Universidad Internacional de La Rioja
Escuela Superior de Ingeniería y Tecnología

Máster Universitario en Inteligencia Artificial

Desarrollo de una herramienta para la evaluación del cumplimiento del marco FAICP y de los riesgos asociados a estándar de inteligencia artificial del NIST en el sector de la navegación de la Agencia Espacial Europea

Trabajo fin de estudio presentado por:	Teodoro Hidalgo Guerrero y Fernando Jesús Fuentes Carrasco
Tipo de trabajo:	Desarrollo de Software
Director/a:	José Ramón Coz Fernández
Fecha:	16/07/2025

Resumen

Este Trabajo Fin de Máster surge de la necesidad de actualizar y mejorar las herramientas para auditar sistemas inteligentes conforme a nuevos marcos como el NIST AI RMF 1.0 y el FAICP. El objetivo es mejorar una herramienta de auditoría asistida por computadora (CAAT) existente, integrando estos marcos para evaluar aspectos clave de la inteligencia artificial, como la gobernanza, la transparencia y el riesgo. Se plantea como pregunta principal si es posible adaptar estos marcos reutilizando los subcontroles del NIST CSF ya presentes en la herramienta, con la hipótesis de que dicha integración es viable mediante mapeos adecuados.

La metodología seguida es el modelo en cascada, estructurando el trabajo en fases: análisis de requisitos, diseño, implementación, verificación interna y validación externa con personal de la ESA. A partir de la herramienta existente, desarrollada en Excel con Visual Basic for Applications, se ha llevado a cabo una evolución significativa, manteniendo la interfaz familiar para los auditores y ampliándola con hojas específicas para los marcos AI RMF y FAICP. Se han incorporado funcionalidades de automatización de cálculos y visualización de resultados mediante mapas de calor.

La herramienta resultante permite evaluar con precisión el cumplimiento normativo y la madurez de los sistemas de IA auditados. Las pruebas internas confirmaron la coherencia lógica y la fiabilidad técnica, mientras que la validación externa destacó su utilidad práctica y facilidad de uso. La integración de los marcos fue validada con éxito.

En conclusión, el trabajo demuestra que es posible traducir principios complejos de gobernanza de IA a un proceso de auditoría tangible y automatizado, aportando una contribución valiosa a sectores críticos. Se recomienda como trabajo futuro la adaptación de la herramienta a la Ley de IA de la UE y su migración a la nueva versión NIST CSF 2.0 para garantizar su sostenibilidad y relevancia.

Palabras clave: Inteligencia Artificial, Ciberseguridad, Auditoría, NIST AI RMF, FAICP

Abstract

This Master's Thesis arises from the need to update and improve tools for auditing intelligent systems in accordance with new frameworks such as NIST AI RMF 1.0 and FAICP. The objective is to enhance an existing Computer-Assisted Audit Tool (CAAT) by integrating these frameworks to assess key aspects of artificial intelligence, such as governance, transparency, and risk. The main research question is whether these frameworks can be adapted by reusing the NIST CSF sub-controls already present in the tool, with the hypothesis that such integration is feasible through appropriate mappings.

The methodology followed is the waterfall model, structuring the work into phases: requirements analysis, design, implementation, internal verification, and external validation with ESA personnel. Building upon an existing tool developed in Excel with Visual Basic for Applications, a significant evolution has been carried out, preserving the familiar interface for auditors and expanding it with specific sheets for the AI RMF and FAICP frameworks. Features for automating calculations and visualizing results through heat maps have been incorporated.

The resulting tool allows for accurate evaluation of regulatory compliance and the maturity of audited AI systems. Internal testing confirmed logical consistency and technical reliability, while external validation highlighted its practical usefulness and ease of use. The integration of the frameworks was successfully validated.

In conclusion, this work demonstrates that it is possible to translate complex AI governance principles into a tangible and automated audit process, providing a valuable contribution to critical sectors. Future work should focus on adapting the tool to the EU AI Act and migrating it to the new NIST CSF 2.0 version to ensure its sustainability and continued relevance.

Keywords: Artificial Intelligence, Cybersecurity, Auditing, NIST AI RMF, FAICP

Índice de contenidos

Índice de figuras

Índice de tablas

1. Introducción

1.1. Motivación

El sector espacial representa una de las industrias de mayor transcendencia a nivel global, impulsando significativamente el desarrollo tecnológico e influyendo en diversas otras industrias (TEDAE, 2020). Actualmente, este sector experimenta una fase de expansión y crecimiento impulsada por la participación de empresas privadas y los avances tecnológicos que permiten nuevas formas de explotación espacial. Dentro de este dinámico escenario, la Agencia Espacial Europea (ESA) se erige como un actor fundamental, responsable de implementar las políticas espaciales definidas por el Consejo Europeo. Su carácter colaborativo le permite competir con otras grandes agencias del sector.

Un componente crucial de la ESA es el sector de Posicionamiento, Navegación y Transporte (PNT), cuyo principal exponente son los Sistemas Globales de Navegación por Satélite (GNSS), siendo GALILEO el sistema propio de la ESA. Este proyecto espacial, cuyo origen y uso es civil, ofrece servicios de posicionamiento y tiempo, proporcionando a la Unión Europea independencia estratégica de otros sistemas como el GPS estadounidense y el GLONASS ruso.

Paralelamente al notable avance tecnológico en el sector espacial, se ha generado un incremento en las amenazas de ciberseguridad. No tanto por la propia evolución de la sofisticación del malware, sino proveniente de la expansión de la superficie de ataque propiciada por las nuevas tecnologías. Esto obliga a una reevaluación constante de la ciberseguridad, pasando de una concepción estática a un enfoque dinámico y evolutivo, donde la seguridad se entiende como un conjunto de procesos organizacionales en continua adaptación. Por ello, la gobernanza de estos procesos se vuelve esencial para la protección de los sistemas inteligentes e información.

Para verificar la correcta implementación, se recurre a las auditorías, analizando tanto los componentes tecnológicos como los procesos, de forma periódica para lograr que estos

procesos se adapten a las nuevas amenazas y riesgos evitando que la organización no se encuentre preparada para defender sus activos. En sus inicios, estas auditorías no debían tener en consideración múltiples estándares para la gestión de riesgos, pero debido a la ingente cantidad de información a procesar en la actualidad y la aparición de distintos marcos que pretenden atacar la gestión de riesgos con distintos enfoques, se apoyan cada vez más en herramientas de auditoría asistida por computadora (CAAT), que permiten realizar una evaluación más eficiente y controlada.

Precisamente la ESA posee múltiples herramientas internas para realizar auditorías en el sector de navegación. Sin embargo, con la creciente adopción de nuevas tecnologías, particularmente la Inteligencia Artificial (IA) en contextos críticos como la navegación autónoma y la gestión de información compleja, existe una necesidad de actualizar estas herramientas. Como la IA ha comenzado a desempeñar un papel cada vez más relevante en la toma de decisiones automatizada, se generan nuevas exigencias técnicas y normativas en relación con la gobernanza, la transparencia y la gestión del riesgo permitiendo un análisis en mayor profundidad o considerar posibles vectores no cubiertos con las anteriores.

Entre los marcos técnicos y normativos que emergen para regular el uso responsable de la IA, contamos con el NIST AI Risk Management Framework (RMF) 1.0 y el FAICP Framework, los cuáles no son soportados por las herramientas que posee la ESA. Por ello, este presente trabajo se centra en la mejora de las CAATs utilizadas en el sector de navegación, con el objetivo de integrar marcos de referencia especializados en la gobernanza y gestión de riesgos de sistemas con IA. La motivación principal radica en la creciente necesidad de alinear los sistemas inteligentes con estándares reconocidos que garanticen su fiabilidad y cumplimiento regulatorio, especialmente en un contexto normativo en evolución.

1.2. Planteamiento

La solución que se plantea en este Trabajo de Fin de Máster (TFM) consiste en el fortalecimiento y actualización de una herramienta de auditoría asistida por computadora (CAAT) utilizada por la ESA en el ámbito del sector de navegación. Esta mejora se orienta hacia

la integración de marcos de referencia especializados en la gestión de riesgos y la gobernanza de sistemas que incorporan Inteligencia Artificial (IA), los cuales actualmente no están contemplados en las herramientas existentes.

En particular, se propone incorporar el NIST AI Risk Management Framework (RMF) 1.0, aprovechando su mapeo con el Cybersecurity Framework (CSF) 1.1, el cual ya es compatible con la herramienta. Para ello, se identificarán las subcategorías del AI RMF no cubiertas por el CSF y se propondrán controles específicos que permitan su evaluación dentro de la auditoría. Esta estrategia facilita la integración incremental y coherente de nuevas capas de análisis sin comprometer la estructura base de la herramienta. Por otro lado, para el FAICP Framework, dado que no existe un mapeo previo con ningún marco implementado actualmente en la herramienta, se construirá una correspondencia directa basada en los principios del CSF 1.1. Este esfuerzo permitirá alinear los criterios del FAICP con un esquema ya familiar para los auditores, garantizando una integración más fluida y operativa.

La propuesta se fundamenta en la necesidad de evaluar de manera más rigurosa aspectos como la ética, la rendición de cuentas, la interpretabilidad, la privacidad y la corrección en los sistemas de IA, especialmente en contextos críticos como la navegación autónoma. Además, se espera que esta mejora contribuya a una mayor capacidad de adaptación normativa de la ESA, en un entorno donde las regulaciones vinculadas a la inteligencia artificial están en plena evolución. Así, el proyecto no solo mejora la eficiencia técnica de las auditorías, sino que también aporta valor estratégico a largo plazo.

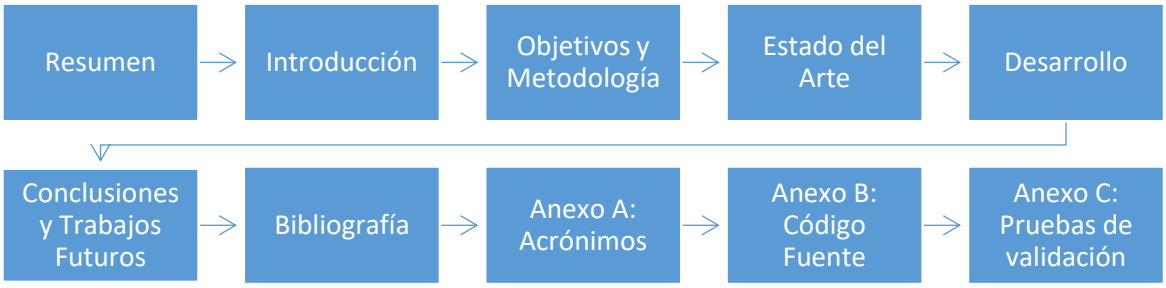
1.3. Estructura de la Memoria

Para documentar el trabajo realizado, se seguirá la siguiente estructura para hablar de los distintos ámbitos de este proyecto:

- **Resumen:** A través de este, se proporciona a los lectores una visión clara sobre el ámbito del proyecto, proporcionando una recopilación de la investigación realizada y las conclusiones resultantes del trabajo realizado.
- **Introducción:** A través de este, se proporciona a los lectores una síntesis del proyecto, incluyendo el problema a resolver, descripción de los objetivos, así como la estructura del presente documento.

- **Estado del Arte:** Recoge información relevante de investigaciones, herramientas y soluciones previas relacionadas con el tema del proyecto. Permite comprender cómo se ha tratado el problema anteriormente y qué aporta de nuevo este trabajo.
- **Desarrollo:** Describe detalladamente el procesado llevado a cabo: contexto de la herramienta actual de la ESA, diseño y desarrollo, pruebas realizadas y resultados parciales que expliquen cómo funciona la herramienta.
- **Conclusiones y Trabajos Futuros:** Resume los resultados obtenidos, analiza si se cumplieron los objetivos y reflexiona sobre las dificultades encontradas. Además, plantea posibles mejores o líneas de trabajo que podrían desarrollarse más adelante.
- **Bibliografía:** Incluye todas las referencias utilizadas para sustentar el trabajo tanto teóricas como técnicas.
- **Anexo A: Acrónimos:** En este anexo, son listados todos los acrónimos encontrados a lo largo de esta memoria, facilitando la simplicidad de la memoria al no ser verbosos durante su redacción.
- **Anexo B: Código fuente:** En este anexo se dispondrá de todas las funciones usadas para la implementación del producto.
- **Anexo C: Pruebas de validación:** En este anexo se encuentran todas las pruebas que han sido preparadas para la validación del producto desarrollado junto con el resultado de estas.

Figura 1. Secciones del Trabajo



Fuente: Elaboración propia

1.4. Desglose del Trabajo realizado

Tabla 1. Desglose del trabajo realizado en la memoria

Sección de la memoria	Autor/es
1. Introducción	Fernando
1.4 Estructura de la memoria	Ambos
2. Objetivo y metodología	Teodoro
3.1 Sector Espacio	Teodoro
3.2.1 Concepto Ciberseguridad	Teodoro
3.2.2 Estado Actual Ciberseguridad	Teodoro
3.2.3 Ciberseguridad en el espacio	Teodoro
3.2.4 Ciberseguridad ESA	Fernando
3.2.5 Auditorías y Ciberseguridad	Fernando
3.4 Auditorías en la ESA	Fernando
4.1 Contexto del Proyecto	Fernando
4.2 Descripción del Proyecto	Fernando
4.3 Funcionalidad Inicial	Fernando
4.4 Análisis de Requisitos	Teodoro
4.5 Diseño y Desarrollo	Teodoro
4.6 Validación Interna	Fernando
4.7. Validación Externa	Fernando

Sección de la memoria	Autor/es
5.1. Conclusiones	Teodoro
5.2. Líneas de Trabajo Futuro	Teodoro
Anexo A. Acrónimos	Fernando
Anexo B. Código Fuente	Teodoro
Anexo C. Pruebas de Validación	Fernando

Fuente: Elaboración propia

Tabla 2. Desglose del trabajo realizado en la herramienta

Acción en la Herramienta	Autor/es
Diseño y Implementación	Teodoro
Realización de pruebas y análisis de resultados	Fernando
Listar subcontroles: AIRM	Fernando
Listar subcontroles: FAICP	Teodoro

Fuente: Elaboración propia

Tabla 3. Desglose del trabajo realizado sobre los estándares

Acciones con Estándares	Autor/es
Verificación y desarrollo de la asignación a estándar AI RMF 1.0 desde CSF 1.1	Fernando
Verificación y desarrollo de la asignación a estándar FAICP desde CSF 1.1	Teodoro

Fuente: Elaboración propia

2. Objetivos y metodología

2.1. Objetivo principal

El objetivo general de este Trabajo de Fin de Máster es realizar una propuesta de mejora de las CAATS actuales que utiliza la ESA, con el fin de permitir realizar una evaluación conforme a los estándares NIST AI RMF 1.0 y FAICP Framework, integrando de esta manera las consideraciones específicas para la gobernanza y gestión de riesgos de la Inteligencia Artificial en los procesos de auditoría del sector de navegación de la ESA.

2.2. Objetivos específicos

Para alcanzar este objetivo general, se han definido los siguientes objetivos específicos:

- **Estudiar el contexto del sector espacial y la ciberseguridad:** Esto implica comprender las particularidades del sector espacial, con especial atención al sector de Posicionamiento, Navegación y Transporte (PNT) y el sistema GALILEO. Además, se analizará el panorama actual de las amenazas de ciberseguridad y la necesidad de una gobernanza dinámica y evolutiva en este ámbito. Este estudio proporcionará la base contextual necesaria para comprender los desafíos y requisitos específicos de la ESA en relación con la seguridad y la IA.
- **Profundizar sobre algunos de los estándares utilizados por las CAATS actuales y los que se adaptarán:** Este objetivo se centra en comprender en detalle el funcionamiento de las herramientas de auditoría asistida por computadora (CAAT) que actualmente emplea la ESA. Además, se realizará un análisis exhaustivo de los marcos de referencia que se integrarán: el NIST AI Risk Management Framework (RMF) 1.0 y el FAICP Framework. Se explorará la relación existente entre el NIST AI RMF 1.0 y el Cybersecurity Framework (CSF) 1.1 realizado por el SCF, así como la elaboración de un mapeo para integrar el FAICP Framework con los estándares ya utilizados. Este análisis permitirá identificar las sinergias y los puntos de integración más efectivos para la mejora de la CAAT.
- **Desarrollar un sistema de información que permita realizar una evaluación conforme a los estándares NIST AI RMF 1.0 y FAICP Framework:** Este objetivo se materializará en la propuesta de mejora concreta de la CAAT. Basándose en el conocimiento adquirido en los

objetivos anteriores, se definirá la arquitectura y los mecanismos necesarios para incorporar la evaluación de los controles y principios definidos en el NIST AI RMF 1.0 y el FAICP Framework dentro de la herramienta de auditoría existente. Se buscará que la integración que mantenga la experiencia de usuario para los auditores de la ESA, facilitando la adopción de la mejora manteniendo el uso de las hojas de cálculo.

- **Probar la herramienta en diversas auditorías simuladas y extraer conclusiones:** Una vez desarrollada la propuesta de mejora, se llevará a cabo una fase de pruebas mediante la simulación de auditorías en escenarios representativos del sector de navegación. El objetivo de estas pruebas será validar la funcionalidad y la eficacia de la CAAT mejorada para evaluar los aspectos relacionados con la gobernanza y los riesgos de la IA, conforme a los estándares integrados. Los resultados de estas pruebas permitirán extraer conclusiones sobre la viabilidad y el valor añadido de la propuesta, así como identificar posibles áreas de mejora futura.

2.3. Metodología del Trabajo

Para la realización de este proyecto, se ha adoptado la metodología tradicional en su variante en cascada. Esta metodología consiste en el desglose de las actividades de desarrollo en fases secuenciales lineales, lo que significa que cada fase se transmite a otra, donde cada fase depende de los resultados de la anterior y corresponde a una especialización de tareas (Petersen et al., 2009). Este enfoque resulta especialmente conveniente en proyectos como el presente, que involucran una etapa de investigación previa particularmente extensa y bien estructurada, la cual ha permitido establecer con claridad los requisitos, objetivos funcionales y no funcionales, así como los criterios de validación del sistema antes de iniciar su implementación.

En nuestro caso, la incorporación de nuevos frameworks en una herramienta de auditoría parte de una base conceptual sólida, en gran parte proporcionada por la interacción directa con la ESA (European Space Agency) y la revisión exhaustiva de la normativa a implementar. El proceso seguido contempla las siguientes fases:

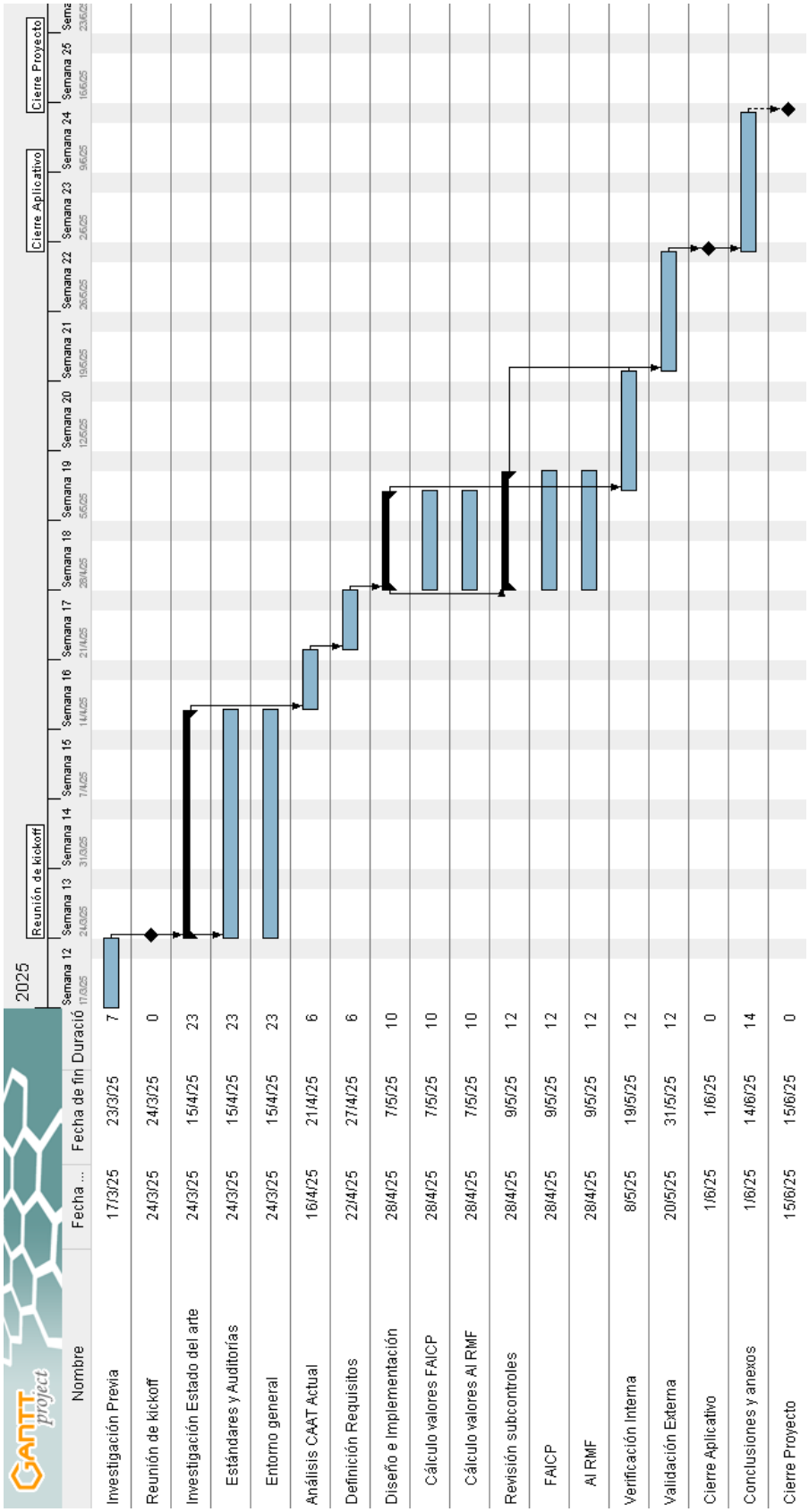
1. **Definición de requisitos:** Se delimita el alcance del sistema y se establecen con precisión los requisitos funcionales y no funcionales. Esta fase resulta crítica, pues establece las

bases para el desarrollo posterior. Los requisitos han sido definidos en colaboración con la ESA, asegurando así una alineación directa con las necesidades reales de uso de la herramienta.

2. **Diseño e implementación:** A partir de los requisitos definidos, se diseña la solución técnica y se implementan los algoritmos necesarios para la integración del nuevo estándar. Esta etapa incluye la construcción progresiva del CAAT, asegurando que cada funcionalidad incorporada cumpla con los criterios establecidos en fases anteriores.
3. **Verificación interna:** Se realizan pruebas funcionales y de integración sobre el sistema desarrollado. Aunque la metodología en cascada no contempla iteraciones constantes, esta fase permite la identificación puntual de errores o mejoras, que pueden derivar en revisiones controladas del diseño sin alterar significativamente la estructura lineal del proyecto. Así, se mantiene la lógica de avance fase a fase, sin introducir cambios disruptivos de último momento.
4. **Validación externa:** La herramienta es evaluada por la propia ESA, simulando un entorno real de uso. Este paso no solo actúa como control de calidad final, sino que también proporciona retroalimentación valiosa desde la perspectiva de usuarios expertos. Aunque es posible que en esta fase surjan nuevas sugerencias o mejoras, cualquier cambio estructural relevante habrá sido ya contemplado e incorporado en fases anteriores gracias al sólido trabajo previo de análisis y diseño.

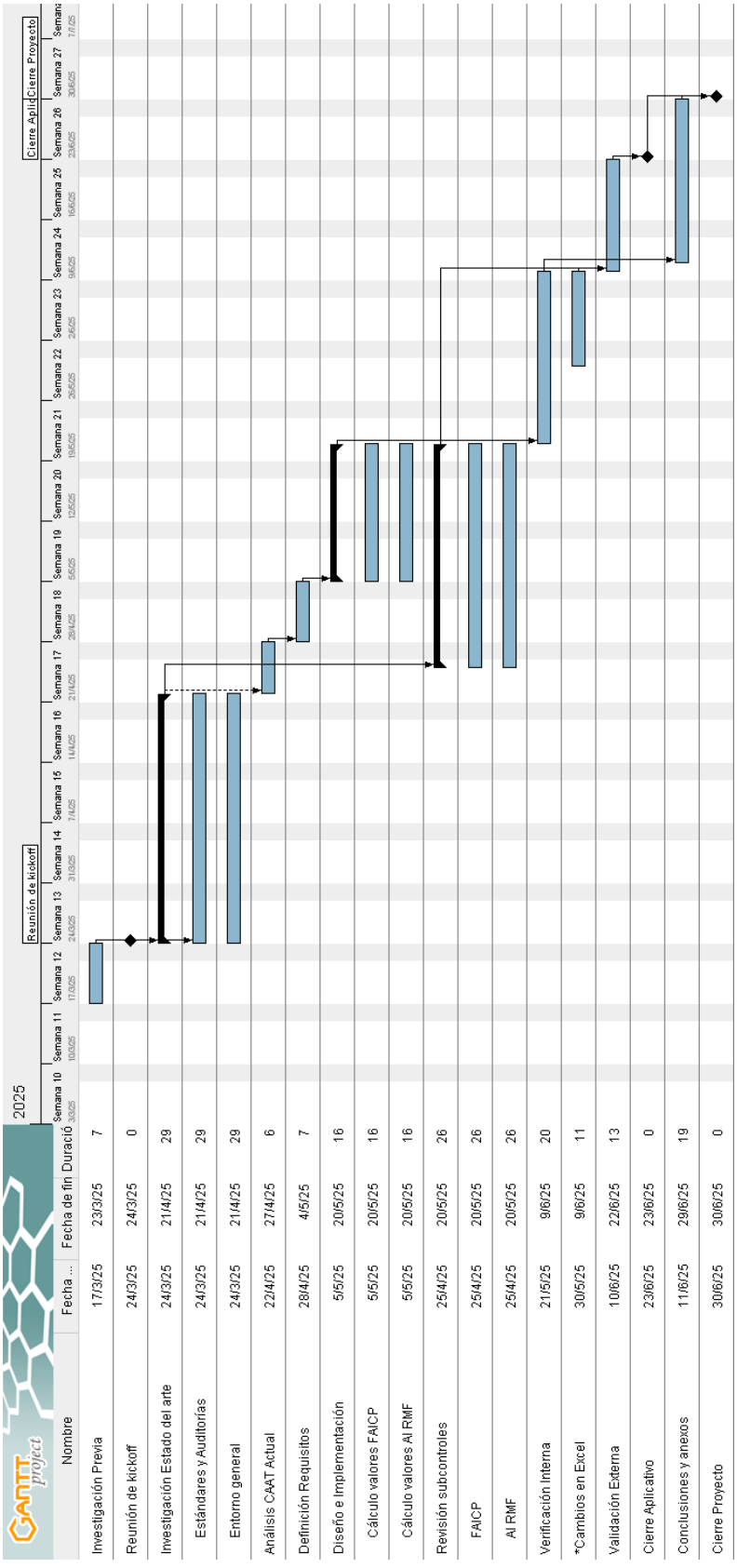
En las Figuras 2 y 3, se muestran tanto el cronograma inicial diseñado para este proyecto, como su ejecución final a través del uso de un diagrama de Gantt.

Figura 2. Cronograma de trabajo inicial



Fuente: Elaboración Propia

Figura 3: Cronograma final.



Fuente: Elaboración Propia

3. Contexto y Estado del Arte

3.1. Sector espacio

3.1.1. Importancia del sector

El sector espacial ha experimentado una evolución extraordinaria en sus aproximadamente 65 años de historia, abarcando aspectos geopolíticos, su ámbito de actuación, su impacto social y su organización económica (Ventura Traveset Bosch, 2021). Actualmente, más de cien países tienen actividad espacial, y el sector está presente en prácticamente todos los ámbitos de la sociedad. La Organización para la Cooperación y el Desarrollo Económico (OCDE) define la Economía del Espacio como "el conjunto de actividades y usos de los recursos que crean valor y beneficios a los seres humanos en el curso de la exploración, investigación, entendimiento, gestión y utilización del espacio" (Coz Fernández & Valiño Castro, 2021). Esta definición es amplia y abarca tanto la explotación económica directa como indirecta del espacio, desde otra perspectiva se indica que alrededor del 60% de la economía mundial depende de los activos espaciales, ya sea de forma directa o indirecta.

La importancia del sector espacial radica en su capacidad tecnológica y la dependencia de la economía en sistemas satelitales, internet y energía (Coz Fernández & Valiño Castro, 2023). Una interrupción de estos servicios tendría consecuencias catastróficas, además de que el sector es un motor clave para la investigación y el desarrollo de nuevas tecnologías, con frecuencia extrapolándose tecnología utilizada en proyectos espaciales para usos cotidianos (TEDAE, 2020). En España, el sector espacial ocupa las primeras posiciones entre las empresas de alta tecnología y ha progresado significativamente en los últimos años. Su carácter es estratégico y posee un enorme potencial de crecimiento futuro. Las empresas del sector desarrollan competencias y capacidades en campos tan variados como la defensa, la seguridad y la agricultura.

Europa ha pasado de ser un mero espectador a una potencia espacial de primer orden, siendo una referencia mundial en ciencia espacial, observación de la Tierra y navegación por satélite (Ventura Traveset Bosch, 2021). El sector espacial europeo se diferencia del estadounidense por tener un presupuesto menor y una mayor dependencia de las ventas comerciales (Coz

Fernández & Valiño Castro, 2023). Además, la parte de gastos militares es menor, lo que implica que las sinergias entre los sectores civil y militar están menos desarrolladas.

En el contexto actual, ser observa una creciente importancia del sector espacial para la Unión Europea (TEDAE, 2020). La UE está impulsando el NewSpace, buscando convertir a Europa en un actor clave en este ámbito, actualmente dominado por Estados Unidos (Ventura Traveset Bosch, 2021). El NewSpace se caracteriza por iniciativas con un alto contenido tecnológico de carácter privado que complementa los grandes programas gubernamentales, permitiendo un acceso al espacio más económico y eficiente (Coz Fernández & Valiño Castro, 2021).

El sector espacial también enfrenta desafíos importantes como la ciberseguridad y la basura espacial (Coz Fernández & Valiño Castro, 2023). La ciberseguridad es crucial en todos los componentes de una misión espacial, incluyendo el segmento terreno, el segmento de comunicaciones y el segmento espacial.

España por su lado juega un papel esencial en el sector europeo, siendo industria líder en actividades espaciales como la observación de la Tierra, el medio ambiente y la exploración espacial (Ventura Traveset Bosch, 2021). Empresas españolas como Airbus Space Systems España, ALTER TECHNOLOGY, DAS Photonics, Elecnor Deimos, GMV, GTD, Hisdesat, Hispasat, IberEspacio, SENER Aeroespacial y Tecnobit - Grupo Oesía tienen capacidades tecnológicas especializadas y participan en importantes programas y misiones (TEDAE, 2020).

Y desde el ámbito de la colaboración público-privada, el sector espacial representa un ejemplo de éxito con la colaboración internacional y la participación de diferentes agentes sociales como universidades, empresas y el sector público (civil y militar) (Coz Fernández & Valiño Castro, 2021). Esta colaboración permite avances tecnológicos que finalmente se diseminan por toda la economía.

3.1.2. ESA

Una parte fundamental del éxito espacial europeo se atribuye a la Agencia Espacial Europea (ESA), un organismo fundado en 1975 y compuesto por 22 estados miembros, cuyo foco está en que el retorno de la inversión europea beneficie a sus ciudadanos agrupando las fortalezas de los distintos países europeos en este campo (ESA, 2023). Esta colaboración a través de la

ESA se ve favorecida por el elevado coste de los proyectos aeroespaciales, generando una considerable experiencia en la realización de proyectos conjuntos. En 2025, el presupuesto actual es de 7.680 millones de euros, destinando un 33,6% a Observación de la Tierra, 12,5% a Navegación y un 10,6% a Conectividad y Comunicaciones seguras (ESA, 2025).

La ESA tiene decenas de misiones activas, como Sentinel 1, Sentinel 2 y Sentinel 5P dentro del programa Copernicus (ESA, 2025), pero destacamos las siguientes debido a su relevancia (ESA, 2022):

- **Copernicus:** Es el programa de la UE para la observación de la Tierra, proveyendo datos e información espacial para diversas aplicaciones.
- **Galileo:** Es el sistema mundial de navegación y posicionamiento por satélite (GNSS) de la UE.
- **EGNOS:** Es un sistema europeo que aumenta la precisión de las señales GNSS.
- **SSA:** Se encarga del monitoreo y protección de los activos espaciales.
- **GOVSATCOM:** Proporciona comunicaciones seguras por satélite para la seguridad de la UE y apoyo en crisis.

3.2. Ciberseguridad

3.2.1. Concepto

La ciberseguridad puede entenderse como una forma de guerra asimétrica en la que los defensores deben proteger una gran variedad de activos frente a atacantes cuya identidad, intenciones y capacidades técnicas son, en la mayoría de los casos, desconocidas. Este desequilibrio estructural implica que la existencia de un sistema completamente seguro es, en la práctica, una utopía. Incluso si existiera la posibilidad de blindar todos los activos, el coste económico asociado —tanto en infraestructura tecnológica como en investigación especializada— resultaría inviable para la mayoría de las organizaciones (Packetlabs, 2023).

Por esta razón, el objetivo de los equipos de ciberseguridad no es alcanzar una seguridad total, sino gestionar los riesgos de forma eficaz. La gestión del riesgo consiste en identificar las amenazas potenciales que pueden impactar en los activos digitales, evaluar la probabilidad de que estas se materialicen, y adoptar medidas que mitiguen su impacto o reduzcan su

probabilidad de ocurrencia (Imperva, 2023). Este enfoque de la ciberseguridad como un proceso y no como un producto implica una revisión y adaptación continua ante la constante evolución del panorama de amenazas (RiskRecon, 2023).

En este sentido, es esencial no confundir el análisis de riesgos con el modelado de amenazas. Mientras que el modelado de amenazas busca reducir o eliminar los riesgos durante la fase de diseño y desarrollo de un sistema, el análisis de riesgos abarca todo el ciclo de vida operativo de dicho sistema, prestando atención a los vectores de ataque que pueden surgir durante su uso en entornos reales (González, 2021). Por tanto, la seguridad no debe estar circunscrita a la fase de desarrollo, sino que debe integrarse de forma transversal en todos los procesos de la organización.

La mayoría de los marcos de referencia actuales para la gestión de la ciberseguridad, como el NIST Cybersecurity Framework o el Secure Controls Framework (SCF), insisten en la necesidad de establecer procedimientos cíclicos para identificar, tratar y revisar los riesgos a lo largo del tiempo. Esta naturaleza iterativa permite adaptar los controles de seguridad a amenazas emergentes y reducir el impacto potencial de ataques exitosos (Secure Controls Framework, 2025).

Un factor clave que impulsa esta evolución es la creciente dependencia de las organizaciones en sistemas de información interconectados. Aplicaciones móviles, entornos de nube, dispositivos IoT y software de colaboración remota amplían la superficie de ataque, creando nuevas oportunidades para que actores maliciosos comprometan la seguridad organizacional (Hussain et al., 2020). Este fenómeno ha conducido a un cambio de paradigma, pasando de una arquitectura de seguridad centrada en el perímetro a modelos más integrales que buscan asegurar cada componente del sistema y sus interconexiones (Jang-Jaccard & Nepal, 2014).

3.2.2. Estado actual

En la actualidad, la ciberseguridad se ha consolidado como una preocupación transversal a todos los sectores productivos y sociales, debido al aumento tanto en la frecuencia como en la sofisticación de las amenazas digitales. Tal como señalan (Cavaciuti-Wishart et al., 2024), el desarrollo acelerado de la inteligencia artificial (IA) ha propiciado la aparición de nuevos tipos de malware diseñados con capacidades adaptativas, lo que incrementa su eficacia en la

evasión de sistemas tradicionales de defensa. Este fenómeno se ve agravado por la expansión de tecnologías emergentes como la computación en la nube, el Internet de las Cosas (IoT) y los dispositivos móviles, que han multiplicado los puntos de entrada vulnerables en las infraestructuras organizativas, ampliando significativamente la superficie de ataque.

A su vez, la democratización del acceso a internet y la creciente dependencia digital en el ámbito económico han transformado los objetivos tradicionales de los ciberataques. Ya no se trata únicamente de obtener información estratégica, sino también de monetizar dicha información mediante ataques secundarios, como el ransomware, el secuestro de cuentas o el fraude financiero (Jang-Jaccard & Nepal, 2014).

A pesar de este panorama, también se observa una evolución paralela en las capacidades defensivas. Según Melaku (2023), se están desarrollando soluciones tecnológicas cada vez más sofisticadas, acompañadas de marcos normativos y arquitecturas de seguridad que permiten adaptarse con mayor agilidad a las amenazas actuales. No obstante, la implementación efectiva de estas herramientas presenta una fuerte disparidad según el tamaño de la organización. Tal como advierten Bueermann y Rohrs (2024), debido a los elevados costes de despliegue, sólo las grandes corporaciones disponen de recursos suficientes para establecer sistemas de defensa eficaces y proactivos, lo cual deja a las pequeñas y medianas empresas (PYMES) en una situación de vulnerabilidad estructural.

Incluso en organizaciones con recursos adecuados, persisten importantes desafíos relacionados con la cultura organizacional y la gobernanza de la ciberseguridad. De acuerdo con Hussain et al. (2020), uno de los principales factores de riesgo no es de naturaleza técnica, sino humana y administrativa. La falta de rigor en la aplicación de los protocolos de seguridad y la ausencia de una gobernanza fuerte reducen la eficacia de cualquier solución tecnológica. El compromiso institucional desde los niveles directivos es esencial para garantizar el cumplimiento sistemático de las medidas de protección, ya que los dispositivos de seguridad pierden su efectividad si los usuarios no comprenden su importancia o si la organización no fomenta una cultura de cumplimiento y responsabilidad.

El estudio de Bueermann y Rohrs (2024) refleja la fragilidad de la situación actual: un 29 % de las organizaciones reconocen haber sufrido al menos un incidente de ciberseguridad durante

el último año, y, de estos, sólo un 40 % fue causado por actores externos. Esto resalta el creciente protagonismo de las amenazas internas, ya sean accidentales o intencionadas. Adicionalmente, el 54 % de las entidades encuestadas manifiestan tener un conocimiento insuficiente sobre las vulnerabilidades presentes en su propia cadena de suministro, mientras que el 64 % de sus directivos admiten desconocer cuáles son estas debilidades, a pesar de cumplir con los estándares mínimos establecidos.

Un ejemplo paradigmático de ataque a la cadena de suministro es el incidente relacionado con MOVEit Transfer en 2023, donde se explotó una vulnerabilidad mediante técnicas de inyección SQL, permitiendo el acceso no autorizado a datos de más de 2.000 organizaciones alrededor del mundo (Verge, 2023). Casos como este ponen de manifiesto que, más allá del despliegue de soluciones tecnológicas, es imprescindible consolidar una gobernanza integral de la ciberseguridad que contemple aspectos organizativos, formativos y estratégicos. La falta de control interno, el desconocimiento de las amenazas y la escasa supervisión de los agentes con acceso privilegiado continúan siendo vectores críticos de riesgo que pueden comprometer incluso a los sistemas más robustos.

3.2.3. Ciberseguridad en el espacio

El sector espacial, por su parte, enfrenta una serie de retos particulares en materia de ciberseguridad, los cuales, si bien presentan características propias, a menudo están asociados a amenazas en la cadena de suministro (Coz Fernández, 2021). En dicha cadena, destacan especialmente los componentes de software reutilizables, denominados COTS (Commercial Off-The-Shelf), que resultan fundamentales para acelerar el desarrollo de misiones espaciales y reducir considerablemente el tiempo requerido para su puesta en marcha (Manulis et al., 2021).

No obstante, la dependencia de estos componentes implica un riesgo significativo: la detección de una vulnerabilidad en uno de ellos puede comprometer múltiples desarrollos simultáneamente y afectar a diversas organizaciones con relativa facilidad. Tenemos dos casos ejemplares: Un caso paradigmático es la vulnerabilidad CVE-2021-44228, identificada en Apache Log4J en 2021, la cual permitía la ejecución remota de código arbitrario por parte de actores maliciosos con una repercusión que afectó al 48 % de las organizaciones a nivel

mundial; Otro caso fue el ataque que comprometió la cadena de suministro de SolarWinds, una empresa dedicada al software de monitoreo de redes, logrando enviar una actualización con un backdoor que infectó a más de 18.000 organizaciones incluyendo agencias gubernamentales de EE.UU (Check Point, 2022).

El desarrollo tecnológico vinculado al espacio está progresando a un ritmo cada vez más acelerado a escala global. Sin embargo, este avance no se limita exclusivamente al ámbito científico, sino que también se expande hacia esferas militares y de defensa, donde las implicaciones de seguridad son aún más críticas. En este contexto, Swope et al. (2024) ofrecen una taxonomía de las amenazas potenciales en el dominio espacial, clasificándolas en cinéticas, no cinéticas, electrónicas y cibernéticas. Dentro de estas últimas, los ciberataques pueden tener efectos severos, como la destrucción o desactivación permanente de sistemas críticos. Además, pueden ser utilizados para interrumpir temporalmente el flujo de información o realizar actividades de espionaje mediante la infiltración y extracción de datos sensibles. La ambigüedad en la intención de este tipo de ofensivas constituye uno de sus elementos más preocupantes, dificultando tanto la atribución como la respuesta efectiva.

En el último año, se ha registrado un incremento notable de ciberataques con fines de espionaje, dado que estos permiten aprovechar la infraestructura comprometida para ejecutar acciones más sofisticadas contra sistemas interconectados. Ejemplos recientes incluyen los ataques dirigidos contra satélites de Ucrania y Rusia durante el conflicto armado, con el objetivo de interrumpir las comunicaciones entre los mandos militares de ambas fuerzas (Gedeon, 2023; Pereira, 2023). Asimismo, se llevaron a cabo acciones de manipulación de señales GNSS mediante técnicas de suplantación, con el propósito de transmitir información errónea relativa al posicionamiento en el campo de batalla.

Un precedente relevante en este ámbito fue el incidente ocurrido con el satélite germano-estadounidense ROSAT, cuya seguridad fue comprometida por actores maliciosos que lograron acceder a los sistemas de la NASA a través de una intrusión remota. Como resultado del ataque, se sustrajo información confidencial que fue presuntamente enviada a Moscú, y posteriormente los atacantes modificaron el ángulo de los paneles solares del satélite, orientándolos directamente hacia el Sol. Esta acción provocó un daño térmico irreversible que inutilizó completamente la plataforma (Holmes, 2008).

3.2.4. Ciberseguridad ESA

En el contexto actual, donde los sistemas espaciales se han convertido en infraestructuras críticas para sectores como la navegación, la defensa, las telecomunicaciones, el transporte o la agricultura, la Agencia Espacial Europea (ESA) reconoce la ciberseguridad como un pilar fundamental para la protección de sus operaciones y el éxito de sus misiones estratégicas. Esta necesidad no solo responde a una exigencia técnica, sino también a compromisos políticos, regulatorios y sociales relacionados con la soberanía tecnológica europea y la confianza digital.

3.2.4.1. Ciberseguridad como parte del diseño de misión

La ciberseguridad en la ESA no se concibe como una capa añadida al final del ciclo de vida de los sistemas espaciales, sino como un componente transversal, que debe estar presente desde la fase de concepción hasta la operación y desmantelamiento de satélites, sistemas GNSS (como Galileo y EGNOS) y plataformas de observación (como Copernicus).

Esto implica que se adopten principios de “Security by Design”, integrando la gestión de riesgos cibernéticos desde la arquitectura misma de cada sistema.

En este sentido, los requisitos de seguridad se definen durante la fase de ingeniería de sistemas, alineados con estándares como el ECSS-Q-ST-80C (norma específica del espacio en Europa) y principios establecidos en marcos internacionales como NIST, ISO 27001 o ENISA FAICP para IA.

3.2.4.2. Infraestructura crítica e interdependencias tecnológicas

Los sistemas gestionados por la ESA, especialmente los relacionados con navegación por satélite (como Galileo), son considerados infraestructuras críticas por la Unión Europea. Cualquier alteración en sus operaciones puede tener consecuencias devastadoras en servicios civiles, emergencias, logística, aviación, transporte marítimo y operaciones militares.

Además, estos sistemas están interconectados con infraestructuras de terceros (redes terrestres, estaciones de control, sistemas en la nube, sensores de terceros), lo que genera interdependencias tecnológicas y una superficie de ataque extendida que debe ser controlada con precisión.

La ESA, por tanto, ha adoptado una visión multicapa de la ciberseguridad, que incluye:

- Protección de la red de estaciones terrestres.
- Encriptación y autenticación de señales entre satélites y centros de control.
- Evaluación de riesgos de software embarcado.
- Segmentación de redes y uso de zonas de seguridad lógica.
- Gestión de identidad digital y control de accesos para usuarios y operadores.

3.2.4.3. Gobierno y cultura de la ciberseguridad

Uno de los pilares de la ESA en este campo es la gobernanza de la ciberseguridad, gestionada desde la dirección de operaciones y tecnología. La agencia promueve una cultura organizacional centrada en la seguridad de la información, en la cual cada nivel jerárquico (desde ingenieros hasta directivos) asume un rol específico en la prevención y respuesta ante incidentes.

Se llevan a cabo acciones de:

- Formación y sensibilización continua en ciberseguridad para el personal técnico y de gestión.
- Simulacros de ciber crisis que incluyen ataques simulados a satélites o a infraestructuras críticas.
- Integración de planes de continuidad del negocio (ISO 22301) y recuperación ante desastres (DRP) adaptados al entorno espacial.
- Desarrollo de centros de operaciones de seguridad (SOC) para el monitoreo continuo de redes y sistemas.

3.2.4.4. Retos emergentes: IA, computación cuántica y amenazas híbridas

La ESA enfrenta hoy retos de nueva generación, como la adopción segura de inteligencia artificial en sistemas autónomos de navegación, lo que ha impulsado la evaluación de marcos como el FAICP Framework de ENISA, enfocado en prácticas de ciberseguridad para IA

Asimismo, el desarrollo de la computación cuántica plantea riesgos importantes en términos de criptografía, lo que lleva a la ESA a explorar soluciones post-cuánticas para garantizar que sus sistemas permanezcan protegidos ante ataques futuros.

Por otro lado, el auge de las amenazas híbridas —que combinan ciberataques, desinformación, sabotaje físico y espionaje— exige una coordinación estratégica con entidades como la Comisión Europea, la Agencia de la UE para el Programa Espacial (EUSPA) y los cuerpos de defensa y seguridad de los Estados miembros.

3.2.4.5. Conclusión

En resumen, la ciberseguridad en la ESA no es un proceso técnico aislado, sino un ecosistema integrado de políticas, estándares, herramientas y cultura organizacional que busca proteger activos estratégicos para Europa. A medida que el entorno digital y geopolítico se vuelve más complejo, la ESA se posiciona como referente en la gestión del riesgo cibernético en el ámbito espacial, integrando estándares internacionales, marcos de seguridad propios y una estrategia que combina tecnología, formación y resiliencia operativa.

3.2.5. Auditorias y Ciberseguridad

Según lo establecido en la norma ISO 19011:2018, una auditoría se define como un proceso estructurado, imparcial y registrado, que tiene como finalidad recolectar evidencias objetivas y analizarlas de manera imparcial para determinar en qué medida se cumplen los criterios establecidos para la auditoría.

En cuanto a su clasificación, las auditorías se dividen en internas y externas:

- **Auditorías internas**, también conocidas como auditorías de primera parte, son aquellas que realiza la propia organización para evaluar sus sistemas o procesos.

- **Auditorías externas** pueden ser de segunda parte, cuando las realiza una parte interesada como un cliente o socio; o de tercera parte, cuando son ejecutadas por entidades independientes que certifican el cumplimiento de normativas, generalmente con validez oficial o gubernamental (Nikolaev, 2021).

Sanchez-García et al. (2024) proponen que las auditorías de riesgo en ciberseguridad pueden también clasificarse según los objetivos perseguidos, los cuales se agrupan en cuatro grandes categorías: evaluación, aseguramiento, cumplimiento y mejora continua. Dentro del ciclo de gestión de riesgos, el proceso de monitoreo y revisión es especialmente relevante, ya que permite retroalimentar y optimizar los sistemas de ciberseguridad de forma progresiva (Sanchez-Garcia et al., 2024; Blokdyk, 2021).

En el ámbito de defensa, la ciberseguridad cobra un rol prioritario como mecanismo de protección de información crítica y clasificada. Por ello, se implementó el modelo CMMC 2.0 (Cybersecurity Maturity Model Certification) (U.S. Department of Defense, 2021), diseñado para asegurar la protección de datos sensibles gestionados por contratistas y subcontratistas del Departamento de Defensa. Este modelo se basa en una estructura por niveles, evaluaciones de estándares de seguridad y cláusulas contractuales específicas. Fue formalmente adoptado el 30 de noviembre de 2020 y, en noviembre de 2021, se reforzó con nuevos requisitos orientados a fortalecer la cultura de ciberseguridad, la resiliencia, el cumplimiento normativo y la confianza entre partes implicadas.

En estudios recientes, Sabillón & M (2019) desarrollaron un modelo denominado CSAM (Cybersecurity Audit Model), validado para uso en diversos contextos —desde organizaciones específicas hasta auditorías integrales de ámbito nacional. Este modelo busca una mayor eficacia en los controles, ofreciendo respuestas efectivas ante amenazas cibernéticas, así como una mejora en la concienciación sobre ciberseguridad tanto a nivel organizacional como individual (Sabillón & M, 2019; Gamble, 2020).

3.3. Estándares

3.3.1. NIST CyberSecurity Framework 1.1

Este marco de trabajo surge de la Orden Ejecutiva 13636, cuyo objetivo fue encontrar un método para mejorar la ciberseguridad de infraestructuras críticas americanas. Este método debía ser "flexible, repetible, rentable y basado en medidas de seguridad de la información y controles que puedan ser adoptados voluntariamente por propietarios y operadores de infraestructura crítica para ayudarlos a identificar, evaluar y gestionar el riesgo cibernético" (National Institute of Standards and Technology, 2018).

Posteriormente, su dominio inicial fue expandido a múltiples organizaciones tanto públicas como privadas, encontrando su aplicación como una primera aproximación formal a la ciberseguridad en entornos espaciales (Scholl & Suloway, 2022). De la misma manera, la ESA utiliza actualmente la versión 1.1 de este marco, aunque plantea migrar a su versión 2.0 (National Institute of Standards and Technology, 2024).

Este marco de trabajo se compone de 3 pilares (National Institute of Standards and Technology, 2018):

- **Core:** Conjunto de actividades, referencias y salidas que se aplican a todas las implementaciones del marco.
- **Niveles de Implementación:** Grado en el que las prácticas de ciberseguridad de una organización se adecuan a las características definidas en el Marco.
- **Perfiles:** Personalización de las actividades del Marco para cada escenario, pudiendo ser varios de estos perfiles mejoras de los anteriores.

Primeramente, el **Core** se conforma por 5 Funciones, que organizan las acciones a cumplir para maximizar la seguridad. Se distingue que estas funciones forman una jerarquía de alto nivel, mientras que estas se subdividen en categorías y a su vez en subcategorías. Se describe a continuación las 5 funciones:

- **Identify:** Comprender el contexto de la organización (sistemas, personas, activos, datos y capacidades) para gestionar el riesgo de ciberseguridad, priorizando esfuerzos según la estrategia y necesidades del negocio.

- **Protect:** Desarrollar e implementar salvaguardas para asegurar la continuidad de los servicios críticos y limitar el impacto de posibles eventos de ciberseguridad.
- **Detect:** Desarrollar e implementar actividades para identificar de manera oportuna la ocurrencia de un evento de ciberseguridad.
- **Respond:** Desarrollar e implementar actividades para tomar acción ante un incidente de ciberseguridad detectado, con el fin de contener su impacto.
- **Recover:** Desarrollar e implementar actividades para mantener la resiliencia y restaurar las capacidades o servicios afectados por un incidente de ciberseguridad, permitiendo una recuperación oportuna a las operaciones normales.

Figura 4. Funciones del NIST CSF 1.1

Fuente: (NIST, 2018)

Al observar la Figura 2, se destaca que todas las Funciones mantienen focos en distintos ámbitos, lo que permite que sus acciones no tengan la necesidad de ejecutarse secuencialmente. Esta ejecución paralela permite dar agilidad a los procedimientos de las organizaciones, resultando en una mejor capacidad de adaptación frente al peligro.

Posteriormente, según National Institute of Standards and Technology (2024) los **Niveles de Implementación** "... caracterizan el rigor de las prácticas de gobernanza y gestión de los riesgos de ciberseguridad de una organización, y proporcionan el contexto de cómo una organización ve los riesgos de seguridad cibernética y los procesos establecidos para gestionar esos riesgos". Se encuentra dividido en 4 niveles: **Parcial**, **Conocimiento de los riesgos**, **Repetible** y **Adaptable**. Los niveles describen una evolución desde respuestas informales y ad hoc hasta enfoques ágiles, informados sobre el riesgo y en continua mejora.

Y finalmente, los **Perfiles Organizativos** describen la postura de ciberseguridad actual u objetivo de una organización en términos de los resultados del Core. Cada Perfil está formado por uno o ambos de los siguientes elementos:

- Un **Perfil Actual** que especifica lo resultado esenciales que una organización está logrando actualmente (o intentado lograr).
- Un **Perfil Objetivo** que especifica los resultados deseados seleccionados y priorizados para alcanzar los objetivos de gestión de riesgos de ciberseguridad.

3.3.2. NIST AI RMF 1.0

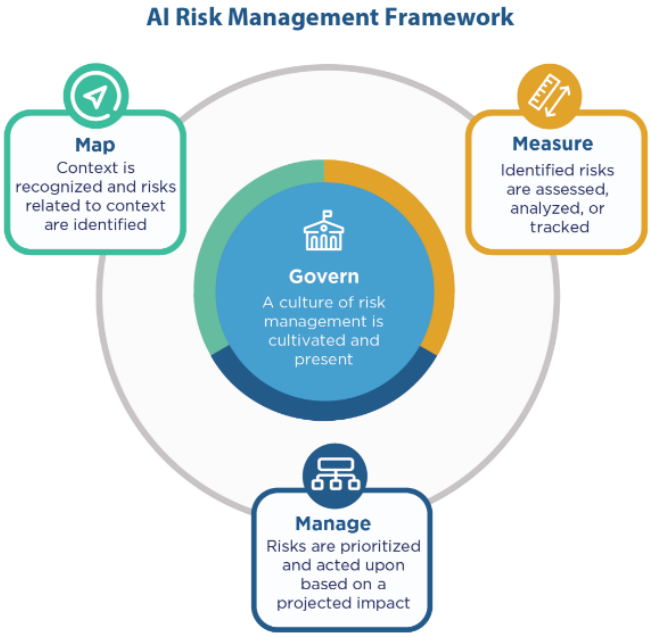
NIST AI Risk Management Framework es un framework desarrollado por NIST para mejorar el control de riesgos a individuales, organizaciones y sociedades asociadas con la inteligencia artificial. Su intención comprende su uso voluntario y mejorar la habilidad de incorporar consideraciones de fiabilidad en el diseño, desarrollo, uso y evaluación de productos, servicios y sistemas IA (NIST, 2021). Igualmente, debido a su novedad el propio NIST motiva a los usuarios y organizaciones a evaluar periódicamente como AI RMF ha mejorado el control de riesgos relacionados con la IA, de esta forma serán capaces de realizar cambios en futuras versiones con toda la retroalimentación recibida (European Union Agency for Cybersecurity, 2023). AI RMF define que un sistema fiable de IA debe alcanzar las siguientes características: Valid and reliable; Safe; Secure and resilient; Accountable and transparent; Explainable and interpretable; Privacy-enhanced; y Fair with harmful bias managed.

El **Core** de este framework proporciona resultados y acciones que permiten el diálogo, la comprensión y las actividades para gestionar los riesgos de la IA y desarrollar de forma responsable sistemas de IA fiables. Este se compone de las siguientes 4 funciones:

- **GOVERN:** Establece la cultura, estructura y políticas organizativas para la gestión de riesgos de la IA, asegurando la alineación con los objetivos e integrándose en todas las demás funciones.
- **MAP:** Establece el contexto de un sistema de IA, identificando riesgos e impactos potenciales mediante la recopilación de información y perspectivas diversas.
- **MEASURE:** Analiza, evalúa y monitoriza los riesgos e impactos de la IA utilizando métodos, métricas y pruebas cuantitativas y cualitativas.

- **MANAGE:** Asigna recursos para tratar los riesgos identificados y medidos, implementando planes de respuesta, priorizando acciones y monitorizando sistemas.

Figura 5. Funciones de AI RMF 1.0



Fuente: *(NIST, 2025)*

3.3.3. FAICP Framework

El *Marco de Prácticas de Ciberseguridad para IA* (FAICP, por sus siglas en inglés) es una iniciativa elaborada por **ENISA** (Agencia de la Unión Europea para la Ciberseguridad) con el objetivo de ofrecer una guía estructurada de buenas prácticas en ciberseguridad, relevantes para los sistemas de Inteligencia Artificial (IA) (European Union Agency for Cybersecurity, 2023). Este marco fue desarrollado en respuesta a los desafíos emergentes de seguridad derivados del uso creciente de la IA en múltiples sectores críticos, y se alinea con propuestas regulatorias como el *Artificial Intelligence Act* y marcos internacionales como el *NIST AI Risk Management Framework*.

El FAICP proporciona una cobertura integral que abarca **todo el ciclo de vida de los sistemas de IA**, desde la concepción, diseño y desarrollo hasta la implementación, mantenimiento y desactivación. También contempla aspectos críticos como la infraestructura TIC que los aloja, las prácticas de seguridad específicas de los modelos de IA, y las amenazas y vulnerabilidades

que afectan tanto a los datos como a los algoritmos. A su vez, incluye medidas relacionadas con la **cadena de suministro**, considerando los múltiples actores y tecnologías que intervienen en la creación y operación de estos sistemas.

3.3.3.1. Estructura del FAICP

El FAICP está organizado en **tres capas complementarias**, que permiten a los diferentes actores (autoridades nacionales, operadores, desarrolladores, auditores, etc.) identificar qué buenas prácticas deben aplicar según su nivel de intervención o exposición en relación con los sistemas de IA.

3.3.3.2. Capa I – Fundamentos de Ciberseguridad

Esta capa está orientada a garantizar la seguridad de las infraestructuras TIC que soportan los sistemas de IA. Aquí se recogen principios básicos de ciberseguridad aplicables a cualquier entorno digital, incluyendo:

- **Gestión de la seguridad del entorno TIC** (infraestructura física, redes, aplicaciones, servicios y usuarios).
- **Evaluación y gestión de riesgos** (análisis de amenazas, vulnerabilidades, impacto y selección de contramedidas).
- **Certificación y cumplimiento normativo** conforme a estándares como ISO/IEC 27001, Common Criteria (ISO/IEC 15408) y directivas europeas como NIS 2 o la Cybersecurity Act.
- **Políticas legales y regulaciones aplicables**, incluyendo protección de datos (GDPR) y resiliencia cibernética.

Esta capa establece una base común sobre la que construir prácticas más especializadas, y subraya la necesidad de asegurar el entorno donde los sistemas de IA operan para prevenir ataques, tanto intencionales (e.g. cibercriminales, insiders) como accidentales o ambientales.

3.3.3.3. Capa II – Ciberseguridad Específica para la IA

Reconociendo el carácter sociotécnico y dinámico de la IA, esta capa introduce prácticas diseñadas para hacer frente a riesgos particulares que surgen durante el desarrollo y operación de modelos de IA. Incluye:

- Evaluación y mitigación de amenazas específicas como:
  - Evasión de modelos (adversarial attacks).
  - Envenenamiento de datos de entrenamiento (data poisoning).
  - Pérdida de transparencia, explicabilidad, equidad y privacidad.
  - Compromiso de componentes del modelo o del pipeline de desarrollo.
- Aplicación de estándares emergentes para IA como:
  - ETSI SAI Threat Ontology, para entender amenazas únicas de IA.
  - ISO/IEC 22989 y 24029, centrados en la calidad, confiabilidad y trazabilidad de los sistemas IA (International Organization for Standardization, 2021, 2022).
- Recomendaciones para garantizar la confiabilidad y seguridad de los modelos, considerando atributos como transparencia, robustez, resiliencia, privacidad, imparcialidad y responsabilidad (en línea con el marco NIST AI RMF).
- Gestión de riesgos en la IA como un proceso **continuo**, adaptativo y enfocado tanto en aspectos técnicos como sociales (e.g., sesgos, desigualdades, impacto en derechos fundamentales).

3.3.3.4. Capa III – Actividades Sectoriales de Ciberseguridad para la IA

Dado que los sistemas de IA se aplican en sectores críticos y variados (salud, energía, transporte, telecomunicaciones, finanzas, etc.), esta capa fomenta la adopción de prácticas adaptadas a las necesidades específicas de cada ámbito. Incluye:

- Recomendaciones para sistemas de IA **de alto riesgo**, según lo definido en el *Artificial Intelligence Act*.
- Evaluación del entorno operativo del sistema y su impacto potencial.
- Incorporación de buenas prácticas y requisitos técnicos conforme a marcos normativos sectoriales.

- Coordinación con autoridades nacionales competentes para garantizar la vigilancia y cumplimiento regulatorio.

Este enfoque reconoce que la IA no opera en un vacío técnico, sino que interactúa con entornos complejos y sensibles, por lo cual la ciberseguridad debe integrarse desde el diseño (*security by design*) con una visión sectorial.

3.3.3.5. Sinergias y Enfoque Multinivel

El FAICP también promueve la armonización entre distintas iniciativas nacionales e internacionales mediante la integración con marcos existentes, como el NIST AI Risk Management Framework, el OECD AI Principles, y la normativa europea en evolución. Busca así facilitar la interoperabilidad, fomentar la innovación responsable y contribuir a la creación de una IA confiable, ética y segura en toda Europa.

3.3.3.6. Conclusión

En resumen, el FAICP constituye un marco práctico, escalable y holístico, diseñado para reforzar la seguridad y la capacidad de recuperación de los sistemas de inteligencia artificial. Ofrece herramientas útiles para diseñadores, operadores y reguladores, en un contexto donde la IA juega un papel cada vez más decisivo para el bienestar social, la competitividad económica y la protección de los valores fundamentales de la Unión Europea.

3.4. Auditorías en la ESA

La Agencia Espacial Europea (ESA), como organización intergubernamental líder en el ámbito aeroespacial, tiene entre sus prioridades estratégicas la protección de los activos de información que sustentan sus programas, especialmente aquellos relacionados con la navegación por satélite (como los sistemas GALILEO y EGNOS). En este contexto, la ciberseguridad no solo es una necesidad técnica, sino una condición crítica para garantizar la continuidad operativa, la integridad de los datos y la resiliencia ante ciber amenazas.

3.4.1.1. Uso del marco COBIT 2019 y CAATs

Uno de los principales marcos de referencia utilizados por la ESA para el gobierno de las tecnologías de la información es COBIT 2019 (Control Objectives for Information and Related Technologies), el cual permite alinear los objetivos de TI con los de la organización y establecer un sistema sólido de control y auditoría (ISACA, 2019). En el TFM se destaca cómo este marco ayuda a estructurar procesos de gestión del riesgo y madurez tecnológica dentro de las auditorías, en conjunto con estándares como NIST y ISO 27001.

En el proceso auditor, se hace uso de CAATs (Computer-Assisted Audit Tools), herramientas informáticas que permiten la automatización de múltiples fases de la auditoría, como la recolección de datos, análisis de registros de eventos, evaluación de controles técnicos y generación de informes (Marei, 2019). Las CAATs son particularmente útiles para manejar volúmenes masivos de datos, como los que se generan en los sistemas de navegación satelital, y detectar anomalías que puedan indicar brechas de seguridad o malas prácticas.

Estas herramientas también contribuyen a garantizar la objetividad y trazabilidad de los hallazgos, además de reducir el margen de error humano y acelerar la respuesta ante posibles incidentes.

3.4.1.2. Normativas aplicadas: ISO 19011 e NIST SP 800-53

Las auditorías en la ESA están estructuradas y documentadas bajo estándares internacionales de alto nivel, que aseguran una cobertura integral de los distintos dominios de ciberseguridad:

- ISO 19011: Esta norma ofrece directrices sobre cómo planificar, ejecutar y gestionar auditorías de sistemas de gestión (International Organization for Standardization, 2018). Establece los principios de auditoría, la competencia de los auditores, y cómo evaluar el desempeño del programa auditor. En el contexto de la ESA, esta norma es la base para el enfoque metodológico y la estructura formal de las auditorías.
- NIST SP 800-53 (rev. 5): Proporciona un conjunto detallado de controles de seguridad y privacidad aplicables a sistemas federales y críticos (Joint Task Force Interagency Working Group, 2020). Estos controles son adaptados por la ESA para asegurar que los sistemas de

navegación y sus componentes cumplan con medidas rigurosas de acceso, respuesta a incidentes, protección de redes y cifrado de datos.

3.4.1.3. Metodología basada en el ciclo PHVA

La ESA adopta una metodología cíclica y sistemática para gestionar sus auditorías, basada en el modelo PHVA (Planificar – Hacer – Verificar – Actuar) (Moen, 2009; Buzzi, 2023). Este ciclo de mejora continua es común en los sistemas de gestión de calidad y se adapta con éxito al entorno de ciberseguridad:

- **Planificar:** Se definen los objetivos, alcance, criterios, equipos de auditoría y métodos a utilizar. En esta fase se realiza una evaluación de riesgos previa, basada en los marcos mencionados (NIST, ISO, COBIT).
- **Hacer:** Se lleva a cabo la auditoría utilizando tanto métodos manuales como CAATs. Aquí se revisan los controles implementados, se analizan logs, configuraciones de red, registros de acceso y políticas de seguridad aplicadas en los sistemas auditados.
- **Verificar:** Se analizan los hallazgos comparándolos con los criterios de conformidad. Se identifican brechas de seguridad, incumplimientos y oportunidades de mejora.
- **Actuar:** En base a los resultados, se elaboran planes de acción correctiva y preventiva. Esta fase puede implicar rediseño de procesos, formación adicional, o integración de nuevas soluciones tecnológicas.

Este enfoque cíclico permite a la ESA asegurar que su sistema de gestión de ciberseguridad evoluciona continuamente frente a nuevas amenazas, vulnerabilidades y exigencias regulatorias.

3.4.1.4. Principal problema: cadena de suministro extendida

Uno de los mayores desafíos identificados en el TFM es la complejidad de la cadena de suministro que participa en los programas de navegación de la ESA. Estos proyectos implican a decenas de contratistas y subcontratistas, lo que genera una cadena de distribución con hasta cuatro niveles de profundidad.

Esta cadena de suministro incluye no sólo fabricantes de componentes físicos, sino también desarrolladores de software, integradores de sistemas, operadores de red y proveedores de servicios en la nube. Cada uno de estos actores representa un punto potencial de riesgo, especialmente si no están alineados con los mismos niveles de exigencia en materia de ciberseguridad.

Las auditorías deben, por tanto, extenderse más allá del perímetro interno de la ESA e involucrar controles sobre estos proveedores. Esto incluye la aplicación de requisitos contractuales, el análisis de cumplimiento normativo de terceros, y en algunos casos, la ejecución de auditorías externas.

El riesgo de propagación de una brecha de seguridad a través de esta red de proveedores es elevado, por lo que el TFM recomienda herramientas como el software ESA-GNSS-CIA-CAATS-2024, diseñado para mapear y evaluar el cumplimiento de la directiva NIS2 en toda la cadena de valor.

3.4.1.5. Conclusión

El enfoque de la ESA en cuanto a auditorías de ciberseguridad es robusto, metodológico y basado en estándares internacionales. El uso combinado de marcos como COBIT 2019, herramientas CAATs y normas como ISO 19011 y NIST SP 800-53 permite auditar de forma eficaz entornos altamente complejos, como el de la navegación por satélite.

Sin embargo, la creciente complejidad de la cadena de suministro representa un reto continuo, que debe abordarse con políticas proactivas, integración de proveedores en el marco de ciberseguridad y herramientas de evaluación automatizadas. La adopción de la directiva NIS2, en este sentido, es un paso clave para garantizar un enfoque integral y resiliente ante las amenazas del entorno digital actual.

4. Desarrollo del Proyecto

4.1. Contexto

La Agencia Espacial Europea (ESA) lidera iniciativas estratégicas en tecnologías espaciales críticas como los sistemas de navegación por satélite GALILEO y EGNOS. En estos entornos, la ciberseguridad no es solo una medida preventiva, sino un componente esencial para garantizar la operatividad, resiliencia y soberanía tecnológica de Europa.

Frente a este reto, la ESA realiza auditorías internas en sus sistemas utilizando herramientas conocidas como CAAT (Computer-Assisted Audit Tools). Estas herramientas permiten aplicar marcos normativos como NIST CSF, ISO 27001, COBIT, CMMC o directivas como la NIS2, evaluando la madurez y efectividad de los controles de seguridad. Dado el volumen de datos, la complejidad de los marcos y la criticidad de los sistemas surge la necesidad de una herramienta integrada, adaptable y automatizada que centralice el proceso.

La respuesta a esta necesidad es el desarrollo de un aplicativo Excel, ESA GNSS CIA – CAATS.

4.2. Descripción

La herramienta está compuesta por múltiples hojas Excel, cada una con una función concreta dentro del proceso de auditoría. A continuación, se describen las principales:

- **Hoja MANUAL**

  Actúa como portada y centro de control del archivo. Proporciona instrucciones generales, el año de referencia de la auditoría y una guía rápida sobre cómo interpretar los resultados. Es útil para contextualizar los estándares incluidos y para que nuevos usuarios comprendan la herramienta.

Tabla 4. Hoja Manual

This file contains the main ESA INTERNAL CAATS for the ESA GNSS Cyber Internal Audits and an adaption of both NIST AI RMF 1.0 and FAICP Framework for a Master final project

	List of Sheets
SC	ESA GNSS CIA CAATS: Subcontrols Assessment

	List of Sheets
CSF	ESA GNSS CIA **Maturity Model** (EGCIA-CM): details

	List of sheets (NIST)
AIRM	ESA GNSS CIA AI COMPLIANCE MODEL (NIST AI RMF): details
AIRM-G	ESA GNSS CIA ARTIFICIAL INTELLIGENCE COMPLIANCE MODEL (EGCIA-AIRM): global insights

	List of Sheets (FAICP)
FAICP	ESA GNSS CIA FAICP COMPLIANCE MODEL (NIST FAICP): details
FAICP-G	ESA GNSS CIA ARTIFICIAL INTELLIGENCE COMPLIANCE MODEL (EGCIA-FAICP): global insights

Graphs default values

Reference Value	Scale			
0,60	0,00			
0,60	0,10			
0,60	0,20			
0,60	0,30			
0,60	0,40			
0,60	0,50			
0,60	0,60			
0,60	0,70			
0,60	0,80			
0,60	0,90			
0,60	1,00			
0,60				
0,60				

Fuente: Adaptación de la herramienta de la ESA

- **Hoja SC (SubControls)**

  Es la hoja base donde el auditor introduce manualmente la puntuación (de 0 a 1) de cada subcontrol de seguridad definido por la ESA. Cada subcontrol está descrito con su código (SC-ID1, SC-ID2…), nombre y peso. Los valores introducidos aquí se propagan al resto de hojas mediante fórmulas o macros, permitiendo analizar el estado de seguridad según distintos marcos normativos.

Tabla 5. Hoja SC (Subcontrols)

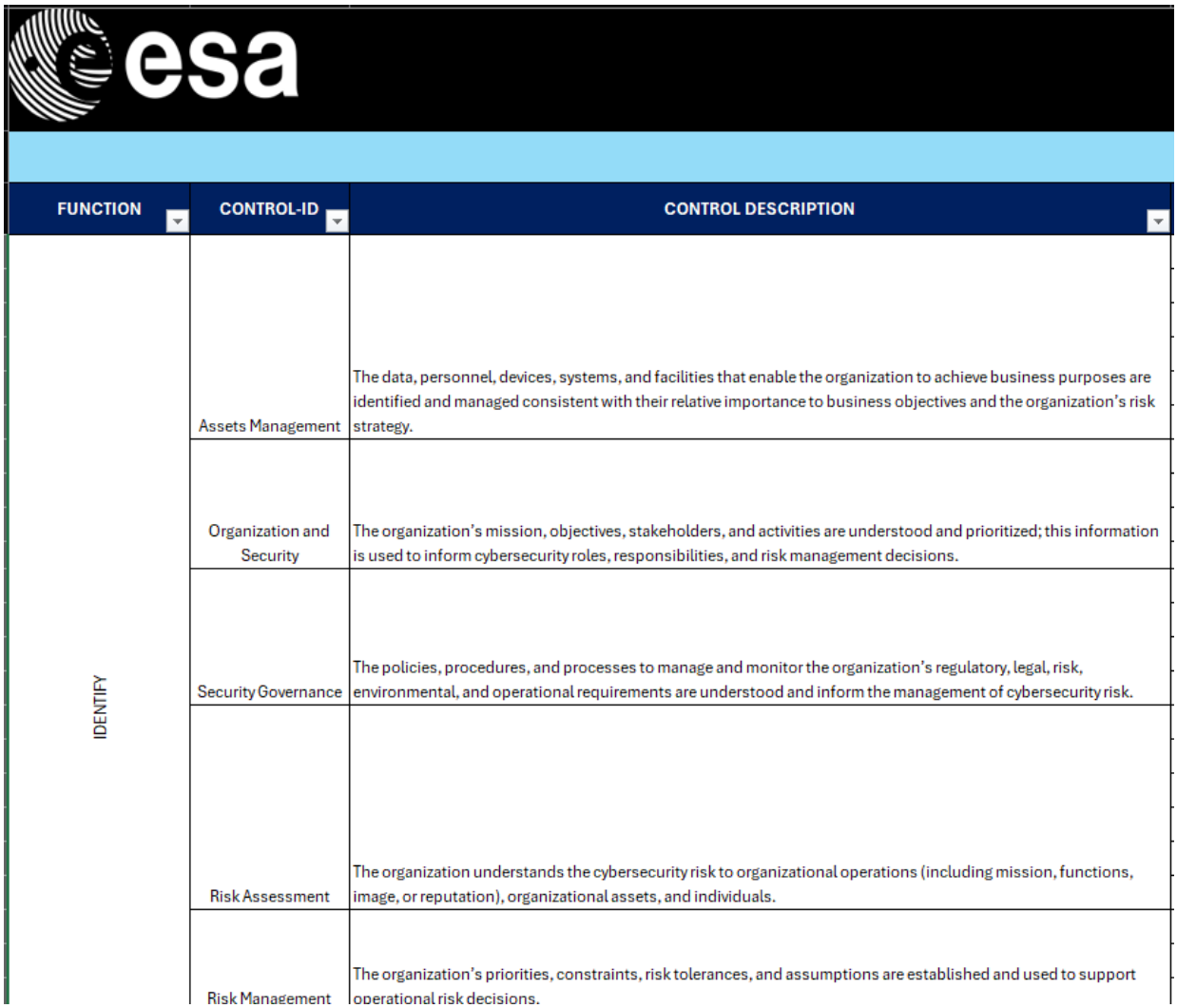
SC-ID	SC-D	W	PROGRAM	2025	2024	AC2025
SC-ID1	Physical devices and systems within the organization are inventoried	1	AUDIT-NAME	0,60	0,60	0,6
SC-ID2	Software platforms and applications within the organization are inventoried	1	AUDIT-NAME	0,60	0,60	
SC-ID3	Architecture and organizational communication and data flows	0,25	AUDIT-NAME	0,60	0,60	
SC-ID4	External information systems are catalogued	0,5	AUDIT-NAME	0,60	0,60	
SC-ID5	Resources (HW, devices, data, personnel, and SW) are prioritized based on their classification, criticality, and business value	1	AUDIT-NAME	0,40	0,60	
SC-ID6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established	1	AUDIT-NAME	0,60	0,60	
SC-ID7	The organization's role in the supply chain is identified and communicated	0,5	AUDIT-NAME	0,60	0,60	0,6
SC-ID8	The organization's place in critical infrastructure and its industry sector is identified and communicated	0,1	AUDIT-NAME	0,60	0,60	
SC-ID9	Dependencies and critical functions for delivery of critical services are established	0,1	AUDIT-NAME	0,60	0,60	
SC-ID10	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	0,25	AUDIT-NAME	0,60	0,60	

Fuente: Adaptación de la herramienta de la ESA

- **Hoja CSF (NIST Cybersecurity Framework)**

  Esta hoja traduce los subcontroles SC a las funciones y categorías del NIST CSF v1.1. Está estructurada por funciones (Identify, Protect, Detect, Respond, Recover), con subcategorías como ID.AM-1, PR.AC-4, etc. Cada control incluye su equivalencia con SC y su madurez correspondiente. Se presentan las puntuaciones actuales y pasadas, además de resúmenes por función.

Tabla 6. Hoja CSF (NIST Cybersecurity Framework), 1/3



FUNCTION	CONTROL-ID	CONTROL DESCRIPTION
IDENTIFY	Assets Management	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.
	Organization and Security	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
	Security Governance	The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
	Risk Assessment	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
	Risk Management	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

Fuente: Adaptación de la herramienta de la ESA

Tabla 7. Hoja CSF (NIST Cybersecurity Framework), 2/3

NIST Cybersecurity Secur
SUBCONTROL DESCRIPTION WITH CSF-CODE
ID.AM-1: Physical devices and systems within the organization are inventoried
ID.AM-2: Software platforms and applications within the organization are inventoried
ID.AM-3: Organizational communication and data flows are mapped
ID.AM-4: External information systems are catalogued
ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
ID.BE-1: The organization's role in the supply chain is identified and communicated
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated
ID.BE-4: Dependencies and critical functions for delivery of critical services are established
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)
ID.GV-1: Organizational cybersecurity policy is established and communicated
ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
ID.GV-4: Governance and risk management processes address cybersecurity risks
ID.RA-1: Asset vulnerabilities are identified and documented
ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources
ID.RA-3: Threats, both internal and external, are identified and documented
ID.RA-4: Potential business impacts and likelihoods are identified
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
ID.RA-6: Risk responses are identified and prioritized
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders
ID.RM-2: Organizational risk tolerance is determined and clearly expressed
ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis

Fuente: Adaptación de la herramienta de la ESA

Tabla 8. Hoja CSF (NIST Cybersecurity Framework), 3/3

SUBCONTROL	CAT	SUBCA	SC21 Assessment	SC20/G2.2 Assessment	SUBCONTROL Maturity Level	CONTROL-ID	C-2025 Assessment	C-2024 Assessment	CONTROL Maturity Model	FUNCTION	F-2025 Assessment	F-2024 Assessment	FUNCTION Maturity Model
SC-ID1	ID.AM	ID.AM-1	0,60	0,60		Assets Management	0,56	0,60		IDENTIFY	0,61	0,60	
SC-ID2	ID.AM	ID.AM-2	0,60	0,60									
SC-ID3	ID.AM	ID.AM-3	0,60	0,60									
SC-ID4	ID.AM	ID.AM-4	0,60	0,60									
SC-ID5	ID.AM	ID.AM-5	0,40	0,60									
SC-ID6	ID.AM	ID.AM-6	0,60	0,60									
SC-ID7	ID.BE	ID.BE-1	0,60	0,60		Organization and Security	0,60	0,60					
SC-ID8	ID.BE	ID.BE-2	0,60	0,60									
SC-ID9	ID.BE	ID.BE-4	0,60	0,60									
SC-ID10	ID.BE	ID.BE-5	0,60	0,60									
SC-ID11	ID.GV	ID.GV-1	0,40	0,60		Security Governance	0,60	0,60					
SC-ID12	ID.GV	ID.GV-2	0,60	0,60									
SC-ID13	ID.GV	ID.GV-3	0,60	0,60									
SC-ID14	ID.GV	ID.GV-4	0,60	0,60									
SC-ID15	ID.RA	ID.RA-1	0,20	0,60		Risk Assessment	0,30	0,60					
SC-ID16	ID.RA	ID.RA-2	0,40	0,60									
SC-ID17	ID.RA	ID.RA-3	0,20	0,60									
SC-ID18	ID.RA	ID.RA-4	0,40	0,60									
SC-ID19	ID.RA	ID.RA-5	0,20	0,60									
SC-ID20	ID.RA	ID.RA-6	0,40	0,60									
SC-ID21	ID.RM	ID.RM-1	0,60	0,60		Risk Management	0,63	0,60					
SC-ID22	ID.RM	ID.RM-2	0,40	0,60									
SC-ID23	ID.RM	ID.RM-3	1,00	0,60									

Fuente: Adaptación de la herramienta de la ESA

- **Hoja AIRM**

  Esta hoja contiene una valoración más amplia e integrada de la madurez general del sistema. Se orienta a interpretar el nivel de implementación desde una perspectiva organizacional más alta. Aquí se reflejan funciones, dominios y métricas combinadas provenientes del resto de hojas.

Tabla *9*. Hoja AIRM, 1/2

esa **ESA GNSS CIA AI COMPLIANCE**

STANDARD Artificial Intelligence Risk Mana

CATEGORY	CATEGORY Description	SUBCATEGORY	SUBCATEGORY Description
GOVERN 1	Policies, processes, procedures, and practices across the organization related to the mapping, measuring, and managing of AI risks are in place, transparent, and implemented effectively.	GOVERN 1.1	Legal and regulatory requirements involving AI are understood, managed, and documented.
		GOVERN 1.2	The characteristics of trustworthy AI are integrated into organizational policies, processes, procedures, and practices.
		GOVERN 1.3	Processes, procedures, and practices are in place to determine the needed level of risk management activities based on the organization's risk tolerance.
		GOVERN 1.4	The risk management process and its outcomes are established through transparent policies, procedures, and other controls based on
		GOVERN 1.5	Ongoing monitoring and periodic review of the risk management process and its outcomes are planned and organizational roles and responsibilities clearly defined, including determining the frequency of periodic review.
		GOVERN 1.6	Mechanisms are in place to inventory AI systems and are resourced
		GOVERN 1.7	Processes and procedures are in place for decommissioning and phasing out AI systems safely and in a manner that does not increase risks or
GOVERN 2	Accountability structures are in place so that the appropriate teams and individuals are empowered, responsible, and trained for mapping, measuring, and managing AI risks.	GOVERN 2.1	Roles and responsibilities and lines of communication related to mapping, measuring, and managing AI risks are documented and are
		GOVERN 2.2	The organization's personnel and partners receive AI risk management training to enable them to perform their duties and responsibilities
		GOVERN 2.3	Executive leadership of the organization takes responsibility for decisions about risks associated with AI system development and deployment.

Fuente: Adaptación de la herramienta de la ESA

Tabla 10. Hoja AIRM, 2/2

E MODEL (NIST AI RMF)

agement: NIST AI RMF AI 100-1 v1.0

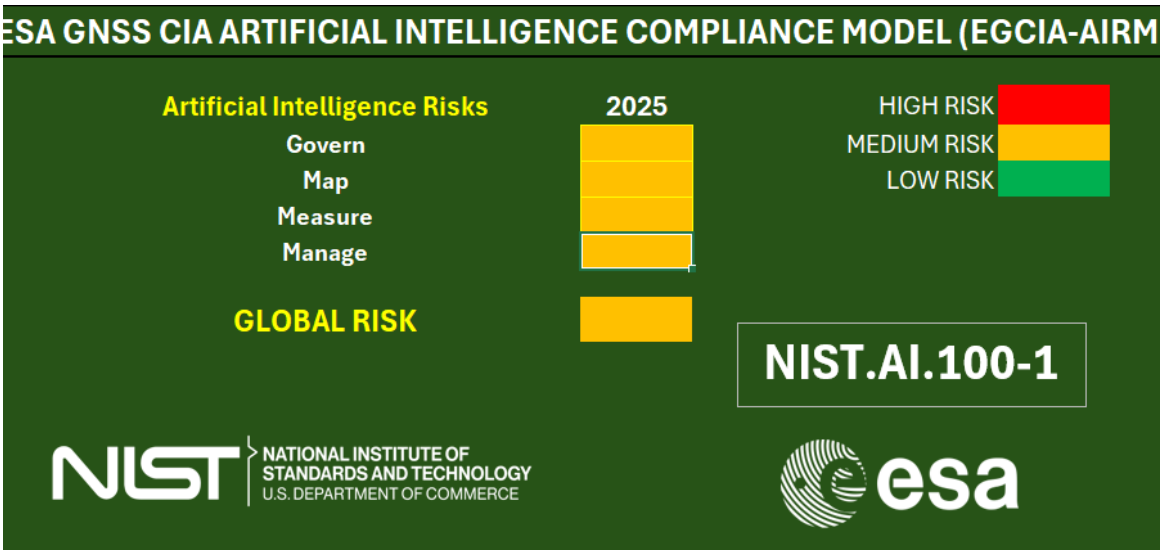
SUBCONTROLS	2025	CATEGORY	FUNCTION
SC-ID7, SC-ID9, SC-ID12, SC-ID13, SC-ID24, SC-ID25, SC-ID26, SC-ID43, SC-ID50, SC-ID54, SC-ID61, SC-ID62, SC-ID68	0,56	0,48	0,44
SC-ID11, SC-ID16, SC-ID17, SC-ID18, SC-ID24, SC-ID25, SC-ID31, SC-ID33, SC-ID47, SC-ID51, SC-ID66, SC-ID67, SC-ID95	0,47		
SC-ID6, SC-ID8, SC-ID14, SC-ID16, SC-ID17, SC-ID18, SC-ID19, SC-ID20, SC-ID21, SC-ID22, SC-ID23, SC-ID24, SC-ID25, SC-ID26, SC-ID31, SC-ID33, SC-ID44, SC-ID47, SC-ID51, SC-ID66, SC-ID67, SC-ID95, SC-ID97	0,49		
SC-ID6, SC-ID8, SC-ID11, SC-ID14, SC-ID16, SC-ID17, SC-ID18, SC-ID19, SC-ID20, SC-ID21, SC-ID22, SC-ID24, SC-ID25, SC-ID26, SC-ID31, SC-ID33, SC-ID44, SC-ID47, SC-ID51, SC-ID66, SC-ID67, SC-ID95, SC-ID97	0,48		
SC-ID6, SC-ID13, SC-ID14, SC-ID15, SC-ID16, SC-ID17, SC-ID18, SC-ID19, SC-ID21, SC-ID22, SC-ID24, SC-ID25, SC-ID26, SC-ID28, SC-ID44, SC-ID51, SC-ID55, SC-ID56, SC-ID58, SC-ID60, SC-ID79, SC-ID82, SC-ID84, SC-ID95, SC-ID98, SC-ID99, SC-ID101, SC-ID102	0,45		
SC-ID1, SC-ID2, SC-ID5, SC-ID41, SC-ID42, SC-ID45, SC-ID46, SC-ID52, SC-ID64, SC-ID68	0,49		
SC-ID24, SC-ID43, SC-ID50, SC-ID54, SC-ID60, SC-ID61, SC-ID62	0,43		
SC-ID6, SC-ID12, SC-ID24, SC-ID80	0,51	0,51	
SC-ID11, SC-ID16, SC-ID17, SC-ID18, SC-ID24, SC-ID25, SC-ID31, SC-ID33, SC-ID36, SC-ID37, SC-ID38, SC-ID39, SC-ID40, SC-ID43, SC-ID44, SC-ID47, SC-ID51, SC-ID66, SC-ID67, SC-ID86, SC-ID95	0,52		
SC-ID6, SC-ID14, SC-ID16, SC-ID17, SC-ID18, SC-ID21, SC-ID24, SC-ID25, SC-ID43, SC-ID44, SC-ID51, SC-ID80, SC-ID95	0,50		
SC-ID16, SC-ID17	0,30		

Fuente: Adaptación de la herramienta de la ESA

- **Hoja AIRM-G**

  Presenta gráficamente los resultados de la hoja AIRM. Utiliza elementos gráficos y comparativas de funciones para mostrar visualmente qué áreas requieren atención o refuerzo.

Tabla 11. Hoja AIRM-G



Fuente: Adaptación de la herramienta de la ESA

- **Hoja FAICP Q&A**

  Contiene una lista de preguntas y respuestas alineadas con el marco FAICP (Framework for AI Cybersecurity Practices), proporcionando soporte al auditor para evaluar riesgos relacionados con inteligencia artificial en ciberseguridad. Funciona como guía para una evaluación cualitativa complementaria.

Tabla 12. Hoja FAICP Q&A, 1/2

esa	ESA GNSS CIA FAICP COMPLIANCE MODEL (NIST FAICP)					
Policy Area	Q-ID	Question description	Mapping with CSF (column NIST5/C)	Value Obtained	Response	Policy Area Response
Human Capital	FAICP-Q-1	**Have you built/do you plan to build synergies with educational authorities/institutions to increase AI cybersecurity capabilities at all levels of education?**	SC-ID16, SC-ID36	0,4	Partially Compliance	Non Compliance
Human Capital	FAICP-Q-2	**Do you offer awareness campaigns about the secure development and use of AI solutions?**	SC-ID16, SC-ID90	0,2	Non Compliance	
Human Capital	FAICP-Q-3	**Do you provide guidance and best practices on how to improve AI security?**	SC-ID11, SC-ID14	0,4	Partially Compliance	
Human Capital	FAICP-Q-4	Do you consider AI cybersecurity in syllabus of courses dedicated to AI or to CS?	SC-ID36, SC-ID59, SC-ID90	0,2	Non Compliance	
Human Capital	FAICP-Q-5	Do you offer practical trainings to the AI stakeholders and can elaborate to which stakeholders?	SC-ID38	1	Fully Compliance	
Human Capital	FAICP-Q-6	Do you organise national, regional and cross-border cybersecurity exercises enabling the upskilling of the AI stakeholders?	SC-ID27, SC-ID28, SC-ID52, SC-ID58, SC-I	0,2	Non Compliance	
From the lab to the market	FAICP-Q-7	**Do you offer any type of support (funding/scholarships/collaboration opportunities) to increase the cybersecurity capabilities of newly innovative solutions that rely on AI?**	SC-ID24, SC-ID90	0,2	Non Compliance	
From the lab to the market	FAICP-Q-8	Do you use any specific means to support SMEs/MEs to secure their AI products?	SC-ID26	1	Fully Compliance	
From the lab to the market	FAICP-Q-9	Do you have or promote testing environments, like sandboxes/cyber ranges/simulation platforms, to test and evaluate AI vulnerabilities before market?	SC-ID47	1	Fully Compliance	
From the lab to the market	FAICP-Q-10	Do you have specific measurements/KPIs/metrics that the AI stakeholders are imposed to use?	SC-ID27, SC-ID70	0,4	Partially Compliance	Non Compliance
From the lab to the market	FAICP-Q-11	**Have you informed national AI stakeholders on cybersecurity requirements set by the NCAs for their AI products?**	SC-ID6, SC-ID11, SC-ID13	0,4	Partially Compliance	
From the lab to the market	FAICP-Q-12	**Do you have a process to monitor if such requirements have been met?**	SC-ID27, SC-ID72, SC-ID78	0,2	Non Compliance	
From the lab to the market	FAICP-Q-13	Do you have a process to inform the national stakeholders about the relevant legal instruments and standards available?	SC-ID13, SC-ID38, SC-ID90	0,2	Non Compliance	

Fuente: Adaptación de la herramienta de la ESA

Tabla 13. Hoja FAICP Q&A, 2/2

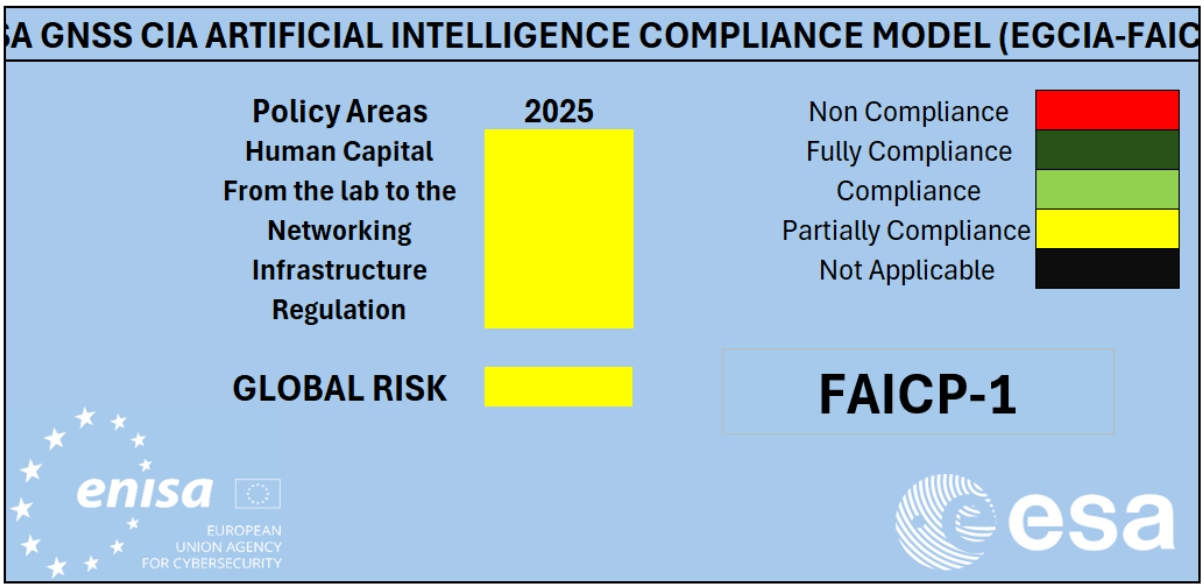
Response	Values Obtained
Non Compliance	0.39 or less
Fully Compliance	More than 0.80
Compliance	Between 0.6 and 0.80
Partially Compliance	Between 0.39 and 0.60
Not Applicable	N/A

Fuente: Adaptación de la herramienta de la ESA

- **Hoja FAICP Q&A – G**

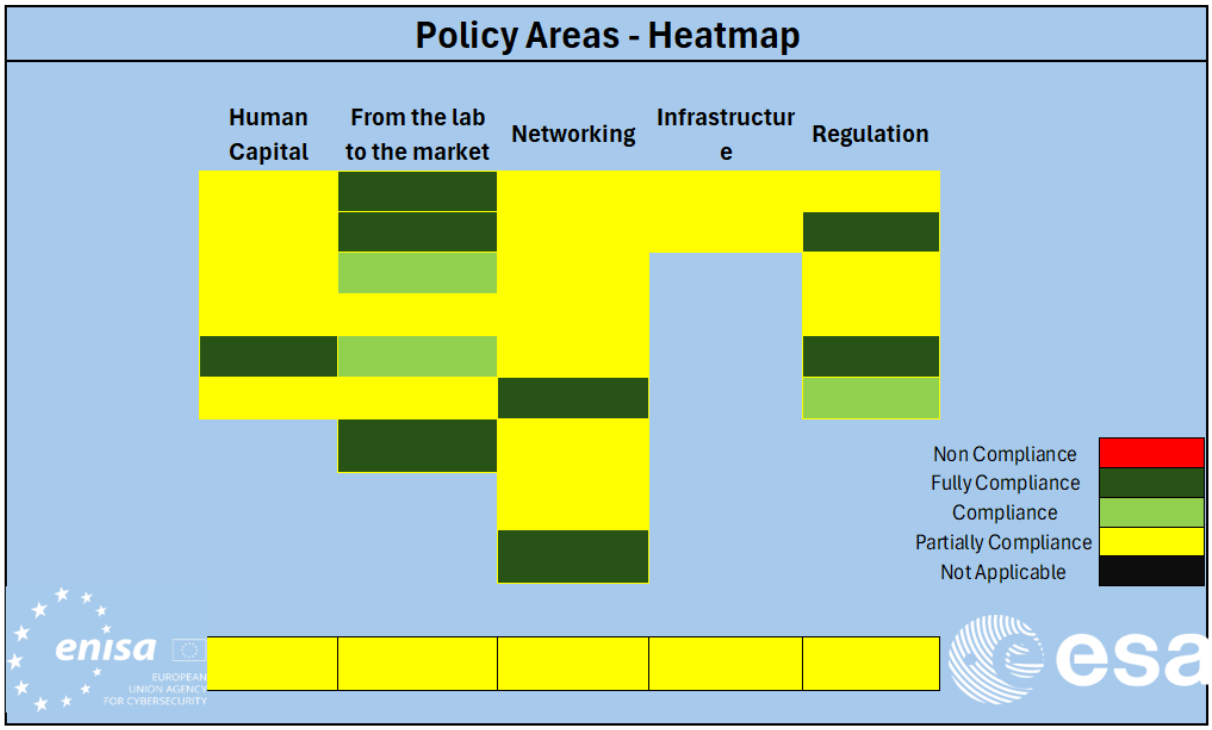
  Esta hoja proporciona una visualización resumida del nivel de cumplimiento del modelo FAICP, estructurada por áreas de política. A través de un panel de evaluación global y un mapa de calor (heatmap), permite identificar de forma rápida y visual el grado de conformidad alcanzado en cada área clave relacionada con la ciberseguridad en inteligencia artificial. Esta representación gráfica complementa la evaluación cualitativa, facilitando la interpretación de resultados y apoyando la toma de decisiones estratégicas.

Tabla 14. FAICP Q&A – G, 1/2



Fuente: Adaptación de la herramienta de la ESA

Tabla 15. FAICP Q&A – G, 2/2



Fuente: Adaptación de la herramienta de la ESA

- **Hoja SIMULATE**

  Esta hoja permite realizar auditorías simuladas. El auditor puede modificar valores de forma hipotética para predecir cómo impactarían ciertos fallos o cambios en la valoración final del sistema. Esta hoja es clave para escenarios de entrenamiento, planificación y resiliencia.

Tabla 16. Hoja Simulate

SC-ID	SUB-CONTROL DESCRIPTION	AUDIT _1	AUDIT _2	AUDIT _3	AUDIT _4	AUDIT _5	AUDIT _6	AUDIT _7	AUDIT _8	AUDIT _9
SC-ID1	Physical devices and systems within the organization are inventoried	0,60	0,80	0,60	0,60	0,80	0,60	0,80	0,60	0,60
SC-ID2	Software platforms and applications within the organization are inventoried	0,60	0,80	0,60	0,60	0,80	0,60	0,60	0,60	0,60
SC-ID3	Architecture and organizational communication and data flows	0,60	0,60	0,60	0,80	0,60	0,80	0,80	0,80	0,60
SC-ID4	External information systems are catalogued	0,60	0,80	0,60	0,80	0,60	0,60	0,80	0,80	0,60
SC-ID5	Resources (HW, devices, data, personnel, and SW) are prioritized based on their classification, criticality, and business value	0,40	0,80	0,60	0,80	0,60	0,60	0,80	0,40	0,40
SC-ID6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established	0,60	0,60	0,60	0,80	0,80	0,80	0,60	0,60	0,60
SC-ID7	The organization's role in the supply chain is identified and communicated	0,60	0,80	0,80	1,00	0,80	0,80	0,80	0,80	0,60
SC-ID8	The organization's place in critical infrastructure and its industry sector is identified and communicated	0,60	1,00	0,60	1,00	1,00	0,80	0,60	1,00	0,60
SC-ID9	Dependencies and critical functions for delivery of critical services are established	1,00	0,80	0,80	1,00	0,80	1,00	1,00	1,00	0,60
SC-ID10	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	1,00	0,80	0,60	1,00	0,60	0,80	1,00	1,00	0,60
SC-ID11	Organizational cybersecurity policy is established and communicated	0,60	0,60	0,60	0,80	1,00	0,80	0,80	0,60	0,40
SC-ID12	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	0,40	0,60	0,60	0,80	0,60	0,60	0,60	0,80	0,60
SC-ID13	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	1,00	1,00	0,60	1,00	0,80	0,80	0,80	0,80	0,60
SC-ID14	Strategy of security, governance and risk management processes address cybersecurity risks	0,40	0,60	0,80	0,80	0,60	0,60	0,40	0,40	0,60
SC-ID15	Asset vulnerabilities are identified and documented	0,40	0,60	0,40	0,80	0,60	0,60	0,60	0,20	0,20
SC-ID16	Cyber threat intelligence is received from information sharing forums and sources	0,40	0,20	0,40	0,40	0,80	0,60	0,60	0,40	0,40
SC-ID17	Threats, both internal and external, are identified and documented	0,40	0,60	0,40	0,60	0,80	0,60	0,60	0,40	0,20
SC-ID18	Potential business impacts and likelihoods are identified (BIA)	0,40	0,60	0,60	0,40	0,60	0,40	0,60	0,40	0,40
SC-ID19	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	0,40	0,60	0,40	0,80	0,80	0,60	0,60	0,20	0,20
SC-ID20	Risk responses are identified and prioritized	0,40	0,60	0,60	0,80	0,60	0,40	0,80	0,20	0,40
SC-ID21	Risk management processes are established, managed, and agreed to by organizational stakeholders	0,40	0,80	0,80	0,80	0,60	0,60	0,80	0,20	0,60

Fuente: Adaptación de la herramienta de la ESA

4.3. Funcionalidad inicial

El comportamiento inicial del aplicativo está diseñado cuidadosamente en torno a tres principios fundamentales que guían su funcionamiento: automatización, modularidad y visualización clara. Estos principios permiten que la herramienta sea eficiente, flexible y fácil de interpretar tanto para usuarios técnicos como no técnicos. La automatización asegura que los procesos internos se realicen con mínima intervención manual, reduciendo errores y

aumentando la consistencia de los resultados. La modularidad permite que cada componente o funcionalidad esté estructurado de forma independiente, facilitando su mantenimiento, actualización o reemplazo. Por último, la visualización clara garantiza que la información generada sea comprensible y útil para la toma de decisiones estratégicas.

El flujo de funcionamiento del aplicativo comienza con la entrada de datos realizada por el auditor en una hoja específica denominada "SC". En esta hoja, el auditor debe asignar una puntuación numérica a cada subcontrol evaluado, como por ejemplo SC-ID1, SC-PR3, entre otros. Estas puntuaciones se basan en una escala estandarizada de madurez que refleja el nivel de implementación de cada subcontrol dentro de la organización. La escala comprende los siguientes valores: 0 indica que el subcontrol no está implementado; 0.2, que existe alguna evidencia inicial; 0.4, que está implementado; 0.6, que ha sido formalizado o documentado; 0.8, que está siendo supervisado y mejorado continuamente; y 1, que se encuentra completamente optimizado. Esta escala permite una evaluación granular y objetiva del estado de madurez de los controles implementados.

Una vez que se han introducido estas puntuaciones, el sistema activa su segundo paso fundamental: la propagación automática de los datos. A través de una serie de fórmulas integradas —algunas de ellas desarrolladas mediante Visual Basic for Applications (VBA)—, las puntuaciones ingresadas por el auditor se diseminan automáticamente hacia otras hojas del aplicativo, como por ejemplo la hoja denominada "CSF". Este proceso automatizado no solo ahorra tiempo, sino que también garantiza la coherencia de los datos entre distintos módulos del sistema, evitando la duplicación de esfuerzos y mejorando la trazabilidad de la información. De esta forma, el aplicativo proporciona una base sólida y confiable para la evaluación de madurez de controles y la toma de decisiones en materia de seguridad y cumplimiento.

4.4. Análisis de requisitos

La fase inicial del desarrollo del proyecto, en consonancia con la metodología de cascada adoptada, consistió en un exhaustivo análisis y definición de los requisitos funcionales y no funcionales del aplicativo. Este proceso fue fundamental para establecer las bases sólidas sobre las cuales se construiría la solución, asegurando su alineación con las necesidades operativas y estratégicas de la Agencia Espacial Europea (ESA) en el ámbito de la auditoría de sistemas de navegación con Inteligencia Artificial.

La definición de estos requisitos se nutrió de una investigación previa detallada, incluyendo el estudio del contexto del sector espacial, el panorama de la ciberseguridad, los estándares de auditoría existentes en la ESA (como COBIT 2019 y el uso de CAATs), y un análisis en profundidad de los nuevos marcos a integrar: NIST AI RMF 1.0 y FAICP Framework. La colaboración directa con la ESA fue un pilar clave en esta etapa, permitiendo una comprensión precisa de los desafíos actuales y los resultados esperados.

Los requisitos identificados se clasificaron en dos categorías principales:

4.4.1. Requisitos Funcionales

Estos requisitos describen las funcionalidades específicas que el aplicativo debe ofrecer para cumplir con sus objetivos:

- **Mejora de la Herramienta CAAT Existente:** El aplicativo debe potenciar y actualizar la herramienta CAAT previamente utilizada por la ESA en el sector de navegación.
- **Integración del Marco NIST AI RMF 1.0:** Debe permitir la evaluación conforme a los principios y subcategorías del NIST AI RMF 1.0, identificando aquellas no cubiertas por el CSF y facilitando la evaluación de controles específicos.
- **Integración del Marco FAICP Framework:** Se requiere la incorporación del FAICP Framework, estableciendo un mapeo directo con los principios del CSF 1.1 para su evaluación.
- **Evaluación de Aspectos Críticos de la IA:** El aplicativo debe posibilitar una evaluación rigurosa de aspectos fundamentales de los sistemas de IA, tales como la ética, la rendición de cuentas, la interpretabilidad, la privacidad y la corrección.

- **Preservación de la Experiencia de Usuario:** La integración de los nuevos marcos debe realizarse manteniendo la familiaridad y el uso de hojas de cálculo para los auditores de la ESA.
- **Automatización de Cálculos:** El sistema debe automatizar los cálculos necesarios para obtener promedios, niveles de riesgo y la generación de gráficos.
- **Propagación Automática de Valores:** Se debe asegurar la correcta propagación de las puntuaciones introducidas por el auditor entre las diferentes hojas y secciones del aplicativo.
- **Cálculo de Nivel de Cumplimiento:** El aplicativo debe determinar el nivel de cumplimiento (ej. "Non Compliance", "Partially Compliance", "Compliance", "Fully Compliance") para valores individuales y áreas de política, basándose en umbrales predefinidos.
- **Cálculo de Riesgos:** Se requiere que la herramienta calcule los niveles de riesgo considerando criterios organizacionales y arquitectónicos.

4.4.2. Requisitos No Funcionales

Estos requisitos definen las cualidades o atributos que el aplicativo debe poseer:

- **Fiabilidad y Robustez:** El aplicativo debe ser fiable, coherente en su lógica interna y robusto en su funcionamiento.
- **Eficiencia Técnica:** La mejora debe traducirse en una mayor eficiencia en los procesos de auditoría asistida por computadora.
- **Adaptabilidad Normativa:** El aplicativo debe contribuir a la capacidad de la ESA para adaptarse a la evolución de las regulaciones relacionadas con la Inteligencia Artificial.
- **Objetividad y Trazabilidad:** Debe soportar la objetividad en la evaluación y asegurar la trazabilidad de los hallazgos de auditoría.
- **Minimización del Error Humano:** La automatización debe contribuir a la reducción de errores manuales.
- **Aceleración de la Respuesta:** La herramienta debe agilizar los procesos de análisis y respuesta ante posibles incidentes o riesgos identificados.
- **Mantenimiento de Funcionalidades Existentes:** Las funcionalidades previas de la herramienta CAAT (propagación, cálculos, macros, modelos de riesgo) deben conservarse y operar correctamente.

- **Facilidad de Detección y Resolución de Errores:** El diseño debe facilitar la identificación y corrección de errores en la lógica de cálculo y el manejo de datos.

4.5. Diseño y desarrollo

Esta sección detalla las decisiones de diseño clave y la implementación técnica llevada a cabo para integrar los marcos NIST AI RMF 1.0 y FAICP Framework en la herramienta CAAT existente de la ESA.

La implementación se centró en extender la funcionalidad de la herramienta existente, asegurando al mismo tiempo la **integración** y **mantenibilidad** del código. El desarrollo práctico se centro en el diseño e implementación de algoritmos para propagar las valoraciones obtenidas en la hoja de subcontroles hacia las nuevas secciones dedicadas AI RMF 1.0 y FAICP.

4.5.1. Asignación de Subcontroles

4.5.1.1. Introducción

En el contexto de la gestión de la ciberseguridad y los riesgos de la Inteligencia Artificial (IA) en la Agencia Espacial Europea (ESA), la capacidad de integrar y armonizar diversos marcos de control es de vital importancia. Dada la familiaridad y el uso extendido del NIST Cybersecurity Framework (CSF) 1.1 por parte de la ESA, se ha priorizado un enfoque que permita la reutilización de los subcontroles ya establecidos. Este objetivo no solo persigue una optimización de los recursos, sino que también facilita a los auditores la visualización y el análisis del cumplimiento frente a otros estándares emergentes, como el NIST AI Risk Management Framework (RMF) 1.0 y el FAICP Framework, a través de una base de control unificada y ya conocida. Esta estrategia busca una transición fluida y eficiente hacia la evaluación de riesgos específicos de la IA, aprovechando la infraestructura y el conocimiento existentes.

4.5.1.2. Estado actual

El punto de partida para la asignación de subcontroles se estableció considerando los mapeos existentes y la necesidad de nuevas correspondencias:

- **Mapeo de AI RMF a CSF:** El mapeo inicial del NIST AI Risk Management Framework (RMF) 1.0 con el NIST Cybersecurity Framework (CSF) 1.1 ya había sido realizado previamente por el Secure Controls Framework (SCF). Si bien esta correspondencia cubría una parte significativa del AI RMF, se identificó que ciertas subcategorías del AI RMF no estaban completamente mapeadas o no encontraban una cobertura adecuada dentro de los controles existentes del CSF. Esta situación requirió una revisión y una propuesta de extensión para asegurar una alineación exhaustiva.
- **Mapeo de FAICP:** A diferencia del NIST AI RMF, el FAICP Framework, una iniciativa de ENISA para prácticas de ciberseguridad en IA, no disponía de un mapeo previo con ningún estándar ya implementado en la herramienta de auditoría de la ESA. Por consiguiente, la asignación de sus subcontroles se abordó desde cero. Se estableció una correspondencia directa basada en los principios y categorías del CSF 1.1, con el fin de facilitar su integración en la herramienta y su comprensión por parte de los auditores, quienes ya operan bajo la lógica del CSF.

4.5.1.3. Propuesta de asignación

La propuesta de asignación de subcontroles se centró en extender la funcionalidad de la herramienta existente, asegurando la integración y mantenibilidad del sistema. El proceso se focalizó en la asignación de subcontroles ya existentes en la herramienta de la ESA a las nuevas secciones dedicadas al AI RMF 1.0 y FAICP, buscando aquellos subcontroles que fueran capaces de responder o trataran sobre el mismo contexto de la subcategoría o Cuestión del marco.

4.5.1.4. AI RMF

Para las subcategorías del NIST AI RMF 1.0 que no fueron mapeadas originalmente con el CSF, se llevó a cabo un proceso de identificación de estas brechas y la propuesta de controles específicos o ajustes en los mapeos existentes para asegurar una cobertura completa. La asignación se realizó seleccionando los subcontroles existentes que mejor se alineaban con el contexto y los objetivos de cada subcategoría del AI RMF.

Tabla 17: Asignación de subcontroles a cada subcategoría del AI RMF

Función	Subcategoría	Subcontroles
GOVERN	3.1	SC-ID16, SC-ID17
GOVERN	4.2	SC-ID18, SC-ID19
GOVERN	5.2	SC-ID20, SC-ID25
MAP	1.1	SC-ID4, SC-ID9
MAP	1.2	SC-ID13, SC-ID14
MAP	2.1	SC-ID9
MAP	2.2	SC-ID18
MAP	2.3	SC-ID11
MAP	3.1	SC-ID10
MAP	3.2	SC-ID18
MAP	3.3	SC-ID12
MAP	3.4	SC-ID16, SC-ID17
MAP	4.1	SC-ID21
MAP	4.2	SC-ID24
MEASURE	1.3	SC-ID26
MEASURE	4.2	SC-ID22
MANAGE	3.2	SC-ID19
MANAGE	4.1	SC-ID26

Función	Subcategoría	Subcontroles
MANAGE	4.2	SC-ID25

Fuente: Elaboración propia

4.5.1.5. FAICP

Para integrar el FAICP Framework, se desarrolló una asignación directa de subcontroles a cada "Cuestión" (Question) del marco. El enfoque adoptado para determinar el nivel de cumplimiento de cada cuestión se basa en el valor mínimo de todos los subcontroles asociados. Esta metodología del "peor escenario" se eligió para garantizar una evaluación de riesgos rigurosa, ya que un fallo en cualquier subcontrol relevante afectaría el cumplimiento general de la cuestión. La asignación se realizó identificando los subcontroles existentes que mejor se correspondían con el contexto de cada "Cuestión" del FAICP.

Tabla 18: Asignación de subcontroles a cada cuestión del FAICP

Policy Area	FAICP Question	Subcontroles
Human Capital	FAICP-Q-1	SC-ID16, SC-ID36
Human Capital	FAICP-Q-2	SC-ID16, SC-ID90
Human Capital	FAICP-Q-3	SC-ID11, SC-ID14
Human Capital	FAICP-Q-4	SC-ID36, SC-ID59, SC-ID90
Human Capital	FAICP-Q-5	SC-ID38
Human Capital	FAICP-Q-6	SC-ID27, SC-ID28, SC-ID52, SC-ID58, SC-ID82
From the lab to the market	FAICP-Q-7	SC-ID24, SC-ID90
From the lab to the market	FAICP-Q-8	SC-ID26

Policy Area	FAICP Question	Subcontroles
From the lab to the market	FAICP-Q-9	SC-ID47
From the lab to the market	FAICP-Q-10	SC-ID27, SC-ID70
From the lab to the market	FAICP-Q-11	SC-ID6, SC-ID11, SC-ID13
From the lab to the market	FAICP-Q-12	SC-ID27, SC-ID72, SC-ID78
From the lab to the market	FAICP-Q-13	SC-ID13, SC-ID38, SC-ID90
Networking	FAICP-Q-14	SC-ID21, SC-ID57
Networking	FAICP-Q-15	SC-ID16
Networking	FAICP-Q-16	SC-ID16
Networking	FAICP-Q-17	SC-ID16, SC-ID90
Networking	FAICP-Q-18	SC-ID16, SC-ID90
Networking	FAICP-Q-19	SC-ID73
Networking	FAICP-Q-20	SC-ID73, SC-ID74, SC-ID77
Networking	FAICP-Q-21	SC-ID21, SC-ID24, SC-ID25
Networking	FAICP-Q-22	SC-ID13

Policy Area	FAICP Question	Subcontroles
Infrastructure	FAICP-Q-23	SC-ID8, SC-ID14, SC-ID23
Infrastructure	FAICP-Q-24	SC-ID70
Regulation	FAICP-Q-25	SC-ID46, SC-ID48
Regulation	FAICP-Q-26	SC-ID13, SC-ID53
Regulation	FAICP-Q-27	SC-ID19, SC-ID23, SC-ID25
Regulation	FAICP-Q-28	SC-ID22, SC-ID23, SC-ID50
Regulation	FAICP-Q-29	SC-ID13, SC-ID53
Regulation	FAICP-Q-30	SC-ID11, SC-ID13, SC-ID26

Fuente: Elaboración propia

4.5.2. Hoja AI RMF

Para permitir la evaluación conforme al marco NIST AI RMF 1.0 dentro del aplicativo CAAT, se diseñaron e implementaron hojas de cálculo específicas que recogen y procesan los datos de evaluación. La valoración bajo este marco requiere el cálculo de diversos indicadores clave, como el promedio ponderado de los valores de las subcategorías, el promedio de los valores por cada categoría y el promedio de los valores por cada función del marco.

La lógica computacional para obtener estos promedios y valores ponderados se implementó utilizando Visual Basic for Applications (VBA). Esta elección se justificó por la necesidad de manejar la complejidad de los cálculos de manera estructurada y asegurar la compatibilidad del aplicativo con diferentes configuraciones de idioma del usuario en Microsoft Excel. Al evitar el uso directo de fórmulas nativas de Excel (cuyos nombres varían según el idioma), se garantiza que la herramienta funcione correctamente independientemente de la configuración regional del equipo donde se ejecute, facilitando su mantenibilidad futura.

4.5.2.1. Cálculo del promedio ponderado de subcontroles

La función **CalculateSubcontrolsWeightedAverage** fue implementada con el propósito de calcular el promedio ponderado de un conjunto específico de valores de subcontroles. Este conjunto se define mediante una lista de identificadores (IDs) de subcontroles proporcionada como entrada. La función considera tanto el valor evaluado para cada subcontrol como un peso asociado.

La función recibe como argumentos:

- Una cadena de texto (**idList**) que contiene los IDs de los subcontroles a incluir en el cálculo, separados por un delimitador (por defecto, la coma ,). Esta cadena puede estar vacía o contener "N/A".
- Un rango de celdas (**idRangeSC**) que especifica la columna donde se encuentran todos los IDs de subcontroles disponibles para búsqueda.
- Un rango de celdas (**weightRangeSC**) que indica la columna donde se ubican los pesos asociados a los subcontroles listados en **idRangeSC**. Se asume que este rango tiene la misma estructura de filas.
- Un rango de celdas (**valueRangeSC**) que especifica la columna donde se encuentran los valores evaluados para los subcontroles listados en **idRangeSC**. Se asume que este rango también tiene la misma estructura de filas.

El funcionamiento interno de la función implica:

1. Inicializar variables para acumular la suma ponderada de los valores y la suma de los pesos.

2. Validar la cadena **idList**: si está vacía o es "N/A", la función devuelve 0, indicando que no hay subcontroles a promediar.
3. Dividir la cadena **idList** en un array de IDs individuales, manejando posibles espacios en blanco.
4. Iterar sobre cada ID del array:
    - Buscar el ID actual en el rango **idRangeSC**. La búsqueda no distingue entre mayúsculas y minúsculas.
    - Si el ID es encontrado, recuperar el peso correspondiente del rango **weightRangeSC** y el valor evaluado del rango **valueRangeSC** utilizando la misma fila donde se encontró el ID. Se incluye manejo de errores para asegurar que los valores recuperados sean numéricos.
    - Si el peso y el valor son numéricos válidos, se añade el producto **valor** * **peso** a la suma ponderada y el peso a la suma total de pesos.
5. Una vez procesados todos los IDs, si la suma total de pesos es mayor que cero, se calcula el promedio ponderado dividiendo la suma ponderada por la suma de pesos. Si la **suma** de **pesos** es **cero** (ya sea porque no se encontraron IDs válidos, los pesos eran cero, o no eran numéricos), la **función** devuelve **0**.

4.5.2.2. Promedio de valores según la categoría y función

La función **CalculateAverage** se utiliza para determinar el promedio aritmético de un conjunto de valores contenidos en un rango de celdas. Su aplicación principal dentro del contexto del NIST AI RMF es obtener promedios de valores de subcategorías a nivel de categoría y función.

La función recibe un único argumento:

- Un rango de celdas (**valueRange** de tipo Range) que se espera contenga los valores numéricos de los que se desea calcular el promedio.

La función devuelve un valor de tipo Variant, que será el promedio calculado como un número de doble precisión (Double) o 0 si el rango no contiene valores numéricos válidos para promediar.

El proceso interno de la función es el siguiente:

1. Inicializa contadores para la suma total de los valores numéricos encontrados (**sum**) y el número de elementos numéricos válidos (**elements**) a cero.
2. Itera a través de cada celda dentro del **valueRange** proporcionado.
3. Para cada celda, verifica si no está vacía y si contiene un valor que puede ser interpretado como numérico.
4. Si la celda cumple ambas condiciones (no vacía y numérica), su valor se convierte a tipo Double, se añade a la **sum** acumulada, y se incrementa el contador **elements**. Las celdas vacías o no numéricas son simplemente ignoradas en el cálculo.
5. Una vez que ha recorrido todas las celdas del rango, si la **sum** total de los valores numéricos es **diferente de cero**, calcula el **promedio** dividiendo la **sum** entre el **número** de elements válidos encontrados.
6. **Si** la **sum es cero** (lo que ocurre si no se encontraron elementos numéricos válidos, o si todos los valores válidos sumaron cero), la **función devuelve 0**.

4.5.3. Hoja FAICP

Para integrar el FAICP Framework, diseñado para asistir al auditor en la evaluación de riesgos de ciberseguridad en sistemas de inteligencia artificial, se desarrollaron las hojas **FAICP Q&A** y **FAICP Q&A - G**. La hoja **FAICP Q&A** constituye la base de la evaluación. Para cada "cuestión" (question) definida en el marco, se calcula un valor que representa su nivel de cumplimiento. Este valor se determina tomando el valor mínimo de todos los subcontroles asociados a dicha cuestión. Esta aproximación, centrada en el valor mínimo, permite evaluar el peor escenario posible dentro del conjunto de subcontroles relevantes para cada cuestión, lo cual es crucial para una evaluación de riesgos rigurosa. Posteriormente, estos valores mínimos por cuestión se utilizan para calcular una valoración agregada para cada "área de políticas" del framework, aplicando nuevamente el criterio del valor mínimo encontrado entre las cuestiones pertenecientes a esa área.

La hoja **FAICP Q&A - G** complementa la anterior, proporcionando una visualización gráfica de los resultados de la evaluación. A semejanza de la hoja **AIRM-G** para el NIST AI RMF, esta hoja presenta de manera clara y concisa los niveles de cumplimiento tanto a nivel de área de

políticas como para cada política individual, facilitando al auditor la interpretación rápida de la evaluación.

4.5.3.1. **Cálculo del valor mínimo de subcontroles**

La función **FindMinimumValueFromSubcontrols** tiene como objetivo identificar el valor numérico mínimo entre un conjunto de subcontroles especificados. Este cálculo es fundamental para FAICP, que se basa en el peor caso (valor mínimo) asociado a una cuestión o área de política.

La función acepta los siguientes argumentos:

- Una cadena de texto (**idList**) con los IDs de los subcontroles a considerar, separados por comas. Puede ser una cadena vacía o "N/A".
- Un rango de celdas (**idRangeSC**) que contiene todos los IDs de subcontroles disponibles para la búsqueda.
- Un rango de celdas (**valueRangeSC**) que contiene los valores evaluados correspondientes a los subcontroles listados en **idRangeSC**.

La lógica implementada opera de la siguiente manera:

1. Inicializa el valor mínimo encontrado a "N/A" y una bandera para controlar si ya se ha encontrado un valor numérico válido.
2. Verifica si la lista **idList** está vacía o es "N/A"; si es así, devuelve "N/A".
3. Divide idList en IDs individuales, ignorando espacios.
4. Itera sobre cada ID:
    - Busca el ID en el rango **idRangeSC**.
    - Si se encuentra el ID, intenta recuperar el valor correspondiente del rango **valueRangeSC**. Se manejan errores para procesar solo valores numéricos.
    - Si el valor recuperado es numérico:
        - Si es el primer valor numérico válido encontrado, se establece como el mínimo inicial.

- Si ya se han encontrado valores, se compara con el mínimo actual y se actualiza si es menor.

5. Al finalizar la iteración, la función devuelve el **valor mínimo registrado** (que será "**N/A**" si no se encontró **ningún valor numérico válido**).

4.5.3.2. Cálculo nivel de cumplimiento

La función **CalculateComplianceLevel** se encarga de traducir un valor numérico cuantitativo en una etiqueta cualitativa que representa un nivel de cumplimiento. Esta función es utilizada para clasificar los resultados numéricos obtenidos de las evaluaciones de los subcontroles, cuestiones o áreas de política según umbrales predefinidos.

La función recibe un único argumento:

- Un valor (**value** de tipo Variant), que puede ser una celda o una variable conteniendo el valor numérico a clasificar.

La función devuelve una cadena de texto (String) indicando el nivel de cumplimiento. Los posibles resultados son: **"Not Applicable"**, **"Non Compliance"**, **"Partially Compliance"**, **"Compliance"**, o **"Fully Compliance".**

Su funcionamiento es directo:

1. Primero, valida si el valor de entrada está vacío o no es numérico. Si es así, devuelve inmediatamente **"Not Applicable".**
2. Si el valor es numérico, lo convierte a tipo Double.
3. Compara el valor numérico con una serie de umbrales:
    - **Menor que 0.4:** "Non Compliance"
    - **Menor que 0.6 (pero 0.4 o mayor):** "Partially Compliance"
    - **Menor que 0.8 (pero 0.6 o mayor):** "Compliance"
    - **0.8 o mayor:** "Fully Compliance"
4. Devuelve la cadena de texto correspondiente al primer umbral que cumple el valor.

4.5.3.3. Cálculo agrupación de compliance por área

La función **CalculateComplianceLevelPolicyArea** está diseñada específicamente para determinar el nivel de cumplimiento textual para un conjunto de valores que representan una área de política dentro del framework FAICP. Su propósito es evaluar un rango de celdas (correspondientes a las cuestiones dentro de un área) y derivar un único indicador cualitativo para el área completa.

La función recibe un único argumento:

- Un rango de celdas (**valueRange** de tipo Range) que contiene los valores numéricos (típicamente, los valores mínimos calculados para cada cuestión) a evaluar dentro de esa área.

Devuelve una cadena de texto con el nivel de cumplimiento del área, utilizando las mismas categorías que **CalculateComplianceLevel**.

Su lógica interna es la siguiente:

1. Itera sobre cada celda dentro del **valueRange** proporcionado.
2. Para que el cálculo del área sea válido, *todas* las celdas dentro del rango deben contener valores numéricos válidos. Si encuentra alguna celda vacía o no numérica durante la iteración, la función devuelve inmediatamente **"Not Applicable"** para toda el área.
3. Si todas las celdas son numéricas, la función procede a encontrar el ***valor mínimo*** dentro de este rango de celdas.
4. Una vez identificado el valor mínimo del rango, la función llama a **CalculateComplianceLevel**, pasándole este valor mínimo.
5. El resultado (la cadena de texto con el nivel de cumplimiento) devuelto por **CalculateComplianceLevel** es el valor de retorno final de **CalculateComplianceLevelPolicyArea**. Esto significa que el nivel de cumplimiento de un área de política se determina por el peor valor (el mínimo) encontrado entre todas las cuestiones que la componen.

4.5.4. Uso del aplicativo

El comportamiento del aplicativo está guiado por tres principios: automatización, modularidad y visualización clara. El flujo de funcionalidad de la herramienta consta de los siguientes pasos:

1. Entrada de datos del auditor:

En la hoja SC, el auditor introduce una puntuación numérica para cada subcontrol (por ejemplo, SC-ID1, SC-PR3, etc.). Los valores siguen una escala estándar de madurez:

- 0 = No implementado
- 0.2 = Alguna evidencia inicial
- 0.4 = Implementado
- 0.6 = Formalizado/documentado
- 0.8 = Supervisado/mejorado
- 1 = Optimizado

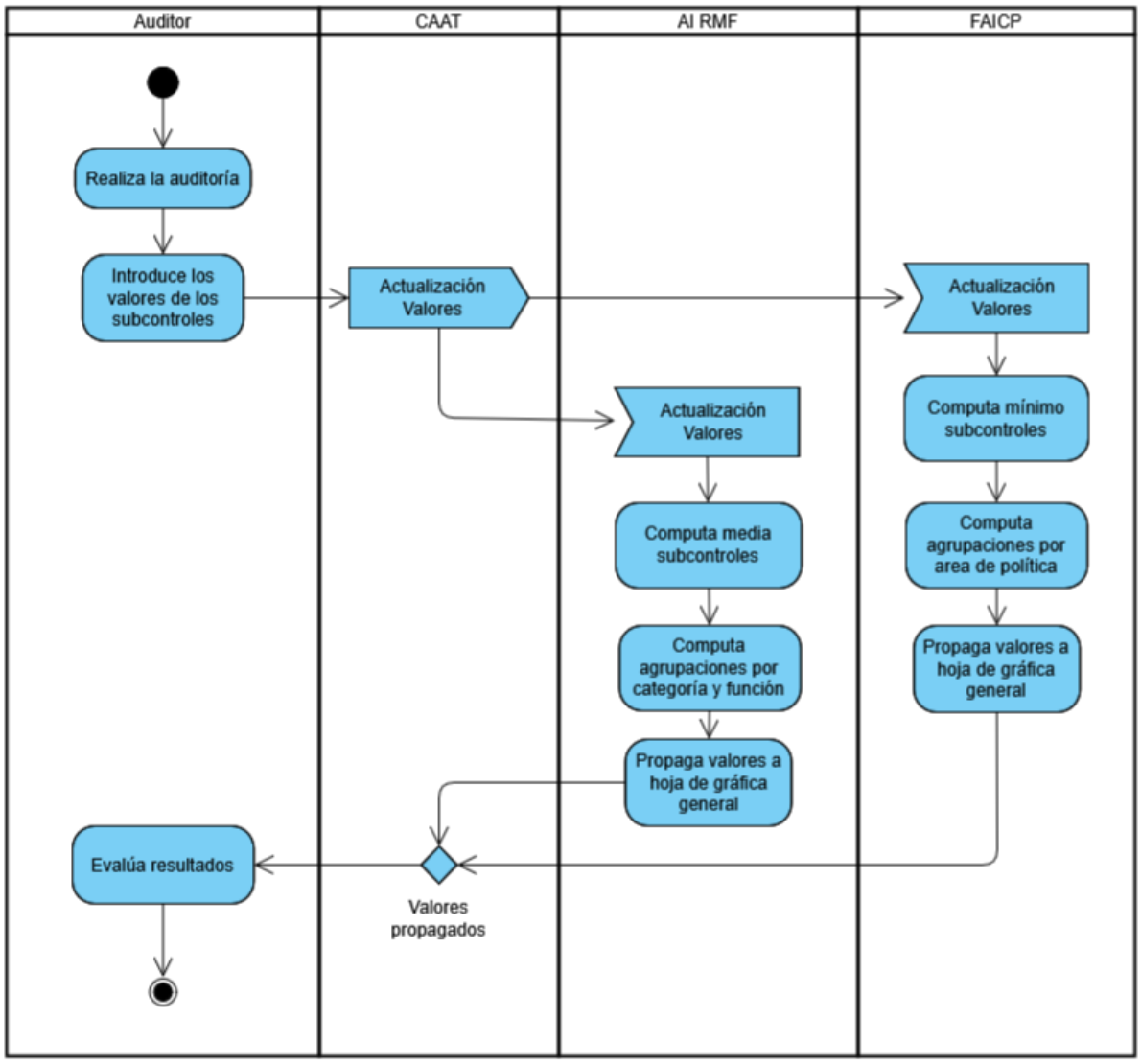
2. **Propagación automática a los estándares:**
   Mediante fórmulas (algunas desarrolladas a través de Visual Basic for Applications), cada puntuación se propaga a hojas como CSF, AIRM o FAICP, en función del mapeo establecido entre subcontroles y estándares. En el caso de los estándares AIRM y FAICP — representados en las hojas "AIRM", "AIRM-G" y "FAICP Q&A"— el mapeo se ha realizado manualmente, identificando similitudes en sus objetivos y realizando una posterior validación para garantizar la consistencia con los subcontroles.
3. **Resumen por funciones y dominios:**
   En cada hoja de estándar, los controles están agrupados por familias o funciones, y se calcula la media o el mínimo de sus puntuaciones, lo que permite determinar niveles de cumplimiento por áreas.
4. **Visualización gráfica:**
   Hojas como AIRM-G presentan estos resultados con gráficas tipo semáforo, lo cual permite identificar de forma inmediata qué funciones presentan mayores riesgos o madurez insuficiente. De manera similar, la hoja FAICP Q&A - G incluye representaciones gráficas

tipo semáforo organizadas por áreas de política, facilitando la evaluación visual del cumplimiento y riesgo asociado en cada bloque temático.

5. **Simulación y análisis de impacto:**

La hoja SIMULATE contiene una batería de escenarios que pueden copiarse y pegarse en el Excel para verificar cómo se comportan los mapeos y las fórmulas asociadas. Aunque es posible modificar manualmente ciertos valores o estados (como deshabilitar un control o ajustar su nivel de madurez), su principal utilidad es servir como banco de pruebas para validar el correcto funcionamiento del sistema de puntuación y propagación automática.

Figura 6. Flujo del aplicativo desarrollado



Fuente: Elaboración propia

4.6. Verificación Interna

Con el objetivo de garantizar la fiabilidad, coherencia lógica y robustez funcional de la herramienta, se diseñó y ejecutó una fase de verificación interna intensiva. Esta fase se centró en validar el comportamiento de la herramienta ante diversos escenarios de uso y asegurar que la lógica de propagación, los cálculos automáticos, las macros y los modelos de riesgo funcionaran conforme a los requisitos definidos.

4.6.1. Objetivos

La verificación interna perseguía tres metas fundamentales:

- Comprobación de la correcta propagación de valores entre hojas (por ejemplo, desde SC a CSF, AI RMF 1.0 y FAICP).
- Validación del funcionamiento de las fórmulas que automatizan los cálculos de medias, riesgo y gráficas.
- Detección y resolución de errores en la lógica de redondeo, casos límite y formato de datos.

4.6.2. Metodología

Para llevar a cabo esta validación se estableció un banco de pruebas compuesto por múltiples auditorías simuladas, organizadas en conjuntos de datos representativos. Cada conjunto se aplicó de forma aislada, permitiendo un análisis detallado de su impacto en cada sección de la herramienta.

El proceso de prueba contempló:

- Hacer uso de conjuntos de pruebas con distintas valoraciones y situaciones.
- Evaluación de las valoraciones de cada conjunto para determinar el estado general.
- Evaluación de las valoraciones de forma individual para comprender su nivel de cumplimiento.
- Observación de la propagación automática de puntuaciones a los estándares CSF, AI RMF 1.0 y FAICP.
- Para cada estándar que hemos tratado, verificaremos las siguientes operaciones por cada hoja:
    - **AI RMF 1.0:**

        - **Hoja base:** Se verificó que los valores para cada subcategoría se hayan calculado correctamente realizando la media ponderada de los distintos subcontroles.
        - **Hoja G:** Se verificó que a nivel de función se haya calculado correctamente la media agrupada de cada categoría, que a su vez proviene de la media de sus subcategorías.
    - **FAICP:**
        - **Hoja base:** Se verificó que los valores para cada pregunta se hayan calculado correctamente realizando el mínimo de los distintos subcontroles asignados.
        - **Hoja G:** Se verificó que a nivel general, las áreas de política muestren correctamente el valor mínimo entre todas las cuestiones asociadas, y a su vez que cada cuestión presentada mantenga su mismo valor que la anterior hoja.

4.6.3. Conjuntos de Prueba

Se definieron cinco conjuntos de datos de entrada para cubrir los principales escenarios de auditoría:

- **PI-1 Auditoría 3 (AUDIT_3) – Evaluación Intermedia Estable:** Seleccionada por tener valores predominantes en el rango medio (0.60-0.80), representando una auditoría moderadamente madura sin extremos. Simula entornos con madurez media donde se esperan oportunidades de mejora pero sin vulnerabilidades críticas.
- **PI-2: Auditoría 8 (AUDIT_8) – Evaluación de Riesgo Crítico:** Elegida porque muchos subcontroles tienen valores bajos (0.20–0.40), evidenciando posibles brechas significativas de seguridad. Se usa como pruebas de respuesta a riesgo elevado, activación de alertas, y validación de tolerancia a fallos críticos.
- **PI-3: Auditoría 4 (AUDIT_4) – Evaluación Óptima:** Muestra un número notable de valoraciones de 1.00, representando un entorno robusto y en cumplimiento avanzado. Simula sistemas bien gestionados, con cumplimiento normativo y mínimos riesgos operativo.

- **PI-4: Auditoría 1 (AUDIT_1) – Mixto Realista:** Contiene una distribución heterogénea con valores desde 0.20 hasta 1.00. Refleja un estado típico de implementación parcial. Representa casos de prueba estándar, ideal para escenarios realistas de evaluación organizacional.
- **PI-5: Auditoría 6 (AUDIT_6) – Casos con Variabilidad Alta:** Seleccionada por mostrar alta dispersión en los valores (de 0.40 a 1.00), útil para validar mecanismos de normalización y análisis de desviaciones. Sirve para evaluar la capacidad del sistema de auditar entornos dispares y detectar desviaciones inusuales.
- **PI-6: Auditoría 9 (AUDIT_9):** Esta auditoría refleja un desempeño predominantemente intermedio, con una mayoría de valoraciones alrededor de 0.40 y 0.60, lo que sugiere procesos parcialmente establecidos y cierta adherencia a los estándares. Sin embargo, se identifican múltiples áreas críticas (valores de 0.20 o inferiores), señalando debilidades puntuales que podrían representar riesgos operativos o de cumplimiento si no se abordan.

4.6.4. Resultados

Los resultados obtenidos en esta fase permitieron validar y ajustar distintos aspectos clave:

- **Propagación lógica:** Se verificó que las equivalencias entre estándares se procesaban correctamente mediante una combinación de fórmulas Excel y scripts en VBA.
- **Redondeo y precisión:** Se hizo uso del formato de valores de Excel para ajustar los valores calculados en esas celdas a con una precisión de 2 dígitos.
- **Diagramas y resúmenes:** Las hojas gráficas (por ejemplo, FAICP Q&A, AIRM-G) reflejaron con precisión los cambios en las medias, y los valores coincidieron con los esperados en cada prueba.

4.6.5. Conclusiones

La fase de verificación interna confirmó que la herramienta cumple satisfactoriamente con los objetivos de cálculo, propagación y representación gráfica esperados. El sistema responde de forma coherente ante una amplia variedad de escenarios y ofrece al auditor una herramienta sólida y flexible para el análisis de cumplimiento de marcos de control como CSF, AI RMF 1.0 y FAICP.

4.7. Validación Externa

Con el objetivo de asegurar que la herramienta desarrollada cumple con los requisitos esperados en un entorno real, se llevó a cabo un proceso de validación externa. Este proceso fue ejecutado por profesionales ajenos al desarrollo, pertenecientes a la ESA, representando el uso previsto de la herramienta en condiciones operativas.

4.7.1. Objetivo

El principal objetivo de esta validación fue contar con una evaluación objetiva e independiente por parte de personas o entidades externas al equipo de trabajo, con experiencia en el dominio del proyecto (navegación, ciberseguridad, auditoría, IA, etc.). La intención era determinar si la herramienta desarrollada satisface los requerimientos planteados inicialmente y si está en condiciones de ser utilizada de forma práctica en entornos reales, además de proporcionar retroalimentación sobre la propuesta de asignación de subcontroles.

4.7.2. Perfil de los Validadores

Para este proceso, se contó con la colaboración de profesionales pertenecientes a la ESA. Los validadores seleccionados cumplieron con los siguientes criterios:

- No estuvieron involucrados en el desarrollo del proyecto.
- Poseen conocimientos técnicos relacionados con la temática del TFM, incluyendo experiencia en auditorías centradas en el uso de Inteligencia Artificial.
- Están familiarizados con herramientas similares o el entorno operativo al que se orienta el proyecto.

4.7.3. Procedimiento de Validación

La validación externa se desarrolló mediante el siguiente procedimiento estructurado:

1. **Entrega de la herramienta:** Se facilitó una copia funcional de la herramienta junto con un manual de usuario y casos de prueba representativos.

2. **Ejercicio de pruebas:** Los validadores ejecutaron pruebas sobre la herramienta, utilizando tanto datos de ejemplo como escenarios definidos en el Excel del proyecto.
3. **Revisión de resultados:** Se analizaron los resultados obtenidos, prestando especial atención a la precisión de los cálculos, la facilidad de uso y la utilidad de los informes generados.
4. **Recogida de feedback:** Se habilitó un formulario de evaluación y se realizaron entrevistas estructuradas para recopilar observaciones, sugerencias de mejora y posibles incidencias.

4.7.4. Resultados Obtenidos

Los resultados de esta validación permitieron confirmar los siguientes puntos:

- **Funcionamiento correcto:** La herramienta respondió correctamente ante los escenarios definidos, cumpliendo los objetivos técnicos planteados.
- **Interfaz comprensible:** La mayoría de los validadores consideraron que la interfaz era clara, aunque algunos propusieron pequeñas mejoras en términos de usabilidad y visualización.
- **Relevancia práctica:** La funcionalidad desarrollada fue valorada como útil y aplicable, especialmente en contextos de auditoría y análisis de riesgos relacionados con navegación y ciberseguridad.
- **Verificación de la asignación de subcontroles:** Se ha verificado que los subcontroles asignados en AI RMF 1.0 y FAICP proporcionan una valoración acorde a los resultados con otros estándares o experiencia práctica.

4.7.5. Conclusiones de la Validación Externa

La validación externa aportó un valor significativo al proyecto, al proporcionar una mirada crítica y fundamentada sobre el producto final. Gracias a esta evaluación, se pudo:

- Corroborar la solidez de la solución técnica desarrollada.
- Detectar aspectos de mejora que no habían sido identificados internamente.
- Aumentar la fiabilidad de la herramienta al aplicarla en entornos reales.

En resumen, la verificación y validación externa reforzaron la confianza en la utilidad y aplicabilidad del proyecto, permitiendo cerrar el ciclo de desarrollo con una herramienta contrastada y alineada con las necesidades reales del usuario final.

5. Conclusiones y Trabajo Futuro

5.1. Conclusiones

Este Trabajo de Fin de Máster se ha centrado en abordar una necesidad crítica y contemporánea en el ámbito de la ciberseguridad y la gobernanza tecnológica: la adaptación de los procesos de auditoría a la creciente integración de la Inteligencia Artificial en sistemas de alta criticidad. El problema tratado fue la necesidad de actualizar las herramientas de auditoría existentes en la Agencia Espacial Europea (ESA) para evaluar adecuadamente los riesgos y el cumplimiento de sistemas de IA, particularmente en el estratégico sector de la navegación.

El objetivo general, por tanto, fue la mejora sustancial de una herramienta CAAT (Computer-Assisted Audit Tool) para incorporar de manera funcional y coherente los marcos de referencia NIST AI RMF 1.0 y FAICP Framework. La solución desarrollada ha demostrado ser no solo válida desde un punto de vista técnico, sino también relevante y aplicable en el contexto operativo de la ESA, logrando con éxito la integración de estos estándares y proporcionando una capacidad de evaluación más completa y matizada.

La consecución de este objetivo principal se ha articulado a través de una serie de objetivos específicos que han sido resueltos de manera sistemática a lo largo del proyecto. En primer lugar, se realizó un estudio exhaustivo del contexto del sector espacial y de la ciberseguridad, lo cual fue un pilar fundamental para dimensionar la importancia del proyecto. Este análisis no se limitó a una revisión superficial, sino que profundizó en la criticidad de los sistemas PNT como GALILEO, estableciendo el marco de alto riesgo en el que operaría la herramienta y justificando la necesidad de un enfoque de auditoría riguroso.

Posteriormente, el proyecto se adentró en un análisis detallado de los estándares existentes y de los que se iban a integrar. Este paso fue crucial, ya que el entendimiento de la estructura del NIST CSF 1.1 y su interrelación con los nuevos marcos de IA permitió formular la hipótesis central del trabajo: la viabilidad de reutilizar una base de controles de ciberseguridad para evaluar la gobernanza de la IA.

Con esta base conceptual sólida, se procedió al desarrollo del sistema de información, extendiendo la herramienta CAAT existente con nuevas hojas de cálculo, lógica de negocio

implementada en VBA y modelos de cálculo automatizados. Un aspecto clave de esta fase fue el compromiso de preservar la experiencia de usuario, garantizando que la integración de nuevas funcionalidades no supusiera una barrera para la adopción por parte de los auditores de la ESA.

Finalmente, el ciclo de desarrollo culminó con una fase de pruebas y validación exhaustiva. La verificación interna, mediante un banco de auditorías simuladas, permitió depurar la lógica de propagación y la precisión de los cálculos, mientras que la validación externa, llevada a cabo por profesionales de la ESA ajenos al proyecto, corroboró de forma independiente la relevancia práctica, la usabilidad y la solidez de la solución propuesta.

Una de las contribuciones más significativas y originales de este trabajo ha sido la demostración práctica y la implementación de una estrategia de mapeo eficiente para integrar marcos de IA complejos. Lejos de ser un mero ejercicio técnico, este proceso constituyó el núcleo metodológico del proyecto.

Para el NIST AI RMF 1.0, se partió de una correspondencia existente que fue analizada críticamente, identificando brechas de cobertura que fueron subsanadas mediante una extensión y refinamiento del mapeo.

Para el FAICP Framework, el desafío fue mayor, ya que no existía ningún mapeo previo. En este caso, la contribución fue el diseño desde cero de una correspondencia directa y lógica con los principios y subcontroles del NIST CSF.

La validación de estos mapeos confirma que es posible evaluar de manera efectiva la gobernanza de la IA a través de controles de ciberseguridad bien definidos, creando un puente crucial entre dos dominios que hasta ahora se trataban de forma aislada. Esta estrategia no solo optimiza el proceso de auditoría al evitar la duplicación de controles, sino que enriquece el análisis al ofrecer una visión holística e integrada de los riesgos tecnológicos.

Como resultado, la herramienta final trasciende su función de simple evaluador de cumplimiento para convertirse en un verdadero instrumento de gestión estratégica. Permite a la ESA realizar un análisis más profundo y riguroso de aspectos intrínsecos a la IA, como la ética, la interpretabilidad, la rendición de cuentas y la equidad, traduciendo estos conceptos abstractos en métricas auditables. La automatización de los cálculos y la clara visualización de

los resultados a través de mapas de calor y paneles gráficos no solo agilizan el trabajo del auditor, sino que facilitan la comunicación de los hallazgos a diferentes niveles de la organización, permitiendo priorizar recursos y esfuerzos de mitigación de manera más efectiva.

En resumen, este proyecto ha respondido con éxito al problema planteado, entregando una solución tangible, validada y alineada con las necesidades de la ESA, que representa una contribución valiosa y práctica a la disciplina de la auditoría de sistemas inteligentes en entornos de alta criticidad.

5.2. Líneas de Trabajo Futuro

Al realizar este proyecto, surgen un abanico de posibilidades para extender el trabajo realizado en este nicho de la auditoría a los sistemas de Inteligencia Artificial. Estas líneas de trabajo futuro no solo representan mejoras incrementales, sino que abordan puntos críticos fundamentales del proceso de auditoría en entornos críticos, asegurando que la herramienta evolucione en paralelo a los desafíos tecnológicos y regulatorios.

5.2.1. Adaptación a regulaciones emergentes

Un primer aspecto sería la ampliación de la herramienta para adaptarse al análisis de las regulaciones emergentes sobre los sistemas de Inteligencia Artificial, como la Ley de IA de la Unión Europea.

La realización de esta opción implica la identificación de las obligaciones concretas que la regulación impone a los sistemas de alto riesgo, como los utilizados en infraestructuras críticas como PNT.

Posteriormente, se analizaría requisito por requisito, creando una nueva capa de mapeo que vincule los artículos legales con los subcontroles técnicos ya existentes en el framework NIST CSF. Este proceso permitiría evaluar el nivel de cumplimiento normativo, como una consecuencia directa de la madurez de los controles técnicos implementados.

Finalmente, la herramienta podría ofrecer una hoja para mostrar en un informe ejecutivo la valoración obtenida, comparándola con los resultados de los marcos de gestión de riesgos como AI RMF y FAICP. Esto permitiría a la ESA visualizar de forma clara si las áreas de riesgo técnico identificadas por NIST se corresponden con las áreas de mayor riesgo legal,

proporcionando una visión integral y unificada que es crucial para la toma de decisiones estratégicas y la demostración de la debida diligencia ante las autoridades.

5.2.2. Análisis precisión valoraciones según subcontroles del NIST CSF y su extensión

Siguiendo este aspecto, otro punto interesante a considerar sería el análisis para validar la efectividad del framework NIST CSF como base para valorar los estándares de IA tratados de una forma más precisa. La asignación actual de subcontroles es una hipótesis de trabajo fundamentada, pero requiere una validación empírica para confirmar su precisión en el mundo real.

Para la realización de esta extensión, se obtendrían datos de auditorías reales, donde los resultados de cumplimiento de AI RMF y FAICP fuesen conocidos o evaluados por un equipo independiente. Estos resultados objetivo se compararían con los generados por la herramienta utilizando únicamente los subcontroles del CSF. Analizar esa diferencia permitiría identificar patrones de divergencia, es decir, aquellos puntos en los que el modelo de la herramienta sobrestima o subestima sistemáticamente el riesgo.

A partir de este diagnóstico, se podría proponer una versión calibrada de la herramienta, ya sea mediante la sugerencia de nuevos subcontroles más granulares para la ESA o, de forma más sutil y potente, ajustando la ponderación de los subcontroles existentes para reflejar con mayor exactitud su impacto real en la gobernanza de la IA, transformando la herramienta de un modelo de "mejor esfuerzo" a uno validado y calibrado.

5.2.3. Evaluación de subcontroles basados en simulación de ataques adversarios

Como se puede notar, este proyecto trata principalmente la evaluación de subcontroles defensivos. Sin embargo, uno de los mayores riesgos en PNT son los ataques deliberados y sofisticados, aprovechando superficies de ataque de IA que pueden pasar desapercibidas por los sistemas de monitorización clásicos. Por ello, es importante poder auditar la resiliencia contra estos ataques, proponiendo el diseño e integración de un framework de simulación de ataques adversarios ("Red Teaming") específico para la IA en sistemas PNT.

Esta extensión comenzaría con una investigación y modelado de ataques relevantes, como el "data poisoning" que manipule los datos de corrección ionosférica en satélites.

Posteriormente, se desarrollaría un conjunto de herramientas para generar estas señales o datos adversarios e inyectarlos en el sistema bajo prueba.

El resultado de estas simulaciones sería una cuantificación de la degradación del rendimiento que se integraría directamente en la herramienta de auditoría. Esto transformaría la evaluación de la seguridad, pasando de una revisión subjetiva de la documentación a una validación objetiva y basada en evidencia, respondiendo a la pregunta fundamental de si los controles implementados son realmente efectivos frente a amenazas activas, aunque pueda no llegar a cubrir todos los posibles ataques existentes.

5.2.4. Adaptación a estándares emergentes de ciberseguridad en IA

Como última sugerencia, y quizás la más fundamental para la sostenibilidad de la herramienta, se propone su adaptación continua al dinámico y especializado panorama de la ciberseguridad en Inteligencia Artificial. El campo de la IA presenta desafíos de seguridad únicos, que han impulsado la creación de marcos de control específicos, haciendo necesario que la herramienta evolucione para mantener su relevancia y precisión.

La realización de esta extensión comenzaría con una investigación y análisis exhaustivo de los nuevos marcos emergentes, como el futuro estándar ISO/IEC 27090 para la seguridad en IA. Posteriormente, se llevaría a cabo un mapeo detallado, creando una nueva capa de correspondencia que vincule los controles y salvaguardas específicas para IA de estos nuevos estándares con la estructura de evaluación de la herramienta.

El principal beneficio de esta integración sería transformar la herramienta de un marco de evaluación generalista a uno especializado y alineado con las mejores prácticas de vanguardia en seguridad de IA. Esto permitiría a la organización obtener una evaluación mucho más precisa de su postura frente a riesgos intrínsecos de estas tecnologías. Además, al consolidar múltiples estándares en una única plataforma, se eliminaría la ineficiencia de realizar auditorías fragmentadas, proporcionando una visión holística y sostenible que se adapta a la rápida evolución del sector.

REFERENCIAS BIBLIOGRÁFICAS

Blokdyk, G. (2020). *Cybersecurity Risk Management A Complete Guide—2021 Edition*. Emereo Publishing.

Bueermann, G., & Rohrs, M. (2024). Global Cybersecurity Outlook 2024. *World Economic Forum*. https://www.weforum.org/publications/global-cybersecurity-outlook-2024/

Buzzi, A. E. (2023). *Walter A. Shewhart: El padre del control estadístico de la calidad*.

Cavaciuti-Wishart, E., Heading, S., Kohler, K., & Zahidi, S. (2024). *Global Risks Report 2024* (Global Risks Report 2024). World Economic Forum. https://www.weforum.org/publications/global-risks-report-2024/in-full/

Check Point. (2022, abril 5). From SolarWinds to Log4j: The global impact of today's cybersecurity vulnerabilities. *Check Point Blog*. https://blog.checkpoint.com/security/from-solarwinds-to-log4j-the-global-impact-of-todays-cybersecurity-vulnerabilities/

Coz Fernández, J. R. (2021). Auditing IT Governance in the Navigation Sector. *Auditing IT Governance in the Navigation Sector*. https://www.isaca.org/resources/news-and-trends/industry-news/2021/auditing-it-governance-in-the-navigation-sector

Coz Fernández, J. R., & Valiño Castro, A. (2021). El impacto industrial y económico de los programas espaciales en Europa tras el covid-19: Sus implicaciones en la política industrial. *Economía industrial*, *420*, 67-80.

Coz Fernández, J. R., & Valiño Castro, A. (2023). Las nuevas capacidades estratégicas para la Unión Europea proporcionadas por el sector espacial. Especial referencia a las PNT. *Economía industrial*, *430*, 65-72.

ESA. (2022). *EU SPACE Programme Overview—European Commission*. https://defence-industry-space.ec.europa.eu/eu-space-programme-overview_en

ESA. (2023). *Media invitation: Information session from ESA's 322nd Council in Paris*. https://www.esa.int/Newsroom/Press_Releases/Media_invitation_Information_session_from_ESA_s_322nd_Council_in_Paris

ESA. (2025a). *Current and future missions*. https://www.esa.int/Enabling_Support/Operations/Current_and_future_missions

ESA. (2025b). *ESA budget by domain 2025*. https://www.esa.int/ESA_Multimedia/Images/2025/01/ESA_budget_by_domain_2025

European Union Agency for Cybersecurity. (2023). *A multilayer framework for good cybersecurity practices for AI: Security and resilience for smart health services and infrastructures.* Publications Office. https://data.europa.eu/doi/10.2824/588830

Gamble, W. (2020). *The Cybersecurity Maturity Model Certification (CMMC) – A pocket guide*. IT Governance Publishing. https://doi.org/10.2307/j.ctv17f12mb

Gedeon, J. (2023, agosto 11). *For the first time, U.S. government lets hackers break into satellite in space*. POLITICO. https://www.politico.com/news/2023/08/11/def-con-hackers-space-force-00110919

González, A. (2021, mayo 17). Dynamic Cybersecurity Risk Assessment. *Dynamic Cybersecurity Risk Assessment*. https://www.tarlogic.com/blog/dynamic-cybersecurity-risk-assessment/

Holmes, M. (2008, diciembre 1). *NASA Computers Hacked By Intruders*. Via Satellite. https://www.satellitetoday.com/government-military/2008/12/01/nasa-computers-hacked-by-intruders/

Hussain, A., Mohamed, A., & Razali, S. (2020). A Review on Cybersecurity: Challenges & Emerging Threats. *Proceedings of the 3rd International Conference on Networking, Information Systems & Security*, 1-7. https://doi.org/10.1145/3386723.3387847

Imperva. (2023). Cybersecurity Risk Management | Frameworks, Analysis & Assessment | Imperva. *Learning Center*. https://www.imperva.com/learn/data-security/cybersecurity-risk-management/

International Organization for Standardization. (2018). *ISO 19011:2018—Guidelines for auditing management systems*. https://www.iso.org/standard/70017.html

International Organization for Standardization. (2021). *ISO/IEC TR 24029-1:2021—Artificial Intelligence (AI)—Assessment of the robustness of neural networks Part 1: Overview*. https://www.iso.org/standard/77609.html

International Organization for Standardization. (2022). *ISO/IEC 22989:2022 -Information technology—Artificial intelligence—Artificial intelligence concepts and terminology*. https://www.iso.org/standard/74296.html

ISACA. (2019). *COBIT® 2019 Framework: Introduction and methodology*. ISACA.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973-993. https://doi.org/10.1016/j.jcss.2014.02.005

Joint Task Force Interagency Working Group. (2020). *Security and Privacy Controls for Information Systems and Organizations* (Revision 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Manulis, M., Bridges, C. P., Harrison, R., Sekar, V., & Davis, A. (2021). Cyber security in New Space. *International Journal of Information Security*, *20*(3), 287-311. https://doi.org/10.1007/s10207-020-00503-w

Marei, D. A. (2019). *The impact of Computer Assisted Auditing Techniques (CAATs) on development of audit process: An assessment of Performance Expectancy of by the auditors*. *7*(2).

Melaku, H. M. (2023). Context-Based and Adaptive Cybersecurity Risk Management Framework. *Risks*, *11*(6), Article 6. https://doi.org/10.3390/risks11060101

Moen, R. (2009). Foundation and History of the PDSA Cycle. *Asian network for quality conference. Tokyo. https://www. deming. org/sites/default/files/pdf/2015/PDSA_History_Ron_Moen. Pdf*, *2009*.

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (No. NIST CSWP 04162018; p. NIST CSWP 04162018). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (No. NIST CSWP 29; p. NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Nikolaev, A. S., Pletneva, N. P., & Pletnev, A. A. (2021). Comparative analysis of the provisions of the standards gost r iso 19011-2012 (iso 19011: 2011) and iso 19011: 2018. *Okhrana truda i tekhnika bezopasnosti na promyshlennykh predpriyatiyakh (Labor protection and safety procedure at the industrial enterprises)*, *3*, 64-69. https://doi.org/10.33920/pro-4-2103-09

NIST. (2018). The CSF 1.1 Five Functions. *NIST*. https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions

NIST. (2021). AI Risk Management Framework. *NIST*. https://www.nist.gov/itl/ai-risk-management-framework

NIST. (2025). *Playbook—AIRC*. NIST AI Resource Center. https://airc.nist.gov/airmf-resources/playbook/

Packetlabs. (2023, diciembre 5). *The Asymmetric Nature of the Cyber Threat Environment*. Packetlabs. https://packetlabs.net/post/the-asymmetric-nature-of-the-cyber-threat-environment

Pereira, D. (2023, junio 30). *New Hacking Group Takes Down Russian Telecom Satellite in Support of Prigozhin's Wagner Group*. OODAloop. https://oodaloop.com/analysis/archive/new-hacking-group-takes-down-russian-telecom-satellite-in-support-of-prigozhins-wagner-group/

Petersen, K., Wohlin, C., & Baca, D. (2009). The Waterfall Model in Large-Scale Development. En F. Bomarius, M. Oivo, P. Jaring, & P. Abrahamsson (Eds.), *Product-Focused Software Process Improvement* (pp. 386-400). Springer. https://doi.org/10.1007/978-3-642-02152-7_29

RiskRecon. (2023). Utilizing Dynamic Cyber Risk Assessments | Risk Recon. *Utilizing Dynamic Cyber Risk Assessments*. https://blog.riskrecon.com/utilizing-dynamic-cyber-risk-assessments

Sabillón, R., & M., J. J. C. (2019). Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, *32*, 33-48. https://doi.org/10.17013/risti.32.33-48

Sanchez-Garcia, I. D., Rea-Guaman, A. M., Feliu, T. S., Calvo-Manzano, J. A., Sanchez-Garcia, I. D., Rea-Guaman, A. M., Feliu, T. S., & Calvo-Manzano, J. A. (2024). Auditoría de riesgos de ciberseguridad: Revisión de Literatura, propuesta y aplicación. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, *53*, 69-87. https://doi.org/10.17013/risti.53.69-87

Scholl, M., & Suloway, T. (2022). *Introduction to Cybersecurity for Commercial Satellite Operations* (No. NIST Internal or Interagency Report (NISTIR) 8270 (Withdrawn)). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8270-draft2

Secure Controls Framework. (2025). *What Is The SCF?* https://securecontrolsframework.com/what-is-the-scf/

Swope, C., Bingen, K. A., Young, M., Chang, M., Songer, S., & Tammelleo, J. (2024). *Space Threat Assessment 2024*. https://www.csis.org/analysis/space-threat-assessment-2024

TEDAE. (2020). *Anuario del Sector Espacial en España 2019*. TEDAE. https://pdfonline.tedae.org/anuario2019/files/downloads/Anuario_ESPACIO%202019_web%20baja.pdf

U.S. Department of Defense. (2021, diciembre). *Cybersecurity Maturity Model Certification—Model Overview*. U.S. Department of Defense. https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview_V2.0_FINAL2_20211202_508.pdf

Ventura Traveset Bosch, J. (2021). El sector espacial: Una extraordinaria oportunidad para Europa. *Cuadernos de estrategia*, *208*, 17-88.

Verge. (2023, septiembre 27). *MOVEit cyberattacks: Keeping tabs on the biggest data theft of 2023*. The Verge. https://www.theverge.com/23892245/moveit-cyberattacks-clop-ransomware-government-business

Anexo A. Acrónimos

Tabla 19. Acrónimos

Acrónimo	Significado
CAAT	Herramienta de Auditoría asistida por computadora
CMMC	Cybersecurity Maturity Model Certification
COBIT	Control Objectives for Information and Related Technology
COTS	Commercial Off-The-Shelf
CSF	Cybersecurity Framework
CVE	Common Vulnerabilities and Exposures
DRP	Disaster Recovery Plan
EGNOS	European Geostationary Navigation Overlay Service
ENISA	European Union Agency for Cybersecurity (Agencia de Ciberseguridad de la Unión Europea)
ESA	European Space Agency
FAICP	Marco de Prácticas de Ciberseguridad para IA
GNSS	Sistema Global de Navegación por Satélite
GPS	Global Positioning System
IA	Inteligencia Artificial

Acrónimo	Significado
ID	Identifier (Identificador)
IoT	Internet of Things
ISO	International Organization for Standardization (Organización Internacional de Normalización)
NIST	National Institute of Standards and Technology
OCDE	Organización para la Cooperación y el Desarrollo Económico
PHVA	Planificar, Hacer, Verificar, Actuar (Ciclo de Deming)
PNT	Posicionamiento, Navegación y Transporte
PYMES	Pequeñas y medianas empresas
RMF	Risk Management Framework
SOC	Security Operations Center (Centro de Operaciones de Seguridad)
SQL	Structured Query Language
TEDAE	Asociación Española de Empresas Tecnológicas de Defensa, Aeronáutica y Espacio
UE	Unión Europea
VBA	Visual Basic for Applications

Fuente: Elaboración propia

Anexo B. Código Fuente

Función cálculo promedio ponderado (AI RMF 1.0)

En base a una lista de subcontroles toma el valor de ese subcontrol y su peso de la hoja SC para realizar una media ponderada de todos estos valores.

Figura 7: Código fuente de la función de cálculo promedio ponderado ½

```
Function CalculateSubcontrolsWeightedAverage(idList As String, idRangeSC As Range, weightRangeSC As Range, valueRangeSC As Range) As Variant
    ' --- Function to calculate the weighted average based on a list of IDs ---
    ' Arguments:
    '   idList: The cell containing IDs separated by commas (e.g., "ID1, ID2, ID3") or "N/A"
    '   idRangeSC: The range of the ID column on the SC sheet (e.g., SC!A2:A1000) <- Ensure it starts on the same row as the other ranges
    '   weightRangeSC: The range of the Weights (W) column on the SC sheet (e.g., SC!C2:C1000)
    '   valueRangeSC: The range of the Values (2025) column on the SC sheet (e.g., SC!E2:E1000)
    '-------------------------------------------------------------------------------

    Dim idArray As Variant
    Dim currentID As Variant
    Dim weight As Double
    Dim value As Double
    Dim weightedSum As Double
    Dim sumOfWeights As Double
    Dim foundCell As Range
    Dim trimmedList As String
    Dim ws As Worksheet ' Variable for the worksheet

    ' Adjust the delimiter if necessary
    Const DELIMITER As String = ","

    ' Remove leading/trailing spaces from the input list
    trimmedList = Trim(idList)

    ' Check if the input is empty
    If trimmedList = "" Then
        CalculateSubcontrolsWeightedAverage = 0
        Exit Function
    End If

    ' Check if the input is only "N/A"
    If UCase(trimmedList) = "N/A" Then
        CalculateSubcontrolsWeightedAverage = 0
        Exit Function
    End If

    ' Initialize calculation variables
    weightedSum = 0
    sumOfWeights = 0

    ' Get the worksheet where the ranges are located
    Set ws = idRangeSC.Worksheet
```

Fuente: Elaboración propia

Figura 8: Código fuente de la función de cálculo promedio ponderado 2/2

```
    ' Split the ID string into an array (removing internal spaces just for the split)
    idArray = Split(Replace(trimmedList, " ", ""), DELIMITER)

    ' Loop through each ID in the list
    For Each currentID In idArray
        If Trim(currentID) <> "" Then ' Ignore empty IDs if there are double commas
            ' Search for the ID on the SC sheet (idRangeSC)
            Set foundCell = idRangeSC.Find(What:=Trim(currentID), LookIn:=xlValues, LookAt:=xlWhole,
MatchCase:=False)

            ' If the ID is found
            If Not foundCell Is Nothing Then
                ' --- START CORRECTION SECTION ---
                ' Get the weight and value using the absolute row found (foundCell.Row)
                ' and the correct column from the weight/value ranges
                On Error Resume Next ' Handle potential error if the value is not numeric
                weight = CDbl(ws.Cells(foundCell.Row, weightRangeSC.Column).value)
                value = CDbl(ws.Cells(foundCell.Row, valueRangeSC.Column).value)
                On Error GoTo 0 ' Disable error handling
                ' --- END CORRECTION SECTION ---

                ' Accumulate totals if the values are valid and numeric
                If Not IsError(weight) And Not IsError(value) Then
                    If IsNumeric(weight) And IsNumeric(value) Then
                        weightedSum = weightedSum + (value * weight)
                        sumOfWeights = sumOfWeights + weight
                    End If
                End If
            End If
        End If
    Next currentID

    ' Calculate the final weighted average
    If sumOfWeights <> 0 Then
        CalculateSubcontrolsWeightedAverage = weightedSum / sumOfWeights
    Else
        ' If after searching all IDs, the sum of weights is 0
        CalculateSubcontrolsWeightedAverage = 0
    End If

End Function
```

Fuente: Elaboración propia

Función cálculo promedio (AI RMF 1.0)

Función para calcular la media de un rango de celdas sin depender de fórmulas.

Figura 9: Código fuente de la función de cálculo promedio

```
Function CalculateAverage(valueRange As Range) As Variant
    ' -- Function that returns the average of the values --
    ' Arguments:
    '   valueRange: The cells containing numeric value
    '-------------------------------------------------------------------------------

    Dim value As Double
    Dim sum As Double
    Dim elements As Integer

    sum = 0
    elements = 0

    ' Loop through each Cell in the list
    For Each currentCell In valueRange
        If Not IsEmpty(currentCell) And IsNumeric(currentCell) Then
            value = CDbl(currentCell)

            sum = sum + value
            elements = elements + 1
        End If
    Next currentCell

    If sum <> 0 Then
        CalculateAverage = sum / elements
    Else
        CalculateAverage = 0
    End If

End Function
```

Fuente: Elaboración propia

Función cálculo de nivel de cumplimiento (FAICP)

Según el valor de la celda, calculará el nivel de cumplimiento, “Non Compliance” si es menor a 0.4, “Partially Compliance” si se encuentra entre 0.4 y 0.6, “Compliance” si se encuentra entre 0.6 y 0.8, “Fully Compliance” si es mayor a 0.8 y “Not Applicable” en caso de que la celda estuviese vacía o no tuviera un valor numérico válido.

Figura 10: Código fuente de la función de cálculo de nivel cumplimiento (FAICP)

```
Function CalculateComplianceLevel(value As Variant) As String
    ' -- Function that returns the compliance level --
    ' Arguments:
    '   value: The cell containing numeric value or "N/A", or a number
    '-------------------------------------------------------------------------------

    If IsEmpty(value) Or Not IsNumeric(value) Then
        CalculateComplianceLevel = "Not Applicable"
        Exit Function
    End If

    ' Convert to Double for comparison after checking IsNumeric
    Dim numericValue As Double
    numericValue = CDbl(value)

    If numericValue < 0.4 Then
        CalculateComplianceLevel = "Non Compliance"
        Exit Function
    End If

    If numericValue < 0.6 Then
        CalculateComplianceLevel = "Partially Compliance" ' Consider "Partially Compliant"
        Exit Function
    End If

    If numericValue < 0.8 Then
        CalculateComplianceLevel = "Compliance" ' Consider "Compliant"
        Exit Function
    End If

    CalculateComplianceLevel = "Fully Compliance" ' Consider "Fully Compliant"

End Function
```

Fuente: Elaboración propia

Función cálculo del valor mínimo (FAICP)

Esta función calcula, en base a una celda con la lista de subcontroles, el valor mínimo entre los subcontroles asignados revisando la hoja SC sin considerar el peso.

Figura 11: Código fuente de la función de cálculo del valor mínimo 1/2

```
Function FindMinimumValueFromSubcontrols(idList As String, idRangeSC As Range, valueRangeSC As Range) As Variant
    ' --- Function to find the minimum value (Value column) among the listed subcontrols ---
    ' Arguments:
    '   idList: The cell containing IDs separated by commas (e.g., "ID1, ID2, ID3") or "N/A"
    '   idRangeSC: The range of the ID column on the SC sheet (e.g., SC!A2:A1000)
    '   valueRangeSC: The range of the Values (2025) column on the SC sheet (e.g., SC!E2:E1000)
    ' Returns:
    '   The minimum value found, or #N/A if none are valid.
    '-------------------------------------------------------------------------------

    Dim idArray As Variant
    Dim currentID As Variant
    Dim value As Variant      ' Use Variant to check initial errors
    Dim currentValue As Double ' To store the current numeric value
    Dim foundCell As Range
    Dim trimmedList As String
    Dim ws As Worksheet

    Dim minimumValue As Variant ' Will store the minimum value found (can be #N/A)
    Dim firstValidValueFound As Boolean ' Flag to handle the first valid value

    ' Delimiter for the ID list
    Const DELIMITER As String = ","

    ' Remove leading/trailing spaces from the input list
    trimmedList = Trim(idList)

    ' Start by assuming nothing will be found, so the initial result is #N/A
    minimumValue = "N/A"
    firstValidValueFound = False

    ' Check if the input is empty
    If trimmedList = "" Then
        FindMinimumValueFromSubcontrols = "N/A"
        Exit Function
    End If

    ' Check if the input is only "N/A"
    If UCase(trimmedList) = "N/A" Then
        FindMinimumValueFromSubcontrols = "N/A"
        Exit Function
    End If

    ' Get the worksheet where the ranges are located
    Set ws = idRangeSC.Worksheet
```

Fuente: Elaboración propia

Figura 12: Código fuente de la función de cálculo del valor mínimo 2/2

```
46
47      ' Split the ID string into an array
48      idArray = Split(Replace(trimmedList, " ", ""), DELIMITER)
49
50      ' Loop through each ID in the list
51      For Each currentID In idArray
52          If Trim(currentID) <> "" Then ' Ignore empty IDs if there are double commas
53              ' Search for the ID on the SC sheet (idRangeSC)
54              Set foundCell = idRangeSC.Find(What:=Trim(currentID), LookIn:=xlValues, LookAt:=xlWhole,
    MatchCase:=False)
55
56              ' If the ID is found
57              If Not foundCell Is Nothing Then
58                  ' Get value (as Variant first to check for errors)
59                  On Error Resume Next ' Temporarily for the initial read
60                  value = ws.Cells(foundCell.Row, valueRangeSC.Column).value
61                  On Error GoTo 0 ' Disable error handling
62
63                  ' --- LOGIC FOR FINDING THE MINIMUM ---
64                  If IsNumeric(weight) And IsNumeric(value) Then
65                      currentValue = CDbl(value) ' Convert value to number
66
67                      If Not firstValidValueFound Then
68                          ' If this is the first valid subcontrol we find,
69                          ' its value is the minimum so far.
70                          minimumValue = currentValue
71                          firstValidValueFound = True
72                      Else
73                          If currentValue < minimumValue Then
74                              minimumValue = currentValue
75                          End If
76                      End If
77                  End If
78                  ' --- END LOGIC FOR FINDING THE MINIMUM ---
79
80              End If
81          End If
82      Next currentID
83
84      ' Return the minimum value found.
85      ' If input was "" or "N/A", it returns the string "N/A"
86      FindMinimumValueFromSubcontrols = minimumValue
87
88  End Function
```

Fuente: Elaboración propia

Función cálculo nivel de cumplimiento a partir del mínimo de un rango (FAICP)

Esta función calcula el nivel de cumplimiento de un rango de celdas obteniendo el valor mínimo de ellas y aplicando posteriormente la función CalculateComplianceLevel.

Figura 13: Código fuente de la función del nivel de cumplimiento a partir del mínimo de un rango

```
Function CalculateComplianceLevelPolicyArea(valueRange As Range) As String
    ' -- Function that returns the compliance level from a range of values --
    ' Arguments:
    '   valueRange: The cells containing numeric value or "N/A"
    '-------------------------------------------------------------------------------

    Dim value As Double
    Dim minValue As Double
    Dim firstValidValueFound As Boolean

    firstValidValueFound = False

    ' Loop through each Cell in the list
    For Each currentCell In valueRange
        ' Check it is a number and not N/A
        If IsEmpty(currentCell) Or Not IsNumeric(currentCell) Then
            CalculateComplianceLevelPolicyArea = "Not Applicable"
            Exit Function
        End If

        value = CDbl(currentCell) ' Convert value to number

        If Not firstValidValueFound Then
            ' If this is the first value we find,
            ' its value is the minimum so far.
            minValue = value
            firstValidValueFound = True
        Else
            ' If we already had a minimum, compare the current value with it
            If value < minValue Then
                ' If the current value is smaller, update the minimum
                minValue = value
            End If
        End If
    Next currentCell

    CalculateComplianceLevelPolicyArea = CalculateComplianceLevel(minValue)

End Function
```

Fuente: Elaboración propia

Anexo C. Pruebas de Validación

Tabla 20. Conjuntos de Prueba

SC-ID	SUB-CONTROL DESCRIPTION	AUDIT_1	AUDIT_2	AUDIT_3	AUDIT_4	AUDIT_5	AUDIT_6	AUDIT_7	AUDIT_8	AUDIT_9
SC-ID1	Physical devices and systems within the organization are inventoried	0,60	0,80	0,60	0,60	0,80	0,60	0,80	0,60	0,60
SC-ID2	Software platforms and applications within the organization are inventoried	0,60	0,80	0,60	0,60	0,80	0,60	0,60	0,60	0,60
SC-ID3	Architecture and organizational communication and data flows	0,60	0,60	0,60	0,80	0,60	0,80	0,80	0,80	0,60
SC-ID4	External information systems are catalogued	0,60	0,80	0,60	0,80	0,60	0,60	0,80	0,80	0,60
SC-ID5	Resources (HW, devices, data, personnel, and SW) are prioritized based on their classification, criticality, and business value	0,40	0,80	0,60	0,80	0,60	0,60	0,80	0,40	0,40
SC-ID6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established	0,60	0,60	0,60	0,80	0,80	0,80	0,60	0,60	0,60
SC-ID7	The organization's role in the supply chain is identified and communicated	0,60	0,80	0,80	1,00	0,80	0,80	0,80	0,80	0,60
SC-ID8	The organization's place in critical infrastructure and its industry sector is identified and communicated	0,60	1,00	0,60	1,00	1,00	0,80	0,60	1,00	0,60
SC-ID9	Dependencies and critical functions for delivery of critical services are established	1,00	0,80	0,80	1,00	0,80	1,00	1,00	1,00	0,60
SC-ID10	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	1,00	0,80	0,60	1,00	0,60	0,80	1,00	1,00	0,60
SC-ID11	Organizational cybersecurity policy is established and communicated	0,60	0,60	0,60	0,80	1,00	0,80	0,80	0,60	0,40
SC-ID12	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	0,40	0,60	0,60	0,80	0,60	0,60	0,60	0,80	0,60
SC-ID13	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	1,00	1,00	0,60	1,00	0,80	0,80	0,80	0,80	0,60
SC-ID14	Strategy of security, governance and risk management processes address cybersecurity risks	0,40	0,60	0,80	0,80	0,60	0,60	0,40	0,40	0,60
SC-ID15	Asset vulnerabilities are identified and documented	0,40	0,60	0,40	0,80	0,60	0,60	0,60	0,20	0,20
SC-ID16	Cyber threat intelligence is received from information sharing forums and sources	0,40	0,20	0,40	0,40	0,80	0,60	0,60	0,40	0,40
SC-ID17	Threats, both internal and external, are identified and documented	0,40	0,60	0,40	0,60	0,80	0,60	0,60	0,40	0,20
SC-ID18	Potential business impacts and likelihoods are identified (BIA)	0,40	0,60	0,60	0,40	0,60	0,40	0,60	0,40	0,40
SC-ID19	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	0,40	0,60	0,40	0,80	0,80	0,60	0,60	0,20	0,20
SC-ID20	Risk responses are identified and prioritized	0,40	0,60	0,60	0,80	0,60	0,40	0,80	0,20	0,40
SC-ID21	Risk management processes are established, managed, and agreed to by organizational stakeholders	0,40	0,80	0,80	0,80	0,60	0,60	0,80	0,20	0,60

Fuente: Adaptación de la herramienta de la ESA

Se han llevado a cabo diversas auditorías técnicas utilizando una herramienta de diagnóstico basada en estándares internacionales como el **NIST.AI.100-1** y el **FAICP-1**. Estas auditorías se fundamentan en el análisis cuantitativo de más de **100 subcontroles** que cubren aspectos clave como gobernanza, gestión de activos, protección, detección, respuesta y recuperación, así como la alineación con políticas públicas y marcos regulatorios.

Cada auditoría ha permitido caracterizar con precisión el estado de implementación de medidas de seguridad, clasificando el nivel de cumplimiento por control mediante una escala de 0.00 a 1.00, e interpretando los resultados mediante mapas de calor, paneles de riesgo y visualizaciones comparativas. Este enfoque no solo identifica áreas fuertes y consolidadas, sino que también resalta debilidades estructurales, brechas normativas y oportunidades de mejora.

A continuación, se presentan los resultados obtenidos en las distintas evaluaciones, que reflejan una evolución gradual del sistema auditado, desde estados de cumplimiento parcial o crítico hacia entornos más robustos y resilientes. El análisis conjunto permite extraer conclusiones estratégicas para la toma de decisiones, priorizar intervenciones y orientar la mejora continua de la postura de ciberseguridad e IA en la organización.

- **Auditoría 1 (AUDIT_1):** Al realizar la simulación los datos de la auditoría AUDIT_1, donde más de la mitad de los controles (55 de 105) se encuentran en una puntuación de 0.40, reflejando una implementación básica o limitada de las medidas de ciberseguridad. Aunque existen puntos fuertes con 10 controles en 1.00 y otros 10 en 0.80—, estos son casos puntuales que no compensan la falta de madurez general. Visualmente, esto se traduce en una prevalencia del color amarillo en el framework NIST.AI.100-1 (**Medium Risk**), y en la matriz del framewok FAICP-1, en la cual, las mayorías de áreas se encuentra bajo el estado **Partially Compliance**. El amarillo dominante indica que la organización se encuentra en un estado de riesgo medio: aún carece de consistencia, profundidad y cobertura en la implementación de sus controles. Las áreas más comprometidas son la evaluación y gestión de riesgos, detección de amenazas y mantenimiento de la integridad del sistema, mientras que la gobernanza de la cadena de suministro y ciertos aspectos de infraestructura crítica destacan como fortalezas aisladas. En conjunto, los resultados reflejan una postura de seguridad en transición, que requiere reforzar sus procesos y mecanismos de control para avanzar hacia un entorno robusto y confiable.

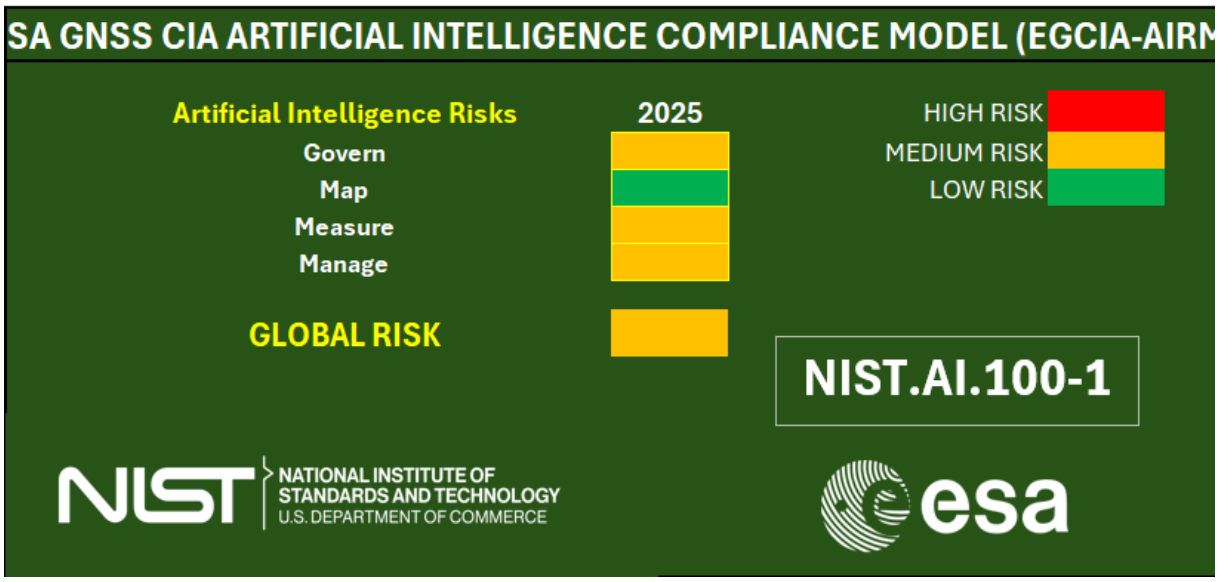
Tabla 21. Hoja SC AUDIT_1

esa

SC-ID	SC-D	W	PROGRAM	2025	2024	AC2025	AC2024
SC-ID1	Physical devices and systems within the organization are inventoried	1	AUDIT-NAME	0,60	0,60	0,6	0,6
SC-ID2	Software platforms and applications within the organization are inventoried	1	AUDIT-NAME	0,60	0,60		
SC-ID3	Architecture and organizational communication and data flows	0,25	AUDIT-NAME	0,60	0,60		
SC-ID4	External information systems are catalogued	0,5	AUDIT-NAME	0,60	0,60		
SC-ID5	Resources (HW, devices, data, personnel, and SW) are prioritized based on their classification, criticality, and business value	1	AUDIT-NAME	0,40	0,60		
SC-ID6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established	1	AUDIT-NAME	0,60	0,60		
SC-ID7	The organization's role in the supply chain is identified and communicated	0,5	AUDIT-NAME	0,60	0,60	0,7	0,6
SC-ID8	The organization's place in critical infrastructure and its industry sector is identified and communicated	0,1	AUDIT-NAME	0,60	0,60		
SC-ID9	Dependencies and critical functions for delivery of critical services are established	0,1	AUDIT-NAME	1,00	0,60		
SC-ID10	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	0,25	AUDIT-NAME	1,00	0,60		

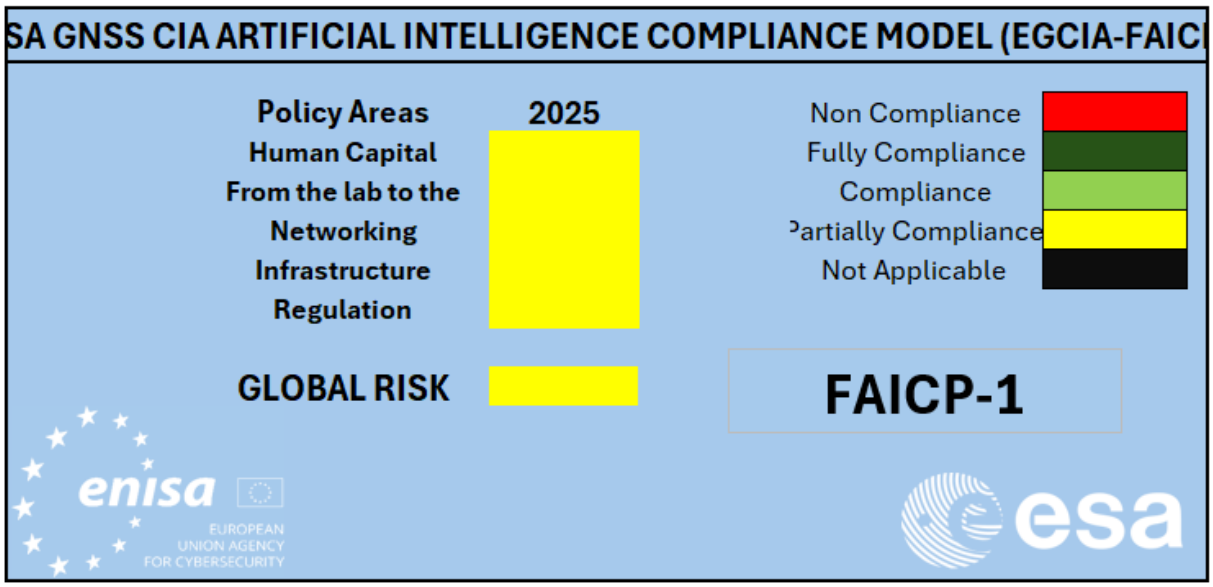
Fuente: Adaptación de la herramienta de la ESA

Tabla 22. Hoja AIRM-G AUDIT_1



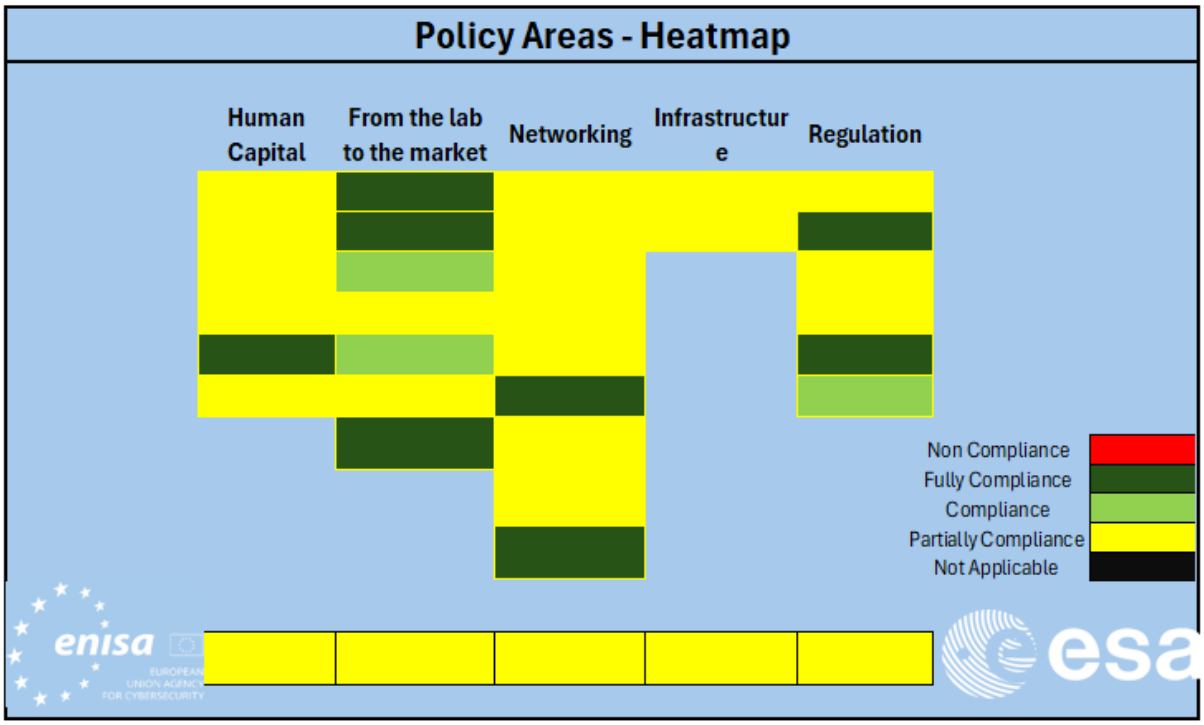
Fuente: Adaptación de la herramienta de la ESA

Tabla 23. Hoja FAICP Q&A AUDIT_1, 1/2



Fuente: Adaptación de la herramienta de la ESA

Tabla 24. Hoja FAICP Q&A AUDIT_1, 2/2



Fuente: Adaptación de la herramienta de la ESA

Auditoría 2 (AUDIT_4): Esta auditoría muestra un cambio notable respecto a la evaluación anterior, reflejando un entorno organizativo que ha mejorado significativamente su madurez en ciberseguridad. Los datos indican que 41 controles (la mayoría) están puntuados con 0.80, lo que sugiere un cumplimiento alto, con procesos implementados de manera consistente y efectiva, aunque con ciertos márgenes aún por optimizar. A esto se suman 18 controles en 1.00, lo cual evidencia una madurez completa y consolidada en varios dominios clave. Solo 23 controles presentan una puntuación intermedia de 0.60, y hay 21 controles en 0.40, que

siguen siendo puntos débiles, aunque menos predominantes que antes. Finalmente, apenas 2 controles fueron calificados con 0.20, lo que indica que las áreas críticas son ahora excepcionales y no generalizadas.

Visualmente, este avance se refleja de forma clara en los paneles generados por la herramienta. El framework NIST.AI.100-1 muestra ahora todas las categorías ("**Govern**", "**Map**", "**Measure**", "**Manage**") con color verde (**Low Risk**), lo que equivale a un riesgo bajo en la evaluación global. Esto representa un entorno controlado, capaz de mapear, medir y gestionar riesgos relacionados con inteligencia artificial de forma madura. Por otro lado, el panel de cumplimiento del framework europeo FAICP-1 aún muestra un predominio del color amarillo, aunque con áreas verdes visibles, lo que sugiere que, desde el enfoque europeo, aún existen aspectos por fortalecer, especialmente en las áreas de "**Human Capital**" y "**Networking**". No obstante, el riesgo global se mantiene en amarillo (**Partially Compliance**), indicando que aunque el cumplimiento ha mejorado, todavía hay margen para consolidar buenas prácticas en toda la organización.

En resumen, esta nueva evaluación posiciona a la organización en un estadio de madurez avanzada, con una estructura de seguridad robusta y en mejora constante. El reto actual ya no es establecer controles desde cero, sino refinar, automatizar y mantener la coherencia en todos los niveles del sistema de seguridad, especialmente en los pocos subcontroles que siguen mostrando debilidades estructurales.

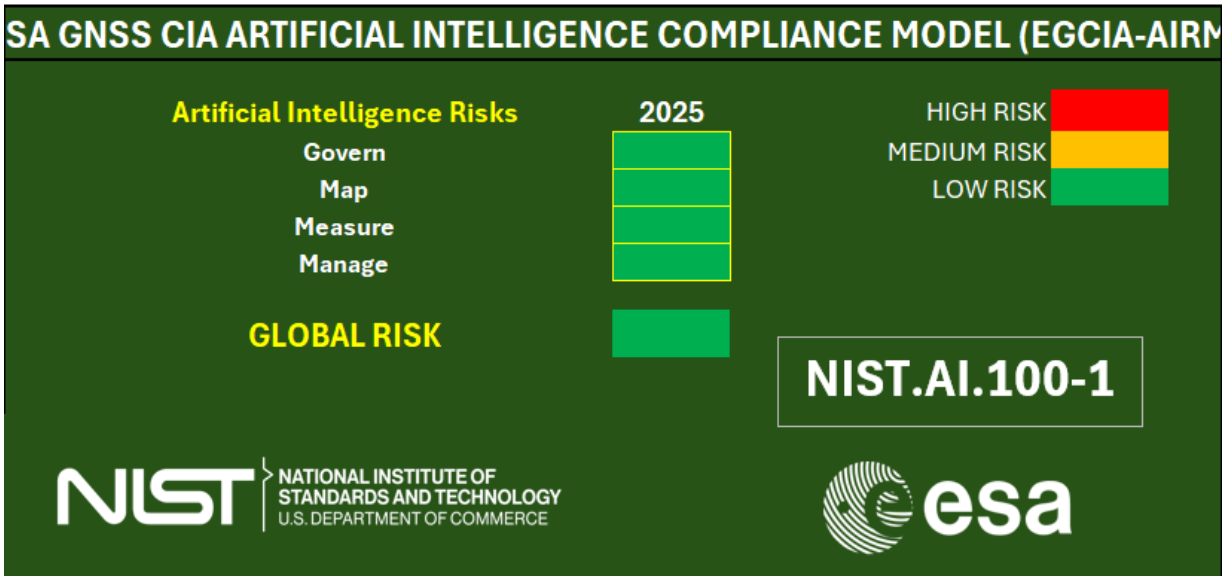
Tabla 25. Hoja SC AUDIT_4

esa

SC-ID	SC-D	W	PROGRAM	2025	2024	AC2025	AC2024
SC-ID1	Physical devices and systems within the organization are inventoried	1	AUDIT-NAME	0,60	0,60	0,7	0,6
SC-ID2	Software platforms and applications within the organization are inventoried	1	AUDIT-NAME	0,60	0,60		
SC-ID3	Architecture and organizational communication and data flows	0,25	AUDIT-NAME	0,80	0,60		
SC-ID4	External information systems are catalogued	0,5	AUDIT-NAME	0,80	0,60		
SC-ID5	Resources (HW, devices, data, personnel, and SW) are prioritized based on their classification, criticality, and business value	1	AUDIT-NAME	0,80	0,60		
SC-ID6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established	1	AUDIT-NAME	0,80	0,60		
SC-ID7	The organization's role in the supply chain is identified and communicated	0,5	AUDIT-NAME	1,00	0,60	1,0	0,6
SC-ID8	The organization's place in critical infrastructure and its industry sector is identified and communicated	0,1	AUDIT-NAME	1,00	0,60		
SC-ID9	Dependencies and critical functions for delivery of critical services are established	0,1	AUDIT-NAME	1,00	0,60		
SC-ID10	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	0,25	AUDIT-NAME	1,00	0,60		

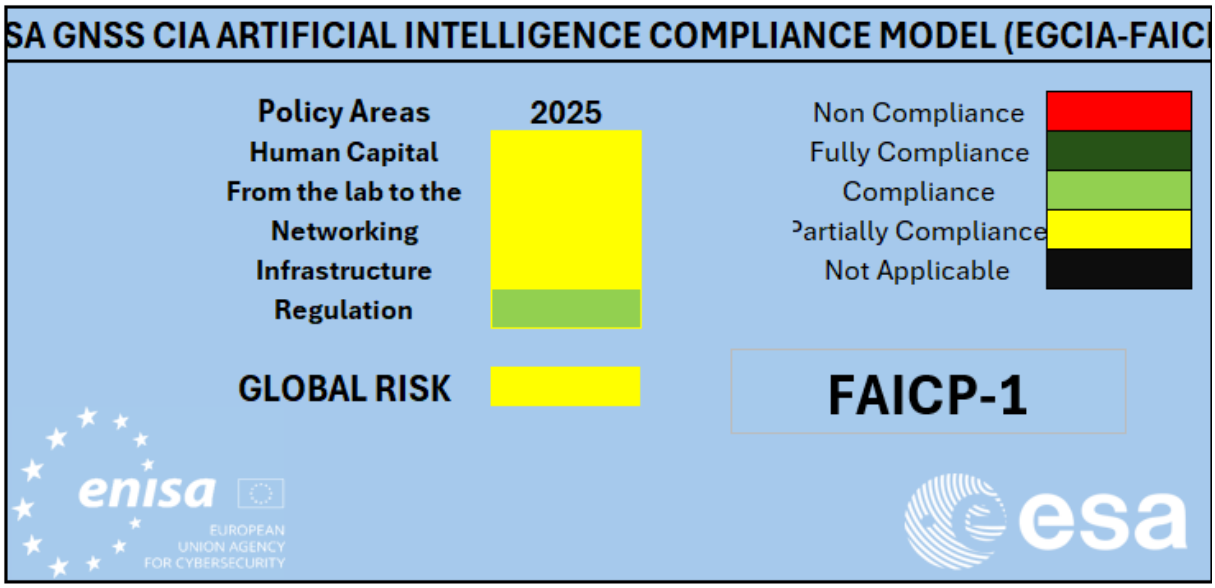
Fuente: Adaptación de la herramienta de la ESA

Tabla 26. Hoja AIRM-G AUDIT_4



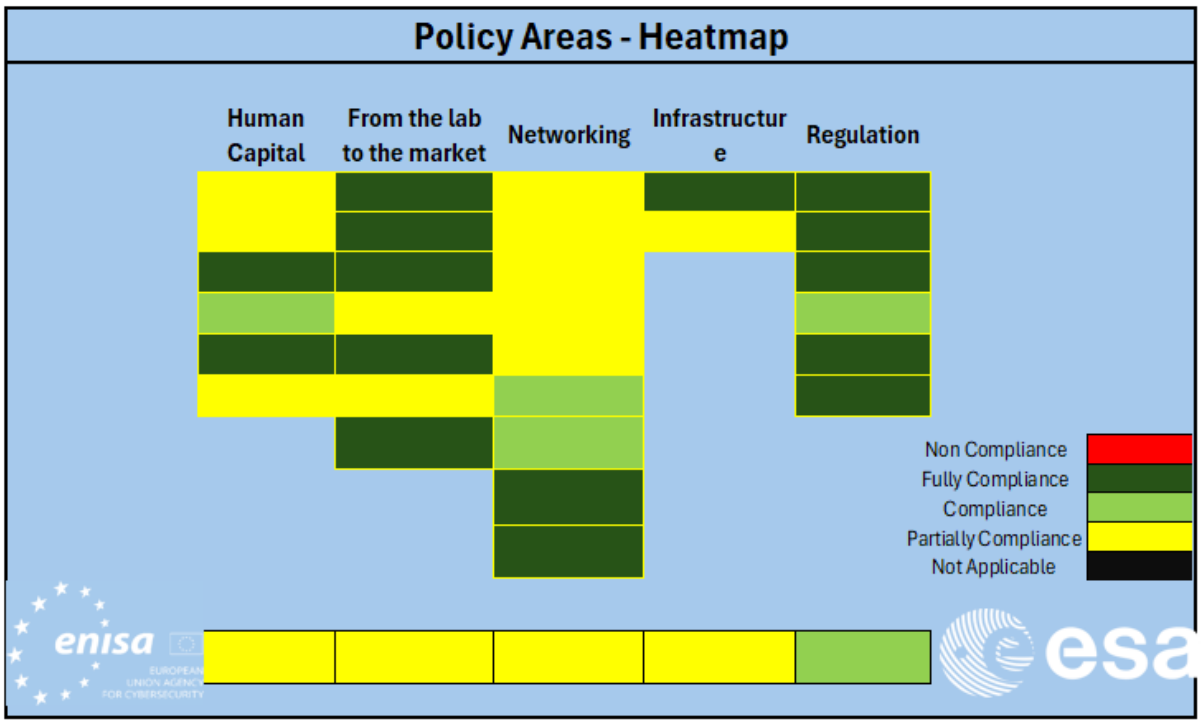
Fuente: Adaptación de la herramienta de la ESA

Tabla 27. Hoja FAICP Q&A AUDIT_4, 1/2



Fuente: Adaptación de la herramienta de la ESA

Tabla 28. Hoja FAICP Q&A AUDIT_4, 2/2



Fuente: Adaptación de la herramienta de la ESA

Auditoría 3 (AUDIT_9): Esta auditoría revela un panorama de cumplimiento desequilibrado, con una fuerte concentración de puntuaciones en los rangos bajos e intermedios. De los 105 controles evaluados, 44 están puntuados con 0.40, lo que indica que casi la mitad de los controles se encuentran en un estado básico de implementación, sin llegar a niveles aceptables de madurez. Además, hay 17 controles con una puntuación crítica de 0.20, lo que representa debilidades estructurales importantes, muchas de ellas probablemente sin procedimientos definidos o con fallos graves en su ejecución. Por el contrario, solo 9 controles alcanzan la puntuación máxima de 1.00, lo que refleja que el cumplimiento total es limitado a unas pocas áreas bien estructuradas, y solo 3 controles se sitúan en un cumplimiento alto con 0.80. Unos 32 controles están en 0.60, lo que apunta a esfuerzos parciales o incipientes que aún no alcanzan el nivel esperado.

Estos datos se reflejan claramente en los resultados visuales generados por la herramienta. El framework NIST.AI.100-1 muestra todos los dominios de riesgo de inteligencia artificial ("**Govern**", "**Map**", "**Measure**", "**Manage**") en color amarillo (**Medium Risk**), lo cual indica un riesgo medio global. Esto sugiere que la organización posee cierta estructura de gobernanza y monitoreo, pero carece de profundidad, consistencia y eficacia suficientes para reducir el riesgo a niveles bajos. El resultado es un entorno vulnerable a incidentes si estos mecanismos no se fortalecen.

Por su parte, el framework FAICP-1 ofrece una visión más crítica. Tanto el indicador de riesgo global como las áreas políticas individuales aparecen en color rojo (**Non Compliance**), lo que significa que la organización se encuentra en una situación de incumplimiento generalizado en múltiples dominios clave: "**Human Capital**", "**Networking**", "**Regulation**" y "**From the Lab to the Market**" muestran claras señales de alarma. El heatmap complementario confirma esta situación, destacando en rojo y amarillo la mayoría de los bloques, y evidenciando la necesidad urgente de intervención.

En resumen, esta auditoría posiciona a la organización en un nivel de alto riesgo, donde las capacidades actuales de ciberseguridad e IA no son suficientes para garantizar resiliencia, cumplimiento normativo ni defensa eficaz frente a amenazas.

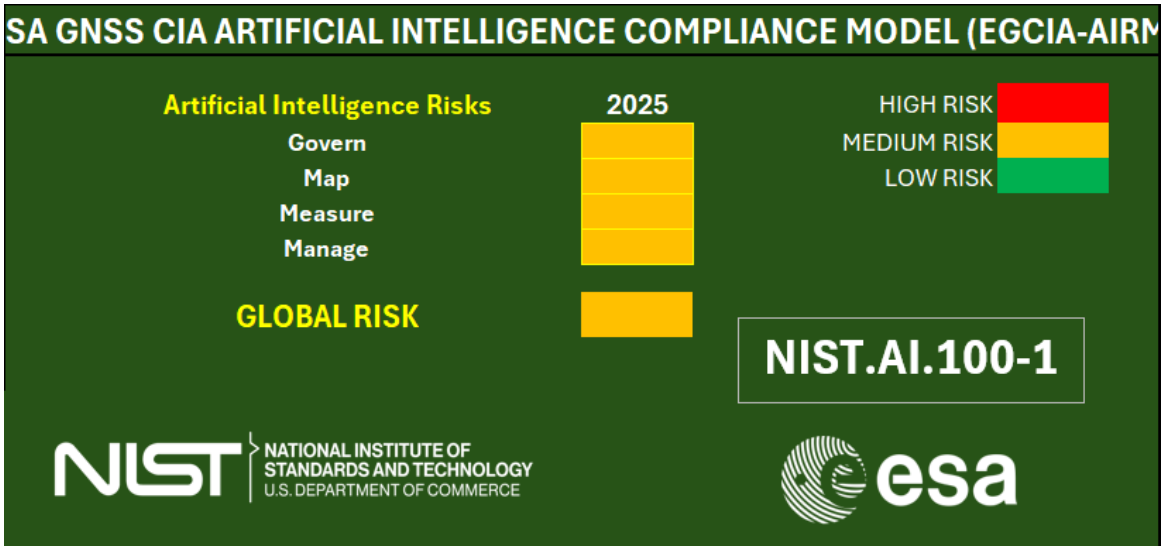
Tabla 29. Hoja SC AUDIT_9

esa

SC-ID	SC-D	W	PROGRAM	2025	2024	AC2025	AC2024
SC-ID1	Physical devices and systems within the organization are inventoried	1	AUDIT-NAME	0,60	0,60	0,6	0,6
SC-ID2	Software platforms and applications within the organization are inventoried	1	AUDIT-NAME	0,60	0,60		
SC-ID3	Architecture and organizational communication and data flows	0,25	AUDIT-NAME	0,60	0,60		
SC-ID4	External information systems are catalogued	0,5	AUDIT-NAME	0,60	0,60		
SC-ID5	Resources (HW, devices, data, personnel, and SW) are prioritized based on their classification, criticality, and business value	1	AUDIT-NAME	0,40	0,60		
SC-ID6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established	1	AUDIT-NAME	0,60	0,60		
SC-ID7	The organization's role in the supply chain is identified and communicated	0,5	AUDIT-NAME	0,60	0,60	0,6	0,6
SC-ID8	The organization's place in critical infrastructure and its industry sector is identified and communicated	0,1	AUDIT-NAME	0,60	0,60		
SC-ID9	Dependencies and critical functions for delivery of critical services are established	0,1	AUDIT-NAME	0,60	0,60		
SC-ID10	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	0,25	AUDIT-NAME	0,60	0,60		

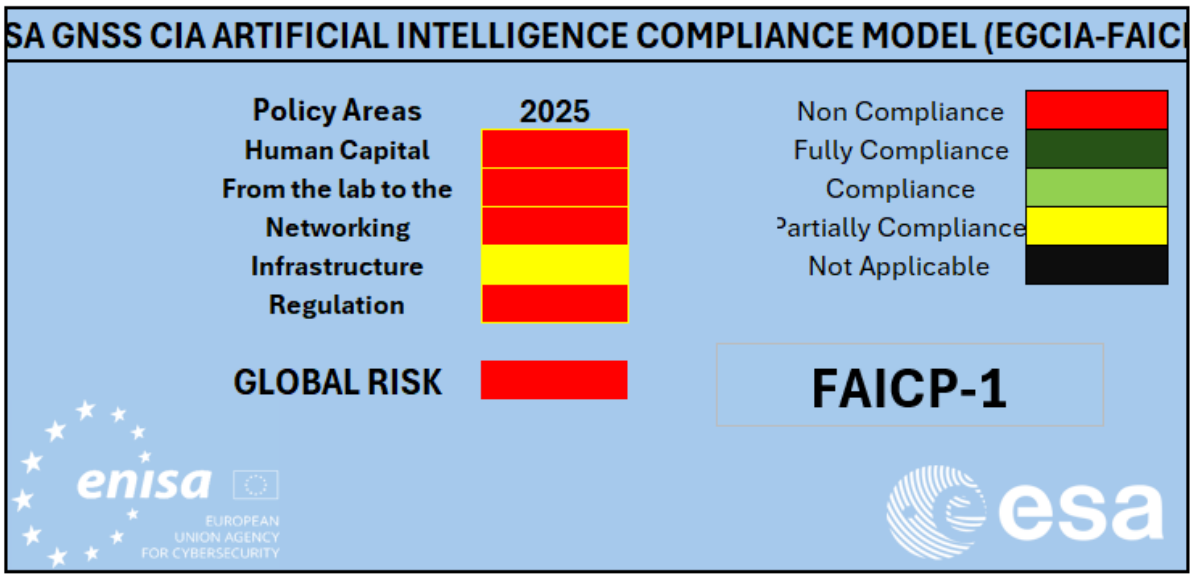
Fuente: Adaptación de la herramienta de la ESA

Tabla 30. Hoja AIRM-G AUDIT_9



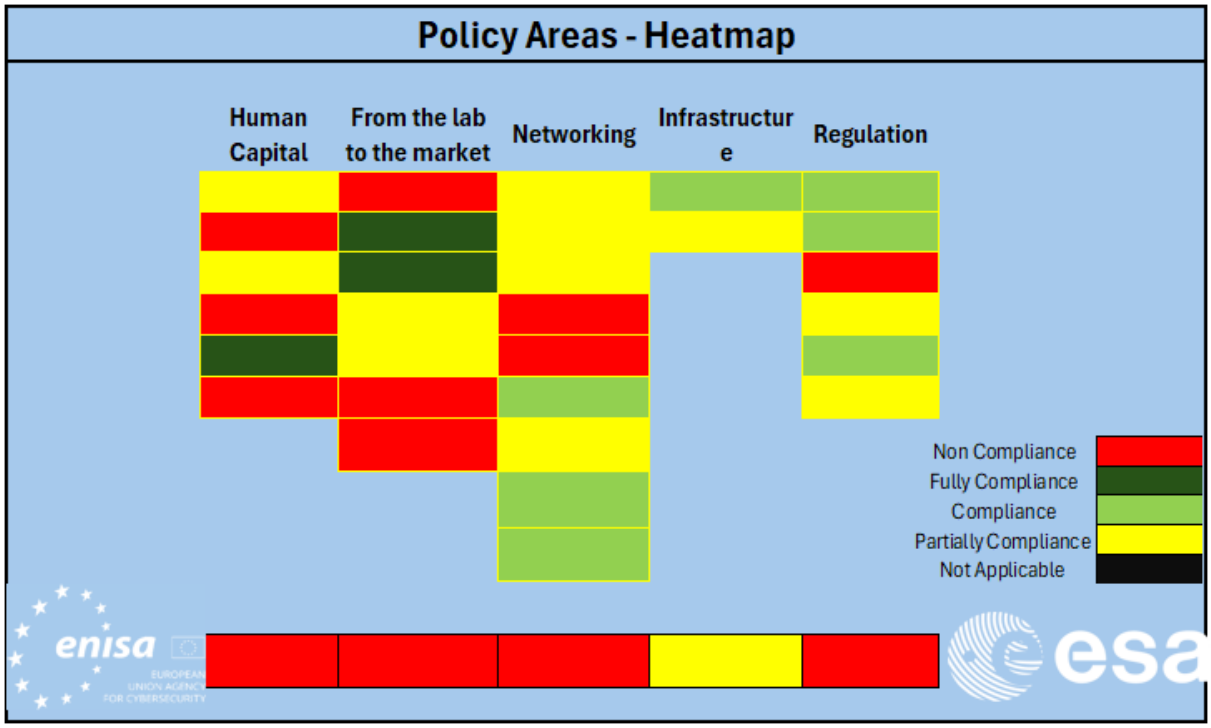
Fuente: Adaptación de la herramienta de la ESA

Tabla 31. Hoja FAICP Q&A AUDIT_9, 1/2



Fuente: Adaptación de la herramienta de la ESA

Tabla 32. Hoja FAICP Q&A AUDIT_9, 2/2



Fuente: Adaptación de la herramienta de la ESA