



**INTERNATIONAL
CIVIL AVIATION
ORGANIZATION**



Taller Regional sobre Redes Mínimas Operativas (MON) y Resiliencia GNSS

Estrategias para la continuidad de las operaciones en la Región SAM

13 al 17 de julio de 2026,
Oficina Regional SAM

Sesión de Apertura:
Análisis Estratégico e Institucional



ICAO

GLOBAL STRATEGIC

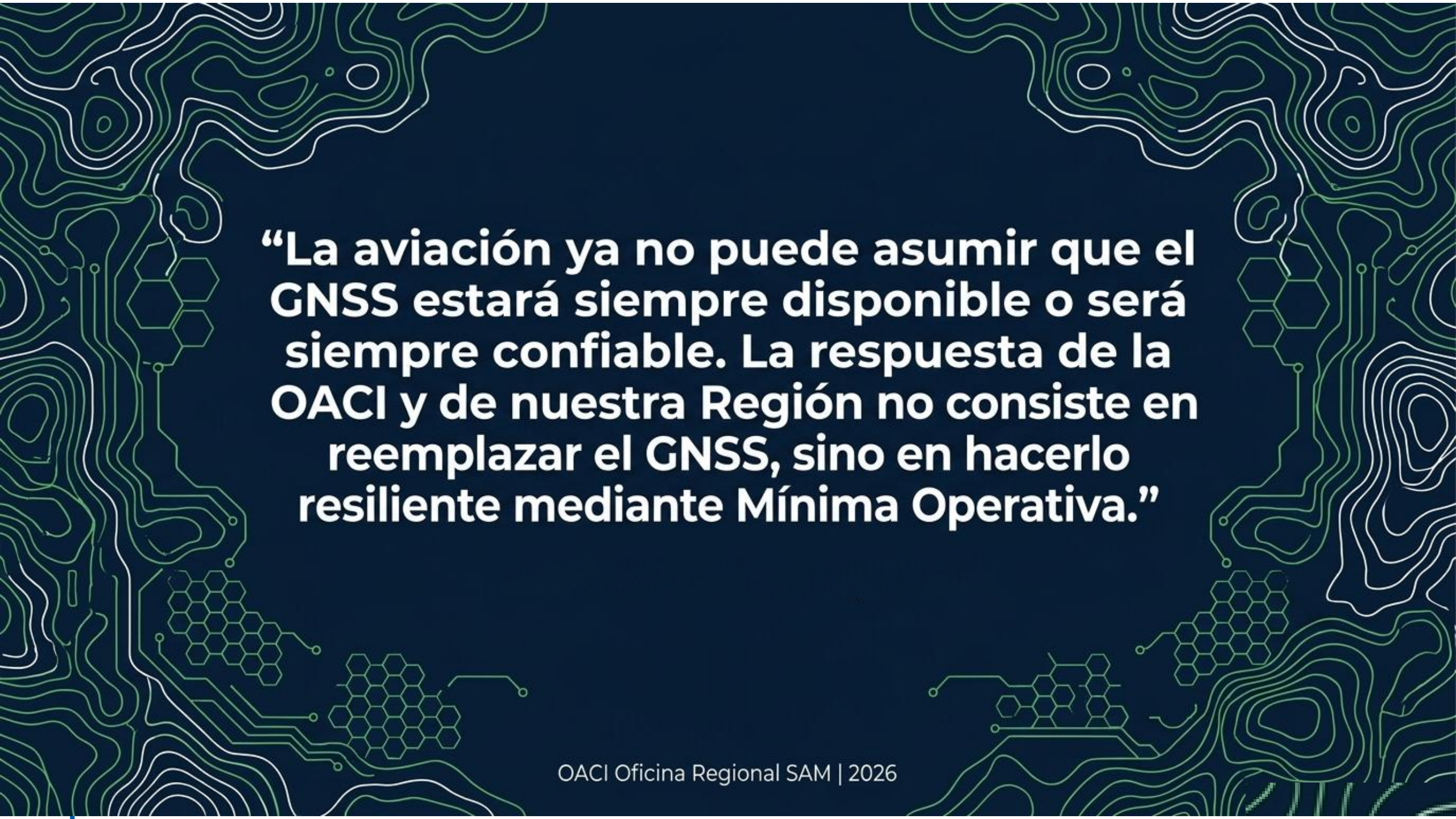
GLOBAL TECHNICAL

REGIONAL

NATIONAL



Schedule



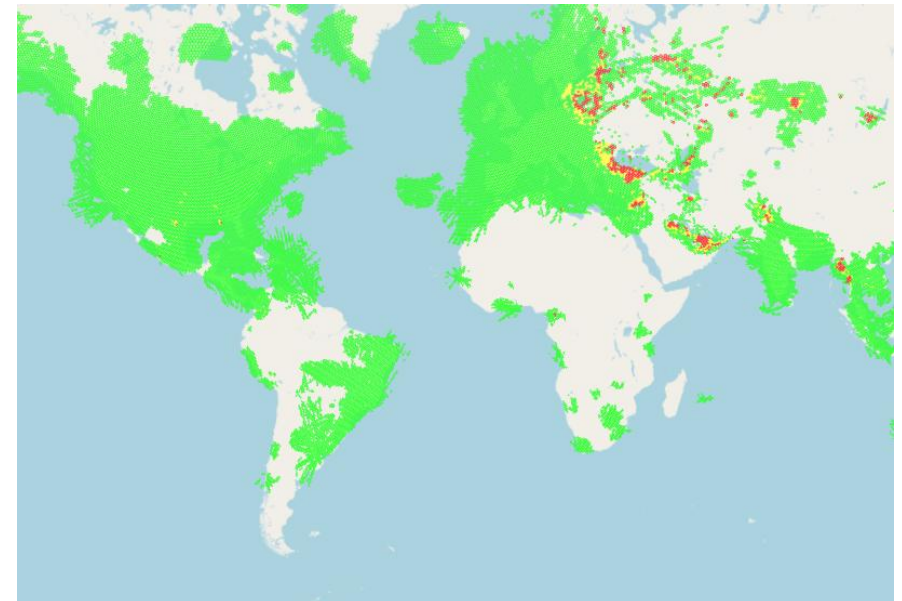
“La aviación ya no puede asumir que el GNSS estará siempre disponible o será siempre confiable. La respuesta de la OACI y de nuestra Región no consiste en reemplazar el GNSS, sino en hacerlo resiliente mediante Mínima Operativa.”



Objetivo

👉 La reunión tiene como objetivo intercambiar experiencias y coordinar acciones regionales relacionadas con la implementación de Redes Mínimas Operativas (MON) y el fortalecimiento de la resiliencia de los sistemas CNS/ATM ante posibles degradaciones o interrupciones de los servicios GNSS.

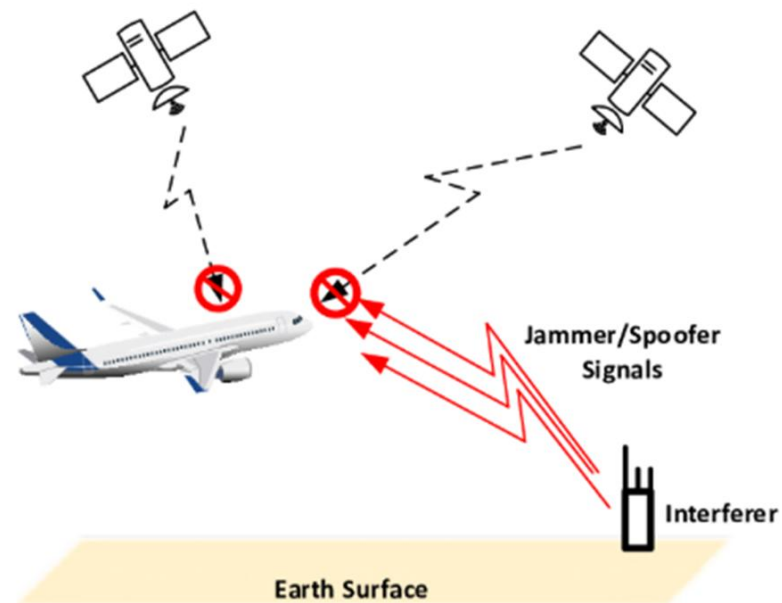
<https://www.icao.int/nacc/meetingdocs?fid=7352>



REPASO DE CONCEPTOS

👉 **Jamming** (Interferencia)

El jamming consiste en la transmisión deliberada o accidental de señales de radio que bloquean o degradan la recepción de las señales GNSS.



¿Qué ocurre?

7

El receptor GPS/GNSS deja de recibir correctamente las señales de los satélites. La potencia de la señal GNSS es extremadamente baja cuando llega a la Tierra (del orden de -160 dBW), por lo que basta una señal interferente relativamente pequeña para inutilizarla.

Efectos

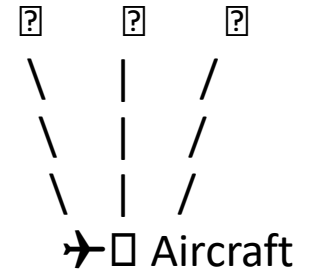
- Pérdida de posición.
- Pérdida de navegación RNAV/RNP.
- Desconexión de funciones dependientes del GNSS.
- Pérdida de sincronización temporal en algunos sistemas.

En una aeronave puede aparecer:

- ☐ GPS PRIMARY LOST
- ☐ NAV ACCUR DOWN
- ☐ GRADEUNABLE RNP

Cambio automático a navegación inercial (IRS/INS) cuando está disponible.

GNSS



↑↑↑ Señal GNSS débil



Jammer terrestre

Ondas RF intensas

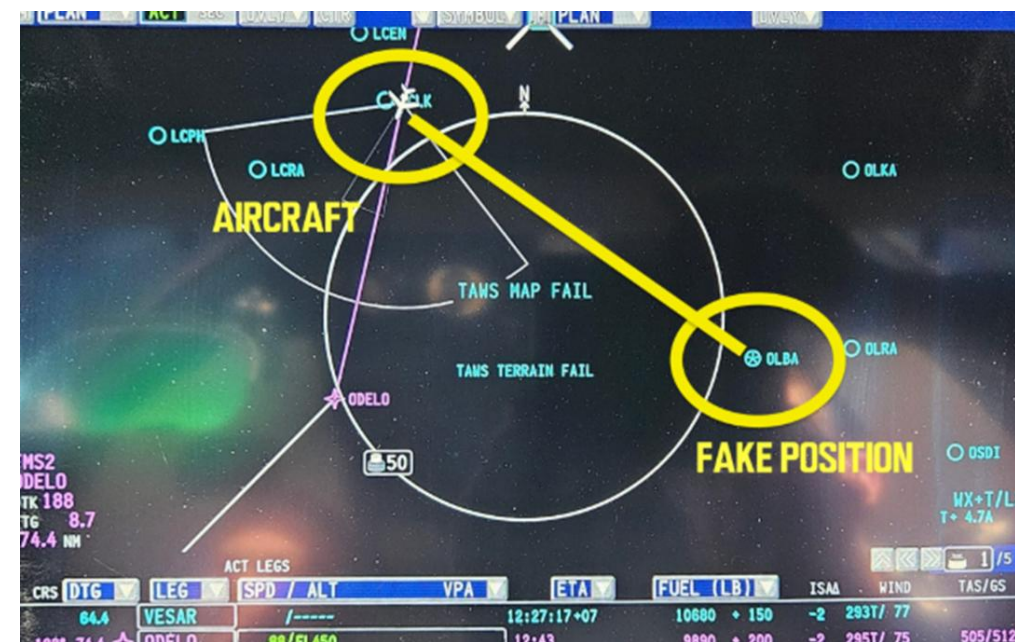
GPS PRIMARY LOST

Spoofing (Suplantación)

El spoofing es mucho más sofisticado.

No bloquea la señal.

En cambio, envía señales GNSS falsas, haciendo creer al receptor que está en otra posición o que el tiempo es diferente.



¿Qué ocurre?

9

El receptor sigue creyendo que recibe GPS.
Pero en realidad recibe una señal falsa.
Entonces calcula:

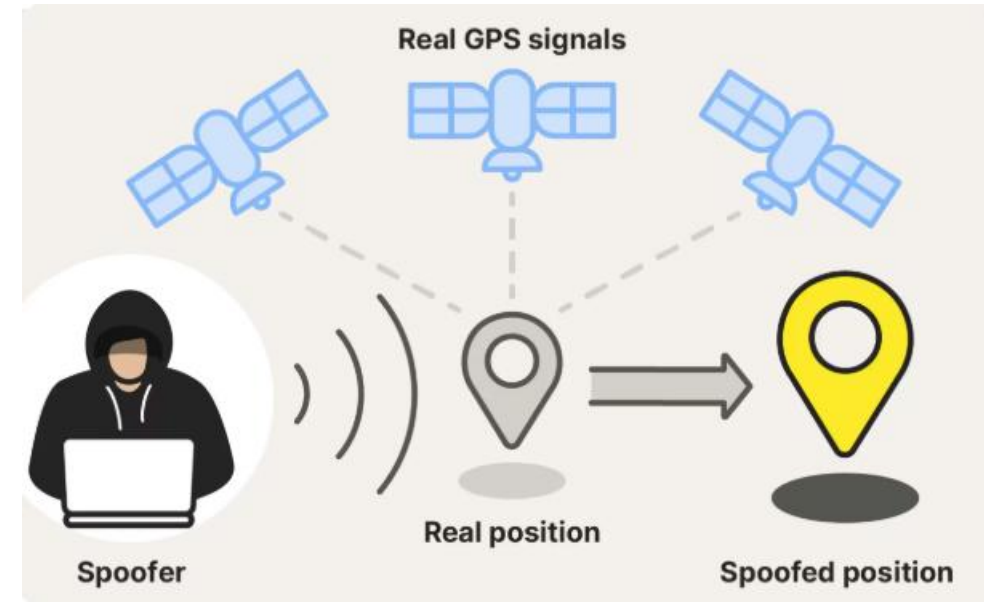
- una posición incorrecta,
- una velocidad incorrecta,
- un tiempo incorrecto.

Efectos

Puede provocar:

- ☐ desviaciones de la ruta,
- ☐ errores de navegación,
- ☐ indicaciones falsas en la cabina,
- ☐ problemas en procedimientos RNAV/RNP,
- ☐ errores en ADS-B Out si depende del GNSS.

En algunos casos el piloto no observa una pérdida del GPS, sino que el sistema continúa funcionando con datos incorrectos.



Meaconing

10

El **meaconing** es una técnica diferente tanto del **jamming** como del **spoofing**, aunque comparte algunas características con este último. En la práctica, puede considerarse una forma de engaño basada en **retransmitir señales auténticas** en lugar de generarlas artificialmente.



¿Qué es el meaconing?

Consiste en:

1. Capturar una señal GNSS auténtica proveniente de los satélites.
2. Retrasarla unos microsegundos o milisegundos.
3. Retransmitirla desde otro transmisor con mayor potencia que la señal original.

Como el receptor GNSS recibe primero la señal más fuerte, puede "creer" que esa señal retransmitida es la original y calcular una posición errónea.

A diferencia del spoofing, aquí **no se generan satélites falsos ni se sintetizan mensajes de navegación**; simplemente se reutilizan señales reales.



¿Por qué alguien usaría meaconing en lugar de spoofing?

12

En realidad, hoy **casi siempre es preferible el spoofing**.

Las razones son:

- el spoofing permite controlar completamente la posición falsa;
- puede modificar velocidad, tiempo y trayectoria;
- puede simular constelaciones completas de satélites.

El meaconing tiene limitaciones importantes:

- sólo retransmite señales reales;
- el error que puede introducir es más limitado;
- resulta más sencillo de detectar mediante técnicas modernas de autenticación y análisis de coherencia.

Por ello, muchos especialistas consideran al meaconing como un **precursor histórico** del spoofing moderno.



JAMMING

(Interferencia)

Transmisión de señales que bloquean o degradan las señales GNSS.

Satélites GNSS



EFFECTO:

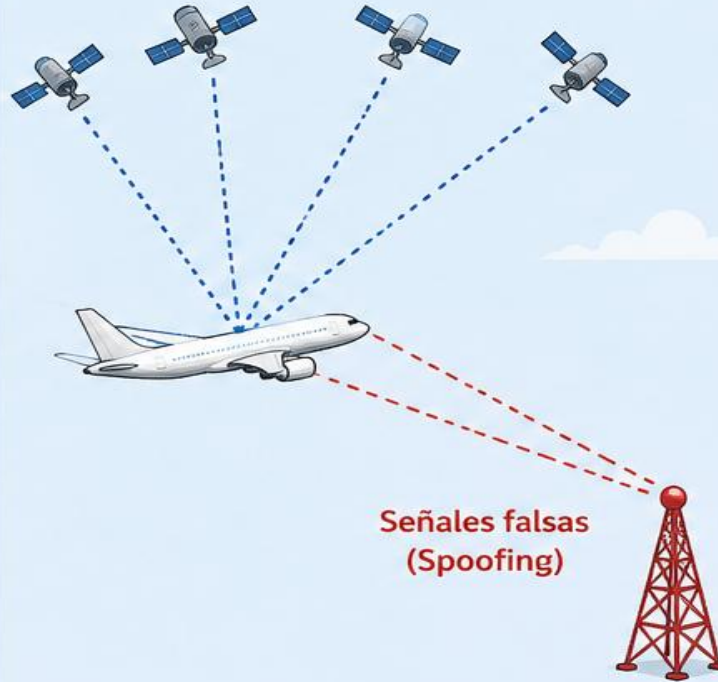
El receptor pierde o degrada la recepción GNSS. Puede aparecer pérdida de posición y navegación.

SPOOFING

(Suplantación)

Transmisión de señales GNSS falsas que engañan al receptor haciéndole creer que está en otra posición o tiempo.

Satélites GNSS



EFFECTO:

El receptor recibe señales falsas como si fueran reales. Produce posición, velocidad y tiempo incorrectos sin que el sistema lo detecte inmediatamente.

MEACONING

(Retransmisión)

Captura de señales GNSS auténticas, retrasadas y retransmitidas para engañar al receptor.

Satélites GNSS



EFFECTO:

El receptor recibe la señal retrasada como si fuera real. Genera errores en la posición y en el tiempo sin pérdida de señal.

¿Cómo lo detectaría una aeronave?

Una aeronave moderna puede advertir anomalías comparando múltiples fuentes de navegación:

GNSS vs. INS/IRS: si la posición GNSS comienza a separarse de la posición inercial, aparece una discrepancia.

GNSS vs. DME/DME: la posición calculada por radioayudas terrestres puede no coincidir con la del GNSS.

GNSS vs. VOR/DME: diferencias significativas indican una posible anomalía.

Datos ATS: el radar secundario o ADS-B pueden mostrar inconsistencias respecto a la trayectoria prevista.



➤ ¿Cuál es más peligroso?

15

Desde el punto de vista operacional:

- **Jamming** suele ser más fácil de detectar porque el sistema avisa que perdió la señal GNSS.
- **Spoofing** puede ser más peligroso porque el sistema puede seguir mostrando información aparentemente válida, aunque sea incorrecta. Si no se detecta mediante procedimientos de verificación cruzada (INS, DME/DME, VOR, radar, ADS-B, etc.), la tripulación podría continuar navegando con una posición errónea.

☞ MON



GNSS Vulnerabilities and Emerging Threats

Radio Navigation Workshop for NAM and SAM Regions
Mexico City, Mexico, 2-4 September 2025

Gerhard BERZ
Head of Navigation
gerhard.berz@eurocontrol.int



31 AGO y 1 SET Workshop Preparatorio para la Conferencia Mundial de Radiocomunicaciones 2027

02 al 11 SET Flight Safety and Monitoring Panel (FSMP) Working Group 23 (WG/23) de la OACI

02 al 04 SET Taller Regional de Radionavegación

THE GOOD NEWS FIRST

Esta diapositiva no niega el problema. Aclara que el problema **NO** es el GPS.



1. NO ES UN PROBLEMA CON LOS SATÉLITES

“ Cuando hablamos de vulnerabilidades GNSS muchas veces se piensa inmediatamente que existe un problema con los satélites. Sin embargo, ese no es el caso. ”



2. LAS CONSTELACIONES FUNCIONAN CORRECTAMENTE

“ Las constelaciones GNSS funcionan correctamente. La disponibilidad de satélites continúa siendo elevada, los sistemas SBAS siguen evolucionando y nuevas tecnologías como DFMC o ARAIM incrementarán aún más la robustez. ”



Alta disponibilidad de satélites



Sistemas SBAS en evolución



Nuevas tecnologías: DFMC / ARAIM

3. ENTONCES, ¿DÓNDE ESTÁ REALMENTE EL PROBLEMA?



El problema está en la **señal** que llega al usuario. Esa señal puede ser interferida deliberadamente mediante **jamming** o manipulada mediante **spoofing**.



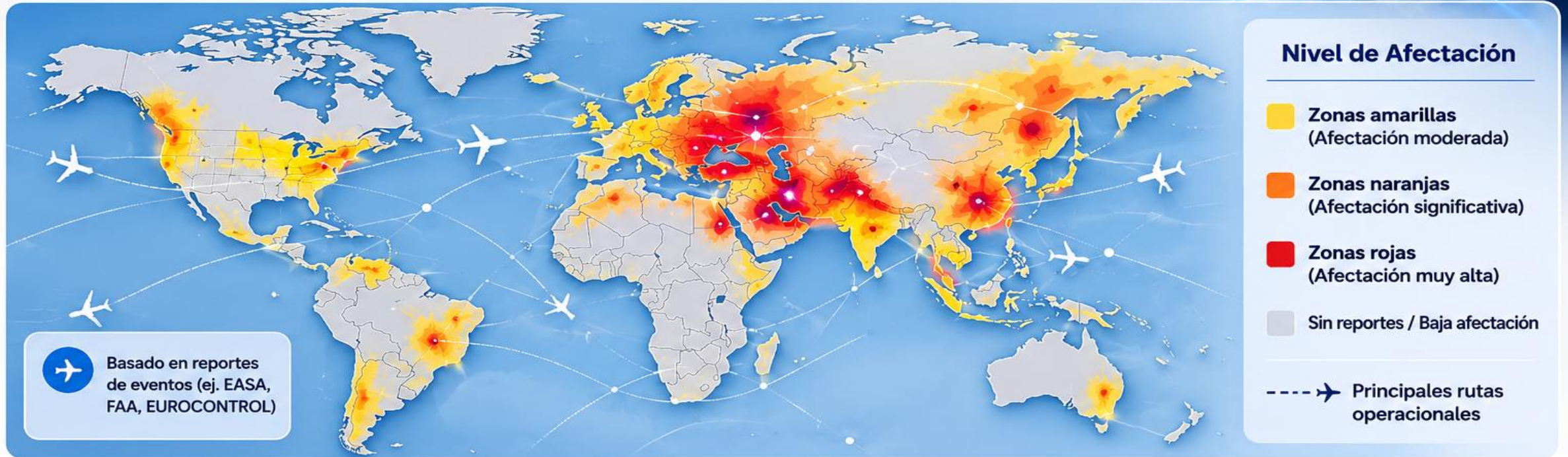
JAMMING



SPOOFING

GNSS INTERFERENCE SUMMARY

“Hace apenas algunos años estos eventos eran considerados excepcionales. Hoy forman parte de la **operación diaria** en diversas regiones del mundo.



Tipos de Interferencia



SPOOFING

- Señales falsas que engañan al receptor.
- Puede alterar la posición reportada.
- Riesgo: desviación de ruta, datos corruptos.



JAMMING

- Interferencia que bloquea la señal GNSS.
- Pérdida total o parcial de la recepción.
- Resultado: degradación de navegación.



Conclusiones Clave



“Observamos que una proporción significativa de vuelos experimenta eventos de interferencia GNSS. En algunos corredores regionales europeos la afectación alcanza valores muy elevados.”



“Este fenómeno dejó de ser un problema local para convertirse en un **desafío internacional.**”



¿QUÉ ES EVAIR REPORTS?

EVAIR (European Visualisation of ATM Incident Reports) es una plataforma desarrollada por Eurocontrol que recopila y consolida reportes de incidentes relacionados con navegación aérea en Europa.



Recopila reportes de ANSP y aerolíneas de toda Europa.



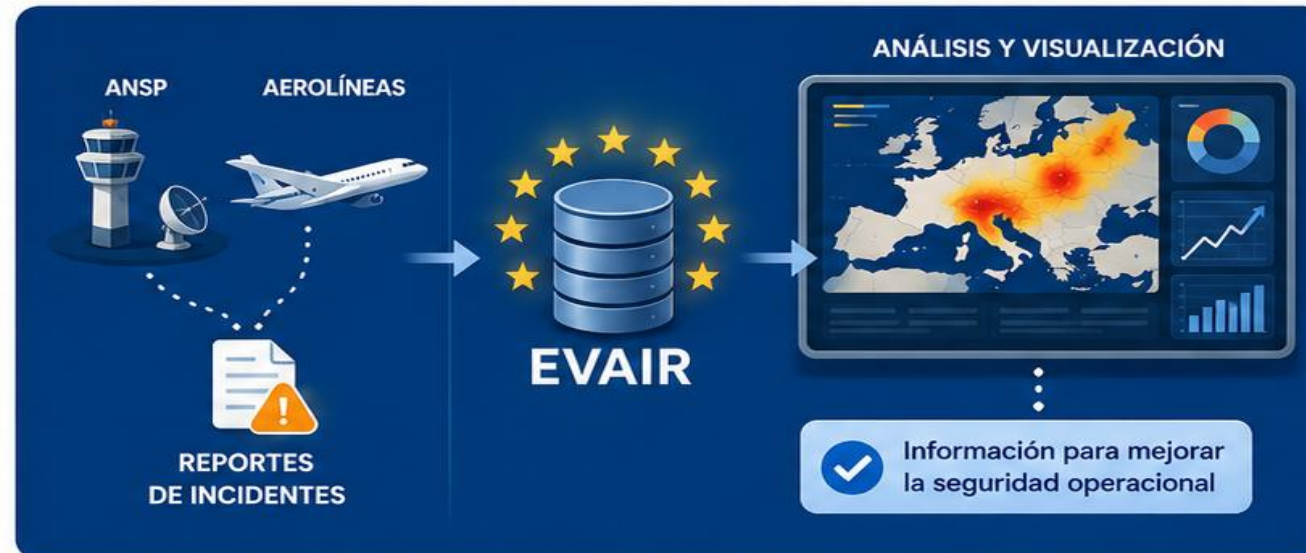
Normaliza y valida la información para asegurar calidad.



Permite visualizar tendencias, patrones y áreas de riesgo.



Apoya la toma de decisiones y la mejora de la seguridad operacional.



1. TODA ESTA INFORMACIÓN PROVIENE DE LOS SISTEMAS EUROPEOS DE REPORTE DE INCIDENTES.



“ Toda esta información proviene de los sistemas europeos de reporte de incidentes. ”

2. LO MÁS RELEVANTE NO ES SOLAMENTE LA CANTIDAD DE EVENTOS REPORTADOS, SINO LA TENDENCIA.



“ Lo más relevante no es solamente la cantidad de eventos reportados, sino la tendencia. ”

3. LOS ANSP Y LAS AEROLÍNEAS RECIBEN TANTOS EVENTOS QUE INCLUSO LA GESTIÓN DE ESOS REPORTES COMIENZA A CONVERTIRSE EN UNA CARGA OPERACIONAL.



“ Los ANSP y las aerolíneas reciben tantos eventos que incluso la gestión de esos reportes comienza a convertirse en una carga operacional. ”

4. ESTO DEMUESTRA LA NECESIDAD DE DESARROLLAR MÉTODOS AUTOMÁTICOS DE DETECCIÓN.



“ Esto demuestra la necesidad de desarrollar métodos automáticos de detección. ”

5. Y ESO ENLAZA PERFECTAMENTE CON LA SIGUIENTE SLIDE.



“ Y eso enlaza perfectamente con la siguiente slide. ”



MONITOREO UTILIZANDO ADS-B



¿PREGUNTA

¿Cómo detectamos interferencias GNSS si el propio GNSS está siendo afectado?

✓ RESPUESTA

Una posibilidad consiste en utilizar la información ADS-B.

UTILIZAR ADS-B PARA DETECTAR INTERFERENCIAS GNSS



¿CÓMO FUNCIONA SHERLOCK?

- Recopilación continua de datos ADS-B de miles de vuelos.
- Análisis de parámetros de navegación (p. ej. posición, altitud, velocidad) y su coherencia.
- Detección de anomalías compatibles con interferencias GNSS (jamming o spoofing).
- Visualización en mapas y reportes para situational awareness.



EUROCONTROL desarrolló una plataforma denominada **SHERLOCK** que analiza continuamente los datos ADS-B para identificar anomalías compatibles con interferencias GNSS.

EVOLUCIÓN DE LOS EVENTOS DETECTADOS MEDIANTE ADS-B

2018 – 2022



Los eventos comenzaron a formar parte de la operación diaria.

2023 – 2024



El **spoofing** se volvió considerablemente más sofisticado.

CONCLUSIÓN



Es un cambio cualitativo, no solamente cuantitativo.



El monitoreo basado en ADS-B permite mantener la conciencia situacional incluso cuando el GNSS está comprometido, aportando inteligencia clave para la seguridad operacional.

El riesgo operacional puede mantenerse incluso muy lejos del origen de la interferencia.



1. Uno de los errores más frecuentes consiste en pensar que una vez que la aeronave abandona el área interferida el problema desaparece.



2. Este estudio demuestra exactamente lo contrario.



3. Algunas aeronaves continúan degradadas durante cientos de millas.

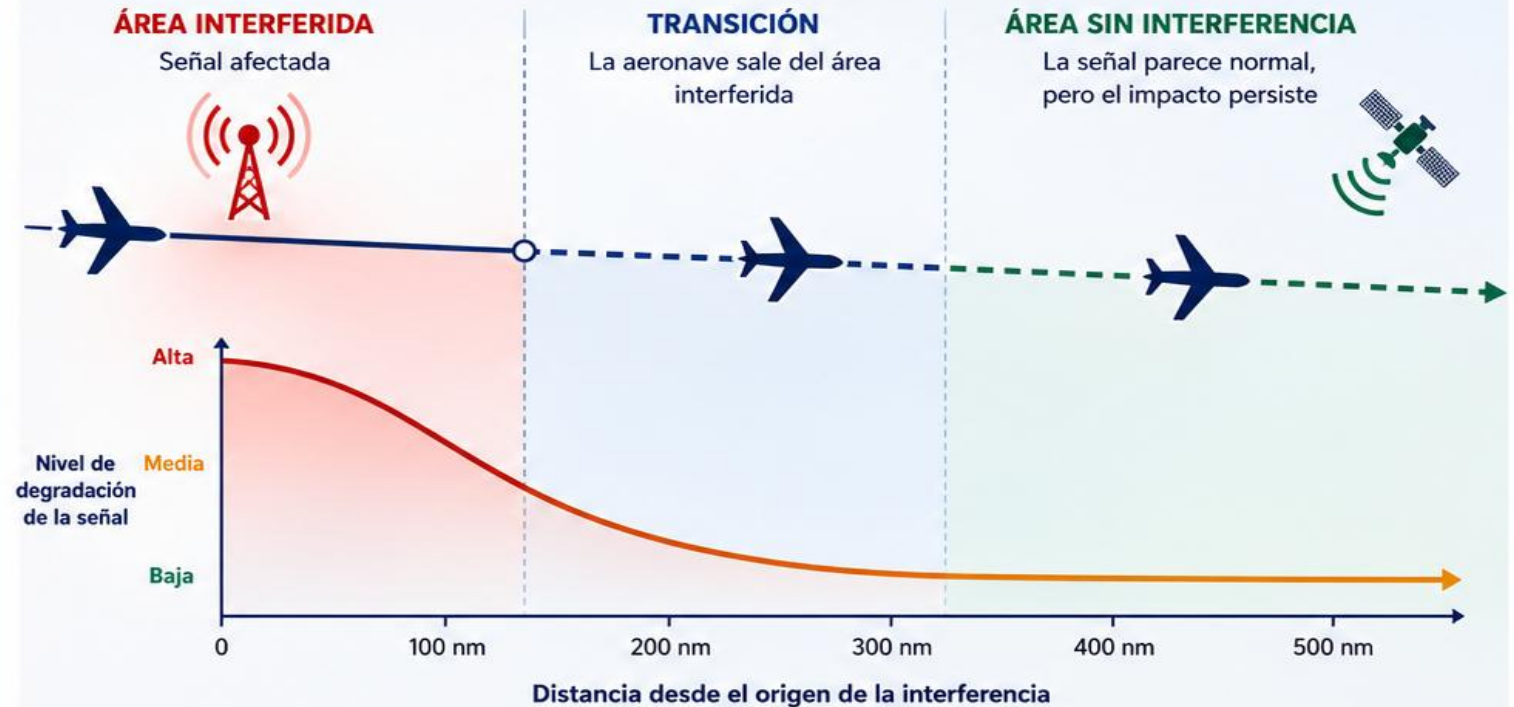


4. Esto significa que el riesgo operacional puede mantenerse incluso muy lejos del origen de la interferencia.



5. Por eso hablamos de resiliencia y no solamente de protección.

DEGRADACIÓN DE AERONAVES DESPUÉS DE ABANDONAR EL ÁREA INTERFERIDA



El impacto en los sistemas y en la navegación puede persistir mucho más allá del área afectada.



TRANSICIÓN:

Por eso, comprender este impacto persistente es el primer paso para construir sistemas y procedimientos más **resilientes**.



EJEMPLO REAL: PÉRDIDA DE GNSS DURANTE UNA APROXIMACIÓN

22

1 RESÚMELO

"Este es un ejemplo real ocurrido durante una aproximación."



2 DESPUÉS

"Una simple pérdida de GNSS terminó afectando múltiples sistemas de la aeronave."



3 NOMBRAS

- AHRS
- TAWS
- ADS-B
- navegación



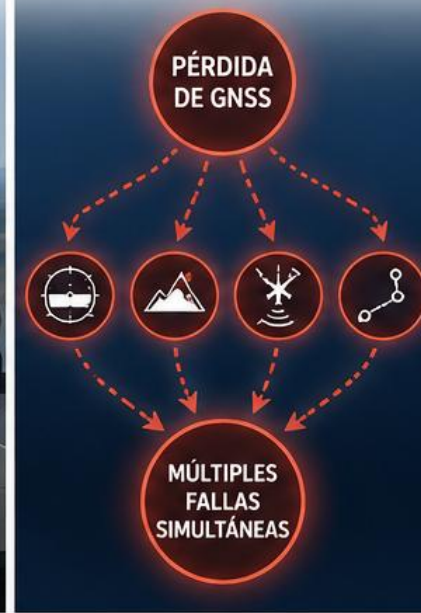
4 LUEGO

"La tripulación necesitó asistencia radar para completar la aproximación."



5 FINALMENTE

"Este ejemplo demuestra cómo un único evento puede desencadenar múltiples fallas simultáneas."



SISTEMAS AFECTADOS



AHRS



TAWS



ADS-B



NAVEGACIÓN



UN ÚNICO EVENTO PUEDE DESENCADENAR MÚLTIPLES FALLAS SIMULTÁNEAS.

El Efecto Cascada en la Cabina de Mando

**Falla del Receptor GPS /
Posición FMS Falsa**

Pérdida de ADS-B In/Out

**Falla del Reloj del
Sistema**

**Pérdida de Sistema de
Referencia de Actitud
(AHRS)**

**Pérdida de Visión Sintética
(SVS inop)**

**Falla de Radar
Meteorológico**

**Alertas Falsas de Proximidad
al Terreno
(TAWS / EGPWS)**

Consecuencia: Carga de trabajo extrema, fallas en cascada y necesidad de vectores de radar (ATC).

El Paradigma de la Vulnerabilidad GNSS



La Fortaleza

Constelación Robusta.

Más de dos décadas de diseño de sistemas de aumentación. Operación muy por encima de la constelación mínima.



La Fragilidad

Señal Vulnerable.

A pesar de una infraestructura espacial perfecta, la señal que llega a la aeronave es débil y susceptible a interferencias de radiofrecuencia (RFI) intencionales o accidentales desde tierra.

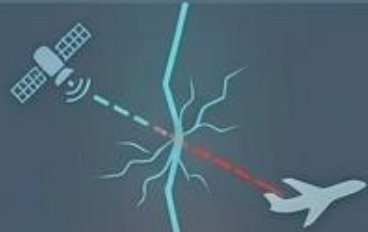
Una infraestructura satelital perfecta no garantiza la disponibilidad de la señal en cabina.

La Respuesta Global: El Marco de la OACI



La OACI no está creando un marco normativo desde cero. Está fortaleciendo los documentos existentes e incorporando requisitos diseñados específicamente para garantizar la resiliencia frente a interferencias GNSS.

El Cambio Estratégico: Hacia el C-PNT

	Visión Tradicional	Complementary PNT (C-PNT)
Enfoque: GNSS como fuente única e infalible.		Enfoque: Fusión Multi-Sensor (GNSS + INS + Terrestre + Tiempo Independiente). 
Arquitectura: Hilo único de dependencia.		Arquitectura: Red de seguridad redundante e independiente. 
Rol Convencional: Sistemas terrestres en vías de desmantelamiento total.		Rol Convencional: Infraestructura mantenida estratégicamente. 

Durante años pensamos en el GNSS como la única fuente.
Hoy, la resiliencia exige un ecosistema PNT complementario.

NAV RON: Resiliencia, no Retroceso



No significa volver atrás.

No es un abandono de la Navegación Basada en Prestaciones (PBN).



Seguro Operativo.

Es la construcción proactiva de una red de resiliencia.

“La infraestructura convencional deja de ser puramente redundante para convertirse en un elemento estratégico de continuidad operacional.”

El Puente Estratégico: Del Marco Global a la Realidad SAM



Hasta ahora hemos **analizado el problema y las directrices globales**. Sin embargo, las soluciones desarrolladas para un continente no pueden aplicarse mediante un simple copy-paste.

La Región SAM presenta desafíos operacionales radicalmente diferentes. Necesitamos una estrategia propia.

Geografía y Desafíos Específicos de la Región SAM



La Selva Amazónica.

Enormes extensiones donde la instalación, energía y mantenimiento terrestre presentan inmensos desafíos logísticos.



La Cordillera de los Andes.

Restricciones severas de orografía que limitan la línea de vista (LOS) y la cobertura de radioayudas convencionales.



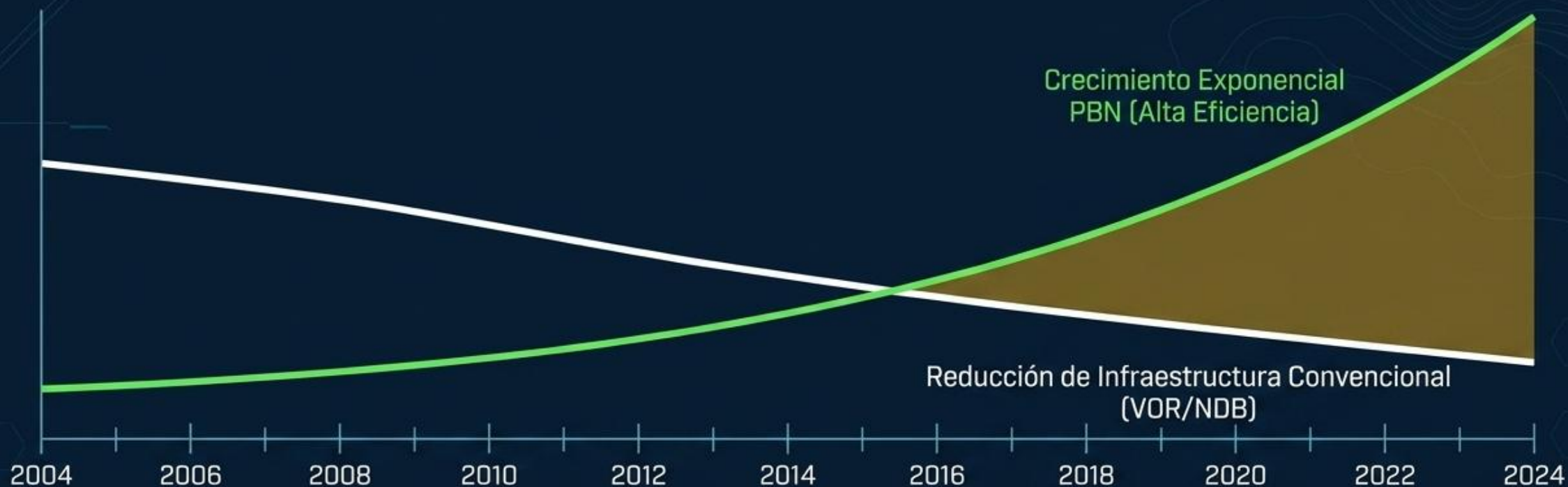
Espacio Oceánico.

Extensas FIRs oceánicas con nulas alternativas de navegación terrestre.



Una red terrestre densa (modelo europeo) es física y económicamente inviable en gran parte de nuestra geografía.

Dos Décadas de Evolución y Dependencia



Insight Box

La dependencia del GNSS no apareció de un día para otro. Fue una evolución tecnológica intencional de más de veinte años. Hoy, degradar el GNSS en SAM significa paralizar la aviación moderna a menos que contemos con una red de respaldo planificada.

La Solución: ¿Qué es la Red Mínima Operativa (MON)?

Una red de infraestructura de radionavegación terrestre, racionalizada y ubicada estratégicamente.

Cobertura Total Tradicional



Cobertura Redundante y Costosa

Red Mínima Operativa - MON



Rutas Estratégicas y Eficientes

1. Garantizar la Navegación.

Permitir a las aeronaves mantener una trayectoria segura en caso de pérdida total de GNSS.

2. Aterrizaje Seguro.

Asegurar aproximaciones instrumentales convencionales (ILS/VOR) en aeródromos estratégicos y de contingencia.

3. Eficiencia de Costos.

Evitar la reinstalación masiva de radioayudas, conservando solo lo estrictamente necesario.

El Ecosistema de Resiliencia Integral



Hoja de Ruta para la Región SAM



Thank You

