COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI

MASTER UNIVERSITARIO EN INGENIERÍA DE TELECOMUNICACIONES

TRABAJO FIN DE MASTER

Implementación de la Regulación DORA en el Sector Financiero: Análisis GAP y Estrategia de Cumplimiento

Autor: Sofía Barquero Jiménez

Director: Hugo Cedillo Martínez

Madrid

Junio 2025

Declaro, bajo mi responsabilidad, que el Proyecto presentado con el título

Implementación de la Regulación DORA en el Sector Financiero: Análisis GAP y Estrategia de Cumplimiento

en la ETS de Ingeniería - ICAI de la Universidad Pontificia Comillas en el

curso académico 2024/2025 es de mi autoría, original e inédito y

no ha sido presentado con anterioridad a otros efectos.

El Proyecto no es plagio de otro, ni total ni parcialmente y la información que ha sido

tomada de otros documentos está debidamente referenciada.

Fdo.: Sofía Barquero Jiménez Fecha: 15/06/2025

Autorizada la entrega del proyecto

EL DIRECTOR DEL PROYECTO

Fdo.: Hugo Cedillo Martínez Fecha: 13 / 06 / 2025

AUTORIZACIÓN PARA LA DIGITALIZACIÓN, DEPÓSITO Y DIVULGACIÓN EN RED DE PROYECTOS FIN DE GRADO, FIN DE MÁSTER, TESINAS O MEMORIAS DE BACHILLERATO

1º. Declaración de la autoría y acreditación de la misma.

El autor Dña. Sofía Barquero Jiménez DECLARA ser el titular de los derechos de propiedad intelectual de la obra: Implementación de la Regulación DORA en el Sector Financiero: Análisis GAP y Estrategia de Cumplimiento, que ésta es una obra original, y que ostenta la condición de autor en el sentido que otorga la Ley de Propiedad Intelectual.

2º. Objeto y fines de la cesión.

Con el fin de dar la máxima difusión a la obra citada a través del Repositorio institucional de la Universidad, el autor **CEDE** a la Universidad Pontificia Comillas, de forma gratuita y no exclusiva, por el máximo plazo legal y con ámbito universal, los derechos de digitalización, de archivo, de reproducción, de distribución y de comunicación pública, incluido el derecho de puesta a disposición electrónica, tal y como se describen en la Ley de Propiedad Intelectual. El derecho de transformación se cede a los únicos efectos de lo dispuesto en la letra a) del apartado siguiente.

3º. Condiciones de la cesión y acceso

Sin perjuicio de la titularidad de la obra, que sigue correspondiendo a su autor, la cesión de derechos contemplada en esta licencia habilita para:

a) Transformarla con el fin de adaptarla a cualquier tecnología que permita incorporarla a internet y hacerla accesible; incorporar metadatos para realizar el registro de la obra e incorporar "marcas de agua" o cualquier otro sistema de seguridad o de protección.
b) Reproducirla en un soporte digital para su incorporación a una base de datos electrónica, incluyendo el derecho de reproducir y almacenar la obra en servidores, a los efectos de garantizar su seguridad, conservación y preservar el formato.
c) Comunicarla, por defecto, a través de un archivo institucional abierto, accesible de modo libre y gratuito a través de internet.
d) Cualquier otra forma de acceso (restringido, embargado, cerrado) deberá solicitarse expresamente y obedecer a causas justificadas.
e) Asignar por defecto a estos trabajos una licencia Creative Commons.
f) Asignar por defecto a estos trabajos un HANDLE (URL *persistente)*.

4º. Derechos del autor.

El autor, en tanto que titular de una obra tiene derecho a:

a) Que la Universidad identifique claramente su nombre como autor de la misma
b) Comunicar y dar publicidad a la obra en la versión que ceda y en otras posteriores a través de cualquier medio.
c) Solicitar la retirada de la obra del repositorio por causa justificada.
d) Recibir notificación fehaciente de cualquier reclamación que puedan formular terceras personas en relación con la obra y, en particular, de reclamaciones relativas a los derechos de propiedad intelectual sobre ella.

5º. Deberes del autor.

El autor se compromete a:

a) Garantizar que el compromiso que adquiere mediante el presente escrito no infringe ningún derecho de terceros, ya sean de propiedad industrial, intelectual o cualquier otro.
b) Garantizar que el contenido de las obras no atenta contra los derechos al honor, a la intimidad y a la imagen de terceros.
c) Asumir toda reclamación o responsabilidad, incluyendo las indemnizaciones por daños, que pudieran ejercitarse contra la Universidad por terceros que vieran infringidos sus derechos e intereses a causa de la cesión.
d) Asumir la responsabilidad en el caso de que las instituciones fueran condenadas por infracción de derechos derivada de las obras objeto de la cesión.

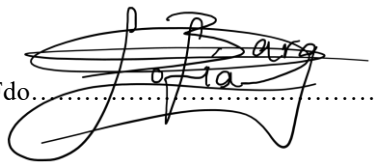
6º. Fines y funcionamiento del Repositorio Institucional.

La obra se pondrá a disposición de los usuarios para que hagan de ella un uso justo y respetuoso con los derechos del autor, según lo permitido por la legislación aplicable, y con fines de estudio, investigación, o cualquier otro fin lícito. Con dicha finalidad, la Universidad asume los siguientes deberes y se reserva las siguientes facultades:

- La Universidad informará a los usuarios del archivo sobre los usos permitidos, y no garantiza ni asume responsabilidad alguna por otras formas en que los usuarios hagan un uso posterior de las obras no conforme con la legislación vigente. El uso posterior, más allá de la copia privada, requerirá que se cite la fuente y se reconozca la autoría, que no se obtenga beneficio comercial, y que no se realicen obras derivadas.
- La Universidad no revisará el contenido de las obras, que en todo caso permanecerá bajo la responsabilidad exclusive del autor y no estará obligada a ejercitar acciones legales en nombre del autor en el supuesto de infracciones a derechos de propiedad intelectual derivados del depósito y archivo de las obras. El autor renuncia a cualquier reclamación frente a la Universidad por las formas no ajustadas a la legislación vigente en que los usuarios hagan uso de las obras.
- La Universidad adoptará las medidas necesarias para la preservación de la obra en un futuro.
- La Universidad se reserva la facultad de retirar la obra, previa notificación al autor, en supuestos suficientemente justificados, o en caso de reclamaciones de terceros.

Madrid, a 15 de junio de 2025

ACEPTA



Fdo……

Motivos para solicitar el acceso restringido, cerrado o embargado del trabajo en el Repositorio Institucional:

Este trabajo debe ser considerado confidencial, ya que se basa en la aplicación real del Reglamento DORA a una entidad del sector financiero en el marco de un proyecto profesional. Aunque se ha procedido a la anonimización del cliente, el contenido incluye información sensible sobre procesos internos de evaluación y cumplimiento normativo, cuya divulgación podría comprometer la estrategia de cumplimiento de dicha entidad. Además, las herramientas desarrolladas como parte del proyecto fueron diseñadas durante el periodo de prácticas en la empresa, lo que implica que tanto la metodología como los recursos utilizados son propiedad intelectual de la organización. Por tanto, se requiere preservar la confidencialidad para proteger tanto los intereses del cliente como los derechos de la empresa titular del proyecto.

COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI

MASTER UNIVERSITARIO EN INGENIERÍA DE TELECOMUNICACIONES

TRABAJO FIN DE MASTER

Implementación de la Regulación DORA en el Sector Financiero: Análisis GAP y Estrategia de Cumplimiento

Autor: Sofía Barquero Jiménez

Director: Hugo Cedillo Martínez

Madrid

Junio 2025

Agradecimientos

Me siento profundamente agradecida a muchas personas que han estado presentes en las distintas etapas de este proyecto. Su apoyo, orientación y confianza han sido fundamentales para alcanzar los objetivos propuestos y para poder cerrar esta etapa con una gran satisfacción personal y profesional.

En primer lugar, a mi familia por todo su apoyo y sus ánimos a lo largo de toda mi etapa universitaria, a mi hermana, a mis tíos y, en especial, a mis padres por darme la oportunidad de estudiar en ICAI, no solo el grado de ingeniería sino también este doble máster que tan buena formación y preparación me ha aportado.

A todos los profesores que he tenido estos dos últimos años, en especial a Javier Jarauta y Gregorio López por estar pendientes de mí y de todos mis compañeros y compañeras, aconsejarnos, guiarnos y escucharnos.

A mi tutor en la empresa, Hugo Cedillo, y a Cristian Capraru, por estar ambos siempre dispuestos a ayudarme y enseñarme y por hacerme tan fácil y cómoda mi entrada a la vida laboral.

A Javier, por ser un apoyo fundamental en mi día a día, escuchando mis preocupaciones y poniéndoles solución y ánimos siempre que lo he necesitado.

A todos mis amigos y amigas de dentro y fuera de la universidad, por hacer estos años inolvidables.

A la universidad, por darme la mejor formación que podría haber pedido.

IMPLEMENTACIÓN DE LA REGULACIÓN DORA EN EL SECTOR FINANCIERO: ANÁLISIS GAP Y ESTRATEGIA DE CUMPLIMIENTO

Autor: Barquero Jiménez, Sofía
Director: Cedillo Martínez, Hugo
Entidad Colaboradora: SIA

RESUMEN DEL PROYECTO

Este Trabajo de Fin de Máster aborda la aplicación del reglamento DORA en una entidad financiera, desarrollando una herramienta en Excel para llevar a cabo un análisis GAP, que identifica áreas de incumplimiento. A partir de este análisis, se diseña una hoja de ruta personalizada con medidas correctivas priorizadas para garantizar el cumplimiento continuo.

Palabras clave: Reglamento DORA, entidad financiera, Excel, automatización, análisis GAP, cumplimiento normativo, medidas correctivas, plan de acción.

1. Introducción

Este Trabajo de Fin de Máster tiene como objetivo implementar el reglamento DORA [1] en una entidad financiera, combinando un análisis normativo con un diagnóstico de su situación actual. Se desarrollará una herramienta en Excel para realizar un análisis GAP, identificando incumplimientos y priorizando medidas correctivas.

El proyecto incluye varias etapas clave: diagnóstico inicial, actualización de políticas internas, implementación de tecnologías, formación especializada en resiliencia operativa y pruebas para evaluar la robustez de los sistemas. Como resultado, se elaborará una hoja de ruta personalizada que asegure el cumplimiento normativo inicial, fomente la sostenibilidad a largo plazo y fortalezca la resiliencia digital de la organización.

2. Definición del proyecto

El objetivo principal del proyecto es implementar el reglamento DORA en una entidad financiera. Esta implementación se obtendrá mediante una herramienta en Excel para el análisis GAP elaborada desde cero y aplicable a cualquier tipo de proyectos de cumplimiento de este reglamento, que identifica incumplimientos y prioriza medidas correctivas. El proyecto incluye un diagnóstico inicial, actualización de políticas, adopción de tecnologías, formación en resiliencia operativa y pruebas de robustez. Finalmente, se diseña una hoja de ruta personalizada para garantizar el cumplimiento continuo y fortalecer la resiliencia digital a largo plazo.

3. Descripción del modelo/sistema/herramienta

La herramienta Excel desarrollada para este proyecto está diseñada para simplificar el análisis GAP y apoyar la implementación de la regulación DORA en entidades financieras. Esta herramienta contiene una lista completa de todos los controles identificados a lo largo del reglamento para llevar a cabo el cumplimiento de este, facilitando no solo la identificación de la aplicabilidad de los controles, sino también la adaptación de la descripción de los requisitos específicos que cada tipo de entidad debe

cumplir. Esto garantiza que el análisis se ajuste a las necesidades de cumplimiento particulares de cada caso. Este enfoque dinámico permite identificar de manera más eficiente las áreas de incumplimiento y priorizar las acciones correctivas necesarias.

Además, la herramienta incluye un sistema automatizado que genera un archivo complementario pensado para el cliente. Este archivo ofrece un servicio más completo y claro, recopilando las acciones correctivas recomendadas en tablas organizadas y visualizando la información mediante cuadros de mando interactivos. De este modo, el cliente puede monitorizar fácilmente el estado actual de cumplimiento, así como la evolución del proceso a medida que se implementan las medidas correctivas, lo que facilita su aplicación y seguimiento.

En conjunto, la herramienta proporciona un análisis detallado, flexibilidad en el filtrado, diferenciación de requisitos y un servicio complementario para el cliente, ofreciendo una solución eficiente y práctica para alcanzar y mantener el cumplimiento normativo.

4. Resultados

A lo largo del proyecto, el mayor logro ha sido el desarrollo de una herramienta propia, diseñada desde cero con un enfoque totalmente práctico y adaptado al análisis de cumplimiento del Reglamento DORA en el entorno financiero. Al principio, el proceso era mucho más manual y genérico y a medida que se profundizó en la normativa y en sus implicaciones reales en el trabajo de consultoría, así como en el proyecto que se estaba llevando a cabo, se decidió que era necesario crear algo más funcional, más cómodo y orientado a cubrir necesidades específicas. Así nació esta herramienta, que permite realizar análisis GAP, clasificar requisitos y evaluar proveedores TIC de una forma mucho más estructurada y ágil. Además, al poder aplicarla en un caso real, se ha tenido la oportunidad de ver qué funciona bien, qué no tanto, y cómo puede evolucionar. Eso ha permitido ajustar y mejorar la herramienta para que no solo cumpla su propósito actual, sino que esté preparada para ser utilizada en futuros proyectos, facilitando el trabajo del consultor, reduciendo tiempos y evitando errores. En resumen, más allá de haber cumplido con los objetivos marcados, se consiguió una solución sólida, funcional y con potencial real de aplicabilidad, que responde directamente a los retos actuales del cumplimiento normativo en un entorno digital cada vez más complejo.

Ilustración 1. Muestra de una de las herramientas como resultados del proyecto

5. Conclusiones

Este proyecto ha permitido profundizar en el Reglamento DORA y en la importancia de la resiliencia operativa digital en el sector financiero. En respuesta a un entorno cada vez más digital y con riesgos tecnológicos, se desarrolló una herramienta optimizada para facilitar y mejorar el análisis del cumplimiento normativo en entidades financieras, aportando eficiencia, estandarización y reducción de errores.

La herramienta se validó en un caso real de análisis GAP, lo que confirmó su utilidad práctica y permitió implementar mejoras continuas. Además, el proyecto favoreció a mi desarrollo profesional y de habilidades clave como el pensamiento crítico, la toma de decisiones técnicas y la gestión del tiempo, gracias a la autonomía otorgada y la combinación con otras responsabilidades profesionales.

Entre sus principales aportaciones destacan la creación de una solución replicable, la optimización del proceso de evaluación, la adaptación a requisitos de proveedores TIC y la mejora en la experiencia de consultoría, reconocida positivamente por el cliente.

Para el futuro, se propone mejorar la automatización en Excel, integrar la herramienta con plataformas avanzadas como ARCHER o Risk4All, y adaptar la metodología a otros marcos regulatorios, ampliando así su alcance y utilidad en el sector financiero. En conjunto, el proyecto establece una base sólida para versiones futuras más automatizadas e integradas, alineadas con la evolución normativa europea y las demandas del entorno digital.

6. Referencias

[1] U. Europea, «REGLAMENTO (UE) 2022/2554 DEL PARLAMENTO EUROPEO Y DEL CONSEJO,» 14 Diciembre 2022. [En línea]. Available: https://www.boe.es/doue/2022/333/L00001-00079.pdf.

IMPLEMENTATION OF DORA REGULATION IN THE FINANCIAL SECTOR: GAP ANALYSIS AND COMPLIANCE STRATEGY

Author: Barquero Jiménez, Sofía
Supervisor: Cedillo Martínez, Hugo
Collaborating Entity: SIA

ABSTRACT

This Master's Thesis addresses the application of the DORA regulation in a financial institution, developing an Excel tool to carry out a GAP analysis, which identifies areas of non-compliance. From this analysis, a customized roadmap is designed with prioritized corrective actions to ensure ongoing compliance.

Keywords: DORA Regulation, financial institution, Excel, automation, GAP analysis, regulatory compliance, corrective measures, action plan.

1. Introduction

This Master's Thesis aims to implement the DORA regulation [1] in a financial entity, combining a regulatory analysis with a diagnosis of its current situation. An Excel tool will be developed to perform GAP analysis, identifying non-compliances and prioritizing corrective measures.

The project includes several key stages: initial diagnosis, updating internal policies, implementation of technologies, specialized training in operational resilience and tests to assess the robustness of the systems. As a result, a customized roadmap will be developed that ensures initial regulatory compliance, fosters long-term sustainability, and strengthens the organization's digital resilience.

2. Project definition

The main objective to be achieved is to implement the DORA regulation in a financial institution. This implementation will be obtained through an Excel tool for GAP analysis developed from scratch and applicable to any type of compliance projects with this regulation, which identifies non-compliance and prioritizes corrective measures. The project includes an initial diagnosis, policy update, adoption of technologies, operational resilience training and robustness testing. Finally, a customized roadmap is designed to ensure ongoing compliance and strengthen long-term digital resilience.

3. Description of the model/system/tool

The Excel tool developed for this project is designed to simplify GAP analysis and facilitate the implementation of the DORA regulation in financial entities. It allows filtering regulatory controls based on the type of entity, identifying the applicability of the controls, and tailoring the description of the requirements to the specific compliance needs of each case.

Additionally, the tool includes an automated system that generates a complementary file intended for the client. This file offers a more comprehensive and clear service, organizing recommended corrective actions into structured tables and presenting the information through interactive dashboards. This enables the client to easily monitor the current compliance status and track progress as corrective measures are implemented, simplifying the application and follow-up process.

Overall, the tool provides detailed analysis, flexibility in filtering, requirement differentiation, and a complementary service for the client, offering an efficient and practical solution to achieve and maintain regulatory compliance.

4. Results

Throughout the project, the greatest achievement has been the development of its own tool, designed from scratch with a totally practical approach and adapted to the analysis of compliance with the DORA Regulation in the financial environment. At first, the process was much more manual and generic and as the regulations and their real implications in the consulting work, as well as in the project that was being carried out, it was decided that it was necessary to create something more functional, more comfortable and oriented to meet specific needs. This is how this tool was born, which allows GAP analysis, requirements to be classified and ICT suppliers to be evaluated in a much more structured and agile way. In addition, by being able to apply it in a real case, we have had the opportunity to see what works well, what does not work so much, and how it can evolve. This has made it possible to adjust and improve the tool so that it not only fulfills its current purpose but is also prepared to be used in future projects, facilitating the work of the consultant, reducing time and avoiding errors. In short, beyond having met the objectives set, a solid, functional solution with real potential for applicability was achieved, which responds directly to the current challenges of regulatory compliance in an increasingly complex digital environment.

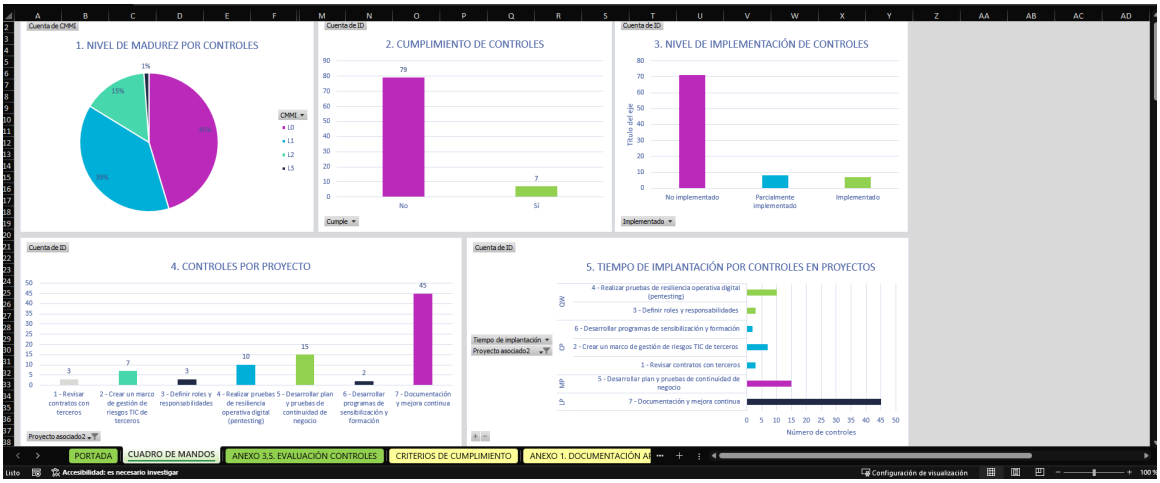


Ilustración 2. Sample of one of the tools as project outcomes

5. Conclusions

This project has allowed us to delve into the DORA Regulation and the importance of digital operational resilience in the financial sector. In response to an increasingly digital environment with technological risks, an optimized tool was developed to facilitate and improve the analysis of regulatory compliance in financial institutions, providing efficiency, standardization and error reduction.

The tool was validated in a real case of GAP analysis, which confirmed its practical usefulness and allowed continuous improvements to be implemented. In addition, the project favored my professional development and key skills such as critical thinking, technical decision-making and time management, thanks to the autonomy granted and the combination with other professional responsibilities.

Among its main contributions are the creation of a replicable solution, the optimization of the evaluation process, the adaptation to the requirements of ICT providers and the improvement in the consulting experience, positively recognized by the client.

For the future, it is proposed to improve automation in Excel, integrate the tool with advanced platforms such as ARCHER or Risk4All, and adapt the methodology to other regulatory frameworks, thus expanding its scope and usefulness in the financial sector. Overall, the project lays a solid foundation for future more automated and integrated versions, aligned with European regulatory developments and the demands of the digital environment.

6. References

[1] European Union, «REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL,» 14 December 2022. [En línea]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554.

Índice de la memoria

Capítulo 1. Introducción ***7***
1.1 Motivación del proyecto 7

Capítulo 2. Recursos utilizados ***9***

Capítulo 3. Estado de la Cuestión ***11***

Capítulo 4. Definición del Trabajo ***13***
4.1 Justificación 13
4.1.1 La importancia del Reglamento DORA y sus implicaciones *13*
4.1.2 Objetivo del proyecto: optimización del cumplimiento y eficiencia en la evaluación ... *14*
4.2 Objetivos 15
4.3 Metodología 16
4.4 Planificación y Estimación Económica 17

Capítulo 5. Sistema/Modelo Desarrollado ***20***
5.1 Análisis de la normativa DORA 20
5.2 Diseño de un marco metodológico para la implementación de DORA 26
5.3 Análisis GAP de la entidad financiera 31
5.4 Plan de acción 35
5.5 Desarrollo de una herramienta Excel 38
5.5.1 Objetivos y utilidad *38*
5.5.2 Estructura y funcionalidades *40*

Capítulo 6. Análisis de Resultados ***54***

Capítulo 7. Conclusiones y Trabajos Futuros ***56***

Capítulo 8. Bibliografía ***58***

ANEXO A – Niveles de madurez modelo CMMI ***62***

ANEXO B – Criterios de cumplimiento DORA ***63***

ANEXO C – Código de automatización ***64***

ANEXO D - Tipos de Entidades Financieras ***68***

ANEXO E – Imágenes de la herramienta principal antigua ***71***

ANEXO F - Imágenes de la herramienta principal evolucionada ***77***

ANEXO G – Imágenes de la herramienta entregada al cliente ***89***

Índice de ilustraciones

Ilustración 1. Muestra de una de las herramientas como resultados del proyecto 10
Ilustración 2. Sample of one of the tools as project outcomes 13
Ilustración 3. Evolución de la normativa [4] 10
Ilustración 4. DORA 12
Ilustración 5. Los 5 pilares del DORA [22] 22
Ilustración 6. Comparación del cumplimiento de dos controles con igual nivel de madurez 33
Ilustración 7. Muestra de una de las herramientas como resultados del proyecto 54
Ilustración 8. Pestaña GAP de herramienta antigua (I) 71
Ilustración 9. Pestaña GAP de herramienta antigua (II) 72
Ilustración 10. Pestaña CUADRO DE MANDOS de la herramienta antigua 73
Ilustración 11. Pestaña AUX de la herramienta antigua 74
Ilustración 12. Pestaña AUX DB de la herramienta antigua (I) 75
Ilustración 13. Pestaña AUX DB de la herramienta antigua (II) 76
Ilustración 14. Pestaña GAP de la herramienta evolucionada (I) 77
Ilustración 15. Pestaña GAP de la herramienta evolucionada (II) 78
Ilustración 16. Pestaña CUADRO DE MANDOS de la herramienta evolucionada 79
Ilustración 17. Pestaña AUX de la herramienta evolucionada 80
Ilustración 18. Pestaña AUX DB de la herramienta evolucionada (I) 81
Ilustración 19. Pestaña AUX DB de la herramienta evolucionada (II) 82
Ilustración 20. Pestaña Aplicabilidad de la herramienta evolucionada (I) 83
Ilustración 21. Pestaña Aplicabilidad de la herramienta evolucionada (II) 84
Ilustración 22. Pestaña Aplicabilidad de la herramienta evolucionada (III) 85
Ilustración 23. Pestaña Aplicabilidad de la herramienta evolucionada (IV) 86
Ilustración 24. Pestaña Aplicabilidad de la herramienta evolucionada (V) 87
Ilustración 25. Pestaña Aplicabilidad de la herramienta evolucionada (VI) 88
Ilustración 26. Portada de la herramienta entregada al cliente 89
Ilustración 27. Pestaña CUADRO DE MANDOS de la herramienta entregada 90

Ilustración 28. Pestaña EVALUACIÓN DE CONTROLES de la herramienta entregada al cliente 91
Ilustración 29. Pestaña CRITERIOS DE CUMPLIMIENTO de la herramienta entregada al cliente 92
Ilustración 30. Pestaña CONTROLES N.A. de la herramienta entregada al cliente..... 93
Ilustración 31. Pestaña DESGLOSE POR PROYECTO de la herramienta entregada al cliente 94
Ilustración 32. Pestaña Aux de la herramienta entregada al cliente 95

Índice de figuras

Figura 1. Diagrama Gantt del desarrollo del proyecto 19
Figura 2. Cumplimiento de controles del cliente evaluado 33
Figura 3. Promedio de nivel de madurez según el ámbito del DORA 34

Índice de tablas

Tabla 1. Relación entre el DORA y los RTS, ITS y Guías 28
Tabla 2. Proyectos plan de acción 37
Tabla 3. Niveles de madurez del modelo CMMI 62
Tabla 4. Criterios de cumplimiento de DORA 63
Tabla 5. Listado de descripciones de herramientas según su aplicabilidad (I)..... 68
Tabla 6. Listado de descripciones de herramientas según su aplicabilidad (II) 69
Tabla 7. Listado de descripciones de entidades según su aplicabilidad (III) 70

Capítulo 1. INTRODUCCIÓN

Este Trabajo de Fin de Máster tiene como objetivo principal la implementación de la regulación DORA (*Digital Operational Resilience Act*) [1] en el contexto de una entidad financiera específica, combinando un análisis exhaustivo de la normativa con un estudio pormenorizado de la situación actual del cliente.

La propuesta metodológica incluye el desarrollo de una herramienta en Excel diseñada específicamente para realizar un análisis GAP detallado. Esta herramienta facilitará la identificación de áreas de incumplimiento respecto a los requerimientos establecidos en la normativa, permitiendo proponer medidas correctivas priorizadas en función de su relevancia y urgencia.

El alcance del proyecto abarca varias etapas clave, comenzando con un diagnóstico inicial integral de los procesos, tecnologías y políticas actuales de la entidad. Posteriormente, se definirá un plan de acción estructurado que incluirá actividades como la actualización y alineación de políticas internas, la implementación de nuevas soluciones tecnológicas, la capacitación especializada del personal en temas de resiliencia operativa y la realización de pruebas rigurosas para evaluar la robustez de los sistemas frente a posibles interrupciones.

Finalmente, el proyecto culminará en la elaboración de una hoja de ruta personalizada que no solo garantizará el cumplimiento inicial de la normativa, sino que también establecerá un marco sostenible para el cumplimiento continuo, adaptándose a las futuras actualizaciones regulatorias y fortaleciendo la resiliencia digital de la organización a largo plazo.

1.1 MOTIVACIÓN DEL PROYECTO

La motivación de este trabajo nace de la importancia y urgencia que este nuevo marco normativo representa en el sector financiero, y la necesidad de llevar a cabo el cumplimiento adecuado dada la entrada en vigor del 17 de enero de 2025.

Las entidades financieras, como se listan y definen en el reglamento, deberán cumplir con nuevos requisitos relacionados con la resiliencia operativa digital y así poder abordar las inconsistencias y limitaciones presentes en las directrices existentes dentro del sector financiero. DORA surge como una solución para armonizar estas normativas, proporcionando un marco integral que permita gestionar de manera más efectiva los riesgos TIC y reforzar la resiliencia operativa digital. Desde el punto de vista de una consultora, es esencial contar con herramientas y estrategias claras para ayudar a los clientes en este proceso. Este trabajo no solo permitirá analizar cómo aplicar DORA en un caso específico, sino también crear una metodología que pueda usarse y aplicarse con futuros clientes de la misma categoría. De esta forma, se podrán desarrollar proyectos que ofrezcan soluciones prácticas, planes de acción detallados y asesoramiento adecuado y personalizado para garantizar que las organizaciones cumplan con esta normativa a tiempo.

Capítulo 2. RECURSOS UTILIZADOS

Los recursos empleados se centran en herramientas y medios clave que permitirán llevar a cabo las distintas fases del proyecto de manera eficiente.

En primer lugar, se utilizará Microsoft Excel como la base principal para desarrollar la herramienta de análisis GAP, la cual permitirá identificar discrepancias entre la situación actual de la entidad financiera y los requisitos establecidos por el reglamento DORA. Esta herramienta no solo facilitará la evaluación inicial, sino que también servirá como soporte para priorizar acciones correctivas y monitorear avances.

Además, para la realización del análisis detallado de las normativas aplicables, se emplearán el reglamento DORA [1] y sus Normas Técnicas de Regulación (RTS,*Regulation Technical Standards*) y Normas Técnicas de Implementación (ITS, *Implementation Technology Standards*), que detallan y complementan la regulación. Los RTS especifican requisitos técnicos sobre procedimientos, metodologías y medidas para lograr la resiliencia operativa, mientras que los ITS establecen formatos y procedimientos prácticos, como informes de incidentes o pruebas de resiliencia. Estas normas se publicaron en dos fases. La primera fue lanzada el 17 de enero de 2024, y abordan los siguientes marcos [2]:

- Normas Técnicas de Regulación (RTS) sobre el marco de gestión del riesgo de las TIC y sobre el marco simplificado de gestión del riesgo de las TIC;
- RTS sobre criterios para la clasificación de incidentes relacionados con las TIC;
- RTS para especificar la política sobre los servicios de TIC que respaldan funciones críticas o importantes prestados por proveedores de servicios de TIC (TPP); y
- Implementación de Normas Técnicas (ITS) para establecer las plantillas para el registro de información.

La segunda tanda de normas fue publicada el 17 de julio de 2024, abordando los siguientes asuntos [3]:

- RTS e ITS sobre el contenido, el formato, las plantillas y los plazos para informar sobre incidentes graves relacionados con las TIC y amenazas cibernéticas significativas;
- RTS sobre la armonización de las condiciones que permiten la realización de las actividades de supervisión;
- RTS que especifica los criterios para determinar la composición del equipo de examen conjunto (JET);
- RTS en pruebas de penetración dirigidas por amenazas (TLPT).
- Directrices sobre la estimación de los costos/pérdidas agregadas causados por incidentes graves relacionados con las TIC; y
- Directrices sobre la cooperación en materia de supervisión.

Además, posterior a esta segunda tanda de normas técnicas de regulación y directrices, se publicó un último RTS el 26 de julio de 2024 especificando los elementos que una entidad financiera debe determinar y evaluar cuándo subcontratar servicios de TIC que respaldan funciones críticas o importantes

Estos marcos normativos proporcionarán la base para entender las obligaciones regulatorias y definir las técnicas necesarias para su implementación.

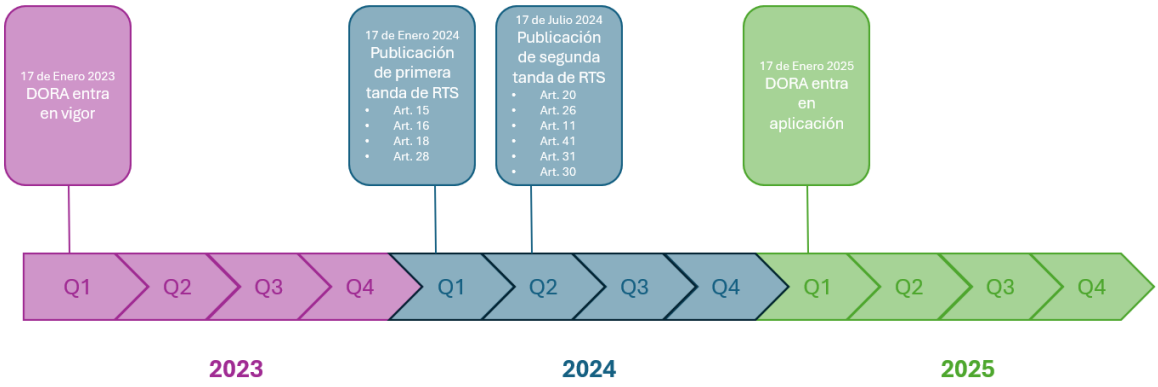


Ilustración 3. Evolución de la normativa [4]

Capítulo 3. ESTADO DE LA CUESTIÓN

La regulación en las entidades financieras ha evolucionado significativamente en las últimas décadas, con un enfoque creciente en garantizar la estabilidad, la seguridad y la resiliencia operativa de un sector clave para la economía global. Antes de la introducción del Reglamento DORA (*Digital Operational Resilience Act*), ya existían algunos marcos regulatorios específicos desarrollados por las Autoridades Europeas de Supervisión, siendo estas la EBA (*European Banking Authority)* [5], la EIOPA (*European Insurance and Occupational Pensions Authority)* [6] y la ESMA (*European Securities and Markets Authority*) [7], que proporcionaban un marco para gestionar aspectos clave de los riesgos tecnológicos.

Por un lado, la EBA pretende establecer un único marco regulador estableciendo medidas de gestión de riesgos TIC y de seguridad en las actividades y servicios de pago mediante directrices como las EBA/GL/2019/04 [8]. La EIOPA aborda la seguridad y supervisión de seguros y pensiones a través de guías como las EIOPA-BoS-20/600 [9]. Por su parte, ESMA desarrollaba normativas específicas para la externalización de servicios a proveedores en la nube, como las ESMA50-164-4285 [10]. Estas normativas han establecido una base sólida para la regulación financiera, abarcando aspectos como la solvencia, la gestión de riesgos y la protección al cliente. Además, este marco regulativo del sector financiero se ha visto de igual manera influenciado por otras regulaciones internas de la Unión Europea entre las que se incluyen el Reglamento NIS, que establece un alto nivel de seguridad en redes y sistemas de información [11]; el GDPR, que regula el tratamiento de datos personales [12]; el MiFID II, enfocado en la transparencia y protección de los inversores en los mercados financieros [13]; y regulaciones como el CRR [14] y el CRD IV [15] aseguran la estabilidad de las entidades de crédito, mientras que directrices como las PSD2 [16] y SIPS [17] refuerzan los sistemas de pagos críticos. En el ámbito externo, normativas internacionales como la Ley Sarbanes-Oxley (SOX), que promueve la transparencia financiera en Estados Unidos [18], y estándares como ISO 27001 y NIST, para la gestión de riesgos TIC y cibernéticos.

Sin embargo, con el rápido avance de la digitalización y el incremento de las amenazas cibernéticas, se ha requerido de un marco unificado y armonizado que abordare específicamente la resiliencia operativa digital.

DORA surge como una solución a esta división de requerimientos, integrando y fortaleciendo los estándares de las normativas preexistentes bajo un marco único y coherente, cuyo objetivo es asegurar que las entidades financieras de todos los tamaños puedan resistir, recuperarse y adaptarse a los riesgos digitales, estableciendo requisitos armonizados en áreas como la gestión de riesgos tecnológicos, la gestión y notificación de incidentes, la gobernanza tecnológica y la gestión de los riesgos relacionados con los proveedores terceros de servicios tecnológicos. Al ser supervisada por las mismas Autoridades Europeas de Supervisión que desarrollaron las normativas previas, DORA no solo alinea y consolida estos estándares, sino que también introduce normas técnicas de regulación que facilitan su implementación uniforme en toda la Unión Europea.

Con DORA, se busca no solo mejorar la capacidad de respuesta ante incidentes tecnológicos, sino también fomentar un entorno más seguro y confiable, promoviendo la estabilidad del sistema financiero europeo en su conjunto.

Ilustración 4. DORA

Capítulo 4. DEFINICIÓN DEL TRABAJO

4.1 JUSTIFICACIÓN

Como ya se ha mencionado en apartados anteriores, en el sector financiero se considera un pilar fundamental la tecnología por lo que garantizar la resiliencia operativa se ha convertido en una prioridad estratégica. El aumento y sofisticación de las ciberamenazas y la alta dependencia de infraestructuras digitales llevaron a la Unión Europea al desarrollo del Reglamento DORA, entre otras, una normativa clave que exige a las entidades financieras y sus proveedores tecnológicos implementar medidas robustas para prevenir, resistir y recuperarse de incidentes disruptivos. El cumplimiento por parte de las entidades financieras de este reglamento permitirá, además de minimizar los riesgos operativos, proteger la estabilidad del sistema financiero y reforzar la confianza de clientes y socios comerciales en la seguridad de los servicios digitales. Para la correcta implementación se requiere un enfoque estructurado, metodologías eficientes y herramientas especializadas que faciliten tanto la evaluación del cumplimiento como la aplicación de medidas correctivas.

4.1.1 LA IMPORTANCIA DEL REGLAMENTO DORA Y SUS IMPLICACIONES

El Reglamento DORA establece un marco normativo diseñado para garantizar la resiliencia digital de las entidades financieras mediante la gestión de riesgos tecnológicos, la gestión de incidentes y la supervisión de terceros proveedores. Su objetivo principal es evitar que incidentes TIC puedan afectar la estabilidad del sector financiero, asegurando la continuidad operativa incluso ante ataques o fallos tecnológicos imprevistos. La normativa exige que las organizaciones adopten estrategias proactivas además de desarrollar y centrarse en el desarrollo de planes de recuperación y respaldo, implementando controles estrictos sobre la seguridad de la información, pruebas de estrés operativas y planes de contingencia efectivos [19]. Su cumplimiento no solo es una obligación regulatoria, sino que también representa una ventaja competitiva al fortalecer la confianza del mercado y permitir a las empresas adoptar nuevas tecnologías con menores riesgos.

4.1.1.1 Consecuencias del incumplimiento y necesidad de un enfoque estructurad

No cumplir con DORA puede acarrear graves consecuencias tanto económicas como reputacionales. Las sanciones financieras impuestas a las entidades que no garanticen la resiliencia de sus sistemas pueden ser significativas, afectando su rentabilidad y sostenibilidad en el mercado. Además, la pérdida de confianza por parte de clientes y reguladores puede generar un impacto aún mayor, poniendo en riesgo la viabilidad de la organización a largo plazo [20]. Para evitar estas situaciones, es se necesitará adoptar un enfoque estructurado que permita evaluar con precisión el nivel de cumplimiento del reglamento, identificando áreas de mejora y aplicando planes de acción efectivos. Sin herramientas adecuadas, este proceso puede volverse complejo y difícil de gestionar, lo que aumenta el riesgo de errores, ineficiencias y omisiones en la implementación de medidas correctivas.

4.1.2 OBJETIVO DEL PROYECTO: OPTIMIZACIÓN DEL CUMPLIMIENTO Y EFICIENCIA EN LA EVALUACIÓN

Este proyecto tiene como objetivo principal desarrollar una metodología de trabajo a través de una herramienta dedicada que permita a los consultores evaluar, monitorizar y mejorar el cumplimiento de DORA de forma eficiente y automatizada. La solución propuesta facilitará la identificación de brechas en el cumplimiento normativo, la implementación de medidas correctivas y el seguimiento del progreso en tiempo real. Gracias a la integración de procesos automatizados, se reducirá el margen de error y se optimizará el tiempo de trabajo, permitiendo a los consultores centrarse en actividades de mayor valor añadido. Además, esta metodología estructurada garantizará la replicabilidad del proceso en diferentes organizaciones, asegurando un cumplimiento normativo coherente y sostenible a largo plazo. Las organizaciones que logren adaptarse a estos cambios estarán en una posición más favorable para crecer y sobresalir en un entorno digital y desafiante en constante evolución. [21]. En definitiva, la implementación de esta herramienta representa un paso clave en la optimización del trabajo de los consultores, garantizando un cumplimiento eficiente del Reglamento DORA y fortaleciendo la resiliencia operativa de las entidades financieras.

4.2 OBJETIVOS

Como ya se ha mencionado en los apartados anteriores, el objetivo principal es explorar la aplicabilidad de esta normativa en un caso concreto, desarrollando herramientas y metodologías que permitan a las organizaciones cumplir con los nuevos requisitos, para no solo garantizar la adecuación de una entidad específica, sino también crear un modelo que pueda ser replicado en otras empresas. Esta meta final se podrá llevar a término con el cumplimiento de diferentes objetivos intermedios que irán aportando valor y avanzando gradualmente en la construcción del proyecto hasta alcanzar el resultado esperado:

1. **Analizar la normativa DORA y su aplicabilidad en el sector financiero para entender sus implicaciones prácticas**: antes de aterrizar la aplicabilidad del reglamento en un caso concreto, es preciso comprender los diferentes requisitos que puedan aplicar o no según el tipo de entidad financiera, así como tener un conocimiento general de todo lo que engloba el DORA, incluyendo sus normas técnicas de regulación.
2. **Diseñar un marco metodológico para la implementación de DORA en una entidad financiera específica:** una vez analizada en profundidad la normativa y las características de la entidad financiera con la que se va a trabajar es preciso adaptar las necesidades del reglamento al tipo y tamaño de la entidad, aplicando el principio de proporcionalidad en el que se basa el DORA.
3. **Diseñar e implementar una herramienta en Excel para identificar áreas de incumplimiento y priorizar acciones correctivas:** Esta herramienta se desarrollará para facilitar la identificación de los aspectos en los que la entidad no cumple con los requisitos de DORA. A través de un análisis detallado, la herramienta permitirá visualizar claramente las brechas de cumplimiento y asignar prioridades a las acciones correctivas necesarias, de acuerdo con su urgencia y relevancia. Su implementación proporcionará una forma eficiente de gestionar las tareas de adaptación al reglamento.
4. **Evaluar la situación actual de una entidad financiera en relación con los requerimientos de DORA mediante un análisis GAP**: Realizar un análisis GAP

con la ayuda de la herramienta Excel es esencial para conocer las diferencias entre el estado actual de la entidad y los requisitos que impone DORA. Este análisis permitirá identificar las áreas en las que la entidad no está preparada para cumplir con la normativa, facilitando la priorización de recursos y esfuerzos en las áreas críticas que necesitan ser ajustadas para alcanzar el cumplimiento.

5. **Crear un plan de acción que contemple la actualización de políticas, la adopción de nuevas tecnologías, la formación de personal y la realización de pruebas de resiliencia:** Este plan incluirá las acciones necesarias para cumplir con DORA, como actualizar las políticas internas, implementar tecnologías adecuadas, capacitar al personal y realizar pruebas para asegurar la resiliencia operativa ante posibles incidentes.
6. **Crear un modelo operativo que pueda replicarse y adaptarse para ayudar a otros clientes en el cumplimiento de DORA**: en base a la herramienta desarrollada, se creará un modelo operativo adaptable que sirva como guía para que la consultora pueda replicar el enfoque en otros clientes, optimizando los recursos y facilitando y adaptando el cumplimiento de DORA en diversas entidades financieras.

4.3 METODOLOGÍA

La metodología que se seguirá en este Trabajo de Fin de Máster se divide en varias etapas que permitirán desarrollar un enfoque claro y completo para cumplir con los objetivos planteados.

Primero, se realizó un estudio detallado de la normativa DORA, incluyendo sus Normas Técnicas de Regulación (RTS por sus siglas en inglés, *Regulatory Technical Standards*) y Normas Técnicas de Implementación (ITS, *Implementing Technical Standards*), con el fin de entender sus requisitos y cómo aplicarlos al sector financiero. A continuación, se analizarán las características específicas de la entidad financiera seleccionada, evaluando su situación actual respecto a los estándares y obligaciones que establece el DORA. Este paso permitirá identificar tanto sus puntos fuertes como las áreas que necesitan mejorar.

La base principal del trabajo será la realización del análisis GAP, haciendo uso de la herramienta creada en Excel, para así identificar las diferencias entre el estado actual de la entidad y lo que exige el reglamento. A lo largo del proyecto, se irá mejorando dicha herramienta para ajustar y adaptar mejor a las necesidades de diferentes tipos de clientes para así garantizar la eficacia y adaptabilidad de esta.

Una vez completado este análisis GAP, se desarrollará un plan de acción claro y específico para la entidad financiera, incluyendo pasos concretos como la actualización de políticas internas, la adopción de nuevas tecnologías, la formación del personal y la realización de pruebas de resiliencia. Este plan estará diseñado para garantizar el cumplimiento de DORA y fortalecer la capacidad de la entidad para enfrentar posibles desafíos tecnológicos en el futuro. Con este enfoque, el proyecto no solo ayudará al cliente a adaptarse a la normativa, sino que también sentará las bases para aplicarlo en otros casos similares.

Finalmente, todo este recorrido sería plasmado en la presente memoria los últimos meses del curso, recogiendo así el desarrollo de las diferentes fases del proyecto.

4.4 PLANIFICACIÓN Y ESTIMACIÓN ECONÓMICA

Para la ejecución del presente Trabajo de Fin de Máster, se estableció una planificación estructurada que abarcó desde el análisis inicial del marco regulatorio hasta la elaboración de la memoria final. El desarrollo se llevó a cabo en diferentes fases distribuidas entre 2024 y 2025, asegurando una implementación ordenada y progresiva. Este proyecto se ha desarrollado en el marco de una beca de prácticas en la empresa SIA, compañía de ciberseguridad de la empresa INDRA, en el departamento de GRC (*Governance, Risk & Compliance,* o Gobierno, Riesgo y Cumplimiento), lo que ha permitido acceder tanto al proyecto como al cliente y su información, así como al material necesario para su desarrollo. Gracias a ello, se ha podido trabajar de manera directa en el análisis de la normativa DORA y su aplicación en un entorno real, asegurando que el enfoque adoptado respondiera a las necesidades y particularidades del cliente y permita posteriormente replicar la metodología en futuros proyectos de la compañía.

La primera fase, comprendida entre junio y septiembre de 2024, estuvo dedicada al análisis del reglamento, con el objetivo de comprender en detalle los requisitos de la normativa DORA, y los de los RTSs e ITSs y sus implicaciones para los diferentes tipos de entidades financieras. Paralelamente, entre agosto y octubre, se definió un marco metodológico específico para el cliente del proyecto, sentando las bases para el desarrollo del mismo y haciendo un análisis de la situación del cliente para así identificar la aplicabilidad de los controles identificados en el reglamento.

El diseño de la herramienta en Excel fue un trabajo continuo a lo largo del proyecto. En una primera etapa, entre julio y octubre de 2024, es decir, durante la definición del marco metodológico que se realizó previo al desarrollo del proyecto, se centró en adaptarse a las necesidades específicas del estudio, asegurando que respondiera a los objetivos planteados para el cliente. Posteriormente, tras aplicar la herramienta en el análisis GAP que duró durante octubre y noviembre, se identificaron mejoras y oportunidades de optimización, lo que llevó a una evolución de esta hasta enero de 2025, garantizando que la herramienta no solo cumpliera su función inicial, sino que también incorporara aprendizajes clave derivados de su aplicación práctica para permitir su utilización en diferentes proyectos centrados en el reglamento DORA.

Como se ha mencionado, en octubre y noviembre de 2024 se llevó a cabo el análisis GAP para la identificación del cumplimiento con respecto al reglamente que presentaba el cliente, lo que dio lugar al inicio de la fase del plan de acción que recogiese las recomendaciones y acciones correctivas proporcionadas al cliente abordar las brechas identificadas y concluir así el proyecto con este.

Finalmente, entre enero y junio de 2025, se llevó a cabo la elaboración de la memoria, documentando todo el proceso, los hallazgos y posibles futuros trabajos que permitan una evolución y una mejora del proceso.

Esta planificación permitió una ejecución estructurada del proyecto, garantizando que cada fase se desarrollara con el tiempo necesario para su correcta implementación y asegurando un enfoque integral en la adaptación a la normativa DORA. Toda la evolución viene recogida en el diagrama de Gantt mostrado en la Figura 1.

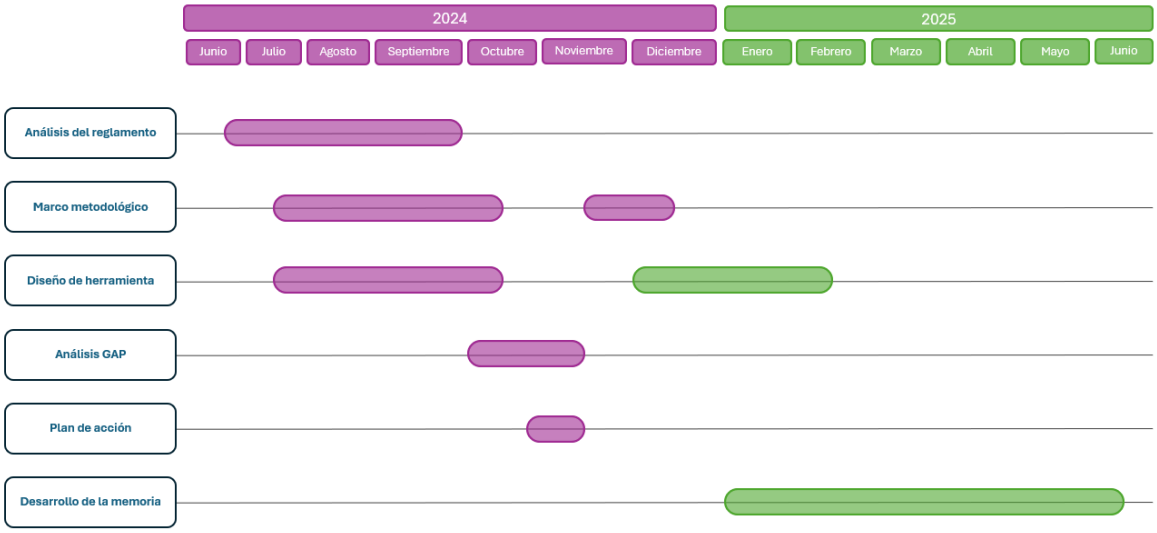


Figura 1. Diagrama Gantt del desarrollo del proyecto

Capítulo 5. SISTEMA/MODELO DESARROLLADO

Como se ha explicado en el apartado de Planificación y Estimación Económica, el desarrollo del proyecto ha seguido una evolución estructurada, permitiendo una adaptación progresiva a las necesidades del cliente y a los requisitos de la normativa DORA, que representa un marco esencial para fortalecer la resiliencia digital de las entidades financieras, exigiendo un cumplimiento riguroso en áreas clave como la gestión de riesgos TIC y la respuesta ante incidentes. A continuación, se desarrollarán y explicarán en detalle las diferentes fases del proyecto en el que se ha llevado a cabo un análisis detallado del reglamento, el diseño y perfeccionamiento de una herramienta específica para el análisis GAP, la identificación de brechas de cumplimiento de la entidad financiera cliente y la definición de un plan de acción para abordar las deficiencias detectadas y conseguir un cumplimiento adecuado del reglamento DORA. Este enfoque ha permitido no solo garantizar el cumplimiento inicial, sino también establecer una base sólida para la mejora continua y la adaptación a futuras actualizaciones normativas que permita reproducir el proceso cuando sea necesario.

5.1 ANÁLISIS DE LA NORMATIVA DORA

Como se ha explicado, la primera fase del proceso consistió en realizar un análisis detallado del reglamento, permitiendo identificar sus principales exigencias y su impacto en las entidades financieras. Esta fase inicial consistió en una revisión minuciosa de los artículos de la normativa, prestando especial atención a aquellos que presentan requisitos diferenciados según el tipo de entidad, como es el caso de las microempresas, que cuentan con ciertas flexibilidades en su aplicación. Además, se estudió la interrelación entre DORA y los RTS, identificando qué aspectos eran ampliados o complementados por estas normas técnicas para evitar redundancias y mejorar la claridad en la definición de los controles a cumplir, definidos posteriormente en el marco metodológico.

El Reglamento DORA es un reglamento internacional que establece un marco común para fortalecer la resiliencia operativa digital del sector financiero en toda la UE, aplicándose a

20 tipos diferentes de entidades financieras y proveedores terceros de servicios TIC, con objetivo de mejorar la ciberseguridad en este sector y garantizar que puedan prevenir, gestionar y recuperarse de incidentes relacionados con las tecnologías de la información y comunicación (TIC).

Las principales áreas de enfoque de DORA se dividen en cinco capítulos clave:

- **Gestión de riesgos de las TIC**: Principios y requisitos del marco de gestión de riesgos de las TIC en el que se debe incluir políticas y procedimientos para identificar, clasificar y evaluar continuamente los activos esenciales y los riesgos tecnológicos asociados, así como implementar medidas de ciberseguridad adecuadas para su mitigación. Además, es responsabilidad del órgano de dirección establecer las estrategias de gestión del riesgo y garantizar el control interno, pudiendo incluso asumir responsabilidad personal en caso de incumplimiento de la regulación.
- **Notificación de incidentes**: se debe implementar un proceso estandarizado para monitorear, gestionar, clasificar y notificar incidentes significativos relacionados con las TIC. Esto incluye la obligación de informar a las autoridades competentes, así como a los clientes y socios afectados, sobre cualquier incidente grave que pueda comprometer sus operaciones. La notificación debe realizarse a través de informes iniciales, intermedios y finales, con la opción de informar voluntariamente sobre incidentes importantes de menor impacto, facilitando así una respuesta rápida y coordinada ante incidentes de alto riesgo.
- **Pruebas de Resiliencia Operativa Digital**: Las entidades financieras deben realizar pruebas regulares de sus sistemas de TIC para evaluar su fortaleza y detectar posibles vulnerabilidades, garantizando así su resiliencia operativa digital. Estas pruebas incluyen evaluaciones de vulnerabilidades, simulacros de ciberataques, y pruebas de penetración basadas en escenarios específicos que simulan amenazas dirigidas al sector financiero. Además, las entidades deben establecer acuerdos para el intercambio de información e inteligencia sobre ciberamenazas y vulnerabilidades, especialmente en el caso de instituciones

grandes o esenciales, que pueden requerir evaluaciones adicionales por parte de terceros.

- **Gestión de Terceros Proveedores de TIC**: establece requisitos específicos para la gestión de terceros proveedores de servicios esenciales, como los proveedores de servicios en la nube. Las entidades financieras deben desempeñar un papel activo en la gestión de riesgos asociados a estos terceros, lo cual incluye la evaluación de riesgos, el monitoreo de su desempeño, y la implementación de planes de contingencia ante posibles interrupciones. También se requiere que establezcan acuerdos contractuales detallados y mapeen las dependencias en la cadena de suministro. Además, los proveedores de TIC esenciales estarán sujetos a supervisión directa y deberán cumplir con los requisitos estipulados en DORA.
- **Intercambios de información:** El intercambio seguro de información sobre ciberamenazas es crucial, y DORA promueve que las entidades financieras colaboren y compartan datos sobre incidentes para fortalecer la resiliencia del sector. Cumplir con estos principios es clave para la seguridad y continuidad operativa. Aunque no es obligatorio, DORA incentiva la cooperación entre instituciones de confianza para sensibilizar sobre riesgos TIC, limitar la propagación de amenazas y compartir estrategias defensivas y de mitigación.

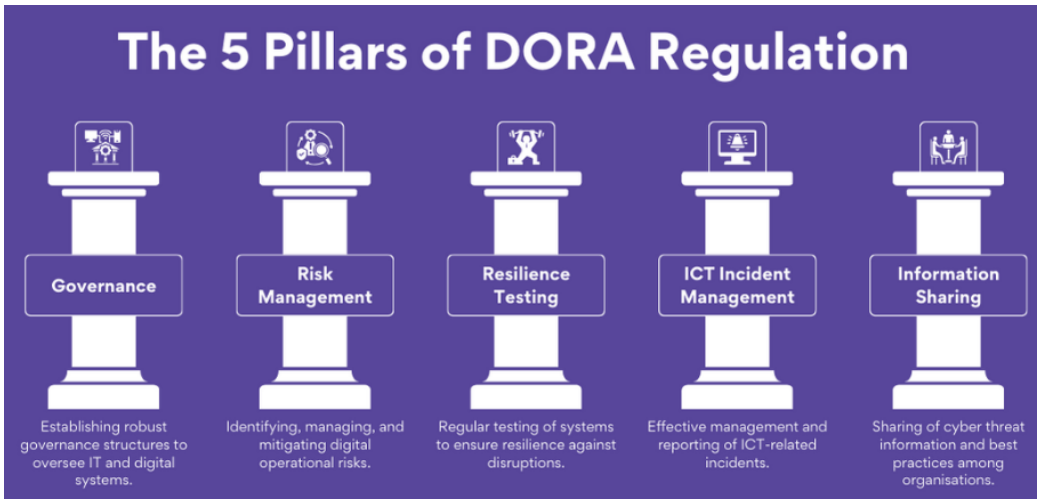


Ilustración 5. Los 5 pilares del DORA [22]

Un principio fundamental de DORA es el de **proporcionalidad**. Este establece que, al aplicar las normas de resiliencia operativa digital, deben considerarse las diferencias significativas entre las entidades financieras, en aspectos como su tamaño, perfil de riesgo general, así como la naturaleza, escala y complejidad de sus servicios, actividades y operaciones.

El reglamento DORA también deberá ser aplicable para los **proveedores de servicios TIC**, que deberán cumplir con los requisitos establecidos por DORA, incluyendo la implementación de controles sólidos de ciberseguridad, mecanismos efectivos de gestión de riesgos y protocolos para la continuidad operativa. Además, deberá someterse a auditorías regulares, garantizar la trazabilidad de sus operaciones y proporcionar informes transparentes a las entidades financieras sobre cualquier incidente que pueda comprometer la resiliencia operativa. Estos proveedores también deberán demostrar la capacidad de recuperarse rápidamente de interrupciones y colaborar estrechamente con sus clientes para mitigar riesgos sistémicos y cumplir con las obligaciones regulatorias. Por otro lado, DORA identifica a los proveedores críticos de servicios TIC como aquellas entidades externas que ofrecen servicios TIC fundamentales para las operaciones de las entidades financieras. Dada la importancia de sus servicios, estos proveedores son considerados piezas clave para la resiliencia operativa del sector financiero.

DORA impone a los **proveedores críticos** requisitos más estrictos para garantizar que su desempeño no comprometa la estabilidad del sistema financiero. Entre las obligaciones destacan:

1. **Supervisión reforzada:** Los proveedores esenciales estarán sujetos a una supervisión específica por parte de autoridades competentes designadas, que evaluarán su cumplimiento normativo y capacidad de gestión de riesgos.
2. **Planes de continuidad:** Deben contar con planes robustos para garantizar la disponibilidad y recuperación de servicios en caso de fallos o ataques cibernéticos.
3. **Evaluación de riesgos:** Es obligatorio identificar, gestionar y mitigar riesgos tecnológicos y operativos en tiempo real.

4. **Transparencia**: Están obligados a reportar incidentes significativos a las entidades financieras y, en algunos casos, a las autoridades regulatorias.

Tras la publicación del DORA y para garantizar su aplicación efectiva, era necesario un conjunto de normas técnicas detalladas. Los RTS (*Regulation Technical Standards)* e ITS *(Implementation Technical Standards)* complementan y precisan estos requisitos, proporcionando criterios específicos, formatos de reporte y procedimientos de supervisión, asegurando así una implementación armonizada y consistente en toda la Unión Europea. Estas normas se publicaron en dos fases. La primera fue lanzada el 17 de enero de 2024, y abordan los siguientes marcos [2]:

- **RTS sobre el marco de gestión del riesgo de las TIC y marco simplificado**: Establece los requisitos para que las entidades financieras implementen un marco robusto de gestión del riesgo de las TIC, con una versión simplificada para aquellas de menor tamaño o complejidad.
- **RTS sobre criterios para la clasificación de incidentes TIC**: Define los criterios para categorizar incidentes relacionados con las TIC según su gravedad, impacto y urgencia, asegurando una respuesta eficiente y armonizada.
- **RTS sobre la política de servicios TIC para funciones críticas**: Regula la forma en que las entidades deben gestionar y supervisar los servicios TIC proporcionados por terceros cuando estos apoyan funciones esenciales.
- **ITS sobre plantillas para el registro de información**: Proporciona formatos estandarizados para documentar y reportar información relevante sobre riesgos e incidentes TIC.

La segunda tanda de normas fue publicada el 17 de julio de 2024, abordando los siguientes asuntos [3]:

- **RTS e ITS sobre incidentes graves TIC y amenazas cibernéticas:** Especifican cómo deben estructurarse los informes sobre incidentes significativos y amenazas cibernéticas, incluyendo plazos y formatos de notificación.

- **RTS sobre armonización de actividades de supervisión**: Busca uniformar los criterios y procesos utilizados por las autoridades para supervisar el cumplimiento de DORA en diferentes jurisdicciones.
- **RTS sobre composición del equipo de examen conjunto (JET)**: Establece cómo deben formarse estos equipos de supervisión conjunta para evaluar el cumplimiento de DORA en entidades transfronterizas.
- **RTS sobre pruebas de penetración dirigidas por amenazas (TLPT)**: Define los requisitos y metodologías para la realización de pruebas de penetración avanzadas, evaluando la resistencia de las entidades ante ataques cibernéticos sofisticados.
- **Directrices sobre costos/pérdidas por incidentes graves TIC**: Proporciona un marco para estimar los daños financieros y operativos derivados de incidentes TIC importantes.
- **Directrices sobre cooperación en supervisión**: Detalla cómo las autoridades supervisoras deben colaborar y compartir información para garantizar una supervisión eficaz y coordinada.

Además, posterior a esta segunda tanda de normas técnicas de regulación y directrices, se publicó un último RTS el 26 de julio de 2024:

- **RTS sobre subcontratación de servicios TIC para funciones críticas**: Especifica los elementos clave que las entidades financieras deben evaluar y gestionar al subcontratar servicios TIC que respalden funciones esenciales, asegurando la mitigación de riesgos.

A partir del 17 de enero de 2025 las entidades financieras deberán cumplir todos los requisitos establecidos por el reglamento DORA y comenzarán las actividades de supervisión de las autoridades competentes.

5.2 DISEÑO DE UN MARCO METODOLÓGICO PARA LA IMPLEMENTACIÓN DE DORA

El diseño del marco metodológico para la implementación del DORA se llevó a cabo prácticamente de forma paralela al análisis exhaustivo del reglamento, con el objetivo de identificar los controles esenciales que deben cumplir las entidades financieras y los proveedores de servicios TIC. Este proceso comenzó con una revisión detallada de todo el reglamento, como se ha explicado en el apartado Análisis de la normativa DORA , prestando especial atención a aquellos artículos en los que los requisitos variaban según el tipo de entidad financiera. Por ejemplo, aplicando el principio de proporcionalidad, en el caso de las microempresas, DORA introduce ciertas flexibilidades en la aplicación de controles de seguridad y gestión del riesgo TIC, por lo que era fundamental diferenciar estos casos al elaborar el marco metodológico.

Además, se realizó un estudio de los RTS e ITS que completan el Reglamento para identificar aquellos artículos de DORA que eran ampliados o completados por estas normas técnicas. Para ello, se llevó a cabo un **mapeo detallado entre DORA y sus RTS/ITS**, lo que permitió:

- **Asegurar una correcta ampliación de los requisitos generales**, incorporando las especificaciones necesarias sin alterar el alcance normativo original.
- **Evitar redundancias**, consolidando la información de manera estructurada y clara.
- **Optimizar la definición de los controles**, facilitando su posterior aplicación en la evaluación GAP y en la elaboración del plan de acción.

Así, se conseguiría una metodología más precisa y alineada con el reglamento, asegurando que los controles reflejaran fielmente la totalidad de los requisitos que pide el DORA.
En la Tabla 1**¡Error! No se encuentra el origen de la referencia.** se recogen los títulos de los diferentes RTS, ITS y guías, los números de identificación establecidos al sacar los borradores, los artículos que complementan, y el número del Reglamento Delegado publicado por la UE correspondiente una vez oficializado cada documento. Esta última

característica se ha ido completando a lo largo de la elaboración del presente proyecto a medida que fuesen siendo publicados, si lo fueron.

Tanda	Título del RTS, ITS o Guía	Número identificativo	Artículo relacionado del DORA	Número oficial del Reglamento Delegado
Primera tanda	RTS sobre criterios para la clasificación de incidentes relacionados con las TIC	83	18. Clasificación de los incidentes relacionados con las TIC y las ciberamenazas	2024/1772
	RTS para especificar la política sobre los servicios de TIC que respaldan funciones críticas o importantes prestados por proveedores de servicios de TIC	84	28. Principios generales (de una buena gestión del riesgo relacionado con las TIC derivado de terceros)	2024/1773
	Implementación de Normas Técnicas (ITS) para establecer las plantillas para el registro de información.	85		2024/2956
	Normas Técnicas de Regulación (RTS) sobre el marco de gestión del riesgo de las TIC y sobre el marco simplificado de gestión del riesgo de las TIC	86	15. Mayor armonización de las herramientas, métodos, procesos y políticas de gestión del riesgo relacionado con las TIC 16. Marco simplificado de gestión del riesgo relacionado con las TIC	2024/1774
Segunda tanda	RTS e ITS sobre el contenido, el formato, las plantillas y los plazos para informar sobre incidentes graves relacionados con las TIC y amenazas cibernéticas significativas	33	19. Notificación de los incidentes graves relacionados con las TIC y notificación voluntaria de las ciberamenazas importantes	2025/301 2025/302
	RTS sobre la armonización de las condiciones que permiten la realización de las actividades de supervisión;	35	41. Armonización de las condiciones que permiten llevar a cabo las actividades de supervisión	2025/295
	RTS que especifica los criterios para determinar la composición del equipo de examen conjunto (JET)	54		-
	RTS en pruebas de penetración dirigidas por amenazas (TLPT).	29	26. Pruebas avanzadas de las herramientas, los sistemas y los procesos de TIC basadas en pruebas de penetración basadas en amenazas	-
	Directrices sobre la estimación de los costos/pérdidas agregadas causados por incidentes graves relacionados con las TIC	34	11. Respuesta y recuperación	-
	Directrices sobre la cooperación en materia de supervisión.	36	31. Designación de proveedores terceros esenciales de servicios de TIC	2024/1502
	RTS que especifica elementos a determinar y evaluar por entidades financieras al subcontratar servicios TIC que apoyen funciones esenciales o importantes	53	30. Cláusulas contractuales fundamentales	-

Tabla 1. Relación entre el DORA y los RTS, ITS y Guías

Este análisis fue esencial para garantizar que, en la descripción de cada control, los requisitos generales de DORA se complementaran correctamente con las especificaciones técnicas correspondientes, evitando lagunas interpretativas o ambigüedades en su aplicación

Debido a la urgencia del proyecto y al enfoque inicial en las necesidades particulares del cliente, la identificación de los controles se realizó de **manera preliminar**, con el objetivo de abordar los requisitos clave del reglamento de forma rápida y eficaz. Los controles identificados fueron agrupados inicialmente según su temática principal, lo que facilitó una organización provisional para la evaluación del cumplimiento en este primer contexto. Este enfoque permitió crear una estructura básica que se utilizaría posteriormente en la elaboración de la herramienta de análisis GAP, asegurando que el consultor pudiera realizar una evaluación efectiva de la situación del cliente.

Sin embargo, este proceso de identificación de controles fue solo el primer paso. Una vez terminado el proyecto con el cliente, el listado de controles se tomaría como base para llevar a cabo un análisis más detallado, con una mejor segregación de los requisitos según los diferentes tipos o tamaños de entidades financieras. La experiencia adquirida permitió identificar oportunidades de optimización en la identificación y clasificación de los controles, asegurando una mayor precisión en su aplicación a distintos tipos de entidades financieras. Este análisis permitirá distinguir los requisitos que aplican a cada entidad en función de su naturaleza y características operativas, garantizando una adaptación más precisa y personalizada a las especificidades de cada tipo de cliente.

Uno de los primeros pasos en esta fase fue la identificación de las entidades financieras sujetas a la regulación DORA, ya que algunas de ellas presentan particularidades en cuanto a la aplicación de los controles. Las entidades financieras afectadas por el DORA, además de los proveedores de servicios TIC, listadas como lo hace el reglamento son:

- Entidades de crédito
- Entidades de pago

- Proveedores de servicios de información sobre cuentas
- Entidades de dinero electrónico
- Empresas de servicios de inversión
- Proveedores de servicios de criptoactivos
- Depositarios centrales de valores
- Entidades de contrapartida central
- Centros de negociación
- Registros de operaciones
- Gestores de fondos de inversión alternativos
- Sociedades de gestión
- Proveedores de servicios de suministro de datos
- Empresas de seguros y de reaseguros
- Intermediarios de seguros, intermediarios de reaseguros e intermediarios de seguros complementarios
- Fondos de pensiones de empleo
- Agencias de calificación crediticia
- Administradores de índices de referencia cruciales
- Proveedores de servicios de financiación participativa
- Registros de titulizaciones

Las definiciones de estas entidades se han incluido en la Tabla 7 del ANEXO D - Tipos de Entidades Financieras, junto con las entidades financieras que no entran en el ámbito de aplicación del reglamento. Tener una visión clara de la definición de los tipos de entidades y de la clasificación de aplicabilidad ayudará a distinguir qué tipo de filtrado se debería aplicar en los controles sobre la organización de estudio.

Una vez identificadas estas entidades, se procedió a revisar y redefinir el listado de controles previamente elaborado. Se realizó un estudio detallado de cada control, analizando su aplicabilidad en función del tipo de entidad. Esto implicó no solo una segregación más precisa de los requisitos, sino también la adaptación de las descripciones de cada control para reflejar mejor su alcance y exigencias específicas.

Además del análisis de estas entidades, se llevó a cabo un estudio específico sobre el impacto del reglamento en los **proveedores de servicios TIC**. Aunque DORA no les impone requisitos de cumplimiento de manera directa como a las entidades financieras, sí exige que estos proveedores se alineen con los principios y estándares de resiliencia digital, dado que forman parte esencial del ecosistema financiero. Esto implica que deben cumplir con acuerdos contractuales estrictos en materia de gestión de riesgos, supervisión y notificación de incidentes, garantizando que los servicios que prestan no representen un punto de vulnerabilidad para las entidades reguladas. Algunas de las áreas en las que los proveedores deberán alinearse con el reglamento son:

- Implementación de **protocolos de ciberseguridad y gestión de riesgos TIC** compatibles con los requisitos de DORA.
- **Capacidad de respuesta ante incidentes**, con procedimientos claros de comunicación y escalado.
- **Garantías de continuidad de negocio y recuperación ante desastres** alineadas con los objetivos de resiliencia de las entidades financieras.
- **Obligaciones contractuales reforzadas**, con cláusulas que aseguren el cumplimiento de los controles necesarios por parte del proveedor.

Para ello, se desarrollaron descripciones diferenciadas que permitieron ajustar cada control a las características particulares de las distintas entidades financieras. Se identificaron escenarios en los que ciertos controles podían tener requerimientos más estrictos o, por el contrario, niveles de exigencia más flexibles, dependiendo del tipo de entidad o de la criticidad de los servicios prestados. Así, durante este proceso, se implementaron cambios en la formulación y documentación de los controles, asegurando que cada uno contara con una descripción clara, detallada y alineada con las exigencias regulatorias de DORA. Además, se hizo una final agrupación de controles, basadas en la agrupación que se haría a la hora de elaborar el plan de acción para proponer acciones recomendadas al cliente.

Finalmente, esta mejora metodológica permitió no solo una mejor adaptación a las necesidades del cliente inicial, sino también el establecimiento de una mejorada base sólida y replicable para futuros proyectos. A partir de esta nueva estructura, se podrá abordar de

manera más eficiente el cumplimiento normativo de diferentes tipos de entidades financieras y garantizar que los proveedores de servicios TIC estén alineados con los estándares exigidos, minimizando los riesgos asociados a la externalización de servicios críticos. Además, esta optimización impactó directamente en la herramienta de Excel diseñada para el análisis GAP, mejorando su capacidad para clasificar los controles según la entidad correspondiente y facilitando el trabajo de los consultores en futuras evaluaciones. Con ello, se logró una metodología más estructurada y adaptable, que permitirá agilizar el análisis y la toma de decisiones en próximos proyectos dentro de este ámbito.

5.3 ANÁLISIS GAP DE LA ENTIDAD FINANCIERA

Previo a la realización del análisis GAP, se debía realizar un estudio del tipo de entidad financiera que representaba el cliente y de las posibles exenciones a las que se enfrentaría en caso de cumplir con las características de ciertos tipos de organizaciones.

La empresa cliente era una entidad financiera que contaba con un número de empleados muy reducido, lo que podría haber llevado a la clasificación de esta como microempresa. Sin embargo, el volumen de facturación y otras características de la empresa hicieron descartar esta posibilidad, entre otras, lo que dejó como conclusión que su naturaleza entraría en la categoría de entidad financiera "general", aplicándole los controles que el reglamento requiere que cumplan todo tipo de entidades financieras.

Una vez aclarada la situación del cliente, se creó una clasificación eficiente de los controles a analizar para posteriormente discutirlos en diferentes reuniones que se llevaron a cabo con distintos equipos de la empresa y así discutir la aplicabilidad según el ámbito de forma eficaz y ordenada. Durante estas reuniones, se solicitó una serie de evidencias documentales que agregarían detalle para evaluar el cumplimiento de los requisitos de DORA. Este análisis reveló que, en la situación actual, el cliente cumplía con un número limitado de controles, mientras que muchos otros no se encontraban implementados o eran insuficientemente desarrollados. Este diagnóstico inicial permitió identificar las principales áreas de mejora y

el nivel de brecha que existía entre la situación actual y el cumplimiento total de los requisitos.

Para la evaluación del cumplimiento del reglamento, se usó como metodología el **modelo de madurez CMMI** (*Capability Maturity Model Integration*) para evaluar el nivel de cumplimiento de los controles. Sin embargo, debido a la diversidad de los controles y la naturaleza específica de cada uno, fue necesario realizar un estudio previo sobre los requisitos de cada control para establecer un nivel mínimo de cumplimiento adecuado. Así, se definió que no todos los controles debían alcanzar el mismo nivel de madurez, ya que algunos podrían considerarse cumplidos con un nivel de madurez más bajo (por ejemplo, L2) en ciertas circunstancias, mientras que otros requerían un nivel más alto, como L3, por requerir estar documentados. La descripción de los distintos niveles de madurez y de los criterios de cumplimiento basados en los niveles de madurez establecidos vienen recogidos en el ANEXO A – Niveles de madurez modelo CMMI y en el ANEXO B – Criterios de cumplimiento DORA, respectivamente.

En la Ilustración 6 se muestra una porción de la herramienta que se proporcionó al cliente una vez terminado el análisis de su situación de cumplimiento, en el que se muestra la comparativa de dos controles cuyo nivel de madurez es L2, pero uno se considera que lo cumple y está implementado mientras el segundo no. Esto ilustra cómo en algunos controles, un nivel L2 podría indicar que el control estaba parcialmente implementado y, por lo tanto, cumplía con el requisito en cierta medida, aunque hubiese capacidad de mejora la cual luego se recomendaba en la "Acción recomendada", mientras que, en otros casos, ese mismo nivel indicaba que el control aún no era suficiente para garantizar el cumplimiento completo. Esto generó la necesidad de una evaluación diferenciada para cada control, adaptada a su contexto y naturaleza, asegurando que el cliente tuviera una visión clara de qué áreas requerían más trabajo para alcanzar un cumplimiento total. Esta necesidad fue identificada durante la realización del proyecto, lo que aportó un punto de mejora para la herramienta que se tendría en cuenta para incluirlo posteriormente.

Título	Estado Actual	Acción recomendada	Referencia en el reglamento	CMMI	Cumple	Nivel de implementación
Cartografiado de la configuración de los activos	Utilizan como herramienta de gestión de activos: - Consola de Sophos - Consola de MS Defender (O365) donde se gestionan la gestión de identidades y correo electrónico(DLP). Tienen implementado 2FA. Tienen permitido el uso de USB.	Incluir en la documentación de la identificacion y clasificación de activos la cartografía de la configuración de los activos, incluidos los que se encuentren en emplazamientos remotos, recursos de red y equipos de hardware, y cartografiarán aquellos considerados esenciales.	DORA, Artículo 8, apartado 4(página 32)	L2	Sí	Implementado
Documentación de procesos de terceros	Tinene identificados los proveedores TIC y su clasificación de Esenciales y No Esenciales a través de un Excel informal. Aplicación BIA tienen documentada proveedores MS cumple con DORA Y Bloomberg (creen que si) Hay que hacer analisis de risgos con los proveedores.	Generar documentación formal de los procesos que dependan de terceros, así como las interconexiones con ellos que sustenten funciones esenciales.	DORA, Artículo 8, apartado 5(página 32)	L2	No	Parcialmente implementado

Ilustración 6. Comparación del cumplimiento de dos controles con igual nivel de madurez

La situación actual del cliente reveló un alto nivel de cumplimiento en los controles identificados. Originalmente, se habían identificado 121 controles que, debido a este incumplimiento, se decidieron agrupar con el objetivo de unificar las medidas correctivas que estuvieran relacionadas, resultando en un total de 86 controles únicos.

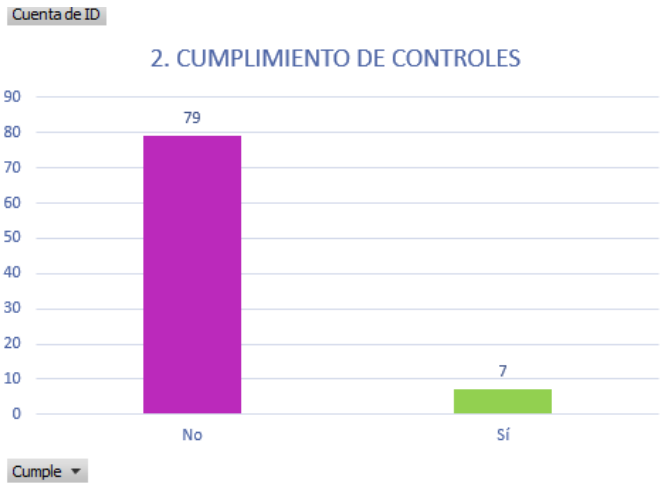


Figura 2. Cumplimiento de controles del cliente evaluado

Una vez identificada esa situación actual, se estableció como **estado objetivo** un nivel de madurez L3. A pesar de que, como ya se ha explicado, algunos controles pudieran considerase que cumplen con el reglamento DORA con un nivel L2, se recomendó llegar a este nivel de madurez superior con el objetivo de definir y documentar de mejor manera los procesos de resiliencia operativa de la organización y así además aportar mayor facilidad a la hora de demostrarlo en posibles evaluaciones de las Autoridades Competentes.

Figura 3. Promedio de nivel de madurez según el ámbito del DORA

Además del estudio del nivel de madurez y cumplimiento de cada uno de los controles, se evaluó de igual manera el **nivel de implementación** de cada uno de los controles en función del estado actual dentro de la entidad:

- **Implementado**: El control está completamente desarrollado y en funcionamiento.
- **Parcialmente implementado**: Existen elementos del control en uso, pero no cumple completamente con los requisitos de DORA.
- **No implementado**: No se ha iniciado la implantación del control o su existencia es meramente teórica.

Adicionalmente, se incorporó un tercer criterio clave para facilitar la planificación del cumplimiento: una **estimación del tiempo** necesario para implementar cada control. Esta clasificación se estructuró en cuatro categorías:

- **QW (Quick Win)**: Implementable en menos de un mes.
- **CP (Corto Plazo)**: Requiere aproximadamente un mes.
- **MP (Medio Plazo)**: Requiere entre 2 y 3 meses.
- **LP (Largo Plazo)**: Su implementación supera los 3 meses.

Con el objetivo de ayudar al cliente a cumplir con el reglamento y fortalecer su resiliencia operativa digital, evitando posibles sanciones económicas, se elaboró un plan de acción específico y detallado para abordar y corregir las áreas de incumplimiento del Reglamento

DORA que estaría basado en los tres criterios de evaluación explicados De esta manera, se proporciona una visión estratégica para la priorización de medidas correctivas y optimizar la aplicación del plan de acción, diferenciando aquellas medidas que ya estaban en marcha y solo requerían ajustes, de aquellas que aún no habían sido abordadas y supondrían un mayor esfuerzo de implementación

5.4 PLAN DE ACCIÓN

A partir de los resultados obtenidos en el análisis GAP, se procedió a la elaboración de un plan de acción personalizado para el cliente que permitiera abordar de manera eficiente las medidas correctivas necesarias para alcanzar el cumplimiento de DORA. Un primer paso en este proceso fue la **agrupación de controles similares** con el objetivo de optimizar la implementación de acciones correctivas más globales. Gracias a esta consolidación, se redujo el número de controles a tratar, pasando de los **121 controles originales a un total de 87**, facilitando así una gestión más estructurada y efectiva del cumplimiento.

Otro aspecto clave de esta fase fue el **macheo entre los requisitos normativos y la situación actual de cada control**. Para garantizar que el resultado final reflejara plenamente las exigencias de DORA, se estableció que la combinación del **estado actual de cada control** junto con la **medida correctiva recomendada** debía cubrir en su totalidad el requisito correspondiente del reglamento. De este modo, se aseguraba que ninguna exigencia normativa quedara desatendida y que las acciones propuestas fueran suficientes para alcanzar el cumplimiento esperado.

Para estructurar aún más la aplicación de las medidas correctivas, los **87 controles finales fueron agrupados en 6 proyectos específicos**, formando así una estructura integral y de cuidadosamente planeada que abarca todas las áreas clave que exige el reglamento. Cada uno de estos proyectos englobaría diferentes actividades que serían desarrolladas en diferentes estimaciones de tiempo y por diferentes tipos de roles, facilitando así la planificación y priorización de las acciones necesarias:

Proyecto	Actividades	Perfiles involucrados	Tiempo estimado	Posibles entregables
Revisión de contratos con terceros	• Identificación de contratos y cláusulas necesarios para regular los requisitos de ciberseguridad, en particular de DORA en los terceros que presten servicios TIC • Desarrollo de los modelos de contratos y clausulados para regular los requisitos de ciberseguridad en particular de DORA en los terceros que presten servicios TIC	• Jefe de proyecto • Consultor Senior de Seguridad • Abogado especialista en Tecnologías de la información	2 meses	Modelos de contratos y modelos de clausulados.
Marco de gestión de riesgos TIC de terceros	• Desarrollo del procedimiento de Acuerdo de intercambio de información • Desarrollo de la política de servicios TIC de proveedores • Desarrollo de la metodología de gestión de riesgos TIC de terceros • Implantación del proceso de gestión de riesgos TIC de terceros • Identificación de los terceros para la prueba de concepto del proceso • Ejecución del a prueba de concepto con 3 proveedores • Presentación de resultados	• Jefe de proyecto • Consultor Senior de Seguridad	4 meses	• Documento "Procedimiento de Acuerdo de Intercambio de información" • Documento "Política de servicios TIC de proveedores" • Documento "Metodología de riesgo TIC de terceros" • Resultado de la ejecución el proceso en 3 proveedores.
Definición de roles y responsabilidades en ciberseguridades	• Identificación de roles y responsabilidades para el cumplimiento de DORA • Mapeo de los roles y responsabilidades con el organigrama del cliente • Desarrollo de la norma de roles y responsabilidades	• Jefe de proyecto • Consultor Senior de seguridad	2 semanas	Documento "Norma y roles y responsabilidades"
Plan de continuidad de negocios	• Identificación de procesos críticos y establecimiento de sus RTO y RPO • Identificación de amenazas y riesgos sobre los procesos críticos • Definición de escenarios de indisponibilidad • Definición de las estrategias de recuperación y respaldo disponibles • Desarrollo del plan de continuidad de negocio • Encapsulamiento del DRP del proveedor IT en un DRP.	• Jefe de proyecto • Consultor Senior de Continuidad de negocio	2 meses	• Plan de continuidad de Negocio • Plan de Contingencia tecnológica

Programa de concienciación en ciberseguridad	Realización de un curso presencial sobre ciberseguridad de 1 hora lectiva al equipo de la empresa cliente.	• Jefe de proyecto • Consultor Senior de Seguridad	1 jornada	• Material lectivo en formato digital • Listado de firmas de los asistentes
Procedimiento de Análisis de riesgo y ejecución del mismo	• Definición del procedimiento de análisis de riesgos de seguridad de la información • Identificación de activos • Valoración y niveles de criticidad • Valoración de amenazas • Verificación de controles • Cálculo del nivel de riesgo • Creación del informe de Análisis de Riesgos • Identificación de salvaguardas necesarias de mitigación del riesgo • Plan de Tratamiento de Riesgos	• Jefe de proyecto • Consultor Senior de Seguridad	1 mes	• Documento "Metodología de Análisis de Riesgos de seguridad de la información" • Informe de Análisis de Riesgos de seguridad de la información • Plan de Tratamiento de Riesgos

Tabla 2. Proyectos plan de acción

Cada uno de estos proyectos contenía los controles que mejor se adaptaban a la temática, conteniendo cada uno su medida correctiva recomendada. Además, como se ha incluido en la Tabla 2, se proporcionó un plan de una estimación de la distribución temporal de cada uno de estos proyectos, para así facilitar la implementación progresiva de las medidas correctivas y conseguir el cumplimiento del reglamento DORA.

Finalmente, toda esta información fue plasmada en una **herramienta desarrollada específicamente para el cliente**, con el propósito de facilitar el seguimiento del cumplimiento de DORA. Aunque en este caso la herramienta se diseñó desde cero, posteriormente se consolidaría como una plantilla reutilizable para futuros proyectos, permitiendo una mayor automatización en el volcado de información clave.

Esta herramienta serviría como un **sistema de control y monitoreo** para que el cliente pudiera registrar los avances en la implementación de las medidas correctivas y garantizar el cumplimiento progresivo del reglamento.

Nota: en las imágenes de la herramienta secundaria es posible que aparezcan proyectos cuyos nombres sean ligeramente diferentes a los indicados en la Tabla 2, debida a la posterior oficialización del plan de acción.

5.5 DESARROLLO DE UNA HERRAMIENTA EXCEL

5.5.1 OBJETIVOS Y UTILIDAD

En el contexto del Gobierno, Riesgo y Cumplimiento (GRC) dentro del sector financiero, contar con una herramienta estructurada para la evaluación del cumplimiento normativo es fundamental. La creciente complejidad de los marcos regulatorios, como DORA, hace que las entidades financieras necesiten sistemas ágiles y precisos que les permitan identificar brechas, priorizar acciones correctivas y garantizar una adaptación eficiente a los requisitos de resiliencia operativa. En este sentido, una herramienta como la desarrollada en este proyecto no solo optimiza el trabajo del equipo de GRC, sino que también mejora la toma de decisiones al proporcionar una visión clara del estado de cumplimiento y los riesgos asociados.

Con el objetivo de facilitar la evaluación del cumplimiento normativo y optimizar el análisis GAP con respecto al Reglamento DORA, se desarrolló una **herramienta específica** que permite gestionar de manera estructurada los controles requeridos por el DORA. Esta herramienta no solo facilita la identificación de áreas de incumplimiento, sino que también sirve como base para la planificación y ejecución de medidas correctivas, asegurando un seguimiento continuo del grado de adaptación de la entidad financiera a la normativa.

Dado que el proyecto se inició con **un cliente concreto en una situación de urgencia**, la primera versión de la herramienta se centró en abordar específicamente los requisitos aplicables a esta entidad financiera en particular. De esta manera, durante el proceso del análisis de la normativa y de la creación del marco metodológico, se hizo una identificación inicial de los controles necesarios requeridos por el DORA para su cumplimiento, así como la diferenciación de la aplicabilidad de cada uno de los elementos del listado para la entidad con la que se estaba trabajando. Sin embargo, a medida que avanzó el proyecto, se identificaron oportunidades de mejora, y el desarrollo de la herramienta se convirtió en un **proceso continuo**, incorporando nuevas funcionalidades y refinamientos que la hicieron más versátil y aplicable a futuras implementaciones. Este proceso continuo consistió principalmente en una elaboración más cuidada del listado y la aplicabilidad de los controles.

El estudio de la aplicabilidad de cada control permitió hacer una diferenciación entre las diferentes entidades mencionadas en el reglamento para así poder hacer un escrutinio más exacto de lo requerido para cada categoría. Además, se identificaron áreas donde la información recogida inicialmente resultaba insuficiente o poco práctica para el análisis detallado. Esto llevó a la incorporación de nuevas columnas en la herramienta, diseñadas para optimizar el trabajo del consultor, aportar mayor claridad y estructurar mejor la información necesaria para el informe final. Estas mejoras no solo facilitaron el trabajo del consultor, proporcionando un marco más claro para la interpretación de los datos, sino que también aseguraron que la información recogida fuera más completa y útil. Por otro lado, entre las principales mejoras implementadas durante este desarrollo progresivo destaca la **creación de una segunda herramienta**, diseñada específicamente como entregable para el cliente cuya función es permitir un seguimiento detallado de la implementación de las acciones recomendadas, facilitando la gestión interna del cumplimiento.

En un principio, este entregable se elaboró de forma manual, trasladando la información relevante desde la herramienta principal. Posteriormente, a modo de mejora y para agilizar el proceso de volcado de información y minimizar errores, se decidió desarrollar una plantilla automatizada que permitiera el traslado de los datos más relevantes de manera estructurada, evitando omisiones o inconsistencias. Esta automatización se hizo a través de un código de MACROS que se puede observar en el ANEXO C – . De este modo, la herramienta evolucionó de un modelo inicial enfocado a un único cliente a un modelo flexible y escalable, capaz de ser reutilizado en otros proyectos sin necesidad de rediseños manuales, optimizando así el trabajo de los consultores y asegurando una mayor eficiencia en futuras implementaciones.

Al integrar elementos como la evaluación de madurez, el nivel de implementación y la estimación del tiempo de corrección, esta herramienta permite al departamento de GRC establecer planes de acción realistas y estratégicos, alineando los esfuerzos internos con las expectativas regulatorias. Esto es especialmente crítico en el sector financiero, donde la capacidad de respuesta ante incidentes y la gestión proactiva de los riesgos tecnológicos son factores determinantes para garantizar la estabilidad y confianza del mercado. En definitiva,

disponer de una herramienta de este tipo no solo facilita el cumplimiento normativo, sino que también refuerza la resiliencia operativa, reduciendo la exposición a sanciones y mejorando la capacidad de adaptación ante cambios regulatorios futuros.

5.5.2 ESTRUCTURA Y FUNCIONALIDADES

5.5.2.1 Versión inicial de la herramienta

Inicialmente, la herramienta se enfocó en las necesidades específicas de la entidad financiera con la que se trabajaba, permitiendo realizar un análisis GAP detallado y visualizar el estado de cumplimiento de cada control. Su propósito principal era optimizar la evaluación de los controles, centralizar la documentación relevante y permitir un seguimiento eficiente de las acciones correctivas. Con el avance del proyecto, se identificaron mejoras y nuevas funcionalidades que fueron implementadas progresivamente para hacerla más versátil y aplicable a futuros clientes. A continuación, se describe en detalle su estructura original y cómo evolucionó a lo largo del tiempo.

En su primera versión, la herramienta se diseñó para abordar de manera eficiente el análisis GAP del cumplimiento de DORA en la entidad financiera con la que se estaba trabajando. Su objetivo era centralizar la información relevante y proporcionar una estructura clara para la evaluación de los controles de cumplimiento, facilitando tanto la recopilación de datos como el análisis de la situación del cliente.

La herramienta estaba compuesta por **cuatro pestañas principales**, cada una con una función específica:

1. **Pestaña "GAP" (Análisis de controles y evaluación de cumplimiento):** Es el **núcleo principal** de la herramienta y contiene una tabla donde se realiza el análisis de cumplimiento de cada control. La tabla incluía las siguientes columnas clave:
    - **Documento:** referencia de la fuente de la que se extrae el control (Reglamento DORA o sus RTS/ITS).
    - **ID:** identificación del artículo y apartado específico dentro del documento normativo.

- **Título y descripción:** resumen y explicación detallada del control evaluado.
- **Ámbito:** clasificación creada para facilitar la organización y análisis de los controles durante las entrevistas con el cliente.
- **Aplica (Sí/No):** determina si el control es pertinente para la entidad evaluada.
- **CMMI (L0 a L5):** nivel de madurez del control según el modelo CMMI, con la posibilidad de marcarlo como **N/A** cuando no aplica debido a circunstancias específicas del cliente.
- **Evidencias proporcionadas:** documentación y pruebas aportadas para justificar el estado del control.
- **Comentarios:** espacio para registrar observaciones relevantes durante las reuniones y auditorías.
- **Estado actual:** diagnóstico del nivel de cumplimiento del control.
- **Acción recomendada:** medidas correctivas necesarias para alcanzar el cumplimiento.
- **Tiempo de implementación:** categorizado en Quick Win (QW), Corto Plazo (CP), Medio Plazo (MP) y Largo Plazo (LP) según la estimación de esfuerzo requerido.
- **Nivel de implementación:** indica si el control está implementado, parcialmente implementado o no implementado.
- **Prioridad:** establece si la acción correctiva es alta o baja en términos de urgencia.

2. **Pestaña "Cuadro de Mandos" (*Dashboard* de visualización de cumplimiento):** Esta pestaña contenía gráficos que proporcionaban una representación dinámica, clara y visual del estado de cumplimiento, basándose en los datos recogidos en la pestaña GAP. La representación gráfica permitía identificar de manera rápida áreas críticas y focalizar los esfuerzos en los controles más relevantes de forma que se optimice la elección de los controles a cumplimentar según su prioridad y su tiempo de implementación. Esto permite una elaboración del plan de acción más eficiente para alcanzar el cumplimiento necesario en el menor tiempo posible.

3. **Pestaña "AuxDB" (*Dashboard* auxiliar):** En esta sección se almacenaban las tablas dinámicas que alimentaban el cuadro de mandos. Gracias a esta estructura, los gráficos del *Dashboard* se actualizaban automáticamente conforme se completaban las evaluaciones y se ingresaban nuevos datos en la pestaña GAP.

4. **Pestaña "Aux" (Tablas de valores predefinidos):** Aquí se definían los valores preestablecidos para varias columnas de la pestaña GAP, como niveles de madurez, tiempos de implementación y estado de cumplimiento. Esto permitía homogeneizar los datos y minimizar errores, asegurando la coherencia de la información y facilitando su análisis.

Las imágenes que muestran estas pestañas explicadas se encuentran en el ANEXO E – Imágenes de la herramienta principal antigua. En ellas, para la fácil visualización de la herramienta, se incluirán capturas de la tabla por trozos, excluyendo la totalidad de los controles definidos (siendo estos 180 en esta versión antigua de la herramienta), para poder observar todas las columnas incluidas. Nótese que la aplicabilidad ya viene rellena en la columna “Aplica” al ser el primer filtro añadido de forma manual para el análisis del cliente con el que se trataba, dada la urgencia del proyecto.

En esta primera fase, la herramienta permitió estructurar y organizar el análisis de cumplimiento de DORA, facilitando la evaluación del cliente mediante un enfoque metódico y sistemático. Sus principales beneficios fueron:

- **Estandarización del análisis GAP**, asegurando que todos los controles fueran evaluados bajo los mismos criterios.
- **Automatización parcial de la visualización de datos**, con gráficos actualizados en tiempo real según la información introducida.
- **Facilidad para identificar incumplimientos y priorizar medidas correctivas**, proporcionando una guía clara para la toma de decisiones.
- **Creación de un modelo base** que luego permitiese ser evolucionado y mejorado de cara a ser replicable en futuros proyectos de la misma naturaleza y facilitando la función del consultor.

Sin embargo, con el avance del proyecto y la experiencia adquirida en el análisis de cumplimiento, se identificaron **oportunidades de mejora** para optimizar aún más la herramienta. En la siguiente sección, se explicará cómo evolucionó y qué nuevas funcionalidades se incorporaron para hacerla más robusta y eficiente.

5.5.2.2 Versión evolucionada de la herramienta

Como se ha mencionado en apartados anteriores, la herramienta inicial se fue mejorando mediante la incorporación de nuevas funcionalidades y ajustes que optimizaron el análisis de cumplimiento y facilitaron el trabajo de los consultores. Estas mejoras se implementaron de forma progresiva, basándose en la experiencia adquirida con el primer cliente y en la identificación de necesidades adicionales para su reutilización en futuros proyectos con el objetivo de mejorar la eficiencia del análisis de cumplimiento y facilitar el trabajo de los consultores en el estudio de los requisitos establecidos por DORA y sus normas técnicas de regulación (RTS/ITS). En esta evolución posterior, se identificaron cinco cambios o mejoras fundamentales:

1. **Incorporación de un filtro por tipo de entidad financiera o proveedor TIC:** no de los cambios más significativos fue la inclusión de un desplegable que permite seleccionar el tipo de entidad financiera o proveedor TIC con el que se esté trabajando. Los tipos de entidades financieras ofrecidos en este desplegable son los que se han identificado que se hayan mencionado o especificado requisitos a lo largo de todos los documentos que conforman el Reglamento. Esta funcionalidad permite filtrar de forma óptima la tabla del GAP apoyando directamente en los cambios establecidos en las columnas de la tabla, los cuales se explicarán a continuación, de manera que se muestren únicamente los controles aplicables a la entidad seleccionada, mejorando la eficiencia y reduciendo la carga de trabajo manual, centrando así el análisis en la normativa relevante para el cliente, eliminando información innecesaria y agilizando la evaluación de cumplimiento.

2. **Cambios en la tabla de la pestaña "GAP":** Para mejorar la trazabilidad y optimizar el análisis, se añadieron y modificaron varias columnas en la tabla principal

a. Nueva columna de "ID": En lugar de mantener separadas las columnas "Documento" e "ID" (que indicaban el origen del control y su referencia normativa), se creó una nueva columna donde ambos valores se combinan en un formato único, por ejemplo, "DORA-9.2". Esto mejora la trazabilidad de cada control evitando colisiones por la posibilidad de existir igual numeración de control, pero en diferente documento, y facilita la búsqueda y consulta de los requisitos en la normativa original.

b. Columna de "Cumplimiento": Se añadió una nueva columna para reflejar mejor el estado del cumplimiento de cada control por parte del cliente. Esta columna es especialmente útil porque, aunque el nivel de madurez recomendado suele ser CMMI L3 (procesos documentados), hay controles en los que un L2 podría ser suficiente según lo requerido en el DORA. Permite priorizar mejor las acciones correctivas y ayuda a estructurar el plan de acción con mayor precisión.

c. Columna de "Ámbito DORA": Se agregó una nueva clasificación basada en los cinco pilares del reglamento DORA que permitiese una mejor estructuración del análisis y que facilitase la generación de informes alineados con el marco regulador:
   i. Gobierno
   ii. Gestión del riesgo
   iii. Gestión y notificación de incidentes
   iv. Gestión de riesgos de terceros
   v. Pruebas de resiliencia operativa

3. **Creación de la pestaña "Aplicabilidad":** Para gestionar de manera más eficiente qué controles aplican a cada entidad, se creó una nueva pestaña denominada "Aplicabilidad", donde se centraliza la información sobre la relevancia de cada control según el tipo de entidad financiera o proveedor TIC. Esta pestaña incluye una tabla estructurada en tres bloques de columnas y una columna adicional que describe el nivel de cumplimiento:

a. Bloque de Aplicabilidad: Contiene una matriz con los controles en filas y las diferentes entidades financieras contenidas en el desplegable incluido en la pestaña de GAP en columnas. Cada celda indica si el control "Aplica" o "No Aplica" a esa entidad específica.

b. Bloque de Descripción: Contiene diferentes versiones de la descripción del control según el tipo de entidad. Hay una columna de "Descripción General" para los casos en los que el requisito no cambia entre entidades, y columnas adicionales para aquellas en las que el control presenta modificaciones específicas. De esta manera, se podría distinguir descripciones diferentes con las modificaciones correspondientes en los casos en los que el reglamento pueda ser más flexible, como para las microempresas, más estricto, como para los depositarios centrales de valores, o simplemente requieran una descripción un poco más específica y personalizado como para el caso de los proveedores TIC.

c. Bloque de preguntas: de igual manera que en el caso anterior, se incluyeron distintas versiones del *checklist* de preguntas asociadas a cada descripción del bloque anterior, permitiendo personalizar la evaluación de acuerdo con la entidad seleccionada.

d. Columna de nivel de cumplimiento: Define el nivel de madurez necesario para cumplir con el control en función del tipo de entidad financiera. Esta información es clave para que la herramienta pueda calcular automáticamente si el cliente cumple o no con el requisito, comparando el nivel de madurez evaluado en la pestaña "GAP" con el nivel requerido en "Aplicabilidad".

4. **Vinculación entre la pestaña "Aplicabilidad" y la pestaña "GAP":** como la pestaña de trabajo para el consultor sería la pestaña “GAP” y la de “Aplicabilidad” para que los datos de la pestaña "Aplicabilidad" se reflejen automáticamente en la pestaña "GAP", se implementaron fórmulas avanzadas que permiten:

a. Determinar la **aplicabilidad** de cada control en función de la entidad seleccionada en el desplegable: en primer lugar, la tabla del GAP ayudará a distinguir los controles que aplican o no a la entidad seleccionada por lo que deberá acceder a la matriz que corresponde al primer bloque de columnas de la pestaña "Aplicabilidad" y volcar el valor ("Aplica" o "No aplica") a la tabla principal. En función de este valor, el resto de las características ("Descripción", "Checklist de preguntas" y "Cumplimiento") se rellenarán o no. Esta consulta viene descrita en la Fórmula 1.

```
=SI.ERROR(SI(INDICE(Aplicabilidad!$C$2:$K$963;COINCIDIR(GAP!A3;Aplicabilidad!$A$2
:$A$963;0);COINCIDIR(GAP!$E$1;Aplicabilidad!$C$1:$K$1;0))="Aplica";"Aplica";"No
Aplica");"")
```

Fórmula 1. Determinación de la aplicación de cada control

b. Obtener la **descripción** del control según el tipo de entidad: en el caso en el que se haya obtenido que ese control sí aplica para la entidad seleccionada, se hará otra consulta a "Aplicabilidad" para determinar la descripción a volcar. Si una entidad tiene requisitos específicos en el control, se extrae la descripción correspondiente. Si no hay especificaciones, se toma la descripción general. Esta consulta viene descrita en la Fórmula 2

```
=SI(L3="No Aplica";"";SI.ERROR(
SI(INDICE(Aplicabilidad!$K$2:$R$963;COINCIDIR(GAP!A3;Aplicabilidad!$A$2:$A$963;0)
;COINCIDIR("Descripción "&GAP!$E$1;Aplicabilidad!$K$1:$R$1;0))<>"";
INDICE(Aplicabilidad!$K$2:$R$963;COINCIDIR(GAP!A3;Aplicabilidad!$A$2:$A$963;0);CO
INCIDIR("Descripción "&GAP!$E$1;Aplicabilidad!$K$1:$R$1;0));
INDICE(Aplicabilidad!$K$2:$K$963;COINCIDIR(GAP!A3;Aplicabilidad!$A$2:$A$963;0))
);""))
```

Fórmula 2. Obtención de la descripción del control según el tipo de entidad financiera seleccionada

c. Asignar el ***checklist* de preguntas** adecuado: del mismo modo que se vuelcan las descripciones, se vuelcan las preguntas a hacerle al cliente. Si ha habido una descripción específica para el tipo de entidad seleccionada, habrá un *checklist* de preguntas también específicos y, si no, se incluirá el general, Fórmula 3.

```
=SI(L3="No Aplica";"";SI.ERROR(
SI(INDICE(Aplicabilidad!$T$2:$Z$963;COINCIDIR(GAP!A3;Aplicabilidad!$A$2:$A$963;0)
;COINCIDIR("Alternativa Preguntas "&GAP!$E$1;Aplicabilidad!$T$1:$Z$1;0))<>"";
```

```
INDICE(Aplicabilidad!$T$2:$Z$963;COINCIDIR(GAP!A3;Aplicabilidad!$A$2:$A$963;0);CO
    INCIDIR("Alternativa Preguntas "&GAP!$E$1;Aplicabilidad!$T$1:$Z$1;0));
INDICE(Aplicabilidad!$T$2:$T$963;COINCIDIR(GAP!A3;Aplicabilidad!$A$2:$A$963;0))
                                        );""))
```

Fórmula 3. Asignación de checklist de preguntas para el consultor según el tipo de entidad financiera seleccionada

d. Calcular automáticamente el estado de cumplimiento: para abordar el nivel de cumplimiento real de cada control, se compara el nivel de madurez registrado en "GAP" con el nivel mínimo requerido en "Aplicabilidad". Si el nivel de madurez del cliente es igual o superior al requerido, la columna de cumplimiento mostrará "Cumple"; si el nivel es inferior, se marcará como "No Cumple", y si el consultor determina que el control no aplica por proporcionalidad, la celda de cumplimiento quedará vacía. Este funcionamiento viene reflejado en la Fórmula 4.

```
            =SI(ESBLANCO(GAP!M3);"";SI(GAP!M3="N/A";"N/A";SI(GAP!N3 >=
INDICE(Aplicabilidad!$S$2:$S$963;COINCIDIR(GAP!A3;Aplicabilidad!$A$2:$A$963;0));"
                                Cumple";"No cumple")))
```

Fórmula 4. Cálculo automático del estado de cumplimiento

Este sistema automatizado reduce errores, optimiza el tiempo de análisis y facilita la actualización de datos, haciendo que la herramienta sea más precisa y eficiente

5. **Creación de una nueva pestaña sobre tipos de entidades**: Finalmente, se incluyó una última pestaña destinada a definir los tipos de entidades financieras recogidas en el alcance de la normativa en función del Artículo 2 de DORA ("Aplicabilidad"). Esta tabla, como se puede ver en la Tabla 7 del ANEXO D - Tipos de Entidades Financieras contiene un listado de entidades financieras sujetas o no al reglamento DORA, la descripción de cada una de ellas, la referencia a los artículos donde se menciona cada tipo de entidad dentro del reglamento en caso de aplicación, y las normativas previas en las que se define cada entidad para facilitar su identificación y contextualización. Gracias a esta pestaña, los consultores pueden consultar rápidamente qué entidades están obligadas a cumplir con DORA, en qué condiciones y en qué se basan sus definiciones regulatorias.

La evolución de la herramienta ha permitido transformar una tabla inicial de análisis GAP en una solución mucho más sofisticada y funcional, con filtros dinámicos, automatización de datos y trazabilidad mejorada. Las mejoras implementadas han optimizado significativamente el trabajo de los consultores, permitiendo realizar evaluaciones más rápidas y precisas, asegurando un análisis de cumplimiento normativo más estructurado y alineado con las necesidades de cada cliente. La comparación entre ambas herramientas Excel se puede hacer observando los anexos ANEXO E – Imágenes de la herramienta principal antigua y ANEXO F - Imágenes de la herramienta principal , en el que, igual que en el ANEXO E, también se ha mostrado solo una porción de los controles incluidos a evaluar, siendo en esta segunda versión un total de 135, aunque dependiendo del tipo de entidad a evaluar (seleccionada en el desplegable que hace de filtro) ajustaría este número según la aplicabilidad.

5.5.2.3 Herramienta secundaria

Como se ha mencionado en apartados anteriores, al final del desarrollo del proyecto se diseñó una segunda herramienta basada en la original, pero con un enfoque más específico para el cliente. Su propósito es permitirle realizar un seguimiento en tiempo real del avance en la implementación de las medidas correctivas recomendadas en el plan de acción. Esta herramienta no solo ofrece una visión clara del grado de cumplimiento del Reglamento DORA en cada etapa de la implementación, sino que también proporciona acceso directo a la información más relevante contenida en el informe de fin de proyecto. Igual que la herramienta original, esta herramienta secundaria se enfocó originalmente al cliente del proyecto y tras su finalización, se implementaron mejoras.

5.5.2.3.1 Estructura y funcionalidad

La estructura definida en la herramienta desde un principio se mantuvo para la evolución. Para ello, se estructuró en diversas pestañas, cada una con una funcionalidad específica:

1. **Portada:** Contiene un texto explicativo detallado sobre el contenido del archivo, describiendo el propósito y uso de cada pestaña. Esta introducción facilita la comprensión del entregable por parte del cliente y agiliza su manejo.

2. **Cuadro de Mandos:** Siguiendo el modelo de la herramienta de análisis GAP, se incorporó un cuadro de mando dinámico con gráficos actualizados en tiempo real, diseñados para proporcionar una visión clara del progreso en la implementación de las medidas correctivas.

3. **Evaluación de controles:** Esta pestaña contiene la tabla principal de evaluación de controles, similar a la del GAP, pero más reducida y enfocada en el seguimiento de la implementación. Sus principales columnas incluyen:

    a. ID: Identificador único asignado a cada acción correctiva, permitiendo una posible agrupación en proyectos para organizar el plan de acción de manera optimizada.

    b. Título: Indica el nombre del control, facilitando su identificación rápida.

    c. Estado Actual: Refleja la situación de la empresa en relación con el control, según la evaluación realizada por el consultor.

    d. Acción Correctiva: Describe la medida recomendada en detalle para lograr el cumplimiento normativo.

    e. CMMI: Nivel de madurez actual, que el cliente puede actualizar conforme avanza la implementación de la acción correctiva.

    f. Cumplimiento: Indica el estado de cumplimiento del control, permitiendo visualizar cuántos controles han pasado de "No Cumple" a "Cumple".

    g. Nivel de Implementación: Puede tomar los valores "Implementado", "Parcialmente Implementado" o "No Implementado", y es editable por el cliente.

    h. Tiempo de Implementación: Clasifica las acciones según su horizonte temporal, como en la herramienta GAP.

i. Proyecto: Al haber organizado el plan de acción de este caso en proyectos como se explicó en el apartado 5.4, la referencia que aporta esta columna facilita el filtrado de medidas dentro del plan de acción si este ha sido organizado en proyectos específicos.

j. Evidencia: Lista los documentos aportados por el cliente como prueba del cumplimiento del control.

k. Referencia a la normativa: Indica dónde aparece el requisito en el Reglamento DORA. Aunque la existencia de esta columna aporta valor, su elaboración requiere una gran inversión de tiempo y es difícil de replicar en futuros proyectos.

l. Ámbito DORA: Permite filtrar los controles según los cinco pilares fundamentales del reglamento.

4. **Criterios de cumplimiento**: Contiene tablas con los niveles de madurez CMMI y los criterios de cumplimiento del DORA, mostrados en el ANEXO A – Niveles de madurez modelo CMMI y en el ANEXO B – Criterios de cumplimiento DORA, respectivamente.

5. **Evidencias aportadas**: Listado de todas las evidencias documentales proporcionadas por el cliente, utilizadas por el equipo consultor para fundamentar sus conclusiones y elaborar el plan de acción.

6. **Controles N.A.:** Contiene los controles que, aunque teóricamente aplicables a la entidad financiera, fueron considerados no aplicables (N/A) y categorizados como tal en el nivel CMMI debido a criterios de proporcionalidad o características específicas de la organización.

7. **Desglose por proyectos:** Presenta una visión estructurada del plan de acción, mostrando todos los proyectos identificados y las medidas correctivas asociadas a cada uno de forma listada y más esquemática.

8. **Aux y AuxDB:** igual que en la herramienta GAP, se crearon estas dos pestañas para crear los valores posibles a tomar en las columnas de cada celda y así unificar las opciones, y las tablas dinámicas que alimentarían las gráficas dinámicas del cuadro de mandos. Sin embargo, estas dos pestañas se ocultarían al entregarla al cliente ya que no le aportaría valor.

5.5.2.3.2 Evolución y mejoras de la herramienta secundaria

Al igual que la herramienta original, esta segunda herramienta evolucionó con el objetivo de mejorar su funcionalidad y facilitar su replicabilidad en futuros proyectos.

1. **Optimización de la referencia normativa:** Para abordar la dificultad de incluir manualmente la referencia a la normativa en cada control, se incorporó una nueva columna denominada "ID_GAP", vinculada al ID de la herramienta de análisis GAP. Esto permite mantener una referencia implícita a la ubicación exacta del requisito normativo sin necesidad de buscarlo manualmente en cada proyecto.

2. **Automatización del proceso mediante macros:** La mejora más significativa fue la creación de un código en macros de Excel, documentado en el ANEXO C – Código de automatización como se explicó en la introducción de la sección, que automatiza el volcado de información desde la herramienta GAP. Su funcionamiento implica:

    a. Filtra automáticamente los controles aplicables según la columna "Aplica" en GAP.
    b. Volcado de manera ordenada las columnas necesarias para la tabla de “Evaluación de controles” desde la tabla del GAP (ID, Título, Estado Actual, Acción Recomendada, CMMI, Cumplimiento, Nivel de Implementación, Tiempo de Implementación y Ámbito DORA.)
    c. Genera automáticamente los ID de cada acción correctiva, utilizando una numeración correlativa basada en el ámbito DORA del control correspondiente.
    d. De igual manera que transfiere la información de los controles a aplicar medidas correctivas, también se vuelca automáticamente la información

referente a los controles marcados como N/A en la pestaña "Controles N.A.", permitiendo que el cliente los tenga en cuenta en caso de futura aplicabilidad.

Esta automatización aporta múltiples ventajas al proceso de seguimiento y control de la implementación de medidas correctivas, facilitando y agilizando la generación del plan de acción, eliminando la necesidad de trasladar manualmente los datos, lo que reduce significativamente los tiempos de trabajo y minimiza los errores de transcripción; asegurando la coherencia en la información transferida, garantizando que los datos reflejados en la evaluación de controles sean fieles a los obtenidos en la herramienta GAP, lo que evita discrepancias y permite un análisis más preciso; y añadiendo un valor significativo al entregable final, ya que proporciona al cliente una herramienta más robusta, dinámica y adaptable a sus necesidades, permitiéndole un seguimiento en tiempo real del avance de la implementación y facilitando la toma de decisiones estratégicas de manera más informada y eficiente.

La creación de esta herramienta secundaria marca la fase final en el desarrollo del proyecto, asegurando que todas las necesidades identificadas y oportunidades de mejora a lo largo del proceso quedan completamente cubiertas. Con su integración, se consigue no solo un seguimiento estructurado y automatizado del cumplimiento del Reglamento DORA, sino también una solución replicable para futuros proyectos, garantizando coherencia y optimización en la evaluación de controles. La automatización implementada facilita considerablemente el trabajo del consultor, permitiéndole realizar evaluaciones de manera más ágil, precisa y sin riesgo de errores manuales, ahorrando tiempo y mejorando la eficiencia en la gestión de la información. De este modo, el proyecto se cierra con una herramienta que no solo ofrece valor añadido al cliente al proporcionarle una visión clara y en tiempo real de su progreso, sino que también optimiza el trabajo del equipo consultor, facilitando la continuidad y escalabilidad del proceso en nuevas implementaciones. Las imágenes de la herramienta entregada al cliente se pueden ver en el ANEXO G – Imágenes de la herramienta entregada al cliente. En ellas se puede ver el entregable ofrecido al cliente y con las diferentes pestañas rellenas en base al estudio hecho del cumplimiento del cliente. Se ha anonimizado cualquier dato que pudiera relacionar directamente a dicho cliente, como

la pestaña en la que se agrupa la documentación aportada por el cliente como evidencias pero se ha mantenido el resto de información que pueda ser relevante como muestra del entregable.

Capítulo 6. ANÁLISIS DE RESULTADOS

El principal resultado de este proyecto ha sido el diseño y desarrollo de una **herramienta digital propia, optimizada y especializada** para facilitar el análisis de cumplimiento del Reglamento DORA en entidades financieras. A diferencia del enfoque inicial más generalista o manual, la solución final responde específicamente a las exigencias técnicas del marco normativo europeo, incorporando funcionalidades adaptadas al análisis de brechas (GAP Analysis), la clasificación de requisitos, y la evaluación de terceros proveedores TIC.

De esta manera, se ha conseguido crear un modelo replicable que permite ser aplicado de forma eficiente en futuros proyectos, reduciendo de forma considerable el tiempo de evaluación, minimizando errores humanos y facilitando el trabajo del consultor. Este avance representa una mejora tangible frente a herramientas previas que requerían una mayor carga operativa manual y no contaban con un enfoque directo al cumplimiento del DORA.

Además, el trabajo se ha completado con una aplicación real de la herramienta en un caso práctico de análisis GAP para una entidad del sector, lo cual ha sido clave para validar que realmente funciona, detectar oportunidades de mejora y afinar detalles que en papel pueden pasar desapercibidos. Esta experiencia ha permitido reforzar su utilidad y adaptabilidad al trabajo diario en consultoría y cumplimiento normativo.

Ilustración 7. Muestra de una de las herramientas como resultados del proyecto

En conclusión, el resultado final remarca un producto funcional y estratégico que refuerza la resiliencia operativa del sector financiero, promoviendo la eficiencia y estandarización de los procesos de cumplimiento regulatorio en un contexto cada vez más exigente. Este avance no solo da cierre al proyecto con éxito, sino que sienta las bases para su aplicación en nuevos escenarios y para el desarrollo de futuras versiones aún más automatizadas e integradas con otros sistemas de control normativo.

Capítulo 7. CONCLUSIONES Y TRABAJOS FUTUROS

La realización de este proyecto ha permitido alcanzar un conocimiento profundo sobre el Reglamento DORA y sobre la importancia crítica que adquiere la resiliencia operativa digital en el sector financiero. La normativa, surgida como respuesta a un contexto cada vez más digitalizado y expuesto a riesgos tecnológicos, exige a las entidades una capacidad estructurada para anticipar, resistir y recuperarse frente a incidentes disruptivos.

Por otro lado, ha permitido desarrollar una herramienta específica y optimizada para facilitar el análisis del cumplimiento del Reglamento DORA en entidades financieras, respondiendo tanto a las exigencias del marco normativo europeo como a las necesidades reales de los equipos de consultoría. Esta iniciativa ha supuesto un avance significativo para agilizar, estandarizar y mejorar la calidad del proceso de evaluación normativa, aportando eficiencia, trazabilidad y reducción de errores operativos.

Durante el desarrollo, la herramienta fue aplicada en un caso real de análisis GAP, lo que permitió validar su funcionamiento en condiciones prácticas, comprobar su utilidad, y detectar mejoras que se incorporaron progresivamente. Esta experiencia práctica no solo consolidó la funcionalidad del instrumento, sino que también facilitó un aprendizaje profundo sobre la normativa DORA, su estructura, sus implicaciones y su aplicación en el entorno financiero.

Uno de los aspectos más enriquecedores del proyecto ha sido la autonomía para proponer y aplicar mejoras, siempre bajo la supervisión de responsables expertos. Esta responsabilidad promovió mi desarrollo profesional y de competencias clave como el pensamiento crítico, la toma de decisiones técnicas, la priorización de funcionalidades con valor añadido, y la capacidad de análisis independiente. Además, la necesidad de compaginar este trabajo con otras responsabilidades profesionales y académicas reforzó habilidades en gestión del tiempo, organización, adaptación a entornos dinámicos y comunicación efectiva.

Entre **las principales aportaciones** destacan:

- La creación de una herramienta replicable y aplicable en futuros proyectos de análisis DORA.
- La optimización del proceso de evaluación normativa, con menor carga operativa y margen de error.
- La identificación y validación de criterios adaptados a las exigencias de terceros proveedores TIC.
- La mejora de la experiencia de consultoría para el cliente, quien ha valorado positivamente el trabajo y ha mostrado interés en futuras colaboraciones.

Como **líneas de trabajo futuras**, se propone seguir optimizando el modelo actual mediante nuevas funcionalidades en Excel que mejoren su automatización y capacidad analítica. También se contempla su integración con plataformas avanzadas como ARCHER o Risk4All, evaluadas durante el proyecto como referentes para el análisis de escenarios operacionales. Asimismo, el enfoque metodológico empleado podría adaptarse a otros marcos regulatorios del sector financiero, ampliando así el alcance y utilidad de la herramienta como solución versátil dentro del ámbito regulatorio.

Como conclusión global, los resultados obtenidos no solo cumplen los objetivos iniciales, sino que establecen una base sólida para desarrollar futuras versiones más automatizadas e integradas, alineadas con la evolución del marco regulatorio europeo y las crecientes demandas del entorno digital financiero.

Capítulo 8. BIBLIOGRAFÍA

[1] U. Europea, «REGLAMENTO (UE) 2022/2554 DEL PARLAMENTO EUROPEO Y DEL CONSEJO,» 14 Diciembre 2022. [En línea]. Available: https://www.boe.es/doue/2022/333/L00001-00079.pdf.

[2] E. E. B. Authority, «ESAs publish first set of rules under DORA for ICT and third-party risk management and incident classification,» 17 Enero 2024. [En línea]. Available: https://www.eba.europa.eu/publications-and-media/press-releases/esas-publish-first-set-rules-under-dora-ict-and-third-party.

[3] E. E. B. Authority, «ESAs published second batch of policy products under DORA,» 17 Julio 2024. [En línea]. Available: https://eba.europa.eu/publications-and-media/press-releases/esas-published-second-batch-policy-products-under-dora.

[4] SOSAFE, «DORA,» [En línea]. Available: https://sosafe-awareness.com/glossary/dora/.

[5] U. Europea., « Reglamento (UE) n.º 1093/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Bancaria Europea),» 24 Noviembre 2010. [En línea]. Available: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:02010R1093-20210626.

[6] U. Europea, «Reglamento (UE) n o 1094/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010 , por el que se crea una Autoridad Europea de Supervisión (Autoridad Europea de Seguros y Pensiones de Jubilación),» 24 Noviembre 2010. [En línea]. Available: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:02010R1094-20200101.

[7] U. Europea, «Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority),» 24 Noviembre 2010. [En línea]. Available: https://www.esma.europa.eu/sites/default/files/library/2015/11/1095-2010_esma_regulation_amended.pdf.

[8] B. d. España, «Directrices sobre gestión de riesgos de TIC y de seguridad (EBA/GL/2019/04),» 28 Noviembre 2019. [En línea]. Available: https://www.bde.es/f/webbde/INF/MenuHorizontal/Normativa/guias/EBA-GL-2019-04-ES.pdf.

[9] E. E. I. a. O. P. Authority, «Guidelines on information and communication technology security and governance. EIOPA-BoS-20/600,» 8 Octubre 2020. [En línea]. Available: https://www.eiopa.europa.eu/system/files/2020-10/eiopa-bos-20-600-guidelines-ict-security-and-governance.pdf.

[10] E. E. S. a. M. Authority, «Directrices sobre la externalización de servicios a proveedores de servicios en la nube,» 10 Mayo 2021. [En línea]. Available: https://www.esma.europa.eu/sites/default/files/library/esma_cloud_guidelines_es.pdf.

[11] U. Europea, «DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión,» 6 Julio 2016. [En línea]. Available: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L1148.

[12] U. Europea, «REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos,» 27 Abril 2016. [En línea]. Available: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679.

[13] U. Europea, «DIRECTIVA 2014/65/UE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 15 de mayo de 2014 relativa a los mercados de instrumentos financieros,» 15 Mayo 2014. [En línea]. Available: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32014L0065.

[14] U. Europea, «REGLAMENTO (UE) No 575/2013 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 26 de julio de 2013 sobre los requisitos prudenciales de las entidades de crédito y las empresas de inversión,» 26 Julio 2013. [En línea]. Available: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32013R0575.

[15] U. Europea, «DIRECTIVA 2013/36/UE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 26 de junio de 2013 relativa al acceso a la actividad de las entidades de crédito y a la supervisión prudencial de las entidades de crédito y las empresas de inversión,» 26 junio 2013. [En línea]. Available: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32013L0036.

[16] U. Europea, «DIRECTIVA (UE) 2015/2366 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior,» 25 Noviembre 2015. [En línea]. Available: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32015L2366.

[17] U. Europea, «REGLAMENTO (UE) No 795/2014 DEL BANCO CENTRAL EUROPEO de 3 de julio de 2014,» 3 Julio 2014. [En línea]. Available: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32014R0795.

[18] C. Alonso, «Global Suite Solutions. ¿Qué es la ley SOX y para qué sirve=,» 27 Septiembre 2023. [En línea]. Available: https://www.globalsuitesolutions.com/es/que-es-sox-y-para-que-sirve/.

[19] Rubricae, «Rubricae,» [En línea]. Available: https://rubricae.com/Blog/que-es-el-reglamento-dora-y-por-que-es-importante/. [Último acceso: 17 Febrero 2025].

[20] Legalnet, «Legalnet,» 31 Enero 2024. [En línea]. Available: https://legalnet.es/el-reglamento-dora/. [Último acceso: 17 Febrero 2025].

[21] J. Berenguer, «Qué es el cumplimiento de DORA y por qué es tan importante en ciberseguridad,» Redes Zone, 9 Febrero 2025. [En línea]. Available: https://www.redeszone.net/noticias/seguridad/cumplimiento-dora-guia-practica/. [Último acceso: 17 02 2025].

[22] A. Tabalin, «A Complete Guide to DORA (Digital Operational Resilience Act),» Metomic, 27 February 2025. [En línea]. Available: https://www.metomic.io/resource-centre/a-complete-guide-to-dora.

[23] A. Tambalin, «A Complete Guide to DORA (Digital Operational Resilience Act),» Metomic, 28 Noviembre 2024. [En línea]. Available: https://www.metomic.io/resource-centre/a-complete-guide-to-dora.

[24] European Union, «REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL,» 14 December 2022. [En línea]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554.

ANEXO A – NIVELES DE MADUREZ MODELO CMMI

Modelo de la madurez de la capacidad	
NIVEL CMMI	**DESCRIPCIÓN ESTADOS CMMI**
L0	Inexistente (0%) ▪Carencia completa de ningún proceso reconocido. ▪No se ha reconocido ni siquiera que existe un problema a resolver.
L1	Inicial / Ad hoc (10%) ▪ Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. ▪Los procedimientos son inexistentes o localizados en áreas concretas. ▪No existen plantillas definidas a nivel corporativo.
L2	Reproducible, pero intuitivo (50%) ▪Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. ▪Se normalizan las buenas prácticas en base a la experiencia y al método. ▪No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. ▪Se depende del grado de conocimiento de cada individuo.
L3	Proceso definido (90%) ▪La organización entera participa en el proceso. ▪Los procesos están implantados, documentados y comunicados mediante entrenamiento.
L4	Gestionado y medible (95%) ▪Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. ▪ Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
L5	Optimizado (100%) ▪Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

Tabla 3. Niveles de madurez del modelo CMMI

ANEXO B – CRITERIOS DE CUMPLIMIENTO DORA

Criterios de cumplimiento de DORA		
NIVEL CMMI	**Nivel de cumplimiento DORA**	**Criterios cumplimiento DORA**
L0	No cumple	No cumple.
L1	No cumple	No cumple.
L2*	Cumple/No cumple	Dependiendo del requerimiento de DORA podría cumplir si no se exige la obligatoriedad de tener formalizado un proceso documentado, en tal caso, el control cumpliría con un L2, y en caso contrario, no cumpliría.
L3	Cumple	Cumple.
L4	Cumple	Cumple.
L5	Cumple	Cumple.

Tabla 4. Criterios de cumplimiento de DORA

ANEXO C – CÓDIGO DE AUTOMATIZACIÓN

```
Sub CopiarFiltradosYGenerarIdentificadorCorregido()
    Dim wsOrigen As Worksheet
    Dim wsDestino As Worksheet
    Dim wsDestinoNA As Worksheet
    Dim tablaDestino As ListObject
    Dim tablaDestinoNA As ListObject
    Dim rngOrigen As Range
    Dim filaNueva As ListRow
    Dim filtroValorAplica As String
    Dim columnasACopiar As Variant
    Dim celdaOrigen As Range
    Dim columnPositions As Collection
    Dim colAmbitoDora As Long
    Dim headerRow As Range
    Dim colIndex As Long
    Dim ultimoAmbito As String
    Dim contador As Long
    Dim identificador As String
    Dim colID As Long
    Dim colIDGAP As Long

    ' Configuración de hojas y tabla
    Set wsOrigen = ThisWorkbook.Sheets("GAP") ' Hoja de origen
    ' Abrir el libro de destino desde la misma carpeta que el archivo de origen
    Set libroDestino = Workbooks.Open(ThisWorkbook.Path & "\HERRAMIENTA - Informe
GAP DORA v1.1.xlsx") 'Archivo de destino
    Set wsDestino = libroDestino.Sheets("EVALUACIÓN CONTROLES") ' Hoja donde
copiar las medidas correctivas
    Set wsDestinoNA = libroDestino.Sheets("CONTROLES N.A.") ' Hoja para controles
N.A.


    Set tablaDestino = wsDestino.ListObjects("TablaEvaluacionControles") ' Cambia
por el nombre de tu tabla en la hoja de destino
    Set tablaDestinoNA = wsDestinoNA.ListObjects("TablaControlesNA") ' Tabla en
"CONTROLES N.A."


    ' Eliminar las filas de la tabla destino (manteniendo el formato)
    If Not tablaDestino.DataBodyRange Is Nothing Then
        tablaDestino.DataBodyRange.Delete
    End If

    ' Eliminar las filas de la tabla destino (manteniendo el formato)
    If Not tablaDestinoNA.DataBodyRange Is Nothing Then
        tablaDestinoNA.DataBodyRange.Delete
    End If

    ' Rango de datos de la hoja de origen
```

```
    Set rngOrigen = wsOrigen.Range("A3:Z150") ' Ajusta el rango según tus datos
reales

    ' Valor de filtro
    filtroValorAplica = "Aplica" ' Filtro por "Aplica"

    ' Columnas a copiar
    columnasACopiar = Array("Título", "Estado actual", "Acción recomendada",
"CMMI", "Cumplimiento", "Grado de implementación", "Tiempo de implementación",
"Evidencias", "Ámbito DORA")
    colAmbitoDora = 26 ' Índice de columna para "Ámbito DORA" (en el GAP está en
la columna "Z")


    ' Encontrar posiciones de las columnas a copiar
    Set headerRow = wsOrigen.Rows(2) ' Supongamos que los encabezados están en la
primera fila
    Set columnPositions = New Collection




    ' ************************************************************************
    '***************COPIA DE DATOS EN "EVALUACIÓN
CONTROLES"*******************
    '************************************************************************

    ' Inicializar variables
    ultimoAmbito = ""
    contador = 1

    ' Buscar la posición de la columna "ID" en la tabla de destino
    colID = Application.Match("ID", tablaDestino.HeaderRowRange, 0)
    If colID > 0 Then
        columnPositions.Add colID ' Añadir posición de "ID" al inicio de la
colección
    End If

    ' Buscar la posición de la columna "ID GAP" en la tabla de destino
    colIDGAP = Application.Match("ID GAP", tablaDestino.HeaderRowRange, 0)
    columnPositions.Add colIDGAP

    ' Buscar las posiciones de las columnas a copiar en la hoja de origen
    For i = LBound(columnasACopiar) To UBound(columnasACopiar)
        On Error Resume Next
        colIndex = Application.Match(columnasACopiar(i), headerRow, 0)
        On Error GoTo 0
        If colIndex > 0 Then
            columnPositions.Add colIndex
        End If
    Next i
```

```
    ' Procesar datos filtrados
    For Each celdaOrigen In rngOrigen.Rows
        ' Comprobar si la fila tiene datos
        If Application.WorksheetFunction.CountA(celdaOrigen) > 0 Then
            ' Filtrar por valor en la columna "Aplica" (columna 12 = "L")
            If Trim(LCase(celdaOrigen.Cells(1, 12).Value)) =
Trim(LCase(filtroValorAplica)) And Trim(LCase(celdaOrigen.Cells(1, 13).Value)) <>
"n/a" Then
                ' Añadir una nueva fila a la tabla destino
                Set filaNueva = tablaDestino.ListRows.Add


                ' Copiar datos columna por columna
                For j = 1 To columnPositions.Count
                    filaNueva.Range(1, j).Value = celdaOrigen.Cells(1,
columnPositions(j)).Value
                    If columnPositions(j) = colIDGAP Then
                        ' Copiar el valor de la columna "ID" de la hoja de origen
en "ID GAP" de la hoja de destino
                        filaNueva.Range(1, colIDGAP).Value = celdaOrigen.Cells(1,
Application.Match("ID", headerRow, 0)).Value
                    End If
                Next j

                ' Generar identificador basado en "Ámbito DORA"
                Dim ambitoDora As String
                ambitoDora = celdaOrigen.Cells(1, colAmbitoDora).Value

                ' Reiniciar contador si cambia el ámbito
                If Left(ambitoDora, 1) <> Left(ultimoAmbito, 1) Then
                    contador = 1
                End If

                ' Crear el identificador
                identificador = "A" & Left(ambitoDora, 1) & "." & contador
                filaNueva.Range(1, colID).Value = identificador

                ' Incrementar contador y actualizar ámbito
                contador = contador + 1
                ultimoAmbito = ambitoDora
            End If
        End If
    Next celdaOrigen




    ' ************************************************************************
    '********************COPIA DE DATOS EN "CONTROLES N.A."**********************
    '************************************************************************
    ' Buscar posiciones de columnas para tabla "CONTROLES N.A."
    Dim columnPositionsNA As Collection
```

```
    Set columnPositionsNA = New Collection

    colIDGAP = Application.Match("ID GAP", tablaDestinoNA.HeaderRowRange, 0)
    columnPositionsNA.Add colIDGAP

     For i = LBound(columnasACopiar) To UBound(columnasACopiar)
        colIndex = Application.Match(columnasACopiar(i), headerRow, 0)
        If colIndex > 0 Then columnPositionsNA.Add colIndex
    Next i

    ' Procesar filas para "CONTROLES N.A."
    For Each celdaOrigen In rngOrigen.Rows
        If Application.WorksheetFunction.CountA(celdaOrigen) > 0 Then

            Dim valorCMMI As String
            valorCMMI = Trim(LCase(celdaOrigen.Cells(1, 13).Value)) ' Columna 13
("M" en la hoja)
            Debug.Print "Valor CMMI: " & valorCMMI & ""

            If valorCMMI = "n/a" And Trim(LCase(celdaOrigen.Cells(1, 12).Value))
= Trim(LCase(filtroValorAplica)) Then
                Set filaNueva = tablaDestinoNA.ListRows.Add
                For j = 1 To columnPositionsNA.Count
                    filaNueva.Range(1, j).Value = celdaOrigen.Cells(1,
columnPositionsNA(j)).Value
                    If columnPositionsNA(j) = colIDGAP Then
                        filaNueva.Range(1, colIDGAP).Value = celdaOrigen.Cells(1,
Application.Match("ID", headerRow, 0)).Value
                    End If
                Next j
            End If
        End If
    Next celdaOrigen


    MsgBox "¡Datos copiados correctamente en la tabla destino!"
End Sub
```

Fragmento de código 1. Código de automatización de volcado de información entre herramientas Excel

ANEXO D - TIPOS DE ENTIDADES FINANCIERAS

Aplica	Nombre	Descripción	Normativa que la define	Artículos del DORA donde se mencionan
SI	**Administradores de índices de referencia cruciales**	Es la persona física o jurídica bajo cuyo control se elabora un índice de referencia y, en articular, administra los mecanismos destinados a determinar el índice de referencia, recopila y analiza los datos de cálculo, determina el índice de referencia y lo publica. «índice de referencia crucial»: un índice de referencia distinto de un índice de referencia de datos regulados, que cumpla una de las condiciones establecidas en el artículo 20, apartado 1, y que aparezca en la lista establecida por la Comisión en virtud de dicho artículo;	Artículo 3, apartado 1, punto 25, del Reglamento (UE) 2016/1011	-
	Agencias de calificación crediticia	Una persona jurídica cuya ocupación incluya la emisión de calificaciones crediticias con carácter profesional	Artículo 3, apartado 1, letra b), del Reglamento (CE) n.o 1060/2009	-
	Centros de negociación	Cualquier mercado regulado, los sistemas multilaterales de negociación (SMN) y los sistemas organizados de contratación (SOC)	Artículo 4, apartado 1, punto 24, de la Directiva 2014/65/UE;	
	Depositarios centrales de valores	Una persona jurídica que gestione un sistema de liquidación de valores conforme a lo que se recoge en el anexo, sección A, punto 3, y que preste al menos otro de los servicios básicos enumerados en el anexo, sección A;	Artículo 2, apartado 1, punto 1, del Reglamento (UE) n.o 909/2014	11.9 , 12.5, 19.8,25.2
	Empresa de servicios de inversión pequeña y no interconectada	1. Una empresa de servicios de inversión se considerará pequeña y no interconectada a efectos del presente Reglamento si cumple todas las condiciones siguientes: a) los AUM, valorados de conformidad con el artículo 17, son inferiores a 1 200 millones EUR; b) las COH, valoradas de conformidad con el artículo 20, son inferiores a: i) 100 millones EUR /día para las operaciones al contado, o ii) 1 000 millones EUR /día para los derivados; c) los ASA, valorados de conformidad con el artículo 19, son iguales a cero; d) el CMH, valorado de conformidad con el artículo 18, es igual a cero; e) el DTF, valorado de conformidad con el artículo 33, es igual a cero; f) el NPR o el CMG, valorados de conformidad con los artículos 22 y 23, son iguales a cero; g) el TCD, valorado de conformidad con el artículo 26, es igual a cero; h) el importe total del balance y de las cuentas de fuera de balance de la empresa de servicios de inversión es inferior a 100 millones EUR; i) los ingresos totales brutos anuales procedentes de los servicios y actividades de inversión de la empresa de servicios de inversión son inferiores a 30 millones EUR, calculados como una media sobre la base de las cifras anuales del período de dos años inmediatamente anterior al ejercicio financiero de que se trate.	artículo 12, apartado 1, del Reglamento (UE) 2019/2033 del Parlamento Europeo y del Consejo	16, 26, 28.2
	Empresa pequeña	Una entidad financiera que emplea a 10 o más personas pero menos de 50 y cuyo volumen de negocios anual o balance anual total es superior a 2 millones EUR pero igual o inferior a 10 millones EUR;	Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo	-
	Empresas de reaseguros	Una empresa que haya recibido autorización con arreglo al artículo 14 para desarrollar actividades de reaseguro;	Artículo 13, punto 4, de la Directiva 2009/138/CE	-
	Empresas de seguros	Una empresa de seguros directos de vida o distintos del seguro de vida que haya recibido autorización, con arreglo a lo dispuesto en el artículo 14;	Artículo 13, punto 1, de la Directiva 2009/138/CE	-
	Empresas de servicios de inversión	Toda persona jurídica cuya profesión o actividad habituales consisten en prestar uno o más servicios de inversión o en realizar una o más actividades de inversión con carácter profesional a tercero	Artículo 4, apartado 1, punto 1, de la Directiva 2014/65/UE	-
	Entidad de crédito	Una empresa cuya actividad consista en recibir del público depósitos u otros fondos reembolsables y en conceder créditos por cuenta propia.	Artículo 4, apartado 1, punto 1, del Reglamento (UE) n.o 575/2013 del Parlamento Europeo y del Consejo	19, 23, 26.8
	Entidad de dinero electrónico exenta en virtud de la Directiva 2009/110/CE	1. Los Estados miembros podrán no aplicar o autorizar a sus autoridades competentes a no aplicar total o parcialmente el procedimiento y las condiciones establecidos en los artículos 3, 4, 5 y 7 de la presente Directiva, a excepción de los artículos 20, 22, 23 y 24 de la Directiva 2007/64/CE, y permitir la inclusión de personas jurídicas en el registro de entidades de dinero electrónico, siempre que se cumplan los dos requisitos siguientes: a) que la totalidad de las actividades empresariales genere una cuantía media de dinero electrónico en circulación que no sobrepase un límite establecido por el Estado miembro y que, en ningún caso, podrá ser superior a los 5 000 000 EUR, y b) que ninguna de las personas físicas responsables de la gestión o explotación de las actividades empresariales haya sido condenada por delitos de blanqueo de dinero o financiación del terrorismo u otros delitos de	Artículo 9, apartado 1, de la Directiva 2009/110/CE	16, 26, 28.2
	Entidad de pago	Una persona jurídica a la cual se haya otorgado autorización, de conformidad con el artículo 11, para prestar y ejecutar servicios de pago en toda la Unión;	Artículo 4, punto 4, de la Directiva (UE) 2015/2366	23
	Entidad de pago exenta en virtud de la Directiva (UE) 2015/2366	Personas físicas o jurídicas que presten servicios de pago enumerados en los puntos 1 a 6 del anexo I, cuando: a) el valor total medio de las operaciones de pago ejecutadas en los 12 meses precedentes por la persona de que se trate, incluidos los posibles agentes con respecto a los cuales asume plena responsabilidad, no exceda de un límite fijado por el Estado miembro, límite que, en todo caso, no podrá ser superior a 3 millones EUR mensuales. Dicho requisito evaluará con respecto a la cuantía total de las operaciones de pago prevista en su plan de negocios, a menos que las autoridades competentes exijan la modificación de dicho plan, y b) ninguna de las personas físicas responsables de la gestión o el ejercicio de la actividad haya sido condenada por delitos de blanqueo de capitales o financiación del terrorismo u otros delitos de carácter financiero.	Artículo 32, apartado 1, de la Directiva (UE) 2015/2366	16, 26, 28.2
	Entidades de contrapartida central	Una persona jurídica que intermedia entre las contrapartes de los contratos negociados en uno o varios mercados financieros, actuando como compradora frente a todo vendedor y como vendedora frente a todo comprador	artículo 2, punto 1, del Reglamento (UE) n.o 648/2012	12.3, 25.2
	Entidades de dinero electrónico	Toda persona jurídica a la cual se haya otorgado autorización, de conformidad con el título II, para emitir dinero electrónico	artículo 2, punto 1, de la Directiva 2009/110/CE;	23
	Fondos de pensiones de empleo	Toda institución con independencia de su forma jurídica, que opere mediante sistemas de capitalización, sea jurídicamente independiente de la empresa promotora o sector y cuya actividad consista en proporcionar prestaciones de jubilación en el contexto de una actividad laboral sobre la base de un acuerdo o contrato suscrito: a) individual o colectivamente entre el empleador o empleadores y el empleado o empleados o sus representantes respectivos, o b) con trabajadores por cuenta propia, a título individual o colectivo, cuando así lo establezca simultáneamente el Derecho del Estado miembro de origen y del Estado miembro de acogida, y que dicho acuerdo tenga su origen en la precitada relación laboral;	Artículo 6, punto 1, de la Directiva (UE) 2016/2341	-
	Fondos de pensiones de empleo pequeño	Un fondo de pensiones de empleo que gestiona planes de pensiones que cuentan con menos de 100 partícipes en total;	Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo	16, 26, 28.2

Tabla 5. Listado de descripciones de herramientas según su aplicabilidad (I)

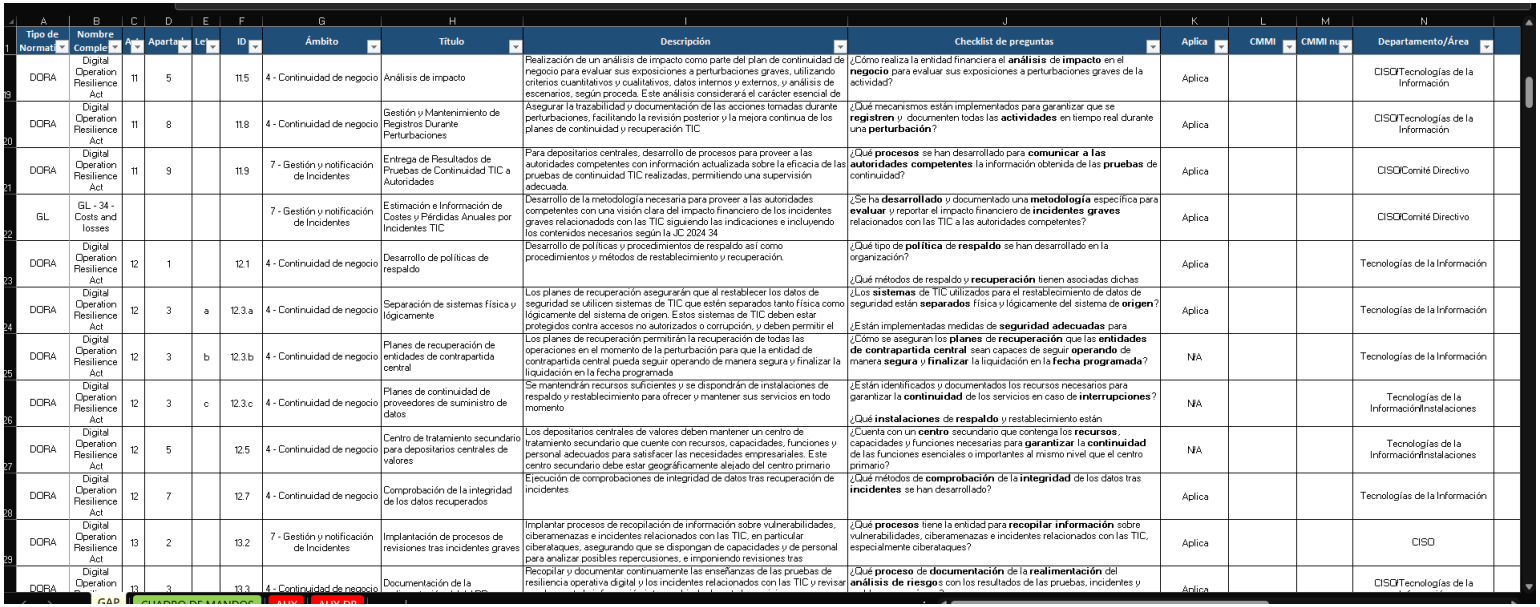
Sí	**Gestores de fondos de inversión alternativo**	Toda persona jurídica cuya actividad habitual consista en gestionar uno o varios FIA (todo organismo de inversión colectiva, así como sus compartimentos de inversión que: i) obtenga capital de una serie de inversores para invertirlo, con arreglo a una política de inversión definida, en beneficio de esos inversores, y ii) no requiera autorización de conformidad con el artículo 5 de la Directiva 2009/65/CE);	Artículo 4, apartado 1, letra b), de la Directiva 2011/61/UE	-
	Intermediarios de reaseguros	Toda persona física o jurídica, distinta de una empresa de reaseguros y de sus empleados, que, a cambio de una remuneración, emprenda o realice una actividad de distribución de reaseguros;	Artículo 2, apartado 1, punto 5, de la Directiva (UE) 2016/97 del Parlamento Europeo y del Consejo	-
	Intermediarios de seguros	toda persona física o jurídica, distinta de una empresa de seguros o de reaseguros y de sus empleados, y distinta asimismo de un intermediario de seguros complementarios, que, a cambio de una remuneración, emprenda o realice una actividad de distribución de seguros	Artículo 2, apartado 1, punto 3, de la Directiva (UE) 2016/97 del Parlamento Europeo y del Consejo	-
	Intermediarios de seguros complementarios	Toda persona física o jurídica, distinta de una entidad de crédito o de una empresa de inversión según se definen en el artículo 4, apartado 1, puntos 1 y 2, del Reglamento (UE) no 575/2013 del Parlamento Europeo y del Consejo (1), que, a cambio de una remuneración, emprenda o realice una actividad de distribución de seguros con carácter complementario, siempre y cuando concurran todas las condiciones siguientes: a) la actividad profesional principal de dicha persona física o jurídica es distinta de la de distribución de seguros; b) la persona física o jurídica solo distribuye determinados productos de seguro que son complementarios de un bien o servicio; c) los productos de seguro en cuestión no ofrecen cobertura de seguro de vida o de responsabilidad civil, salvo cuando tal cobertura sea complementaria del bien o servicio suministrado por el intermediario en su actividad profesional principal;	Artículo 2, apartado 1, punto 4, de la Directiva (UE) 2016/97 del Parlamento Europeo y del Consejo	-
	Mediana empresa	Una entidad financiera distinta de una pequeña empresa, que emplea a menos de 250 personas y cuyo volumen de negocios anual es igual o inferior a 50 millones EUR o cuyo balance anual es igual o inferior a 43 millones EUR	Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo	-
	Microempresa	Una entidad financiera distinta de un centro de negociación, una entidad de contrapartida central, un registro de operaciones o un depositario central de valores, que emplea a menos de diez personas y cuyo volumen de negocios anual o balance anual total es igual o inferior a 2 millones EUR;	Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo	5.3, 6.4, 6.5, 6.6., 8.3, 8.7, 11.3, 11.6, 11.7, 11.10, 12.4, 13.2, 13.7, 24, 25.3, 26, 28.2, 30.3,
	Proveedor intragrupo de servicios de TIC	Una empresa que forma parte de un grupo financiero y presta principalmente servicios de TIC a entidades financieras del mismo grupo o a entidades financieras que pertenecen al mismo sistema institucional de protección, también a sus sociedades matrices, filiales o sucursales o a otras entidades que compartan propiedad o control	Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo	31.8
	Proveedor tercero de servicios de TIC establecido en un tercer país	Un proveedor tercero de servicios de TIC que sea una persona jurídica establecida en un tercer país que haya celebrado un acuerdo contractual con una entidad financiera para la prestación de servicios de TIC	Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo	29.2, 31.12,
	Proveedor tercero esencial de servicios de TIC	Un proveedor tercero de servicios de TIC designado como esencial de conformidad con el artículo 31	Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo	31
	Proveedores de servicios de criptoactivos autorizados	Una persona jurídica u otra empresa cuya actividad o negocio consiste en la prestación profesional de uno o varios servicios de criptoactivos a clientes y que está autorizada a prestar servicios de criptoactivos de conformidad con el artículo 59	Artículo 3, apartado 1, punto 15 del Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo	-
	Proveedores de servicios de financiación participativa	toda persona jurídica que preste servicios de financiación participativa; «servicio de financiación participativa»: la conexión de los intereses de los inversores y de los promotores de proyectos en materia de financiación empresarial mediante el uso de plataformas de financiación participativa, que consista en cualquiera de las actividades siguientes: i) la facilitación de la concesión de préstamos, ii) la colocación sin base en un compromiso firme, como dispone el punto 7 de la sección A del anexo I de la Directiva 2014/65/UE, de valores negociables y de instrumentos admitidos para la financiación participativa emitidos por los promotores de proyectos o por una entidad instrumental, y la recepción y transmisión de órdenes de clientes, como dispone el punto 1 de dicha sección, en relación con esos valores negociables e instrumentos admitidos para la financiación participativa;	Artículo 2, apartado 1, letra e), del Reglamento (UE) 2020/1503 del Parlamento Europeo y del Consejo	-
	Proveedores de servicios de información sobre cuentas	Las personas físicas o jurídicas que presten únicamente los servicios de pago a que se refiere el punto 8 del anexo I quedarán exentas de la obligación de aplicar el procedimiento y cumplir las condiciones a que se refieren las secciones 1 y 2, con la excepción del artículo 5, apartado 1, letras a), b), e) a h), j), l), n), p) y q), el artículo 5, apartado 3, y los artículos 14 y 15. Se aplicará lo dispuesto en la sección 3, con la excepción del artículo 23, apartado 3.	Artículo 33, apartado 1, de la Directiva (UE) 2015/2366;	23
	Proveedores de servicios de suministro de datos	un proveedor de servicios de suministro de datos en el sentido de: -Sistema de información autorizado ("SIA" o, en sus siglas en inglés, "ARM") a prestar el servicio notificación del detalle de las operaciones a las autoridades competentes o a ESMA en nombre de las ESI. -Agente de publicación autorizado ("APA", en sus siglas en español e inglés) a prestar el servicio de publicación de informes de transparencia post-negociación en nombre de las ESI. -Proveedor de información consolidada ("PIC" o, en sus siglas en inglés "CTP"), autorizado a prestar el servicio de recopilación de informes de transparencia post-negociación de mercados regulados, SMN, SOC y APA y de consolidación de los mismos en un flujo de datos electrónicos continuo, que proporcione información sobre precios y volúmenes para cada instrumento financiero.	Reglamento (UE) n.o 600/2014, a que se refiere su artículo 2, apartado 1, puntos 34 a 36	10.4, 12.3
	Proveedores terceros de servicios de TIC.	Una empresa que presta servicios de TIC	Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo	-
	Registros de operaciones	Una persona jurídica que recopila y conserva de forma centralizada las inscripciones de derivados;	Artículo 2, punto 2, del Reglamento (UE) n.o 648/2012	-
	Registros de titulizaciones	Persona jurídica que recopila y conserva de forma centralizada el historial de las titulizaciones.	Artículo 2, punto 23, del Reglamento (UE) 2017/2402 del Parlamento Europeo y del Consejo	-
	Sociedades de gestión	Toda sociedad cuya actividad habitual consista en la gestión de OICVM (Organismos de Inversión Colectiva en Valores Mobiliarios) constituidos en forma de fondos comunes de inversión o de sociedades de inversión (gestión de carteras colectivas de OICVM)	Artículo 2, apartado 1, letra b), de la Directiva 2009/65/CE;	-

Tabla 6. Listado de descripciones de herramientas según su aplicabilidad (II)

No	**Los gestores de fondos de inversión alternativos tal como se contemplan en el artículo 3, apartado 2, de la Directiva 2011/61/UE;**	a)Los GFIA que, directa o indirectamente, a través de una empresa con la que el GFIA esté relacionado por motivos de gestión o control común, o por una participación directa o indirecta sustancial, gestionen carteras de FIA cuyos activos gestionados, incluidos los activos adquiridos mediante recurso al apalancamiento, no rebasen en total un umbral de 100 millones EUR, o b) los GFIA que, directa o indirectamente, a través de una empresa con la que el GFIA esté relacionado por motivos de gestión o control común, o por una participación directa o indirecta sustancial, gestionen carteras de FIA cuyos activos gestionados no rebasen en total un umbral de 500 millones EUR, cuando las carteras de los FIA consistan en FIA que no estén apalancados y no tengan derechos de reembolso que puedan ejercerse durante un período de cinco años después de la fecha de inversión inicial en cada FIA.	**Artículo 3, apartado 2, de la Directiva 2011/61/UE;**	
	Las empresas de seguros y de reaseguros tal como se contemplan en el artículo 4 de la Directiva 2009/138/CE	1. Sin perjuicio de lo dispuesto en el artículo 3 y en los artículos 5 a 10, la presente Directiva no se aplicará a la empresa de seguros que cumpla todas las condiciones que figuran a continuación: a) los ingresos anuales brutos de la empresa por primas escritas no exceden de 5 000 000 EUR; b) el total de las provisiones técnicas de la empresa, bruto de los importes recuperables procedentes de los contratos de reaseguro y de las entidades con cometido especial, a que se refiere el artículo 76, no excede de 25 000 000 EUR; c) cuando la empresa pertenece a un grupo, el total de las provisiones técnicas del grupo, bruto de los importes recuperables procedentes de los contratos de reaseguro y de las entidades con cometido especial no excede de 25 000 000 EUR; d) las actividades de la empresa no incluyen actividades de seguro o reaseguro que cubren riesgos de pasivos, créditos y cauciones excepto en aquellos casos en que estos constituyen riesgos accesorios a efectos del artículo 16, apartado 1; e) las actividades de la empresa no incluyen operaciones de reaseguro que exceden de 500 000 EUR de sus ingresos anuales brutos por primas escritas o de2 500 000 EUR de sus provisiones técnicas, bruto de los importes recuperables procedentes de los contratos de reaseguro y de las entidades con cometido especial, o más del 10 % de sus ingresos anuales brutos por primas escritas o más del 10 % de sus provisiones técnicas, bruto de los importes recuperables procedentes de los contratos de reaseguro y de las entidades con cometido especial. 2. En caso de que se supere alguno de los importes establecidos en el apartado 1 durante tres años consecutivos, la presente Directiva se aplicará a partir del cuarto año. 3. No obstante lo dispuesto en el apartado 1, la presente Directiva se aplicará a todas las empresas de seguros que soliciten autorización para ejercer actividades de seguro y reaseguro cuyos ingresos anuales brutos por primas escritas o el bruto de las provisiones técnicas de los importes recuperables de los contratos de reaseguro y de las entidades con cometido especial se espera que en los cinco años siguientes excedan cualquiera de los importes establecidos en el apartado 1. 4. La presente Directiva dejará de aplicarse a las empresas de seguros con respecto a las cuales las autoridades de supervisión hayan comprobado que cumplen todas las condiciones que figuran a continuación: a) durante los tres últimos años consecutivos no se ha superado ninguno de los límites establecidos en el apartado 1; y b) no se espera que en los próximos cinco años se supere ninguno de los importes establecidos en el apartado 1. El párrafo primero del presente artículo no se aplicará en tanto que la empresa de seguros interesada realice actividades de conformidad con los artículos 145 a 149.	**Artículo 4 de la Directiva 2009/138/CE**	
	Los fondos de pensiones de empleo que gestionen planes de pensiones que, en conjunto, no tengan más de quince partícipes en total;			
	Las personas físicas o jurídicas exentas en virtud de los artículos 2 y 3 de la Directiva 2014/65/UE;	Artículo 2 Excepciones 1. La presente Directiva no se aplicará a: a) las empresas de seguros ni a las empresas que ejerzan las actividades de reaseguro y de retrocesión contempladas en la Directiva 2009/138/CE, cuando ejerzan las actividades contempladas en dicha Directiva; b) las personas que presten servicios de inversión exclusivamente a sus empresas matrices, a sus filiales o a otras filiales de sus empresas matrices; c) las personas que presten un servicio de inversión, cuando dicho servicio se preste de manera accesoria en el marco de una actividad profesional, y siempre que esta última esté regulada por disposiciones legales o reglamentarias o por un código deontológico profesional que no excluyan la prestación de dicho servicio; d) las personas que negocien por cuenta propia con instrumentos financieros distintos de los derivados sobre materias primas, derechos de emisión, o derivados de estos, y que no presten ningún otro servicio de inversión o realicen ninguna otra actividad de inversión con instrumentos financieros distintos de los derivados sobre materias primas o de derechos de emisión o derivados de estos, a no ser que tales personas: i) sean creadores de mercado, ii) sean miembros o participantes de un mercado regulado o un SMN, o tengan un acceso electrónico directo a un centro de negociación, iii) apliquen una técnica de negociación algorítmica de alta frecuencia, o iv) negocien por cuenta propia cuando ejecutan órdenes de clientes. Las personas exentas al amparo de las letras a), i) o j), no tendrán que cumplir las condiciones establecidas en el presente punto para quedar exentas; e) los operadores con obligaciones de conformidad con arreglo a la Directiva 2003/87/CE que, cuando negocien derechos de emisión, no ejecuten órdenes de clientes y no presten servicios o actividades de inversión más que la negociación por cuenta propia, siempre y cuando no apliquen técnicas de negociación algorítmica de alta frecuencia; f) las personas que presten servicios de inversión consistentes exclusivamente en la gestión de sistemas de participación de los trabajadores; g) las personas que presten servicios de inversión que consistan únicamente en la gestión de sistemas de participación de trabajadores y en la prestación de servicios de inversión exclusivamente a sus empresas matrices, a sus filiales o a otras filiales de sus empresas matrices; h) los miembros del SEBC, a otros organismos nacionales con funciones similares en la Unión Europea, a otros organismos públicos que se encargan de la gestión de la deuda pública o intervienen en ella en la Unión Europea así como a las instituciones financieras internacionales de las que son miembros dos o más Estados miembros que tengan la intención de movilizar fondos y prestar asistencia financiera en beneficio de aquellos de sus miembros que estén sufriendo graves problemas de financiación o que corran el riesgo de padecerlos; i) las instituciones de inversión colectiva y los fondos de pensiones, independientemente de que estén o no coordinados a nivel de la Unión, ni a los depositarios y gestores de dichas instituciones; j) las personas que: i) negocien por cuenta propia, incluidos los creadores de mercado, con derivados sobre materias primas o con derechos de emisión o derivados de estos, excluidas las personas que negocien por cuenta propia cuando ejecutan órdenes de clientes, o ii) presten servicios de inversión, pero no por cuenta propia, en derivados sobre materias primas o en derechos de emisión o derivados sobre tales derechos a los clientes o proveedores de su actividad principal, siempre que:	**Artículos 2 y 3 de la Directiva 2014/65/UE;**	
	Los intermediarios de seguros, los intermediarios de reaseguros y los intermediarios de seguros complementarios que sean microempresas o pequeñas o medianas empresas			
	Las oficinas de cheques postales tal como se contemplan en el artículo 2, apartado 5, punto 3, de la Directiva 2013/36/UE.	5. La presente Directiva no se aplicará: 1) al acceso a la actividad de las empresas de inversión en la medida en que esté regulado por la Directiva 2004/39/CE, 2) a los bancos centrales, 3) a las oficinas de cheques postales, [...] 10) en España, al Instituto de Crédito Oficial,	**Artículo 2, apartado 5, punto 3, de la Directiva 2013/36/UE.**	

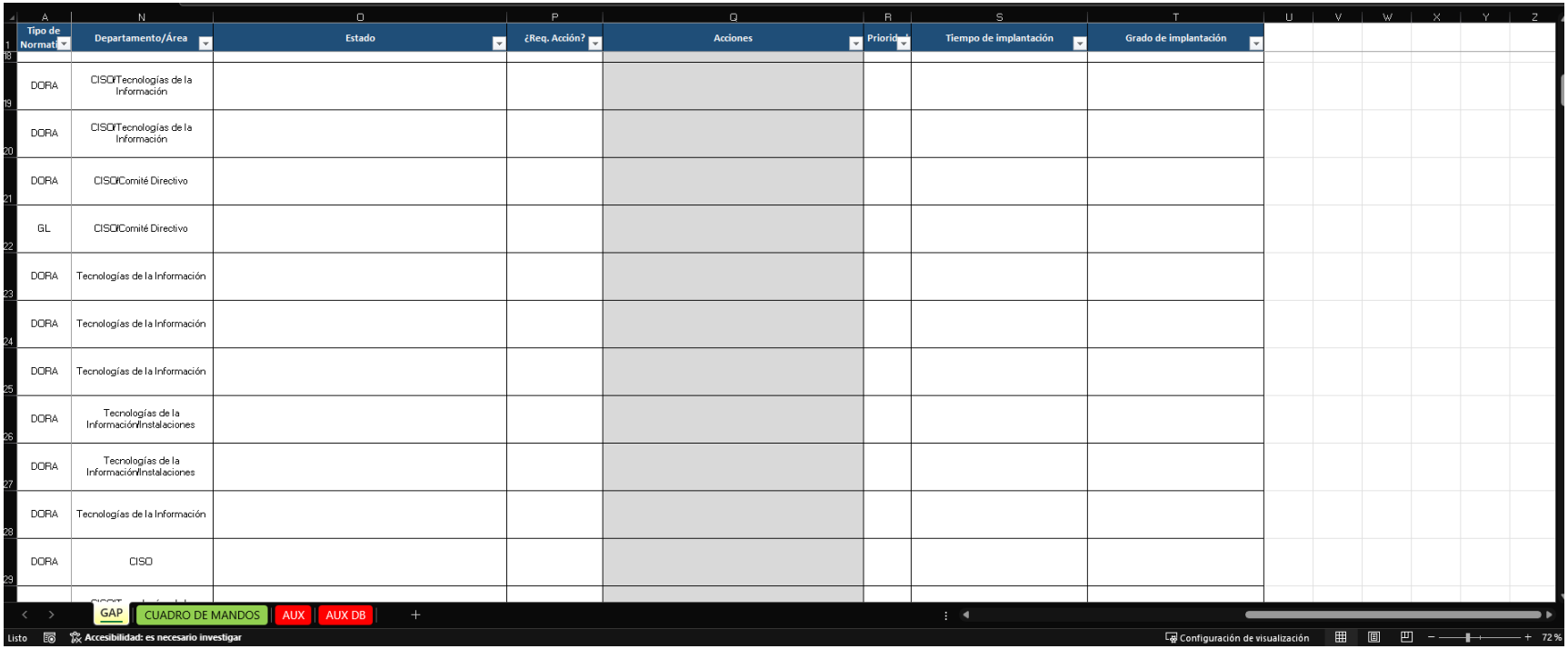
Tabla 7. Listado de descripciones de entidades según su aplicabilidad (III)

ANEXO E – IMÁGENES DE LA HERRAMIENTA PRINCIPAL ANTIGUA



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Tipo de Normati	Nombre Comple	Artí	Apartad	Let	ID	Ámbito	Título	Descripción	Checklist de preguntas	Aplica	CMMI	CMMI nu	Departamento/Área
19	DORA	Digital Operation Resilience Act	11	5		11.5	4 - Continuidad de negocio	Análisis de impacto	Realización de un análisis de impacto como parte del plan de continuidad de negocio para evaluar sus exposiciones a perturbaciones graves, utilizando criterios cuantitativos y cualitativos, datos internos y externos, y análisis de escenarios, según proceda. Este análisis considerará el carácter esencial de	¿Cómo realiza la entidad financiera el **análisis** de **impacto** en el **negocio** para evaluar sus exposiciones a perturbaciones graves de la actividad?	Aplica			CISO\Tecnologías de la Información
20	DORA	Digital Operation Resilience Act	11	8		11.8	4 - Continuidad de negocio	Gestión y Mantenimiento de Registros Durante Perturbaciones	Asegurar la trazabilidad y documentación de las acciones tomadas durante perturbaciones, facilitando la revisión posterior y la mejora continua de los planes de continuidad y recuperación TIC	¿Qué mecanismos están implementados para garantizar que se **registren** y documenten todas las **actividades** en tiempo real durante una **perturbación**?	Aplica			CISO\Tecnologías de la Información
21	DORA	Digital Operation Resilience Act	11	9		11.9	7 - Gestión y notificación de Incidentes	Entrega de Resultados de Pruebas de Continuidad TIC a Autoridades	Para depositarios centrales, desarrollo de procesos para proveer a las autoridades competentes con información actualizada sobre la eficacia de las pruebas de continuidad TIC realizadas, permitiendo una supervisión adecuada.	¿Qué **procesos** se han desarrollado para **comunicar a las autoridades competentes** la información obtenida de las **pruebas** de continuidad?	Aplica			CISO\Comité Directivo
22	GL	GL - 34 - Costs and losses					7 - Gestión y notificación de Incidentes	Estimación e Información de Costes y Pérdidas Anuales por Incidentes TIC	Desarrollo de la metodología necesaria para proveer a las autoridades competentes con una visión clara del impacto financiero de los incidentes graves relacionados con las TIC siguiendo las indicaciones e incluyendo los contenidos necesarios según la JC 2024 34	¿Se ha **desarrollado** y documentado una **metodología** específica para **evaluar** y reportar el impacto financiero de **incidentes graves** relacionados con las TIC a las autoridades competentes?	Aplica			CISO\Comité Directivo
23	DORA	Digital Operation Resilience Act	12	1		12.1	4 - Continuidad de negocio	Desarrollo de políticas de respaldo	Desarrollo de políticas y procedimientos de respaldo así como procedimientos y métodos de restablecimiento y recuperación.	¿Qué tipo de **política** de **respaldo** se han desarrollado en la organización? ¿Qué métodos de respaldo y **recuperación** tienen asociadas dichas	Aplica			Tecnologías de la Información
24	DORA	Digital Operation Resilience Act	12	3	a	12.3.a	4 - Continuidad de negocio	Separación de sistemas física y lógicamente	Los planes de recuperación asegurarán que al restablecer los datos de seguridad se utilicen sistemas de TIC que estén separados tanto física como lógicamente del sistema de origen. Estos sistemas de TIC deben estar protegidos contra accesos no autorizados o corrupción, y deben permitir el	¿Los **sistemas** de TIC utilizados para el restablecimiento de datos de seguridad están **separados** física y lógicamente del sistema de **origen**? ¿Están implementadas medidas de **seguridad adecuadas** para	Aplica			Tecnologías de la Información
25	DORA	Digital Operation Resilience Act	12	3	b	12.3.b	4 - Continuidad de negocio	Planes de recuperación de entidades de contrapartida central	Los planes de recuperación permitirán la recuperación de todas las operaciones en el momento de la perturbación para que la entidad de contrapartida central pueda seguir operando de manera segura y finalizar la liquidación en la fecha programada	¿Cómo se aseguran los **planes** de **recuperación** que las **entidades de contrapartida central** sean capaces de seguir **operando** de manera **segura** y **finalizar** la liquidación en la **fecha programada**?	N/A			Tecnologías de la Información
26	DORA	Digital Operation Resilience Act	12	3	c	12.3.c	4 - Continuidad de negocio	Planes de continuidad de proveedores de suministro de datos	Se mantendrán recursos suficientes y se dispondrán de instalaciones de respaldo y restablecimiento para ofrecer y mantener sus servicios en todo momento	¿Están identificados y documentados los recursos necesarios para garantizar la **continuidad** de los servicios en caso de **interrupciones**? ¿Qué **instalaciones** de **respaldo** y restablecimiento están	N/A			Tecnologías de la Información\Instalaciones
27	DORA	Digital Operation Resilience Act	12	5		12.5	4 - Continuidad de negocio	Centro de tratamiento secundario para depositarios centrales de valores	Los depositarios centrales de valores deben mantener un centro de tratamiento secundario que cuente con recursos, capacidades, funciones y personal adecuados para satisfacer las necesidades empresariales. Este centro secundario debe estar geográficamente alejado del centro primario	¿Cuenta con un **centro** secundario que contenga los **recursos**, capacidades y funciones necesarias para **garantizar** la **continuidad** de las funciones esenciales o importantes al mismo nivel que el centro primario?	N/A			Tecnologías de la Información\Instalaciones
28	DORA	Digital Operation Resilience Act	12	7		12.7	4 - Continuidad de negocio	Comprobación de la integridad de los datos recuperados	Ejecución de comprobaciones de integridad de datos tras recuperación de incidentes	¿Qué métodos de **comprobación** de la **integridad** de los datos tras **incidentes** se han desarrollado?	Aplica			Tecnologías de la Información
29	DORA	Digital Operation Resilience Act	13	2		13.2	7 - Gestión y notificación de Incidentes	Implantación de procesos de revisiones tras incidentes graves	Implantar procesos de recopilación de información sobre vulnerabilidades, ciberamenazas e incidentes relacionados con las TIC, en particular ciberataques, asegurando que se dispongan de capacidades y de personal para analizar posibles repercusiones, e imponiendo revisiones tras	¿Qué **procesos** tiene la entidad para **recopilar información** sobre vulnerabilidades, ciberamenazas e incidentes relacionados con las TIC, especialmente ciberataques?	Aplica			CISO
	DORA	Digital Operation	13	3		13.3	4 - Continuidad de negocio	Documentación de la	Recopilar y documentar continuamente las enseñanzas de las pruebas de resiliencia operativa digital y los incidentes relacionados con las TIC y revisar	¿Qué **proceso** de **documentación** de la **realimentación** del **análisis de riesgo**s con los resultados de las pruebas, incidentes y	Aplica			CISO\Tecnologías de la

Ilustración 8. Pestaña GAP de herramienta antigua (I)



Tipo de Normati	Departamento/Área	Estado	¿Req. Acción?	Acciones	Priorid	Tiempo de implantación	Grado de implantación
DORA	CISO\Tecnologías de la Información						
DORA	CISO\Tecnologías de la Información						
DORA	CISO\Comité Directivo						
GL	CISO\Comité Directivo						
DORA	Tecnologías de la Información						
DORA	Tecnologías de la Información						
DORA	Tecnologías de la Información						
DORA	Tecnologías de la Información\Instalaciones						
DORA	Tecnologías de la Información\Instalaciones						
DORA	Tecnologías de la Información						
DORA	CISO						

GAP | CUADRO DE MANDOS | AUX | AUX DB

Listo | Accesibilidad: es necesario investigar | Configuración de visualización | 72 %

Ilustración 9. Pestaña GAP de herramienta antigua (II)

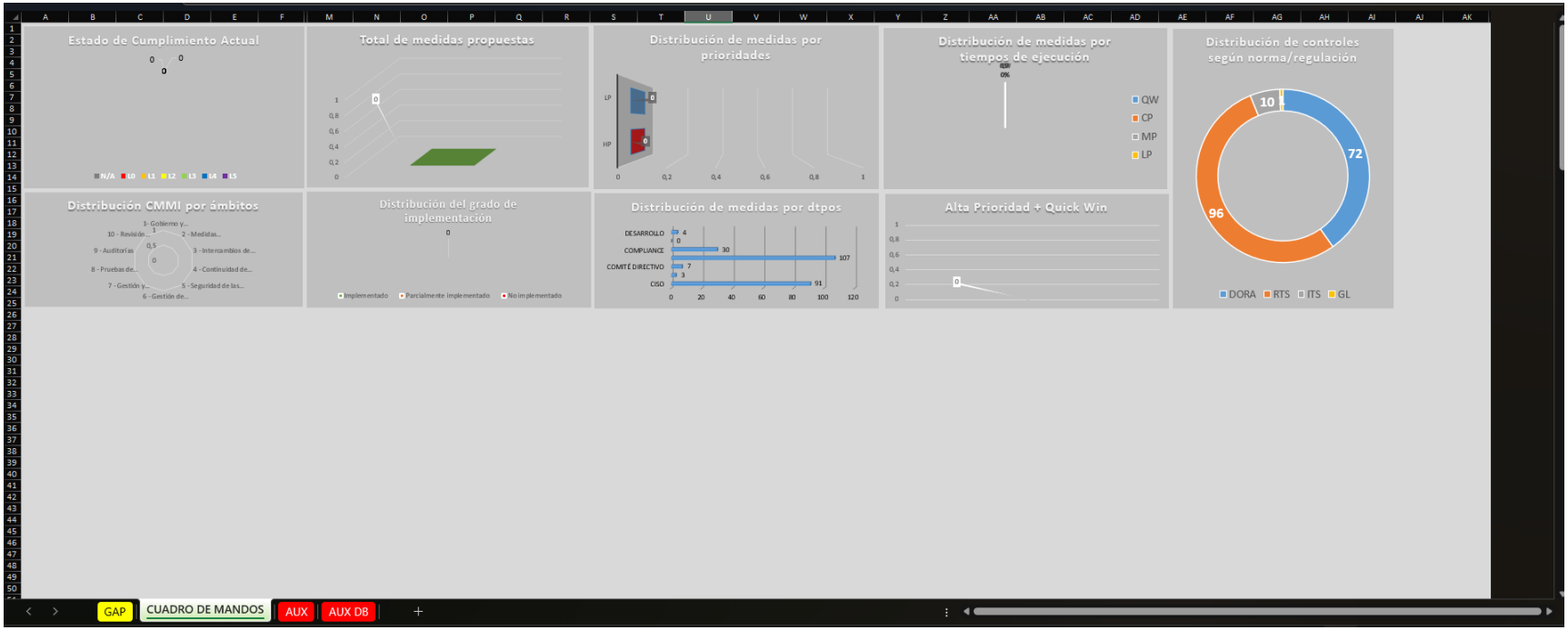
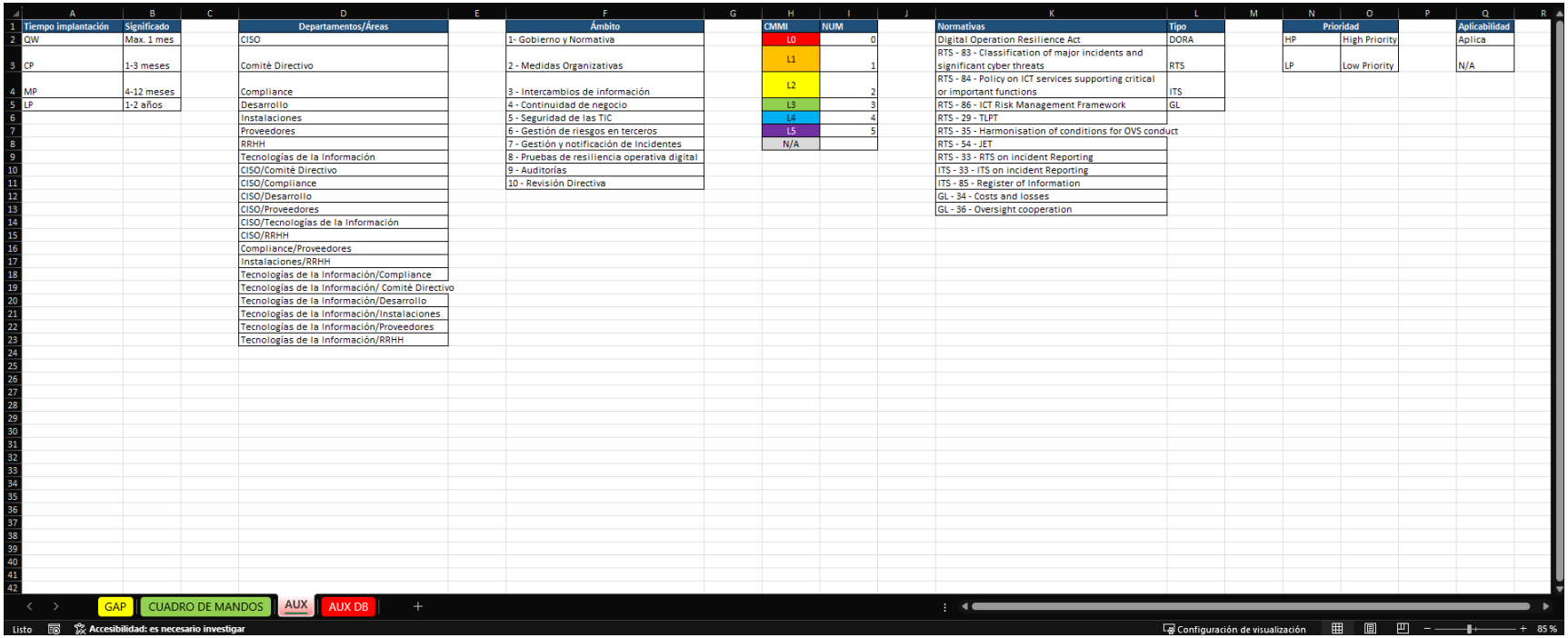


Ilustración 10. Pestaña CUADRO DE MANDOS de la herramienta antigua



Tiempo implantación	Significado
QW	Max. 1 mes
CP	1-3 meses
MP	4-12 meses
LP	1-2 años

Departamentos/Áreas
CISO
Comité Directivo
Compliance
Desarrollo
Instalaciones
Proveedores
RRHH
Tecnologías de la Información
CISO/Comité Directivo
CISO/Compliance
CISO/Desarrollo
CISO/Proveedores
CISO/Tecnologías de la Información
CISO/RRHH
Compliance/Proveedores
Instalaciones/RRHH
Tecnologías de la Información/Compliance
Tecnologías de la Información/ Comité Directivo
Tecnologías de la Información/Desarrollo
Tecnologías de la Información/Instalaciones
Tecnologías de la Información/Proveedores
Tecnologías de la Información/RRHH

Ámbito
1- Gobierno y Normativa
2 - Medidas Organizativas
3 - Intercambios de información
4 - Continuidad de negocio
5 - Seguridad de las TIC
6 - Gestión de riesgos en terceros
7 - Gestión y notificación de incidentes
8 - Pruebas de resiliencia operativa digital
9 - Auditorías
10 - Revisión Directiva

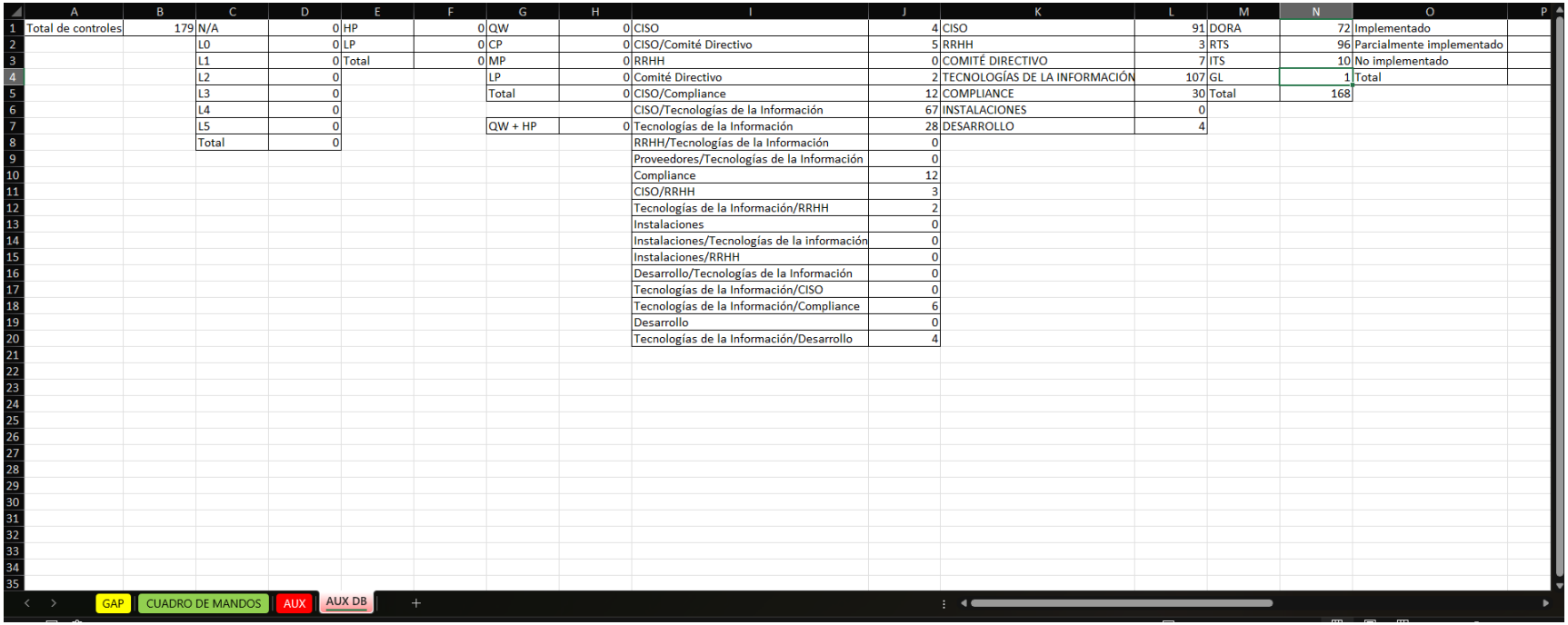
CMMI	NUM
L0	0
L1	1
L2	2
L3	3
L4	4
L5	5
N/A	

Normativas	Tipo
Digital Operation Resilience Act	DORA
RTS - 83 - Classification of major incidents and significant cyber threats	RTS
RTS - 84 - Policy on ICT services supporting critical or important functions	ITS
RTS - 86 - ICT Risk Management Framework	GL
RTS - 29 - TLPT	
RTS - 35 - Harmonisation of conditions for OVS conduct	
RTS - 54 - JET	
RTS - 33 - RTS on incident Reporting	
ITS - 33 - ITS on incident Reporting	
ITS - 85 - Register of Information	
GL - 34 - Costs and losses	
GL - 36 - Oversight cooperation	

Prioridad	
HP	High Priority
LP	Low Priority

Aplicabilidad
Aplica
N/A

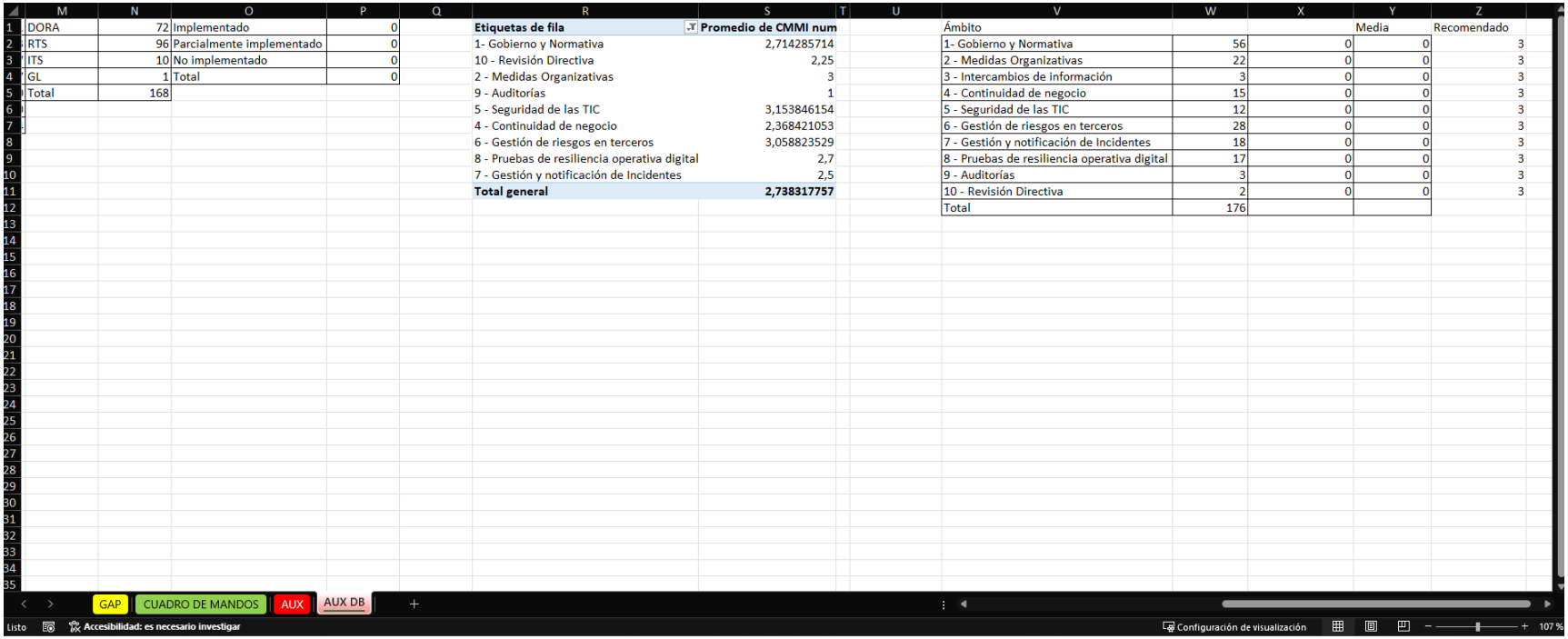
Ilustración 11. Pestaña AUX de la herramienta antigua



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	Total de controles	179	N/A	0	HP	0	QW	0	CISO	4	CISO	91	DORA	72	Implementado	
2			L0	0	LP	0	CP	0	CISO/Comité Directivo	5	RRHH	3	RTS	96	Parcialmente implementado	
3			L1	0	Total	0	MP	0	RRHH	0	COMITÉ DIRECTIVO	7	ITS	10	No implementado	
4			L2	0			LP	0	Comité Directivo	2	TECNOLOGÍAS DE LA INFORMACIÓN	107	GL	1	Total	
5			L3	0			Total	0	CISO/Compliance	12	COMPLIANCE	30	Total	168		
6			L4	0					CISO/Tecnologías de la Información	67	INSTALACIONES	0				
7			L5	0			QW + HP	0	Tecnologías de la Información	28	DESARROLLO	4				
8			Total	0					RRHH/Tecnologías de la Información	0						
9									Proveedores/Tecnologías de la Información	0						
10									Compliance	12						
11									CISO/RRHH	3						
12									Tecnologías de la Información/RRHH	2						
13									Instalaciones	0						
14									Instalaciones/Tecnologías de la información	0						
15									Instalaciones/RRHH	0						
16									Desarrollo/Tecnologías de la Información	0						
17									Tecnologías de la Información/CISO	0						
18									Tecnologías de la Información/Compliance	6						
19									Desarrollo	0						
20									Tecnologías de la Información/Desarrollo	4						
21																
22																
23																
24																
25																
26																
27																
28																
29																
30																
31																
32																
33																
34																
35																

GAP | CUADRO DE MANDOS | AUX | AUX DB

Ilustración 12. Pestaña AUX DB de la herramienta antigua (I)



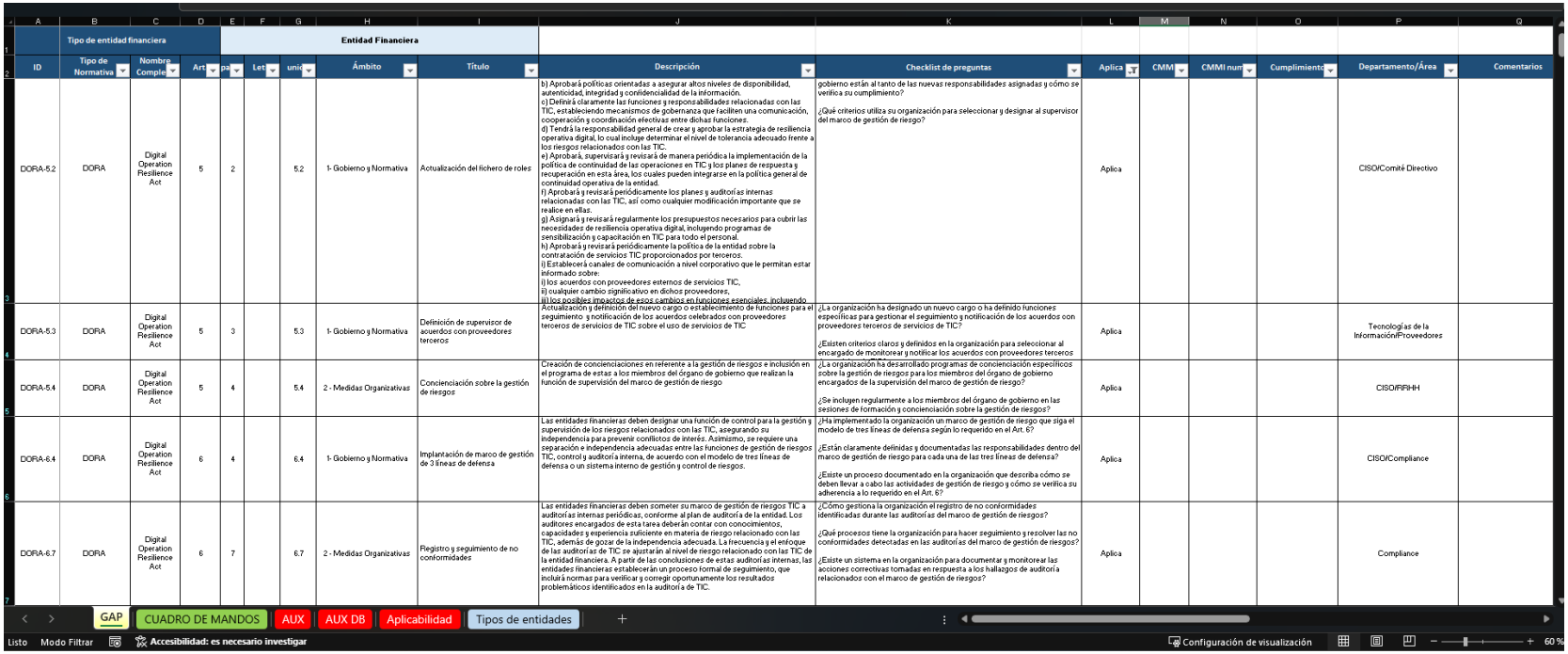
	M	N	O	P
1	DORA	72	Implementado	0
2	RTS	96	Parcialmente implementado	0
3	ITS	10	No implementado	0
4	GL	1	Total	0
5	Total	168		

Etiquetas de fila	Promedio de CMMI num
1- Gobierno y Normativa	2,714285714
10 - Revisión Directiva	2,25
2 - Medidas Organizativas	3
9 - Auditorías	1
5 - Seguridad de las TIC	3,153846154
4 - Continuidad de negocio	2,368421053
6 - Gestión de riesgos en terceros	3,058823529
8 - Pruebas de resiliencia operativa digital	2,7
7 - Gestión y notificación de Incidentes	2,5
Total general	**2,738317757**

Ámbito	W	X	Media	Recomendado
1- Gobierno y Normativa	56	0	0	3
2 - Medidas Organizativas	22	0	0	3
3 - Intercambios de información	3	0	0	3
4 - Continuidad de negocio	15	0	0	3
5 - Seguridad de las TIC	12	0	0	3
6 - Gestión de riesgos en terceros	28	0	0	3
7 - Gestión y notificación de Incidentes	18	0	0	3
8 - Pruebas de resiliencia operativa digital	17	0	0	3
9 - Auditorías	3	0	0	3
10 - Revisión Directiva	2	0	0	3
Total	176			

Ilustración 13. Pestaña AUX DB de la herramienta antigua (II)

ANEXO F - IMÁGENES DE LA HERRAMIENTA PRINCIPAL EVOLUCIONADA

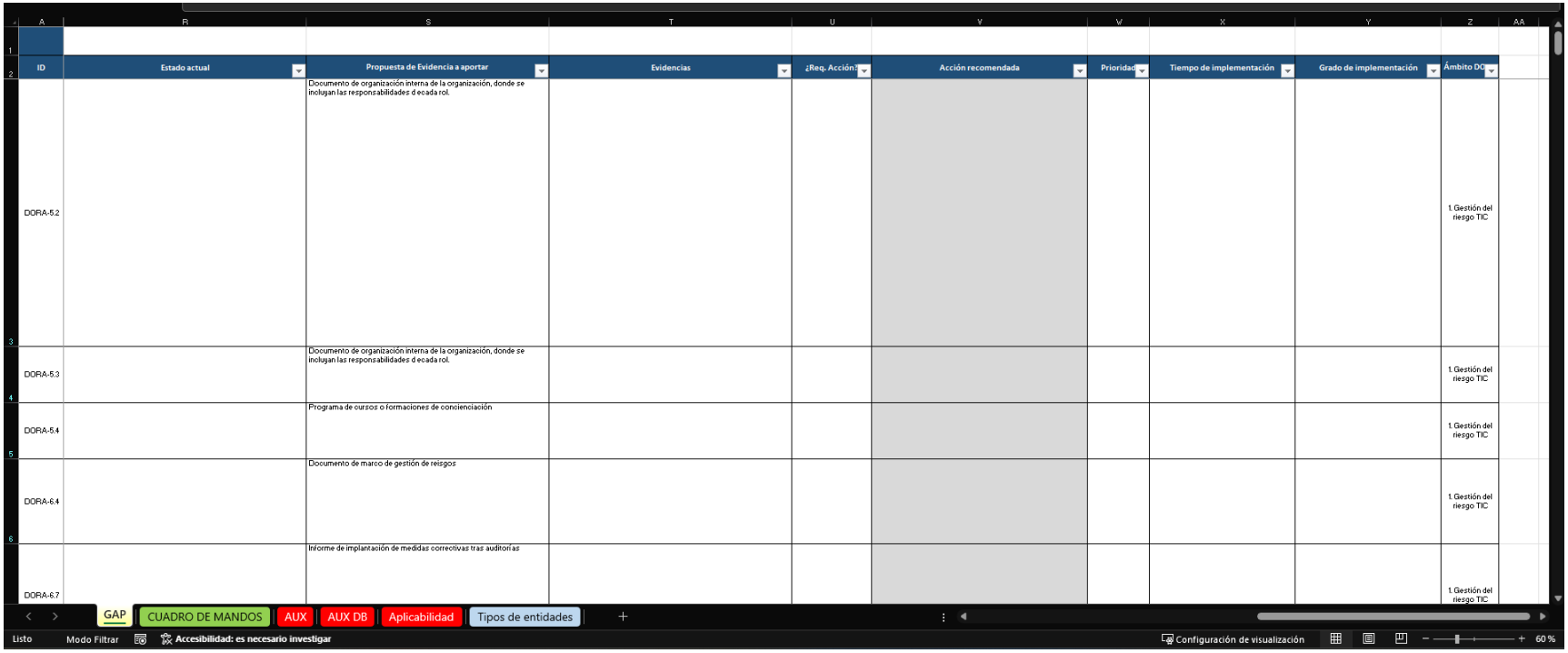


	Tipo de entidad financiera						Entidad Financiera											
	ID	Tipo de Normativa	Nombre Comple	Art	pa	Let	unid	Ámbito	Título	Descripción	Checklist de preguntas	Aplica	CMM	CMMI num	Cumplimiento	Departamento/Área	Comentarios
3	DORA-5.2	DORA	Digital Operation Resilience Act	5	2		5.2	1- Gobierno y Normativa	Actualización del fichero de roles	b) Aprobará políticas orientadas a asegurar altos niveles de disponibilidad, autenticidad, integridad y confidencialidad de la información. c) Definirá claramente las funciones y responsabilidades relacionadas con las TIC, estableciendo mecanismos de gobernanza que faciliten una comunicación, cooperación y coordinación efectivas entre dichas funciones. d) Tendrá la responsabilidad general de crear y aprobar la estrategia de resiliencia operativa digital, lo cual incluye determinar el nivel de tolerancia adecuado frente a los riesgos relacionados con las TIC. e) Aprobará, supervisará y revisará de manera periódica la implementación de la política de continuidad de las operaciones en TIC y los planes de respuesta y recuperación en esta área, los cuales pueden integrarse en la política general de continuidad operativa de la entidad. f) Aprobará y revisará periódicamente los planes y auditorías internas relacionadas con las TIC, así como cualquier modificación importante que se realice en ellas. g) Asignará y revisará regularmente los presupuestos necesarios para cubrir las necesidades de resiliencia operativa digital, incluyendo programas de sensibilización y capacitación en TIC para todo el personal. h) Aprobará y revisará periódicamente la política de la entidad sobre la contratación de servicios TIC proporcionados por terceros. i) Establecerá canales de comunicación a nivel corporativo que le permitan estar informado sobre: i) los acuerdos con proveedores externos de servicios TIC, ii) cualquier cambio significativo en dichos proveedores, iii) los posibles impactos de esos cambios en funciones esenciales, incluyendo	gobierno están al tanto de las nuevas responsabilidades asignadas y cómo se verifica su cumplimiento? ¿Qué criterios utiliza su organización para seleccionar y designar al supervisor del marco de gestión de riesgo?	Aplica				CISO/Comité Directivo	
4	DORA-5.3	DORA	Digital Operation Resilience Act	5	3		5.3	1- Gobierno y Normativa	Definición de supervisor de acuerdos con proveedores terceros	Actualización y definición del nuevo cargo o establecimiento de funciones para el seguimiento y notificación de los acuerdos celebrados con proveedores terceros de servicios de TIC sobre el uso de servicios de TIC	¿La organización ha designado un nuevo cargo o ha definido funciones específicas para gestionar el seguimiento y notificación de los acuerdos con proveedores terceros de servicios de TIC? ¿Existen criterios claros y definidos en la organización para seleccionar al encargado de monitorear y notificar los acuerdos con proveedores terceros	Aplica				Tecnologías de la Información/Proveedores	
5	DORA-5.4	DORA	Digital Operation Resilience Act	5	4		5.4	2 - Medidas Organizativas	Concienciación sobre la gestión de riesgos	Creación de concienciaciones en referente a la gestión de riesgos e inclusión en el programa de estas a los miembros del órgano de gobierno que realizan la función de supervisión del marco de gestión de riesgo	¿La organización ha desarrollado programas de concienciación específicos sobre la gestión de riesgos para los miembros del órgano de gobierno encargados de la supervisión del marco de gestión de riesgo? ¿Se incluyen regularmente a los miembros del órgano de gobierno en las sesiones de formación y concienciación sobre la gestión de riesgos?	Aplica				CISO/RRHH	
6	DORA-6.4	DORA	Digital Operation Resilience Act	6	4		6.4	1- Gobierno y Normativa	Implantación de marco de gestión de 3 líneas de defensa	Las entidades financieras deben designar una función de control para la gestión y supervisión de los riesgos relacionados con las TIC, asegurando su independencia para prevenir conflictos de interés. Asimismo, se requiere una separación e independencia adecuadas entre las funciones de gestión de riesgos TIC, control y auditoría interna, de acuerdo con el modelo de tres líneas de defensa o un sistema interno de gestión y control de riesgos.	¿Ha implementado la organización un marco de gestión de riesgo que siga el modelo de tres líneas de defensa según lo requerido en el Art. 6? ¿Están claramente definidas y documentadas las responsabilidades dentro del marco de gestión de riesgo para cada una de las tres líneas de defensa? ¿Existe un proceso documentado en la organización que describa cómo se deben llevar a cabo las actividades de gestión de riesgo y cómo se verifica su adherencia a lo requerido en el Art. 6?	Aplica				CISO/Compliance	
7	DORA-6.7	DORA	Digital Operation Resilience Act	6	7		6.7	2 - Medidas Organizativas	Registro y seguimiento de no conformidades	Las entidades financieras deben someter su marco de gestión de riesgos TIC a auditorías internas periódicas, conforme al plan de auditoría de la entidad. Los auditores encargados de esta tarea deberán contar con conocimientos, capacidades y experiencia suficiente en materia de riesgo relacionado con las TIC, además de gozar de la independencia adecuada. La frecuencia y el enfoque de las auditorías de TIC se ajustarán al nivel de riesgo relacionado con las TIC de la entidad financiera. A partir de las conclusiones de estas auditorías internas, las entidades financieras establecerán un proceso formal de seguimiento, que incluirá normas para verificar y corregir oportunamente los resultados problemáticos identificados en la auditoría de TIC.	¿Cómo gestiona la organización el registro de no conformidades identificadas durante las auditorías del marco de gestión de riesgos? ¿Qué procesos tiene la organización para hacer seguimiento y resolver las no conformidades detectadas en las auditorías del marco de gestión de riesgos? ¿Existe un sistema en la organización para documentar y monitorear las acciones correctivas tomadas en respuesta a los hallazgos de auditoría relacionados con el marco de gestión de riesgos?	Aplica				Compliance	

GAP | CUADRO DE MANDOS | AUX | AUX DB | Aplicabilidad | Tipos de entidades

Listo | Modo Filtrar | Accesibilidad: es necesario investigar | Configuración de visualización | 60 %

Ilustración 14. Pestaña GAP de la herramienta evolucionada (I)



ID	Estado actual	Propuesta de Evidencia a aportar	Evidencias	¿Req. Acción?	Acción recomendada	Prioridad	Tiempo de implementación	Grado de implementación	Ámbito DO
DORA-5.2		Documento de organización interna de la organización, donde se incluyan las responsabilidades d ecada rol.							1. Gestión del riesgo TIC
DORA-5.3		Documento de organización interna de la organización, donde se incluyan las responsabilidades d ecada rol.							1. Gestión del riesgo TIC
DORA-5.4		Programa de cursos o formaciones de concienciación							1. Gestión del riesgo TIC
DORA-6.4		Documento de marco de gestión de reisgos							1. Gestión del riesgo TIC
DORA-6.7		Informe de implantación de medidas correctivas tras auditorías							1. Gestión del riesgo TIC

Ilustración 15. Pestaña GAP de la herramienta evolucionada (II)

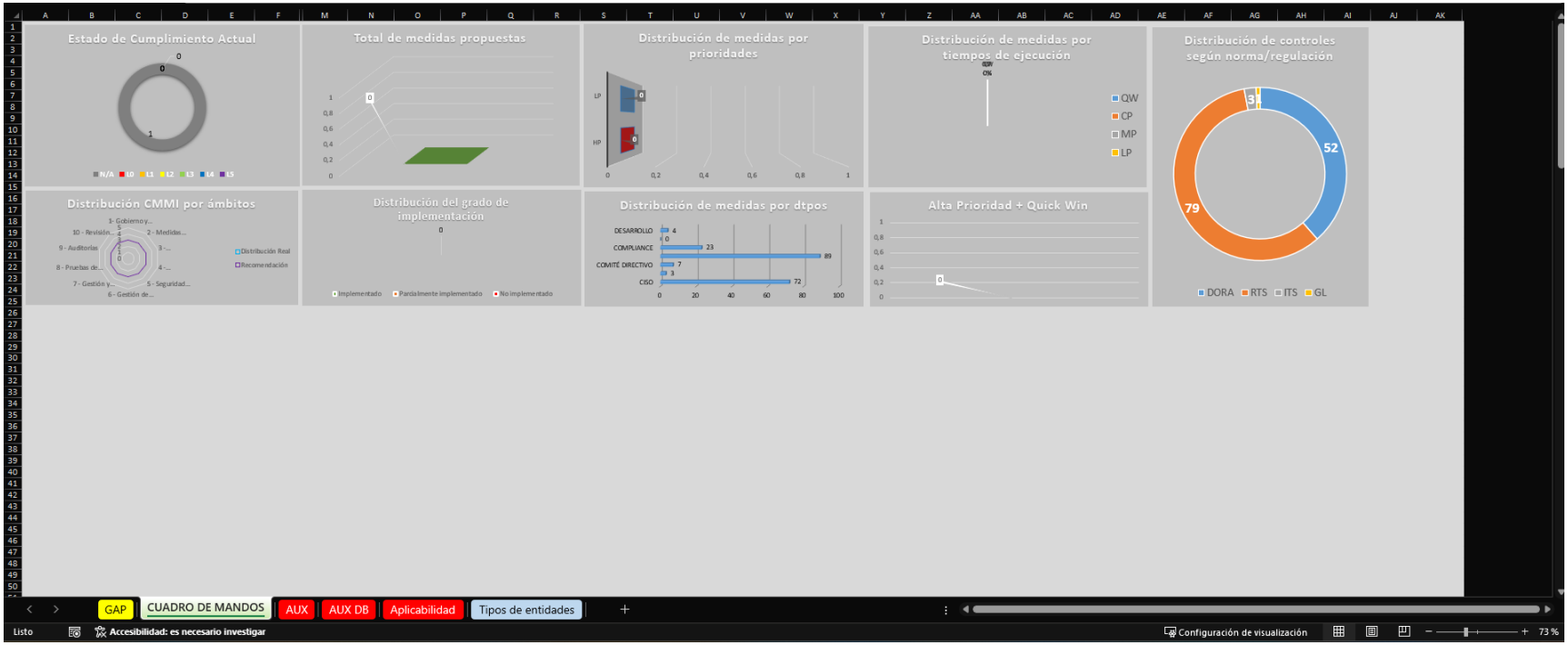
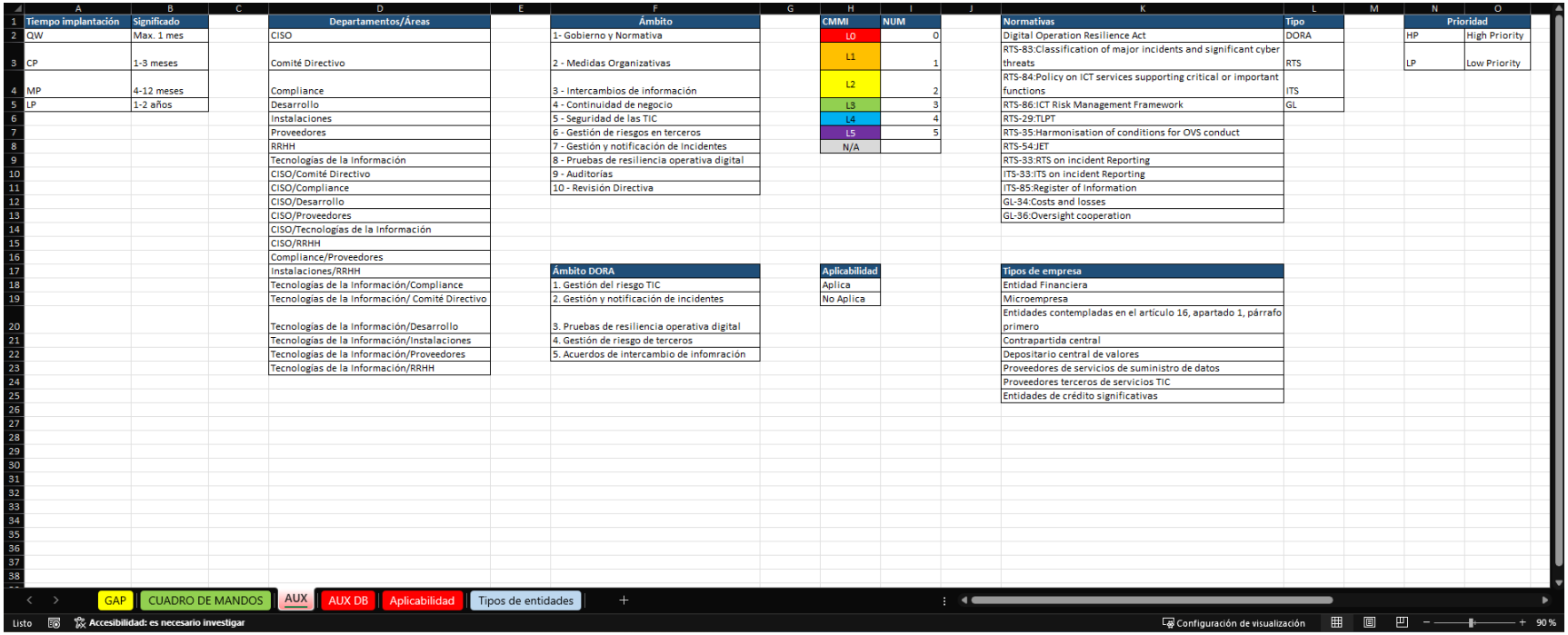


Ilustración 16. Pestaña CUADRO DE MANDOS de la herramienta evolucionada



Tiempo implantación	Significado
QW	Max. 1 mes
CP	1-3 meses
MP	4-12 meses
LP	1-2 años

Departamentos/Áreas
CISO
Comité Directivo
Compliance
Desarrollo
Instalaciones
Proveedores
RRHH
Tecnologías de la Información
CISO/Comité Directivo
CISO/Compliance
CISO/Desarrollo
CISO/Proveedores
CISO/Tecnologías de la Información
CISO/RRHH
Compliance/Proveedores
Instalaciones/RRHH
Tecnologías de la Información/Compliance
Tecnologías de la Información/ Comité Directivo
Tecnologías de la Información/Desarrollo
Tecnologías de la Información/Instalaciones
Tecnologías de la Información/Proveedores
Tecnologías de la Información/RRHH

Ámbito
1- Gobierno y Normativa
2 - Medidas Organizativas
3 - Intercambios de información
4 - Continuidad de negocio
5 - Seguridad de las TIC
6 - Gestión de riesgos en terceros
7 - Gestión y notificación de incidentes
8 - Pruebas de resiliencia operativa digital
9 - Auditorías
10 - Revisión Directiva

Ámbito DORA
1. Gestión del riesgo TIC
2. Gestión y notificación de incidentes
3. Pruebas de resiliencia operativa digital
4. Gestión de riesgo de terceros
5. Acuerdos de intercambio de infomración

CMMI	NUM
L0	0
L1	1
L2	2
L3	3
L4	4
L5	5
N/A	

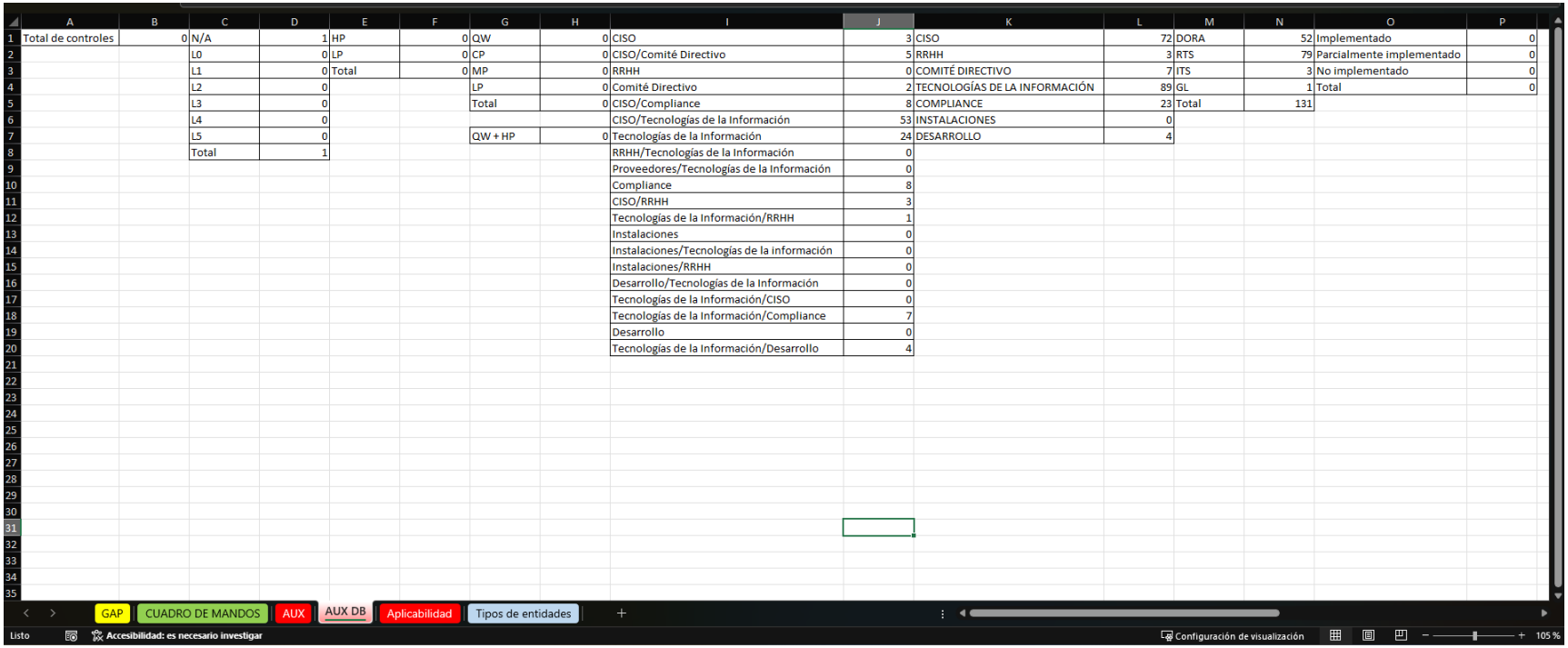
Aplicabilidad
Aplica
No Aplica

Normativas	Tipo
Digital Operation Resilience Act	DORA
RTS-83:Classification of major incidents and significant cyber threats	RTS
RTS-84:Policy on ICT services supporting critical or important functions	ITS
RTS-86:ICT Risk Management Framework	GL
RTS-29:TLPT	
RTS-35:Harmonisation of conditions for OVS conduct	
RTS-54:JET	
RTS-33:RTS on incident Reporting	
ITS-33:ITS on incident Reporting	
ITS-85:Register of Information	
GL-34:Costs and losses	
GL-36:Oversight cooperation	

Tipos de empresa
Entidad Financiera
Microempresa
Entidades contempladas en el artículo 16, apartado 1, párrafo primero
Contrapartida central
Depositario central de valores
Proveedores de servicios de suministro de datos
Proveedores terceros de servicios TIC
Entidades de crédito significativas

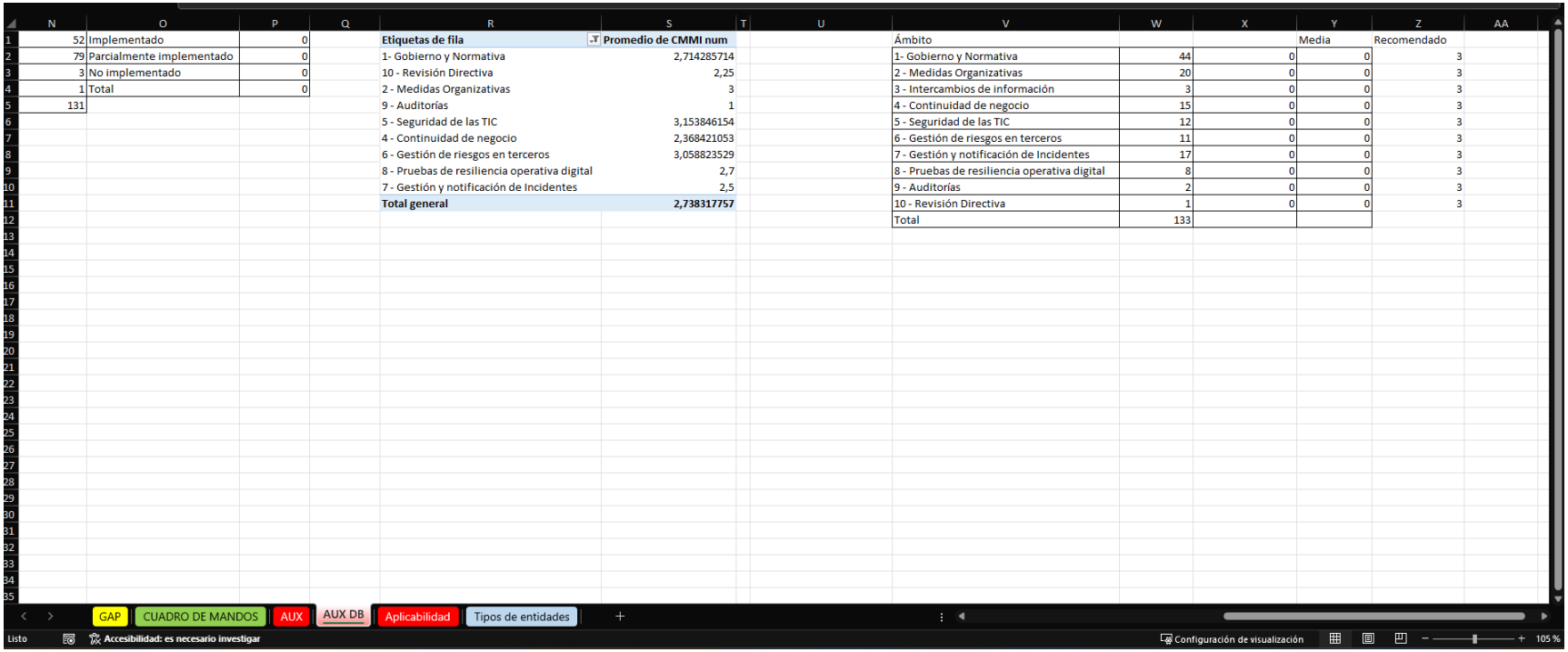
Prioridad	
HP	High Priority
LP	Low Priority

Ilustración 17. Pestaña AUX de la herramienta evolucionada



Total de controles	0	N/A	1	HP	0	QW	0	CISO	3	CISO	72	DORA	52	Implementado	0	
		L0	0	LP	0	CP	0	CISO/Comité Directivo	5	RRHH	3	RTS	79	Parcialmente implementado	0	
		L1	0	Total	0	MP	0	RRHH	0	COMITÉ DIRECTIVO	7	ITS	3	No implementado	0	
		L2	0			LP	0	Comité Directivo	2	TECNOLOGÍAS DE LA INFORMACIÓN	89	GL	1	Total	0	
		L3	0			Total	0	CISO/Compliance	8	COMPLIANCE	23	Total	131			
		L4	0					CISO/Tecnologías de la Información	53	INSTALACIONES	0					
		L5	0			QW + HP	0	Tecnologías de la Información	24	DESARROLLO	4					
		Total	1					RRHH/Tecnologías de la Información	0							
								Proveedores/Tecnologías de la Información	0							
								Compliance	8							
								CISO/RRHH	3							
								Tecnologías de la Información/RRHH	1							
								Instalaciones	0							
								Instalaciones/Tecnologías de la información	0							
								Instalaciones/RRHH	0							
								Desarrollo/Tecnologías de la Información	0							
								Tecnologías de la Información/CISO	0							
								Tecnologías de la Información/Compliance	7							
								Desarrollo	0							
								Tecnologías de la Información/Desarrollo	4							

Ilustración 18. Pestaña AUX DB de la herramienta evolucionada (I)

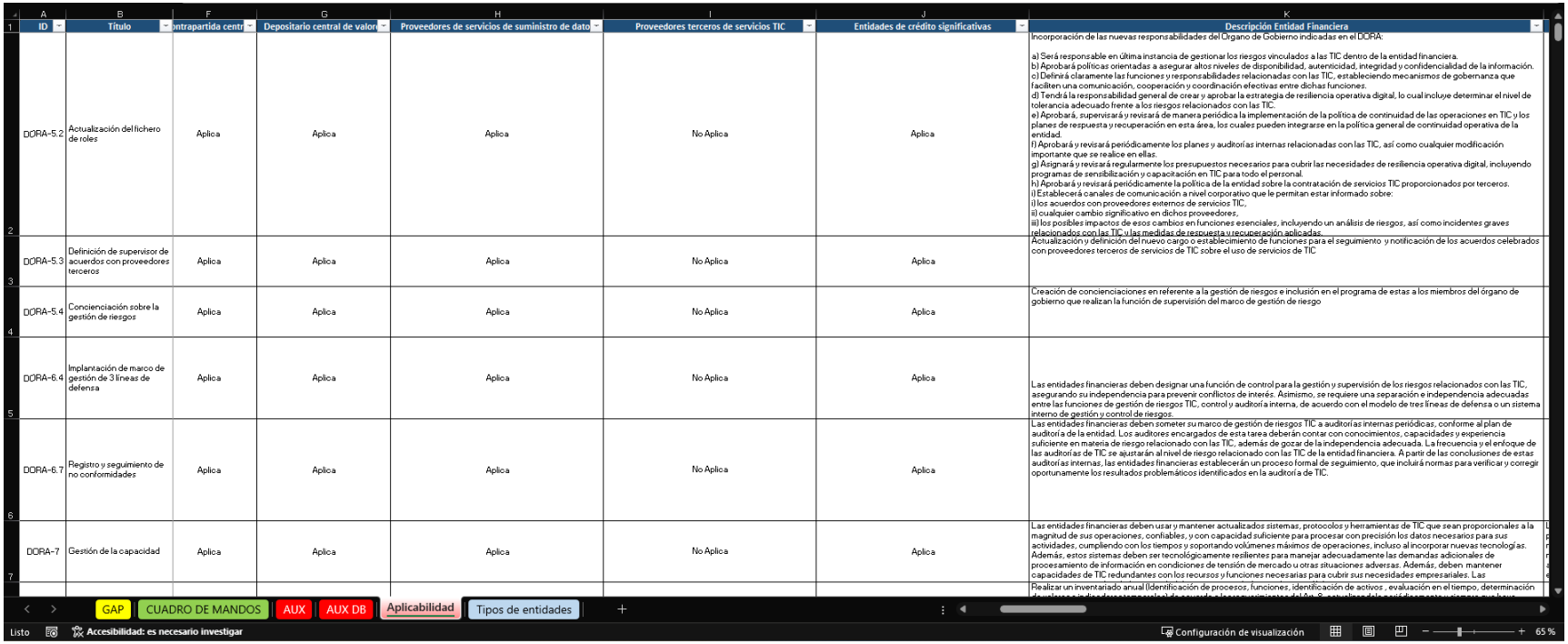


52	Implementado	0	
79	Parcialmente implementado	0	
3	No implementado	0	
1	Total	0	
131			

Etiquetas de fila	Promedio de CMMI num
1- Gobierno y Normativa	2,714285714
10 - Revisión Directiva	2,25
2 - Medidas Organizativas	3
9 - Auditorías	1
5 - Seguridad de las TIC	3,153846154
4 - Continuidad de negocio	2,368421053
6 - Gestión de riesgos en terceros	3,058823529
8 - Pruebas de resiliencia operativa digital	2,7
7 - Gestión y notificación de Incidentes	2,5
Total general	**2,738317757**

Ámbito			Media	Recomendado
1- Gobierno y Normativa	44	0	0	3
2 - Medidas Organizativas	20	0	0	3
3 - Intercambios de información	3	0	0	3
4 - Continuidad de negocio	15	0	0	3
5 - Seguridad de las TIC	12	0	0	3
6 - Gestión de riesgos en terceros	11	0	0	3
7 - Gestión y notificación de Incidentes	17	0	0	3
8 - Pruebas de resiliencia operativa digital	8	0	0	3
9 - Auditorías	2	0	0	3
10 - Revisión Directiva	1	0	0	3
Total	133			

Ilustración 19. Pestaña AUX DB de la herramienta evolucionada (II)

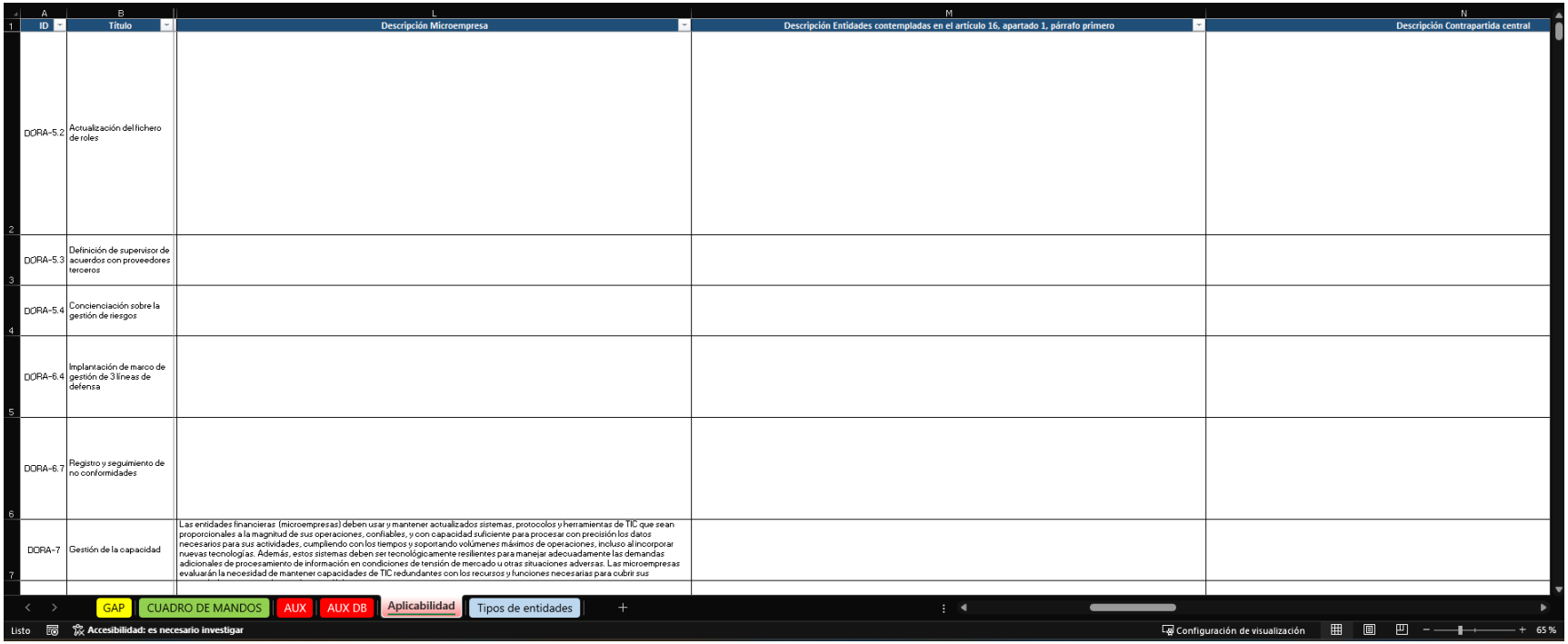


	A	B	F	G	H	I	J	K
1	ID	Título	ontrapartida centr	Depositario central de valor	Proveedores de servicios de suministro de dato	Proveedores terceros de servicios TIC	Entidades de crédito significativas	Descripción Entidad Financiera
2	DORA-5.2	Actualización del fichero de roles	Aplica	Aplica	Aplica	No Aplica	Aplica	Incorporación de las nuevas responsabilidades del Órgano de Gobierno indicadas en el DORA: a) Será responsable en última instancia de gestionar los riesgos vinculados a las TIC dentro de la entidad financiera. b) Aprobará políticas orientadas a asegurar altos niveles de disponibilidad, autenticidad, integridad y confidencialidad de la información. c) Definirá claramente las funciones y responsabilidades relacionadas con las TIC, estableciendo mecanismos de gobernanza que faciliten una comunicación, cooperación y coordinación efectivas entre dichas funciones. d) Tendrá la responsabilidad general de crear y aprobar la estrategia de resiliencia operativa digital, lo cual incluye determinar el nivel de tolerancia adecuado frente a los riesgos relacionados con las TIC. e) Aprobará, supervisará y revisará de manera periódica la implementación de la política de continuidad de las operaciones en TIC y los planes de respuesta y recuperación en esta área, los cuales pueden integrarse en la política general de continuidad operativa de la entidad. f) Aprobará y revisará periódicamente los planes y auditorías internas relacionadas con las TIC, así como cualquier modificación importante que se realice en ellas. g) Asignará y revisará regularmente los presupuestos necesarios para cubrir las necesidades de resiliencia operativa digital, incluyendo programas de sensibilización y capacitación en TIC para todo el personal. h) Aprobará y revisará periódicamente la política de la entidad sobre la contratación de servicios TIC proporcionados por terceros. i) Establecerá canales de comunicación a nivel corporativo que le permitan estar informado sobre: i) los acuerdos con proveedores externos de servicios TIC, ii) cualquier cambio significativo en dichos proveedores, iii) los posibles impactos de esos cambios en funciones esenciales, incluyendo un análisis de riesgos, así como incidentes graves relacionados con las TIC y las medidas de respuesta y recuperación aplicadas.
3	DORA-5.3	Definición de supervisor de acuerdos con proveedores terceros	Aplica	Aplica	Aplica	No Aplica	Aplica	Actualización y definición del nuevo cargo o establecimiento de funciones para el seguimiento y notificación de los acuerdos celebrados con proveedores terceros de servicios de TIC sobre el uso de servicios de TIC
4	DORA-5.4	Concienciación sobre la gestión de riesgos	Aplica	Aplica	Aplica	No Aplica	Aplica	Creación de concienciaciones en referente a la gestión de riesgos e inclusión en el programa de estas a los miembros del órgano de gobierno que realizan la función de supervisión del marco de gestión de riesgo
5	DORA-6.4	Implantación de marco de gestión de 3 líneas de defensa	Aplica	Aplica	Aplica	No Aplica	Aplica	Las entidades financieras deben designar una función de control para la gestión y supervisión de los riesgos relacionados con las TIC, asegurando su independencia para prevenir conflictos de interés. Asimismo, se requiere una separación e independencia adecuadas entre las funciones de gestión de riesgos TIC, control y auditoría interna, de acuerdo con el modelo de tres líneas de defensa o un sistema interno de gestión y control de riesgos.
6	DORA-6.7	Registro y seguimiento de no conformidades	Aplica	Aplica	Aplica	No Aplica	Aplica	Las entidades financieras deben someter su marco de gestión de riesgos TIC a auditorías internas periódicas, conforme al plan de auditoría de la entidad. Los auditores encargados de esta tarea deberán contar con conocimientos, capacidades y experiencia suficiente en materia de riesgo relacionado con las TIC, además de gozar de la independencia adecuada. La frecuencia y el enfoque de las auditorías de TIC se ajustarán al nivel de riesgo relacionado con las TIC de la entidad financiera. A partir de las conclusiones de estas auditorías internas, las entidades financieras establecerán un proceso formal de seguimiento, que incluirá normas para verificar y corregir oportunamente los resultados problemáticos identificados en la auditoría de TIC.
7	DORA-7	Gestión de la capacidad	Aplica	Aplica	Aplica	No Aplica	Aplica	Las entidades financieras deben usar y mantener actualizados sistemas, protocolos y herramientas de TIC que sean proporcionales a la magnitud de sus operaciones, confiables, y con capacidad suficiente para procesar con precisión los datos necesarios para sus actividades, cumpliendo con los tiempos y soportando volúmenes máximos de operaciones, incluso al incorporar nuevas tecnologías. Además, estos sistemas deben ser tecnológicamente resilientes para manejar adecuadamente las demandas adicionales de procesamiento de información en condiciones de tensión de mercado u otras situaciones adversas. Además, deben mantener capacidades de TIC redundantes con los recursos y funciones necesarias para cubrir sus necesidades empresariales. Las
								Realizar un inventariado anual (Identificación de procesos, funciones, identificación de activos , evaluación en el tiempo, determinación

GAP | CUADRO DE MANDOS | AUX | AUX DB | Aplicabilidad | Tipos de entidades

Listo | Accesibilidad: es necesario investigar | Configuración de visualización | 65 %

Ilustración 20. Pestaña Aplicabilidad de la herramienta evolucionada (I)



ID	Título	Descripción Microempresa	Descripción Entidades contempladas en el artículo 16, apartado 1, párrafo primero	Descripción Contrapartida central
DORA-5.2	Actualización del fichero de roles			
DORA-5.3	Definición de supervisor de acuerdos con proveedores terceros			
DORA-5.4	Concienciación sobre la gestión de riesgos			
DORA-6.4	Implantación de marco de gestión de 3 líneas de defensa			
DORA-6.7	Registro y seguimiento de no conformidades			
DORA-7	Gestión de la capacidad	Las entidades financieras (microempresas) deben usar y mantener actualizados sistemas, protocolos y herramientas de TIC que sean proporcionales a la magnitud de sus operaciones, confiables, y con capacidad suficiente para procesar con precisión los datos necesarios para sus actividades, cumpliendo con los tiempos y soportando volúmenes máximos de operaciones, incluso al incorporar nuevas tecnologías. Además, estos sistemas deben ser tecnológicamente resilientes para manejar adecuadamente las demandas adicionales de procesamiento de información en condiciones de tensión de mercado u otras situaciones adversas. Las microempresas evaluarán la necesidad de mantener capacidades de TIC redundantes con los recursos y funciones necesarias para cubrir sus		

Ilustración 21. Pestaña Aplicabilidad de la herramienta evolucionada (II)

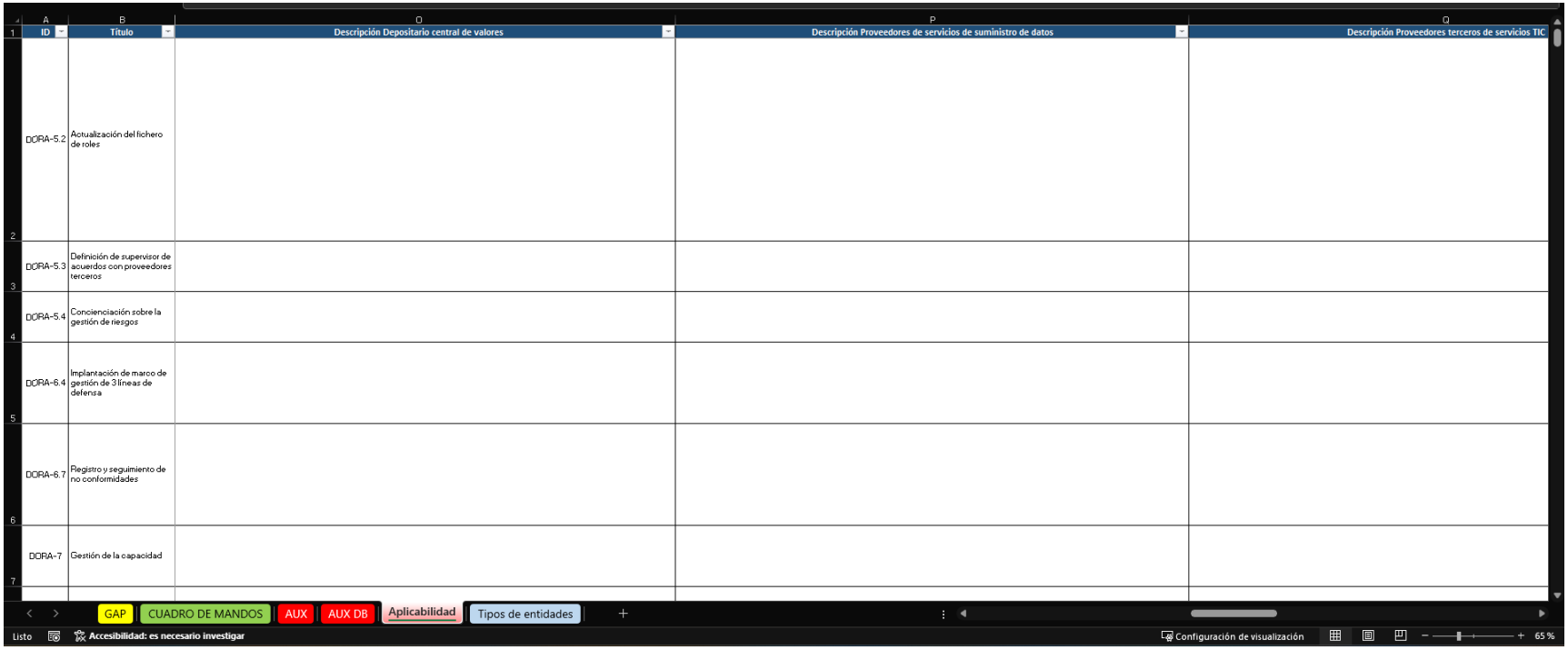
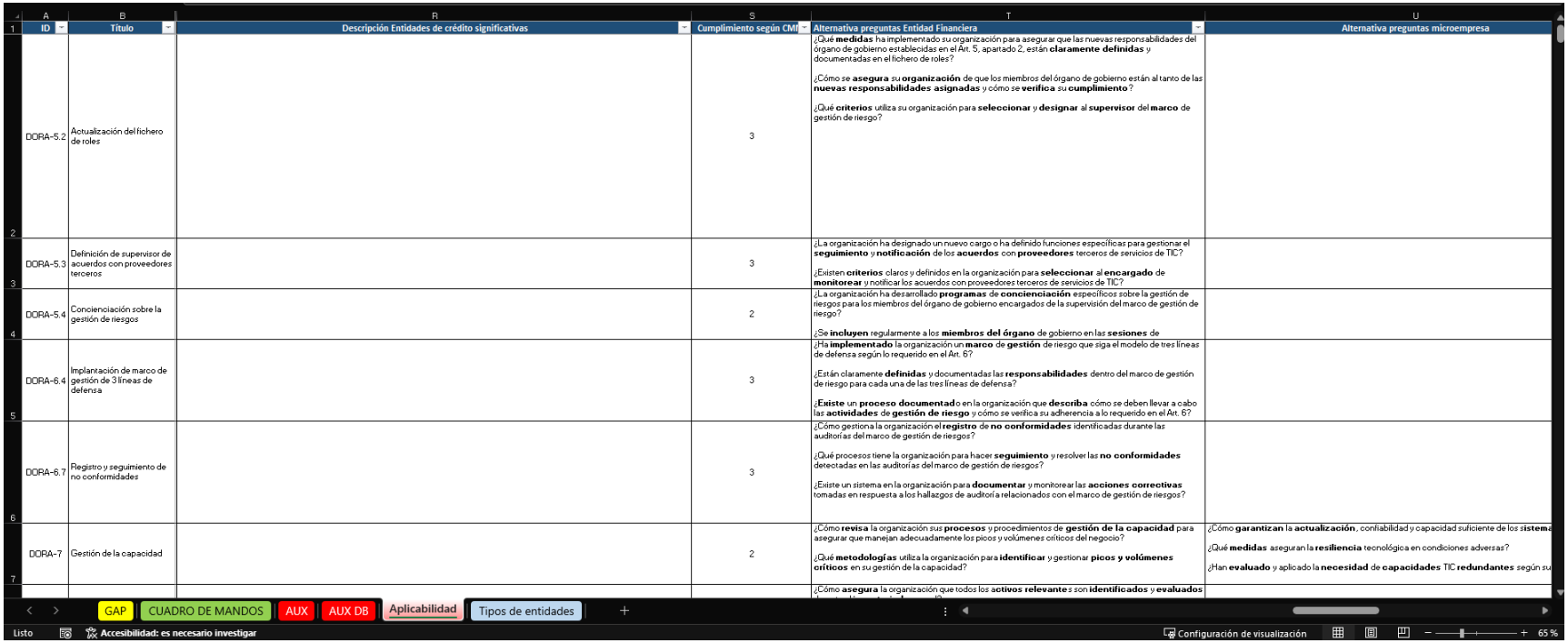
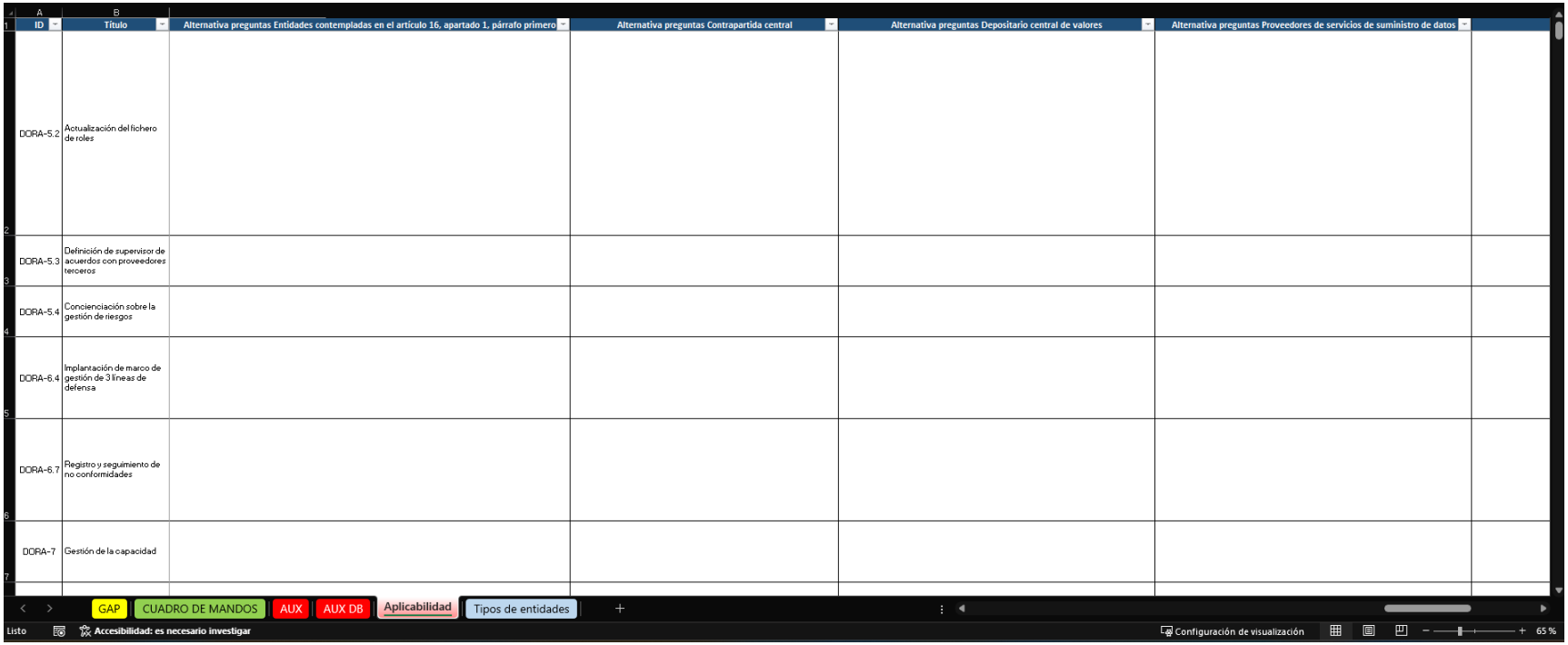


Ilustración 22. Pestaña Aplicabilidad de la herramienta evolucionada (III)



ID	Título	Descripción Entidades de crédito significativas	Cumplimiento según CMF	Alternativa preguntas Entidad Financiera	Alternativa preguntas microempresa
DORA-5.2	Actualización del fichero de roles		3	¿Qué **medidas** ha implementado su organización para asegurar que las nuevas responsabilidades del órgano de gobierno establecidas en el Art. 5, apartado 2, están **claramente definidas** y documentadas en el fichero de roles? ¿Cómo se **asegura** su **organización** de que los miembros del órgano de gobierno están al tanto de las **nuevas responsabilidades asignadas** y cómo se **verifica** su **cumplimiento**? ¿Qué **criterios** utiliza su organización para **seleccionar** y **designar** al **supervisor** del **marco** de gestión de riesgo?	
DORA-5.3	Definición de supervisor de acuerdos con proveedores terceros		3	¿La organización ha designado un nuevo cargo o ha definido funciones específicas para gestionar el **seguimiento** y **notificación** de los **acuerdos** con **proveedores** terceros de servicios de TIC? ¿Existen **criterios** claros y definidos en la organización para **seleccionar** al **encargado** de **monitorear** y notificar los acuerdos con proveedores terceros de servicios de TIC?	
DORA-5.4	Concienciación sobre la gestión de riesgos		2	¿La organización ha desarrollado **programas** de **concienciación** específicos sobre la gestión de riesgos para los miembros del órgano de gobierno encargados de la supervisión del marco de gestión de riesgo? ¿Se **incluyen** regularmente a los **miembros del órgano** de gobierno en las **sesiones** de	
DORA-6.4	Implantación de marco de gestión de 3 líneas de defensa		3	¿Ha **implementado** la organización un **marco** de **gestión** de riesgo que siga el modelo de tres líneas de defensa según lo requerido en el Art. 6? ¿Están claramente **definidas** y documentadas las **responsabilidades** dentro del marco de gestión de riesgo para cada una de las tres líneas de defensa? ¿**Existe** un **proceso documentad**o en la organización que **describa** cómo se deben llevar a cabo las **actividades** de **gestión de riesgo** y cómo se verifica su adherencia a lo requerido en el Art. 6?	
DORA-6.7	Registro y seguimiento de no conformidades		3	¿Cómo gestiona la organización el **registro** de **no conformidades** identificadas durante las auditorías del marco de gestión de riesgos? ¿Qué procesos tiene la organización para hacer **seguimiento** y resolver las **no conformidades** detectadas en las auditorías del marco de gestión de riesgos? ¿Existe un sistema en la organización para **documentar** y monitorear las **acciones correctivas** tomadas en respuesta a los hallazgos de auditoría relacionados con el marco de gestión de riesgos?	
DORA-7	Gestión de la capacidad		2	¿Cómo **revisa** la organización sus **procesos** y procedimientos de **gestión de la capacidad** para asegurar que manejan adecuadamente los picos y volúmenes críticos del negocio? ¿Qué **metodologías** utiliza la organización para **identificar** y gestionar **picos y volúmenes críticos** en su gestión de la capacidad?	¿Cómo **garantizan** la **actualización**, confiabilidad y capacidad suficiente de los **sistema** ¿Qué **medidas** aseguran la **resiliencia** tecnológica en condiciones adversas? ¿Han **evaluado** y aplicado la **necesidad** de **capacidades** TIC **redundantes** según su
				¿Cómo **asegura** la organización que todos los **activos relevante**s son **identificados** y **evaluados**	

Ilustración 23. Pestaña Aplicabilidad de la herramienta evolucionada (IV)



ID	Título	Alternativa preguntas Entidades contempladas en el artículo 16, apartado 1, párrafo primero	Alternativa preguntas Contrapartida central	Alternativa preguntas Depositario central de valores	Alternativa preguntas Proveedores de servicios de suministro de datos
DORA-5.2	Actualización del fichero de roles				
DORA-5.3	Definición de supervisor de acuerdos con proveedores terceros				
DORA-5.4	Concienciación sobre la gestión de riesgos				
DORA-6.4	Implantación de marco de gestión de 3 líneas de defensa				
DORA-6.7	Registro y seguimiento de no conformidades				
DORA-7	Gestión de la capacidad				

Ilustración 24. Pestaña Aplicabilidad de la herramienta evolucionada (V)

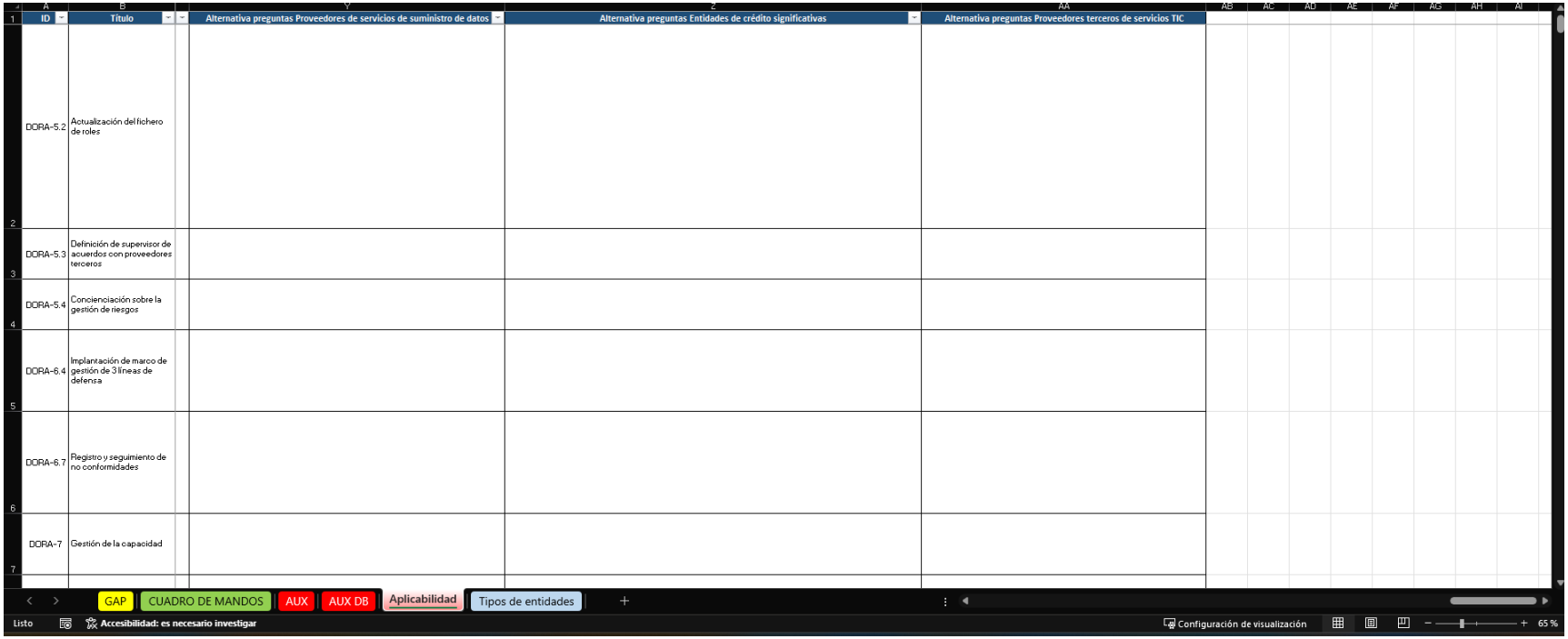


Ilustración 25. Pestaña Aplicabilidad de la herramienta evolucionada (VI)

ANEXO G – IMÁGENES DE LA HERRAMIENTA ENTREGADA AL CLIENTE

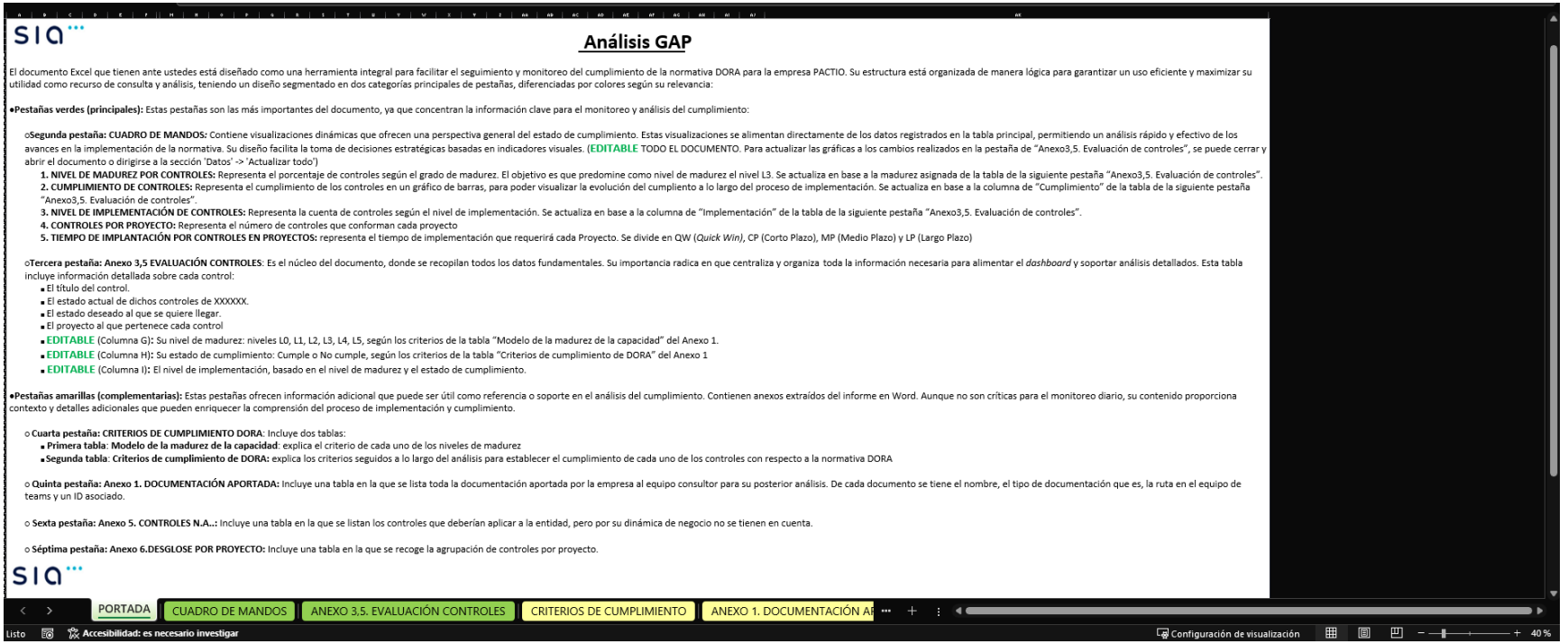


Ilustración 26. Portada de la herramienta entregada al cliente

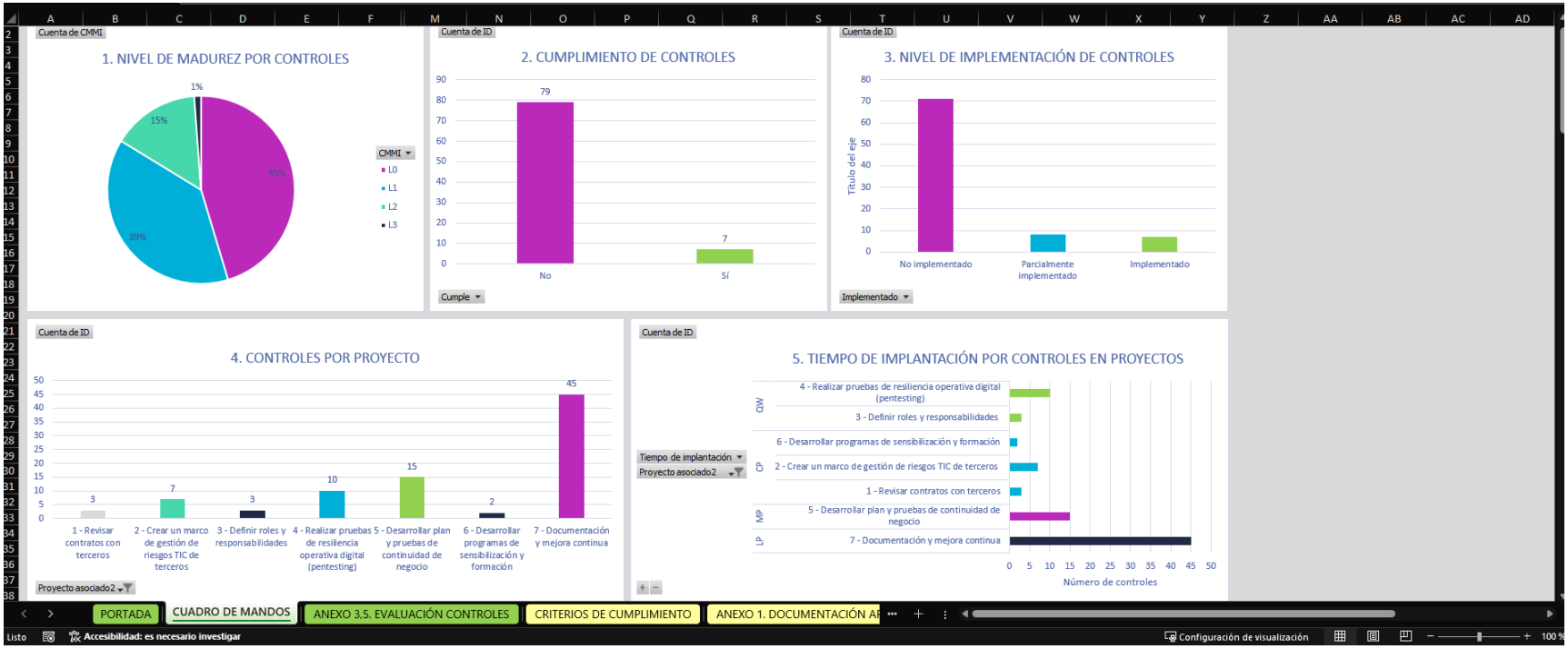
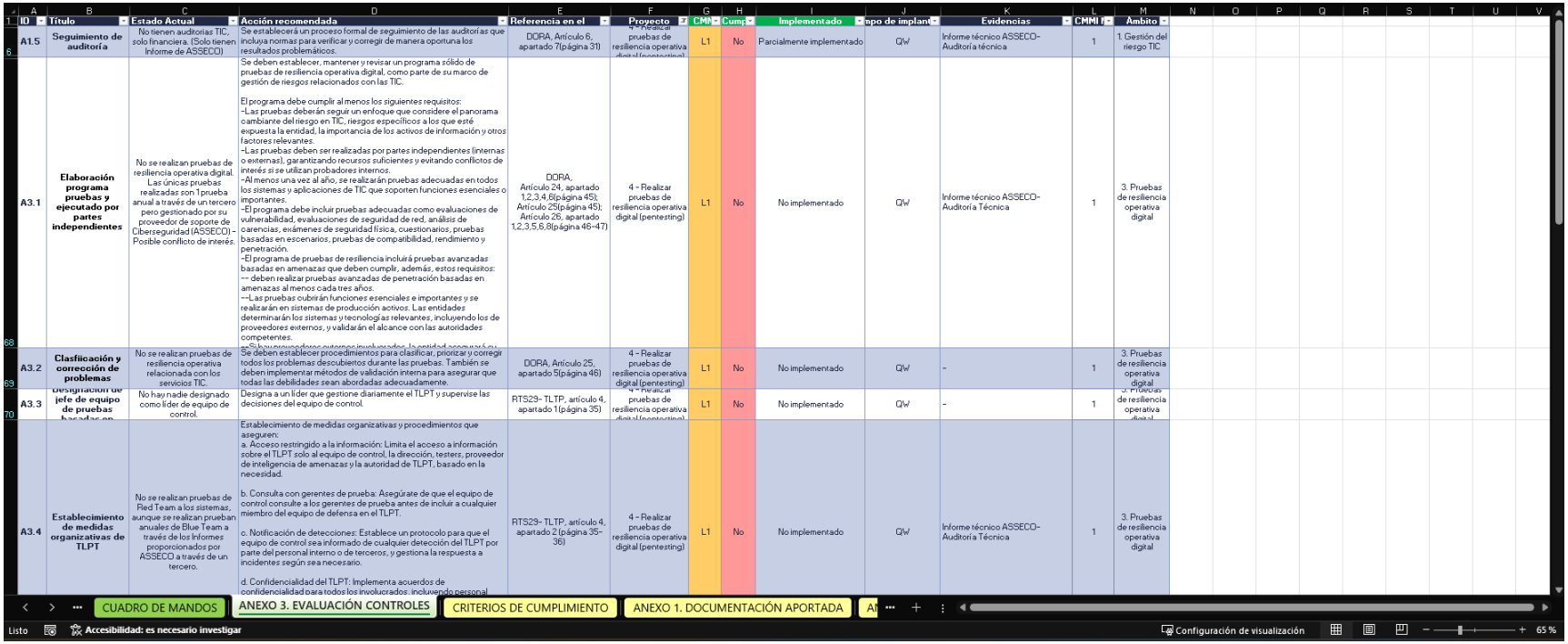


Ilustración 27. Pestaña CUADRO DE MANDOS de la herramienta entregada

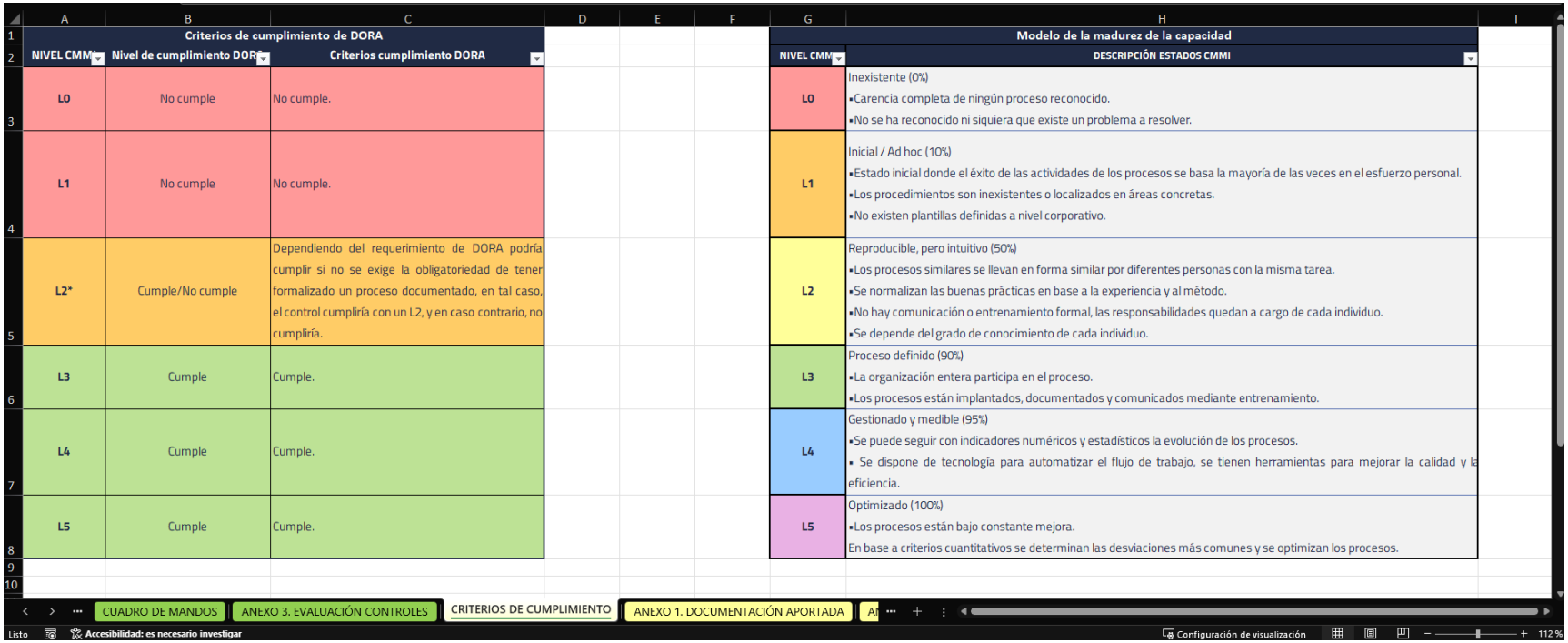


ID	Título	Estado Actual	Acción recomendada	Referencia en el	Proyecto	CMM	Cump	Implementado	Tipo de implant	Evidencias	CMMI	Ámbito
A1.5	Seguimiento de auditoría	No tienen auditorías TIC, solo financiera. (Solo tienen Informe de ASSECO)	Se establecerá un proceso formal de seguimiento de las auditorías que incluya normas para verificar y corregir de manera oportuna los resultados problemáticos.	DORA, Artículo 6, apartado 7(página 31)	4 - Realizar pruebas de resiliencia operativa digital (pentesting)	L1	No	Parcialmente implementado	Q/W	Informe técnico ASSECO-Auditoría técnica	1	1. Gestión del riesgo TIC
A3.1	Elaboración programa pruebas y ejecutado por partes independientes	No se realizan pruebas de resiliencia operativa digital. Las únicas pruebas realizadas son 1 prueba anual a través de un tercero pero gestionado por su proveedor de soporte de Ciberseguridad (ASSECO) - Posible conflicto de interés.	Se deben establecer, mantener y revisar un programa sólido de pruebas de resiliencia operativa digital, como parte de su marco de gestión de riesgos relacionados con las TIC. El programa debe cumplir al menos los siguientes requisitos: -Las pruebas deberán seguir un enfoque que considere el panorama cambiante del riesgo en TIC, riesgos específicos a los que esté expuesta la entidad, la importancia de los activos de información y otros factores relevantes. -Las pruebas deben ser realizadas por partes independientes (internas o externas), garantizando recursos suficientes y evitando conflictos de interés si se utilizan probadores internos. -Al menos una vez al año, se realizarán pruebas adecuadas en todos los sistemas y aplicaciones de TIC que soporten funciones esenciales o importantes. -El programa debe incluir pruebas adecuadas como evaluaciones de vulnerabilidad, evaluaciones de seguridad de red, análisis de carencias, exámenes de seguridad física, cuestionarios, pruebas basadas en escenarios, pruebas de compatibilidad, rendimiento y penetración. -El programa de pruebas de resiliencia incluirá pruebas avanzadas basadas en amenazas que deben cumplir, además, estos requisitos: -- deben realizar pruebas avanzadas de penetración basadas en amenazas al menos cada tres años. --Las pruebas cubrirán funciones esenciales e importantes y se realizarán en sistemas de producción activos. Las entidades determinarán los sistemas y tecnologías relevantes, incluyendo los de proveedores externos, y validarán el alcance con las autoridades competentes.	DORA, Artículo 24, apartado 1,2,3,4,6(página 45); Artículo 25(página 45); Artículo 26, apartado 1,2,3,5,6,8(página 46-47)	4 - Realizar pruebas de resiliencia operativa digital (pentesting)	L1	No	No implementado	Q/W	Informe técnico ASSECO-Auditoría Técnica	1	3. Pruebas de resiliencia operativa digital
A3.2	Clasificación y corrección de problemas	No se realizan pruebas de resiliencia operativa relacionada con los servicios TIC.	Se deben establecer procedimientos para clasificar, priorizar y corregir todos los problemas descubiertos durante las pruebas. También se deben implementar métodos de validación interna para asegurar que todas las debilidades sean abordadas adecuadamente.	DORA, Artículo 25, apartado 5(página 46)	4 - Realizar pruebas de resiliencia operativa digital (pentesting)	L1	No	No implementado	Q/W	-	1	3. Pruebas de resiliencia operativa digital
A3.3	Designación de jefe de equipo de pruebas basadas en	No hay nadie designado como líder de equipo de control.	Designa a un líder que gestione diariamente el TLPT y supervise las decisiones del equipo de control.	RTS29- TLTP, artículo 4, apartado 1(página 35)	4 - Realizar pruebas de resiliencia operativa digital (pentesting)	L1	No	No implementado	Q/W	-	1	3. Pruebas de resiliencia operativa digital
A3.4	Establecimiento de medidas organizativas de TLPT	No se realizan pruebas de Red Team a los sistemas, aunque se realizan pruebas anuales de Blue Team a través de los Informes proporcionados por ASSECO a través de un tercero.	Establecimiento de medidas organizativas y procedimientos que aseguren: a. Acceso restringido a la información: Limita el acceso a información sobre el TLPT solo al equipo de control, la dirección, testers, proveedor de inteligencia de amenazas y la autoridad de TLPT, basado en la necesidad. b. Consulta con gerentes de prueba: Asegúrate de que el equipo de control consulte a los gerentes de prueba antes de incluir a cualquier miembro del equipo de defensa en el TLPT. c. Notificación de detecciones: Establece un protocolo para que el equipo de control sea informado de cualquier detección del TLPT por parte del personal interno o de terceros, y gestiona la respuesta a incidentes según sea necesario. d. Confidencialidad del TLPT: Implementa acuerdos de confidencialidad para todos los involucrados, incluyendo personal	RTS29- TLTP, artículo 4, apartado 2 (página 35-36)	4 - Realizar pruebas de resiliencia operativa digital (pentesting)	L1	No	No implementado	Q/W	Informe técnico ASSECO-Auditoría Técnica	1	3. Pruebas de resiliencia operativa digital

CUADRO DE MANDOS | ANEXO 3. EVALUACIÓN CONTROLES | CRITERIOS DE CUMPLIMIENTO | ANEXO 1. DOCUMENTACIÓN APORTADA

Listo | Accesibilidad: es necesario investigar | Configuración de visualización | 65 %

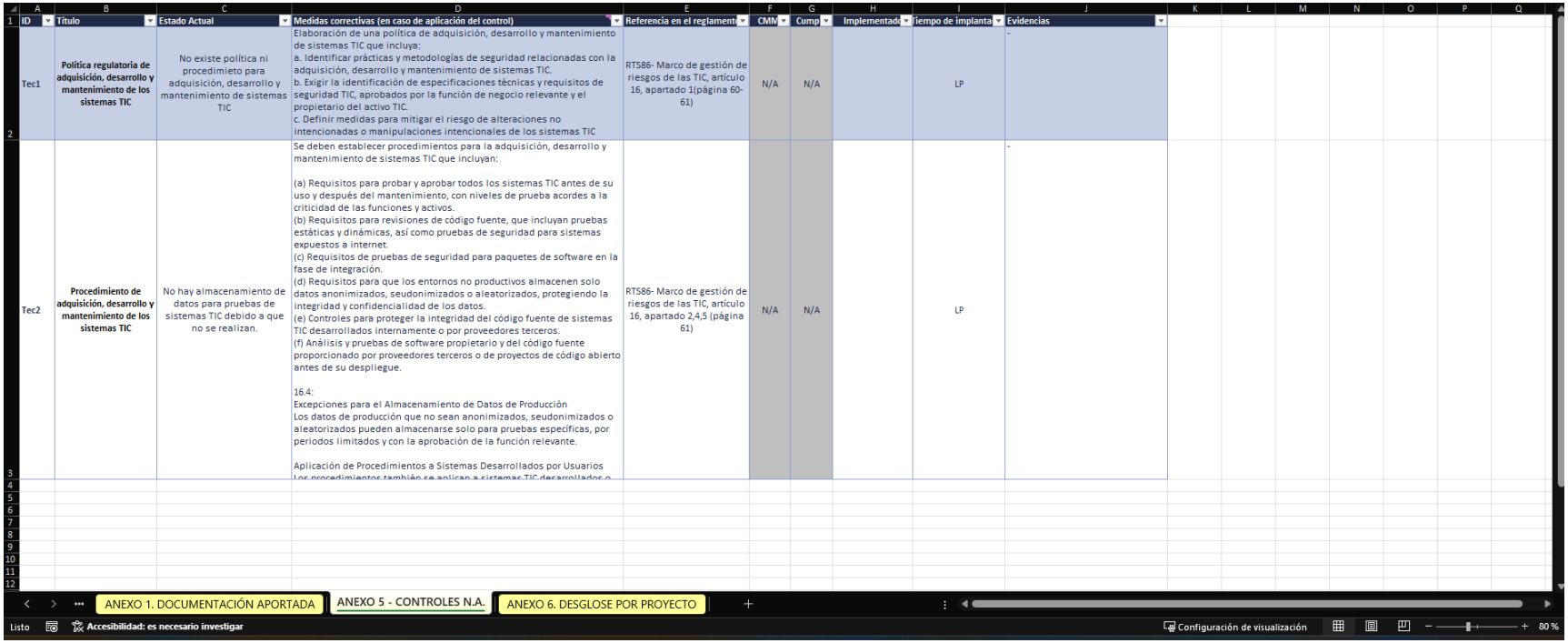
Ilustración 28. Pestaña EVALUACIÓN DE CONTROLES de la herramienta entregada al cliente



Criterios de cumplimiento de DORA		
NIVEL CMMI	Nivel de cumplimiento DORA	Criterios cumplimiento DORA
L0	No cumple	No cumple.
L1	No cumple	No cumple.
L2*	Cumple/No cumple	Dependiendo del requerimiento de DORA podría cumplir si no se exige la obligatoriedad de tener formalizado un proceso documentado, en tal caso, el control cumpliría con un L2, y en caso contrario, no cumpliría.
L3	Cumple	Cumple.
L4	Cumple	Cumple.
L5	Cumple	Cumple.

Modelo de la madurez de la capacidad	
NIVEL CMMI	DESCRIPCIÓN ESTADOS CMMI
L0	Inexistente (0%) •Carencia completa de ningún proceso reconocido. •No se ha reconocido ni siquiera que existe un problema a resolver.
L1	Inicial / Ad hoc (10%) •Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. •Los procedimientos son inexistentes o localizados en áreas concretas. •No existen plantillas definidas a nivel corporativo.
L2	Reproducible, pero intuitivo (50%) •Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. •Se normalizan las buenas prácticas en base a la experiencia y al método. •No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. •Se depende del grado de conocimiento de cada individuo.
L3	Proceso definido (90%) •La organización entera participa en el proceso. •Los procesos están implantados, documentados y comunicados mediante entrenamiento.
L4	Gestionado y medible (95%) •Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. • Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
L5	Optimizado (100%) •Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

Ilustración 29. Pestaña CRITERIOS DE CUMPLIMIENTO de la herramienta entregada al cliente

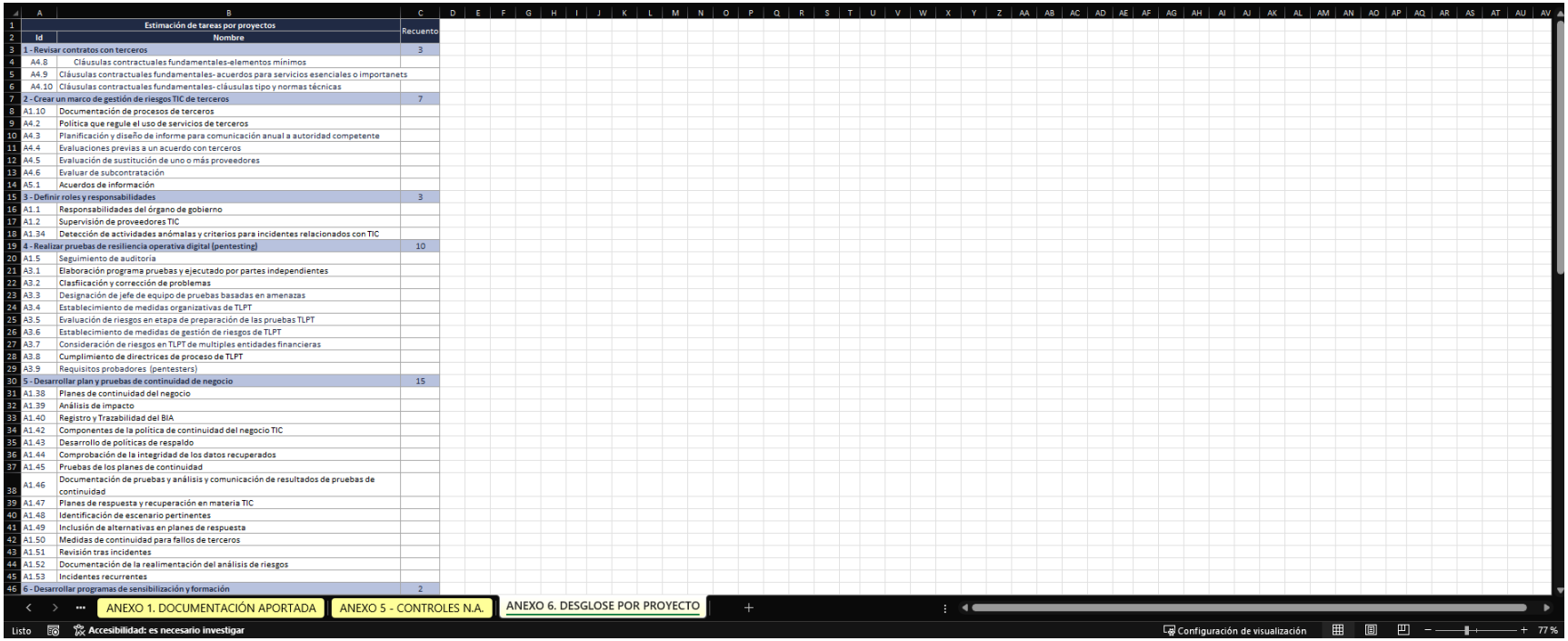


ID	Título	Estado Actual	Medidas correctivas (en caso de aplicación del control)	Referencia en el reglament	CMM	Cump	Implementad	Tiempo de implanta	Evidencias
Tec1	**Política regulatoria de adquisición, desarrollo y mantenimiento de los sistemas TIC**	No existe política ni procedimieto para adquisición, desarrollo y mantenimiento de sistemas TIC	Elaboración de una política de adquisición, desarrollo y mantenimiento de sistemas TIC que incluya: a. Identificar prácticas y metodologías de seguridad relacionadas con la adquisición, desarrollo y mantenimiento de sistemas TIC. b. Exigir la identificación de especificaciones técnicas y requisitos de seguridad TIC, aprobados por la función de negocio relevante y el propietario del activo TIC. c. Definir medidas para mitigar el riesgo de alteraciones no intencionadas o manipulaciones intencionales de los sistemas TIC	RTS86- Marco de gestión de riesgos de las TIC, artículo 16, apartado 1(página 60-61)	N/A	N/A		LP	-
Tec2	**Procedimiento de adquisición, desarrollo y mantenimiento de los sistemas TIC**	No hay almacenamiento de datos para pruebas de sistemas TIC debido a que no se realizan.	Se deben establecer procedimientos para la adquisición, desarrollo y mantenimiento de sistemas TIC que incluyan: (a) Requisitos para probar y aprobar todos los sistemas TIC antes de su uso y después del mantenimiento, con niveles de prueba acordes a la criticidad de las funciones y activos. (b) Requisitos para revisiones de código fuente, que incluyan pruebas estáticas y dinámicas, así como pruebas de seguridad para sistemas expuestos a internet. (c) Requisitos de pruebas de seguridad para paquetes de software en la fase de integración. (d) Requisitos para que los entornos no productivos almacenen solo datos anonimizados, seudonimizados o aleatorizados, protegiendo la integridad y confidencialidad de los datos. (e) Controles para proteger la integridad del código fuente de sistemas TIC desarrollados internamente o por proveedores terceros. (f) Análisis y pruebas de software propietario y del código fuente proporcionado por proveedores terceros o de proyectos de código abierto antes de su despliegue. 16.4: Excepciones para el Almacenamiento de Datos de Producción Los datos de producción que no sean anonimizados, seudonimizados o aleatorizados pueden almacenarse solo para pruebas específicas, por periodos limitados y con la aprobación de la función relevante. Aplicación de Procedimientos a Sistemas Desarrollados por Usuarios	RTS86- Marco de gestión de riesgos de las TIC, artículo 16, apartado 2,4,5 (página 61)	N/A	N/A		LP	-

ANEXO 1. DOCUMENTACIÓN APORTADA | ANEXO 5 - CONTROLES N.A. | ANEXO 6. DESGLOSE POR PROYECTO

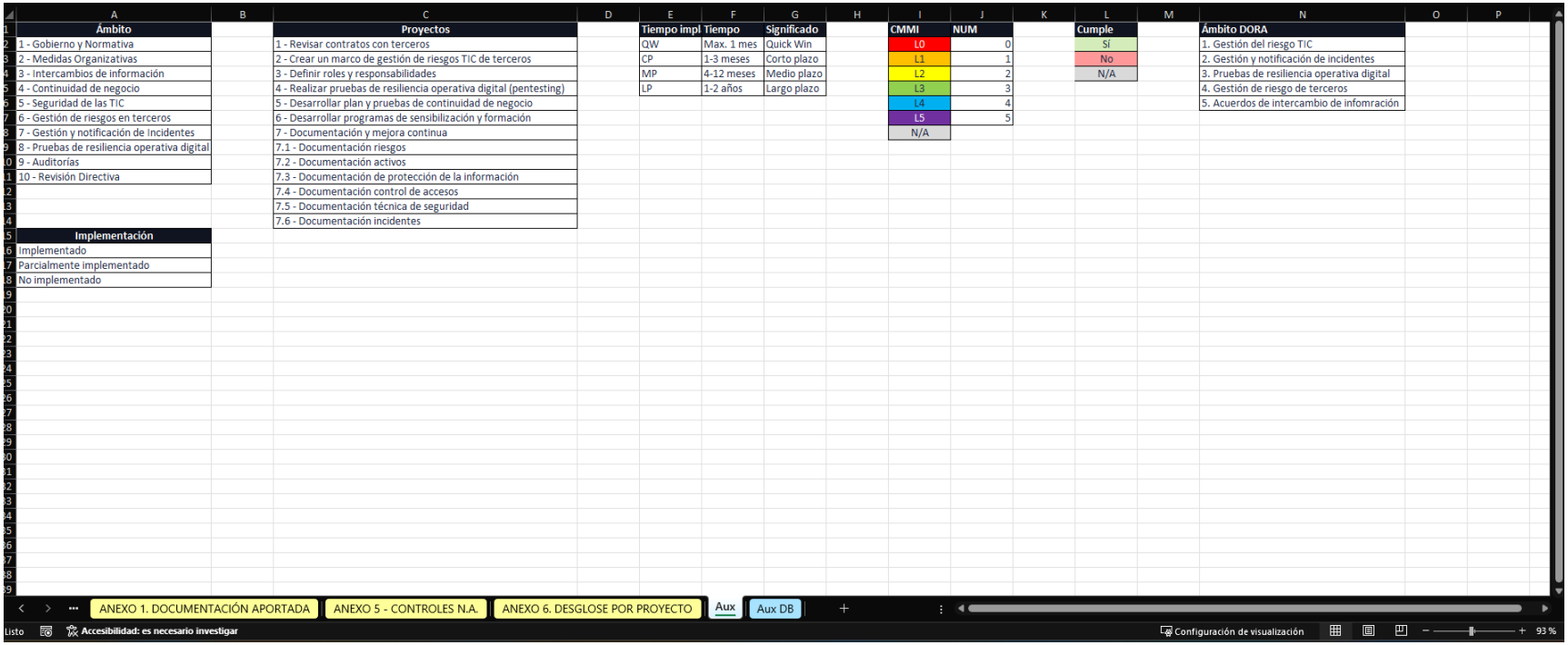
Listo | Accesibilidad: es necesario investigar | Configuración de visualización | 80 %

Ilustración 30. Pestaña CONTROLES N.A. de la herramienta entregada al cliente



	A	B	C
1	Estimación de tareas por proyectos		Recuento
2	Id	Nombre	
3	1 - Revisar contratos con terceros		3
4	A4.8	Cláusulas contractuales fundamentales-elementos mínimos	
5	A4.9	Cláusulas contractuales fundamentales- acuerdos para servicios esenciales o importanets	
6	A4.10	Cláusulas contractuales fundamentales- cláusulas tipo y normas técnicas	
7	2 - Crear un marco de gestión de riesgos TIC de terceros		7
8	A1.10	Documentación de procesos de terceros	
9	A4.2	Política que regule el uso de servicios de terceros	
10	A4.3	Planificación y diseño de informe para comunicación anual a autoridad competente	
11	A4.4	Evaluaciones previas a un acuerdo con terceros	
12	A4.5	Evaluación de sustitución de uno o más proveedores	
13	A4.6	Evaluar de subcontratación	
14	A5.1	Acuerdos de información	
15	3 - Definir roles y responsabilidades		3
16	A1.1	Responsabilidades del órgano de gobierno	
17	A1.2	Supervisión de proveedores TIC	
18	A1.34	Detección de actividades anómalas y criterios para incidentes relacionados con TIC	
19	4 - Realizar pruebas de resiliencia operativa digital (pentesting)		10
20	A1.5	Seguimiento de auditoría	
21	A3.1	Elaboración programa pruebas y ejecutado por partes independientes	
22	A3.2	Clasificación y corrección de problemas	
23	A3.3	Designación de jefe de equipo de pruebas basadas en amenazas	
24	A3.4	Establecimiento de medidas organizativas de TLPT	
25	A3.5	Evaluación de riesgos en etapa de preparación de las pruebas TLPT	
26	A3.6	Establecimiento de medidas de gestión de riesgos de TLPT	
27	A3.7	Consideración de riesgos en TLPT de multiples entidades financieras	
28	A3.8	Cumplimiento de directrices de proceso de TLPT	
29	A3.9	Requisitos probadores (pentesters)	
30	5 - Desarrollar plan y pruebas de continuidad de negocio		15
31	A1.38	Planes de continuidad del negocio	
32	A1.39	Análisis de impacto	
33	A1.40	Registro y Trazabilidad del BIA	
34	A1.42	Componentes de la política de continuidad del negocio TIC	
35	A1.43	Desarrollo de políticas de respaldo	
36	A1.44	Comprobación de la integridad de los datos recuperados	
37	A1.45	Pruebas de los planes de continuidad	
38	A1.46	Documentación de pruebas y análisis y comunicación de resultados de pruebas de continuidad	
39	A1.47	Planes de respuesta y recuperación en materia TIC	
40	A1.48	Identificación de escenario pertinentes	
41	A1.49	Inclusión de alternativas en planes de respuesta	
42	A1.50	Medidas de continuidad para fallos de terceros	
43	A1.51	Revisión tras incidentes	
44	A1.52	Documentación de la realimentación del análisis de riesgos	
45	A1.53	Incidentes recurrentes	
46	6 - Desarrollar programas de sensibilización y formación		2

Ilustración 31. Pestaña DESGLOSE POR PROYECTO de la herramienta entregada al cliente



Ámbito
1 - Gobierno y Normativa
2 - Medidas Organizativas
3 - Intercambios de información
4 - Continuidad de negocio
5 - Seguridad de las TIC
6 - Gestión de riesgos en terceros
7 - Gestión y notificación de incidentes
8 - Pruebas de resiliencia operativa digital
9 - Auditorías
10 - Revisión Directiva

Implementación
Implementado
Parcialmente implementado
No implementado

Proyectos
1 - Revisar contratos con terceros
2 - Crear un marco de gestión de riesgos TIC de terceros
3 - Definir roles y responsabilidades
4 - Realizar pruebas de resiliencia operativa digital (pentesting)
5 - Desarrollar plan y pruebas de continuidad de negocio
6 - Desarrollar programas de sensibilización y formación
7 - Documentación y mejora continua
7.1 - Documentación riesgos
7.2 - Documentación activos
7.3 - Documentación de protección de la información
7.4 - Documentación control de accesos
7.5 - Documentación técnica de seguridad
7.6 - Documentación incidentes

Tiempo impl	Tiempo	Significado
QW	Max. 1 mes	Quick Win
CP	1-3 meses	Corto plazo
MP	4-12 meses	Medio plazo
LP	1-2 años	Largo plazo

CMMI	NUM
L0	0
L1	1
L2	2
L3	3
L4	4
L5	5
N/A	

Cumple
Sí
No
N/A

Ámbito DORA
1. Gestión del riesgo TIC
2. Gestión y notificación de incidentes
3. Pruebas de resiliencia operativa digital
4. Gestión de riesgo de terceros
5. Acuerdos de intercambio de infomración

Ilustración 32. Pestaña Aux de la herramienta entregada al cliente