de gestión de seguridad de la información y es el núcleo certificado de la serie, apoyado por controles 27002, gestión de riesgos 27005, preparación TIC para continuidad de negocio, seguridad de red 27033 y gestión de incidentes 27035.
- La ISO 31000 proporciona el marco genérico de riesgos y la IEC 62443 cubre los sistemas de control industrial.
- La evidencia de certificación también respalda las auditorías de la CMA de USOAP y las obligaciones de los Anexos 17 y 19.

Evaluación de ciberseguridad basada en:

- Plan de Acción de Ciberseguridad de la OACI
- Guía de Política de Ciberseguridad de la OACI
- Documento 8973 de la OACI "Manual de Seguridad Aérea"
- ICAO-CANSO-AIRBUS "Plantilla de Política de Ciberseguridad en Gestión del Tráfico Aéreo"
- Anexo 17, 19 de la OACI
- Guía de Evaluación de Riesgos de Ciberseguridad de CANSO
- Documento OACI 10213 Codirecciones Globales de Riesgos Cibernéticos
- ACI - Manual de Ejecutivos de Ciberseguridad para Aeropuertos
- Normas ISO 27000, 31000
- El NIST SP 800-30 es un Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST)
- EUROCAE (Organización Europea de Equipos de Aviación Civil) y RTCA "Guía sobre Ciberseguridad de la Aviación"

OACI

La superficie de ataque ATM

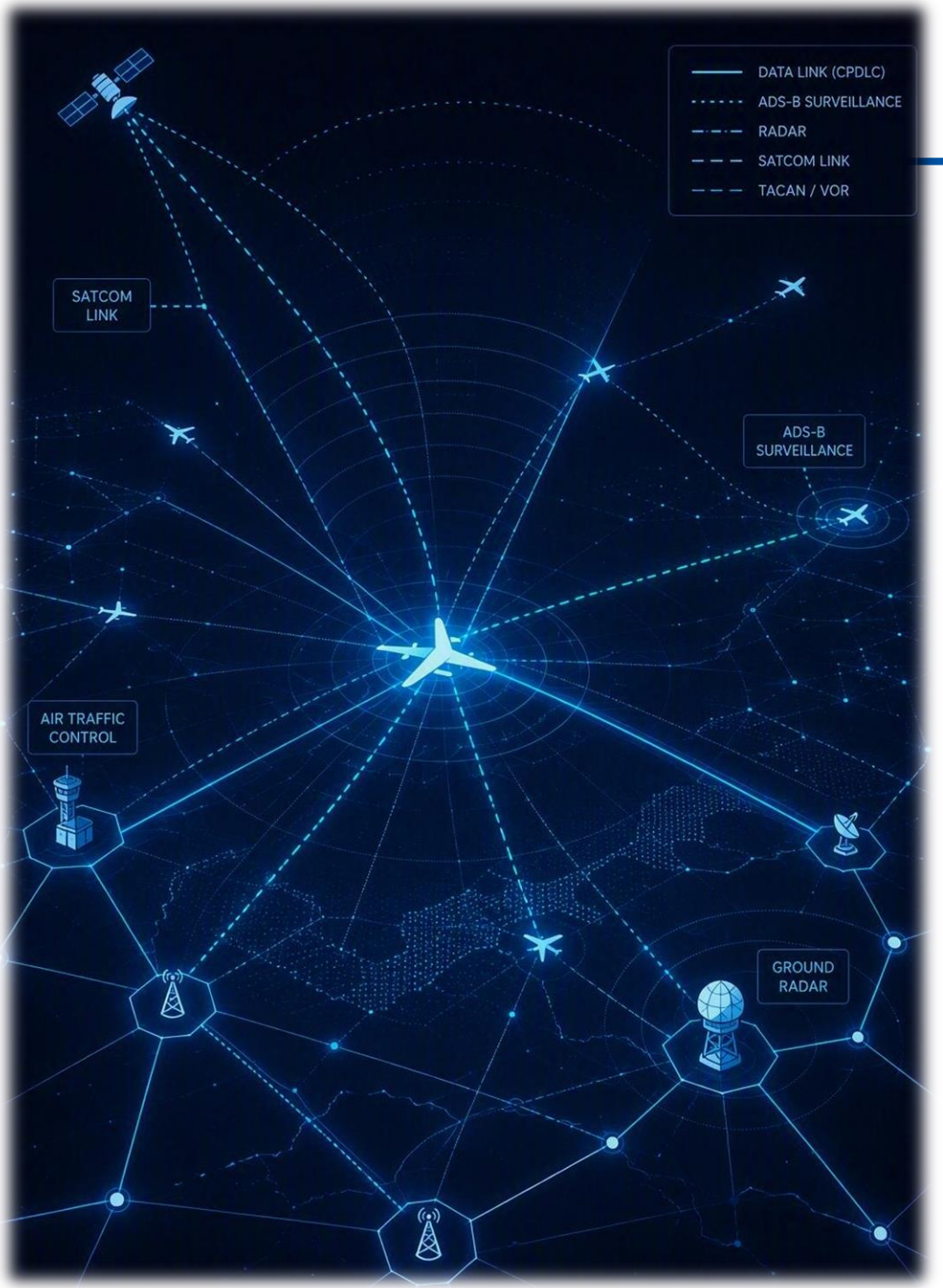
Vigilancia: ADS-B, multilateración y radar dependen de datos de difusión que pueden ser falsificados o interferidos.

Navegación: interferencia y suplantación GNSS, mitigada mediante redes operativas mínimas VOR/DME y monitorización de integridad SBAS/GBAS.

Comunicaciones: enlaces CPDLC, VHF y SATCOM, además de redes regionales de datos ATM como MEVA, REDDIG y CANSNET.

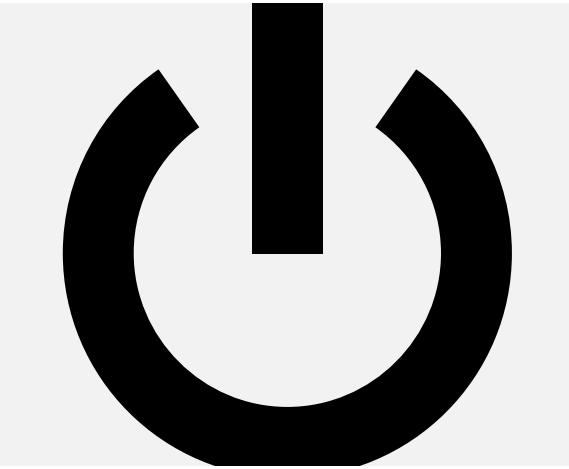
Sistemas de información: AIM, FF-ICE, MET y datos del plan de vuelo expuestos a alteraciones y acceso no autorizado.

Infraestructura y socios: TI, OT y sistemas de control industrial, junto con toda interconexión con partes interesadas externas.



OACI

Panorama de amenazas para ATM (Doc 10213)



Disponibilidad

- Ransomware.
- Denegación de servicio distribuida.
- Degradación de la energía y el sistema HVAC.
- Pérdida de conectividad IP.

Integridad

- Datos falsificados de MET, plan de vuelo y vigilancia.
- Suplantación GNSS.

Confidencialidad

- Robo de propiedad intelectual y datos.
- Exfiltración de ransomware.

Evaluación del riesgo

Un proceso definido: ISO 31000 establece alcance, contexto y criterios, luego identificación, análisis, evaluación, tratamiento, seguimiento e informe.

Aplicado a ATM: **ISO**/IEC 27005 permite a los ANSP evaluar ataques de vigilancia, interferencias GNSS y denegación de servicio contra voz y datos del ATC.

Orientado por la inteligencia: La evaluación debe estar centrada en amenazas e integrarse en el ciclo de vida del sistema, en lugar de realizarse como un ejercicio periódico en papel.

Propiedad clara: Cada activo de los servicios de navegación aérea — datos, sistemas y personal — requiere un propietario definido responsable de su protección.

No hay un punto común de vulnerabilidad: Reflejar el principio de seguridad de que no hay un único punto de fallo en toda la arquitectura de seguridad.

La Biblioteca de Control Doc 9985

Nueve categorías de control

- dirección de políticas; organización, cultura y gestión; recursos humanos; seguridad física y medioambiental; operaciones TIC; mecanismos técnicos e infraestructuras; adquisición y desarrollo; supervisión y auditoría; y cumplimiento.

Protección de la disponibilidad

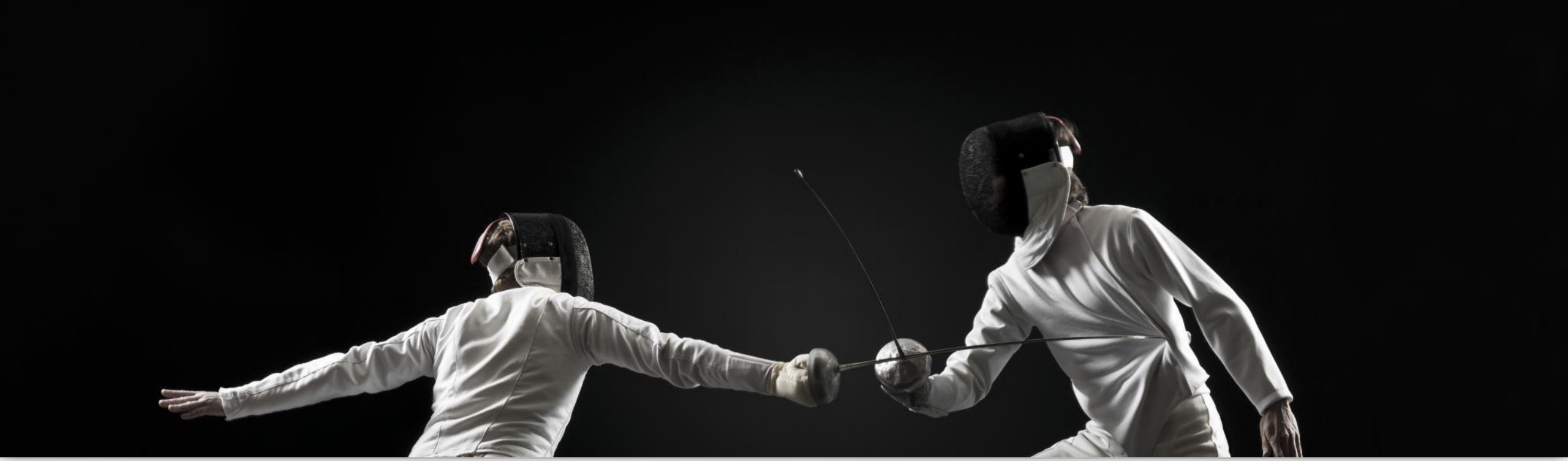
Un proceso de continuidad gestionado, acuerdos de nivel de servicio, monitorización de capacidad, copias de seguridad probadas y almacenamiento fuera del sitio.

Protección de la integridad

- Salvaguardas para los datos en tránsito frente a alteraciones, errores de enrutamiento y duplicación, reforzadas mediante comprobaciones de validación.

Protección de la confidencialidad

- Clasificación de información, acuerdos de confidencialidad, controles de enrutamiento y mecanismos de prevención de fugas.



Continuidad del negocio

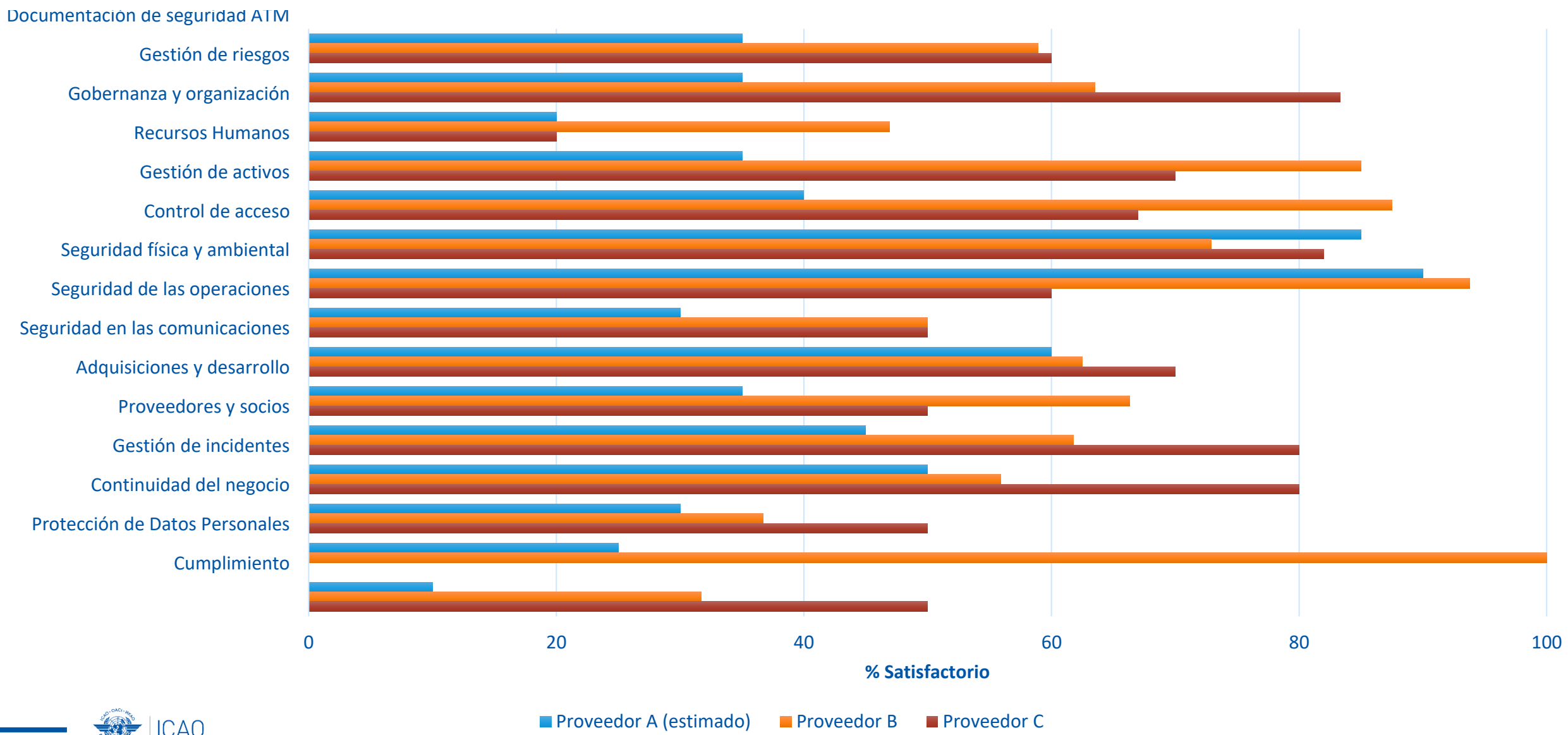
- Ninguna defensa es perfecta; el coste y los recursos limitan los sacrificios, por lo que un incidente sigue siendo posible.
- El Anexo 11 exige que las autoridades ATS preparen y promulguen planes de contingencia coordinados con los FIR adyacentes.
- Planificar la recuperación en el sitio, la recuperación del sistema y la continuidad operativa según tiempos de recuperación definidos.

OACI

Autoevaluación

- La lista de verificación de ciberseguridad de la ANSP permite a un proveedor evaluarse a sí mismo según la Plantilla de Política de Ciberseguridad de los Servicios de Navegación Aérea en quince dominios.
- Los dominios van desde la documentación, la gestión de riesgos y la gobernanza hasta el control de acceso, la seguridad física del CNS/ATM, operaciones, proveedores, gestión de incidentes y continuidad del negocio hasta el cumplimiento normativo.
- El alcance cubre unidades TWR, APP y ACC, infraestructura CNS y sistemas digitales AIM y MET, con cada elemento asignado a las cláusulas ISO/IEC 27001:2022.

Resultados de la evaluación entre tres proveedores



El proveedor A fue evaluado cualitativamente; sus valores se estiman a partir de hallazgos narrativos. Madurez global: Proveedor B 64,9%, Proveedor C aproximadamente 58%.

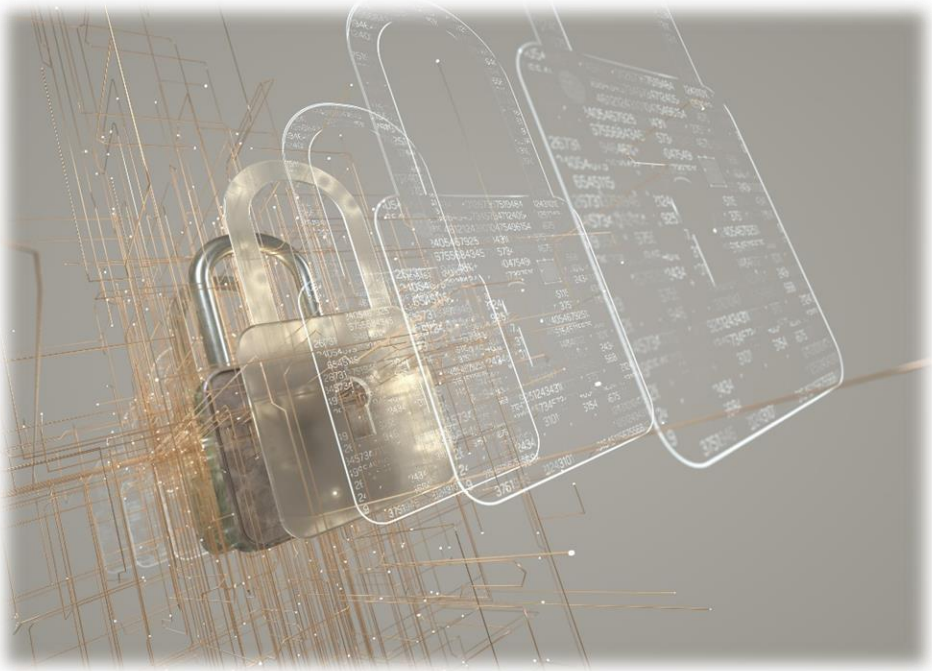
Fortalezas

- Control de acceso bien gestionado a través de las capas física, lógica y administrativa
- Seguridad física y ambiental robusta de las instalaciones CNS/ATM
- Segmentación de redes IT/OT y zonas de confianza implementadas de forma efectiva
- Prácticas de gestión de activos y recursos humanos generalmente establecidas
- Ciberseguridad incluida en la incorporación del personal y en la comunicación rutinaria de sensibilización

Debilidades

- No hay un marco formal de gobernanza de ciberseguridad ni una responsabilidad individual definida
- Brechas de seguridad en operaciones: no hay monitorización continua, gestión de vulnerabilidades o parches
- Continuidad del negocio no vinculada al riesgo cibernético; sin BIA, copias de seguridad sin probar, sin ejercicios
- El cumplimiento y la auditoría independiente son el dominio más débil entre los tres proveedores
- Seguridad de proveedores y terceros no gestionada formalmente ni auditada
- Inventarios incompletos de activos, especialmente en OT y sitios remotos

Gobernanza y próximos pasos



La Plantilla de Política de Ciberseguridad de los servicios de navegacoón aérea, desarrollada por la OACI NACC junto con CANSO y Airbus, insta a los proveedores a establecer un ***sistema de gestión basado en riesgos*** *con compromiso de la alta dirección, roles claros y supervisión estatal independiente del proveedor.*

Para el personal de ATM, los siguientes pasos son prácticos: ***ejecutar la lista de comprobación, priorizar las lagunas por riesgo, poner en práctica los planes de contingencia y unirse a mecanismos de intercambio de información de confianza****.*

Gracias

OACI