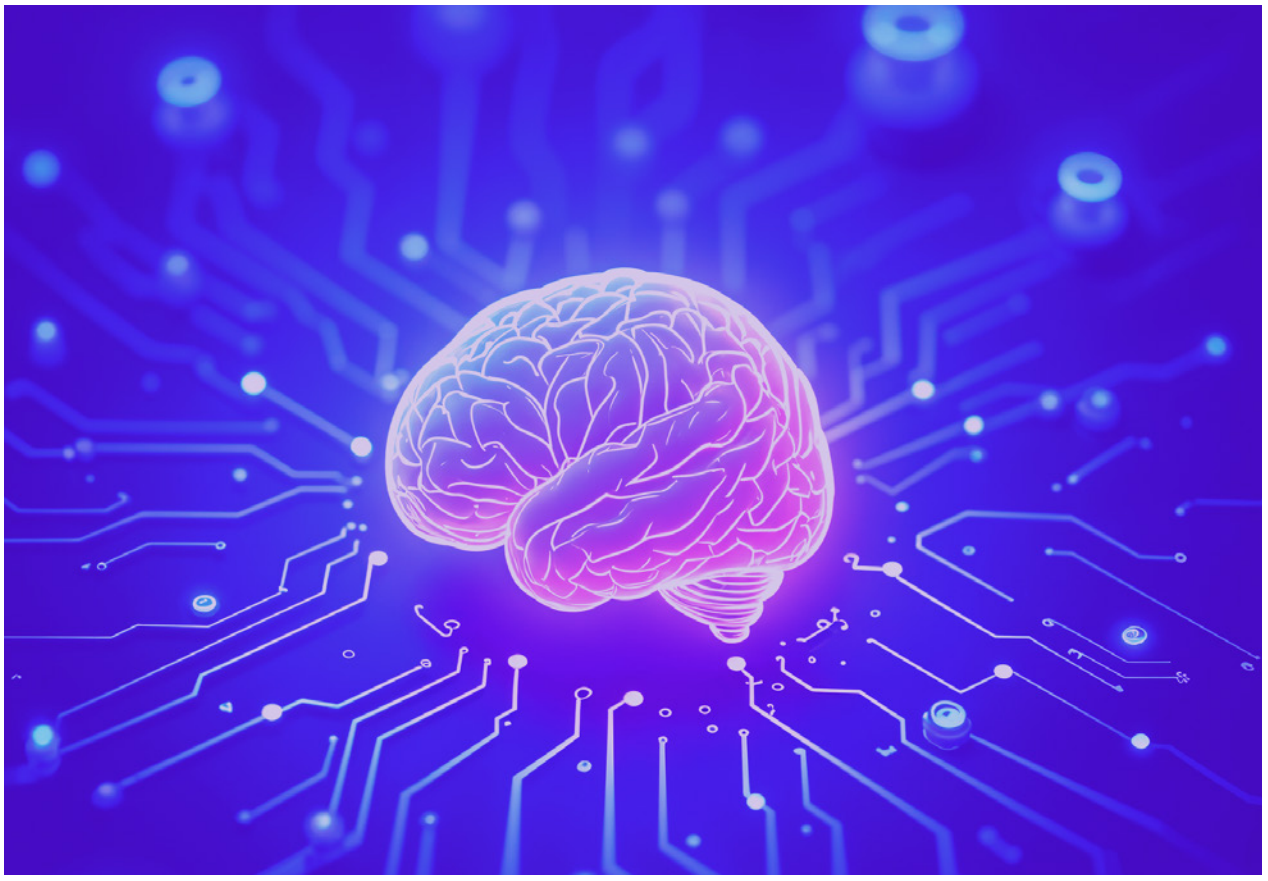


COSPAS-SARSAT, INTELIGENCIA ARTIFICIAL Y CIBERSEGURIDAD

CONVERGENCIA TECNOLÓGICA PARA LA CIBERDEFENSA GLOBAL

Por BR (R) **GERARDO RUBÉN BIDEGAIN**

Palabras Clave:

> COSPAS-SARSAT
> Ciberseguridad Espacial
> Inteligencia Artificial
> MEOSAR
> Infraestructura Crítica
> Resiliencia operativa
> Cooperación internacional

1. Introducción

El Sistema Internacional **COSPAS-SARSAT (C/S)** constituye una de las expresiones más destacadas de cooperación tecnológica internacional, diseñado para detectar y localizar balizas de emergencia, como ser las ***"Emergency Position Indicating Radio Beacons" (EPIRBs);*** "Emergency Locator Transmitters" (ELTs) y ***"Personal Locator Beacons"*** (PLBs), que permiten salvar vidas en contextos marítimos, aéreos y terrestres respectivamente. Desde su concepción en 1982, el C/S ha operado como un instrumento humanitario crítico, pero su relevancia trasciende el mero rescate de vidas; se erige como *una infraestructura estratégica que integra múltiples plataformas satelitales, redes terrestres y sistemas de gestión de información*.

Es una iniciativa de cooperación internacional, de carácter humanitario y sin fines de lucro, que tiene como objetivo principal la detección y localización de balizas de emergencia para asistir en operaciones de "Search and Rescue" – "Búsqueda y Rescate" (SAR) en todo el mundo. Su nombre es un acrónimo de **"COSPAS"** (en ruso "Cosmicheskaya Sistema Poiska Avariynyh Sudovpara" - "Sistema Espacial para la Búsqueda de Buques en Peligro") y **"SARSAT"** (en inglés "Search And Rescue Satellite-Aided Trackingpara" - "Rastreo por Satélite para Búsqueda y Rescate").

Las balizas según el ámbito de uso se clasifican de la siguiente manera:

> **EPIRBs,** es una baliza de emergencia diseñada para **uso marítimo**. Se activa manualmente o automáticamente al entrar en contacto con el agua y envía una señal de socorro que ayuda a los servicios de rescate a localizar embarcaciones en peligro.
> **ELTs**, es una baliza de emergencia para **uso aeronáutico.** Se instala en aeronaves y se activa automáticamente con un impacto severo o manualmente por la tripulación. Su función es transmitir una señal de socorro que permite a los equipos SAR localizar el lugar de un accidente aéreo.
> **PLBs**, es una baliza de emergencia personal para **uso principalmente en tierra**, pero también su uso es posible en el mar o aire. Está diseñada para ser transportada por individuos y se activa manualmente.

2. Evolución histórica del COSPAS-SARSAT (1982–2025)

El Sistema C/S surgió en plena Guerra Fría como un proyecto de cooperación multilateral sin precedentes, involucrando a la Unión Soviética, Estados Unidos, Canadá y Francia. Su objetivo inicial fue la localización de personas en peligro mediante el uso de satélites **"Low Earth Orbit" (Satélites de Órbita Baja-LEO)** y **"Geostationary Equatorial Orbit"** (Satélites de Órbita Geoestacionaria-GEO), combinando capacidades de detección de señales de emergencia con Centros de Control Terrestre distribuidos internacionalmente.

Los satélites de **"Medium Earth Orbit" (Satélites de Órbita Terrestre Media - MEO)** fueron incorporados al Sistema C/S como parte de la evolución hacia el segmento **"Medium Earth Orbit Search and Rescue" (MEOSAR).** Este avance comenzó con pruebas y evaluaciones en la década de 2000, con la participación de constelaciones de satélites como:

> Galileo, es el sistema de navegación por satélite de la Unión Europea, diseñado para ofrecer posicionamiento global preciso y autónomo. La constelación está compuesta por satélites en órbita media y proporciona servicios tanto civiles como gubernamentales.
> GLONASS, es el sistema de navegación por satélite desarrollado por Rusia como alternativa al GPS. Operativo desde la década de 1990, ofrece servicios de posicionamiento y navegación a nivel global mediante una constelación de satélites en órbita terrestre media.
> GPS, es el sistema de navegación por satélite de EE.UU. Proporciona servicios de posicionamiento, navegación y sincronización a nivel mundial mediante una constelación de satélites en órbita terrestre media. Es ampliamente utilizado en aplicaciones civiles, comerciales y militares.

El Sistema MEOSAR estuvo operativo a partir del 13 de diciembre de 2016, cuando se inició la distribución operativa de datos de alertas de rescate. Posteriormente, el 25 de abril de 2023, el Consejo de COSPAS-SARSAT declaró la **"Capacidad Operativa Inicial" (IOC)** del sistema mencionado, consolidando su rol como la principal tecnología **para la localización de balizas de emergencia de 406 MHz.**

Esta incorporación ha permitido mejorar significativamente la precisión, rapidez y cobertura global en las operaciones SAR. Es un servicio satelital internacional destinado a detectar y localizar señales de socorro emitidas por balizas en situaciones de emergencia, facilitando operaciones SAR en tierra, mar o aire, al combinar las ventajas de los satélites LEO, ubicada entre

La creciente digitalización y la amenaza de ciberataques han convertido la integración de Inteligencia Artificial (IA) y Ciberseguridad Espacial (CE) en un elemento central para garantizar la resiliencia del sistema frente a amenazas contemporáneas.

los 160 y 2.000 km de altitud. Esta órbita es utilizada por satélites de observación, comunicaciones, investigación científica y estaciones espaciales debido a su baja latencia y proximidad a la Tierra y los GEO, se encuentra a unos 35.786 km sobre el ecuador. Los satélites en esta órbita giran a la misma velocidad que la Tierra, por lo que permanecen fijos sobre un punto del planeta. Es ideal para comunicaciones, meteorología y retransmisiones.

El sistema se consolidó mediante mejoras en la precisión de localización y expansión de su cobertura global. Entre los desarrollos más significativos se encuentran:

> La integración de satélites de nueva generación (LEO de órbita polar y GEO modernizados).
> La Implementación de protocolos de comunicación digital y cifrado avanzado.
> La extensión de la cooperación con organismos internacionales como la Unión Internacional de Telecomunicaciones (ITU); Organización de Aviación Civil Internacional (ICAO); Organización Marítima Internacional (IMO) y Agencia Espacial Europea (ESA).
> Los primeros estudios sobre el impacto de ciberamenazas y posibles escenarios de interferencia tecnológica, incluyendo vulnerabilidades de la cadena de suministro y ataques de día cero.

El Sistema C/S ha evolucionado hacia un sistema robusto y altamente interoperable, capaz de integrarse con otras plataformas de rescate y monitoreo internacional, constituyéndose como modelo de infraestructura crítica global. Su avance ha estado marcado por la modernización tecnológica y la expansión de su cobertura, consolidándose como una infraestructura crítica de importancia estratégica internacional. **La creciente digitalización y la amenaza de ciberataques han convertido la integración de Inteligencia Artificial (IA) y Ciberseguridad Espacial (CE) en un elemento central para garantizar la resiliencia del sistema frente a amenazas contemporáneas.**

3. Arquitectura técnica del sistema

El Sistema C/S se estructura en tres segmentos interdependientes:

1. **Segmento Espacial:** Satélites LEO, GEO y MEO equipados con receptores para señales de emergencia en 406 MHz.
2. **Segmento Terrestre:**
> **Local User Terminals (LUTs)**: Estaciones de recepción de las señales satelitales.
> **Mission Control Centers (MCCs):** procesan la información, realizan correlación de señales y envían alertas a los Centros de Coordinación Locales de Rescate.
3. **Segmento de Balizas (EPIRBs, ELTs, PLBs):**
> Dispositivos autónomos con capacidad de transmisión inmediata ante situaciones de emergencia.
> Incorporación de tecnologías de GPS para localización precisa.

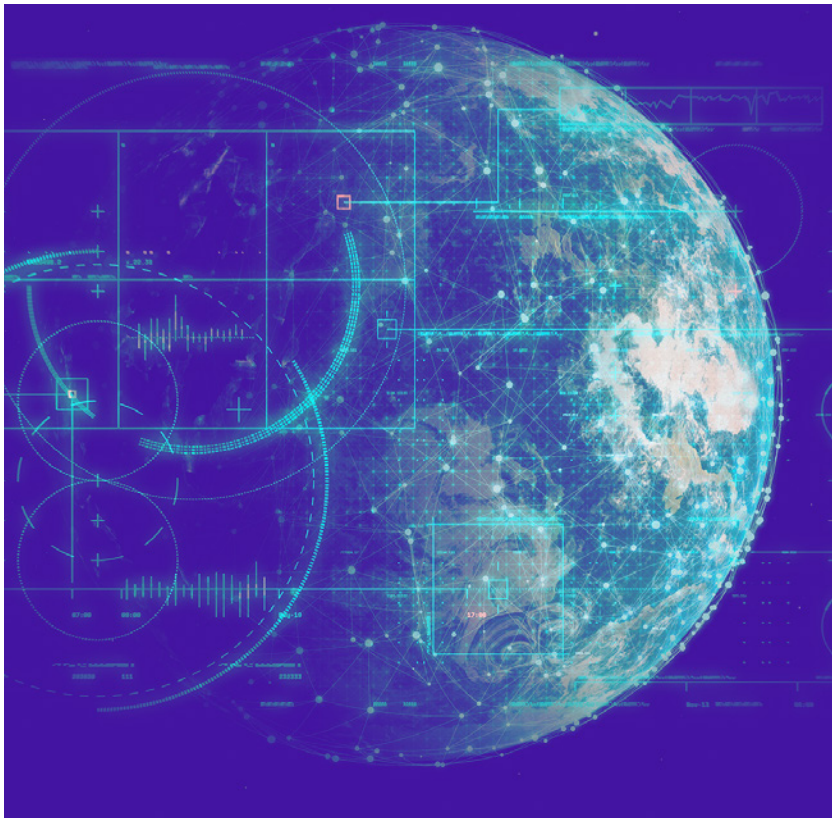
Este esquema técnico permite *alta disponibilidad, redundancia y resiliencia frente a fallos puntuales o ciberataques, aunque no está exento de vulnerabilidades emergentes.* Estos desarrollos permitieron que el Sistema C/S pasara de ser un *sistema de rescate humanitario básico a convertirse en una infraestructura estratégica de alto valor, cuya resiliencia y operatividad resultan fundamentales no solo para la seguridad humana, sino también para la estabilidad tecnológica y estratégica internacional.*

4. COSPAS-SARSAT como infraestructura crítica internacional

Más allá de su misión humanitaria, **el C/S se reconoce como una infraestructura crítica internacional, ya que impacta la seguridad marítima, aérea y terrestre de múltiples naciones y constituye un nodo vital en la interoperabilidad satelital global.** Por ello, es necesario **clasificar este sistema como prioridad estratégica,** estableciendo protocolos de monitoreo, planes de contingencia multinacionales y políticas de cooperación tecnológica internacional.

Junto con su misión humanitaria, el C/S asume funciones estratégicas que impactan la seguridad internacional, ya que:

> Garantiza la continuidad de operaciones de rescate global.



- Constituye un nodo crítico en la interoperabilidad satelital internacional.
- Su operación afecta directamente la seguridad de sistemas marítimos, aeronáuticos y terrestres de múltiples países.

En la era de la digitalización y la creciente complejidad de la ciberamenaza, la cual la podemos definir como *"toda acción, evento o posibilidad que busca vulnerar la seguridad de sistemas informáticos, redes o infraestructuras críticas mediante medios digitales, pudiendo implicar robo de información, sabotaje, interrupción de servicios o manipulación de datos".*

La convergencia de IA y CE, *"es el conjunto de medidas, políticas y tecnologías orientadas a proteger satélites, sistemas de control en tierra, enlaces de comunicación y servicios espaciales frente a ciberamenazas; siendo su objetivo garantizar la disponibilidad, integridad y confidencialidad de la información y las operaciones en el ámbito espacial"*, se vuelve un componente indispensable para garantizar la resiliencia del sistema.

Este trabajo intenta analizar la CE desde una perspectiva histórica, técnica y estratégica, abordando tanto las vulnerabilidades cibernéticas existentes como el potencial de la IA para mitigar riesgos. Asimismo, se proponen estrategias de protección orientadas a fortalecer la seguridad y sostenibilidad del entorno espacial, considerando las principales vulnerabilidades cibernéticas, el potencial de la IA y la formulación de estrategias de protección para fortalecer la seguridad del sistema en cuestión.

5. Vulnerabilidades y amenazas en el contexto de Ciberseguridad Espacial

El sistema enfrenta múltiples vulnerabilidades:

- **Spoofing:** señales falsas que pueden inducir a errores en la localización de emergencias.
- **Jamming:** interferencia intencionada de la frecuencia 406 MHz, degradando la recepción de señales.
- **Supply Chain:** Vulnerabilidad de cadena de suministro, que permiten comprometer sistemas críticos a través de proveedores o fallas aún no parcheadas.
- **Ataques de Día Cero:** es un ataque que explota una vulnerabilidad **desconocida** del software o hardware, que aún no ha sido detectada ni corregida por los desarrolladores.
- **Accesos no autorizados a los MCCs:** potencial manipulación de datos críticos.
- **Interdependencia tecnológica:** dependencia de satélites y redes externas que pueden ser vulnerables.

6. Aplicaciones de la Inteligencia Artificial en el Sistema SAR

La IA aporta mejoras significativas al sistema:

- **Clasificación automática de señales:** filtra falsas alarmas y prioriza rescates.
- **Mantenimiento predictivo:** anticipa fallos de hardware y optimiza la disponibilidad de satélites y estaciones terrestres.
- **Optimización logística:** planificación de rutas de respuesta y coordinación de equipos de rescate.
- **Predicción de incidentes y análisis de riesgos:** La IA permite anticipar escenarios complejos de emergencia, evaluar probabilidades de ocurrencia y vincular estos análisis con estrategias de Ciberseguridad, mejorando la resiliencia del sistema.

7. Inteligencia Artificial aplicada a la Ciberdefensa satelital

La IA se ha consolidado como una herramienta esencial en el

CV

BM (R) GERARDO RUBÉN BIDEGAIN

Brigadier Gerardo Rubén Bidegain, Licenciado en Sistemas Aéreos y Aeroespaciales y posgrados en Gestión para la Defensa Nacional y Producción de Información Estratégica. Especialista en Comunicaciones, con cargos en Dirección de Comunicaciones e Informática FAA, Presidencia de la Nación, Sistema COSPAS-SARSAT y J-VI C3 I GE. Participó en proyectos estratégicos, cumbres presidenciales y misiones internacionales, incluyendo Observador Militar ONU en Mozambique. Reconocimientos: Medalla ONU, premios institucionales y distinciones docentes.

ámbito de la Ciberdefensa, al potenciar las capacidades de detección, análisis y respuesta ante amenazas digitales. Su integración en sistemas de seguridad permite identificar patrones anómalos en tiempo real, automatizar respuestas ante incidentes y anticiparse a posibles ataques mediante técnicas predictivas. Estos avances mejoran significativamente la eficiencia de los equipos de seguridad y reducen el tiempo de reacción frente a incidentes.

En lugar de tratar estos beneficios en distintas secciones, es más efectivo presentar un enfoque integrado: *la IA no solo facilita la detección de intrusiones o la contención automatizada de amenazas, sino que también optimiza la gestión de riesgos y la asignación de recursos en entornos complejos.* De esta forma, su rol no se limita a la reacción, sino que se extiende a la prevención y adaptación continua frente a un panorama de amenazas en constante evolución.

La IA desempeña un rol clave en Ciberdefensa:

- **Detección de intrusiones (IDS) en satélites:** identifica comportamientos anómalos o no autorizados.
- **Respuesta automática a amenazas:** bloquea ataques y genera protocolos de mitigación en tiempo real.
- **Simulación de ciberataques:** permite anticipar vulnerabilidades emergentes y entrenar al personal en escenarios controlados.

Para fortalecer la resiliencia y capacidad estratégica del sistema, se proponen las siguientes líneas de acción para un observatorio de Ciberdefensa:

1. Fomentar alianzas internacionales de investigación permanente en Ciberseguridad espacial, inteligencia artificial y resiliencia operativa.
2. Fomentar alianzas internacionales con organismos como ITU, ESA, ICAO y la Secretaría de C/S para compartir información sobre amenazas y mejores prácticas.
3. Implementar un marco normativo nacional con criptografía post-cuántica, estándares de Ciberseguridad y protocolos de protección de infraestructura crítica.
4. Realizar ejercicios conjuntos de Ciberseguridad y SAR para entrenar personal y validar protocolos de respuesta ante contingencias.
5. Formar talentos multidisciplinarios, combinando expertos en IA, Ciberseguridad, ingeniería espacial y operaciones de rescate.

En el ámbito de la Ciberdefensa, la IA posibilita la detección temprana de intrusiones y anomalías en sistemas satelitales, la automatización de respuestas

frente a ataques y la simulación de escenarios complejos para el entrenamiento de personal especializado. La implementación de estas tecnologías permite anticipar amenazas, reducir tiempos de reacción y fortalecer la resiliencia de la infraestructura crítica.

La integración de IA con sistemas de monitoreo continuo y análisis predictivo constituye un componente esencial para la protección del C/S frente a ataques híbridos, interferencias estratégicas y manipulación de datos críticos. Asimismo, la IA facilita la elaboración de informes prospectivos y la planificación de estrategias de mitigación basadas en escenarios de riesgo.

8. Escenarios prospectivos y riesgos estratégicos

El contexto global actual indica que la proliferación de actores con capacidades cibernéticas avanzadas y la interdependencia tecnológica de infraestructuras interconectadas generan riesgos estratégicos complejos. La preparación ante estos escenarios requiere el desarrollo de estrategias multinacionales, el fortalecimiento de alianzas internacionales y la implementación de tecnologías avanzadas de Ciberdefensa.

El sistema enfrenta riesgos derivados de la militarización del espacio, la proliferación de actores con capacidades cibernéticas y el aumento de interdependencias tecnológicas:

- Conflictos híbridos con ataques cibernéticos sobre satélites LEO, GEO y MEO.
- Interferencia estratégica en operaciones SAR durante crisis humanitarias.
- Competencia internacional por control y acceso a frecuencias críticas.
- Riesgo de desinformación y manipulación de datos críticos en operaciones de rescate.

9. Sugerencias para fortalecer y proteger el Sistema COSPAS-SARSAT

Sugerencia 1: Clasificación de COSPAS-SARSAT como infraestructura crítica prioritaria: El Sistema C/S constituye una infraestructura esencial para la seguridad y salvamento internacional, operando en un marco multilateral que permite la detección y localización de personas, buques y aeronaves en situación de emergencia. Dada su relevancia estratégica, el sistema en cuestión debería ser clasificado como **"Infraestructura Crítica Prioritaria"**, reconociendo formalmente su vulnerabilidad frente a amenazas cibernéticas y físicas.

Esta clasificación implicaría la implementación de **"Protocolos de Monitoreo Continuo"** sobre todos los componentes críticos del sistema, incluyendo satélites, estaciones terrenas y enlaces de comunicaciones, con especial énfasis en la detección temprana de intrusiones, interferencias o anomalías operativas que puedan comprometer la integridad, disponibilidad o confiabilidad del servicio.

Asimismo, se sugiere el diseño y puesta en marcha de **"Planes de Contingencia Multinacionales"**, coordinados entre los Estados miembros de C/S, que contemplen escenarios de interrupción parcial o total del sistema. Dichos planes podrían incluir:

1. **Procedimientos de respaldo y redundancia:** Establecer rutas alternativas de comunicación, capacidades de retransmisión y satélites de reemplazo en caso de fallo.
1. **Cooperación internacional y protocolos de alerta:** Definir mecanismos de comunicación rápida entre centros de control de diferentes países para garantizar una respuesta coordinada ante emergencias.
1. **Pruebas y simulacros periódicos:** Realizar ejercicios regulares que validen la efectividad de los procedimientos de contingencia y el tiempo de respuesta frente a incidentes cibernéticos o físicos.
1. **Evaluación y actualización continua:** Mantener un registro dinámico de vulnerabilidades, amenazas emergentes y mejores prácticas internacionales, asegurando que la protección del sistema evolucione al ritmo de los avances tecnológicos y tácticas de ataque.

La adopción permitiría adoptar reforzar la **resiliencia operativa del Sistema C/S**, asegurando que continúe cumpliendo su misión crítica de salvar vidas y brindar servicios de alerta de emergencia a nivel global, incluso ante incidentes de Ciberseguridad de alta complejidad o conflictos internacionales.

Sugerencia 2: Mapear vulnerabilidades y diseñar planes de mitigación cibernética: Dada la creciente sofisticación de las amenazas cibernéticas, es imprescindible que el Sistema C/S cuente con un **"Programa Integral de Identificación de Vulnerabilidades"** y **"Mitigación de Riesgos"**, garantizando la continuidad y confiabilidad de sus operaciones críticas. Para ello, se propone implementar las siguientes acciones:

1. **Mapeo exhaustivo de vulnerabilidades:** Realizar un inventario detallado de todos los componentes del sistema (satélites, estaciones terrenas, enlaces de comunicación, servidores y software de gestión), identificando posibles puntos de ataque, debilidades en protocolos de comunicación y riesgos asociados a terceros proveedores. Este mapeo debe actualizarse periódicamente, considerando nuevas tecnologías y amenazas emergentes.
2. **Pruebas de penetración cibernética controladas bajo**

estándares internacionales: Ejecutar simulaciones de ataques bajo entornos controlados para evaluar la resiliencia del sistema frente a intrusiones, ransomware, interferencias satelitales o manipulación de datos críticos. Los resultados de estas pruebas deben servir para priorizar acciones correctivas y fortalecer los mecanismos de defensa.

3. **Redundancia tecnológica:** Implementar **sistemas paralelos y rutas de comunicación** alternativas que garanticen la continuidad operativa ante fallas de hardware, interrupciones de enlace o ataques dirigidos. Esto incluye servidores de respaldo, enlaces satelitales duplicados y mecanismos automáticos de conmutación ante fallos.
4. **Planes de mitigación integrales:** Con base en el mapeo de vulnerabilidades y las pruebas de penetración, se deben desarrollar **procedimientos de respuesta y recuperación,** incluyendo la priorización de activos críticos, protocolos de comunicación de incidentes y ejercicios de simulación de escenarios de contingencia.

La adopción de estas medidas permitiría que el Sistema C/S mantenga una **postura defensiva proactiva,** reduciendo significativamente el riesgo de interrupciones operativas y asegurando que el sistema pueda continuar ofreciendo servicios esenciales de alerta y rescate en situaciones de emergencia a nivel global.

Sugerencia 3: Fortalecer la cooperación internacional y el intercambio seguro de información. El Sistema C/S opera bajo un esquema multinacional, donde la coordinación entre estados miembros es esencial para garantizar la efectividad de las operaciones SAR. En este contexto, se podría establecer medidas que aseguren tanto la colaboración como la protección de información crítica frente a amenazas cibernéticas y operativas, de acuerdo al siguiente detalle:

1. **Protocolos estandarizados de intercambio de información con autenticación robusta y cifrado:** Desarrollar y adoptar procedimientos uniformes que permitan la transferencia segura de datos de emergencias entre Centros de Control, estaciones terrenas y agencias SAR. Esto incluye el uso de protocolos de autenticación robustos y firmas digitales para validar la integridad de la información.
2. **Acuerdos de cooperación multinacional: Formalizar "Memorandos de Entendimiento y Convenios Operativos"** que definan roles, responsabilidades y mecanismos de alerta temprana entre los estados miembros, asegurando una respuesta coordinada ante incidentes y la disponibilidad de recursos compartidos.
3. **Redes de comunicación resilientes y segregadas:** Implementar canales de comunicación redundantes y segmentados que minimicen el riesgo de interrupciones o interferencias externas, garantizando que la información crítica pueda fluir incluso en escenarios de ataque cibernético o fallas técnicas.
4. **Capacitación conjunta y ejercicios de interoperabilidad:** Organizar simulacros regulares y programas de formación multinacional que entrenen al personal en la operación conjunta del sistema, manejo seguro de información y respuesta ante incidentes, fortaleciendo la confianza y la coordinación entre países.
5. **Monitoreo y auditoría continua:** Establecer mecanismos de seguimiento permanente para evaluar la efectividad de la cooperación internacional y detectar posibles brechas de seguridad o fallos operativos, incorporando mejoras continuas basadas en lecciones aprendidas y estándares internacionales de ciberseguridad.

En el ámbito de la Ciberdefensa, la IA posibilita la detección temprana de intrusiones y anomalías en sistemas satelitales, la automatización de respuestas frente a ataques y la simulación de escenarios complejos para el entrenamiento de personal especializado.

La implementación de estas medidas fortalecería la **resiliencia global del Sistema C/S**, asegurando que los flujos de información crítica sean confiables y que la cooperación multinacional se mantenga eficiente incluso frente a amenazas cibernéticas sofisticadas, ataques dirigidos o interrupciones operativas.

Sugerencia 4: Implementar programas de capacitación y concientización en Ciberseguridad para personal clave. La protección del Sistema C/S no recae exclusivamente en medidas tecnológicas, sino también en el factor humano, considerado uno de los eslabones más críticos en la seguridad de infraestructuras estratégicas. Por ello, se recomienda establecer un "Programa Integral de Formación" y concientización en Ciberseguridad dirigido al personal operativo, técnico y de gestión involucrado en la operación del sistema, a través de:

1. **Capacitación especializada:** Desarrollar cursos y talleres avanzados que aborden **amenazas cibernéticas emergentes, protocolos de seguridad, respuesta a incidentes y manejo de sistemas críticos,** adaptados al nivel de responsabilidad de cada rol dentro de la organización.
2. **Simulaciones de incidentes y ejercicios prácticos: Implementar ejercicios regulares de ciberataques simulados** que permitan al personal practicar la detección, mitigación y recuperación ante incidentes, fortaleciendo la reacción ante escenarios reales y mejorando la coordinación interdepartamental.
3. **Programas de concientización continua:** Establecer campañas permanentes que refuercen la cultura de seguridad, fomentando hábitos como el uso de contraseñas seguras, identificación de correos sospechosos, manejo seguro de dispositivos y protocolos de comunicación seguros.
4. **Evaluación y certificación del personal:** Incorporar mecanismos de **evaluación periódica** de conocimientos y competencias en Ciberseguridad, así como certificaciones reconocidas internacionalmente, garantizando que el personal mantenga un nivel adecuado de preparación frente a riesgos emergentes.
5. **Actualización ante nuevas amenazas:** Adaptar los contenidos y metodologías de capacitación de forma continua, considerando **avances tecnológicos, vulnerabilidades detectadas y nuevas tácticas de ataque,** para asegurar que el personal esté siempre preparado para enfrentar desafíos contemporáneos.

La implementación de esta recomendación permitirá que el Sistema C/S cuente con una **fuerza humana altamente capacitada y consciente de los riesgos,** reduciendo significativamente la probabilidad de errores operativos o brechas de seguridad.

Sugerencia 5: Desarrollar infraestructura tecnológica de última generación y sistemas de resiliencia operativa. Para garantizar la continuidad y confiabilidad del Sistema C/S ante fallas técnicas, desastres naturales o ataques cibernéticos, es imprescindible invertir en infraestructura tecnológica avanzada y mecanismos de resiliencia operativa que minimicen la interrupción del servicio y protejan los activos críticos, mediante:

1. **La Modernización de Estaciones Terrenas:** Actualizar equipos de recepción, transmisión y procesamiento de señales, incorporando tecnologías de alto desempeño, sistemas de monitoreo automatizados que detecten anomalías en tiempo real y la actualización constante de software y hardware para reforzar la Ciberseguridad.
2. **Redundancia integral de sistemas**: Implementar **duplicación de enlaces de comunicación y servidores críticos,** de manera que ante cualquier fallo o ataque se

active automáticamente un sistema de respaldo sin pérdida de funcionalidad.

3. **Sistemas de recuperación ante desastres**: Establecer centros de respaldo geográficamente distribuidos, con capacidad de asumir operaciones completas en caso de interrupción de los centros principales, asegurando que la disponibilidad del servicio no se vea comprometida.
4. **Tecnologías de Ciberdefensa incorporadas: Integrar soluciones avanzadas de detección de intrusiones, análisis de tráfico anómalo y protección de "endpoints"**, que operen en paralelo con los sistemas de control del servicio, garantizando la defensa proactiva frente a amenazas cibernéticas sofisticadas.
5. **Monitoreo Predictivo y Mantenimiento Preventivo:** Desarrollar herramientas de **análisis predictivo basadas en IA** que permita anticipar fallas, optimizar recursos y reducir el tiempo de inactividad.

La implementación de estas medidas asegurará que el Sistema C/S mantenga **alta disponibilidad y confiabilidad operativa,** fortaleciendo su capacidad para cumplir su misión crítica de alerta y rescate en emergencias, incluso frente a escenarios de alto riesgo tecnológico o ciberataques complejos.

Sugerencia 6: Implementar un sistema de monitoreo y evaluación continua del desempeño y la seguridad. La resiliencia y eficiencia del Sistema C/S dependen de un **seguimiento constante de su operación y de la seguridad de sus componentes críticos.** Por ello, se recomienda establecer un "Sistema integral de monitoreo y evaluación continua", que permita detectar fallas, vulnerabilidades y oportunidades de mejora de manera proactiva, mediante el:

1. **Monitoreo en tiempo real:** Integrar **plataformas centralizadas de supervisión** que recojan datos de satélites, estaciones terrenas y enlaces de comunicación, permitiendo la detección inmediata de anomalías operativas, ciberataques o fallas técnicas.
2. **Indicadores de desempeño y seguridad:** Definir métricas específicas para evaluar la **disponibilidad del servicio, tiempos de respuesta, eficacia de los protocolos de contingencia y nivel de protección cibernética,** asegurando un análisis cuantitativo del funcionamiento del sistema.
3. **Alertas y notificaciones automatizadas:** Configurar sistemas que generen **alertas tempranas** ante desviaciones críticas, vulnerabilidades detectadas o amenazas emergentes, permitiendo la activación inmediata de planes de mitigación y contingencia.
4. **Auditorías periódicas y revisiones de seguridad:** Realizar evaluaciones formales y auditorías externas para validar la eficacia de los controles implementados, la robustez de la infraestructura tecnológica y la preparación del personal frente a incidentes, incluyendo simulacros de ciberataques. Estos **simulacros de ciberataques** deben ser ejercicios controlados que **imiten ataques reales a sistemas informáticos o redes críticas,** con el objetivo de probar la capacidad de respuesta, detectar vulnerabilidades, entrenar al personal y validar los protocolos de seguridad sin afectar la operación real del sistema. Son ejercicios controlados que imitan ataques reales a sistemas informáticos o redes críticas,

con el objetivo de probar la capacidad de respuesta, detectar vulnerabilidades, entrenar al personal y validar los protocolos de seguridad sin afectar la operación real del sistema.

5. **Retroalimentación y mejora continua:** Implementar un ciclo sistemático de análisis y ajuste, donde los resultados de monitoreo, simulacros y auditorías alimenten mejoras operativas, tecnológicas y de Ciberseguridad, garantizando que el sistema evolucione frente a nuevas amenazas y requerimientos.

La adopción de estas medidas permitirá que el Sistema C/S mantenga una **operación confiable, segura y resilientes,** garantizando que la infraestructura crítica esté siempre disponible para cumplir su misión de alerta y rescate internacional, incluso en escenarios complejos o bajo presión de amenazas cibernéticas.

10. Conclusiones

El Sistema Internacional C/S se erige como una de las infraestructuras críticas más relevantes a nivel global, articulando cooperación tecnológica, humanitaria y estratégica entre múltiples países y organismos internacionales. Su evolución desde 1982 hasta la consolidación del MEOSAR transformó un dispositivo de salvamento en una red de alcance planetario, capaz de sostener operaciones SAR de manera inmediata, precisa y coordinada.

En el escenario actual, marcado por la digitalización, la interdependencia tecnológica y la creciente sofisticación de las ciberamenazas, la mera modernización tecnológica resulta insuficiente. **La protección del C/S requiere integrar la IA y la Ciberseguridad Espacial como ejes transversales, no solo para garantizar la continuidad operativa, sino también para preservar la confianza internacional en el sistema.**

La IA ofrece ventajas disruptivas en el filtrado de falsas alarmas, mantenimiento predictivo, optimización logística y detección de intrusiones, constituyéndose en una herramienta indispensable para anticipar vulnerabilidades y responder en tiempo real frente a incidentes complejos. De igual modo, la cooperación multinacional, la estandarización de protocolos y la capacitación permanente del personal se consolidan como pilares de la resiliencia operativa.

Las sugerencias planteadas —clasificación del Sistema C/S como infraestructura crítica prioritaria, mapeo exhaustivo de vulnerabilidades, cooperación internacional reforzada, formación especializada, inversión en infraestructura de última generación y monitoreo continuo— delinean un marco estratégico integral para la protección y sostenimiento del sistema.

El análisis prospectivo indica que la militarización del espacio, los conflictos híbridos y la competencia por el control de frecuencias críticas configuran riesgos cada vez más tangibles. En este contexto, la resiliencia del Sistema C/S no debe depender únicamente de tecnologías avanzadas, sino de una gobernanza multinacional robusta, flexible y adaptativa, capaz de articular respuestas conjuntas frente a amenazas globales.

En definitiva, el futuro del Sistema C/S depende de su capacidad para adaptarse al nuevo paradigma de seguridad tecnológica. La convergencia entre IA y Ciberseguridad Espacial constituye una necesidad estratégica, fortaleciendo la continuidad de operaciones de rescate, preservando la estabilidad de la infraestructura crítica y garantizando que el sistema cumpla su misión humanitaria y estratégica en un entorno global crecientemente desafiante.

BIBLIOGRAFÍA

COSPAS-SARSAT Secretariat. (s.f.). *System Overview and Operations Manual.* Recuperado de https://www.sarsat.noaa.gov/cospas-sarsat-system-overview/

-

International Telecommunication Union (ITU). (2024). *Radio Regulations.* Recuperado de https://www.itu.int/pub/R-REG-RR

-

European Space Agency (ESA). (2024). *How ESA ensures cybersecurity in space.* Recuperado de https://www.esa.int/About_Us/Cyber_resilience_at_ESA/How_ESA_ensures_cybersecurity_in_space

-

International Civil Aviation Organization (ICAO). (2018). *Safety Management Manual* (Doc 9859). Recuperado de https://aviassist.org/icao-safety-management-manual/-

Freedman, L. (2013). *Strategy: A History.* Oxford University Press.

-

International Maritime Organization (IMO). (2019). *Global Maritime Distress and Safety System (GMDSS) Manual.* Recuperado de https://www.imo.org/en/OurWork/Safety/Pages/IMO-circulars-related-to-the- GMDSS.aspx

-

United Nations Office for Outer Space Affairs (UNOOSA). (2021). *Guidelines for the Long-term Sustainability of Outer Space Activities.* Recuperado de https://www.unoosa.org/documents/pdf/PromotingSpaceSustainability/Publication_Final_English_June2021.pdf