



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE GRADO

*Estudio de blindajes antijamming para antenas GNSS en buques
de la Armada*

Grado en Ingeniería Mecánica

ALUMNO: Marcos Muiño Martínez

DIRECTORES: José María Núñez Ortuño

CURSO ACADÉMICO: 2025-2026

Universida_{de}Vigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE GRADO

*Estudio de blindajes antijamming para antenas GNSS en buques
de la Armada*

Grado en Ingeniería Mecánica
Intensificación en Tecnología Naval
Cuerpo General

UniversidadeVigo

RESUMEN

En el actual escenario multidominio, la Guerra Electrónica de la Navegación (NAVWAR) ha convertido la denegación de los servicios GNSS mediante *jamming* y *spoofing* en una amenaza crítica para la operatividad y la seguridad marítima. Frente al elevado coste de las matrices de antenas activas (CRPA), este Trabajo de Fin de Grado diseña, simula y valida un sistema de apantallamiento electromagnético pasivo y de bajo coste basado en cavidades cilíndricas.

Mediante un modelado en MATLAB, se ha caracterizado la geometría circular, el fenómeno de la difracción de borde y su impacto en el diagrama de radiación de una antena de parche cerámico. Simultáneamente, se ha estudiado el efecto del blindaje sobre la precisión, derivado de la degradación de la Dilución de Precisión (PDOP).

Los resultados demuestran la viabilidad de un compromiso táctico óptimo, sin bloquear señales satelitales por encima de los 27°, el cilindro minimiza drásticamente las amenazas procedentes del horizonte con atenuaciones de hasta 10 dBi, al tiempo que preserva un PDOP operativo seguro (inferior a 6). Este trabajo concluye ofreciendo una contramedida pasiva, robusta y eficiente que garantiza la supervivencia del posicionamiento naval en entornos electromagnéticamente hostiles.

PALABRAS CLAVE

GNSS, *jamming*, *spoofing*, PDOP, Apantallamiento Pasivo

AGRADECIMIENTOS

En primer lugar, me gustaría agradecer a mi tutor del proyecto, por acompañarme durante todo este proceso. Quiero agradecer las aportaciones del CC Villalpando, así como dar las gracias a todos los oficiales de la flota a los que he molestado en su ajetreada agenda para pedir ayuda, Lydia, Carlos, David, muchas gracias.

No puedo olvidarme de mis amigos, siempre poniendo el listón alto. El ejemplo y motivación que sois no me permite quedarme atrás, vosotros sois mi motivación y apoyo diario. En especial a David Silva y Marck Evans, no os podía fallar.

El agradecimiento más especial solo podía ser para mi familia. A mi madre, por ser incansable, esforzándose y controlándome como si fuese tutora del propio proyecto. A mi padre, primer voluntario para ayudarme y sacar adelante el prototipo, que funcione es gracias a ti. Y a mi hermano y su ayuda desinteresada en que haga un mejor trabajo.

.

CONTENIDO

Contenido	1
Índice de Figuras	3
Índice de Tablas.....	5
1 Introducción y objetivos	7
1.1 Antecedentes	7
1.2 Motivación	7
1.3 Objetivos	8
1.4 Estructura del trabajo	9
2 Estado del arte	11
2.1 Sistemas GNSS	11
2.1.1 Historia y evolución de los sistemas GNSS	11
2.1.2 Fundamentos de los sistemas GNSS.....	12
2.1.3 Estructura y composición de la señal de navegación.....	15
2.1.4 Precisión del posicionamiento, factor geométrico (DOP) y multitrayecto	16
2.1.5 Importancia en el ámbito de la defensa, vulnerabilidades y uso en la Armada.....	19
2.2 Guerra Electrónica de la Navegación (NAVWAR).....	21
2.2.1 Interferencias intencionadas (Jamming)	21
2.2.2 Suplantación de identidad (Spoofing)	23
2.3 Técnicas de Protección Electrónica mediante Antenas Anti-Interferencia.....	25
2.3.1 Antenas de Patrón de Recepción Controlado (CRPA)	25
2.3.2 Antenas LENA.....	26
2.3.3 Antenas Choke Ring	27
2.3.4 Estructuras de Apantallamiento y Cavidades Resonantes	27
3 Desarrollo del TFG.....	29
3.1 Fundamentos Electromagnéticos del Apantallamiento Físico	29
3.1.1 Limitaciones electromagnéticas del apantallamiento	30
3.2 Software Empleado	31
3.2.1 Matlab	31
3.2.3 U-Center	32
3.3 Diseño y simulación computacional	32
3.3.1 Diseño de la antena GNSS.....	33
3.3.2 Dimensiones óptimas frente a protección.....	34
3.3.3 Efecto de la protección sobre el DOP	35

3.3.4 Diseño teórico de la cavidad.....	39
3.3.5 Comprobación teórica de la cavidad.....	40
3.3.6 Comparativa sólido frente a malla.....	41
3.4 Validación Experimental.....	42
3.4.1 Hardware.....	42
3.4.2 Diseño de la protección física.....	43
3.4.3 Comprobación de la precisión	45
3.4.4 Comprobación de la protección	47
4 Resultados	49
4.1 Resultados de diseño y simulación computacional.....	49
4.2 Resultados de la validación experimental.....	50
4.2.1 Resultados de la comprobación de la precisión	50
4.2.2 Resultados de la comprobación de protección.....	51
5 Conclusiones y líneas futuras	53
5.1 Viabilidad del uso de blindaje GNSS en buques de la Armada.....	53
5.1.1 Conclusiones desde el punto de vista mecánico	53
5.1.1 Conclusión desde el punto de vista electromagnético	54
5.1.2 Conclusión Operativa	57
5.2 Líneas Futuras	58
5.2.1 Integración con Antenas CRPA.....	58
5.2.2 Estudio de viabilidad del uso de choke ring en la Armada.....	58
6 Bibliografía.....	59
Anexo I: Implicaciones Sociales, Económicas, Ambientales	63
Anexo II: Reflexiones Éticas y Sociales	65
Anexo III: Glosario de abreviaturas y acrónimos	67
Anexo IV: Repositorio GitHub	69
Anexo V: Tablas de datos de precisión	71

ÍNDICE DE FIGURAS

Figura 2-1 Pasada y órbita del sistema <i>TRANSIT</i> [2]	12
Figura 2-2 Intersección de 3 satélites [4]	13
Figura 2-3 Esquema de los segmentos que componen GNSS.....	14
Figura 2-4 Composición de la modulación [7].....	16
Figura 2-5 Comparativa entre una buena y mala distribución de satélites.....	17
Figura 2-6 Pico de interferencia frente a señal GNSS [15].....	22
Figura 2-7 Pérdida de posicionamiento por <i>jamming</i> en un buque de la Armada	23
Figura 2-8 Esquemmatización de un ataque de <i>spoofing</i> [16].....	23
Figura 2-9 Simulación de secuencia de ataque de <i>spoofing</i> en Matlab.....	24
Figura 2-10 Presentación AIS tras ataque de <i>spoofing en el Mar Negro</i> [14]	25
Figura 2-11 Antena GAJT-710MST TM [24] y <i>beamforming</i> frente a ataque [25].....	26
Figura 2-12 Diaframa de antena LENA en dBi [18]	27
Figura 2-13 Antena Choke Ring comercial [30] y su diagrama característico [28].....	27
Figura 2-14 Apantallamiento improvisado en un buque mercante	28
Figura 3-1 Rayos incidentes, reflejados, difractados, y otros fenómenos asociados [35].....	31
Figura 3-2 Captura de pantalla de la interfaz de Trimble.....	32
Figura 3-3 Modelado y diagrama de radiación de la antena de parche cerámico	34
Figura 3-4 Mapa de protección frente a radio y diámetro respecto a un ataque del horizonte	35
Figura 3-5 Evolución del PDOP frente a la máscara.....	37
Figura 3-6 Evolución del PDOP a lo largo de una semana en antenas sin protección física	38
Figura 3-7 Evolución del PDOP a lo largo de una semana en antenas con protección física	38
Figura 3-8 Combinación de experiencia de protección y máscara.....	39
Figura 3-9 Representación y diagrama de radiación del conjunto cavidad antena	40
Figura 3-10 Comparativa de los diagramas de protección	42
Figura 3-11 Antena ELT0123 [39].....	43
Figura 3-12 Receptor EVK-M8T [40].....	43
Figura 3-13 Corte del Aluminio con amoladora angular.....	44
Figura 3-14 Medidas paliatorias iniciales frente a las tensiones en el primer prototipo.	45
Figura 3-15 Prototipo 2 acoplado con antena ELT0123.	45
Figura 3-15 Comparación de distribución satelital y DOP en ambos casos de estudio para GPS ...	47
Figura 4-1 Comprobación inicial del correcto funcionamiento de la antena	50
Figura 4-2 Gráfica de PDOP frente al tiempo	51
Figura 4-3 Comparación del caso nominal frente a un caso de protección del segundo prototipo..	52

Figura 4-4 Comparación de ambos prototipos, radio 18cm (izquierda) y 10cm (derecha).....	52
Figura 5-1 Antena SIMRAD de la F82	54
Figura 5-2 Gráfica de dispersión sin blindaje.....	54
Figura 5-3 Gráfica de dispersión con blindaje	55

ÍNDICE DE TABLAS

Tabla 2-1 Listado de antenas GNSS en la armada	19
Tabla 5-1 Datos obtenidos para el intervalo de 13:58-20:11 del día 21/02/2026	56

1 INTRODUCCIÓN Y OBJETIVOS

Este capítulo inicial sirve para enmarcar el Trabajo Fin de Grado en su contexto operativo repasando los antecedentes del problema. A partir de ahí, se desgranar los motivos que justifican el estudio y las metas concretas que persigue cumplir. Para cerrar la introducción, se ofrece un breve esquema de cómo está estructurada la memoria.

1.1 Antecedentes

Desde sus inicios, la navegación ha estado sustentada de forma directa por la capacidad de conocer la posición propia; el cabotaje dio paso a la estima que a su vez fue perfeccionada con la astronomía; se vuelve de esta manera la profesión de marino en una de cambio continuo en la que la nación con el posicionamiento más preciso ha sido capaz de navegar más lejos, por mejores rutas y con mayor seguridad, lo cual se ha visto reflejado en la geopolítica durante siglos. La investigación y avance en este campo nunca se ha detenido desde entonces, llegando a nuestros días en forma de GNSS, donde las constelaciones de satélites puestos en órbita por las principales potencias permiten una situación continua y fiable de receptores tanto en tierra como en alta mar. Y pese a varios años de eficiencia demostrada no faltan ejemplos de ataques y operaciones en contra de los sistemas GNSS, poniendo en evidencia que incluso una tecnología aparentemente madura como la localización por satélite debe aumentar su disponibilidad y precisión frente a las nuevas amenazas de la guerra de la navegación, que amenazan con degradar su eficiencia en los escenarios multidominio de la actualidad.

Es difícil imaginar un puente de un buque donde no se pueda consultar las coordenadas cartesianas de la posición actual, pero no fue hasta los años 70 que las primeras unidades de la Armada integraron estas tecnologías, primero de forma experimental con los sistemas TRANSIT, y finalmente extendido a toda la fuerza con antenas satélite capaces de posicionarse con las distintas constelaciones que componen el GNSS. Aun sin olvidar los métodos tradicionales e investigar en alternativas, no se puede obviar el posicionamiento por satélite como soporte fundamental de las operaciones navales, lo que no se reduce únicamente a nuestra precisión de navegación, siendo fundamental para enfrentamientos de superficie, posicionamiento de unidades propias y hostiles, así como operaciones de negación del mar. Se hace evidente la necesidad de preservar esta capacidad ante cualquier degradación ya sea accidental o provocada.

1.2 Motivación

Detrás de la realización de este proyecto no existe sino una necesidad real de nuestras unidades desplegadas en zonas de operaciones donde la negación de la señal satélite es una realidad y la amenaza

silenciosa del *spoofing* se encuentra latente. Cuando se enfrenta una amenaza real es necesario abordarla con una voluntad firme de ayudar a mantener la seguridad del personal y material que se expone a estas crecientes amenazas a la navegación. El fin último es dar una solución viable, no solo teóricamente, ya que resulta inútil crear una protección físicamente funcional a partir de simulaciones, si no es posible implantarla de forma sencilla en los lugares donde se necesita con urgencia. También debe de obtenerse una solución práctica que permita a las unidades en la vanguardia protegerse con seguridad manteniendo su confianza en las constelaciones satélite sin necesidad de recurrir a la estima o sistemas inerciales como principal fuente de posicionamiento acumulando errores inaceptables en un campo de batalla actual. Se hace así evidente la necesidad de combinar ambos resultados lo que permitiría una fácil producción e instalación mezclado con una eficacia demostrada mediante simulación y experimentación. Esto permite dejar atrás el uso de apantallamientos improvisados que, por culpa de sus dimensiones aleatorias, acaban generando más problemas de interferencia que beneficios reales.

Si bien las protecciones que se plantean en este trabajo no son las únicas contempladas en el panorama actual, sus capacidades y posibles beneficios requieren un estudio. Se pueden encontrar antenas satélites en el mercado con aplicaciones de protección similares a las deseadas, aun así, es crucial dar valor a una solución que, no solo pueda llegar a ser igual de efectiva, sino que además implica un coste mucho menor de adquisición e instalación, ahorrando un gasto excesivo a la Armada. Esta idea cobra especial fuerza cuando una figura como el AJEMA la respalda con las siguientes palabras en sus líneas generales de la armada para 2025: *“El equilibrio presupuestario es esencial para disponer de una Armada que pone en valor el recurso de personal, la preparación de la Fuerza y el empleo operativo de sus capacidades”* [1]. Este proyecto gira en torno a esta idea de dar prioridad al valor de los recursos propios de personal, los más valioso, sobre el gasto desmedido y en muchas ocasiones innecesario.

1.3 Objetivos

El objetivo último de este proyecto es el estudio y prueba del uso de cavidades como blindaje efectivo contra interferencias de tipo *jamming* y *spoofing* en antenas GNSS en los buques de la Armada. Se busca obtener una solución tangible de altura y diámetro de la estructura de protección teniendo en cuenta los efectos negativos que pueda llevar a provocar dicha estructura. Será necesario entonces cumplir los objetivos parciales de forma escalonada para llegar a un resultado final que verdaderamente aporte valor a nuestra fuerza naval; estos los plantearemos de la siguiente manera:

- **Estudio de eficiencia contra perturbaciones en función de las dimensiones de la cavidad.** El primer objetivo debe ser el encontrar unas dimensiones óptimas para la cavidad. Estas dimensiones vendrán determinadas por la combinación de máxima eficiencia frente a perturbaciones obtenidas a partir de múltiples iteraciones de radio y altura de la cavidad con herramientas de simulación.
- **Estudio de la pérdida de precisión en función de sus dimensiones de la cavidad.** Se sabe de antemano que la instalación de este tipo de protección reduce la línea de visión con cierto segmento de la bóveda celeste y sus satélites, lo que reduce la precisión del posicionamiento. Es necesario dar un valor numérico a esta pérdida de precisión por ese y otros posibles fenómenos relacionados con la geometría.
- **Búsqueda de la solución óptima.** Una antena completamente eficaz contra ataques es inútil si pierde el enlace con demasiados satélites ya que se compromete de forma crítica la precisión pudiendo llegar a dejar inoperativo el servicio de GNSS. Se hace evidente un apartado dedicado a buscar la combinación óptima entre un blindaje efectivo y funcional.
- **Diseño y validación de prototipo.** A partir de la supuesta solución óptima se construirá un prototipo de validación para estudiar pérdida de precisión y degradación y confirmar los valores obtenidos en el apartado anterior.

1.4 Estructura del trabajo

Para alcanzar los objetivos descritos, la presente memoria se ha estructurado en los siguientes capítulos:

- **1) Introducción:** Establece el contexto operativo y los antecedentes que motivan el estudio, estableciendo la meta principal del proyecto.
- **2) Estado del Arte:** Analiza el panorama actual del papel de la tecnología GNSS en la Guerra Electrónica de Navegación (NAVWAR) y las tecnologías de protección de antenas existentes, construyendo el marco teórico que fundamenta la solución propuesta.
- **3) Desarrollo del TFG:** Detalla el núcleo técnico del trabajo, abarcando desde el dimensionamiento y las simulaciones electromagnéticas iniciales hasta la construcción y configuración del entorno de validación empírica.
- **4) Resultados:** Expone de forma crítica los datos obtenidos en las pruebas de campo.
- **5) Conclusiones y Líneas Futuras:** Evalúa la viabilidad operativa de implementar este tipo de blindajes en las unidades de la Armada Española, proponiendo los siguientes pasos lógicos para la investigación tecnológica.
- **6) Bibliografía:** Recopilación de las fuentes normativas y técnicas consultadas.
- **7) Anexos:** Recopilación de material complementario.

2 ESTADO DEL ARTE

Este apartado analiza el panorama actual del papel de la tecnología GNSS enfocada en la Guerra Electrónica de Navegación (NAVWAR) y las tecnologías de protección de antenas existentes, construyendo el marco teórico que fundamenta la solución propuesta.

2.1 Sistemas GNSS

Los sistemas de navegación por satélite o GNSS (*Global Navigation Satellite Systems*) constituyen una familia de tecnologías diseñadas para proporcionar posicionamiento, navegación y sincronización temporal en cualquier lugar del planeta. Su desarrollo ha sido uno de los avances tecnológicos más significativos del siglo XX y XXI, con repercusiones directas en numerosos sectores civiles, militares, científicos y comerciales.

2.1.1 Historia y evolución de los sistemas GNSS

El origen de los sistemas de navegación por satélite (GNSS) se remonta al contexto geopolítico de la Guerra Fría, cuando la necesidad estratégica de obtener un posicionamiento preciso e inmediato impulsó la carrera tecnológica entre las grandes potencias. El punto de inflexión inicial tuvo lugar en 1957 con la puesta en órbita del primer satélite artificial de la historia, el Sputnik I, por la Unión Soviética; la variación constante de la frecuencia radio que recibía la superficie de este satélite inspiró a los científicos del *Applied Physics Laboratory* (APL) de la Universidad Johns Hopkins a analizar el desplazamiento Doppler de la señal de radio emitida por el Sputnik I, descubriendo que era posible determinar con exactitud la posición del transmisor; inversamente se razonó que conocida la posición exacta de un satélite en órbita un receptor en tierra podría ser localizado con precisión [2]. Este hallazgo sentó las bases para el desarrollo de TRANSIT en 1960, el primer sistema de navegación por satélite operativo utilizado por la Marina de los Estados Unidos, el cual seguía basando su funcionamiento en el cálculo de la frecuencia Doppler de satélites que fueron situados en órbitas polares. Las señales emitidas por el satélite en una de sus pasadas permitían calcular al receptor un punto fijo con cierto error [3], como se representa gráficamente en la Figura 2-1 . Pese a sus limitaciones de disponibilidad temporal y precisión, demostró la viabilidad de la tecnología.

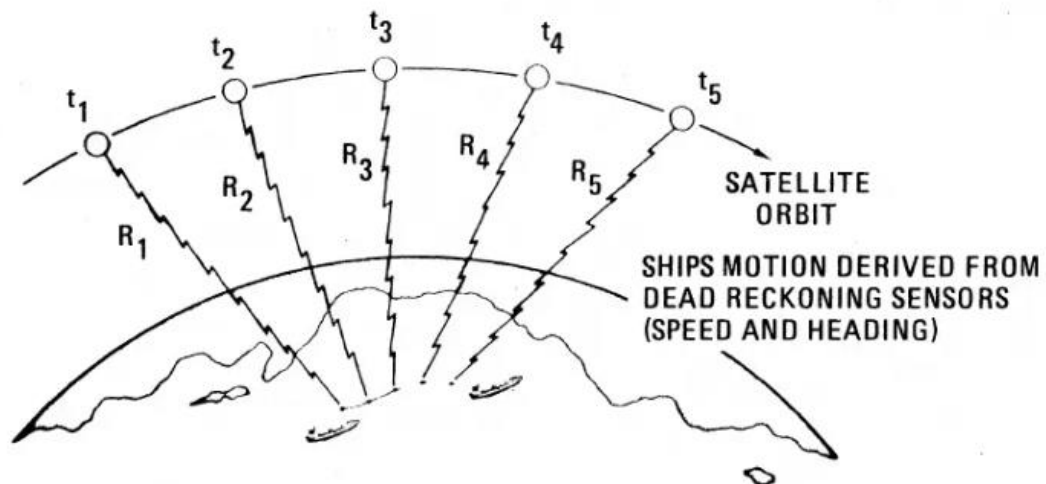


Figura 2-1 Pasada y órbita del sistema *TRANSIT* [2]

Ante la necesidad de un sistema más robusto, el Departamento de Defensa de los EE. UU. inauguró en 1973 el programa NAVSTAR-GPS, lanzando su primer satélite experimental en 1978 y alcanzando su capacidad operativa plena en 1995, dejando atrás la medición del Doppler, dando paso a la trilateración mediante señales radio de los satélites. De forma paralela, la Unión Soviética desarrolló el sistema GLONASS para contrarrestar la hegemonía estadounidense, consolidando la naturaleza dual (civil y militar) de estas tecnologías. Un hito fundamental en la evolución hacia el uso civil masivo se produjo tras el derribo del vuelo KAL 007 en 1983, que por un presunto fallo de su sistema inercial acabó entrando sin autorización en espacio aéreo soviético a cientos de kilómetros de su ruta. La tragedia llevó al gobierno estadounidense a autorizar el uso público de la señal GPS, una apertura que culminó en el año 2000 con la eliminación de la "disponibilidad selectiva" (SA), una técnica que variando los parámetros de los satélites introducía un error voluntario con el fin de degradar la señal, mejorando drásticamente la precisión para usuarios no militares. En la actualidad, la evolución de estos sistemas ha derivado en un entorno multi-constelación con la incorporación de Galileo (Europa) y BeiDou (China), garantizando una cobertura global redundante y de alta precisión.

2.1.2 Fundamentos de los sistemas GNSS

El funcionamiento de estos sistemas se basa en la medición de distancias (denominadas técnicamente pseudodistancias) entre los satélites de la constelación y el receptor, utilizando el principio geométrico de la trilateración. Los satélites emiten radioseñales continuas en frecuencias portadoras como L1 (1575.42 MHz), L2 (1227.60 MHz) y L5 (1176.45 MHz) [4].

Teóricamente, al conocer el tiempo de vuelo de la señal, se puede calcular la distancia al satélite, lo que genera una esfera de radio conocido, centrada en el mismo. La intersección de las esferas de tres satélites permitiría determinar las coordenadas espaciales (x, y, z) del receptor, como en el supuesto de la Figura 2-2. Sin embargo, este cálculo asume que el reloj del receptor está perfectamente sincronizado con los relojes atómicos de los satélites, algo imposible en equipos de usuario. Esta desincronización introduce una cuarta incógnita, el error o sesgo del reloj del receptor.

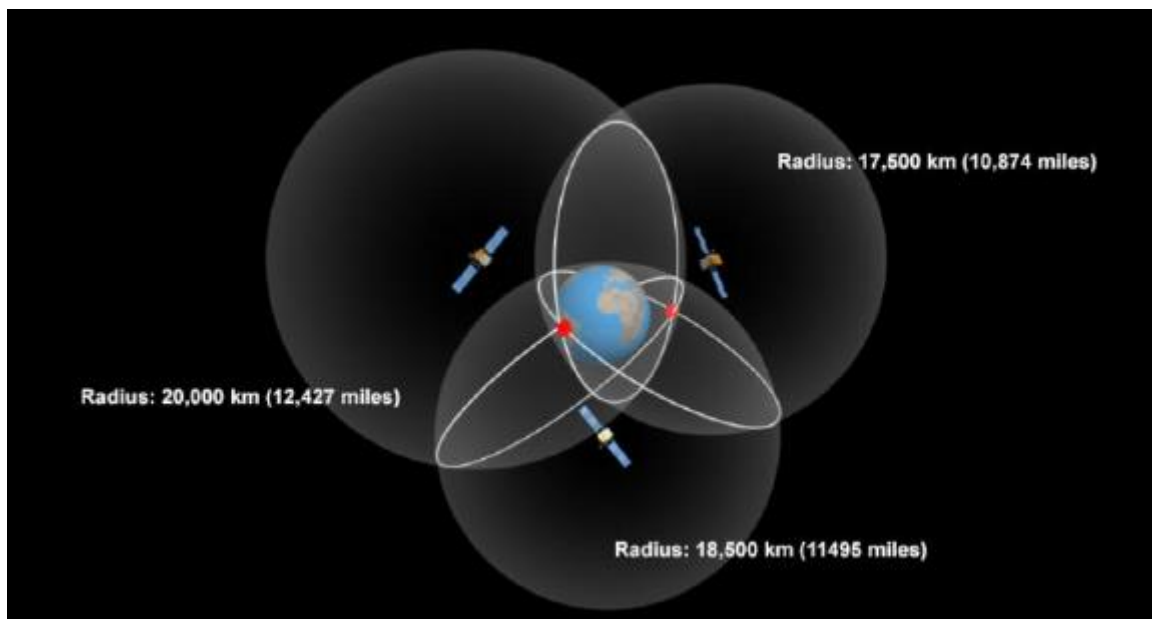


Figura 2-2 Intersección de 3 satélites [4]

Por consiguiente, para obtener una solución válida, es indispensable la señal de un cuarto satélite. Esto permite plantear un sistema de cuatro ecuaciones para resolver las cuatro incógnitas (latitud, longitud, altitud y tiempo), eliminando la ambigüedad temporal y precisando la posición.

La función primordial de los Sistemas Globales de Navegación por Satélite (GNSS) es proveer servicios de Posicionamiento, Navegación y Tiempo (PNT) a nivel global de forma ininterrumpida. Para lograrlo, todos los sistemas actuales comparten una arquitectura operativa estandarizada que se divide en tres bloques funcionales o segmentos bien diferenciados [4]:

- **Segmento Espacial:** El segmento espacial constituye la infraestructura del sistema que se encuentra en órbita. Su función principal es la generación y transmisión continua de señales de radiofrecuencia en la Banda L (debido a su resistencia tanto frente a la ionosfera como a la atenuación de los hidrometeoros), que contienen dos tipos de información crítica: la posición orbital precisa del satélite (efemérides) y el tiempo exacto; siendo este último un dato crucial relacionado estrechamente con la precisión donde un microsegundo equivale a cientos de metros de error, por lo que se utilizan relojes atómicos de rubidio o cesio.

Este segmento no es estático; está compuesto por constelaciones de satélites diseñadas para asegurar que, en cualquier punto de la superficie terrestre y en cualquier momento, un usuario tenga línea de visión directa (*Line of Sight* - LOS) con al menos cuatro satélites, el mínimo necesario para resolver las incógnitas de posición (X, Y, Z) y tiempo (t). Aunque la mayoría de estos vehículos se sitúan en órbitas terrestres medias (MEO) para garantizar una cobertura mundial con el menor número de unidades, sistemas modernos como BeiDou integran también satélites en órbita geoestacionaria (GEO) y órbita inclinada geosíncrona (IGSO) para reforzar la señal en regiones específicas. Su misión es transmitir unidireccionalmente señales de radiofrecuencia (banda L) que contienen códigos de navegación y marcas de tiempo generadas por relojes atómicos de alta estabilidad (rubidio o cesio/hidrógeno).

- **Segmento de Control:** Infraestructura terrestre distribuida globalmente responsable de supervisar la "salud" de la constelación, dado que los satélites están sujetos a perturbaciones gravitatorias (efectos de la Luna y el Sol), presión de radiación solar y deriva de los relojes

atómicos, los datos transmitidos a los usuarios deben ser corregidos. Este segmento se divide típicamente en:

- **Estación de Control Maestra (MCS):** Procesa los datos, calcula las correcciones de órbita y reloj, y genera el mensaje de navegación.
- **Estaciones de Monitorización:** Distribuidas globalmente para rastrear las señales de los satélites pasivamente y enviar datos a la MCS.
- **Antenas de Tierra (*Up-link*):** Se utilizan para subir los datos corregidos y comandos a los satélites (generalmente en banda S).
- **Segmento de Usuario:** Este segmento engloba a todos los receptores que procesan las señales GNSS para calcular posición, velocidad y tiempo (PVT). Desde un punto de vista de ingeniería de defensa y el objeto de este TFG, este es el segmento más vulnerable. El receptor es totalmente pasivo; no emite señales, solo escucha. Debido a la enorme distancia que recorre la señal, la potencia recibida a nivel de suelo es extremadamente baja, lo que hace que el segmento de usuario sea susceptible a ataques si no se protege adecuadamente mediante antenas especializadas.

En el panorama actual, el entorno de navegación por satélite ha evolucionado de arquitecturas monolíticas a un verdadero sistema de sistemas como el que se esquematiza en la Figura 2-3 . Esta redundancia es crítica desde el punto de vista de la defensa. La disponibilidad de múltiples constelaciones permite a un receptor militar operar en entornos degradados, aprovechando la diversidad de frecuencias y geometrías orbitales.

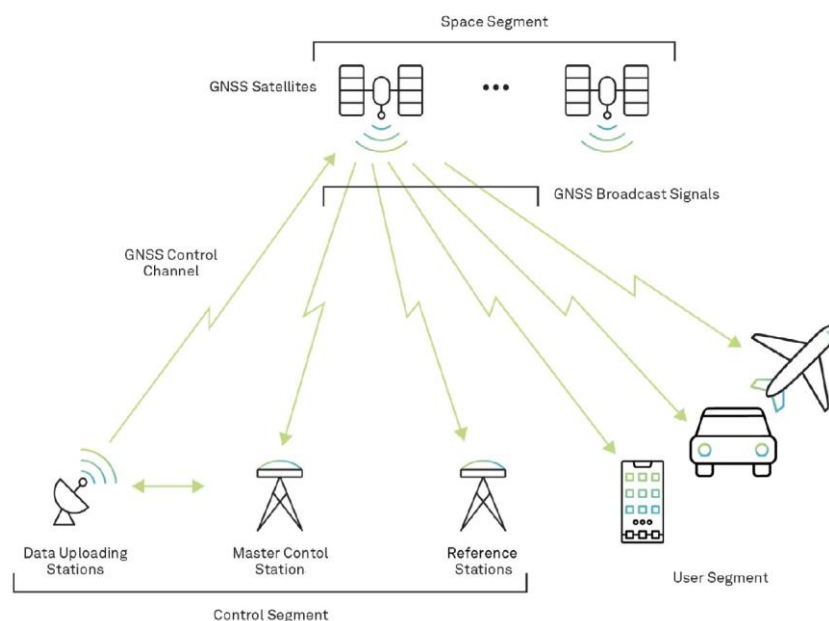


Figura 2-3 Esquema de los segmentos que componen GNSS

Actualmente, operan cuatro constelaciones globales (GNSS) principales de manera independiente pero compatible:

- **NAVSTAR-GPS (EE. UU.):** El sistema pionero, plenamente operativo desde 1995. Orbita en planos MEO y utiliza el sistema de referencia WGS-84. En su vertiente de defensa, las últimas iteraciones (Bloque III) implementan la señal M-Code, diseñada con mayor potencia y técnicas de modulación avanzadas para resistir intentos de *jamming*.

- **GLONASS (Federación Rusa):** Reactivado plenamente en la década de 2010. Se diferencia técnicamente por utilizar acceso múltiple por división de frecuencia (FDMA) en sus señales heredadas, lo que implica que cada satélite transmite en una frecuencia ligeramente diferente. Esto supone un reto y una ventaja para el diseño de antenas: requiere mayor ancho de banda, pero dificulta el bloqueo simultáneo de toda la constelación con un *jammer* de banda estrecha.
- **BeiDou (China):** Completado recientemente (BDS-3), se caracteriza por su arquitectura de órbita mixta única, que combina satélites MEO globales con satélites GEO e IGSO. Esta configuración optimiza su rendimiento y disponibilidad en la región Asia-Pacífico, garantizando una visibilidad satelital superior en entornos urbanos y montañosos de esas regiones.
- **Galileo (Unión Europea):** Aunque es el único sistema bajo control exclusivamente civil, su diseño contempla servicios específicos de alta seguridad que lo convierten en un activo estratégico de primer orden para aplicaciones gubernamentales y militares. El primer servicio es *Open Service* (OS) y *Open Service Navigation Message Authentication* (OSNMA) que ofrece posicionamiento civil y comercial con una precisión métrica mientras que para el ámbito militar encontramos el *Public Regulated Service* (PRS), un servicio encriptado, robusto y de acceso restringido a usuarios autorizados por los gobiernos; muestra gran resistencia al *jamming* al transmitir las señales en frecuencias separadas (bandas E1 y E6) con modulaciones de banda ancha (BOC) que las hacen más resistentes a las interferencias y al ruido que las señales civiles estándar [5].

Para complementar la cobertura global, existen sistemas de navegación por satélite regionales (RNSS) que operan de forma autónoma pero restringida a áreas geográficas concretas. Su inclusión en el análisis es relevante porque sus satélites, a menudo en órbitas altas (IGSO/GEO), proporcionan líneas de visión casi cenitales, difíciles de bloquear con *jammers* terrestres. En esta categoría se encuentran el QZSS japonés y el NAVIC Indú.

2.1.3 Estructura y composición de la señal de navegación

El enlace que conecta el segmento espacial con el segmento de usuario es una señal de radiofrecuencia compleja, diseñada no solo para transportar información, sino también para permitir la medición precisa de tiempos de propagación mediante técnicas de correlación. Desde un punto de vista espectral, los satélites GNSS transmiten en la banda L del espectro electromagnético (frecuencias entre 1 y 2 GHz), elegida por ofrecer un compromiso óptimo entre una baja atenuación por lluvia y una refracción ionosférica corregible.

La señal GNSS se compone de tres capas o elementos fundamentales modulados entre sí, utilizando generalmente modulación por desplazamiento de fase binaria (BPSK - *Binary Phase Shift Keying*). Según la especificación oficial IS-GPS-200 [6], en relación con la constelación GPS, esta estructura en capas se desglosa, como muestra la Figura 2-4, de la siguiente manera:

- **La Portadora (*Carrier*):** Es la onda sinusoidal de radiofrecuencia pura que actúa como vehículo de transporte. Su frecuencia determina la longitud de onda, parámetro físico crítico para el diseño de las antenas y, en el contexto de este trabajo, para el dimensionamiento de las medidas físicas de protección.
- **El Código de *Ranging* (PRN):** Es una secuencia binaria pseudoaleatoria (*Pseudo-Random Noise*) que se modula sobre la portadora a una tasa de 1.023 Mbps. En la señal civil, se utilizan los Códigos de Gold, familias de secuencias matemáticas que poseen propiedades de autocorrelación y correlación cruzada casi ideales. Su función principal es el *ranging*, que

permite al receptor determinar el tiempo de tránsito de la señal Delta midiendo el retardo de fase del código recibido respecto a una réplica generada internamente.

- **El Mensaje de Navegación:** Son los datos binarios de muy baja velocidad (50 bps) que se superponen a la señal. Estos datos se estructuran en tramas y subtramas de 1500 bits que contienen la información vital del satélite: su estado de salud, las correcciones de los relojes atómicos y, crucialmente, las efemérides (parámetros orbitales precisos) necesarias para calcular las coordenadas (X, Y, Z) del satélite en el instante de la transmisión [4].

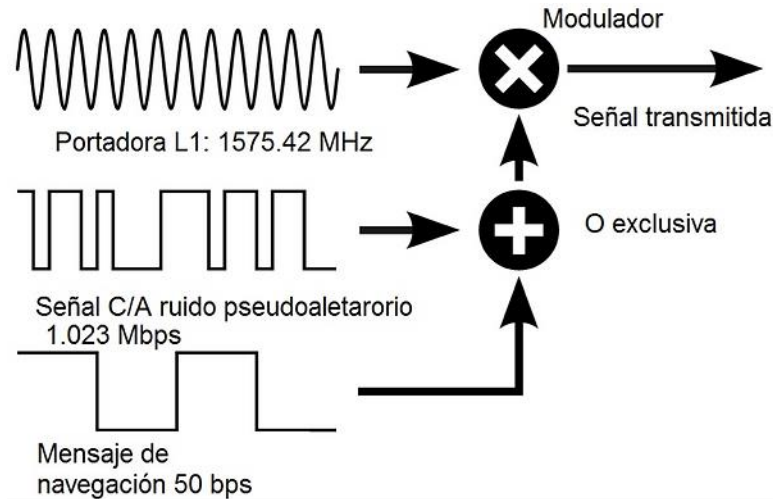


Figura 2-4 Composición de la modulación [7]

Un aspecto técnico crucial en el diseño de esta señal es la técnica de acceso al medio. Para permitir que todos los satélites de la constelación transmitan simultáneamente en la misma frecuencia central sin interferirse mutuamente, se emplea la técnica CDMA (*Code Division Multiple Access*) basada en espectro ensanchado por secuencia directa (DSSS).

Cada satélite tiene asignado un código PRN único que es ortogonal al resto. Esto implica que, matemáticamente, el producto de dos códigos diferentes integrado en el tiempo es prácticamente cero. Gracias a esta propiedad, el receptor puede sintonizar y aislar un satélite concreto, correlando su señal con la réplica local correcta, mientras que el resto de las señales de otros satélites están incorreladas y se perciben simplemente como un leve incremento en el ruido de fondo. Esta técnica proporciona una Ganancia de Procesado (*Processing Gain*) teórica de unos 43 dB, lo que permite recuperar la señal incluso cuando está bajo el nivel de ruido [6].

Sin embargo, esta arquitectura presenta dos vulnerabilidades inherentes, cuyo análisis en apartados posteriores motivarán el diseño de protecciones físicas.

En primer lugar, al ser los códigos civiles de conocimiento público, un atacante puede generar réplicas falsas de la señal (*spoofing*) para engañar al lazo de seguimiento del receptor. En segundo lugar, la señal llega a la superficie terrestre con una potencia extremadamente baja, inferior al ruido térmico ambiental. Esta debilidad estructural hace que el sistema sea muy susceptible a interferencias intencionadas (*jamming*), ya que cualquier señal de ruido con una potencia ligeramente superior en la misma banda puede saturar el receptor y bloquear la demodulación de los códigos [4].

2.1.4 Precisión del posicionamiento, factor geométrico (DOP) y multitrayecto

La exactitud final con la que un receptor GNSS puede determinar su ubicación no es un valor absoluto, sino el resultado de combinar dos factores independientes: la calidad de las medidas de distancia a los satélites y la disposición geométrica de estos en la bóveda celeste. Matemáticamente, el error en la posición tridimensional σ_{pos} se puede expresar como el producto del error medio en la

medición de la pseudodistancia, conocido como σ_{UERE} (*User Equivalent Range Error*), por un factor de amplificación puramente geométrico denominado DOP (*Dilution of Precision*):

$$\sigma_{pos} = DOP \cdot \sigma_{uere}$$

Mientras que el UERE depende de factores físicos como el ruido de los relojes atómicos, errores de efemérides o retardos atmosféricos no corregidos, el DOP cuantifica la robustez matemática de la configuración satelital visible, es decir la eficiencia de su distribución [8]. La diferencia entre una geometría óptima y una que no lo es más sencillo de comprender con el ejemplo de la Figura 2-5 .

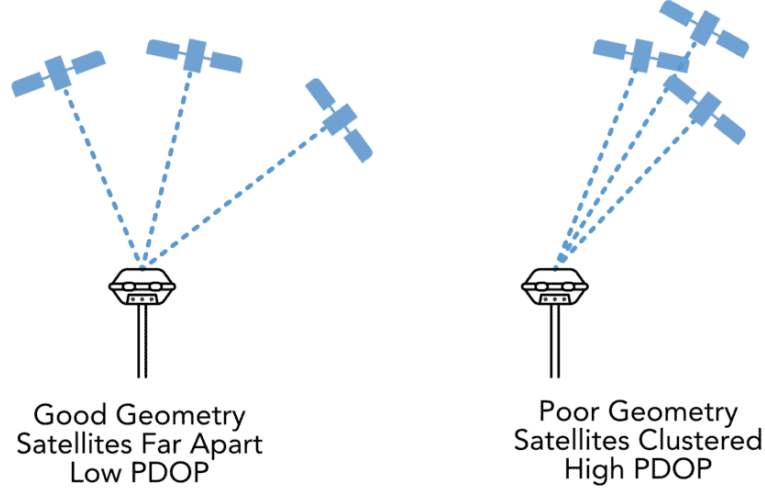


Figura 2-5 Comparativa entre una buena y mala distribución de satélites

Es posible calcular el DOP a partir de la traza de la matriz de covarianza de los errores de estimación de posición ($cov(\Delta x)$). Según el análisis matricial propuesto por *Jwo* [9] y formalizado por investigaciones de *Misra* y *Enge* [10], para una solución de mínimos cuadrados, la relación entre los errores de medición y el error de posición depende de la inversa de la matriz de geometría H (donde H contiene los vectores unitarios hacia los satélites).

$$cov(\Delta x) = \sigma_{UERE}^2 \cdot (H^T H)^{-1} = \sigma_{UERE}^2 \cdot Q$$

Donde Q es la matriz de cofactores definida como:

$$Q = (H^T H)^{-1} = \begin{pmatrix} q_{xx} & q_{xy} & q_{xz} & q_{xt} \\ q_{yx} & q_{yy} & q_{yz} & q_{yt} \\ q_{zx} & q_{zy} & q_{zz} & q_{zt} \\ q_{tx} & q_{ty} & q_{tz} & q_{tt} \end{pmatrix}$$

Un valor de DOP bajo (idealmente < 2) implica que los satélites están ampliamente distribuidos en acimut y elevación, maximizando el volumen del poliedro formado por el usuario y los satélites. Por el contrario, si los satélites visibles se encuentran agrupados en una pequeña región del cielo (poco volumen angular), la matriz se vuelve mal condicionada, el valor de DOP aumenta drásticamente y cualquier pequeño error en la medición de la distancia se magnifica en la solución final.

Existen distintas variantes del DOP que corresponden a los elementos de la diagonal principal de la matriz de covarianza de error, siendo las más relevantes para este estudio:

- **GDOP (Geometric DOP):** Representa la incertidumbre total, incluyendo las 3 dimensiones espaciales y la temporal (reloj).
- **PDOP (Positional DOP):** Aísla el error en posición 3D (es la métrica de referencia para evaluar la calidad de la constelación). Será el que utilizemos principalmente en los cálculos del proyecto

al obtener un valor absoluto de posición a partir de él. Aunque la componente vertical pueda parecer de menor entidad para este estudio la diferencia entre PDOP y el HDOP, como se mencionará a continuación, es despreciable en el estudio.

Su cálculo se establecerá como la raíz cuadrada de la traza de la submatriz espacial 3×3 :

$$PDOP = \sqrt{Tr(cov_{xyz})} = \sqrt{q_{xx} + q_{yy} + q_{zz}}$$

- **HDOP (Horizontal DOP) y VDOP (Vertical DOP):** Desglosan el error en componentes horizontal y vertical. Dado que el diseño de cavidad cilíndrica afecta predominantemente a la visibilidad lateral, el VDOP es el parámetro más sensible a las variaciones en la altura del cilindro, protector tal como demostró Santerre en sus estudios sobre la distribución del cielo [11].

El concepto de DOP cobra una relevancia capital en el diseño de protecciones físicas para antenas, objeto de este TFG. Al instalar una barrera física para bloquear interferencias procedentes del horizonte (*jamming* terrestre), se introduce inevitablemente una máscara física de elevación artificial. Esta máscara restringe la visibilidad de los satélites con ángulos de elevación bajos, reduciendo el número de satélites disponibles para el cálculo de la PVT y forzando una geometría más cenital. Este fenómeno tiene dos consecuencias directas:

1. **Degradación del PDOP:** Al eliminar los satélites bajos, se reduce la separación angular, empeorando la precisión general.
2. **Degradación Crítica del VDOP:** Los satélites cercanos al horizonte son los que aportan una mayor información para resolver la componente Z (altura). Al eliminarlos, el error vertical (VDOP) crece mucho más rápido que el horizontal. Estudios sobre geometrías limitadas sugieren que, en escenarios de alta obstrucción, la degradación vertical puede requerir técnicas de "*Altimeter Aiding*" (ayuda barométrica) para estabilizar la solución de navegación [9]. Esto no será crítico en nuestro planteamiento ya que en buques de superficie la preocupación principal es el HDOP al considerar la altura de la antena receptora constante.

Por tanto, el diseño del apantallamiento debe buscar un punto de equilibrio crítico maximizando el bloqueo de señales hostiles sin elevar el DOP por encima de umbrales operativos aceptables.

Al margen de la geometría satelital (DOP), es imperativo considerar el error inducido por el entorno inmediato de la antena, el efecto multitrayecto o *multipath*. Este fenómeno se produce cuando la señal GNSS no llega al receptor únicamente a través de la línea de visión directa (LOS), sino que se superpone con versiones replicadas, retardadas y atenuadas de sí misma que han sido reflejadas en superficies conductoras cercanas (suelo, estructuras del buque o, críticamente, las paredes de una protección física mal diseñada).

Estas reflexiones distorsionan la función de correlación en el receptor, introduciendo errores tanto en la fase de la portadora como en el código, lo que se traduce en desviaciones de posición que pueden oscilar desde unos pocos centímetros hasta varios metros. Según Kaplan y Hegarty [4], el *multipath* es la fuente de error dominante en receptores modernos una vez corregidos los errores atmosféricos, siendo especialmente pernicioso en entornos navales debido a la alta reflectividad de la superficie del mar y la superestructura metálica de los buques. Para el objeto de este proyecto, el control del *multipath* es un requisito de diseño fundamental. La cavidad protectora debe bloquear las interferencias externas sin convertirse ella misma en una cámara de eco que degrade la integridad de la señal legítima mediante reflexiones internas.

2.1.5 Importancia en el ámbito de la defensa, vulnerabilidades y uso en la Armada

Aunque el uso civil de los sistemas GNSS se ha generalizado globalmente, su origen y concepción primaria son eminentemente militares. En el teatro de operaciones moderno, el posicionamiento satelital se ha convertido en la columna vertebral de la guerra centrada en redes, proporcionando una ventaja táctica decisiva en los dominios terrestre, naval y aéreo. Sus aplicaciones van más allá de la simple navegación de plataformas; son críticas para la sincronización temporal de sistemas de comunicaciones encriptadas, el guiado de municiones de precisión (PGM), las operaciones de búsqueda y rescate (SAR) y el seguimiento de fuerzas propias (*Blue Force Tracking*) como establece la doctrina conjunta [12] lo que permite mantener una consciencia situacional superior y reducir el riesgo de fuego amigo.

En el ámbito nacional, la Armada Española ha jugado un papel histórico fundamental en la transición de la navegación astronómica a la satelital. Antes de la implantación total del GPS, la Armada fue usuaria temprana del sistema TRANSIT, el primer sistema de navegación por satélite operativo del mundo desarrollado por la Marina de los EE. UU.

Buques emblemáticos como el portaaviones *Dédalo* (R-01) o las fragatas de la clase *Baleares* (F-70) comenzaron a integrar receptores de navegación satelital en las décadas de 1970 y 1980, permitiendo una precisión en alta mar desconocida hasta la fecha.

Independientemente de los avanzados sistemas inerciales y el alto adiestramiento de las tripulaciones en navegación de estima, la navegación por satélite ha cobrado una dependencia operativa capital, lo que la convierte en un activo crucial en el reciente campo de batalla del espectro electromagnético. La baja potencia de la señal GNSS recibida en superficie la convierte en el "talón de Aquiles" de los sistemas dependientes de PNT (*Positioning, Navigation and Timing*). En un entorno de conflicto asimétrico o de alta intensidad, el adversario buscará negar esta capacidad mediante técnicas de guerra electrónica de la navegación (NAVWAR).

Todos los buques de la armada sin excepción cuentan con tecnología y posicionamiento mediante GNSS en la actualidad. Resulta lógico en un trabajo de esta entidad repasar las opciones a las que ha recurrido la Armada, recogidas en la Tabla 2-1 Listado de antenas GNSS en la armada. Dicha tabla se centra en las embarcaciones de mayor relevancia, especialmente las que tengan más probabilidades de enfrentar un entorno degradado en el futuro.

Clase/Buque	Antena GNSS	
	Civil	Militar
F-100 Álvaro de Bazán	TRIMBLE	LITTON
L-61 Juan Carlos I	SAAB R6	SKYDEC
L-51 Galicia	SIMRAD	LEICA
F-80 Santa María	SIMRAD	WRN-6
A-15 Cantabria	SIMRAD	SKYDEC

Tabla 2-1 Listado de antenas GNSS en la armada

La principal diferencia entre las antenas GNSS civiles y las militares reside en su capacidad de supervivencia ante entornos de guerra electrónica. Mientras que el sector civil prioriza la relación coste-precisión, operando con señales públicas altamente vulnerables a interferencias, el ámbito militar exige arquitecturas de *hardware* robustas combinadas con tecnologías activas. De este modo, las antenas militares operan en conjunto con receptores criptográficos (como los módulos SAASM o el servicio

Galileo PRS) para procesar señales cifradas, garantizando un posicionamiento fiable en escenarios hostiles donde un sistema comercial quedaría completamente inoperativo.

Más allá de la navegación pura, en los navíos de guerra es habitual encontrar otras antenas GNSS que a menudo pasan desapercibidas, como las dedicadas en exclusiva al sistema AIS o las que actúan como referencia temporal (*Timing*). La sincronización precisa del tiempo es un factor importancia estratégica en las operaciones navales modernas, ya que los sistemas de combate y las redes de comunicaciones cifradas dependen continuamente de esta variable para funcionar sin interrupciones.

Por tanto, el uso de los sistemas de posicionamiento por satélite en las unidades de la Armada Española trasciende la mera ubicación en la carta náutica. En buques de combate de primera línea, como las fragatas de la clase Álvaro de Bazán (F-100) y las futuras clase Bonifaz (F-110), la señal GNSS constituye un vector crítico para la operatividad de sus sistemas de armas. La precisión de las coordenadas del propio buque es el parámetro fundamental con el que se inician los sistemas de guiado antes de un lanzamiento. Aunque la documentación táctica de la Armada (específicamente las *Capabilities and Limitations* del sistema de combate de las F-100) establece valores de precisión exactos, en este trabajo se utilizarán aproximaciones basadas en fuentes abiertas para mantener el carácter no clasificado del TFG.

El caso más representativo dentro del arsenal de la Armada es el misil antibuque y de ataque a tierra RGM-84 Harpoon (Block II). Esta versión incorpora un paquete de guiado avanzado que fusiona una Unidad de Medición Inercial (IMU) con un receptor GPS, dotando al buque de la capacidad de atacar objetivos en el litoral e infraestructuras terrestres con un error de apenas 10 a 13 metros en condiciones normales.

Sin embargo, esta capacidad de ataque de precisión está estrictamente supeditada a la calidad de la señal satelital en el momento del disparo. Siguiendo la doctrina estándar de la OTAN, la calidad del posicionamiento se evalúa mediante el parámetro FOM (*Figure of Merit*). Para autorizar el lanzamiento de un arma guiada contra coordenadas estáticas terrestres minimizando el riesgo de daños colaterales, el Sistema de Control de Armas exige que la plataforma lanzadora mantenga un FOM 1. Traducido a valores operativos, un FOM 1 impone un umbral de error máximo de 25 metros. Si el buque sufre interferencias intencionadas (*jamming*) que degraden la señal y eleven la incertidumbre posicional por encima de este límite, el sistema reportará una solución de tiro insegura. En la práctica, esto inhabilita al misil para misiones de precisión a tierra, suponiendo una pérdida inaceptable en la capacidad de disuasión y proyección de la fuerza naval. Cabe mencionar que esta vulnerabilidad se verá parcialmente mitigada con la entrada en servicio de las fragatas F-110, cuyos misiles NSM (*Naval Strike Missile*) emplearán navegación por referencia del terreno (TERCOM) para corregir posibles errores de inicialización.

De forma análoga, el Fuego Naval de Apoyo proporcionado por la artillería principal (como los cañones Mk.45 Mod.2 de 127 mm de las F-100) sufre una vulnerabilidad geométrica directa ante la degradación del entorno electromagnético. El Sistema de Control de Tiro (FCS) calcula la solución balística fundamentándose en un triángulo estricto: las coordenadas del objetivo, las variables meteorológicas y la ubicación exacta del buque. Al emplear munición convencional, cualquier aumento en la incertidumbre posicional de la plataforma lanzadora se transfiere de manera lineal al punto de impacto. En un escenario táctico de apoyo a la Infantería de Marina, este decremento en la precisión conlleva un riesgo inasumible de fuego amigo o daños colaterales, forzando la cancelación inmediata de la misión de fuego. El límite máximo de tolerancia para este error de posicionamiento viene dictaminado por la publicación nacional clasificada D-SF-31.

2.2 Guerra Electrónica de la Navegación (NAVWAR)

El concepto de *Navigation Warfare* (NAVWAR) se define como el conjunto de acciones militares coordinadas para asegurar el acceso a la información de posicionamiento, navegación y tiempo (PNT) para las fuerzas propias, mientras se deniega simultáneamente esta capacidad al adversario. Dentro de la doctrina de Guerra Electrónica, la NAVWAR se estructura sobre tres pilares fundamentales: el Apoyo Electrónico (ES), la Protección Electrónica (EP) y el Ataque Electrónico (EA).

Antes de centrarnos en la protección electromagnética, que será el objetivo final de este proyecto, es necesario analizar en profundidad las amenazas correspondientes al ataque electromagnético. Estas acciones ofensivas explotan la debilidad inherente de la señal GNSS (baja potencia y estructura pública conocida) para degradar o anular el servicio. Las dos técnicas principales de ataque, que dictan los requisitos de diseño del apantallamiento propuesto, son la interferencia por ruido o *jamming* y la generación de señales engañosas o *spoofing*.

2.2.1 Interferencias intencionadas (*Jamming*)

El *jamming* es la forma más directa de ataque electrónico contra los sistemas GNSS. Su principio de funcionamiento explota la extremada debilidad de la señal satelital al llegar a la superficie terrestre. La señal GPS se recibe con una potencia aproximada de -160 dBW en la superficie terrestre, quedando bajo el ruido térmico. Los receptores logran recuperar esta señal gracias a la ganancia de procesamiento que otorga el código CDMA; sin embargo, este margen es finito.

Un ataque de *jamming* consiste en la emisión deliberada de energía de radiofrecuencia en la misma banda (L1, L2, etc.) con el objetivo de elevar el umbral de ruido (*noise floor*) hasta que la relación *Jamming*-a-Señal (J/S) supera la capacidad de anti-interferencia del receptor. Al perder el receptor la capacidad de correlacionar el código, se produce una denegación de servicio (DoS), impidiendo el cálculo de la posición. Debido a la baja potencia de la señal legítima, no se requieren equipos de alta tecnología para lograr este efecto; un inhibidor de bajo coste y poca potencia (milivatios) puede bloquear la recepción en un radio de varios kilómetros, lo que convierte a esta amenaza en un riesgo asimétrico constante.

La historia reciente recoge numerosos incidentes que evidencian la gravedad de esta vulnerabilidad. En el ámbito civil, es de renombre el incidente del Aeropuerto de Newark (EE. UU.) documentado por la FAA, donde un sistema de aumentación basado en tierra (GBAS) sufría desconexiones diarias recurrentes. La investigación reveló que la causa era un camionero que utilizaba un inhibidor personal de bajo coste (PPD) para anular el rastreador GPS de su empresa; al pasar por la autopista adyacente, su dispositivo interfería involuntariamente con los sistemas críticos de control aéreo [13].

En el ámbito militar y geopolítico, el uso de *jammers* de alta potencia es una táctica consolidada. Un informe exhaustivo del *Center for Advanced Defense Studies* (C4ADS) documentó casi 10.000 incidentes de interferencia GNSS vinculados a actividades rusas entre 2016 y 2018. Estos eventos, concentrados en zonas como Siria, Crimea y el Mar Negro, no solo afectaron a buques y aeronaves militares, sino que degradaron la navegación civil en regiones enteras como medida de protección de bases estratégicas o figuras VIP, demostrando que el control del espectro es un dominio activo de combate [14].

La vulnerabilidad de los sistemas de navegación por satélite frente a NAVWAR representa un desafío crítico y de absoluta actualidad para la operatividad y la seguridad marítima a nivel global. Incluso los conflictos de mayor actualidad presentan esta amenaza. Las actuales tensiones geopolíticas en el Estrecho de Ormuz y el Golfo Pérsico han desencadenado episodios masivos de interferencia GNSS afectando a más de 1.100 buques comerciales en apenas 24 horas, alterando sus sistemas AIS y capacidades PNT [15].

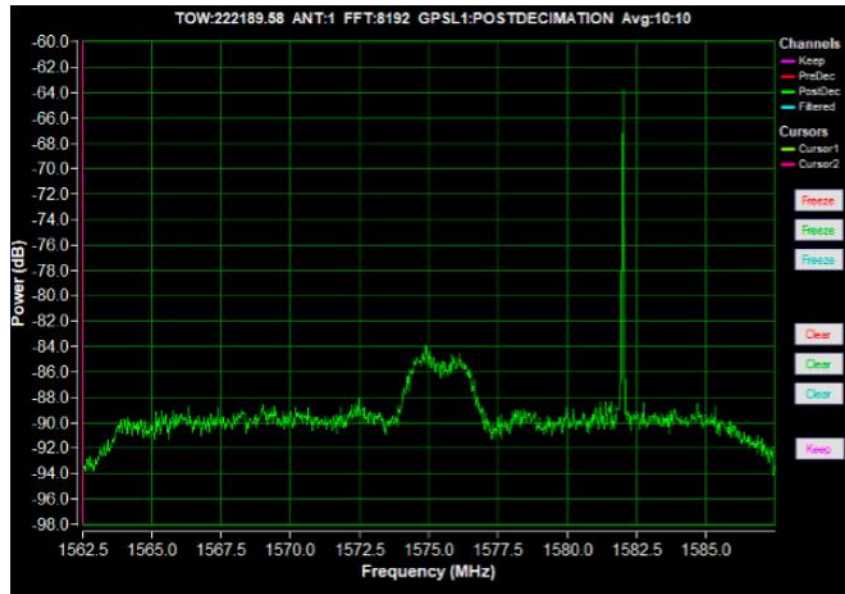


Figura 2-6 Pico de interferencia frente a señal GNSS [15]

La Figura 2-6 ilustra de forma muy acertada este fenómeno regido por la ecuación de transmisión de Friis. Considerando un escenario de interferencia en el vacío, la potencia del *jammer* recibida J en relación con la potencia de la señal satelital deseada S se puede expresar en decibelios como:

$$\left(\frac{J}{S}\right) dB = EIRP_j [dBm] + G_r - L_{fs} - S [dBm]$$

Donde:

- $EIRP_j$: Es la Potencia Isotrópica Radiada Equivalente del *jammer* (potencia de transmisión + ganancia de su antena).
- L_{fs} : Son las pérdidas por espacio libre, definidas como $20 \times \log_{10} 4\pi d/\lambda$, siendo d la distancia entre el *jammer* y el receptor.
- G_r : Es la ganancia de la antena receptora en la dirección de llegada de la interferencia.

Esta ecuación revela una vulnerabilidad crítica: dado que la potencia de la señal legítima (S) es extremadamente baja e invariable, un atacante tiene dos vectores para denegar el servicio: aumentar su potencia de emisión o acercarse al objetivo (reduciendo d). Sin embargo, la fórmula también expone la solución defensiva que fundamenta este TFG: si logramos reducir drásticamente el término G_r mediante apantallamiento físico en los ángulos de llegada de la señal del *jammer* (generalmente cercanos al horizonte), podemos mantener la relación J/S por debajo del umbral de saturación, protegiendo así la operatividad del receptor.

La doctrina de la Armada, en este caso específico los procedimientos de escuadrilla de la 31 escuadrilla (Se evitarán valores exactos para proteger la confidencialidad), establece el alcance de un único perturbador a las 23 millas náuticas, pudiendo extenderse hasta las 30 millas náuticas. Las acciones paliatorias se comenzarán a 40 millas de la zona o unidades sospechosas. Los efectos se vuelven apreciables en consolas y equipos de presentación de la información. La tecnología detrás de un *jammer* es sencilla, al alcance de cualquier fuerza armada del mundo. Incluso empresas como JAMMERMaster® comercian con particulares encontrando en su catálogo equipos de bloqueo de señal GPS de grado militar, aunque es su mayoría son de pequeña entidad [16].

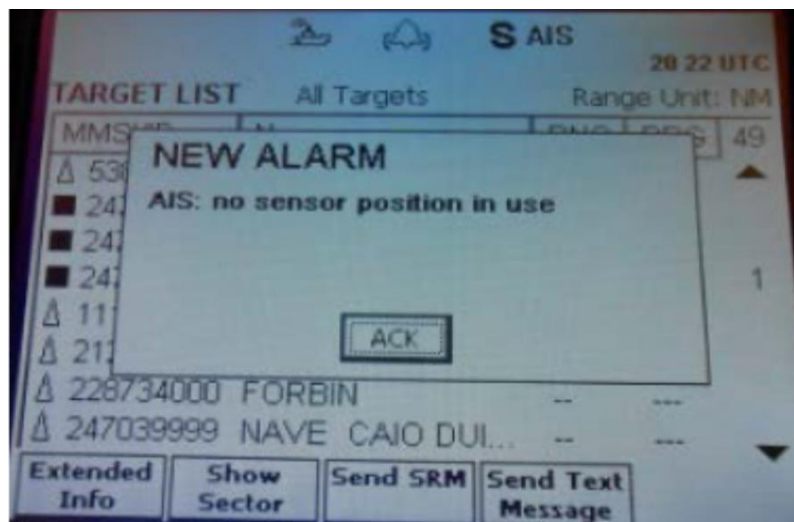


Figura 2-7 Pérdida de posicionamiento por *jamming* en un buque de la Armada

Un escenario habitual en zonas degradadas es el que se presenta en la Figura 2-7. Analizando una amenaza real cualquiera, existente en las múltiples zonas de operaciones donde se encuentran unidades de la Armada se plantea un escenario con un equipo R-330Zh Zhitel. Con una potencia una supuesta potencia de 100W a una distancia aproximada de 7 millas náuticas, la perturbación tras las pérdidas de propagación tendría un valor de 63dB en el buque, donde una señal superior a 45dB le haría perder su señal GNSS [17] completamente. Es necesario proteger en torno a 20dB.

2.2.2 Suplantación de identidad (*Spoofing*)

A diferencia del *jamming*, cuyo objetivo es la negación bruta del servicio, el *spoofing* representa una amenaza mucho más insidiosa y sofisticada: la inyección de señales falsas para tomar el control de los bucles de seguimiento del receptor víctima. Mientras que el *jamming* es fácilmente detectable por la pérdida de señal, un ataque de *spoofing* exitoso es transparente para el usuario, quien continúa recibiendo coordenadas de posición y tiempo que el atacante manipula a voluntad. Esta técnica explota el conocimiento público de la estructura de los códigos C/A civiles, permitiendo a un transmisor hostil generar réplicas sintéticas indistinguibles de las auténticas [16], modificando de forma total o parcial el resultado del posicionamiento como esquematiza la Figura 2-8.

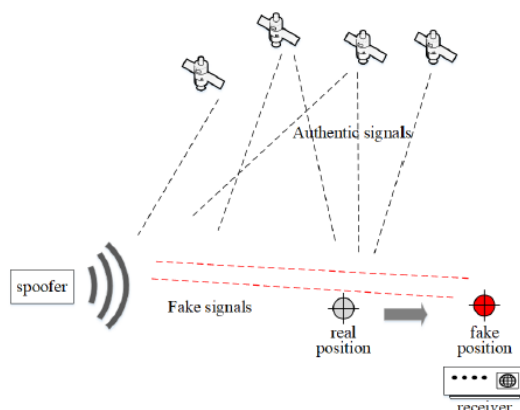
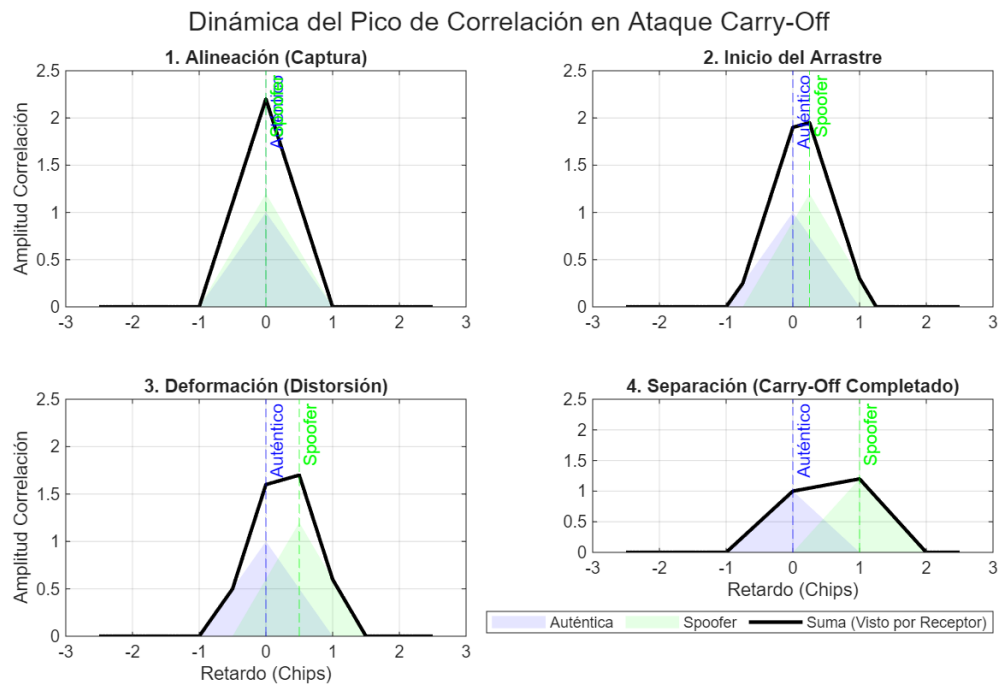


Figura 2-8 Esquematización de un ataque de *spoofing* [16]

La modalidad de ataque más efectiva y difícil de detectar se denomina ataque de arrastre o *carry-off*. En su fase inicial, el atacante emite la señal falsa con una potencia muy baja y perfectamente sincronizada en fase y frecuencia con la señal satelital legítima. Progresivamente, el *spoofers* incrementa su potencia hasta superar ligeramente a la real, momento en el que el receptor víctima, diseñado para sintonizar la señal de mayor correlación, "salta" involuntariamente y se engancha a la señal falsa. Para

resumir este proceso se ha generado la Figura 2-9 en Matlab. Una vez capturado el bucle de seguimiento, el atacante introduce desviaciones sutiles y graduales en el retardo temporal de la señal; esto arrastra la solución de navegación del receptor hacia las coordenadas falsas deseadas sin provocar saltos bruscos que activen las alarmas de integridad del sistema [20].



La relevancia táctica de esta amenaza quedó patente en uno de los incidentes más controvertidos de la historia reciente de la defensa: la captura del dron estadounidense RQ-170 Sentinel por parte de Irán en 2011. Según los análisis posteriores, las fuerzas iraníes habrían empleado técnicas de *spoofing* para manipular el sistema de navegación del UAV, haciéndole creer que se encontraba sobre su base en Afganistán para forzar un aterrizaje automático en territorio hostil. Este evento marcó un punto de inflexión, demostrando que el *spoofing* podía utilizarse no solo para desorientar, sino para secuestrar plataformas autónomas avanzadas [21].

Asimismo, en el teatro de operaciones europeo, el informe del C4ADS ya citado documentó el uso masivo de *spoofing* para la protección de figuras VIP. Se registraron miles de casos en los que los receptores GNSS de buques en el Mar Negro situaban repentinamente su posición en aeropuertos terrestres a kilómetros de distancia (como el aeropuerto de Sochi o Gelendzhik), un efecto que resulta muy evidente como muestra la Figura 2-10. Esta técnica, conocida como círculo de defensa, busca desviar cualquier munición guiada por GPS o dron que intente acercarse al objetivo protegido, redirigiéndola hacia zonas seguras predefinidas [14].

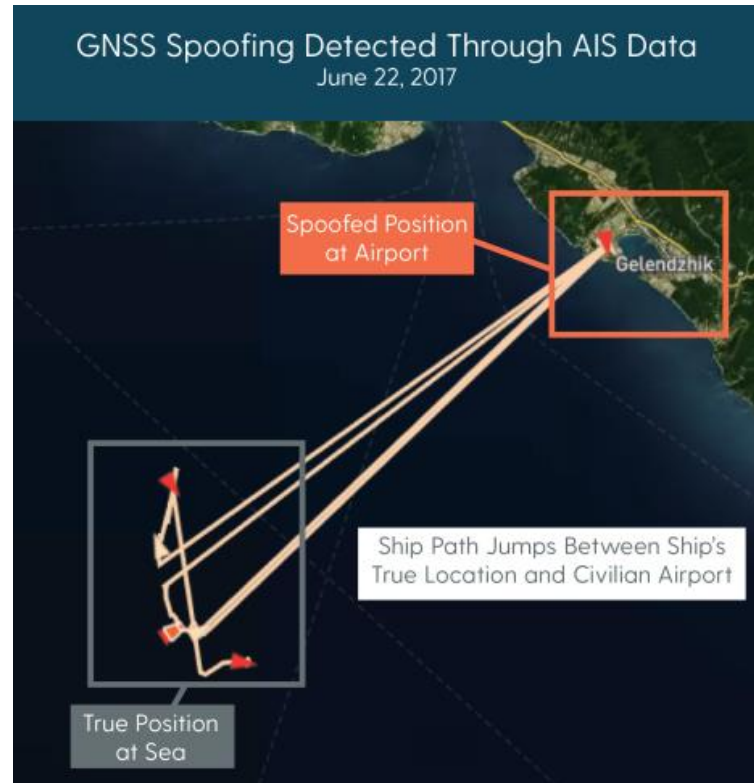


Figura 2-10 Presentación AIS tras ataque de *spoofing* en el Mar Negro [14]

2.3 Técnicas de Protección Electrónica mediante Antenas Anti-Interferencia

Frente a la creciente amenaza de la Guerra Electrónica de Navegación, la ingeniería de defensa ha desarrollado diversas contramedidas enmarcadas en la categoría de Protección Electrónica (EP). Si bien existen algoritmos de procesamiento de señal capaces de filtrar interferencias a nivel de receptor, la primera y más eficaz línea de defensa reside en el diseño de la antena [22]. El objetivo fundamental de estas soluciones de hardware es el filtrado espacial: modificar el diagrama de radiación de la antena para maximizar la ganancia hacia los satélites legítimos centrados generalmente en elevaciones medias y altas, afectando así al valor del DOP ya que se elimina la línea de visión con cierto número de satélites, y atenuar o anular la ganancia en la dirección de las amenazas que generalmente provienen del horizonte o cotas bajas [23].

A continuación, se describen las principales arquitecturas en uso.

2.3.1 Antenas de Patrón de Recepción Controlado (CRPA)

Consideradas el estándar de oro en aplicaciones militares de alto nivel, las CRPA (*Controlled Reception Pattern Antennas*) son sistemas activos compuestos tradicionalmente por un array de múltiples elementos radiantes (habitualmente entre 4 y 7 elementos) [22]. Mediante procesadores digitales de señal y algoritmos de formación de haces (*beamforming*) o anulación (*null-steering*), estas antenas pueden detectar dinámicamente la dirección de llegada de una interferencia y generar un "nulo" o zona ciega en su diagrama de radiación hacia ese punto específico.

El procesador digital de la antena aplica un peso complejo (w_k) a la señal recibida por cada elemento (x_k). La salida combinada del sistema (y) se puede expresar como:

$$y = \sum_{k=1}^N w_k * x_k(t)$$

Mediante algoritmos adaptativos, el sistema ajusta estos pesos (w_k) en tiempo real para que, al sumar las señales, la interferencia se cancele destructivamente (se suma en contrafase) mientras que la señal del satélite se mantenga constructiva. En el diagrama de la Figura 2-11 se aprecia como los nulos de la antena se orientan en la dirección de la señal a atenuar (representada de color rojo) mientras que la señal legítima (azul) siempre encuentra un valor elevado de ganancia.

Aunque son extremadamente eficaces permitiendo la anulación simultánea de múltiples fuentes de *jamming*, su elevado coste, consumo energético y complejidad de integración limitan su uso masivo, reservándose principalmente para plataformas de alto valor estratégico. Es así como se encontrarán instaladas en múltiples buques de guerra de marinas aliadas como el modelo GAJT-710MS™ de la empresa HEXAGON®, en cuya ficha técnica [24] asegura ser capaz de asegurar una protección de 40 dB frente a ataques de *jamming* gracias a su estructura CRPA y tecnología GAJT®

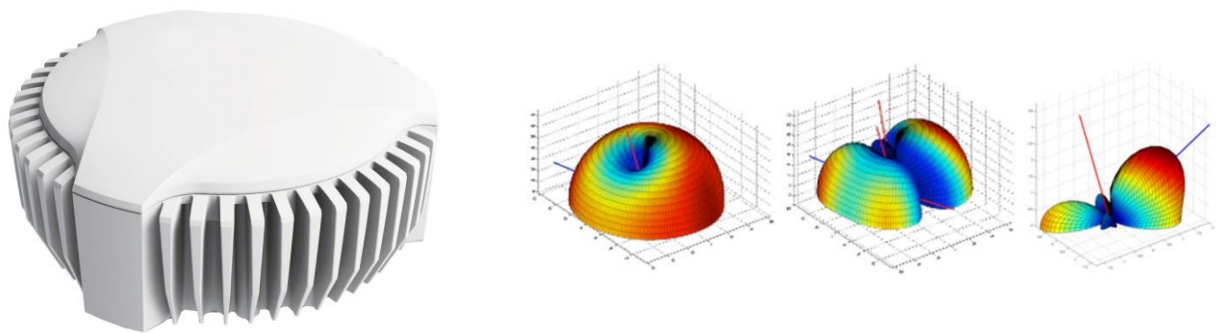


Figura 2-11 Antena GAJT-710MS™ [24] y *beamforming* frente a ataque [25]

2.3.2 Antenas LENA

Como una alternativa más eficiente y ligera a los arrays complejos, se encuentra la tecnología LENA (*Low Elevation Nulling Antenna*). Esta arquitectura se puede conceptualizar como una CRPA simplificada que utiliza únicamente dos elementos radiantes en lugar de un array múltiple [26].

El diseño típico de una LENA consiste en un par apilado de antenas helicoidales cuadrifilares. Al combinar las señales de estos dos elementos verticales, el sistema es capaz de generar un nulo profundo de 360° en el horizonte mediante la suma y cancelación de fases, sin necesidad de la compleja electrónica de formación de haces de un array de 7 elementos. Cuando el sistema detecta energía de interferencia por encima de un umbral, conmuta automáticamente a este "estado nulo", reduciendo drásticamente la ganancia (hasta -12 dBic) en ángulos de baja elevación (típicamente entre -5° y +15°), apreciable en el diagrama de la Figura 2-12, donde se sitúan la mayoría de las amenazas terrestres [26] [27].

Esta reducción a solo dos elementos permite a las antenas LENA ofrecer una protección robusta contra el *jamming* terrestre con un factor de forma mucho más compacto y un consumo de potencia reducido, haciéndolas ideales para plataformas donde el peso y el volumen son críticos.

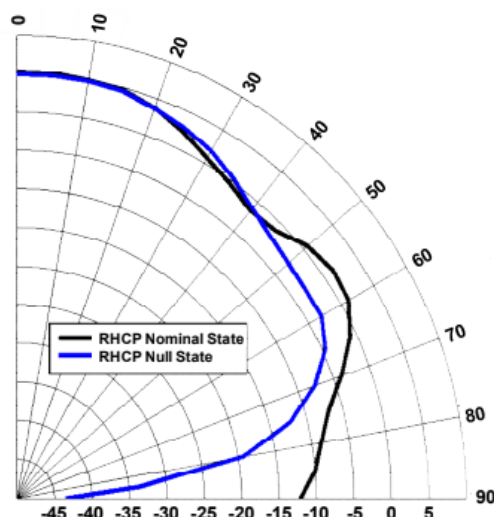


Figura 2-12 Diaframa de antena LENA en dBi [18]

2.3.3 Antenas Choke Ring

Originalmente diseñadas para aplicaciones geodésicas de alta precisión, estas antenas se caracterizan por estar montadas sobre una base metálica con surcos concéntricos de profundidad cuarto de onda ($\lambda/4$) de una señal GPS, entre 4 y 5 cm. Estos surcos se convierten en muros de impedancia infinita frente a estas señales gracias a su diseño. Aunque su propósito principal es mitigar el efecto *multipath* (rebotes de señal en estructuras o el suelo), su geometría física proporciona una atenuación natural significativa a las señales que llegan con elevaciones muy bajas o negativas [28].

En implementaciones modernas de alta gama, la arquitectura Choke Ring se combina a menudo con bancos de filtros de cavidad internos para proteger el LNA (*Low Noise Amplifier*) contra la saturación por señales fuera de banda [29]. Sin embargo, su gran tamaño y peso las hacen poco prácticas para vehículos aéreos o plataformas dinámicas ligeras.

Los datos técnicos representados en la Figura 2-13 auguran unas posibles ventajas tácticas más allá de sus originales funciones geodésicas.

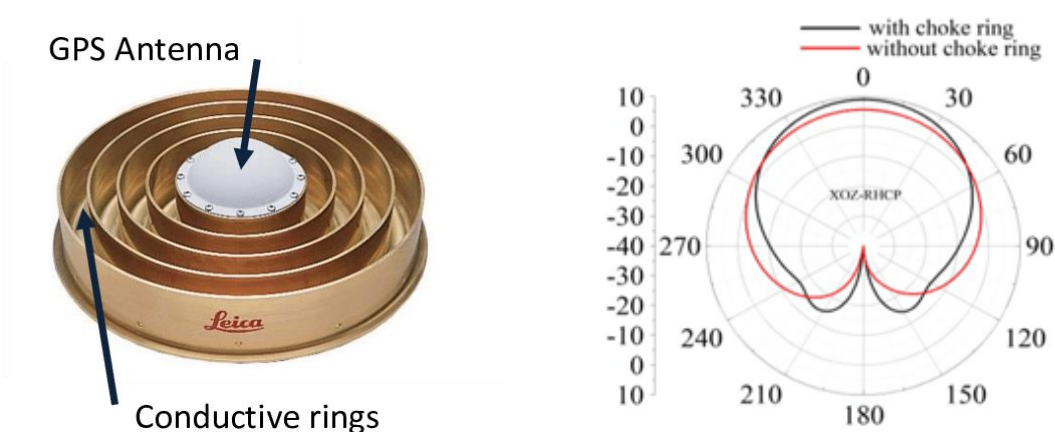


Figura 2-13 Antena Choke Ring comercial [30] y su diagrama característico [28]

2.3.4 Estructuras de Apantallamiento y Cavidades Resonantes

Como alternativa eficiente, económica y pasiva frente a los costosos sistemas adaptativos (CRPA), existen las técnicas de control físico del diagrama de radiación. Estas soluciones se basan en la instalación de estructuras mecánicas dedicadas, como cavidades cilíndricas o planos de tierra extendidos,

diseñadas para imponer una máscara de elevación artificial fija alrededor del elemento radiante obstruyendo de forma pasiva con la señal emitida por *jammers* y *spoofers* [31].



Figura 2-14 Apantallamiento improvisado en un buque mercante

La Figura 2-14 es uno de los múltiples ejemplos de cavidades improvisadas, cuyo principio operativo no es únicamente geométrico, sino electromagnético. Al situar la antena GNSS en el interior de una cavidad abierta superiormente, se busca modificar la ganancia de la antena para anular la recepción en ángulos de elevación bajos (cerca al horizonte, $0^\circ - 15^\circ$), que es el sector de llegada de la inmensa mayoría de las amenazas terrestres que ya se han discutido.

3 DESARROLLO DEL TFG

Conocida la amenaza a nuestras antenas de GNSS, y analizado el entorno de las señales RF se empieza a hacer evidente el camino a seguir por este estudio. Todos los sistemas *antijamming* siguen principios físicos y presentan funcionamientos diferentes, pero la premisa es la misma, reducir de manera considerable la ganancia en la dirección de las señales no deseadas. La cavidad que se busca dimensionar no es inteligente, como las antenas CRPA, por lo que la precisión del posicionamiento se verá degradada en cualquier escenario en el que se utilice. Es aquí donde entra el otro factor crucial del desarrollo, cuanta precisión se puede permitir perder una unidad frente a la protección que se le está proporcionando.

Antes de proseguir se debe establecer los valores que se consideran óptimos como resultado de esta investigación. En el primero de los campos, la protección, se considerará el objetivo cumplido si obtenemos una ganancia de la antena que ronde los -20dBi sobre el horizonte. Suponiendo un *jammer* de 1W, a una distancia de 1km, la pérdida de propagación en espacio libre a la frecuencia L1 (1575.42 MHz), ronda los 96dB y -20dBi de ganancia en el horizonte sería suficiente para atenuar críticamente esta señal frente a las señales satélite.

El segundo parámetro de diseño lo marca la necesidad de los buques de la Armada, fijando el error máximo de posición tolerable en 40 yardas (aproximadamente 36 metros). Asumiendo un valor típico de 5 metros para el Error de Rango Equivalente del Usuario (UERE), y sabiendo que el error posicional es el producto directo del UERE por la dilución geométrica (apartado 2.1.4), el sistema admitiría un factor de degradación máximo teórico de 7,2. Se establece aquí un máximo de DOP conservador de 6. Este valor establecerá cuál es la máscara de elevación máxima que imponga el blindaje.

Para alcanzar el objetivo final hay que empezar por la utilización de software de simulación. Mediante el uso de herramientas informáticas se obtendrán unas medidas idóneas para una protección. Una vez establecidas, estas dimensiones se tienen que enfrentar a una experimentación frente a antenas reales para poder obtener resultados empíricos que validen el uso y diseño del protector

3.1 Fundamentos Electromagnéticos del Apantallamiento Físico

Las cavidades protectoras ya han probado que funcionan en el ámbito de la Armada, donde oficiales de la fragata F-101 han corroborado su uso de forma efectiva. La cavidad basa su eficacia en la explotación de tres fenómenos físicos fundamentales

1. **Bloqueo de Línea de Visión (LOS):** Las paredes de la cavidad actúan como una barrera física opaca a la radiofrecuencia, impidiendo que la señal del atacante incida directamente sobre el parche cerámico de la antena.

2. **Efecto Pelicular (Skin Effect):** Cuando una onda electromagnética incide sobre un buen conductor, la corriente inducida decae exponencialmente a medida que penetra en el material, este comportamiento se conoce como efecto pelicular, y es especialmente importante para ondas electromagnéticas de alta frecuencia (caso de las señales GNSS). La distancia a la cual la densidad de corriente se reduce al 37% de su valor superficial se denomina profundidad de penetración (δ). A la frecuencia de operación de 1.575 GHz (L1), esta profundidad es microscópica, aproximadamente 2.1 micrómetros para el aluminio, 1.6 micrómetros para el cobre y menos de 0.5 micrómetros para aleaciones de acero (debido a su alta permeabilidad magnética). Según la teoría de propagación en medios con pérdidas, a una profundidad de 3δ , la onda ha perdido prácticamente toda su energía por absorción. Por lo tanto, cualquier estructura metálica sólida es electromagnéticamente opaca y proporciona niveles de atenuación teóricos superiores a los 100 dB. Tal y como establece en el texto de referencia "Microwave Engineering" de David M. Pozar, específicamente en el apartado de ondas planas en buenos conductores [32], en el diseño de blindajes de microondas el grosor del metal deja de ser un factor crítico; las verdaderas vulnerabilidades del sistema nunca provienen de la transmisión a través del material, sino exclusivamente de las fugas por discontinuidades, ranuras o difracción en los bordes de la geometría. Este establece la principal razón detrás del funcionamiento de los blindajes GNSS.
3. **Atenuación por Difracción:** Según la Teoría Geométrica de la Difracción (GTD), las ondas electromagnéticas que inciden en el borde superior del cilindro sufren una difracción que curva la señal hacia el interior de la cavidad. Sin embargo, esta señal difractada llega al elemento radiante con una atenuación severa. El diseño propuesto en este TFG busca maximizar esta atenuación optimizando la altura y el radio de la cavidad [33]. Este fenómeno se abordará a continuación.

En cuanto a su construcción, la viabilidad de estas protecciones depende críticamente de los materiales empleados, existiendo dos vertientes de diseño:

- **Cavidades Conductoras (PEC):** Cilindros metálicos (aluminio o cobre). Son sencillos de fabricar y generan un bloqueo excelente, pero presentan el riesgo de generar reflexiones internas (*multipath*) que podrían degradar la señal legítima si las dimensiones no son resonantes con la frecuencia L1.
- **Cavidades Absorbentes (RAM):** Recubren la pared interior con Material Absorbente de Radar (RAM) sintonizado a 1.5 GHz. Esta solución es superior, ya que no solo bloquea la amenaza externa, sino que absorbe cualquier rebote interno, "limpiando" la señal recibida [34].

Aunque menos sofisticadas que las soluciones electrónicas activas, las protecciones pasivas son una solución real, altamente viables y utilizada actualmente en infraestructuras críticas y entornos militares. Sin embargo, un uso desmedido y no calculado de estas protecciones físicas puede llegar a degradar la propia señal recibida o incluso no proteger la antena frente a un aumento de la efectividad de las interferencias por una geometría inadecuada.

3.1.1 Limitaciones electromagnéticas del apantallamiento

En el diseño de sistemas de protección pasiva contra interferencias electromagnéticas, resulta muy simple modelar la propagación de la señal asumiendo los principios de la óptica. Suponiendo estos principios las ondas se propagan en línea recta, y cualquier obstáculo físico opaco genera una región de sombra absoluta tras de sí. Sin embargo, la óptica geométrica solo es válida cuando la longitud de onda de la señal es de una magnitud notablemente inferior en comparación con las dimensiones del obstáculo, tendiendo la primera a 0.

En el contexto de los sistemas de navegación por satélite (GNSS), la señal portadora de la banda L1 posee una longitud de onda de aproximadamente 19cm. A esta escala, las dimensiones de los sistemas de apantallamiento táctico son del mismo orden de magnitud que la propia longitud de onda. En este

régimen, las leyes de la óptica clásica no son aplicables y los efectos de difracción pasan a ser el fenómeno dominante en los contornos de la estructura [33].

El fenómeno específico que rige la entrada de una señal electromagnética en la región de sombra del obstáculo se conoce como difracción de borde o arista (*knife-edge diffraction*). La base matemática para modelar este comportamiento fue sentada por Joseph B. Keller mediante la Teoría Geométrica de la Difracción (GTD) [35], y posteriormente perfeccionada para superficies conductoras por Kouyoumjian y Pathak mediante la Teoría Uniforme de la Difracción (UTD) [36].

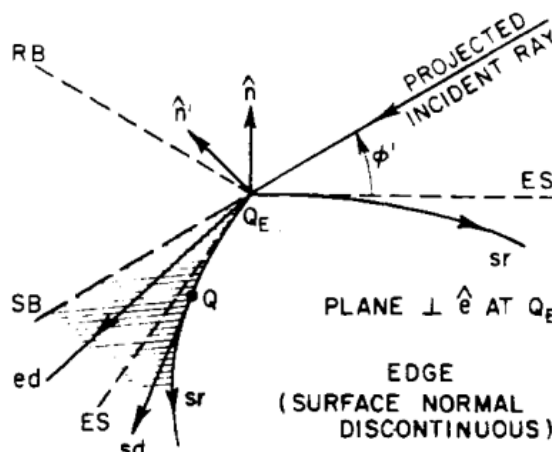


Figura 3-1 Rayos incidentes, reflejados, difractados, y otros fenómenos asociados [35]

Siguiendo la esquematización en la Figura 3-1, se aprecia como cuando un frente de onda incidente impacta con la arista superior de una pared metálica conductora, no se refleja en su totalidad. En su lugar, el borde iluminado excita corrientes superficiales y actúa como una fuente secundaria que radia energía nuevamente en forma de un frente de onda cilíndrico [36]. Una fracción de esta onda difractada se introduce directamente hacia el interior del obstáculo.

Para la ingeniería de sistemas *anti-jamming*, la consecuencia directa de la difracción de borde es la imposibilidad física de alcanzar un aislamiento infinito utilizando únicamente pantallas. La onda difractada impone un límite a la atenuación que la cavidad puede ofrecer frente a ataques procedentes del horizonte.

3.2 Software Empleado

3.2.1 Matlab

. Para la realización de la totalidad de las simulaciones presentadas en este trabajo, se ha seleccionado MATLAB como entorno principal de desarrollo. MATLAB (*Matrix Laboratory*) es una plataforma de cálculo numérico y programación de alto nivel, considerada el estándar industrial en ingeniería de telecomunicaciones y aeroespacial para el desarrollo de algoritmos, análisis de datos y modelado de sistemas.

La elección de MATLAB frente a otras alternativas de simulación electromagnética pura (como CST Studio o HFSS) o lenguajes de programación de propósito general (como Python o C++) se defiende por su capacidad de integrar con facilidad diferentes conceptos de manera sencilla y rápida de aprender. En especial la relativa sencillez de integrar conceptos orbitales con estructuras físicas.

Esta necesidad de conectar la mecánica orbital (cálculo de constelaciones), el electromagnetismo (diseño de la antena y el cilindro) y el procesamiento digital de señal (análisis de *jamming* y *spoofing*) no hubiese sido fácil de plantear en plataformas en las que carecemos de experiencia. MATLAB permite

simular la física de la antena y, en el mismo script, utilizar su diagrama de radiación resultante para calcular métricas de navegación como el PDOP, algo que sería extremadamente complejo de automatizar combinando software de diseño 3D con scripts externos.

Es también especialmente útil a la hora de construir representaciones gráficas. mapas de calor 3D para la optimización de la cavidad, diagramas de radiación volumétricos y análisis espectrales complejos sin necesidad de herramientas de post-procesado externas.

3.2.2 GNSS Planner

Para el estudio de la viabilidad geométrica del apantallamiento, se ha recurrido a la herramienta de planificación *Trimble GNSS Planning*. Esta plataforma profesional permite simular la disponibilidad de las distintas constelaciones satelitales (GPS, Galileo, GLONASS, BeiDou) en cualquier coordenada geográfica y en una ventana temporal específica, basándose en los almanaques orbitales actualizados.

En el contexto de este trabajo, el software de Trimble resulta fundamental para evaluar la principal desventaja táctica del cilindro protector, la restricción del campo de visión de la antena. Mediante esta herramienta, es posible forzar por *software* la aplicación de la máscara de elevación artificial generada por las paredes de la cavidad geométrica. Su capacidad de establecer parámetros particulares (Figura 3-2) facilita realmente la visualización y evaluación de resultados, así como la calidad del estudio.

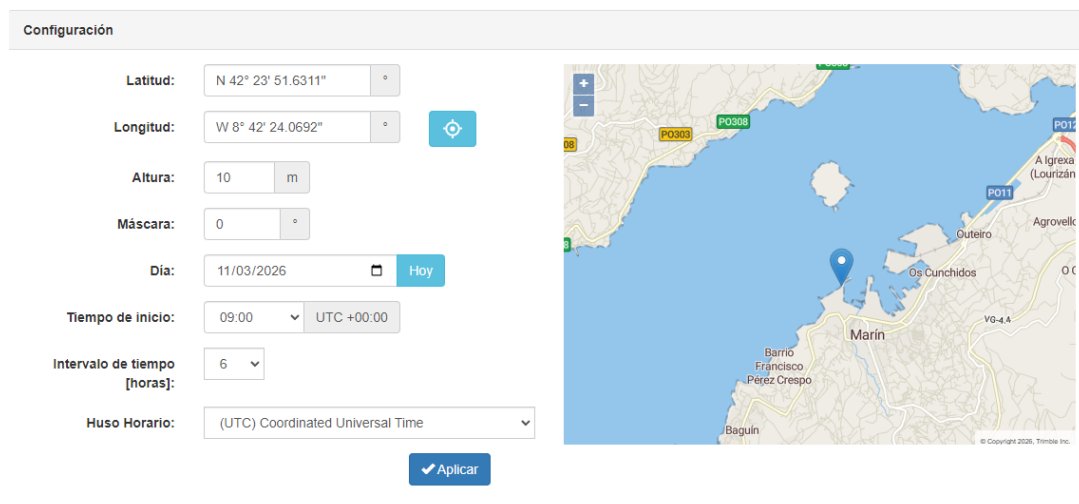


Figura 3-2 Captura de pantalla de la interfaz de Trimble

3.2.3 U-Center

Para la fase de experimentación y validación física del prototipo, se ha empleado el software *u-center* desarrollado por la compañía suiza *u-blox*. Se trata de un entorno de evaluación de receptores GNSS de grado industrial que permite la monitorización, configuración y análisis exhaustivo de las tramas de datos NMEA y UBX en tiempo real.

El papel de *u-center* en este proyecto es actuar como el instrumento de medida para cuantificar la eficiencia real del blindaje. Durante las pruebas con el hardware físico, la interfaz proporciona acceso directo a las métricas del receptor

3.3 Diseño y simulación computacional

Abordar el diseño del blindaje mediante el método de prueba y error carece del rigor científico necesario en ingeniería de radiofrecuencia. Para evitar los problemas de interferencia que generan las soluciones improvisadas actuales (basadas en el uso de contenedores metálicos de dimensiones

aleatorias), el primer paso de este estudio consistirá en modelar una antena GNSS genérica a partir de la cual se acabarán obteniendo unas dimensiones óptimas de la cavidad.

3.3.1 Diseño de la antena GNSS

Para evaluar el impacto de las estructuras de protección frente a interferencias (*jamming*), el primer paso del desarrollo consistió en modelar un receptor GNSS representativo. Se optó por diseñar una antena de parche *microstrip* sobre sustrato cerámico, ya que es la topología estándar utilizada en la inmensa mayoría de los receptores GPS comerciales y marítimos en la banda L1 (1575.42 MHz), debido a su bajo perfil, bajo coste y robustez. El código utilizado en Matlab es el primero que se recoge en el Anexo IV.

Tal y como se represente en la Figura 3-3, la estructura física de la antena de parche está constituida por dos elementos fundamentales: un plano de masa inferior metálico de color verde y un parche conductor superior visto de color naranja, responsable de la radiación.

El elemento crítico de este diseño es el sustrato dieléctrico. En lugar de utilizar materiales convencionales como FR4 ($\epsilon_r = 4.4$), se ha seleccionado una cerámica de alta permitividad $\epsilon_r = 20$ con un espesor de 4mm. La elección de una alta constante dieléctrica permite la miniaturización de la antena, ya que la longitud de onda guiada (λ_g) se reduce significativamente según la relación:

$$\lambda_g = \lambda_0 / \sqrt{\epsilon_{eff}}.$$

Se obtiene así un parche cuadrado de dimensiones reducidas (aprox. 30x30 mm), ideal para aplicaciones embarcadas donde el espacio es limitado.

Para la alimentación, se ha configurado una alimentación coaxial (*probe feed*) desplazado a la diagonal del parche. Esta ubicación estratégica excita dos modos ortogonales con un desfase de 90°, generando la Polarización Circular a Derechas (RHCP) necesaria para maximizar la recepción de los satélites GPS y mitigar las pérdidas por desalineación de polarización.

Durante la etapa de simulación electromagnética, mediante el Método de los Momentos (MoM) en MATLAB, se identificaron y subsanaron dos problemas críticos que condicionaron el código final:

El error de frecuencia de resonancia (Efecto de Bordes) fue el principal obstáculo de esta simulación. Inicialmente, se dimensionó el parche utilizando las fórmulas teóricas básicas de la línea de transmisión. Sin embargo, la primera simulación arrojó una resonancia centrada en 1.37 GHz en lugar de los 1.575 GHz deseados. Este desplazamiento se debe a que las fórmulas teóricas ideales no modelan con total precisión los "campos de borde" en sustratos gruesos y de alta permitividad. Para solucionarlo se implementó un factor de corrección empírico en el script basado en la relación entre la frecuencia obtenida y la deseada ($1.37/1.575 = 0.87$). Esto permitió reescalar las dimensiones físicas del parche (L y W) y la posición del alimentador para centrar la resonancia exactamente en la portadora GPS sin necesidad de iteraciones infinitas.

El segundo gran obstáculo que apareció fue una saturación de los recursos computacionales debido al mallado. El uso de un dieléctrico con $\epsilon_r = 20$ reduce drásticamente la longitud de onda en el interior del material produciendo que el motor de mallado automático de MATLAB intente discretizar la antena en elementos infinitesimales (submilimétricos) para cumplir con el criterio de precisión estándar, generando cientos de miles de incógnitas que desbordaban la memoria RAM disponible, provocando el bloqueo del sistema. Para solucionarlos forzamos un mallado manual controlado (*mesh* con *MaxEdgeLength* fijado a 3.5 mm). Esta técnica de "baja poligonización" reduce la carga computacional en varios órdenes de magnitud, permitiendo obtener el diagrama de radiación en segundos con una precisión más que aceptable para validar la ganancia y la directividad, evitando el colapso del simulador.

La antena resultante, tras aplicar las correcciones, presenta un diagrama de radiación típico de una antena de parche, con un lóbulo principal dirigido al cenit (perpendicular a la superficie) y una ganancia

directiva adecuada. Este modelo, validado y optimizado computacionalmente, sirve como el "excitador base que posteriormente será integrado dentro de las estructuras de protección cilíndrica en los apartados siguientes. El resultado inicial aparece en la Figura 3-3 junto al mallado del parche.

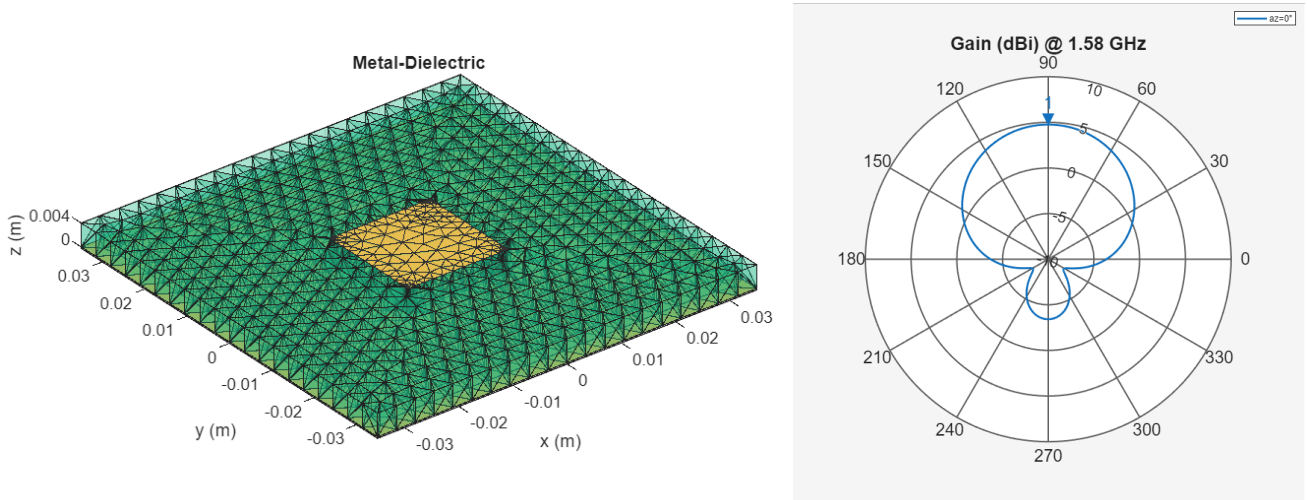


Figura 3-3 Modelado y diagrama de radiación de la antena de parche cerámico

3.3.2 Dimensiones óptimas frente a protección

Una vez definido el elemento radiante como parche cerámico, el siguiente paso crítico es dimensionar la cavidad cilíndrica para maximizar la relación de protección. El objetivo no es simplemente bloquear la visión geométrica, sino maximizar la diferencia de ganancia entre la señal deseada (satélite en el cenit, $\theta = 0^\circ$) y la señal interferente (*jammer/spoofer*) en el horizonte o a baja elevación ($\theta = 80^\circ - 90^\circ$).

Para evitar un diseño basado en prueba y error, y poder obtener un resultado visual, se implementó en MATLAB el segundo script del Anexo IV de barrido paramétrico (se combinan en orden elementos de dos grupos de valores probando así todas las combinaciones), iterando entre dos variables de diseño:

- Radio (R): Variando desde 4 cm (muy ajustado pensando en la placa) hasta 30 cm.
- Altura (H): Variando desde 2 cm hasta 30 cm.

El algoritmo simula todas las combinaciones posibles ($R \cdot H$) y evalúa cada geometría mediante una Figura de Mérito (FoM) personalizada, definida como:

$$FoM = G(cenit) - G(amenaza)$$

Donde $G(cenit)$ es la ganancia hacia el satélite y $G(amenaza)$ es la ganancia hacia un ataque proveniente desde 0° , 5° y 10° sobre el horizonte, siendo los rangos de 0 a 5 grados los que más interesan. El script penaliza drásticamente cualquier diseño que, por ser demasiado profundo o estrecho, bloquee la visión del satélite ($G(cenit) < 0$ dBi).

Durante el análisis, se hace evidente que la solución puramente geométrica ($\tan(\alpha) = H/R$) es insuficiente. Las simulaciones de onda completa mostraron que las ondas electromagnéticas no se detienen abruptamente en el borde metálico del cilindro, sino que sufren difracción en el borde (*edge diffraction*). Esto genera depresiones en el diagrama de radiación y permite que parte de la energía del *jammer* sea capaz de esquivar la pared del cilindro incluso si geométricamente no debería tener línea de visión. Este comportamiento físico justificó la necesidad de la simulación demostrándose que para obtener una atenuación efectiva de >15 dB en ángulos rasantes, la altura física del cilindro debía ser mayor a la calculada geométricamente para compensar el efecto de difracción.

El resultado del barrido generó un mapa de calor que permitió identificar unas zonas óptimas; aquellas con un compromiso donde el radio es suficiente para no desintonizar la antena (aprox. 10.5 cm)

y la altura (aprox. 18cm) proporciona la máxima inmunidad sin convertir el sistema en una guía de onda profunda que atenúe la señal GPS. El estudio de la idoneidad de la solución en términos de la precisión de posicionamiento, será un tema que se abordará posteriormente en la Memoria.

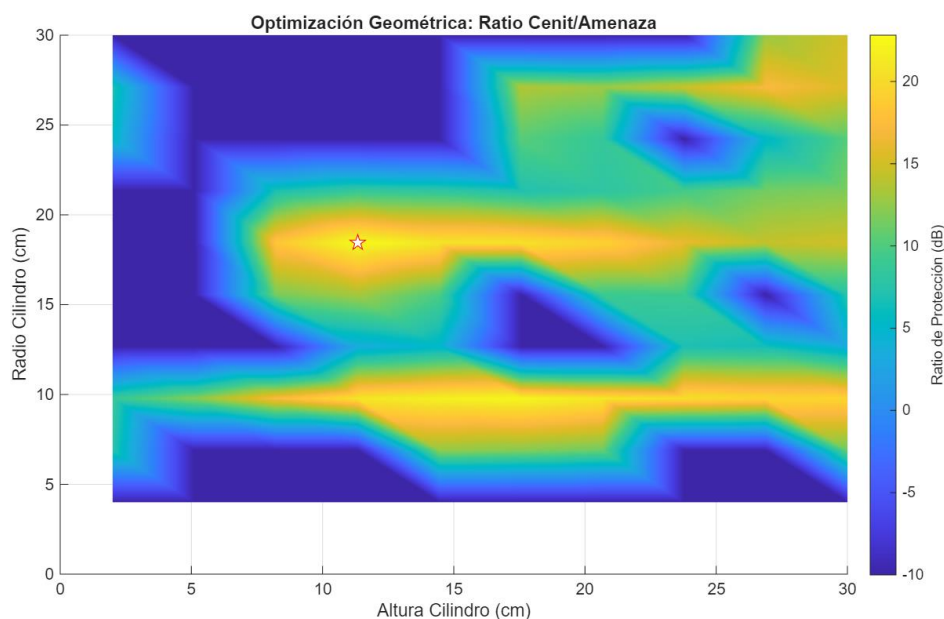


Figura 3-4 Mapa de protección frente a radio y diámetro respecto a un ataque del horizonte

La obtención del mapa de calor de la Figura 3-4 da pie a las primeras hipótesis e ideas de diseño. Las marcadas líneas horizontales demuestran que, tanto la altura como el radio, son importantes para determinar el grado de protección. En dicha figura se observa que las líneas horizontales coinciden con aquellas configuraciones en las que el diámetro de la cavidad es múltiplo de media longitud de onda, es decir, en la banda L1 aproximadamente 9.5 cm.

Durante la realización de esta experiencia ha surgido la pregunta ¿es crucial el grosor de la cavidad para su diseño? La respuesta es negativa tal y como comentó en el apartado 2.1.4 cuando se presentaba el concepto de profundidad de penetración. A frecuencias de microondas, como es el caso de la banda L1, las corrientes inducidas por una onda electromagnética incidente no penetran en el material, sino que se concentran en su superficie exterior. La profundidad de penetración (δ), (recuerde aproximadamente un 37%), es de apenas unos $2\mu\text{m}$ para buenos conductores como el aluminio o el cobre [37] [32]. Dado que la atenuación de transmisión se considera prácticamente total (comportamiento de conductor eléctrico perfecto) al superar unas cinco veces dicha profundidad (0.01mm), cualquier plancha metálica comercial superior a 0.01mm bloquearía la onda incidente por completo. Es fácil de concluir que el análisis matemático del grosor no aporta ningún valor a este estudio, y su elección se definirá en función a disponibilidad y facilidad de mecanizado.

3.3.3 Efecto de la protección sobre el DOP

Es en este punto que el proyecto adquiere una distinción y estudio especialmente relevante. Cualquiera es capaz de colocar una antena dentro de una lata y protegerse de los ataques de pequeña entidad; pero es en este punto que el razonamiento táctico entra en juego y se vuelve obligatoria la evaluación de cuanta precisión están dispuestas a perder las unidades. El auténtico valor del proyecto es encontrar el punto de trabajo donde se cumplen las dos necesidades de protección y precisión.

Primero se busca encontrar un valor de la máscara límite, en un escenario concreto, que permita mantener una situación con la precisión que requieren las distintas operaciones navales. El objetivo del análisis es evaluar la evolución del PDOP en función del ángulo de corte impuesto por el cilindro (θ_{mask}). El PDOP permitirá estimar un valor de la incertidumbre final en la posición 3D; un valor bajo indica una geometría robusta, mientras que un valor alto implica una solución de navegación inestable.

La simulación, realizada con el tercer código del Anexo IV se configuró con los siguientes parámetros:

- Escenario: Ubicación del receptor en Marín (42.39°N, 8.70°W), altitud 10 m.
- Datos de Constelación: Se utilizó un archivo de almanaque YUMA correspondiente a una semana activa real, permitiendo propagar las órbitas de los satélites de la constelación de GPS operativos mediante el modelo simplificado IS-GPS-200. Los almanaques en formato YUMA son archivos de texto estructurado que contienen los parámetros orbitales aproximados y el estado de salud de toda y únicamente la constelación GPS; se utilizan para aproximar a medio plazo su propagación. Es decir, se utilizan para analizar sus futuras posiciones y estimar en este caso su visibilidad respecto la antena a la hora de usar la protección y a partir de la distribución se obtiene el PDOP.
- Ventana Temporal: Se simuló un periodo de 24 horas con una resolución temporal de 10 minutos, asegurando la evaluación de todas las configuraciones geométricas posibles de la constelación.
- Variable de Diseño: El ángulo de máscara (θ_{mask}) se varió desde 0° (visibilidad total) hasta 80° en pasos de 2°.

Para cada elevación de máscara y unidad de tiempo se harán los siguientes cálculos:

1. Cálculo de las coordenadas topocéntricas (Azimut y Elevación) de todos los satélites.
2. Filtrado de satélites cuya elevación es inferior a (θ_{mask}). (simulación del bloqueo físico).
3. Construcción de la Matriz de Diseño H con los satélites visibles ($n \geq 4$)
4. Cálculo de la Matriz de Covarianza $Q = (H^T H)^{-1}$ y extracción del valor de PDOP.

Este resultado devuelve un valor máximo de máscara permitido que, introduciendo en las primeras figuras de estudio de dimensiones, derivará en la obtención de un rango de valores admisibles de dimensiones.

El límite del PDOP como se especificó al principio del apartado será establecido en 6. Esta será la máxima degradación que se le permitirá ejercer sobre la distribución orbital a la protección. No es un número inventado, se ha establecido a partir de 2 parámetros que se han seleccionado en la introducción del apartado 3 como norma. El error máximo en el posicionamiento, que por doctrina ha de ser en torno a 40 yardas, reduciéndose en el caso de fuego a tierra con 25m para misiles y 5m para fuego naval de apoyo, y el $\sigma UERE$ que para una constelación GPS como se ha dicho anteriormente ronda los 5m. El resultado presentado en la Figura 3-5 establece una máscara de 27 ° como el límite operativo. Se empieza asumiendo que esta máscara es puramente física, pero con el avance del estudio se verá como bloqueos físicos superiores a este en ningún caso ejercen una máscara de tal magnitud.

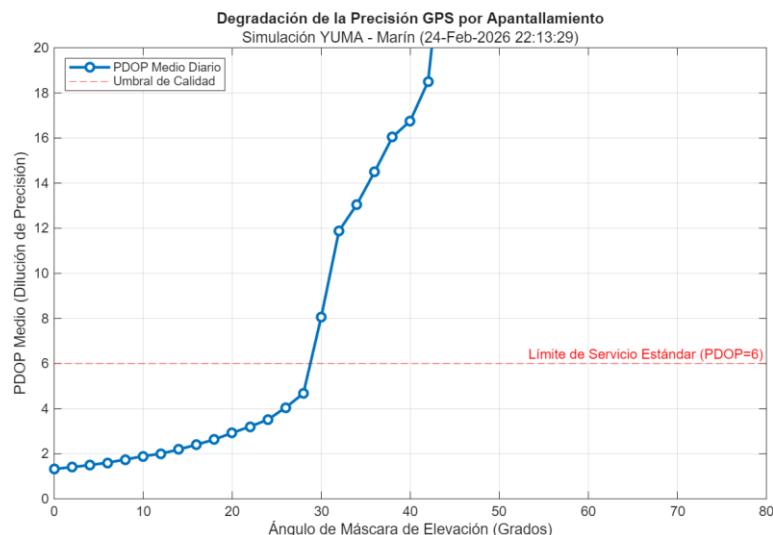


Figura 3-5 Evolución del PDOP frente a la máscara

Otro estudio del PDOP se hace evidente y es que este no es un valor que se mantiene constante con el paso de las horas. Lo que sí que se mantiene con el paso del tiempo es un rango de variación máximo, y es necesario ver como este rango de variación se puede llegar a ver afectado por la introducción de una protección física.

El objetivo principal de esta simulación es dar valores y analizar numéricamente el impacto que tiene la incorporación de la cavidad cilíndrica sobre el rendimiento del receptor GNSS. El diseño de protecciones físicas contra *jamming* implica un compromiso de diseño evidente y es que, al crear una barrera electromagnética para bloquear las interferencias procedentes del horizonte, se bloquea inevitablemente la línea de visión (LoS) de los satélites legítimos que se encuentran en ángulos de elevación bajos.

Para evaluar cómo esta reducción del campo de visión afecta a la precisión geométrica del sistema, se ha analizado la variación del parámetro PDOP a partir del cuarto script del Anexo IV. La simulación se ha llevado a cabo propagando las órbitas de la constelación GPS durante un periodo continuo de una semana (168 horas). Se ha establecido el receptor en un escenario táctico marítimo real, concretamente en el Mar Báltico, con coordenadas $57.5^{\circ}N$ $19.5^{\circ}E$. Las coordenadas no se seleccionan al azar y se aprovecha cualquier oportunidad para darle un toque de realismo. En este caso situando el supuesto receptor en una de las zonas geográficas donde más casos de *jamming* se dan, en las proximidades de Kaliningrado, donde buques de la Armada y han experimentado estos ataques.

Para garantizar el rigor y una correcta simulación orbital, los cálculos geométricos se han alimentado nuevamente de archivos de almanaque en formato YUMA. La elección de este estándar en formato texto permite extraer los parámetros keplerianos de toda la constelación GPS y propagar sus posiciones mediante algoritmos propios basados en la normativa oficial IS-GPS-200. De este modo, se evita la dependencia de *software* de simulación comercial y teniendo un control absoluto los cálculos matemáticos del PDOP.

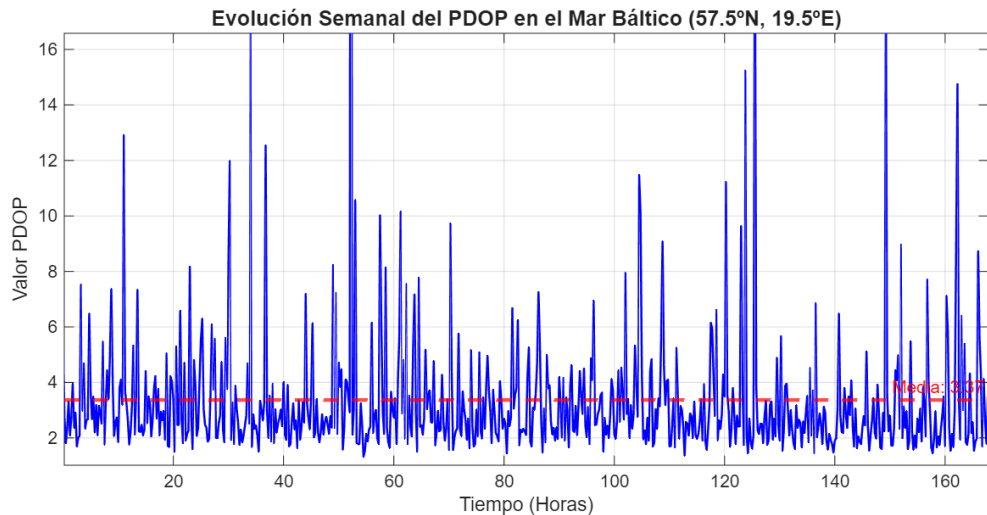


Figura 3-6 Evolución del PDOP a lo largo de una semana en antenas sin protección física

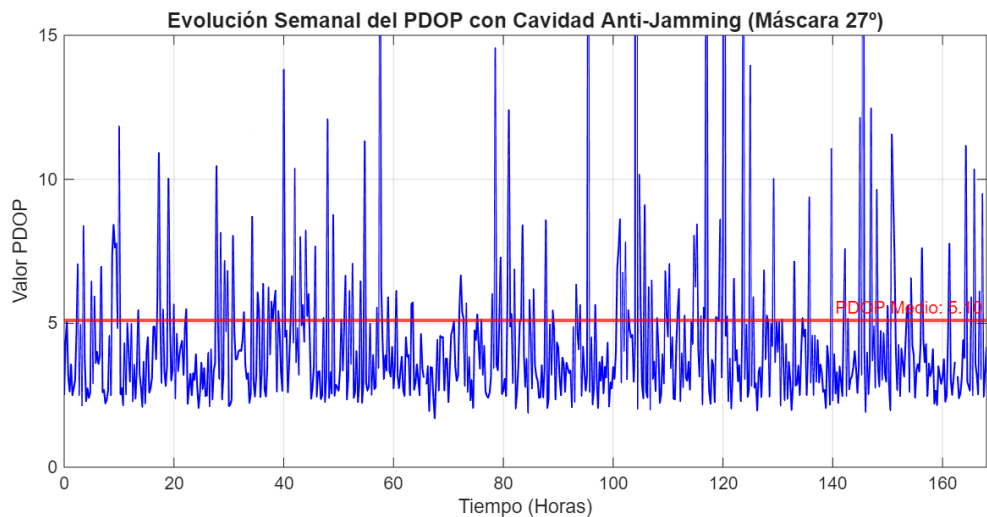


Figura 3-7 Evolución del PDOP a lo largo de una semana en antenas con protección física

A la luz de los resultados de la Figura 3-6 y la Figura 3-7 se hace evidente, y de forma muy visual, el coste geométrico del uso de una protección física.

En el que se puede llamar escenario nominal (Figura 3-4), se aprecia una evolución notablemente estable y periódica centrada en 3.37 con un límite superior que ronda 5 descontando los picos, y un límite inferior más evidente que no baja en ningún caso de 1.5. En el segundo escenario *anti-jamming* (Figura 3-5), como era de esperar al perder una sección considerable de LoS con la bóveda celeste, sube la media a un PDOP de 5.10. Un primer resultado positivo ya que se aproxima al valor dado en el apartado anterior. El nuevo límite inferior vuelve a ser fácilmente reconocible en un caso ligeramente peor de $PDOP=2$ y un límite superior que obviando los repuntes se estabiliza en 6.5. Se puede concluir y forma francamente positiva que en ambos casos el rango se mantiene en 4.5, aunque es reseñable destacar que los picos de degradación en la precisión son más frecuentes con el uso de la cavidad cilíndrica.

Los puntos máximos de degradación llaman la atención y parecen muy preocupantes a primera vista. Es un fenómeno que no depende de la protección ya que se encuentran también en el caso nominal. Este fenómeno se entiende como un colapso del tetraedro orbital, dicho de otra forma, la agrupación excesiva de satélites respecto al cenit. Se genera así la matriz de diseño H mal condicionada que amplifica matemáticamente el error de posicionamiento de forma exagerada. Este fenómeno natural se ve agravado por la pérdida de LoS con los satélites por debajo de los 27° , no especialmente en magnitud, pero en frecuencia, haciendo que la degradación se produzca en mayor número de ocasiones.

Las consecuencias se reducen a los siguientes casos:

- **Degradación del valor medio:** El PDOP medio de la semana asciende a un valor de 5.0. Esto implica que el error de posicionamiento estimado en condiciones normales será aproximadamente el doble que sin la cavidad.
- **Aparición de picos críticos:** A lo largo de las horas de simulación, la pérdida de satélites bajos provoca momentos de mala geometría, disparando el valor del PDOP y provocando la aparición de más picos que en una situación nominal.

A partir de las simulaciones hay que sacar una serie de conclusiones a mantener durante el avance del proyecto. A pesar de la evidente degradación de la geometría que afecta directamente a la precisión, al aumentar la media del PDOP y los picos de degradación, este resultado se considera lo que se denomina un compromiso operativo exitoso. En un entorno marítimo hostil como el que hemos querido suponer el Báltico, la alternativa a no llevar la cavidad no es tener un PDOP excelente de 3.25, sino sufrir una denegación de servicio total debido al *jamming*, o incluso en el peor de los casos, sufrir un ataque de *carry-off* navegando a merced de fuerzas hostiles.

Por tanto, sacrificar precisión milimétrica a cambio de asegurar la continuidad de la navegación mediante una máscara de 27° demuestra ser una solución táctica viable y altamente recomendable para embarcaciones que operan en zonas de guerra electrónica.

3.3.4 Diseño teórico de la cavidad

A lo largo de las simulaciones se han ido obteniendo ciertos valores de protección y dilución de la precisión que se han tenido que interpretar. Para obtener unas dimensiones de la estructura de apantallamiento, hay que compaginar una adecuada protección frente a ataques con una precisión propia de la conducción de operaciones navales. Para encontrar este punto de trabajo óptimo se combinan los resultados del mapa de calor del ataque desde el horizonte con el valor de la máscara máxima operativa.

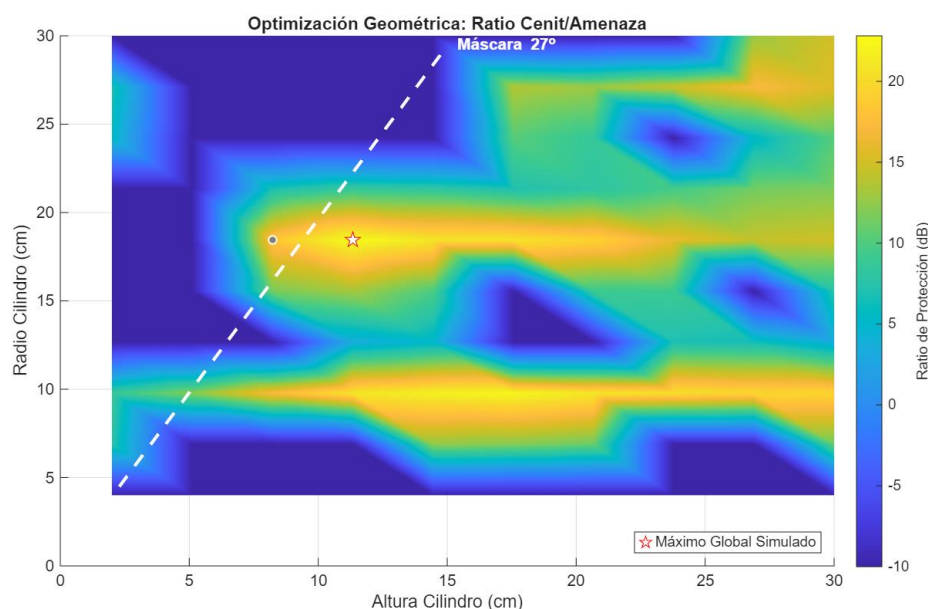


Figura 3-8 Combinación de experiencia de protección y máscara

A la izquierda de la línea de puntos en la Figura 3-8 quedan todos aquellos valores para los que el cilindro presenta dimensiones compatibles con un $\text{PDOP} \leq 6$. De entre ellos es necesario ajustarse a los que ofrezcan las mejores condiciones de protección.

Es este punto donde se cambia el enfoque y se salta de las simulaciones en MATLAB a la experimentación con antenas reales. El cambio se hace partiendo de lo que aparenta ser una base sólida; un rango de altura de 8,3 a 9,2 cm y un diámetro que puede variar entre 18,3 y 18,4 cm. Para este pequeño

intervalo la protección oscila entre los -20 y -27 dB siendo máximo en el punto de intersección con la máscara, por lo que se intentará aproximar este valor lo máximo posible.

3.3.5 Comprobación teórica de la cavidad

El objetivo principal de esta última fase de simulación computacional ha sido validar de forma estricta el comportamiento electromagnético de la cavidad con las dimensiones físicas definitivas ($R = 18.4\text{cm}$, $H = 8.2\text{cm}$), estableciendo un valor de 24° para la máscara provocada por la protección física. Hasta este punto, la optimización había sugerido estas cotas como el punto de equilibrio ideal, pero resultaba necesario antes de pasar a la experimentación con un prototipo real, comprobar cómo se ve afectado el patrón de radiación de la antena implementando el quinto código de Matlab del Anexo IV.

Adicionalmente, desde el punto de vista computacional, la simulación de una estructura metálica de 36.8cm de diámetro a frecuencias de microondas de L1 supone un reto de procesamiento por la elevada cantidad de elementos finitos requeridos. Por ello, el código desarrollado implementa una estrategia de mallado adaptativo manual, frente al automático que daba ciertos errores y consumía gran cantidad de memoria RAM nuevamente. Esta técnica permite resolver las ecuaciones de Maxwell y obtener el diagrama de radiación con alta fidelidad.

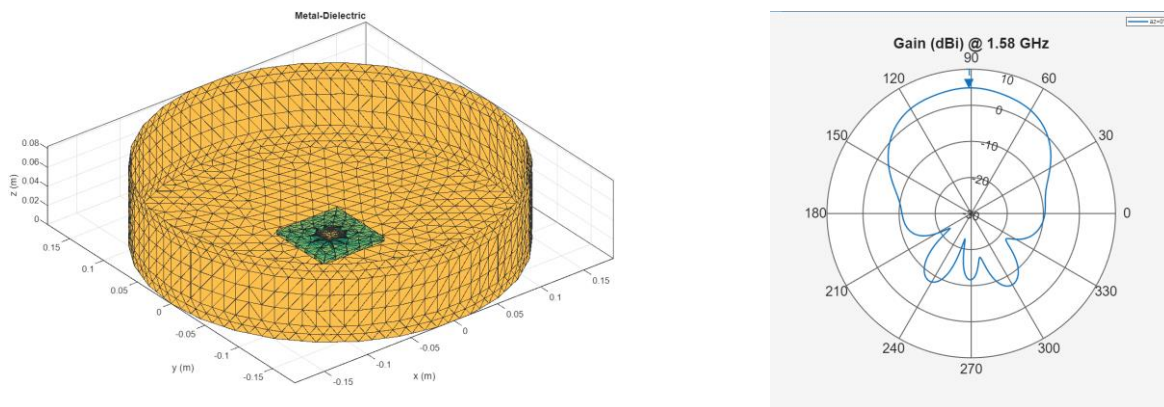


Figura 3-9 Representación y diagrama de radiación del conjunto cavidad antena

Tras la ejecución del código la primera reacción podría ser decepcionante. Frente a los -20dB que se estimaba de atenuación en el horizonte, el diagrama de la Figura 3-9 estima una atenuación total de -10dB, francamente menor. Este resultado no es un fallo del diseño, y su explicación reside en la física de las ondas de esta magnitud.

A 1.575 GHz la longitud de onda de la señal GPS es del mismo orden de magnitud que las dimensiones de la cavidad. Por lo tanto, la señal interferente no se comporta como un rayo óptico que desaparece al encontrar un obstáculo opaco, sino que sufre un fenómeno de difracción de borde (*knife-edge diffraction*). La onda electromagnética del atacante induce corrientes superficiales al chocar contra el labio superior del cilindro de aluminio, logrando que una fracción de la energía rebase la arista y alcance el parche cerámico.

A pesar de este fenómeno de difracción, una reducción geométrica de -10dB implica que la potencia de la señal interferente recibida es aproximadamente un 90% más débil. Este nivel de atenuación pasiva es un logro operativo que, sumado al procesamiento interno del receptor, puede significar la diferencia entre mantener el gobierno de la embarcación o sufrir una denegación de servicio total.

No obstante, son solo especulaciones basadas en simplificaciones computacionales, y una prueba real es requerida para poner a prueba las auténticas capacidades del blindaje.

3.3.6 Comparativa sólido frente a malla

Tras definir las dimensiones óptimas, se planteó la disyuntiva constructiva entre utilizar una protección metálica sólida (lámina continua) o una estructura de rejilla/malla (Jaula de Faraday).

Para que un mallado bloquee una onda electromagnética, la separación entre filamentos depende estrictamente de la longitud de onda (λ) de la señal interferente, en este caso el *jammer* o *spoofers*. La regla a seguir para que un mallado actúe como un muro sólido es que la separación máxima, que se denominará (s) entre los filamentos debe ser, como mínimo, 10 veces más pequeña que la longitud de onda ($\lambda/10$). Si se requiere una protección de alto grado, como es este supuesto, se espera utilizar un intervalo más corto con ($\lambda/20$) que estableció el profesor Ott como estándar de la industria [38]. Se estima así la jaula de Faraday idónea:

- Límite máximo absoluto ($\lambda/10$): $s = 19\text{cm}/10 = 1.9\text{cm}$.
- Diseño óptimo recomendado ($\lambda/20$): $s = 19\text{cm}/20 = 0.95\text{cm}$.

Es aquí donde surge un dilema ya que en el caso de superar el centímetro de separación la antena sería vulnerable a los ataques. No sería raro además que frente a las duras condiciones de la mar los endeble filamentos se deformen dando paso a estas condiciones indeseables.

Desde el punto de vista mecánico y aerodinámico, una estructura de malla es superior al reducir el peso y la carga al viento (efecto vela). Sin embargo, desde el punto de vista electromagnético, su comportamiento no es ideal. Será necesario comprobar mediante el sexto código del Anexo IV cuál sería la opción idónea electromagnéticamente.

Durante el desarrollo, nos encontramos con una limitación técnica en la herramienta de simulación disponible (MATLAB Antenna Toolbox versión antigua), que impedía la importación directa de geometrías STL complejas para simular cada barrote de la malla individualmente. Para resolver esto, se adoptó una metodología híbrida:

1. Simulación Rigurosa (Sólido): Se simuló el comportamiento del cilindro sólido utilizando el objeto *cavityCircular* y el método de los momentos (MoM), obteniendo el límite teórico de aislamiento máximo.
2. Modelado de Eficacia de Blindaje (Malla): Se derivó la respuesta de la malla aplicando un modelo teórico de degradación de blindaje (*Shielding Effectiveness*) sobre la curva del sólido. Se estimó que una malla típica para banda L presenta fugas cuando la atenuación requerida supera los 15-20 dB.

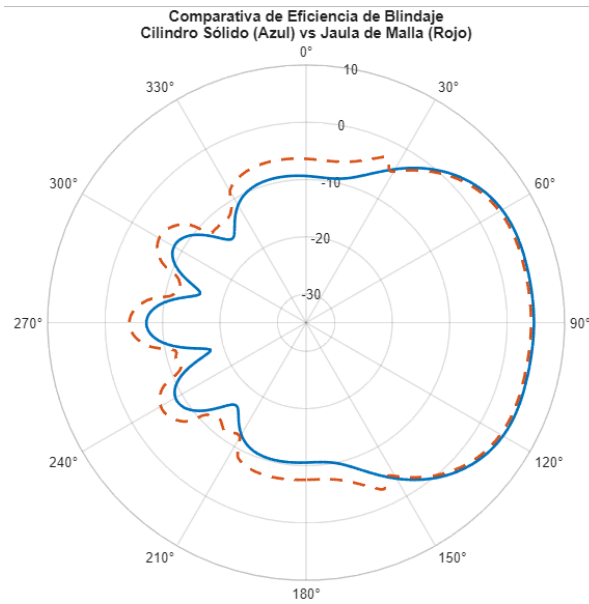


Figura 3-10 Comparativa de los diagramas de protección

La comparativa que se puede apreciar en la Figura 3-10 reveló dos fenómenos críticos en la solución de malla:

- **Degradación del Aislamiento Lateral:** En los ángulos de ataque (5° - 10°), la malla permite el paso de señal interferente a través de los intersticios, reduciendo la protección efectiva entre 10 y 15 dB en comparación con el sólido.
- **Aumento de la Radiación Trasera:** La malla presenta una peor relación delante-atrás (*Front-to-Back Ratio*), mostrando fugas traseras significativas. Esto hace al sistema más vulnerable a interferencias por rebotes desde la cubierta del barco (*multipath*).

Aunque la malla ofrece ventajas aerodinámicas, se seleccionó el cilindro sólido para el prototipo final. La prioridad del sistema es la integridad de la señal ante ataques de *jamming*. La pérdida de aproximadamente 5dB de aislamiento que introduce la malla se consideró inaceptable para una aplicación de seguridad crítica, optándose por la robustez electromagnética y la estanqueidad frente al ambiente marino que ofrece la pared sólida.

3.4 Validación Experimental

3.4.1 Hardware

Para llevar a cabo la validación del sistema de apantallamiento físico y contrastar los resultados teóricos, se ha seleccionado como antena GNSS el modelo comercial ELT0123. Se trata de un equipo de grado topográfico diseñado para operar como estación base, garantizando así una alta fiabilidad en la adquisición de datos brutos. El aspecto clave de esta elección radica en su arquitectura interna ya que bajo su radomo el equipo aloja un elemento radiante basado en tecnología de parche cerámico. Si bien es cierto que este *hardware* comercial posee una estructura multibanda más compleja que el modelo usado en las simulaciones previas, su principio de funcionamiento electromagnético comparte la misma base física, lo que legitima la comparación directa entre el modelo matemático y la prueba de campo.

Sus características electromagnéticas son óptimas para la conducción de la experiencia. A nivel de radiofrecuencia, este modelo destaca por ser una antena de navegación satelital de frecuencia completa. Ofrece soporte omnidireccional para las principales constelaciones globales: GPS (bandas L1, L2 y L5), GLONASS (G1, G2, G3), Galileo (E1, E5a, E5b) y BeiDou. También sus características mecánicas son

compatibles con los experimentos y sus medidas, recogidas en su ficha técnica [39], serán analizadas para el acorde montaje del blindaje



Figura 3-11 Antena ELT0123 [39]

Se ha seleccionado el kit de evaluación EVK-M8T compatible con el propio *software* de u-blox. Este dispositivo de grado industrial integra el avanzado *chipset* GNSS de la serie M8, destacando por su capacidad de seguimiento concurrente de múltiples constelaciones, lo que garantiza un análisis exhaustivo de la geometría espacial disponible en el entorno de pruebas. En el contexto de este Trabajo de Fin de Grado, la elección específica de la variante "T" (*Timing y Raw Data*) resulta fundamental, ya que permite la extracción directa de datos crudos de navegación y mensajes propietarios de bajo nivel mediante el protocolo UBX [40].



Figura 3-12 Receptor EVK-M8T [40]

3.4.2 Diseño de la protección física

Saltando a la realidad es necesario en primer lugar hacerse con los materiales necesarios. En una situación ideal se utilizaría un recubrimiento de acero inoxidable por su resistencia al ambiente marino corrosivo o incluso polímero impreso en 3D con recubrimiento conductivo reduciendo el peso notablemente. Sin embargo, para simplificar su fabricación y hacerlo asequible a las capacidades de cualquier dotación el primer prototipo se hará de aluminio, específicamente el idóneo sería aluminio de la serie 5000; aleado con magnesio presenta una resistencia a la corrosión impropia del aluminio normal.

Como conclusión del apartado anterior se ha llegado a la suposición que un blindaje cilíndrico de 18,4 cm de radio y 8,3 cm de altura, siendo una solución viable al problema planteado, ofreciendo una protección adecuada sin comprometer la precisión de manera excesiva. Al ser valores compatibles con la antena ELT0123 el diseño de la cavidad no será un obstáculo.

El diseño, buscando cumplir con la premisa de sencillez extrema en el montaje, no requiere de aplicaciones CAD. Para seleccionar la chapa idónea, cualquier diseño excesivo se simplifica a dos cálculos, primero el perímetro de la base a partir del diámetro, y la altura a partir de los datos de la antena.

La ficha técnica de la antena [39] no refleja la distancia desde la base hasta la localización exacta del elemento radiante. Medido sobre la antena son 16,6cm, lo que sumado a la altura original del cilindro alcanza los 24,8 cm. El perímetro se obtiene a partir de un simple cálculo:

$$2\pi r = 2\pi \cdot 18.4 = 115,661cm$$

Idealmente con una sola lámina de aluminio se formaría completamente la pared de la cavidad, sin embargo, surge aquí el primer problema del diseño. No se comercializa de forma extendida planchas de aluminio superiores a $100 \times 50cm$. Los requisitos de empresas especializadas, que sí podrían haber provisto la materia prima con medidas específicas, podrían ser factibles en bases y arsenales donde existen grandes servicios de carpintería. Se ha decidido finalmente que, aunque una lámina hecha a medida sería lo ideal, se usará para el prototipo una de $100 \times 50cm$, gracias a su fácil adquisición por un consumidor cualquiera. La otra propiedad a tener en cuenta es su grosor, siendo la lámina más adecuada la más fina. Una chapa de menor grosor es más simple de cortar y moldear y, como se estableció en el apartado 3.3.2, con superar los $2\mu m$ resultaría suficiente para ejercer de protección. La lamina adquirida excede este umbral con 0,5mm.

Para obtener el cilindro de altura 24,8 se ha cortado la lámina original en 2 segmentos de $100 \times 24,8cm$ con la ayuda de una amoladora angular como muestra la Figura 3-13 . Con un cálculo sencillo se pintan los puntos donde se espera colocar las uniones. Existen múltiples uniones válidas para unir ambas chapas, como tornillos, tuercas, incluso las bridas aguantarían la tensión. Es importante comprender que sea cual sea el método de unión en ningún caso debe ofrecer una abertura superior a 1cm. Como ya se analizó en el apartado 3.3.3, analizando la viabilidad del mallado, cualquier separación superior a esta daría lugar a filtraciones de ondas electromagnéticas no deseadas desde ese ángulo. En el caso del prototipo tras perforar los puntos designados con una broca, se unieron las chapas con pequeñas tuercas



Figura 3-13 Corte del Aluminio con amoladora angular.

El mayor problema de este diseño ha sido combatir las tensiones del aluminio derivadas de las uniones y agravadas por el uso de dos láminas unidas en lugar de una única. La estructura tendía a deformarse adquiriendo una forma ovalada, lo que afectaría ligeramente a los análisis. Para combatir este efecto y forzar la forma cilíndrica se utilizaron cabos a lo largo del perímetro, así como cinta aislante forzando una tensión que derivase en una deformación hacia la forma ideal, incluso pinzas para facilitar los trabajos; todos mostrados en la Figura 3-14 . La cinta aislante puede permanecer en la estructura dando cierta rigidez sin afectar a sus propiedades electromagnéticas. Es necesario tener presente que es una medida paliatoria incapaz de resistir las condiciones de un ambiente marino.



Figura 3-14 Medidas paliatorias iniciales frente a las tensiones en el primer prototipo.

Los múltiples problemas durante la fase de validación derivaron en el diseño de un segundo prototipo. Sus medidas se obtuvieron a partir de la zona inferior de la Figura 3-8 , incumpliendo con la premisa de la máscara. Esto fue necesario al comprobar que la máscara real no coincidía con la máscara física lo que llevo o a concebir un nuevo blindaje de radio 10cm y altura variable entre 8 y 16 cm. El diseño también cumple con un bloqueo eficaz del plano de tierra, buscando mejorar el rendimiento electromagnético frente a su predecesor. Este nuevo diseño permite variar el rango de la máscara fija en torno a los 45° lo que sería inadmisibile si el bloqueo solo dependiese de esta. Como se aprecia en la Figura 3-15 , es un diseño más elaborado, perfeccionando su mecanizado e integración con la antena



Figura 3-15 Prototipo 2 acoplado con antena ELT0123.

3.4.3 Comprobación de la precisión

La forma más evidente, y a la vez eficaz, de comprobar si el prototipo de blindaje GNSS cumple con las especificaciones de precisión establecidas al comienzo del apartado 3, será tomar muestras durante días, en momentos diferentes, de la pérdida de satélites tras la instalación de la cavidad, llevando a cabo una documentación constante de la distribución resultante de la bóveda celeste.

Es un estudio que aproxima de forma razonable el error de precisión que sufrirá un buque con la cavidad instalada. Escenarios temporales variados permiten una mayor variedad de distribuciones

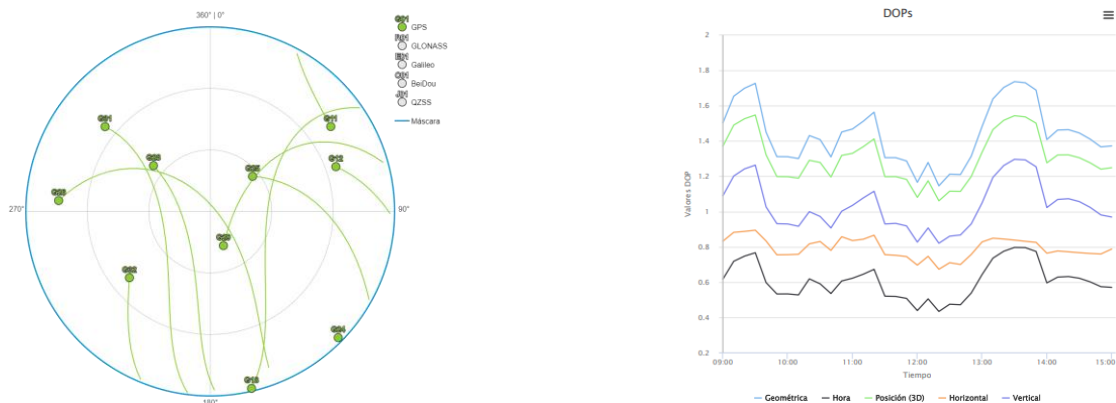
diferentes, aportando un mayor grado de homogeneidad al estudio. Se podría discutir si la posición fija de una antena satélite es equiparable a la de un buque que se desplaza miles de millas náuticas y ve la distribución satelital cambiar tan drásticamente. En relación con este análisis se puede concluir que la diferencia es mínima ya que la dinámica orbital de la constelación GNSS domina por completo sobre la cinemática de la embarcación.

Los satélites de las principales constelaciones operan en órbitas de altitud media (MEO) desplazándose a velocidades cercanas a los 14.000 km/h, con periodos orbitales de aproximadamente 12 horas. En comparación, la velocidad de tránsito de un buque mercante (en torno a 20 nudos) es despreciable. Por tanto, un receptor estático operando ininterrumpidamente durante varios días experimenta una rotación completa de la geometría satelital, capturando un espectro de escenarios y distribuciones de la bóveda celeste totalmente equivalentes a los que enfrentaría un navío en ruta.

Para materializar esta validación se ha establecido un entorno de pruebas utilizando la antena receptora ELT0123. El protocolo de ensayo ha consistido en registrar las tramas de navegación en dos escenarios comparativos. Primero el funcionamiento nominal a cielo abierto y el funcionamiento restringido tras acoplar físicamente el prototipo de cavidad cilíndrica.

Mediante la extracción continua de datos, se ha documentado el número de vehículos espaciales en seguimiento (*tracked satellites*) y sus coordenadas de azimuth y elevación en el momento del muestreo. Este contraste entre el cielo visible y el horizonte bloqueado por el apantallamiento permite dar un valor a la pérdida real de LoS con los vehículos espaciales y calcular experimentalmente la degradación del parámetro PDOP, sentando las bases para la discusión de los resultados obtenidos.

Antes del ensayo se analiza la situación esperada con el uso de la aplicación *Trimble GNSS planning* con la vista puesta a la mañana del día 10/04/2026, exactamente a las 0900 hora española. La aplicación aporta tanto predicciones de la gráfica del cielo y DOP entre otros permitiendo establecer una máscara como la que se espera que aplique la protección. Es necesario establecer una referencia geográfica, en este caso el Edificio de Investigación del CUD (N 42° 23' 51.6311" ; W 8° 42' 24.0692"), con la altura del receptor fijada a 10 metros.



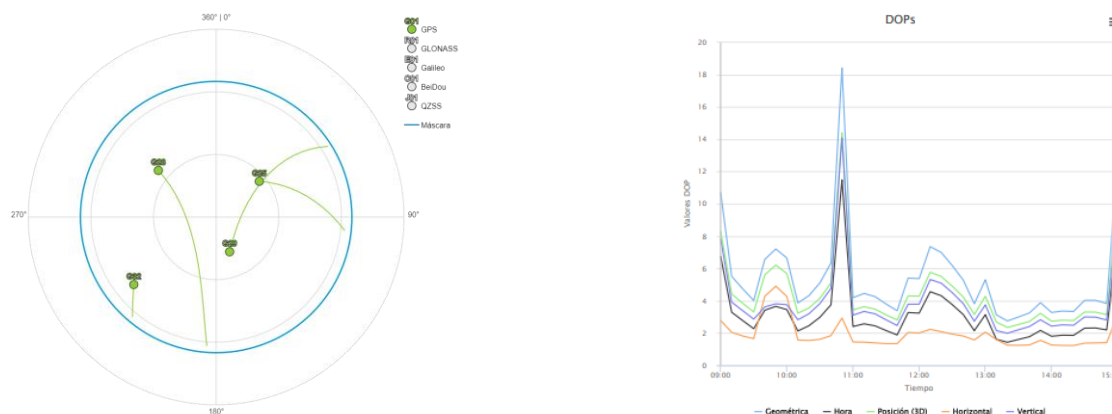


Figura 3-16 Comparación de distribución satelital y DOP en ambos casos de estudio para GPS

Una vez comparada y corroborada la distribución del momento con la esperada por *Trimble GNSS planner*, representado en la Figura 3-16, se instalará el blindaje para poder analizar los efectos de este a lo largo del tiempo. La aplicación U-center de U-Blox permite la grabación de los distintos parámetros del entorno permitiendo obtener resultados comparables con las estimaciones del planificador.

Todos los datos recopilados mediante este proceso deben ser recogidos en tablas que permitan evaluar los resultados y obtener conclusiones. Los datos serán extraídos mediante el séptimo algoritmo del Anexo IV y tras ser reducido se presentará la información en tablas en el Anexo V Anexo.

3.4.4 Comprobación de la protección

En este apartado experimental se busca demostrar la validez de la cavidad cilíndrica como blindaje frente a interferencias intencionadas, con el objetivo de corroborar y superar los resultados teóricos obtenidos en las simulaciones previas (Apartado 3.3.5). Para lograrlo, se diseñó un procedimiento empírico consistente en la monitorización continua de la constelación GPS, evaluando el impacto directo de la protección física sobre la relación portadora a densidad de ruido (C/N_0)

Con el propósito de garantizar la fiabilidad de las mediciones y mitigar en la medida de lo posible las reflexiones espurias, el montaje experimental se emplazó en un entorno a cielo abierto y elevado, maximizando así la visibilidad de la bóveda celeste desde el horizonte (0°) hasta el cenit (90°). No obstante, cabe señalar que el efecto del multitrayecto siempre estará parcialmente presente debido a la naturaleza urbana del entorno de pruebas.

Las mediciones se realizaron utilizando nuevamente el receptor u-blox EVK-M8T asociado a la antena ELT0123. Durante el ensamblaje, resultó crítico asegurar una correcta instalación del cilindro de aluminio, sellando perimetralmente la unión entre la base de la antena y el blindaje para prevenir cualquier fuga de radiofrecuencia proveniente de ángulos inferiores al horizonte. La configuración experimental se estructuró en dos fases de grabación de datos mediante el *software* u-center:

- **Medición de referencia (*Baseline*):** Grabación del espectro a cielo abierto con la antena al descubierto para establecer los niveles nominales de recepción de los distintos satélites.
- **Medición con blindaje:** Grabación temporal prolongada, abarcando el tránsito orbital completo de los satélites, con la cavidad cilíndrica instalada. En esta fase, la señal incidente queda expuesta a los fenómenos de atenuación y difracción geométrica provocados por el metal. Además, la iteración de estas medidas introduciendo modificaciones en el montaje permitirá extraer conclusiones sobre la efectividad real y proponer futuras optimizaciones.

En lugar de evaluar el diseño provocando la pérdida total del posicionamiento mediante un ataque real de *jamming*, práctica inviable debido a las severas interferencias que causaría a terceros en el entorno

marítimo e infraestructuras civiles, se seleccionó el parámetro C/N_0 (medido en dBHz) como métrica de protección. Este valor cuantifica el margen entre la potencia de la señal útil recibida y el umbral de ruido de fondo.

Dado que un ataque de *jamming* consiste, en esencia, en elevar artificialmente este piso de ruido, la atenuación física que el cilindro ejerce sobre la señal de un satélite en ángulos bajos será equivalente a la degradación que sufriría la emisión de un *jammer* hostil situado en esa misma posición geométrica. Por consiguiente, el diferencial negativo del C/N_0 en los satélites rasantes frente a la medición de referencia permite deducir matemáticamente la ganancia de protección del sistema, validando el prototipo de forma segura y sin necesidad de emitir interferencias ilícitas en el espectro radioeléctrico.

Para procesar la ingente cantidad de datos orbitales generados, se recurrió de nuevo a MATLAB. El código desarrollado (adjunto en el Anexo IV, código octavo) automatiza la lectura de los registros temporales (*logs*) de u-center, extrayendo secuencialmente el identificador de cada satélite en vista (PRN), su elevación calculada y la calidad de la señal. Con esta información, el algoritmo elabora una representación gráfica que enfrenta la elevación del satélite respecto a su valor de C/N_0 , permitiendo visualizar de forma clara y directa el perfil de atenuación provocado por el blindaje.

4 RESULTADOS

El apartado anterior detalló el proceso de estudio desde los primeros análisis matemáticos hasta las pruebas en un prototipo físico de validación. Es en este apartado donde se exponen y analizan los resultados de todas las actividades llevadas a cabo, lo que facilitará próximamente la extracción de ciertas conclusiones

4.1 Resultados de diseño y simulación computacional

El proceso de diseño y validación computacional, llevado a cabo mediante herramientas de simulación electromagnética de onda completa en MATLAB, ha permitido optimizar y caracterizar el apantallamiento físico de la antena GNSS frente a amenazas de *jamming*. Como se detalla en apartados posteriores, la optimización llevó a la elección de unas dimensiones óptimas de 18.4 cm de radio y 8.2 cm de altura para la cavidad cilíndrica, dando lugar a una máscara física de 24°, que posteriormente fue comparado con otro de radio 10 cm y altura variable.

Los resultados de la simulación computacional demuestran el éxito inicial del diseño mediante el cumplimiento de las dos premisas fundamentales:

- **Alteración favorable del patrón de radiación:** Atenuando las señales provenientes del horizonte. A pesar de que la magnitud de la protección obtenida en el punto 3.3.5 ha sido menor a la primeramente estipulada en el apartado 3.3.2., se aborda la validación con la esperanza de un valor mínimo de atenuación en el horizonte.
- **Compromiso operativo (Análisis PDOP):** La simulación orbital confirma que el blindaje impone una máscara de elevación artificial inferior a ese límite establecido de 27°. Aunque esto reduce el número de satélites visibles y aumenta el valor del PDOP respecto al escenario nominal a cielo abierto, el error de posición se mantiene en márgenes operativos tolerables. De forma más reseñable el segundo prototipo incluso con máscaras físicas de 45° no debería ser un modelo factible desde el punto de vista de la protección esperando valores exagerados de PDOP

En conclusión, los modelos computacionales validan que la geometría propuesta sentando la adecuada base que necesita una validación a partir de un prototipo.

4.2 Resultados de la validación experimental

4.2.1 Resultados de la comprobación de la precisión

Mediante la experimentación con la antena ELT0123 se han obtenido múltiples resultados en forma de grabaciones de u-center las cuales recogen toda la información obtenida a través de los vehículos espaciales. Es necesario comparar su rendimiento en términos de PDOP y número de satélites visibles, es decir, que segmento espacial y cuanto lo atenúa. Para ello fue necesario comprobar que la antena funcionaba correctamente antes de cada grabación, comparando lo real con la predicción de GNSS *planer*, lo que se dio en todos los casos como se ve en el ejemplo de la Figura 4-1 .

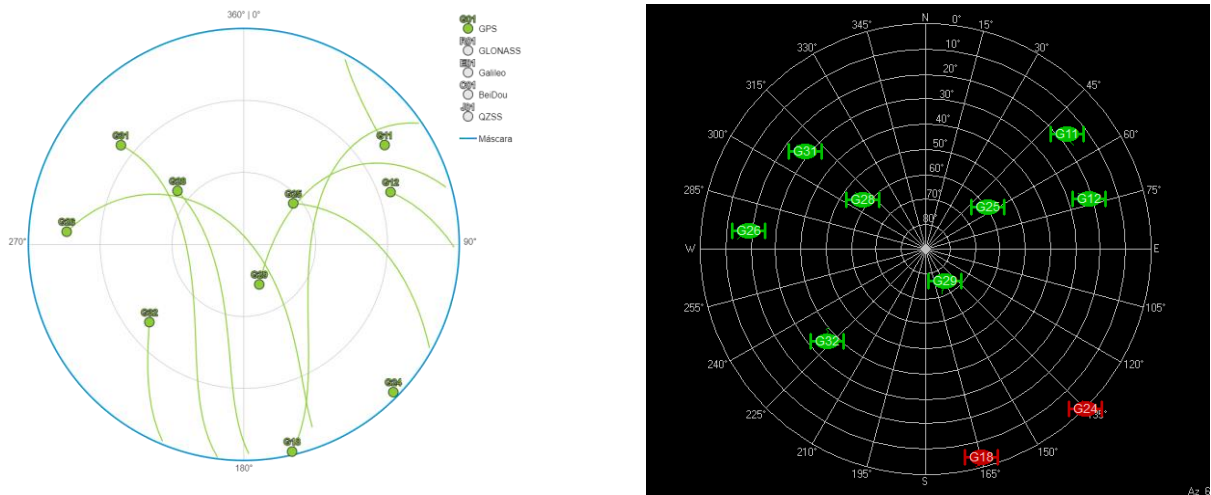


Figura 4-1 Comprobación inicial del correcto funcionamiento de la antena

Se han realizado 10 experiencias a cielo abierto cuya duración oscila entre 4 y 8 horas, todos los datos relevantes para el análisis de la precisión han sido extraídos usando el séptimo código del Anexo IV, y recogido en tablas que han sido reducidas para ser recogidas en el Anexo V. Aunque el número de vehículos espaciales enlazados se reduce respecto la condición nominal, se han obtenido mejores resultados de los esperados en las simulaciones. Una máscara física de 25° no ha demostrado bloquear aquellos satélites por debajo del umbral, manteniendo su cobertura de forma fiable varios grados por debajo. Es necesario establecer la máscara real que ejerce el blindaje por lo que se calculó la media de elevaciones a las que se pierde la conexión con los vehículos espaciales. Analizando las grabaciones se establece como punto de pérdida de enlace como el último (o primer) punto de recepción de señal en la trayectoria del satélite incluido el caso de cobertura intermitente.

Esta situación influye directamente al análisis del PDOP. Aunque su incremento es evidente como cabía esperar tras el desarrollo del apartado 3.3.3.; el aumento de la media se reduce respecto los 1,76 estipulados. El valor medio entre los análisis fija un valor de variación entre el valor nominal y protegido de 0.6, óptimo para mantener una buena precisión. En la Figura 4-2 se aprecia el aumento inmediato del PDOP tan pronto se instala el primer prototipo, derivado directamente de la pérdida de los satélites con menor elevación

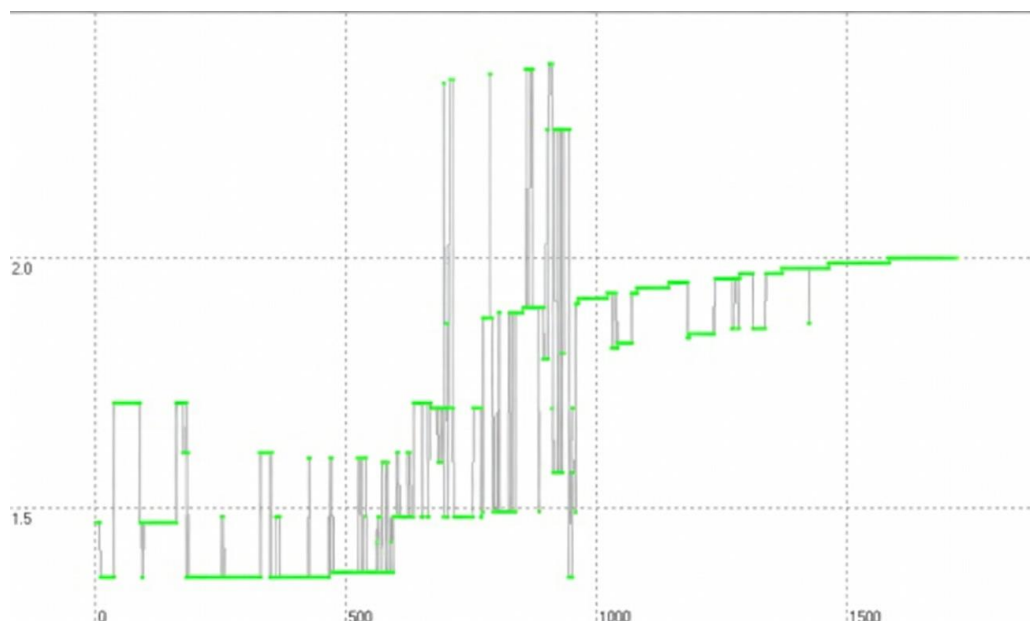


Figura 4-2 Gráfica de PDOP frente al tiempo

Las conclusiones a sacar de este apartado son especialmente relevantes para la instalación de estos dispositivos. Su cumplimiento de los umbrales de precisión y para navegación y fuego a tierra serán determinantes, pero en ningún caso se debe olvidar la función principal del blindaje y este es la protección. También es importante reconocer en este punto el escaso valor que ha tenido la máscara fija, al haberse obtenido valores realmente similares en ambos casos, siendo el peor de los dos el segundo prototipo, lo que se aprecia en sus rangos de PDOP, ligeramente más elevados en los datos recogidos en el Anexo V, especialmente observando los valores del día 23 donde se utilizó al primer prototipo por la mañana y el segundo por la tarde.

4.2.2 Resultados de la comprobación de protección

El octavo algoritmo recogido en el Anexo IV traza de manera automatizada el perfil de recepción completo de la antena, graficando la dispersión de valores de C/N_0 respecto la elevación del vehículo espacial del que se ha obtenido. La protección se visualiza computacionalmente con facilidad a través de la formación de un desplome atenuado en la gráfica resultante.

Se puede establecer a partir de la comparación entre el escenario nominal y el protegido en la Figura 4-3 la máscara real que impone el blindaje frente a la poco realista de las simulaciones teniendo en cuenta que incluso con el uso del segundo prototipo con su máscara física de 45° , solo se aprecia pérdida de satélites por debajo de los 20° . A mayores permite establecer de forma clara dos zonas diferenciadas:

- **Zona de Operación Segura:** Para ángulos de elevación altos, el código verifica que C/N_0 se mantiene en valores óptimos (típicamente > 40 dBHz), garantizando que el diseño no interfiere con la navegación legítima del buque.
- **Zona de Bloqueo:** Se sitúa al cruzar el umbral de diseño geométrico que a partir de la figura 4-3 se establece en 20° , al ser donde se revela la atenuación abrupta en la relación C/N_0 reduciéndose de forma exagerada de 40 a 28 dB, posteriormente en 8° vuelve a caer hasta que la recepción es nula a los 2° . En concreto las gráficas corresponden a la grabación del día 17 y 21 respectivamente.

la Figura 4-3 presenta mapas de densidad bidimensionales que ilustran el comportamiento electromagnético de las señales GNSS captadas. En estas gráficas, el eje horizontal representa el ángulo de elevación del satélite y el vertical refleja su calidad de señal (C/N_0). Cada punto representa una señal captada con cierta calidad a cierta altura, adquiriendo colores más intensos cuantas más señales iguales

haya obtenido. La línea vertical situada a 25° se establece como referencia visual para marcar la zona de protección estimada.

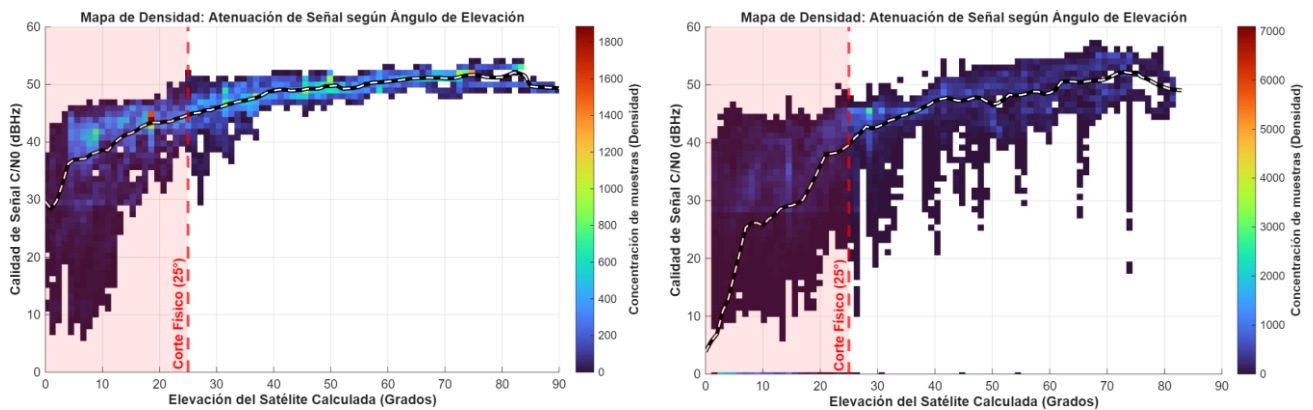


Figura 4-3 Comparación del caso nominal frente a un caso de protección del segundo prototipo

De esta forma, el código de MATLAB no solo automatiza la lectura de datos, sino que cuantifica la frontera exacta donde el cilindro supuestamente entra en acción, validando que, cualquier señal de *jamming* o *spoofing* proveniente del horizonte táctico, sufrirá una penalización severa por difracción y bloqueo metálico antes de alcanzar la etapa de radiofrecuencia del receptor.

La relación de protección ha obtenido valores muy similares para ambos prototipos. Sin embargo, cabe reseñar que el segundo, con mayor máscara, ha obtenido con mayor regularidad protecciones superiores, eso sí, a cambio de una máscara de elevación superior. Esto se puede deber a múltiples factores más allá del diseño, de los cuales se podría destacar una mejor conexión con el plano de tierra por su diseño más elaborado. El caso más evidente de esta diferencia es el uso del prototipo 1 la mañana del día 22 frente al uso del prototipo 2 a lo largo de la tarde, representado en la Figura 4-4. Es necesario reseñar que esta figura muestra el caso más extremo y en ningún caso el más fiel. Para poder hacer comparaciones efectivas en un campo donde las mediciones difieren temporalmente con el paso de los satélites por sus órbitas, únicamente se podrían comparar datos recopilados en el mismo instante temporal, lo que fue imposible por la disponibilidad de una única antena.

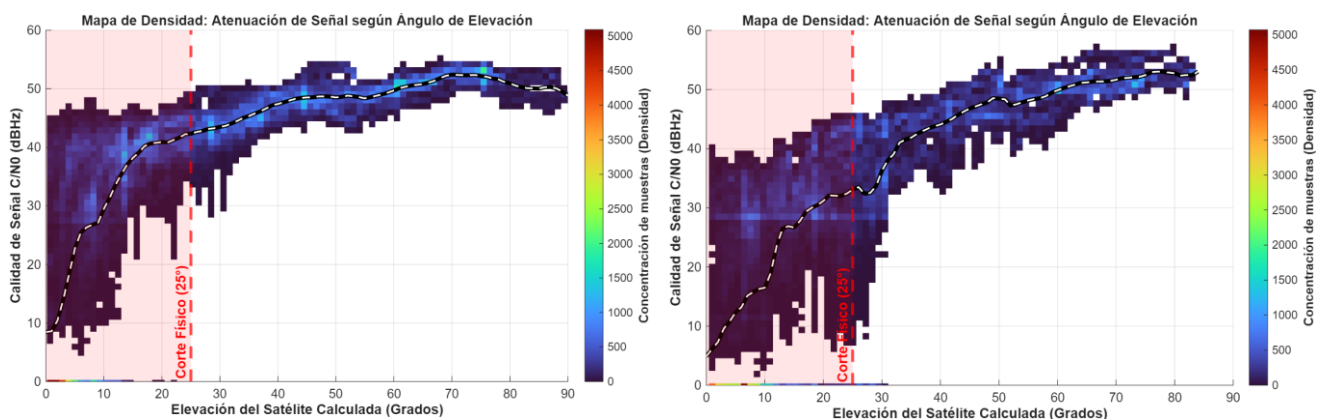


Figura 4-4 Comparación de ambos prototipos, radio 18cm (izquierda) y 10cm (derecha)

5 CONCLUSIONES Y LÍNEAS FUTURAS

En este apartado se presentarán las conclusiones obtenidas y se explicará si se alcanzaron o no (y por qué razón, en este último caso) los objetivos establecidos al inicio del TFG. Se presentarán, asimismo, las posibles líneas futuras en las que se podría seguir trabajando para mejorar y ampliar el TFG presentado.

5.1 Viabilidad del uso de blindaje GNSS en buques de la Armada

5.1.1 Conclusiones desde el punto de vista mecánico

Por mucho que la protección sea efectiva, su implementación en buques de la Armada solo se puede llevar a cabo si su instalación es compatible con las antenas GNSS en uso actualmente. Además, existen otros factores que afectan a su instalación siendo el más evidente el espacio disponible. La colocación del blindaje puede llegar a ser incompatible debido a la distribución de antenas en la superestructura. Otro factor que no se debe despreciar es el efecto vela y el aumento de carga sobre los mástiles que, aunque pequeño, no es indigno de estudio. Lo mismo sucede con el concepto de resistencia a la corrosión y si la cavidad puede durar en buen estado con el paso del tiempo.

Atendiendo al primer factor mecánico reseñado, cabe destacar el primer problema real que se encontraría la fuerza de combate. De primeras el blindaje diseñado no es compatible con todo el rango de antenas, y sin necesidad de un estudio previo se hace evidente en el caso de las fragatas F-80. En concreto la F-82, donde uno de sus GPS civiles SIMRAD no es susceptible de incorporar este blindaje ya que colisionaría con la antena del ADS-B como se aprecia en la Figura 5-1. Este caso, aunque no tan evidente, se podría dar en múltiples de los buques de guerra necesitados de blindaje por lo que un estudio y medidas en la propia unidad serían requeridas.



Figura 5-1 Antena SIMRAD de la F82

Más allá de las propiedades físicas del diseño, el estudio llevado a cabo ha conseguido demostrar la facilidad con la cual un grupo con mínima experiencia es capaz de fabricar la cavidad cumpliendo con las especificaciones físicas de diámetro y altura. Es una conclusión verdaderamente positiva teniendo en cuenta que, incluso dotaciones en zona de operaciones con recursos mínimos, pueden implantar esta solución con facilidad sin requerir mecanizados complejos.

5.1.1 Conclusión desde el punto de vista electromagnético

Es aquí donde finalmente se unen los dos conceptos en torno a los cuales ha pivotado el desarrollo y se analiza si se ha obtenido un resultado de DOP compatible con la protección alcanzada.

El contraste directo entre los mapas de densidad obtenidos a cielo abierto y con la cavidad cilíndrica instalada permite extraer conclusiones definitivas sobre el comportamiento electromagnético del prototipo diseñado. El análisis de las curvas de tendencia (relación C/N_0 frente a elevación) confirma el éxito funcional del blindaje como filtro espacial de radiofrecuencia, cumpliendo e incluso mejorando las atenuaciones que predijeron las simulaciones de Matlab en el apartado 3.3.5. destacando tres fenómenos electromagnéticos clave:

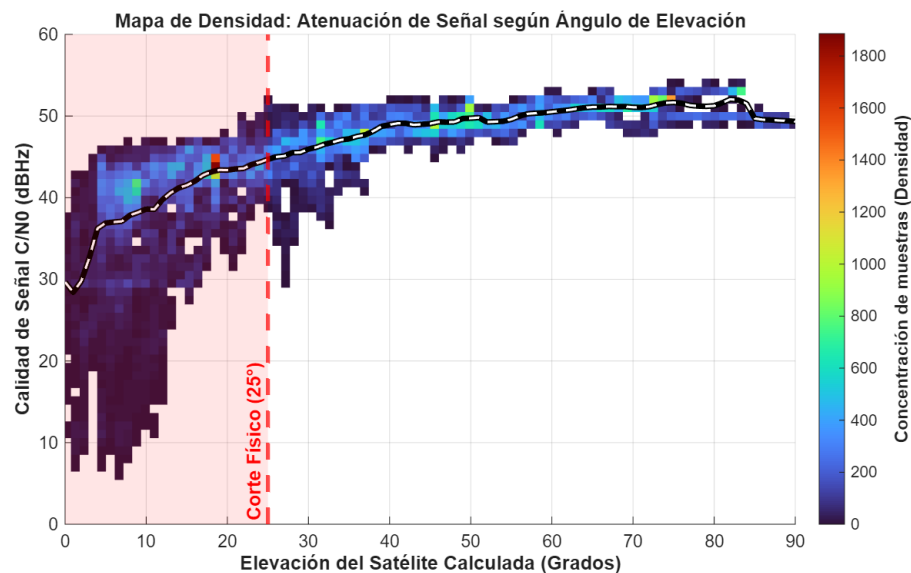


Figura 5-2 Gráfica de dispersión sin blindaje

En la medición de referencia sin protección como se muestra en la Figura 5-2 (en este caso concreto es la referente al intervalo de tiempo de las 0800 a las 1400 del día 17/03/2026), la antena presenta un perfil de recepción omnidireccional típico, logrando captar satélites en el horizonte (0° a 10° de elevación) con niveles de señal muy robustos, promediando los 30-38 dBHz. Esta zona representa la principal vulnerabilidad táctica de un buque frente a un ataque de *jamming*.

Al introducir el cilindro como se aprecia en la Figura 5-3 (perteneciente a la grabación del día 21/03/2026 entre las 1500 y las 2100), el escenario electromagnético en esta región cambia radicalmente. La línea de tendencia media sufre un desplome abrupto, cayendo por debajo de los 15 dBHz en elevaciones inferiores a 10°, y revelando una concentración masiva de muestras en 0 dBHz (zona de pérdida total de enlace o *tracking*). Se ha logrado una atenuación diferencial de aproximadamente 20 dBHz en el horizonte operativo. Esto demuestra que la estructura metálica ha generado con éxito una zona de sombra electromagnética, bloqueando no solo la línea de visión directa sino de forma electromagnética, imponiendo una penalización severa a cualquier frente de onda que intente penetrar de forma paralela a la cubierta del buque.

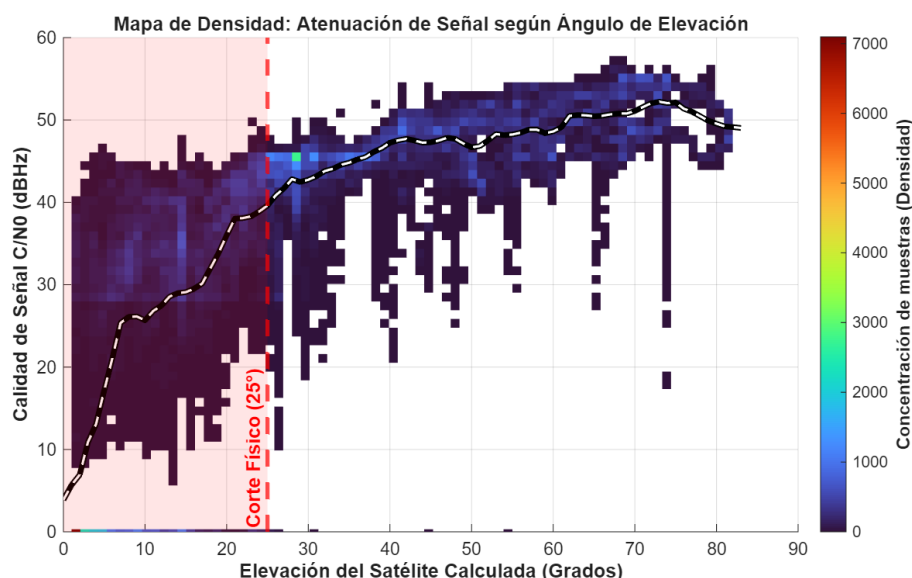


Figura 5-3 Gráfica de dispersión con blindaje

Uno de los mayores riesgos al encerrar una antena en una cavidad es la degradación de la señal útil debido a resonancias internas o al estrechamiento excesivo del lóbulo principal. Sin embargo, al observar la región de elevación cenital (entre 60° y 90°), ambas gráficas convergen. Tanto la antena desnuda como la protegida mantienen una calidad de señal óptima que ronda los 50 dBHz.

Este comportamiento corrobora que el diseño geométrico del cilindro y su ángulo de corte han sido dimensionados correctamente. El blindaje es electromagnéticamente "invisible" para los satélites situados en la bóveda superior, garantizando que el buque mantiene un posicionamiento de alta integridad sin sufrir atenuaciones indeseadas en la señal legítima.

La gráfica con protección representada en la figura 5-3 también resulta de gran valor académico al capturar las imperfecciones del mundo físico. En la zona de sombra entre los 0 y 20 grados se observa que, aunque la gran mayoría de señales se atenúan de forma exagerada, persiste una nube difusa de puntos de baja energía. Dado que la pared de la cavidad es electromagnéticamente opaca por el efecto pelicular, estas trazas residuales son la representación gráfica del fenómeno de difracción de borde, y principal aliado de los ataques desde el horizonte. Las ondas rasantes impactan contra el labio superior del cilindro y se curvan hacia el interior de la cavidad. Aunque logran alcanzar el parche receptor, lo hacen con su energía críticamente mermada, confirmando que la geometría actual fuerza a la onda interferente a disiparse, sin embargo, su presencia refuerza la idea de la cavidad como protección complementaria y no solución.

Los resultados pueden parecer positivos a primera vista sin embargo las gráficas se ven alteradas por efectos como el multitrayecto, que aumentan la recepción de los satélites aun sin LoS con la antena. Desde el punto de vista del entorno de pruebas, la presencia de obstáculos urbanos introduce trayectorias *multipath*, propiciando que señales provenientes del horizonte reboten en estructuras adyacentes y

penetren en el tubo desde ángulos cenitales limpios. También a nivel constructivo, la mínima discontinuidad en el sellado perimetral contra el plano de masa puede habilitar fugas de radiofrecuencia, sumado a la posible inducción de corrientes de modo común a lo largo de la malla del cable de datos. Finalmente, la propia arquitectura del receptor u-blox EVK-M8T penaliza la obtención de un cero absoluto en la gráfica; sus bucles de seguimiento poseen una sensibilidad tan extrema que son capaces de mantener el enlace satelital incluso con la energía ínfima y degradada que logra sortear todas las barreras físicas anteriores.

Asimismo, lo que afecta a los resultados de protección beneficia a los de precisión y se obtienen unos valores del PDOP superiores a los simulados aparentemente compatibles con la navegación segura. El análisis cuantitativo de los parámetros de precisión y de los errores en coordenadas cartesianas (eECEF), recogidos en el Anexo V, y presentados por grabaciones como se muestra en la Tabla 5-1, permite evaluar de forma empírica el impacto colateral que el blindaje electromagnético impone sobre la solución de navegación del buque. La interpretación conjunta de estas métricas revela conclusiones fundamentales sobre el comportamiento del sistema

Parámetro	Unidades	Mínimo	Máximo	Media	Desviación típica
VDOP	-	1.06	4.34	1.56	0.46
HDOP	-	0.8	2.89	1.05	0.17
PDOP	-	1.34	5.21	1.89	0.4
Vehículos Espaciales	-	6	12	9.5	1.2
eECEF total	M	6.30e-02	6.73e+00	2.25e+00	1.14

Tabla 5-1 Datos obtenidos para el intervalo de 13:58-20:11 del día 21/02/2026

Primeramente, se revela la disminución controlada de la precisión por la degradación de la geometría orbital. La consecuencia electromagnética más directa de introducir una cavidad cilíndrica es la limitación drástica del campo de visión de la antena. Al forzar una máscara de elevación física que bloquea las señales rasantes, se eliminan del cálculo de navegación los satélites cercanos al horizonte. Estos satélites son precisamente los que proporcionan la mejor geometría para calcular la posición en el plano bidimensional. Como resultado, en las sesiones de los días 18 y 19 de marzo, se registran picos máximos en los valores de dilución de precisión geométrica, con PDOP, HDOP y VDOP alcanzando valores de saturación de 99.99 en momentos puntuales. Esto evidencia instantes de baja disponibilidad satelital geométrica dictaminada por el bloqueo del metal.

A mayores se pone de manifiesto la supervivencia del enlace y la conservación de señal de los satélites elevados. A pesar de la agresiva atenuación impuesta en ángulos bajos, los datos demuestran que el cono de visibilidad cenital preservado por el diseño es lo suficientemente amplio para mantener la operatividad del sistema, en ningún caso equivalente al estipulado inicialmente equivalente al de la máscara fija. A lo largo de todas las sesiones de grabación, el valor medio de satélites en seguimiento se mantuvo de forma robusta entre los 8.53 y los 10.61 vehículos espaciales, no bajando nunca del mínimo estricto de 4 satélites simultáneos requeridos para obtener un *Fix* tridimensional, a pesar de alcanzar este valor en ciertas ocasiones como la mañana del día 18/03/2026. Se puede entonces concluir que el blindaje cilíndrico en ningún caso tiene consecuencias críticas si bien es cierto que la degradación de la precisión es siempre perjudicial por muy pequeña que sea.

Queda probado como las secciones establecidas de radio óptimo visibles en la Figura 3-4 del apartado 3.3.2 han resultado eficaces en cuanto a la relación de protección. Por tanto, los buques buscando incorporar un blindaje de esta entidad debería barajar los valores de radio 19 o 10 cm pudiendo

tomar ciertas libertades en cuanto a la altura de este, no siendo recomendada una máscara física mayor a 45° al no haber sido evaluada a lo largo de la validación.

5.1.2 Conclusión Operativa

Lo más crucial del estudio es contestar la pregunta si los blindajes GNSS tienen cabida o no en los buques de la Armada. La evaluación final de este prototipo exige responder a la disyuntiva fundamental que plantea el diseño: ¿justifica la ganancia en protección el sacrificio de la precisión del sistema? El análisis cruzado de los datos recopilados y la doctrina naval dictaminan de que sí.

En un escenario táctico de alta intensidad, la prioridad del buque no es alcanzar precisiones milimétricas, sino garantizar la disponibilidad e integridad de la solución de navegación y capacidad de combatir. Perder la señal GNSS por completo debido a un ataque electrónico implica la neutralización instantánea de capacidades ofensivas críticas, imposibilitando el lanzamiento de misiles guiados o la ejecución de misiones de fuego naval de apoyo. Las tablas de error posicional (eECEF) demuestran como la máscara del blindaje degrada la precisión, elevando el error a un entorno de 3 a 5 metros llegando en los peores casos registrados a 20 metros. Sin embargo, este margen de error es una degradación compatible con la supervivencia del buque, manteniéndose muy por debajo del límite estricto de 25 metros requerido para mantener un FOM 1 y autorizar soluciones de tiro. Por consiguiente, la integración de barreras físicas en las antenas GNSS de los buques representa una contramedida pasiva de muy alto valor táctico y un coste de implementación mínimo. Por otro lado, estos errores puntuales no podrían ser asumidos en entornos de operaciones como la caza de minas, donde las precisiones más elevadas son requeridas. Se buscarían en estas circunstancias otra solución más precisa, barajando incluso la prohibición de la caza de minas en entornos degradados electromagnéticamente.

Respecto a la naturaleza de la amenaza, la cavidad cilíndrica ha demostrado comportarse como un filtro espacialmente útil. Al basar su funcionamiento en la atenuación del frente de onda (efecto pelicular), la pared de aluminio no discrimina la entidad de la señal hostil, lo que confiere al sistema la capacidad de mitigar simultáneamente tanto ataques de interferencia por ruido como de suplantación de señal, independientemente de la sofisticación del ataque de *spoofing*, la barrera física actuará como un filtro infranqueable para las señales provenientes de los ángulos bloqueados.

No obstante, esta protección está estrictamente supeditada a la elevación del vector de ataque. Dado que la inmensa mayoría de los emisores hostiles en el entorno naval operativo irradian desde ángulos rasantes, el blindaje resulta efectivo. La necesidad de mantener la bóveda superior abierta para garantizar la recepción de satélites legítimos genera una vulnerabilidad intrínseca frente a amenazas aéreas y en situaciones de navegación costera. Si un dron o aeronave enemiga dotada de capacidades de *spoofing* logra situarse en la vertical del buque, infiltrándose en el cono de visibilidad cenital, el escudo físico resultaría ineficaz, incluso en el caso de que el buque se enfrenta a una orografía desfavorable a poca distancia de la costa. Para mitigar esta brecha residual, el blindaje mecánico debe entenderse no como una solución única, sino como el primer eslabón defensivo que debe trabajar en conjunción con algoritmos criptográficos y de autenticación a nivel de software en el propio receptor.

No se puede terminar el análisis operativo de la cavidad sin remarcar que esta no es una medida ni mucho menos definitiva. Su protección en el horizonte no sobrepasa los 20dB que se establecieron en un principio como mínimo por lo que el posicionamiento GNSS no sobreviviría a exposiciones intensas de ruido interferente. Es así como la instalación de un blindaje con las especificaciones del apartado 5.1.1 no exime a una dotación de descuidar el resto de los métodos de posicionamiento, al mantenerse latentes ambas amenazas de la NAVWAR, aunque estén atenuadas.

Su simplicidad y fácil implantación invitan a barajar las posibles combinaciones con equipos y antenas activas para aumentar la relación de protección mientras se conserva un segmento considerable de la bóveda celeste para posicionamiento. Es sencillo imaginar este trabajo evolucionar a la integración de sistemas para blindajes GNSS en la Armada.

5.2 Líneas Futuras

5.2.1 Integración con Antenas CRPA

Esta tarea propone la evolución del sistema pasivo presentado en este TFG hacia un modelo basado en un concepto tan naval como es la "defensa en profundidad". En este caso específico sería una defensa electromagnética que integra el apantallamiento geométrico con tecnología de antenas CRPA. Mientras que la cavidad proporciona una protección física como elemento pasivo, las CRPAs adquieren un rol activo, siendo capaces de modificar dinámicamente su patrón de recepción para anular interferencias.

La justificación para este desarrollo es reforzar un sistema de posicionamiento naval con una resiliencia ya extraordinaria. Los receptores GNSS militares cuentan con múltiples capas de protección y cabe hacerse la pregunta si una más ayudará o en este caso podría entorpecer la labor de los otros sistemas. Teniendo en cuenta que una antena CRPA utiliza un array de antenas menores, siendo capaz de conformar nulos de ganancia directamente hacia la fuente del *jammer* o *spoofers*, es especialmente preocupante que la instalación de una cavidad altere su capacidad de dirigir estos nulos correctamente.

5.2.2 Estudio de viabilidad del uso de choke ring en la Armada

Históricamente, este diseño de anillos concéntricos ha quedado relegado a estaciones geodésicas terrestres con el único propósito de eliminar el error por multitrayecto, filtrando de forma agresiva cualquier frente de onda que rebotara en el suelo. No obstante, presenta un potencial táctico considerable en el ámbito de la Guerra de Navegación. Dado que la inmensa mayoría de los ataques de *jamming* y *spoofing* en el entorno naval provienen del horizonte, el rechazo natural de una *choke ring* a las elevaciones rasantes actuaría como un escudo físico de mayor entidad que la cavidad. El siguiente paso lógico tras este TFG sería modelar cómo interactuaría el patrón de radiación de estos anillos frente a una amenaza naval, integrado idealmente en una superestructura metálica de una fragata en alta mar, analizando su ganancia real frente a emisores hostiles.

6 BIBLIOGRAFÍA

- [1] Armada Española, «Líneas Generales de la Armada 2025,» Ministerio de Defensa, Madrid, 2025.
- [2] B. Hofmann-Wellenhof, H. Lichtenegger y E. Wasle, GNSS-Global Navigation Satellite Systems: GPS, GLONASS, Galileo and more, Viena: Springer Verlag, 2008.
- [3] T. A. Stansell, «The TRANSIT, Navigation Satellite System,» de *Navigation*, 1979, pp. 93-126.
- [4] E. D. Kaplan y C. J. Hegarty, Understanding GPS/GNSS: Principles and Applications, Artech House, 2017.
- [5] European Union Agency for the Space Programme, «European GNSS (Galileo) Open Service Definition Document (OS-SDD), Issue 1.3,» Publications Office of the European Union, Prague, 2023.
- [6] Global Positioning Systems Directorate, «IS-GPS-200N: Navstar GPS Space Segment/Navigation User Interfaces,» U.S. Space Force, 2022.
- [7] C. D. Muñoz, «Estructura de las Señales del GPS,» *Hacia el Espacio*, 2016.
- [8] United States Department of Defense, «Global Positioning System Standard Positioning Service Performance Standard,» 2002.
- [9] D.-J. Jwo, «Efficient DOP Calculation for GPS with and without Altimeter Aiding,» Institute of Maritime Technology, National Taiwan Ocean University, Keelung, Taiwan.
- [10] P. Misra y P. Enge, Global Positioning System: Signals, Measurements, and Performance, Ganga-Jamuna Press, 2011.
- [11] R. Santerre, «Impact of GPS satellite sky distribution on precise positioning,» de *Manuscripta Geodaetica*, 1991, pp. 28-53.
- [12] Joint Chiefs of Staff, «Joint Publication 3-14: Space Operations,» Department of Defense, Washington, D.C., 2020.

- [13] Grabowski, «GPS Interference and the Newark Airport GBAS Instalation,» Federal Aviation Administration, 2012.
- [14] C4ADS, «Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria.,» Center for Advanced Defense Studies, Washington, D.C., 2019.
- [15] Inside GNSS, «GNSS Interference Complicates Navigation as Hormuz Shipping Disruption Deepens,» 2 03 2026. [En línea]. Available: <https://insidegnss.com/gnss-interference-complicates-navigation-as-hormuz-shipping-disruption-deepens/>. [Último acceso: 11 03 2026].
- [16] Hexagon | NovAtel, «Spoofed or jammed? Busting the myths of GNSS interference and mitigation,» Hexagon Autonomy & Positioning division, Calgary, 2025.
- [17] Jammer Master, «Jammer Master,» [En línea]. Available: <https://jammermaster.com/blog/what-is-a-signal-jammer-and-how-does-it-work/>. [Último acceso: 10 03 2026].
- [18] Y. Wang y e. al, «Performance Analysis of a Normal GNSS Receiver Model under Different Types of Jamming Signals,» *Measurement*, vol. 214, p. 112786, 2023.
- [19] K. Radoš, M. Brkić y D. Begušić, «Recent Advances on Jamming and Spoofing Detection in GNSS,» *Sensors*, vol. 24, nº 13, 2024.
- [20] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon y P. M. Kintner, «Assessing the spoofing threat: Development of a portable GPS civilian spoofer,» de *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008)*, Savannah, 2008.
- [21] D. P. Shepard, J. A. Bhatti y T. E. Humphreys, «Drone hack: Spoofing attack demonstration on a civilian unmanned aerial vehicle,» *GPS World*, vol. 23, nº 8, pp. 30-33, 2012.
- [22] R. L. Fante y J. J. Vaccaro, «Cancellation of jammers and interference using a coherent wideband adaptive array,» *IEEE Transactions on Aerospace and Electronic Systems*, vol. 36, nº 4, pp. 1168-1178, 2000.
- [23] Meteksan Defence, «Anti-Jamming GNSS Systems: Spatial Filtering Techniques,» Meteksan Defence, 2024.
- [24] Hexagon | VERIPOS, «GAJT-710MS™ Product Sheet,» Hexagon Autonomy & Positioning, Aberdeen, 2020.
- [25] M. Jones, «gpsworld,» 12 abril 2017. [En línea]. Available: <https://www.gpsworld.com/anti-jam-technology-demystifying-the-crpa/>. [Último acceso: 11 febrero 2026].
- [26] Toyon Research Corporation, «Low Elevation Nulling Antenna (LENA) Datasheet,» Goleta, CA, 2025.
- [27] Oceaneering, «C-Nav977XF Low Elevation Angle Nulling Antenna (LEANA) Brochure,» 2024.
- [28] S. H. a. X. Z. a. X. W. a. H. Yi, «Design of a high accuracy ranging choke ring antenna,» *2023 International Conference on Microwave and Millimeter Wave Technology (ICMMT)*, pp. 1-3, 2023.

- [29] D. Tatarnikov, «GNSS Antennas that Protect and Observe,» *xyHt Magazine*, 2015.
- [30] E. Wallischeck, GPS Vulnerabilities in the Transportation Sector, 2016.
- [31] D. J. Moelker, «Multiple Antennas for Advanced GNSS Multipath Mitigation and Beamforming,» Delft University of Technology, Delft, Netherlands, 1997.
- [32] D. M. Pozar, Microwave Engineering, Hoboken, NJ: John Wiley & Sons, 2011.
- [33] C. A. Balanis, Antenna Theory: Analysis and Design (4th Edition), Wiley, 2016.
- [34] P. Savi y e. al., «Analysis of Radar Absorbing Materials for encasing GPS antennas».
- [35] J. B. Keller, «Geometrical Theory of Diffraction,» *Journal of the Optical Society of America*, vol. 52, pp. 116-130, 1962.
- [36] R. G. Kouyoumjian y P. H. Pathak, «A uniform geometrical theory of diffraction for an edge in a perfectly conducting surface,» *Proceedings of the IEEE*, vol. 62, nº 11, pp. 1448-1461, 1974.
- [37] C. A. Balanis, Advanced Engineering Electromagnetics, Hoboken, NJ: John Wiley & Sons, 2012.
- [38] H. W. Ott, Electromagnetic Compatibility Engineering, Hoboken, NJ: John Wiley & Sons, 2009.
- [39] Eltehs - GNSS OEM Store, «Especificaciones Técnicas Antena GNSS ELT0123,» Riga, 2026.
- [40] u-blox AG, «EVK-M8T User Guide,» u-blox AG, 2018.

ANEXO I: IMPLICACIONES SOCIALES, ECONÓMICAS, AMBIENTALES

Como cualquier proyecto de ingeniería de esta entidad, el compromiso del autor debe extenderse más allá de un simple estudio y experimentación rigurosos. Valorar y analizar las implicaciones derivadas del desarrollo del proceso resulta de valor capital para el ingeniero, y por tanto materia digna de mención en este trabajo de fin de grado.

Pese a ser un estudio nacido en el seno de una institución militar, la vulnerabilidad de los sistemas de posicionamiento, navegación y sincronización (PNT) no es una amenaza exclusiva de buques de guerra. Establecer un estándar en el uso de cavidades protectoras frente a las improvisadas que portan las marinas mercantes sería un gran salto en la seguridad de la navegación. Al asegurar la continuidad de la señal, la solución propuesta actúa como un sistema de seguridad vital, garantizando la navegación y protegiendo las cadenas de suministro globales de las que depende la sociedad.

Desde el punto de vista económico, este proyecto se ha concebido bajo una estricta premisa de eficiencia y viabilidad industrial. En el mercado actual, la protección frente a interferencias GNSS se confía principalmente a las antenas CRPA. Pese a su rendimiento superior, suponen un coste económico extraordinariamente elevado, requiriendo matrices de múltiples elementos, electrónica de procesamiento de señal compleja y complejas labores de integración. El coste por unidad de un sistema CRPA de grado militar o comercial avanzado puede ascender a decenas de miles de euros. Por el contrario, una cavidad cilíndrica representa una alternativa de diseño pasivo, robusto y de fabricación extremadamente económica, reduciendo el coste unitario a unas pocas decenas de euros. Esta drástica reducción de costes tiene una implicación directa en el ahorro de dinero público. Instituciones estatales (como la Armada, Salvamento Marítimo o la Guardia) operan cientos de unidades. Equipar la totalidad de una flota con tecnología CRPA resulta económicamente inviable para los presupuestos públicos en tiempo de paz. La estandarización de este apantallamiento pasivo permite un despliegue masivo y universal, logrando una relación coste-beneficio insuperable.

Obviando el peligro de los ataques a buques con cargas peligrosas, los cuales ya han causado catástrofes ambientales en el pasado, existe una gran ventaja en el ámbito del medioambiente con la instalación masiva de este blindaje. Frente a las soluciones activas, que requieren de tierras raras para la electrónica compleja, consumen energía constante del buque y generan residuos electrónicos (RAEE) al final de su vida útil, la cavidad diseñada es una estructura puramente pasiva. No requiere alimentación eléctrica y está propuesta para su fabricación en aluminio marino o acero inoxidable, materiales 100% reciclables que pueden ser reintroducidos en la economía circular sin generar impacto ambiental residual una vez el equipo sea dado de baja.

ANEXO II: REFLEXIONES ÉTICAS Y SOCIALES

El desarrollo de sistemas de apantallamiento electromagnético pasivo para la protección de señales GNSS plantea importantes reflexiones éticas y sociales, presentes en cualquier tecnología vinculada a la navegación y la defensa. En un contexto geopolítico donde la interferencia intencionada ha dejado de ser una amenaza exclusivamente militar para afectar de forma directa a la marina mercante y a la seguridad civil, esta tecnología nace con el propósito moral de salvaguardar la vida humana en el mar. Evitar la pérdida de posicionamiento o el control de la embarcación en aguas restringidas no es una solución absoluta para la prevención de colisiones, encallamientos y posibles desastres ecológicos; pero no le quita valor ser un apoyo más en estos campos, dotando a este proyecto de un claro carácter humanitario y de protección pública.

Su principal ventaja técnica e industrial, la simplicidad de fabricación y su accesibilidad económica, se convierte inmediatamente en su mayor vulnerabilidad ética. Un sistema diseñado para garantizar la operatividad de servicios de rescate, guardacostas o buques mercantes legítimos, exige la obligación ética de asegurar que este abaratamiento de costes no se traduzca jamás en una desprotección inaceptable de nuestras dotaciones. La eficiencia presupuestaria no debe priorizarse frente a la seguridad humana. Por tanto, la implementación de este cilindro protector debe concebirse como una ayuda genuina a la navegación para plataformas de bajo coste (como vehículos no tripulados) o como un sistema redundante de emergencia, pero bajo ningún concepto debería ser escogido como sustituto de tecnologías superiores en unidades navales de alto valor si ello implica comprometer la seguridad operativa y la vida de las tripulaciones.

podría ser fácilmente replicado por actores malintencionados. Organizaciones criminales, grupos de piratería o terrorismo podrían emplear esta misma solución geométrica en lanchas rápidas o drones para evadir los sistemas de inhibición de frecuencias desplegados por las Fuerzas y Cuerpos de Seguridad del Estado. Esta dualidad exige ser conscientes de la responsabilidad que conlleva el desarrollo de soluciones abiertas, aunque desde una perspectiva ética utilitarista, el beneficio global de proteger infraestructuras críticas e inocentes justifica plenamente su investigación.

En definitiva, la ingeniería debe mantenerse siempre al servicio de la sociedad, aplicando el principio de precaución. Aunque este proyecto ofrece una alternativa viable, rigurosa y eficaz ante la creciente amenaza de la guerra electrónica, resulta necesario formular dos preguntas fundamentales como reflexión final desde el punto de vista institucional, ¿dónde se establece la frontera moral entre la eficiencia económica en la licitación de equipos navales y el deber irrenunciable de proporcionar la máxima protección tecnológica disponible a quienes arriesgan su vida en el mar?

ANEXO III: GLOSARIO DE ABREVIATURAS Y ACRÓNIMOS

A continuación se detalla el significado de las siglas y acrónimos técnicos, operativos y doctrinales empleados a lo largo de esta memoria, ordenados alfabéticamente:

- **AIS:** *Automatic Identification System* (Sistema de Identificación Automática).
- **C/N0:** *Carrier-to-Noise Density Ratio* (Relación Portadora a Densidad de Ruido).
- **CDMA:** *Code Division Multiple Access* (Acceso Múltiple por División de Código).
- **CRPA:** *Controlled Reception Pattern Antenna* (Antena de Patrón de Recepción Controlado).
- **DOP:** *Dilution of Precision* (Dilución de la Precisión).
- **DoS:** *Denial of Service* (Denegación de Servicio).
- **ECEF:** *Earth-Centered, Earth-Fixed* (Sistema de Coordenadas Centrado en la Tierra y Fijo a la Tierra).
- **FOM:** *Figure of Merit* (Figura de Mérito).
- **GNSS:** *Global Navigation Satellite System* (Sistema Global de Navegación por Satélite).
- **GPS:** *Global Positioning System* (Sistema de Posicionamiento Global).
- **GTD / UTD:** *Geometrical Theory of Diffraction / Uniform Theory of Diffraction* (Teoría Geométrica/Uniforme de la Difracción).
- **HDOP / VDOP / PDOP:** *Horizontal / Vertical / Position Dilution of Precision* (Dilución de Precisión Horizontal / Vertical / Posicional).
- **IMU:** *Inertial Measurement Unit* (Unidad de Medición Inercial).
- **LENA:** *Low Elevation Nulling Antenna* (Antena de Anulación en Baja Elevación).
- **LNA:** *Low Noise Amplifier* (Amplificador de Bajo Ruido).
- **LoS:** *Line of Sight* (Línea de Visión / Línea de Vista).
- **MoM:** *Method of Moments* (Método de los Momentos).
- **NAVWAR:** *Navigation Warfare* (Guerra de Navegación / Guerra Electrónica de Navegación).
- **NMEA:** *National Marine Electronics Association* (Estándar de comunicación de datos de navegación).
- **NSM:** *Naval Strike Missile* (Misil de Ataque Naval).
- **PGM:** *Precision Guided Munition* (Munición Guiada de Precisión).
- **PNT:** *Positioning, Navigation, and Timing* (Posicionamiento, Navegación y Sincronización Temporal).
- **PRN:** *Pseudo-Random Noise* (Ruido Pseudoaleatorio - Identificador de satélites).
- **PRS:** *Public Regulated Service* (Servicio Público Regulado del sistema Galileo).
- **RAM:** *Radar Absorbing Material* (Material Absorbente de Radar).
- **RHCP:** *Right Hand Circular Polarization* (Polarización Circular a Derechas).
- **RMS:** *Root Mean Square* (Error Cuadrático Medio).

- **SAASM:** *Selective Availability Anti-Spoofing Module* (Módulo Anti-Spoofing de Disponibilidad Selectiva).
- **TERCOM:** *Terrain Contour Matching* (Navegación por Referencia de Contorno del Terreno).
- **UAV:** *Unmanned Aerial Vehicle* (Vehículo Aéreo No Tripulado).
- **UBX:** Protocolo de datos binarios propietario de la empresa u-blox.
- **UERE:** *User Equivalent Range Error* (Error de Rango Equivalente del Usuario).

ANEXO IV: REPOSITORIO GITHUB

Con el objetivo de garantizar la transparencia, la reproducibilidad de los experimentos y facilitar la auditoría de los algoritmos desarrollados para este Trabajo Fin de Grado, el código fuente íntegro ha sido extraído de esta memoria y alojado en un repositorio público de control de versiones.

Este repositorio contiene la totalidad de los *scripts* de MATLAB diseñados para el proyecto, abarcando desde la simulación electromagnética de onda completa mediante el Método de los Momentos (MoM), hasta la extracción y el posterior procesamiento estadístico de las tramas NMEA y UBX extraídas del receptor u-blox.

- **Título del repositorio:** Simulaciones Electromagnéticas y Procesado GNSS (TFG)
- **Autor:** Marcos Muiño Martínez
- **Plataforma:** GitHub
- **Enlace de acceso:** [<https://github.com/MarosMuino/Estudio-de-blindajes-antijamming-para-antenas-GNSS-en-buques-de-la-Armada>]

Los códigos se ordenan siguiendo el mismo orden en el que aparecen mencionados a lo largo de la memoria:

- Primero: ANTENA_DE_PARCHES_1.m donde se diseña una antena genérica de GNSS
- Segundo: DIMENSIONAMIENTO_2.m donde se devuelve un mapa de calor que muestra el valor de la protección en función de las dimensiones del cilindro
- Tercero: PDOP_FRENTE_A_MASCARA_3.m devuelve una gráfica para establecer el valor máximo de máscara que se puede permitir el blindaje sin degradar exageradamente la precisión (almanaques YUMA)
- Cuarto: RANGO_PDOP_CON_MASCARA_4.m devuelve la variación del rango de PDOP a lo largo de un período de tiempo determinado y máscara establecida (almanaques YUMA)
- Quinto: DIAGRAMA_ANTENA_CON_CAVIDAD_5.m obtenemos el valor nuevo diagrama de protección de la antena
- Sexto: COMPARACION_CAVIDAD_MALLA_6.m grafica el diagrama resultante usando cavidad normal o con malla
- Séptimo: UBX_A_TABLAS_DE_PRECISION_7.m recupera datos de precisión de posicionamiento a partir de grabaciones de u-center
- Octavo: UBX_A_AZIMUT_CN0_8.m grafica los valores de densidad de señal recibida respecto acimut de los satélites con datos de grabaciones de u-blox

ANEXO V: TABLAS DE DATOS DE PRECISI3N

Parameter | Unit | Minimum | Maximum | Mean | Std Dev | RMS

13/03/2026 20:15-08:11

VDOP	-	0.95	99.99	1.45	3.08	3.40
HDOP	-	0.76	99.99	1.03	3.08	3.25
PDOP	-	1.23	99.99	1.74	3.07	3.53
Satellites	-	8	11	9.58	0.73	9.60
eECEF_X	m	-3.42e+00	5.41e+00	5.34e-09	1.80e+00	1.80e+00
eECEF_Y	m	-1.89e+00	1.58e+00	3.04e-09	7.79e-01	7.79e-01
eECEF_Z	m	-3.06e+00	1.06e+01	-6.12e-09	1.47e+00	1.47e+00
eECEF_total	m	1.18e-01	1.12e+01	2.10e+00	1.27e+00	2.45e+00

15/03/2026 22:02-08:05

VDOP	-	0.89	2.35	1.34	0.29	1.37
HDOP	-	0.70	1.24	0.94	0.12	0.95
PDOP	-	1.14	2.65	1.64	0.30	1.66
Satellites	-	8	12	9.72	0.90	9.76
eECEF_X	m	-4.81e+00	6.61e+00	-6.23e-09	2.22e+00	2.22e+00
eECEF_Y	m	-2.92e+00	2.06e+00	-8.15e-10	1.02e+00	1.02e+00
eECEF_Z	m	-3.25e+00	3.44e+00	-8.13e-11	1.50e+00	1.50e+00
eECEF_total	m	1.05e-01	7.37e+00	2.58e+00	1.24e+00	2.86e+00

17/03/2026 09:22-15:35

VDOP	-	0.89	3.12	1.28	0.25	1.30
HDOP	-	0.70	1.80	0.91	0.13	0.92
PDOP	-	1.14	3.36	1.57	0.27	1.60
Satellites	-	6	12	10.14	1.25	10.22
eECEF_X	m	-5.43e+00	9.46e+00	9.45e-09	1.99e+00	1.99e+00
eECEF_Y	m	-3.56e+00	4.08e+00	-1.54e-09	1.03e+00	1.03e+00
eECEF_Z	m	-5.94e+00	8.20e+00	-7.33e-09	1.65e+00	1.65e+00
eECEF_total	m	7.57e-02	9.93e+00	2.43e+00	1.35e+00	2.78e+00

18/03/2026 08:22-14:27

VDOP	-	0.88	99.99	1.48	3.95	4.22
HDOP	-	0.71	99.99	1.08	3.96	4.10
PDOP	-	1.15	99.99	1.77	3.94	4.32
Satellites	-	4	12	9.94	1.44	10.04
eECEF_X	m	-6.54e+00	1.27e+01	-3.29e-09	2.70e+00	2.70e+00
eECEF_Y	m	-6.32e+00	4.91e+00	2.04e-09	1.18e+00	1.18e+00
eECEF_Z	m	-5.69e+00	9.03e+00	-6.13e-09	2.19e+00	2.19e+00
eECEF_total	m	4.53e-02	1.50e+01	3.05e+00	2.04e+00	3.67e+00

18/03/2026 14:32-20:23

VDOP	-	0.92	99.99	1.64	4.60	4.88
HDOP	-	0.76	99.99	1.29	4.61	4.79
PDOP	-	1.20	99.99	2.00	4.59	5.00
Satellites	-	5	11	8.53	1.07	8.60
eECEF_X	m	-1.12e+01	1.38e+01	-1.42e-09	3.30e+00	3.30e+00
eECEF_Y	m	-4.08e+00	4.80e+00	3.19e-10	1.31e+00	1.31e+00
eECEF_Z	m	-6.24e+00	8.84e+00	-7.57e-09	2.65e+00	2.65e+00
eECEF_total	m	1.87e-01	1.45e+01	3.77e+00	2.33e+00	4.43e+00

19/03/2026 08:15-15:23

VDOP	-	0.89	99.99	1.30	1.38	1.90
HDOP	-	0.70	99.99	0.93	1.37	1.66
PDOP	-	1.13	99.99	1.60	1.38	2.11
Satellites	-	7	12	9.67	0.93	9.72
eECEF_X	m	-4.31e+00	4.79e+00	4.00e-09	1.63e+00	1.63e+00
eECEF_Y	m	-2.84e+00	3.01e+00	1.42e-10	9.43e-01	9.43e-01
eECEF_Z	m	-6.31e+00	5.87e+00	-8.31e-10	1.45e+00	1.45e+00
eECEF_total	m	6.91e-02	7.38e+00	2.04e+00	1.21e+00	2.37e+00

19/03/2026 15:23-21:57

VDOP	-	1.06	4.34	1.56	0.46	1.63
HDOP	-	0.80	2.89	1.05	0.17	1.07
PDOP	-	1.34	5.21	1.89	0.47	1.95
Satellites	-	6	10	8.90	0.91	8.95
eECEF_X	m	-1.04e+01	1.42e+01	2.15e-09	4.04e+00	4.04e+00
eECEF_Y	m	-9.24e+00	4.68e+00	-4.67e-10	2.10e+00	2.10e+00
eECEF_Z	m	-8.74e+00	1.51e+01	-1.94e-08	3.29e+00	3.29e+00
eECEF_total	m	7.93e-02	2.01e+01	4.61e+00	3.21e+00	5.61e+00

21/03/2026 13:58-20:11

VDOP	-	0.90	2.54	1.39	0.37	1.43
HDOP	-	0.66	1.78	0.95	0.18	0.97
PDOP	-	1.12	3.10	1.68	0.40	1.73
Satellites	-	6	12	9.59	1.20	9.67
eECEF_X	m	-4.88e+00	5.64e+00	1.46e-09	1.86e+00	1.86e+00
eECEF_Y	m	-3.26e+00	2.83e+00	-5.59e-10	1.17e+00	1.17e+00
eECEF_Z	m	-3.36e+00	4.36e+00	3.62e-09	1.24e+00	1.24e+00
eECEF_total	m	6.30e-02	6.73e+00	2.25e+00	1.14e+00	2.52e+00

21/03/2026 20:23-07:08

VDOP	-	0.94	2.02	1.27	0.16	1.28
HDOP	-	0.72	1.34	0.89	0.11	0.89
PDOP	-	1.24	2.38	1.55	0.17	1.56
Satellites	-	7	12	10.55	1.05	10.61
eECEF_X	m	-2.71e+00	2.90e+00	3.15e-09	8.55e-01	8.55e-01
eECEF_Y	m	-1.55e+00	1.63e+00	-3.28e-09	4.13e-01	4.13e-01
eECEF_Z	m	-3.54e+00	3.55e+00	-6.32e-09	9.86e-01	9.86e-01
eECEF_total	m	4.98e-02	4.12e+00	1.18e+00	6.86e-01	1.37e+00

22/03/2026 07:15-13:32

VDOP	-	0.89	99.99	1.34	2.86	3.15
HDOP	-	0.75	99.99	1.05	2.86	3.05
PDOP	-	1.17	99.99	1.67	2.85	3.30
Satellites	-	6	12	9.28	1.08	9.34
eECEF_X	m	-5.90e+00	6.41e+00	-1.37e-09	1.81e+00	1.81e+00
eECEF_Y	m	-2.12e+00	2.51e+00	-4.39e-10	8.28e-01	8.28e-01
eECEF_Z	m	-5.40e+00	5.02e+00	2.87e-09	1.96e+00	1.96e+00
eECEF_total	m	3.81e-02	8.14e+00	2.50e+00	1.24e+00	2.79e+00

22/03/2026 13:35-20:32

VDOP	-	0.95	2.98	1.40	0.26	1.43
HDOP	-	0.79	1.80	1.00	0.13	1.01
PDOP	-	1.23	3.29	1.72	0.27	1.75

Satellites	-	6	11	9.14	0.92	9.19
eECEF_X	m	-5.83e+00	6.92e+00	1.93e-09	2.42e+00	2.42e+00
eECEF_Y	m	-2.64e+00	2.66e+00	-7.77e-10	9.98e-01	9.98e-01
eECEF_Z	m	-4.84e+00	6.80e+00	4.42e-09	2.11e+00	2.11e+00
eECEF_total	m	2.56e-01	9.10e+00	3.01e+00	1.50e+00	3.36e+00