VI INDICADOR DE MADUREZ EN CIBERSEGURIDAD

Observatorio de la ciberseguridad

Una iniciativa de:

CSC CYBER SECURITY CENTRE

isms forum

www.ismsforum.es

AUTORES

PARTICIPANTES

Blanca Rivas

David Esteban

David Llorente

Iván Sánchez

Luis Pérez

Mariano González

Olga Forné

Óscar Sánchez

Pedro López

Santiago Minguito

Toni García

GESTIÓN DE PROYECTOS

Beatriz García

Elena Fernández

Susana Marín

Sumario

1. ISMS Forum y su iniciativa: el Observatorio de la Ciberseguridad

ISMS Forum es una organización sin ánimo de lucro que nació en enero de 2007 con el objetivo de impulsar el desarrollo, el conocimiento y la cultura de la Seguridad de la Información en España. Con una visión inclusiva y colaborativa, se ha consolidado como el principal foro especializado a nivel nacional donde empresas, organismos públicos y privados, investigadores y profesionales pueden compartir experiencias, colaborar y mantenerse actualizados sobre los avances en materia de ciberseguridad. Los principios que guían su labor incluyen la transparencia, la independencia, la objetividad y la neutralidad.

Originalmente, ISMS Forum comenzó su andadura como el Capítulo Español del **ISMS International User Group (IUG)**, una entidad dedicada a promover el conocimiento y la implementación de Sistemas de Gestión de la Seguridad de la Información en línea con la familia de estándares **ISO 27000**. Actualmente, la organización opera bajo la marca **International Information Security Community**, con una representación centralizada en España.

La Asociación organiza una amplia variedad de iniciativas que abordan la Seguridad de la Información desde perspectivas globales y especializadas. Entre ellas, destacan las Jornadas Internacionales, el **Data Privacy Institute**, la **Cloud Security Alliance**, el **Cyber Security Center**, el **Cyber Resilience Center**, El **Grupo de Inteligencia Artificial** y diversos talleres específicos y programas de formación en ciberseguridad y protección de datos. También gestionan certificaciones como la **Certified Data Privacy Professional (CDPP)**, la **Certificación de Delegado de Protección de Datos (CDPD)** y la **Certified Cyber Security Professional (CCSP)**, **Certified Artificial Intelligence Professional (CAIP)**, además de promover la obtención del **Certificate Of Cloud Security Knowledge (CCSK)**.

En 2020, ISMS Forum consolidó su posición como la mayor comunidad de expertos y organizaciones en el ámbito de la Seguridad de la Información en España, gracias a su promoción de la excelencia y formación continua de sus miembros. Esta comunidad también facilita la comunicación con las autoridades regulatorias y

fomenta el intercambio de conocimientos entre los actores más relevantes del sector, con el objetivo de mejorar la ciberseguridad en España.

Asimismo, la Asociación sigue avanzando en su misión de concienciar sobre los riesgos asociados al uso intensivo de las Tecnologías de la Información y la Comunicación (TIC), aspecto clave para asegurar el desarrollo socioeconómico del país.

Como parte de su compromiso con la innovación y la mejora continua, ISMS Forum ha creado el **Observatorio de la Ciberseguridad** (disponible en https://observatoriociber.ismsforum.es/), una plataforma diseñada para facilitar el análisis de los principales riesgos, desafíos y áreas de preocupación en ciberseguridad.

2. Objetivos del Observatorio de la Ciberseguridad

Los principales objetivos del Observatorio de la Ciberseguridad son:

- Proporcionar una plataforma para el **análisis continuo del nivel de madurez** y evolución de la seguridad de la información, así como para identificar nuevos desafíos y tendencias emergentes en este campo.
- **Desarrollar indicadores a nivel nacional** que reflejen el estado de la ciberseguridad en organizaciones públicas y privadas, permitiendo una visión clara y precisa del panorama actual.
- **Fomentar la investigación** y el avance del conocimiento en materia de ciberseguridad, impulsando iniciativas innovadoras y colaborativas en el sector.
- **Establecer métricas y referencias nacionales** que ayuden a evaluar y mejorar las prácticas de ciberseguridad en las empresas y entidades.
- Facilitar la cooperación y el diálogo con instituciones clave y organismos reguladores, contribuyendo al **desarrollo de políticas y marcos normativos** en el ámbito de la ciberseguridad.

3. Estudio sobre el nivel de madurez en ciberseguridad en la empresa española

La gestión de riesgos sigue siendo un proceso continuo y dinámico, tal como lo establece el Instituto Nacional de Estándares y Tecnología (NIST). Este proceso implica identificar, evaluar y responder a los riesgos, permitiendo a las organizaciones no solo reaccionar a los eventos, sino también anticiparlos de manera proactiva. Para gestionar los riesgos de manera eficaz, las organizaciones deben tener una comprensión profunda tanto de la probabilidad de que ocurra un evento cibernético como de los impactos que podrían derivarse de él. Esta premisa constituye el pilar fundamental sobre el que ISMS Forum presenta la sexta edición de su Observatorio de Ciberseguridad.

Este estudio tiene como objetivo proporcionar una visión actualizada del estado de la ciberseguridad en las empresas nacionales y brindar información valiosa para los profesionales del sector, ofreciendo una visión evolutiva y comparativa respecto a los estudios de años previos.
Un aspecto clave del estudio es la generación de un indicador de madurez anual que permita evaluar de manera continua la evolución interanual de los riesgos cibernéticos y su interrelación con otros factores, como el creciente uso de la inteligencia artificial (IA) y las nuevas normativas de protección de datos.

Marco metodológico actualizado: Diferencias clave entre NIST CSF 1.0 y 2.0 e incorporación de nuevas tecnologías y desafíos
El estudio se basa en el Cybersecurity Framework 2.0 del Instituto Nacional de Estándares y Tecnología (NIST), un estándar internacional de referencia que ha sido actualizado para abordar el cambiante panorama de la ciberseguridad en 2024.

Mientras que el NIST CSF 1.0 se enfocaba en cinco dominios principales (Identificación, Protección, Detección, Respuesta y Recuperación), el NIST CSF 2.0 añade el dominio de Gobierno. Este nuevo dominio reconoce la necesidad de integrar la ciberseguridad en la gobernanza corporativa y estratégica, facilitando una estructura que permite a las organizaciones gestionar de forma más holística sus riesgos cibernéticos. La inclusión de Gobierno permite una supervisión continua de políticas, una clara asignación de roles y la gestión de riesgos en la cadena de

suministro, lo que representa una ventaja estratégica al alinear la ciberseguridad con los objetivos globales de la organización.

El NIST CSF 2.0 también reorganiza y refuerza las categorías de los dominios existentes, ajustándose mejor a las necesidades actuales de mitigación de riesgos y adaptándose a los desafíos asociados a tecnologías emergentes como la inteligencia artificial, la computación en la nube y el Internet de las cosas (IoT).

Estas actualizaciones en la estructura y categorías del framework ofrecen una guía detallada que permite a las organizaciones desarrollar una postura de ciberseguridad más resiliente y adaptativa.

El marco del NIST sigue siendo una guía globalmente adoptada por organizaciones de todos los tamaños y sectores. En esta edición, el Observatorio de Ciberseguridad utiliza el nuevo marco para evaluar la madurez de las organizaciones en cada uno de estos seis dominios, además de proporcionar un índice sintético o global que permite medir su nivel de madurez en ciberseguridad de manera integral.

Nuevos desafíos tecnológicos y su impacto en el riesgo cibernético

El panorama de riesgos cibernéticos se ha vuelto significativamente más complejo debido a la adopción masiva de tecnologías emergentes como la inteligencia artificial, la computación en la nube, y el Internet de las cosas (IoT). Estas tecnologías, aunque ofrecen grandes oportunidades para mejorar la eficiencia operativa y la toma de decisiones, también introducen nuevas amenazas que requieren una gestión de riesgos mucho más dinámica y adaptada.

El Cybersecurity Framework 2.0 del NIST ha sido diseñado para abordar estos nuevos desafíos, con actualizaciones que proporcionan orientación sobre cómo mitigar riesgos asociados con tecnologías emergentes y amenazas cada vez más sofisticadas. Aunque su adopción sigue siendo voluntaria, el marco se ha convertido en un estándar clave para organizaciones que buscan mejorar su postura de seguridad en un entorno tecnológico y regulatorio en constante evolución.

4. Aplicación de los dominios establecidos por el marco de ciberseguridad 2.0 del NIST

A medida que los entornos tecnológicos y las amenazas cibernéticas evolucionan rápidamente, las organizaciones enfrentan la necesidad constante de adaptar sus estrategias de ciberseguridad. En respuesta a este contexto, el Instituto Nacional de Normas y Tecnología (NIST) de los Estados Unidos ha actualizado su Marco de Ciberseguridad (Cybersecurity Framework, CSF) a la versión 2.0. Esta nueva versión, lanzada en Febrero de 2024, representa una evolución significativa desde la versión 1.1 de 2018, adaptándose a los desafíos actuales y anticipando los riesgos futuros en el ámbito digital.

Uno de los cambios más notables en el CSF 2.0 es la incorporación de una sexta función, **Gobierno,** la cual aborda la importancia de una gestión de ciberseguridad con enfoque estratégico y organizacional. Además, se han revisado y reorganizado las categorías en las funciones existentes, para ofrecer a las organizaciones una estructura más detallada y clara que facilite la implementación de prácticas de seguridad efectivas.

Con este marco renovado, las organizaciones pueden **identificar**, **proteger, detectar, responder** y **recuperarse** de amenazas cibernéticas con un enfoque más estructurado, al tiempo que fortalecen su **gobernanza** y sus capacidades de gestión de riesgos en toda la cadena de suministro y en sus operaciones internas.

Ilustración 1: framework NIST CSF 2.0

Gobierno – *(Contexto de la organización, Estrategia de gestión de riesgos, Gestión de riesgos de la cadena de suministro de ciberseguridad, Funciones, responsabilidades y autoridades, Políticas, procesos y procedimientos, Supervisión).*

La nueva función de Gobierno se introduce en la versión 2.0 para enfatizar la importancia de una estructura organizativa sólida en la gestión de ciberseguridad. Incluye categorías para establecer el contexto organizativo y la estrategia de riesgos, y amplía la gestión de riesgos en la cadena de suministro de ciberseguridad. Además, asigna responsabilidades claras y asegura la supervisión constante de las políticas y procesos de seguridad, un paso crítico para garantizar una gobernanza efectiva y continua de las prácticas de ciberseguridad en toda la organización.

Identificar – *(Gestión de activos, Evaluación de riesgos, Mejora).*

La función Identificar se centra en la identificación de activos críticos y la evaluación de riesgos, integrando ahora una categoría de "Mejora" para adaptarse a los cambios continuos en el entorno de amenazas. Este enfoque permite a las organizaciones ajustar sus estrategias de ciberseguridad de manera proactiva, aumentando su capacidad para identificar vulnerabilidades y establecer medidas preventivas.

Proteger – *(Gestión de identidad, autenticación y control de acceso, Concientización y capacitación, Seguridad de los datos, Seguridad de plataformas, Resiliencia de la infraestructura tecnológica).*

En esta función, el enfoque de protección se amplía para incluir una categoría de “Seguridad de plataformas” y “Resiliencia de la infraestructura tecnológica,” subrayando la necesidad de garantizar la seguridad de los entornos de infraestructura y la continuidad de los servicios críticos. Las actividades de protección están diseñadas para controlar el acceso y capacitar al personal, fortaleciendo así la preparación ante amenazas.

Detectar – *(Anomalías y Eventos, Monitoreo continuo de seguridad, Procesos de detección).*

La función Detectar ayuda a identificar eventos de ciberseguridad a través de un monitoreo continuo, permitiendo respuestas rápidas. La estructura en la versión 2.0 no solo refuerza la detección de eventos anómalos, sino que también permite mejorar los procesos de identificación de amenazas en tiempo real, un factor esencial en la defensa preventiva.

Responder – (*Gestión de incidentes, Comunicaciones, Análisis, Mitigación).*

Esta función se ha reforzado en la versión 2.0 con un enfoque detallado en la "Gestión de incidentes" y estrategias de comunicación. La capacidad de respuesta incluye análisis de incidentes, mitigación rápida y comunicaciones efectivas para coordinar la respuesta a nivel interno y externo, ayudando a contener el impacto de los incidentes.

Recuperar – *(Planificación de la recuperación, Mejoras, Comunicaciones).*

La función Recuperar busca mantener la resiliencia y restaurar las operaciones. La planificación de la recuperación, junto con mejoras y comunicaciones estructuradas, garantiza que las organizaciones puedan volver a sus actividades normales tras un incidente, permitiendo una recuperación eficiente y evaluando constantemente el proceso para futuros ajustes.

5. Tipología de muestra

La Ilustración 2 muestra la distribución del volumen de facturación anual (o presupuesto total en el caso de Administraciones Públicas) de las empresas participantes. Se observa que la gran mayoría de las empresas participantes en esta edición son organizaciones con elevada facturación, estando por encima de los 100 millones de euros un 34,61% de ellas o por encima de los 1.000 millones de euros un 42,31% de las mismas.

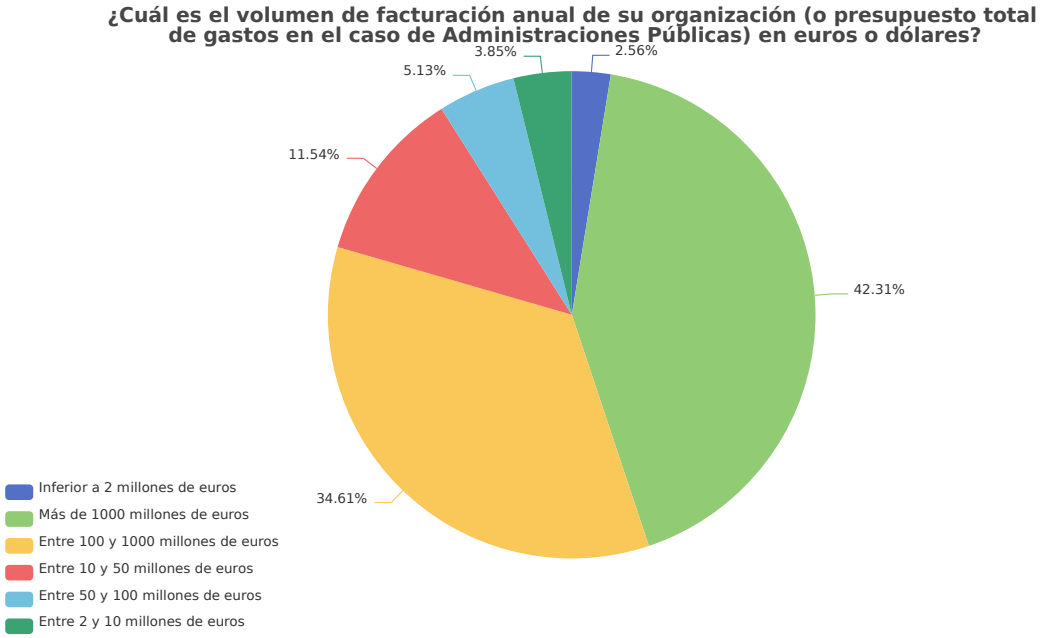


Ilustración 2: Volumen de facturación anual de las empresas participantes

Esta distribución supone una ligera disminución de la participación de empresas de mayor tamaño (>1.000 millones) respecto los estudios de años anteriores, pero del mismo modo aumenta ligeramente la de empresas con facturación entre 100 y 1.000 millones de euros. Por tanto, podemos decir que los datos indican una muestra predominantemente compuesta por empresas grandes o muy grandes.

Los restantes segmentos representan valores menores: 5,13% con facturación entre 50 y 100 millones de euros, 11,54% entre 10 y 50 millones, 3,85% entre 2 y 10 millones, y finalmente, solo el 2,56% de las organizaciones tiene un volumen inferior a 2 millones de euros.

De nuevo, los datos nos dicen que la muestra está principalmente compuesta por grandes corporaciones o entidades con presupuestos significativos.

Ilustración 3: Puesto de trabajo ocupado por el encuestado.

En la Ilustración anterior podemos ver el cargo o puesto que ocupan los encuestados dentro de sus organizaciones. La mayoría de los encuestados (73,08%) son directivos o responsables últimos de la seguridad de la información dentro de sus organizaciones, lo que indica que los datos obtenidos provienen de personal con alta responsabilidad en la gestión de la seguridad informática.

Este dato supone un descenso del 13,22% respecto el dato del estudio anterior, que se situaba en el 86,3% pero, del mismo modo, ha aumentado de manera importante el porcentaje de participantes con un cargo de Dirección/Responsable de TI, aumentando un 7,52% (pasando del 2,74% del estudio previo al 10,26% actual)-

El resto de los participantes se distribuye entre especialistas en seguridad de la información (6,41%), otros puestos de dirección (6,41%), especialistas de TI (1,28%) o Consultores de Seguridad de la Información (2,56%), en línea con estudios anteriores.

Por lo tanto, del análisis de los datos, podemos decir que en el presente estudio se ha contado con una mayor participación de Directores y Responsables de TI, así como una mayor variedad de perfiles profesionales, lo cual añade mayor interés al presente estudio.

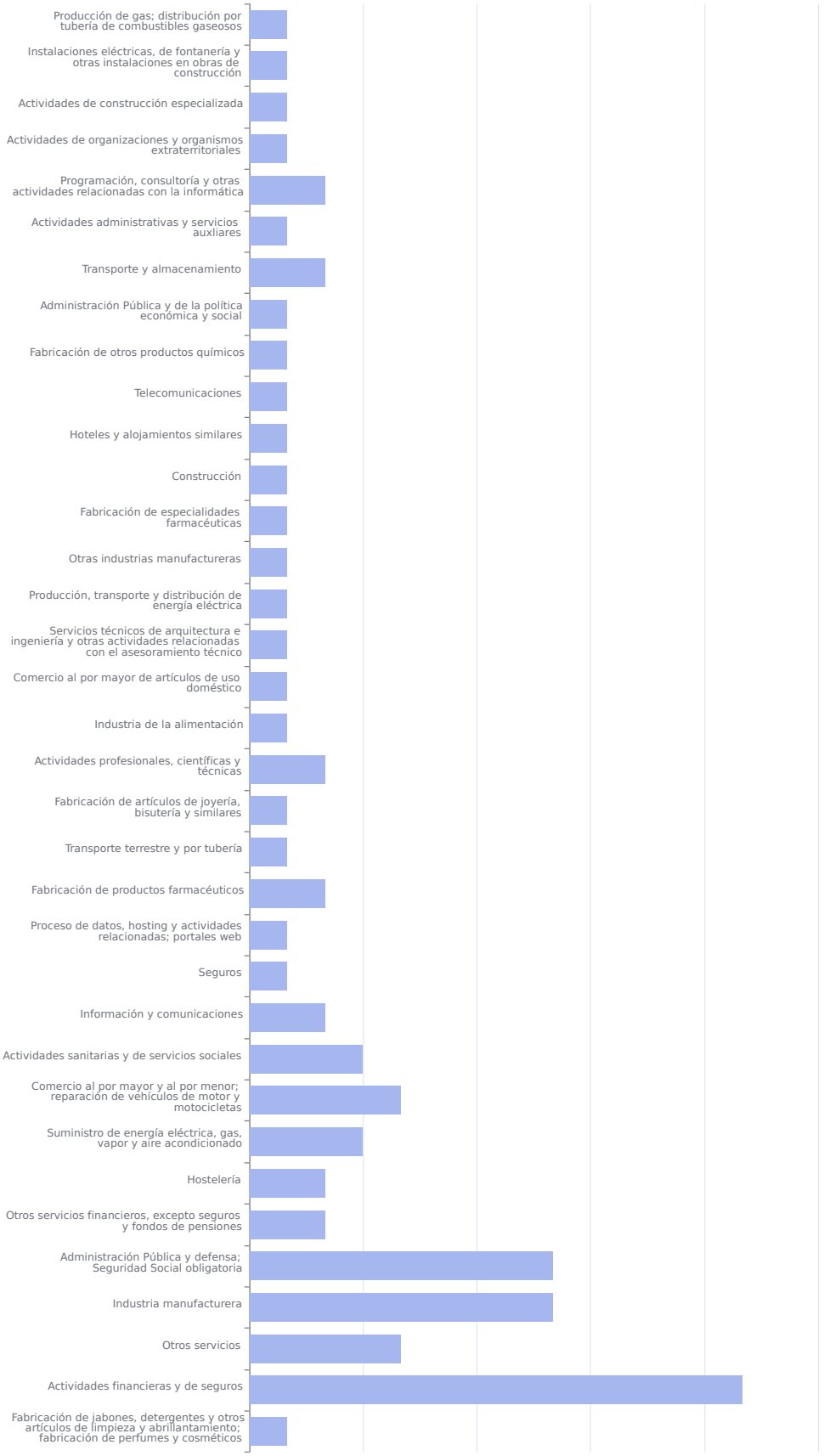


Ilustración 4: Sector de actividad de las empresas participantes.

En la ilustración anterior podemos encontrar los sectores de actividad de las empresas participantes en el estudio. En la presente edición hemos contado con la participación de 77 organizaciones, que se reparten a lo largo de 35 sectores de actividad. Esto también supone un cambio puesto que, en el estudio anterior, las organizaciones participantes se repartían a lo largo de 28 sectores de actividad, por lo que el presente estudio está ligeramente más atomizado (más sectores representados con pocas respuestas) pero del mismo modo añade un enorme valor al estudio al poder contar con una visión más amplia de sectores de actividad.

En línea con estudios anteriores, los sectores más representados incluyen actividades financieras y de seguros y administración pública y defensa, los cuales concentran una parte significativa de la muestra. Sin embargo, este año aumenta significativamente el número de respuestas en el sector de la Industria Manufacturera, pasando de 2 a las 8 respuestas de la presente edición.

Por lo tanto, el estudio cuenta con un amplio rango de sectores e industrias representadas, aunque con un peso considerable de sectores financieros, de administración pública e industria manufacturera, lo cual puede influir en las necesidades y desafíos específicos en términos de seguridad de la información.

En resumen, de los datos que hemos recopilado en la presente edición, podemos concluir que la tipología de la muestra se caracteriza por una predominancia de empresas grandes con alto volumen de facturación y con un enfoque en sectores financieros, administración pública e industria manufacturera. Los encuestados, en su mayoría, son responsables de seguridad de la información con una importante presencia de responsables de TI, lo que aporta una perspectiva especializada en el análisis.

Esta combinación de factores sugiere que los resultados del estudio reflejan las percepciones y experiencias de organizaciones grandes y complejas, con un alto nivel de madurez en temas de seguridad de la información.

6. Nivel de madurez

Desde la actualización del **NIST Cybersecurity Framework (CSF) 2.0** en 2024, se incorporó el dominio de **Gobierno**, reforzando la integración de la ciberseguridad en la gobernanza corporativa de forma estratégica y holística. Con 2025 como segundo año bajo esta estructura, se consolida un enfoque más completo sin perder trazabilidad respecto a años anteriores, ya que CSF 2.0 mantiene la comparabilidad con CSF 1.0 reorganizando las preguntas sin alterar su esencia. Esto permite contrastar los datos actuales con resultados históricos y proyectar tendencias, ofreciendo una visión evolutiva de la madurez en ciberseguridad.

Los resultados de 2025 confirman la recuperación iniciada en 2024 tras las caídas de 2023, con niveles maduros y optimizados que se consolidan en los dominios de Identificar, Detectar, Responder, Recuperar y Gobierno. Sin embargo, lo más relevante es la proyección para 2026, que anticipa un salto cualitativo:

- Optimizado alcanzaría el 36%, el valor más alto de la serie histórica.
- Maduros se mantendrían en torno al 45%, consolidando la estabilidad en capacidades críticas.
- Los niveles básicos e inexistentes se reducirían prácticamente a cero, reflejando una madurez global sin precedentes.

Este escenario proyectado posiciona 2026 como un año clave para la transformación, donde la ciberseguridad deja de ser reactiva para convertirse en un componente estratégico plenamente integrado en la gobernanza corporativa.

La proyección para 2026 no es una estimación teórica, sino que se ha elaborado a partir de las respuestas de los propios encuestados, a quienes se solicitó de forma explícita que valoraran la previsión de evolución de la madurez de sus organizaciones para el próximo ejercicio. Este enfoque permite incorporar la expectativa de los responsables de ciberseguridad como indicador cualitativo complementario al dato cuantitativo, aportando una visión más realista sobre la evolución esperada del sector.

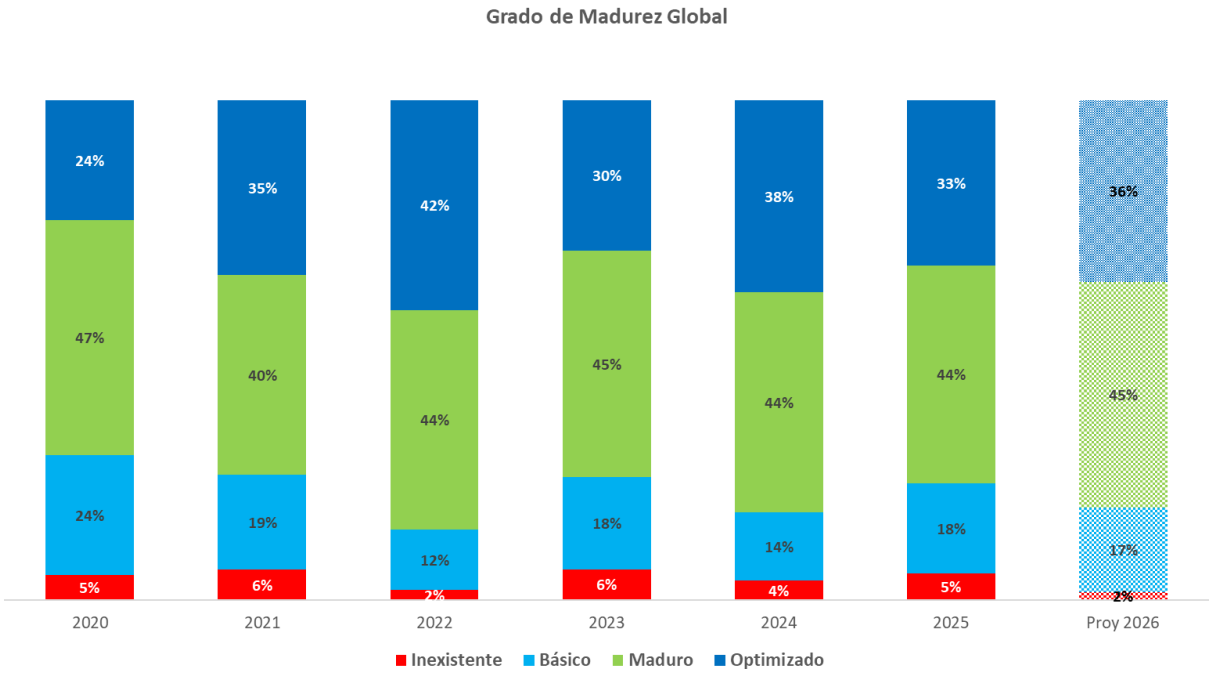


Ilustración 5: Evolución y Proyección del Grado de Madurez Global en Ciberseguridad (2020-2026)

6.1. Dominio 1: Identificar

El dominio Identificar mantiene su papel central en la gestión del riesgo cibernético consolidando la madurez alcanzada por las organizaciones españolas en los últimos años. En 2025, los resultados reflejan una evolución equilibrada entre la gestión de activos, los procedimientos de respuesta y la identificación de vulnerabilidades, con una mejora visible en la capacidad de análisis y documentación frente al contexto de amenazas emergentes.

Inventario y gestión de activos

La capacidad de las organizaciones para identificar y mantener actualizado su inventario de dispositivos, sistemas, aplicaciones y recursos de información continúa fortalecida. En 2025, **el 47 % de las entidades se sitúa en un nivel maduro y el 23 % en optimizado, mientras que solo un 5 % permanece en nivel inexistente.**

Esta progresión confirma la consolidación de mecanismos de descubrimiento automático, gestión de configuraciones (CMDB) y asignación clara de roles y responsabilidades. Las mejoras observadas evidencian una integración más sistemática entre seguridad y gobierno de TI, lo que permite priorizar controles y recursos de manera más eficiente.

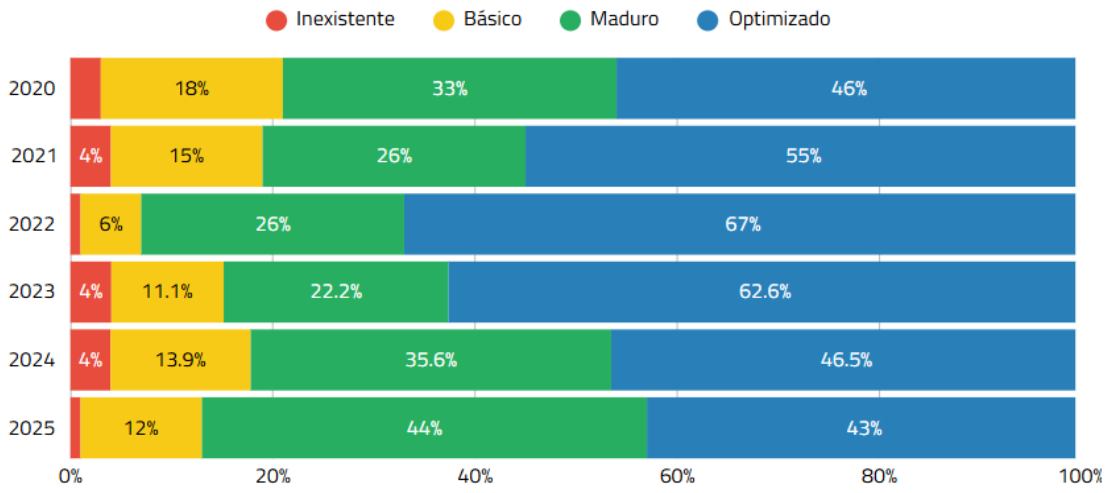
Procedimientos de respuesta ante incidentes.

La documentación, actualización y prueba regular de los procedimientos de respuesta mantienen una tendencia positiva. En 2025, el 53 % de las organizaciones alcanza el nivel maduro y el 22 % el optimizado, con un ligero aumento de los niveles inferiores. Este resultado indica un mantenimiento ante la preparación previa al incidente, gracias a la definición de flujos de comunicación, matrices de responsabilidad (RACI) y simulacros periódicos.

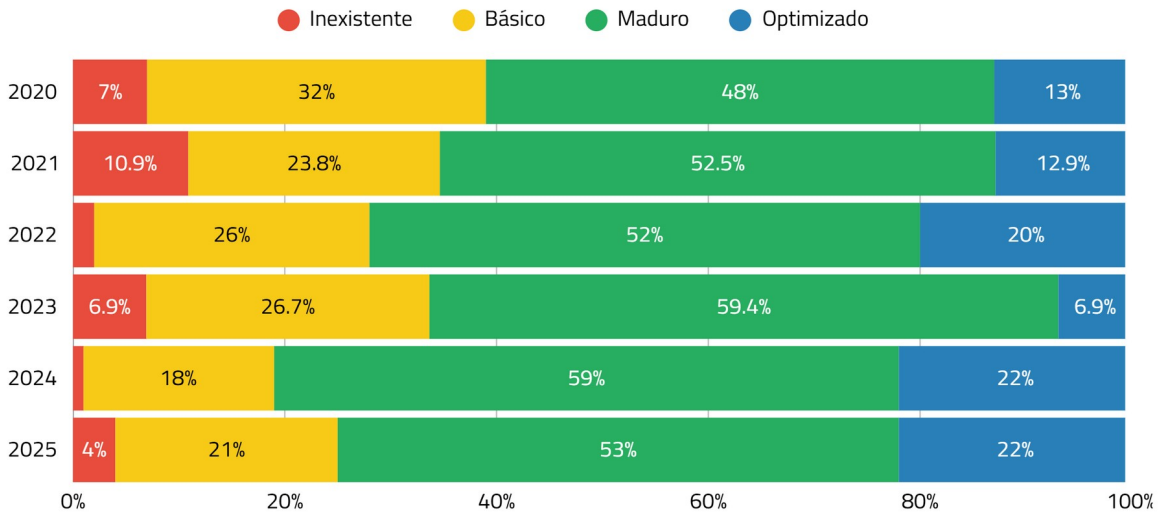
Identificación y documentación de vulnerabilidades y amenazas

La gestión de vulnerabilidades sigue siendo el componente más dinámico del dominio. En 2025, **el 44 % de las organizaciones alcanza el nivel maduro y el 43 % el optimizado** (ligera disminución), lo que supone un incremento sostenido frente a 2024. Este avance se asocia al uso creciente de plataformas de threat intelligence, la integración de escáneres automáticos y análisis de exposición externa y la mejora en la coordinación entre ciberseguridad, infraestructuras y proveedores. Aun así, el 13 % de entidades en niveles iniciales evidencia la necesidad de reforzar las capacidades analíticas y de priorización de riesgos en algunos sectores.

¿Las vulnerabilidades y amenazas de ciberseguridad están identificadas, documentadas y se analiza el riesgo en base a la probabilidad e impacto en el negocio?



¿Los procedimientos de respuesta ante incidentes de ciberseguridad están documentados, actualizados y se prueban regularmente?



¿Existe un inventario de dispositivos, sistemas, aplicaciones y recursos de información, junto con la gestión de roles y responsabilidades de ciberseguridad asociada?

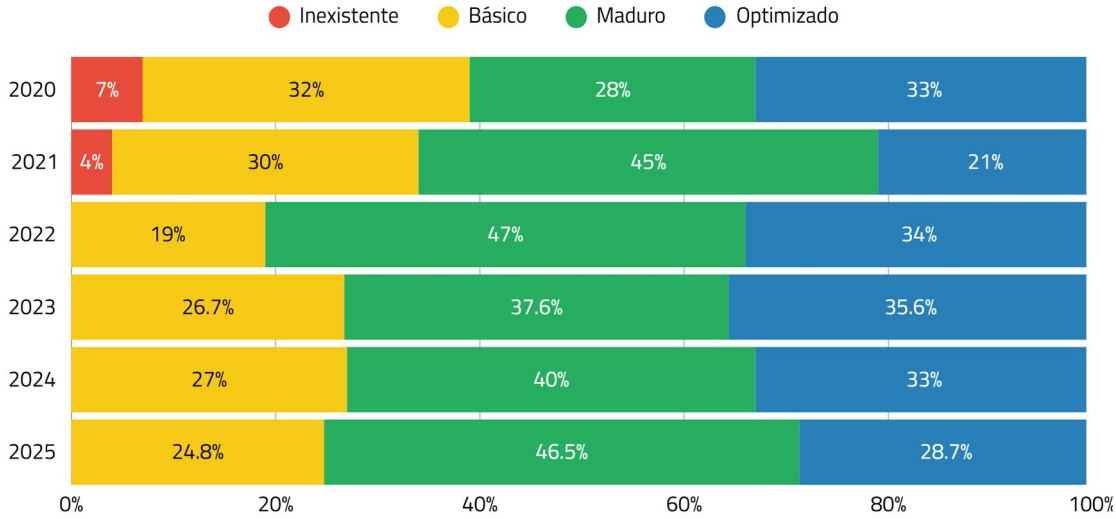


Ilustración 6: Evolución de la tendencia del domino Identificar

Media del dominio y dispersión sectorial

La media general del dominio se mantiene con una dispersión notable entre sectores. Los ámbitos de información y comunicaciones, servicios financieros y actividades profesionales y técnicas continúan liderando el indicador, mientras que sanidad, transporte y almacenamiento, y determinadas ramas de la Administración Pública muestran mayor variabilidad y margen de mejora. Las diferencias se explican por la desigual inversión en gestión de activos y por la madurez heterogénea en los procesos de evaluación de riesgos.

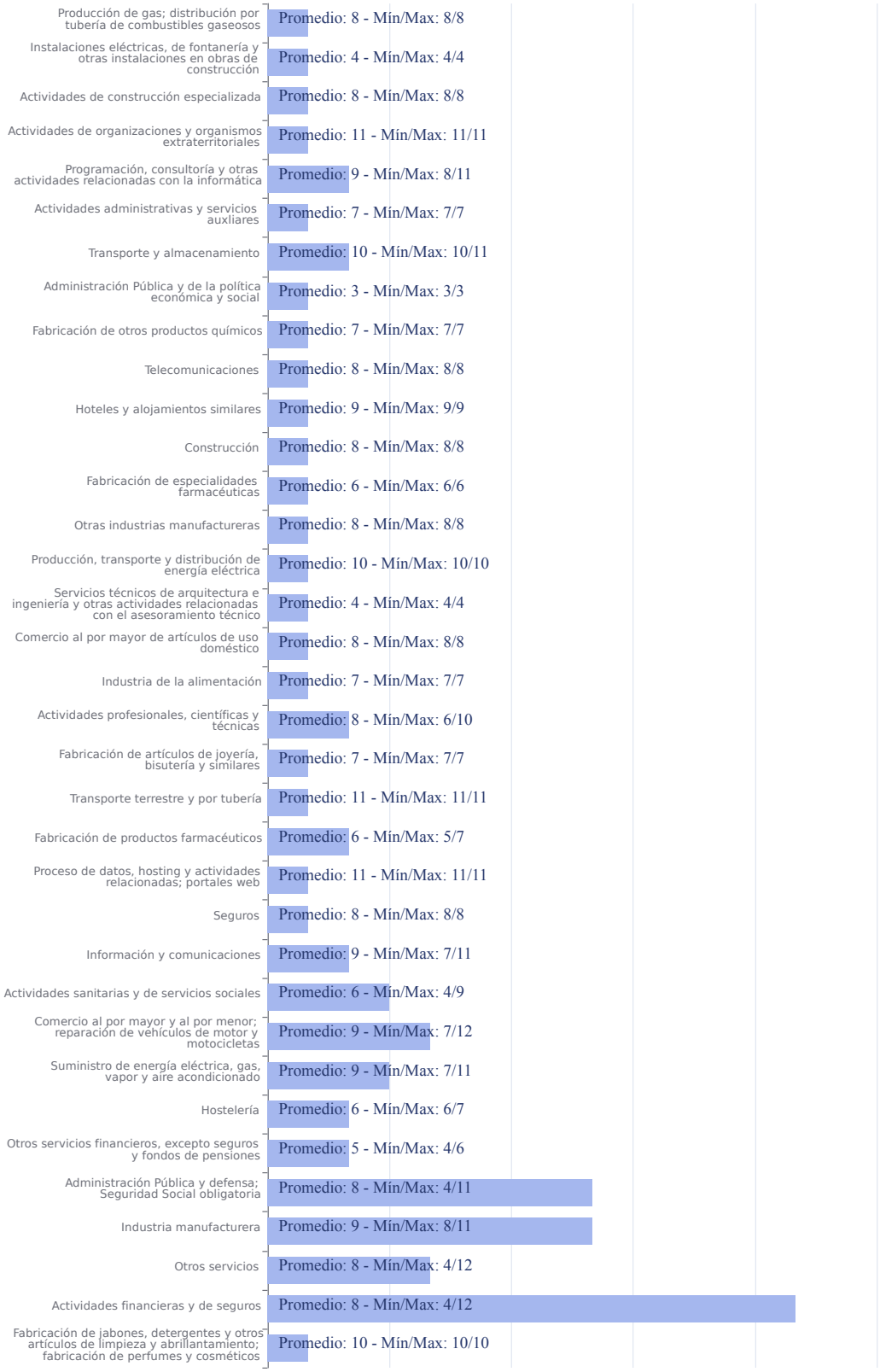


Ilustración 7: Indicador "Identificar" por sector de actividad

Conclusión y perspectivas del dominio

El dominio Identificar reafirma su papel como cimiento de la resiliencia organizativa. Las organizaciones con procesos maduros en inventario y gestión de vulnerabilidades muestran mayor capacidad de anticipación ante incidentes y una visión de riesgo más alineada con la estrategia corporativa.

6.2. Dominio 2: Proteger

Si se analiza la serie temporal al completo (2020-2025), se puede observar una evolución general positiva en la madurez de las empresas españolas en relación con la función 'Proteger'. En términos generales, los niveles 'Inexistente' han disminuido progresivamente, lo que indica una mayor adopción de prácticas de ciberseguridad. Sin embargo, a partir de 2023 se detecta una tendencia de estancamiento o incluso retroceso en los niveles más altos de madurez (Optimizado), acompañada de un ascenso poco significativo en los niveles 'Básico' e 'Inexistente'. Esta situación sugiere que, si bien muchas organizaciones han avanzado en la implementación de controles, existe una dificultad para consolidar prácticas avanzadas y sostenibles en el tiempo, debido, entre otros motivos, a la evolución constante del entorno tecnológico y al incremento potencial de amenazas, lo que ha podido influir en que las organizaciones sean cada vez más exigentes a la hora de evaluar sus capacidades de protección.

Poniendo el foco en los resultados del año 2025, podemos observar una situación mixta, puesto que, aunque se mantiene una mejora respecto a los niveles más bajos de implantación de controles, se evidencia una disminución en el porcentaje de empresas en niveles 'Optimizado' en cuatro de los procesos clave, lo que podría reflejar una pérdida de impulso en la mejora continua. Es destacable que solo se observa mejora en las capacidades de mantenimiento de los sistemas y se mantienen los porcentajes relacionados con la implantación de medidas técnicas de seguridad. En conjunto, 2025 muestra una consolidación en niveles 'Maduros', pero con señales de alerta respecto a la sostenibilidad de los avances logrados en años anteriores.

En cuanto a la gestión de identidades y accesos siguiendo el principio de menor privilegio y la segregación de funciones, si observamos el último año, vemos como se incrementan 15 puntos porcentuales las respuestas del nivel 'Básico' y disminuye 13 puntos porcentuales en el nivel 'Optimizado'. Esta caída en el nivel optimizado es la segunda más importante en los controles analizados y sugiere una pérdida de madurez muy relevante en algunas organizaciones. Analizando la serie temporal al completo, observamos una mejora sostenida en la reducción del nivel 'Inexistente' (del 6% en 2020 al 1% en 2025). Sin embargo, el nivel 'Optimizado' alcanzó su punto máximo en 2022 (54%) y ha descendido al 40% en 2025, mientras que 'Básico' aumentó al 27%.

La formación y concienciación de empleados en ciberseguridad también ha mostrado una disminución del nivel de madurez en el último año. En 2025, **el 38% de las organizaciones se encuentran en un nivel optimizado, y el 35% en un nivel maduro**, en comparación con el 48% y 42% respectivamente en 2024.

Es de destacar que los resultados del último año sitúan los porcentajes de niveles optimizado y maduro en una situación similar a la de 2021. Esto sugiere una posible pérdida de foco en programas de formación o una rotación de personal que afecta la continuidad de la concienciación.

En la gestión del ciclo de vida del dato, se puede observar la caída más relevante en el nivel optimizado en 2024 (de 42% en 2024 a 22% en 2025), situándose incluso en el nivel más bajo de la serie histórica. Por dar más contexto sobre esta caída, es importante indicar que los datos de toda la serie histórica han sido muy variables de año en año. El nivel 'Optimizado' alcanzó su punto más alto en 2022 (48%) pero cayó al 22% en 2025, mientras que 'Maduro' subió al 58%. Aunque esto indica que las empresas mantienen buenas prácticas, hay una clara pérdida de excelencia en la gestión avanzada de datos, posiblemente debido a la falta de inversión o a la complejidad regulatoria. Por otro lado, al igual que en los reportes anteriores, se puede indicar que la variabilidad en los niveles de madurez sigue reflejando fluctuaciones en la capacidad de algunas organizaciones para mantener prácticas consistentes de protección de datos.

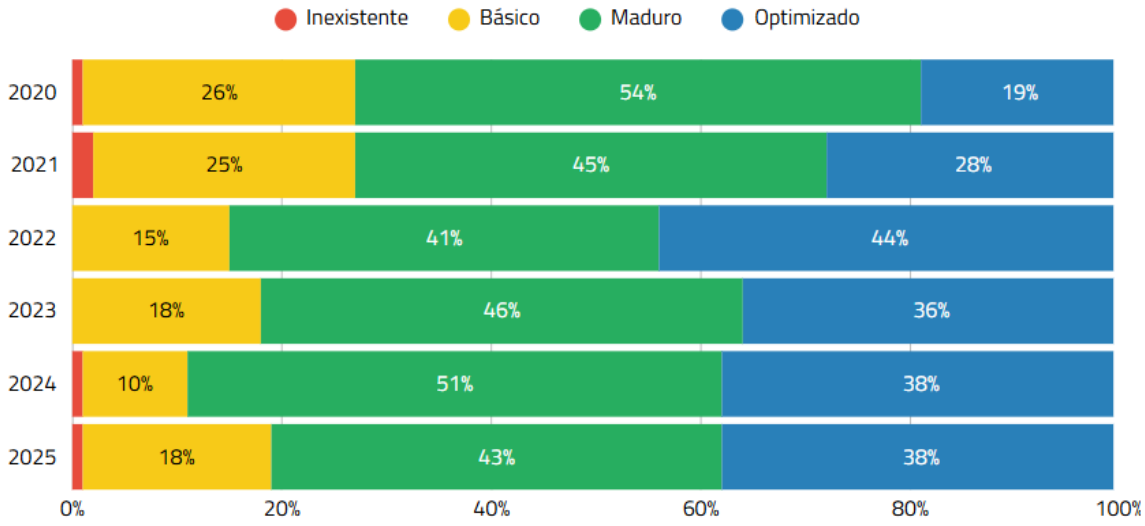
La protección de sistemas y activos de información también ha visto reducido su nivel de madurez en 2025 (11 puntos porcentuales). Si se analiza la serie histórica al completo, en 2025, **el 30% de las organizaciones están en un nivel**

optimizado, comparado con solo el 23% en 2020. Es de destacar que la pérdida de los 11 puntos del nivel optimizado ha sido asumida en gran medida por el nivel maduro (7%) situándose el 4% restante en el nivel inexistente, que desde 2022 había permanecido en el 0%. La situación refleja una estabilización en niveles medios de madurez, pero advierte de desafíos para alcanzar la excelencia operativa.

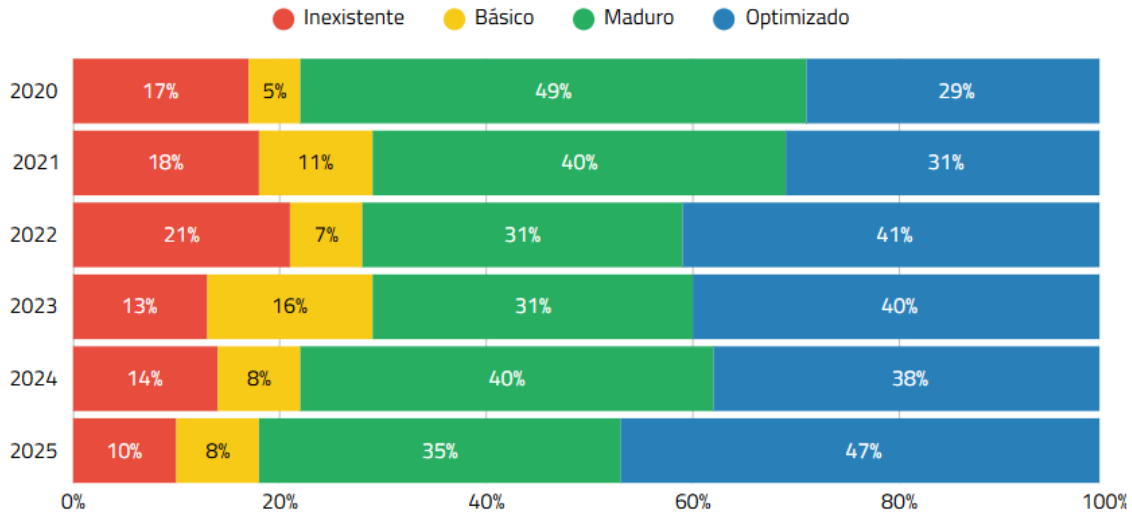
El mantenimiento de sistemas de información y control industrial ha sido una de las pocas áreas donde se observa una mejora clara en 2025, con un **47% en 'Optimizado', el valor más alto de la serie**. Sin embargo, el nivel 'Inexistente' sigue siendo elevado (10%), lo que indica que aún hay organizaciones con carencias importantes en este ámbito. El alto porcentaje de organizaciones con un nivel inexistente podría indicar un área de riesgo que requiere atención inmediata.

La implementación de medidas técnicas de seguridad se mantiene estable en 2025, consolidando su tendencia positiva en la serie histórica. Al igual que en 2024, en 2025, el **38% de las organizaciones alcanzan el nivel optimizado,** aunque el porcentaje de empresas con nivel maduro se ha reducido en un 8% en el último año, trasladándose a un nivel básico. En cualquier caso, la suma de los niveles de madurez más altos (Optimizado y Maduro), se ha incrementado un 8% en la serie histórica, pasando de un 73% en 2020 a un 81%, lo que indica un crecimiento histórico sostenido.

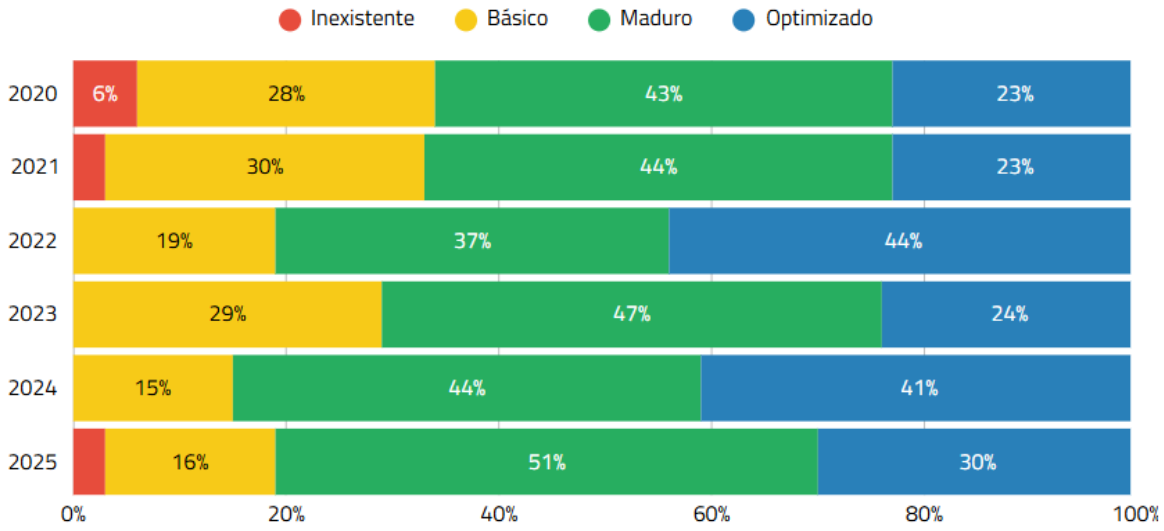
¿Se dispone de medidas técnicas de seguridad asociadas a la política y procedimientos de seguridad que proporcionen seguridad y resiliencia a los sistemas y activos de información?



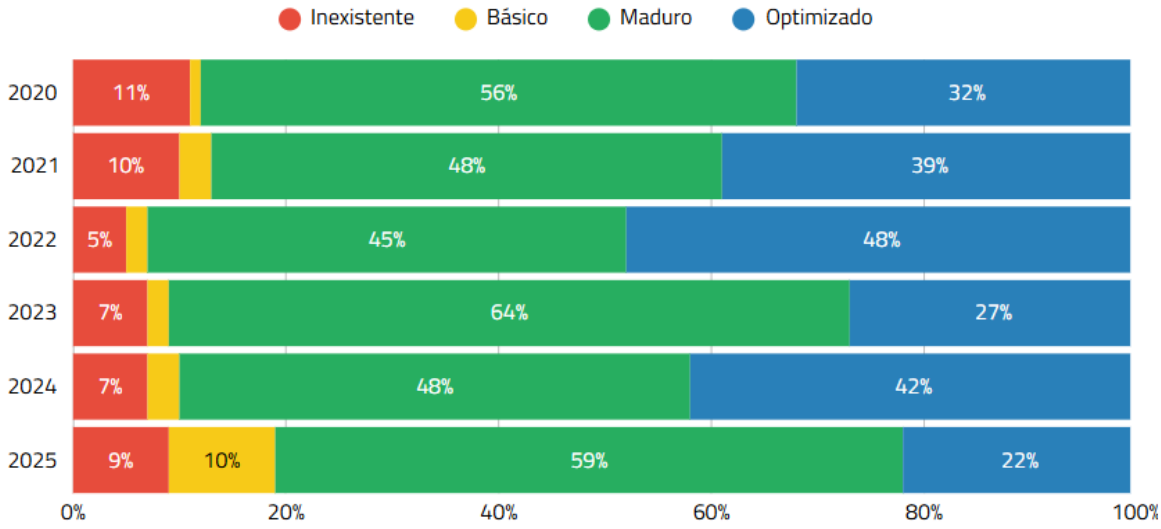
¿Se realiza un mantenimiento de los sistemas de información y control industrial, de forma controlada?



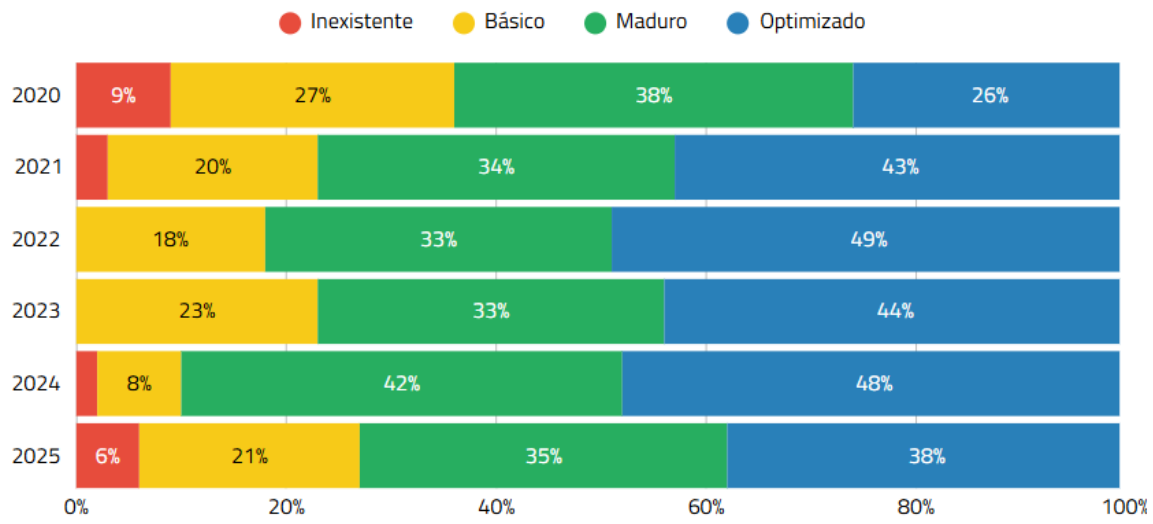
¿Se realiza una protección de los sistemas en base a la gestión, implementación y mantenimiento de los procesos y procedimientos asociados a la política de seguridad?



¿Se realiza una gestión del ciclo de vida del dato para proteger la confidencialidad, integridad y disponibilidad de la información?



¿Todos los empleados y colaboradores están formados, concienciados y entienden sus roles y responsabilidades en materia de ciberseguridad?



¿Se realiza una gestión de identidades y accesos a los activos, siguiendo el principio de menor privilegio y segregación de funciones?

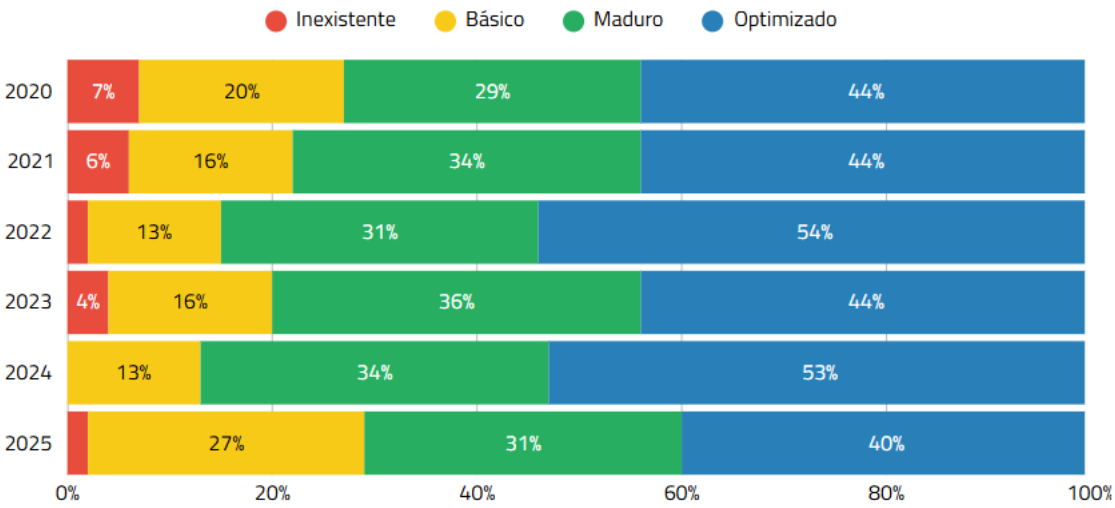
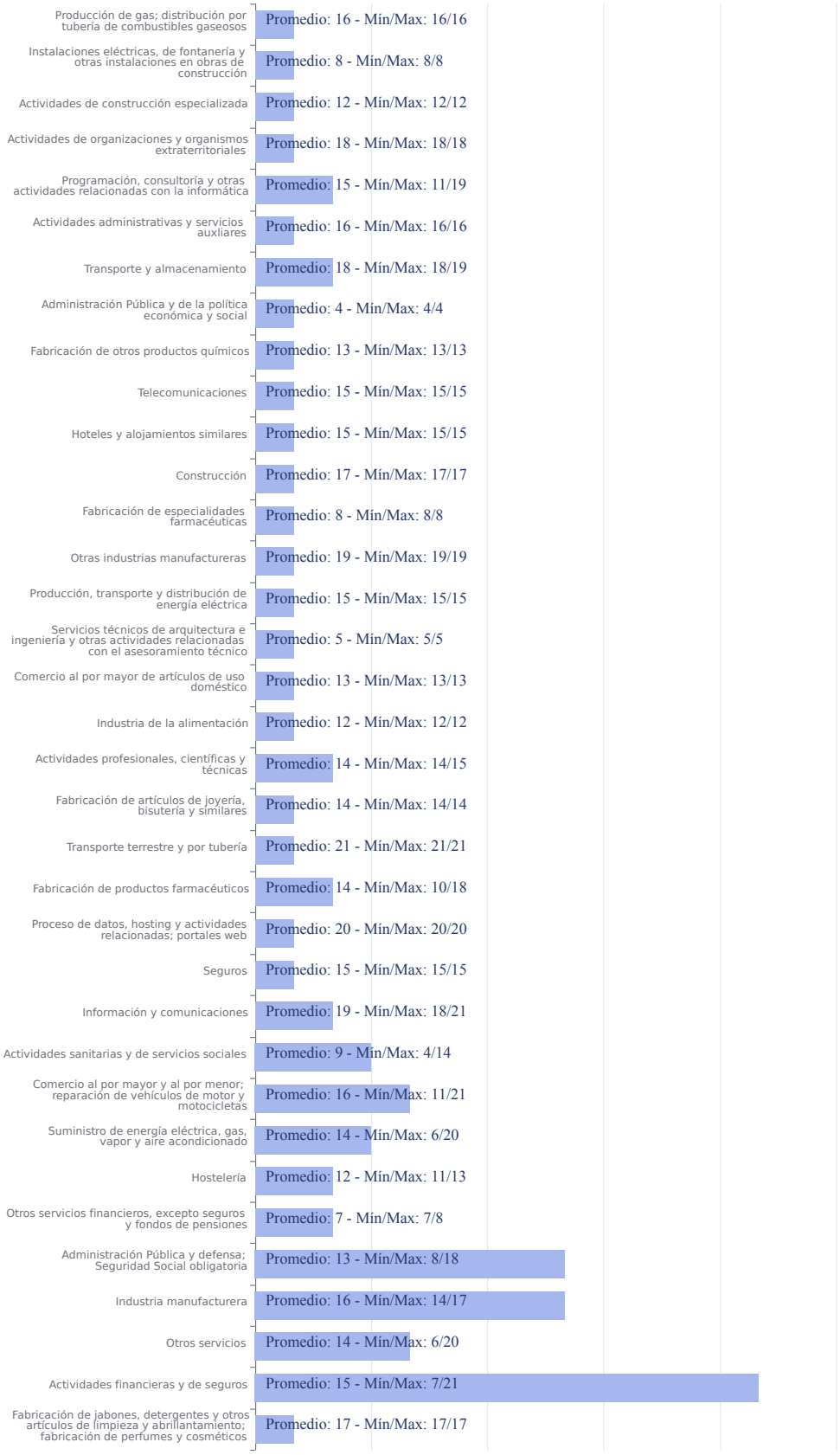


Ilustración 8: Evolución de la tendencia del domino Proteger

La media de las respuestas del dominio proteger es entorno al 17, lo que, además de suponer un avance con respecto al 2024 (con un promedio de 14), es un resultado que demuestra una madurez media/alta en la implantación de medidas técnicas de seguridad, mantenimiento de sistemas, protección de activos de información, gestión del ciclo de vida del dato, formación de empleados, y gestión de identidades.

Los sectores que presentan mayor fortaleza en el dominio proteger son transporte terrestre y por tubería; y proceso de datos, hosting y actividades relacionadas; portales web, aunque el tamaño de la muestra es bajo para ambos grupos.
Inconsistencia en sectores: el indicador muestra grandes inconsistencias en los sectores de “actividades financieras y de seguros” (al igual que en 2024); “actividades sanitarias y de servicios sociales”, “programación, consultoría y otras actividades relacionadas con la informática”, “Administración Pública y defensa” (al igual que en 2024), “fabricación de productos farmacéuticos”, “suministro de energía eléctrica, gas, vapor y aire acondicionado” y “comercio al por mayor y al por menor; reparación de vehículos de motor y motocicleta”. Áreas de Mejora: el sector con mayor margen de mejora es el de Administración Pública y de la política económica y social (con sólo 4 puntos), seguido por el Servicios técnicos de arquitectura e ingeniería y otras actividades relacionadas con el asesoramiento técnico (con 5 puntos).



lustración 9: Indicador "Proteger" por sector de actividad

6.3. Dominio 3: Detectar

En 2025, el dominio Detectar muestra una evolución hacia positivo de las empresas que ya habían iniciado en esta disciplina, y, en cambio, un empeoramiento en aquellas que declaran estar en un nivel por debajo de básico, es decir, inexistente.

En general, se observa una ligera tendencia a la polarización en ambos extremos, los que ya estaban en un nivel considerable siguen mejorando, mientras que los que estaban en niveles más bajos tienden a empeorar ligeramente. La banda media se muestra elástica, con mejoras y empeoramientos casi en paralelo en las diferentes casuísticas analizadas.

Se aprecia una evolución de la adopción a dos velocidades y el inicio de una brecha entre los que ya habían empezado y van acelerando hacia mejor, y el preocupante incremento de los que todavía no han empezado a implantar detección o que habían empezado pero van frenando y pierden fuerza mostrando peores registros.

Vamos a verlo pormenorizado por las variables específicas de la encuesta que se resumen en: sistemas de recolección de eventos, análisis para la detección de actividad anómala, monitorización de actividad de usuarios (incluídos proveedores) para la identificación de eventos de ciberseguridad, y por último la existencia, actualización y testeo de los procedimientos que forman parte de los procesos de detección de incidentes.

La existencia de sistemas para la recolección de eventos como elemento tecnológico básico ha mostrado retroceso en las organizaciones menos maduras, esto puede ser debido a la proliferación de amenazas avanzadas que, si no va acompañada de sistemas de detección capaces de evidenciar esas amenazas más sofisticadas, la sensación resultante es que la capacidad de detección es menor.

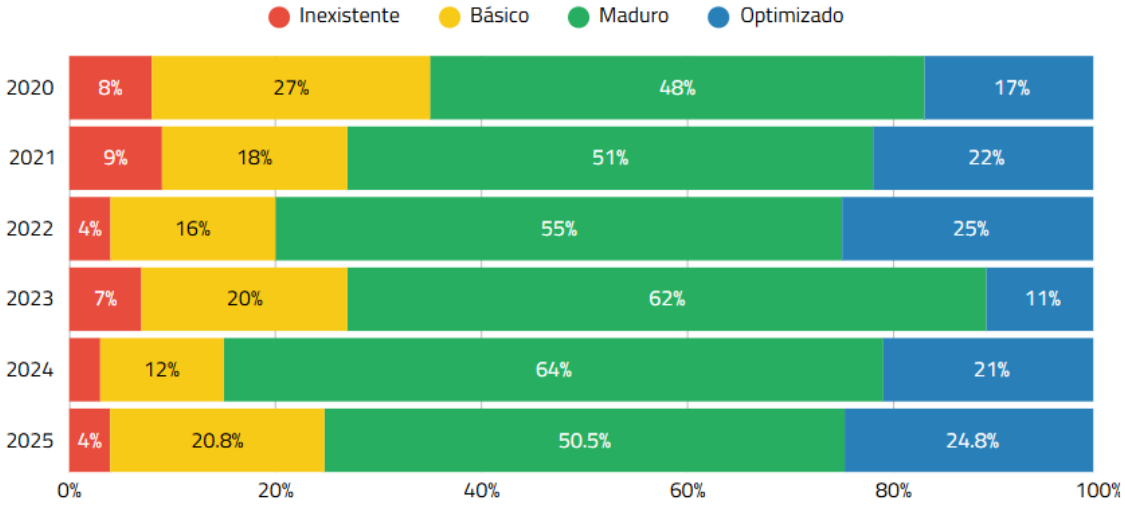
La categoría **“inexistente” (3% en 2025)** vuelve a empeorar, invirtiendo la tendencia de mejora que había registrado en el año anterior (1% en 2024), aunque sigue mejorando el dato alarmante de 2023 donde registró un 9% de empresas sin esta capacidad tecnológica para recolectar eventos de seguridad.

La capacidad de detección de actividad anómala sigue un patrón similar a la de disponibilidad de sistemas de recolección de eventos. Las empresas que no habían empezado han empeorado (con un 5% de empresas que declaran no tener nada, lo que supone un +2% en la categoría "Inexistente" respecto a 2024) y las que sí habían empezado van evolucionando positivamente. Este patrón muestra de nuevo una brecha entre las empresas que tienen muy baja madurez en la detección proactiva y el resto que ya iniciaron su camino y muestran una ligera elasticidad en su percepción del estado actual, manteniéndose en cifras similares, lo que es lógico por la propia evolución cambiante y sofisticación de las amenazas, y por las posibles dificultades en la implementación o mantenimiento de herramientas de monitorización avanzada.

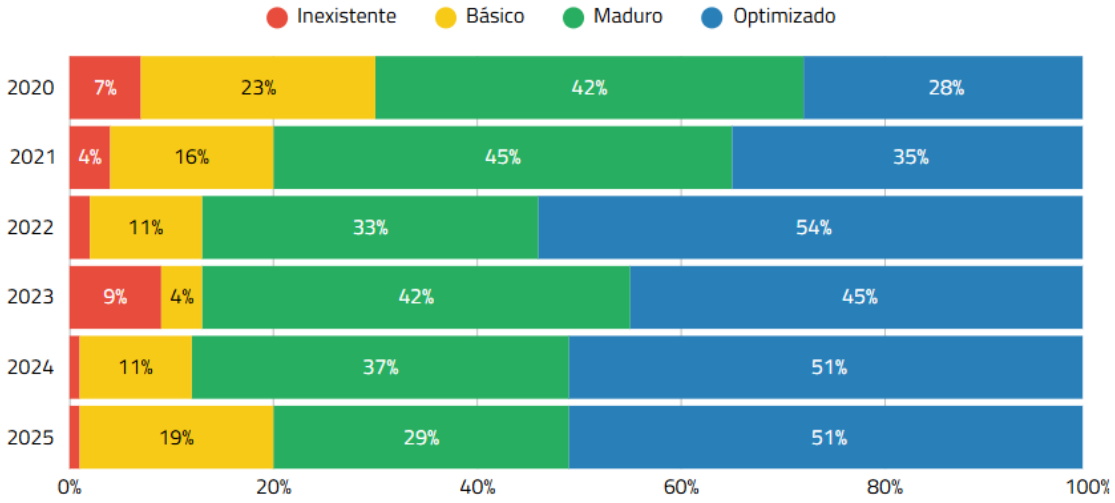
La monitorización de actividad de usuarios (incluídos proveedores) con la finalidad de identificar eventos de ciberseguridad se mantiene estable en torno al 51% en las empresas con el nivel “optimizado”, es decir el mas alto en este aspecto, mientras que decrece ocho puntos en las del nivel ligeramente inferior que se declaran en un nivel “básico” en lugar de “maduro”. El nivel de madurez “inexistente” se mantiene en un 1% igual que el año anterior. La franja media ha retrocedido en la monitorización de actividad de usuarios (incluidos proveedores).

La definición y actualización de procedimientos de detección de incidentes se ha polarizado ligeramente con un +2% en ambos extremos “optimizado” e “inexistente” lo que confirma que los esfuerzos de mejora en la banda alta se ven contrarrestados por algo de empeoramiento en la banda baja, mostrando dos velocidades de adopción de controles. Los maduros aceleran, los menos maduros deceleran.

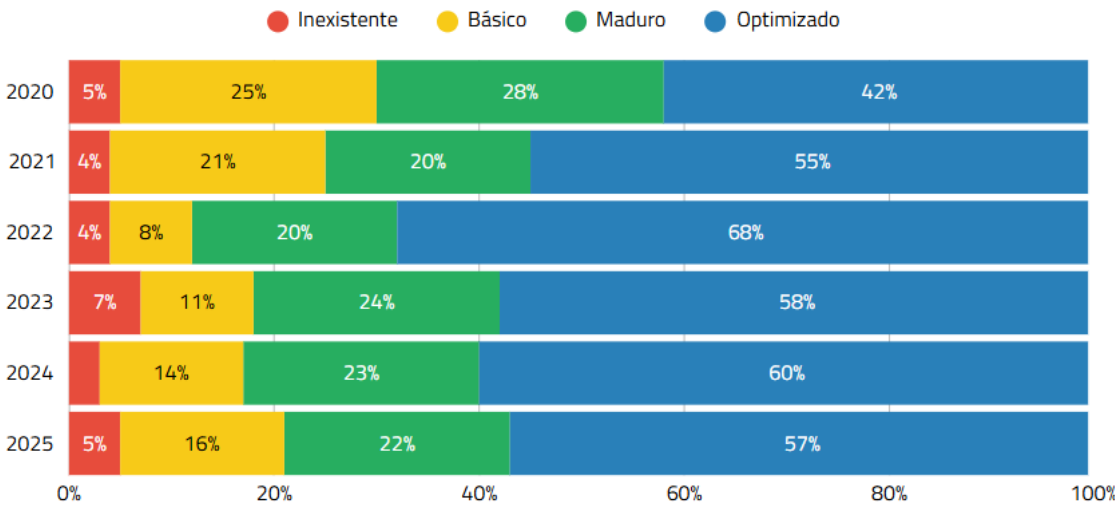
¿Los procedimientos y los roles que forman parte de los procesos de detección de incidentes están definidos, se actualizan y se prueban regularmente?



¿La actividad de los usuarios (incluidos proveedores) en los sistemas y las redes están monitorizados para la identificación de eventos de ciberseguridad?



¿Lleva a cabo su organización análisis para la detección de actividad anómala?



¿Dispone su organización de sistemas para la recolección de eventos?

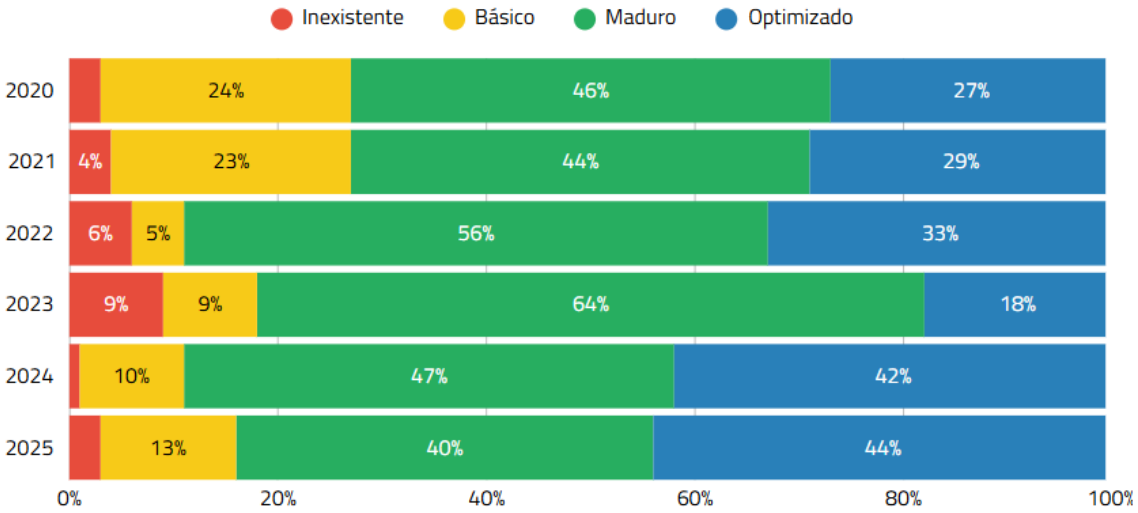


Ilustración 10: Evolución de la tendencia del domino Detectar

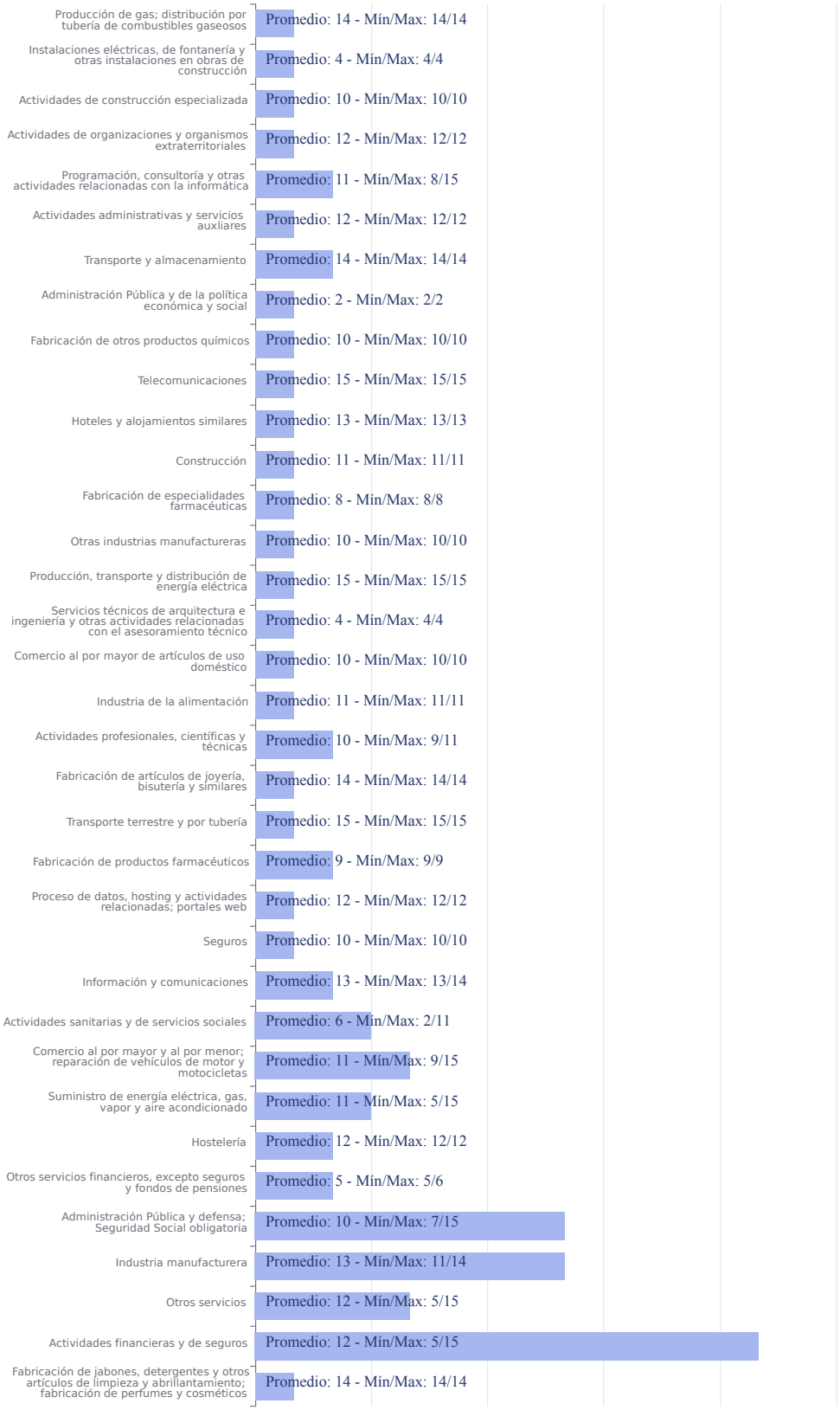


Ilustración 11: Indicador "Detectar" por sector de actividad

6.4. Dominio 4: Responder

En 2025, el dominio Responder mantiene una tendencia de consolidación, aunque hay áreas que muestran mejoras moderadas y otras experimentan ligeros retrocesos tras el avance de 2024.

Desde el observatorio, evidenciamos como las organizaciones parecen haber alcanzado un punto de madurez sostenida, donde los procesos de respuesta, análisis forense e investigación de alertas están bien establecidos, pero el ritmo de optimización se desacelera. Se observa una ligera pérdida de impulso en la mejora continua y la comunicación formalizada, lo que podría indicar que, tras los esfuerzos de recuperación de 2024, las prioridades se han equilibrado hacia la estabilización operativa más que hacia la evolución del modelo de respuesta.

En 2025, el dominio **Responder refleja una madurez estable en la mayoría de sus áreas,** consolidando el progreso alcanzado en 2024. Los datos sugieren que las organizaciones han afianzado sus procesos de respuesta ante incidentes y de gestión post-incidente, pero con una menor expansión hacia niveles optimizados.

El proceso formal de mejora continua muestra un leve avance. En 2024, el 18% de las organizaciones se encontraban en el nivel optimizado, cifra que en **2025 asciende tímidamente al 19%**, mientras que el nivel maduro retrocede en torno al 49%. Este comportamiento indica que, si bien las capacidades de respuesta siguen siendo sólidas, la evolución hacia modelos de mejora continua más automatizados o integrados se ha ralentizado, probablemente por una priorización de la estabilidad operativa frente a la expansión de capacidades.

En la identificación temprana de vulnerabilidades y amenazas, el panorama es más positivo. El nivel optimizado asciende hasta el 32%, dejando el maduro en un 52%, consolidando la tendencia de fortalecimiento en las capacidades de detección, mitigación y contención. Este incremento sugiere que las organizaciones están integrando de forma más sistemática la gestión preventiva en sus procesos de respuesta.

La realización de análisis forense tras incidentes experimenta una ligera mejora en los niveles intermedios, pero una pequeña contracción en el nivel más alto de

madurez. En 2025, el **21% de las organizaciones alcanza el nivel optimizado**, frente al 37% de 2024, mientras que el maduro se incrementa al 45%. Esta redistribución indica un avance hacia prácticas más uniformes y estandarizadas, con menos extremos de madurez. No obstante, el descenso en el nivel optimizado podría señalar una limitación en recursos especializados o en automatización de análisis post-incidente.

En cuanto a la investigación de alertas, los resultados de 2025 confirman que sigue siendo una de las áreas más consolidadas del dominio. **Más del 39% de las organizaciones se encuentran en el nivel optimizado, y el 44% en el nivel maduro**, consolidando una base de operación sólida en los equipos de monitoreo y detección. Aunque se observa un leve retroceso respecto a 2024 (donde el 52% estaba optimizado), la tendencia global sigue siendo muy positiva, reflejando una madurez sostenida en la gestión de alertas y eventos.

Finalmente, la formalización de roles y comunicación ante incidentes muestra una pequeña pérdida de impulso. En 2025, **el 22% de las organizaciones alcanza el nivel optimizado, frente al 23% de 2024, y el nivel maduro baja ligeramente al 47%**.

Sin embargo, los niveles “inexistente” y “básico” se mantienen bajos (8% y 23% respectivamente), lo que confirma que la mayoría de las organizaciones mantienen procesos bien definidos de coordinación y comunicación, aunque sin mejoras significativas respecto al año anterior.

En conjunto, los resultados de 2025 muestran que el dominio Responder ha alcanzado un estado de madurez consolidada: las organizaciones han estabilizado sus procesos de respuesta e investigación, con mejoras marginales y ligeras oscilaciones entre los niveles altos de madurez. El enfoque actual parece orientarse más hacia la optimización continua y la eficiencia operativa, que hacia la expansión de nuevas capacidades. Esta estabilización sugiere que el dominio ha entrado en una fase de madurez estructural, donde la mejora incremental y la automatización serán los próximos retos para mantener el progreso sostenido.

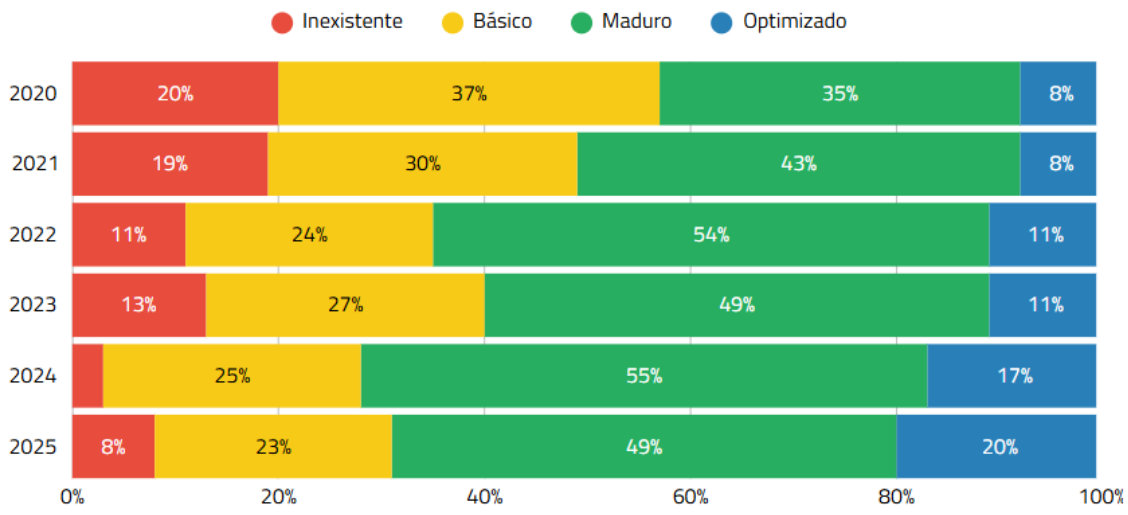
El análisis por sectores revela diferencias notables en el nivel de madurez del dominio Responder, con una clara concentración de los valores promedio entre 12 y 14 puntos, lo que sugiere una madurez globalmente consolidada, aunque con

brechas significativas entre industrias. Los sectores financieros y de seguros y transporte terrestre y por tubería se sitúan en la parte alta con promedios de 14 y 18, respectivamente, reflejando una fuerte capacidad de respuesta ante incidentes, alta formalización de procesos y un uso más extendido de prácticas optimizadas. También destacan industria manufacturera y administración pública y defensa, ambas con promedios de 13 a 14 puntos, lo que indica una madurez avanzada y una gestión bien estructurada de la respuesta a incidentes.

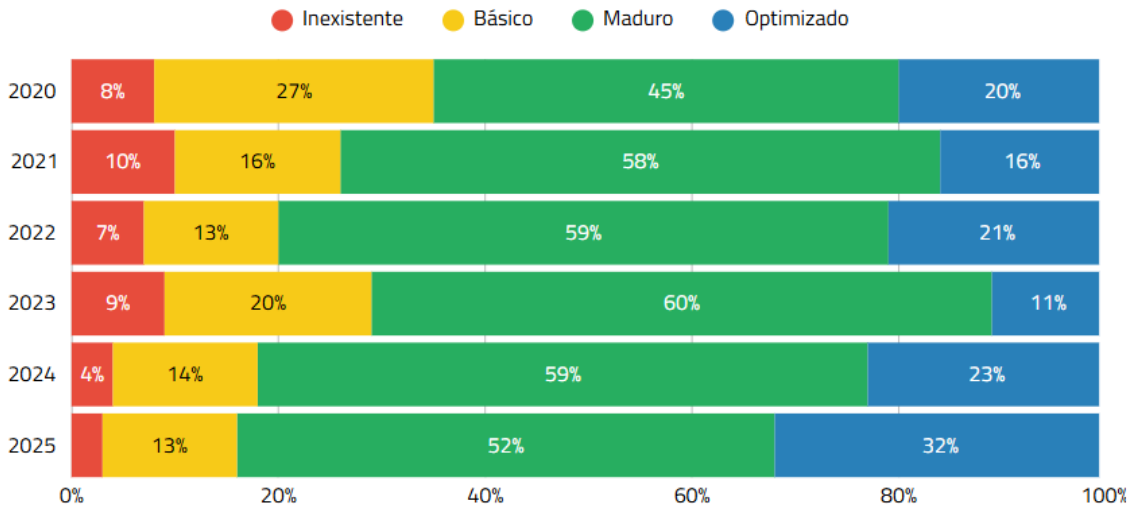
Por el contrario, los sectores: sanitario y de servicios sociales, hostelería y actividades profesionales y científicas muestran los valores más bajos, con promedios entre 6 y 8 puntos, evidenciando madurez limitada y procesos aún en desarrollo. Estos sectores, tradicionalmente más enfocados en la continuidad del negocio que en la respuesta técnica, presentan oportunidades claras para fortalecer sus capacidades de detección, investigación y comunicación post-incidente.

En conjunto, los datos reflejan un panorama heterogéneo: los sectores regulados o con alta exposición al riesgo financiero lideran la madurez del dominio Responder, mientras que aquellos con menor presión normativa o menor inversión en ciberseguridad mantienen un nivel intermedio o básico. Esta variabilidad pone de relieve la necesidad de ajustar las estrategias de respuesta a incidentes según la criticidad del sector y su nivel de madurez digital, priorizando la profesionalización y estandarización de procesos en los ámbitos menos avanzados.

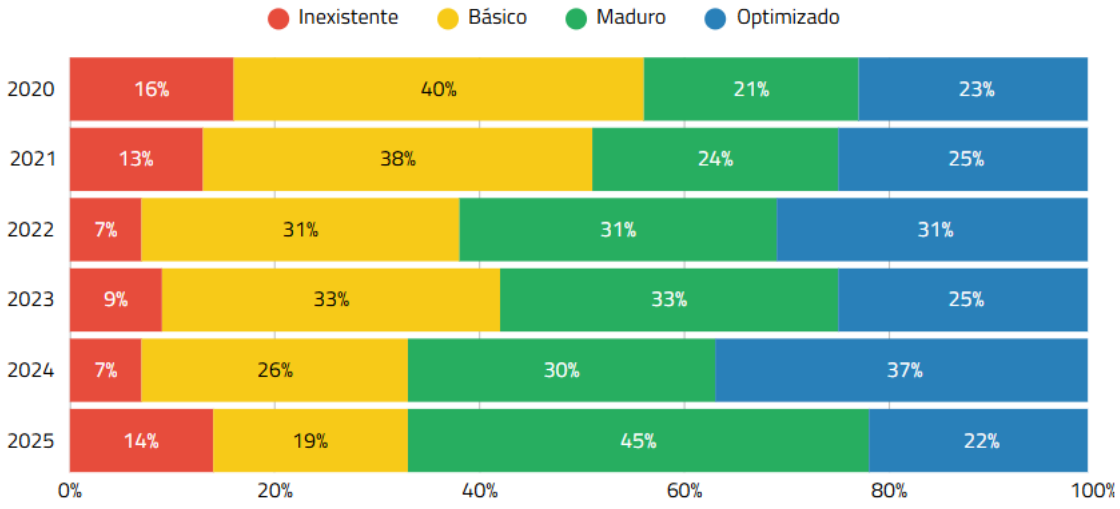
¿Cuenta su organización con un proceso formal para la mejora continua de la respuesta ante incidentes, en base a lecciones aprendidas de incidentes pasados?



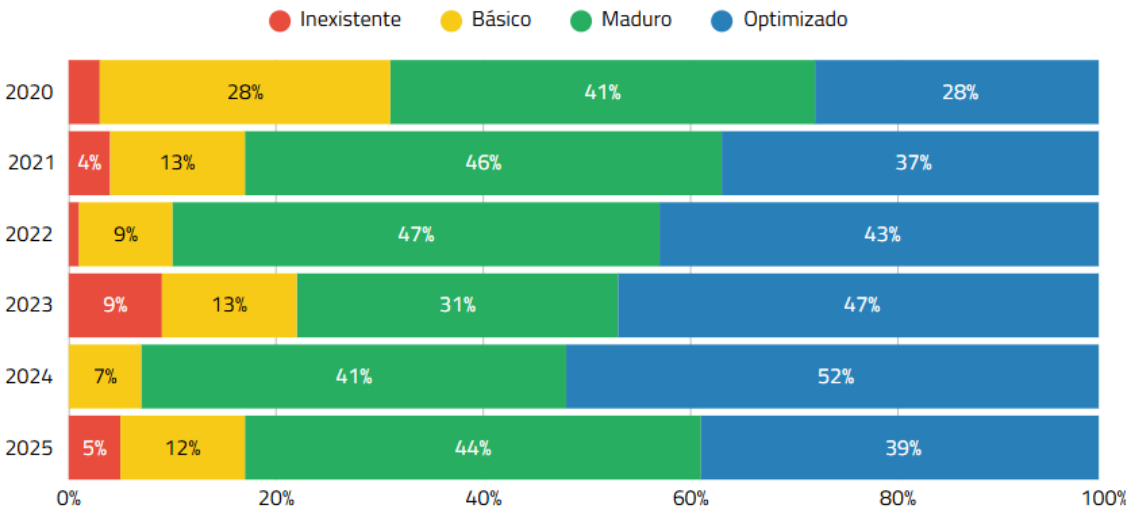
¿Lleva a cabo su organización la identificación temprana de vulnerabilidades y amenazas y cuenta con procesos de mitigación y contención para evitar la expansión de un potencial incidente?



¿Tras un incidente de seguridad, se lleva a cabo un análisis detallado mediante análisis forense?



¿Las alertas generadas por los sistemas de detección son investigadas?



¿El proceso, los roles y los principales interlocutores en la comunicación (interna y externa) en la respuesta ante incidentes están formalizados?

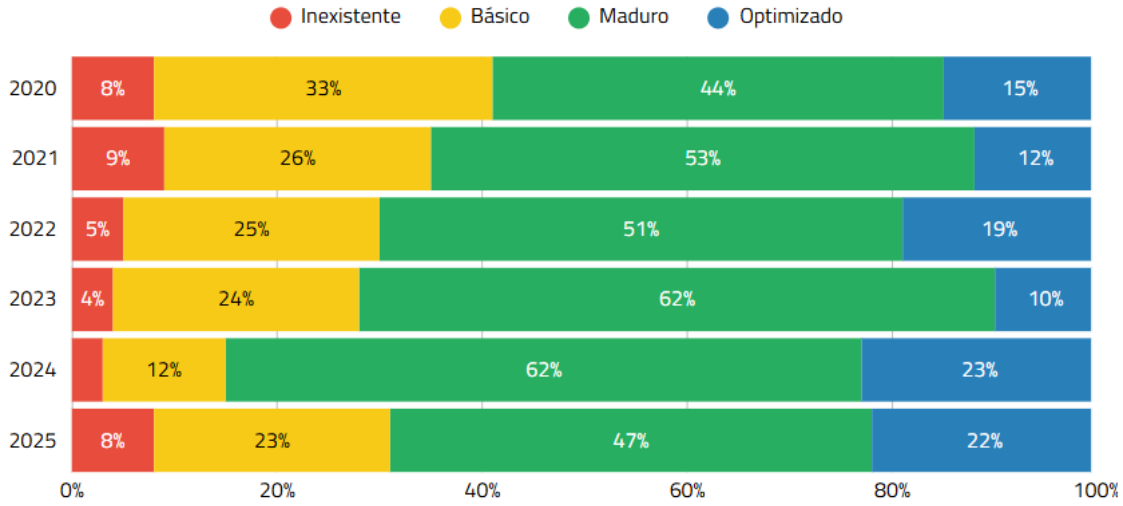


Ilustración 12: Evolución de la tendencia del domino Responder

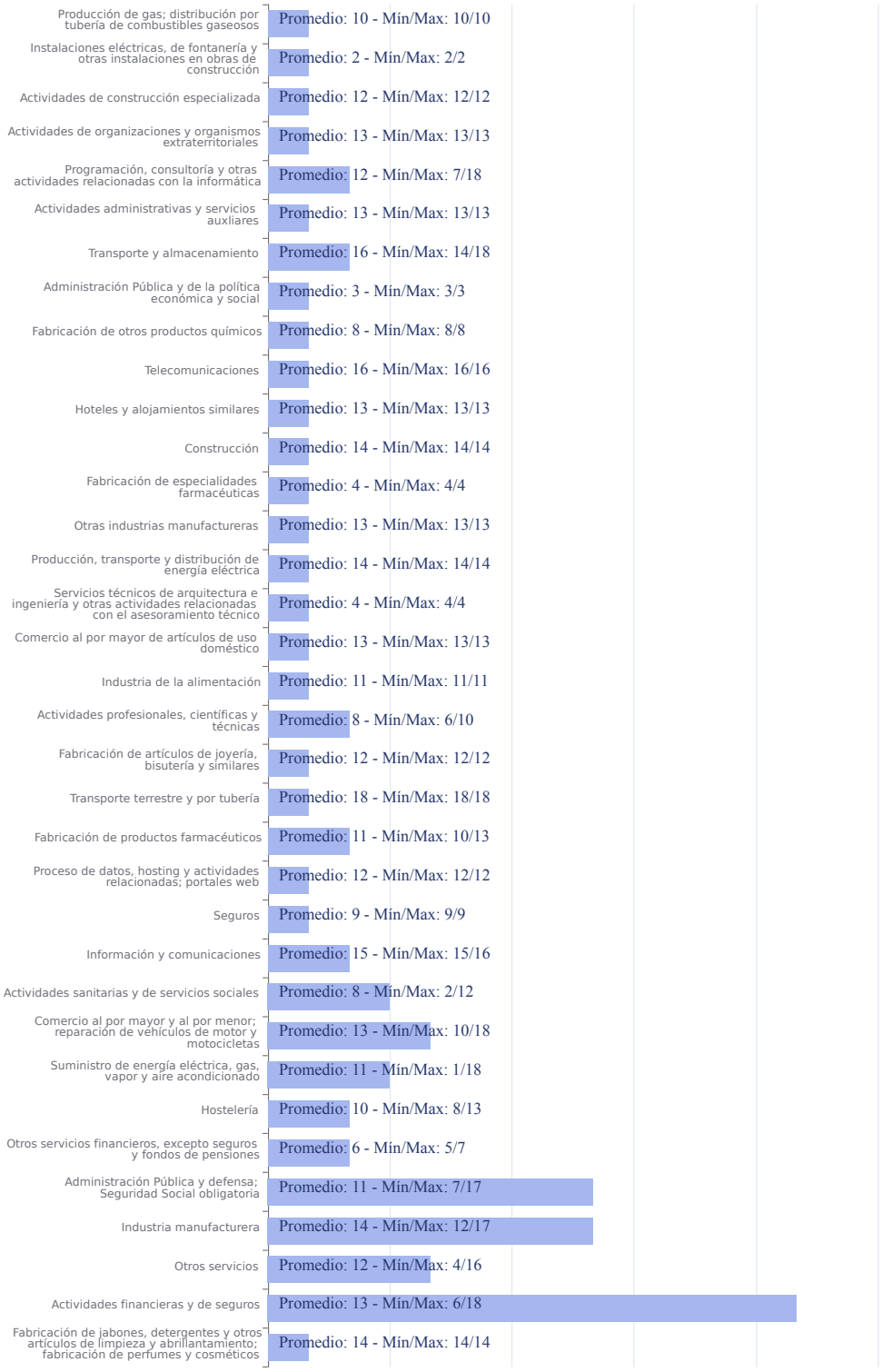


Ilustración 13: Indicador "Responder" por sector de actividad

6.5. Dominio 5: Recuperar

En 2025, el dominio Recuperar muestra una leve regresión respecto al año anterior, rompiendo la tendencia de mejora que se había iniciado en 2024. Los resultados de esta edición evidencian un estancamiento en la madurez de los planes de recuperación, acompañado de un aumento del nivel básico en las tres dimensiones evaluadas: la comunicación durante el proceso de recuperación, la actualización de los planes y la formalización y prueba regular de los mismos.

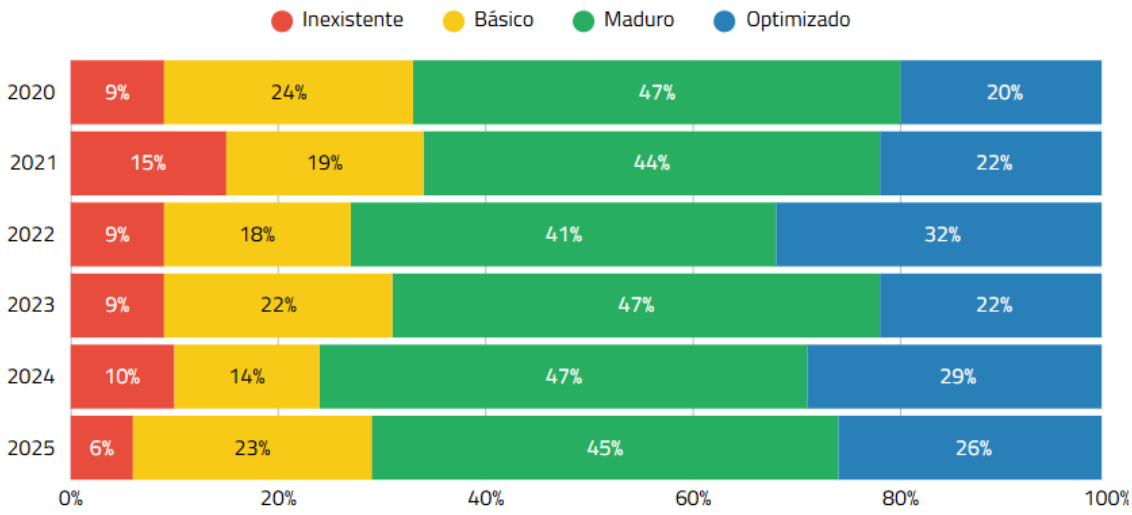
Este cambio de tendencia sugiere que, si bien las organizaciones han consolidado ciertos procesos mínimos de recuperación, todavía enfrentan dificultades para avanzar hacia niveles de madurez más altos y mantener una práctica continua de mejora.

En lo que respecta a la definición de actividades y roles en la comunicación interna y externa durante la recuperación, el porcentaje de organizaciones en **nivel maduro desciende ligeramente del 47 % al 45 %, mientras que el nivel básico aumenta del 14% al 23%.** Este desplazamiento indica que, aunque la mayoría de las organizaciones cuentan con mecanismos definidos de comunicación, en muchos casos estos no se actualizan ni se formalizan con la frecuencia deseada.

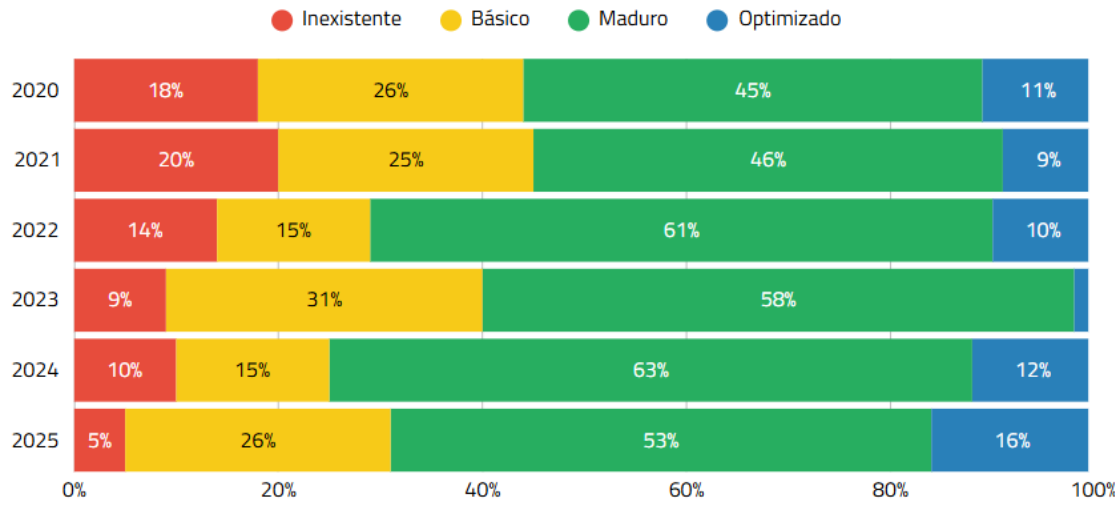
Una tendencia similar se observa en la actualización proactiva de los planes y estrategias de recuperación, donde el nivel maduro desciende del 63% en 2024 al 53% en 2025, mientras que el nivel básico aumenta significativamente, pasando del 15% al 26%. Esto revela una pérdida de continuidad en los ejercicios de revisión y una menor incorporación de lecciones aprendidas, lo que podría deberse a la priorización de otros ámbitos operativos o a la falta de recursos específicos dedicados a la mejora de la resiliencia.

Por último, la formalización y prueba regular de los planes de recuperación mantiene un comportamiento muy similar: **el nivel maduro se reduce del 62% al 52%, mientras que el básico crece del 16% al 26%**. Este patrón apunta a una disminución de la práctica sistemática de pruebas y simulacros, que son fundamentales para validar la eficacia real de los procedimientos de recuperación ante incidentes.

¿Las actividades y roles en la comunicación (interna y externa) durante un proceso de recuperación están definidos, y los principales interlocutores identificados?



¿Los planes y estrategias de recuperación se actualizan regular y proactivamente para incorporar mejoras y lecciones aprendidas?



¿Los planes y estrategias de recuperación de los sistemas clave de negocio ante incidentes de ciberseguridad se encuentran formalizados y se prueban regularmente?

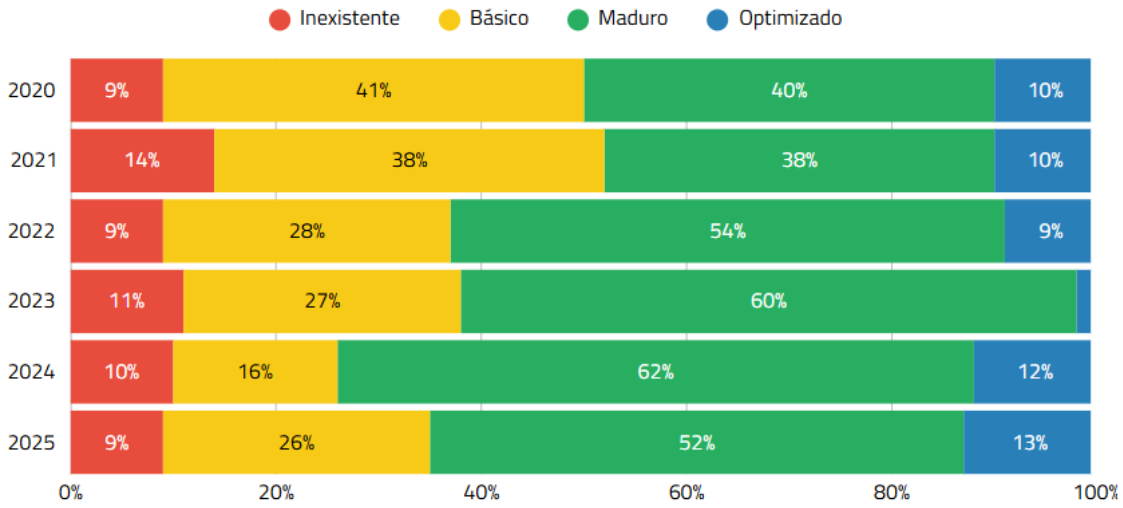


Ilustración 14: Evolución de la tendencia del domino Recuperar

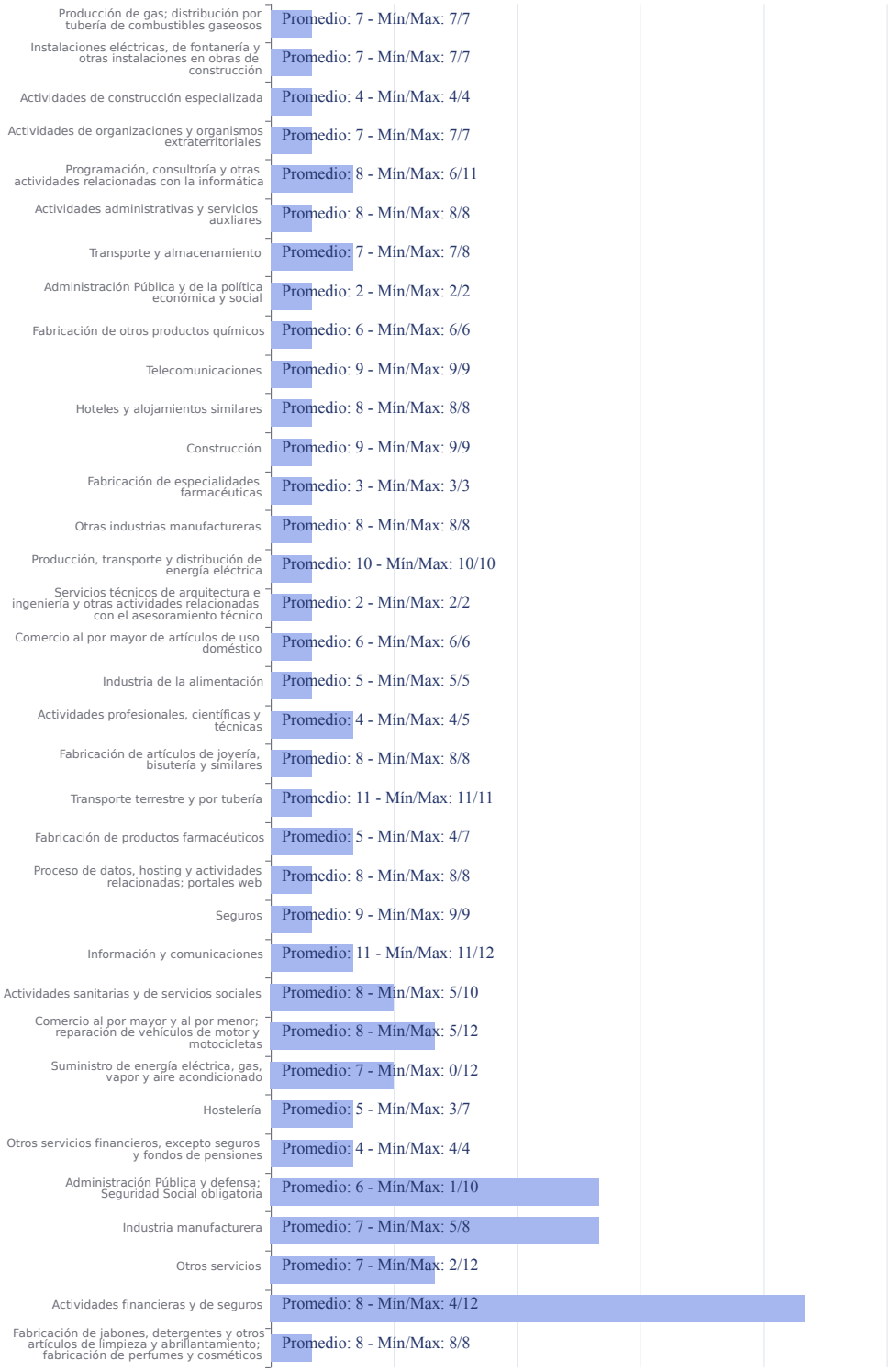


Ilustración 15: Indicador "Recuperar" por sector de actividad.

6.6. Dominio 6: Gobierno

La madurez en la definición y comunicación de roles, responsabilidades y requisitos regulatorios se ha visto mermada en los últimos resultados. En 2025, se ha reducido el porcentaje de o**rganizaciones con procesos optimizados en este aspecto, situándose en un 61%,** el mismo valor registrado en 2020.

La madurez en los procesos de gestión del riesgo, incluyendo el establecimiento del nivel de tolerancia y la comunicación con las partes interesadas, también se ha visto afectado. En 2024, el 55% de las organizaciones tienen estos procesos optimizados, sin embargo, en **2025 este dato pasa a ser tan solo un 36%**, siendo el peor valor desde 2020. No obstante, la categoría de “Inexistente” se mantiene en un 6%, siendo mejores datos que en 2020, donde esta cifra ascendía a un 14%. Esto refleja un interés en seguir mejorando la formalización y transparencia de la gestión del riesgo.

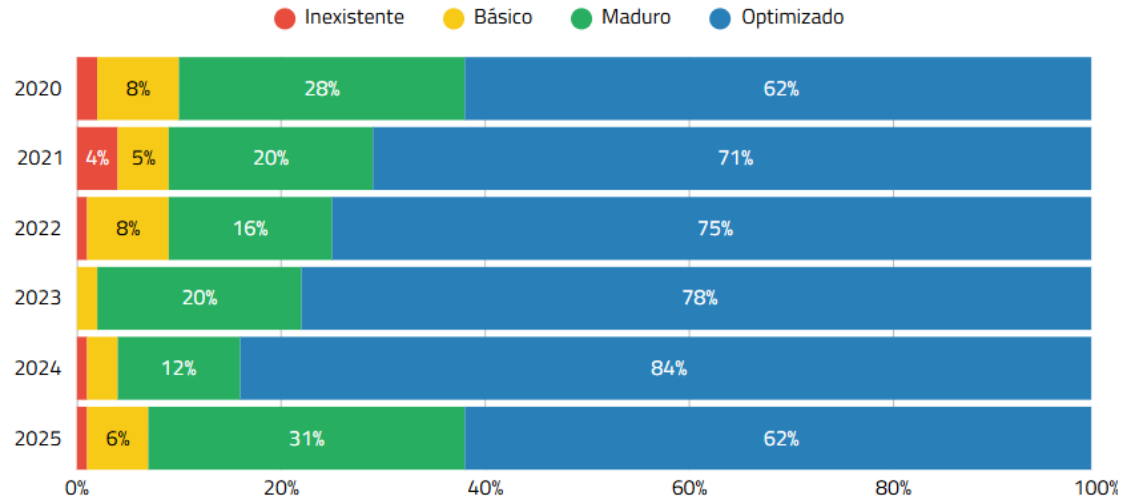
Se ha observado una ligera mejora en los niveles de madurez de la gestión de riesgos en la cadena de suministros. En 2024 la cifra de organizaciones en nivel optimizado era de un 27%, y este año **2025 ha llegado a un 32%,** siendo la mejor cifra después de 2022 (35%). La categoría "Inexistente" se ha visto ligeramente aumentada, de un 7% en 2024 a un 10% en 2025. En este aspecto, se ven patentes los desafíos en la implementación de controles consistentes en toda la cadena de suministro.

En cuanto a la identificación y comunicación de dependencias y requisitos críticos, se observa una tendencia similar a la del año 2021. En 2024, un 49% de **las organizaciones alcanzaron un nivel optimizado, siendo tan solo un 26% en 2025**, muy parecido a los resultados de 2021 (28%). **La categoría “Maduro”** es la que ha experimentado un aumento, pasando de un 32% en 2024 a **un 47% en 2025,** demostrando una evolución hacia una mayor integración de la ciberseguridad en la estrategia organizacional y un interés en seguir asegurando que las funciones críticas sean identificadas y gestionadas en alineación con la misión y objetivos de la organización.

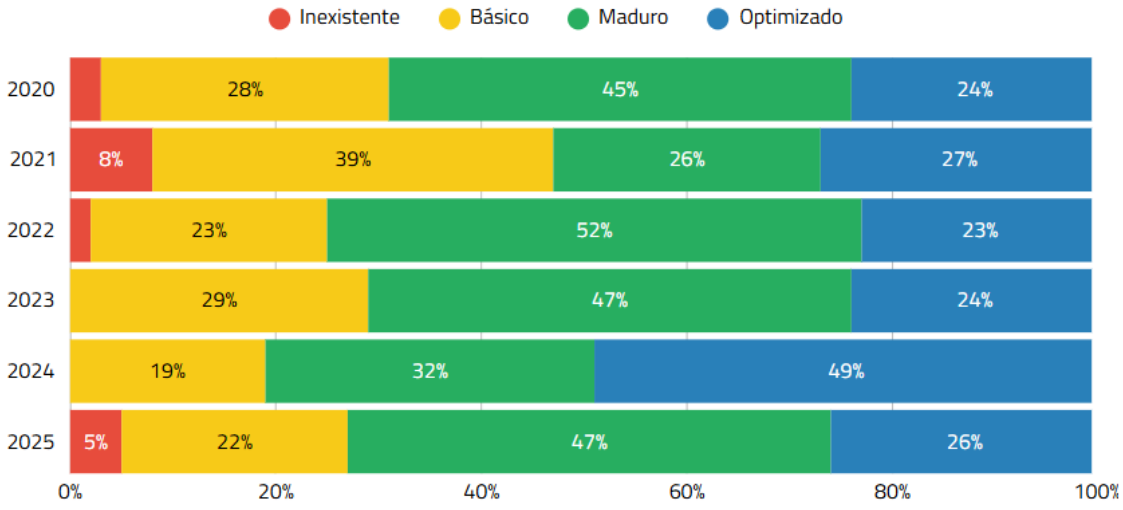
Los datos de los últimos seis años muestran en general un progreso constante en el dominio de Gobierno. A pesar de que los datos de 2025 son ligeramente inferiores a los de 2024, las organizaciones siguen avanzado en la implementación y madurez de sus prácticas de gestión del riesgo, tanto internas como en su cadena de suministro, y en la comunicación de políticas y dependencias críticas.

Este análisis refleja una concienciación en el fortalecimiento en la gobernanza de ciberseguridad, con una adopción cada vez mayor de prácticas avanzadas y estructuradas, lo que refuerza la resiliencia organizacional frente a riesgos emergentes.

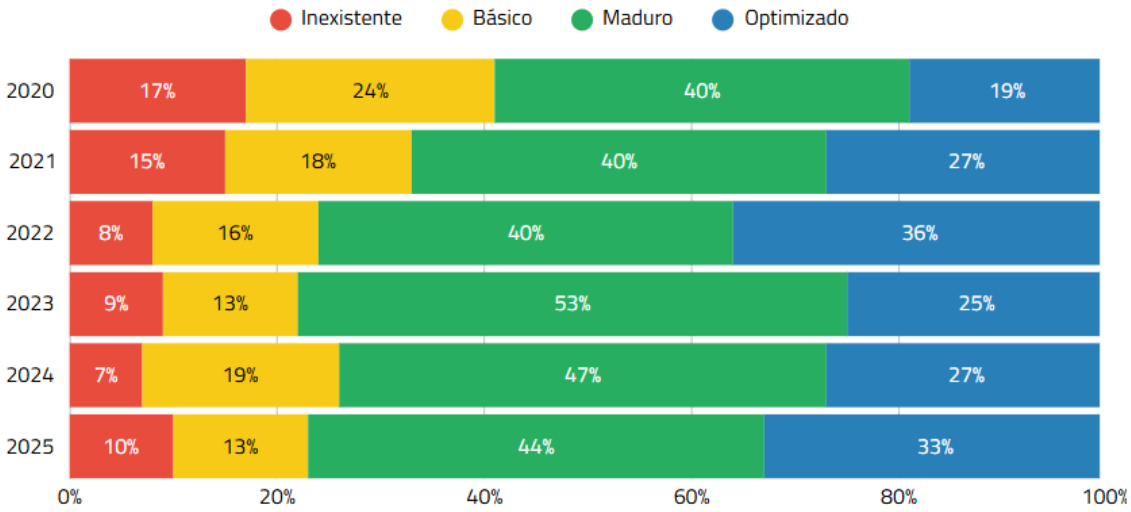
¿Existe y esta comunicada una política donde se definen los roles y responsabilidades junto con requerimientos legales y regulatorios dentro del marco de los procesos de gobierno y gestión del riesgo de ciberseguridad?



¿Se identifican y comunican las dependencias y los requisitos de servicios y funciones críticas, asociadas a la misión, visión y objetivos de la organización?



¿Los procesos de gestión del riesgo de la cadena de suministro (proveedores y terceros) están establecidos y aceptados por la organización, así como las medidas apropiadas establecidas en los contratos?



¿Los procesos de gestión del riesgo, así como del nivel de tolerancia están establecidos, gestionados, acordados e informados con las partes interesadas?

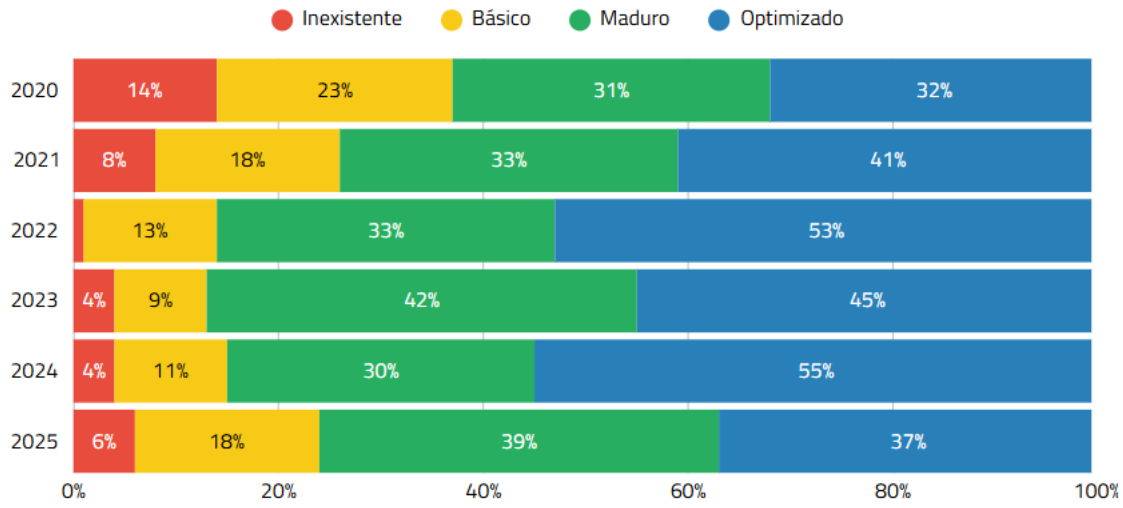


Ilustración 16: Evolución de la tendencia del domino Gobierno

En este apartado se presentan los datos relativos al dominio de Gobierno, que evalúa el grado en que las organizaciones integran la ciberseguridad dentro de sus estructuras de gobernanza y establecen políticas, roles y responsabilidades claras en la gestión de riesgos. Este indicador resalta la importancia de establecer políticas y procesos claros para gestionar la ciberseguridad a nivel estratégico, garantizando una supervisión constante y una asignación de responsabilidades efectiva en toda la organización.

El promedio general para el dominio Gobierno es de aproximadamente 10, lo que indica un nivel de madurez medio en términos de gobernanza en ciberseguridad. Los sectores con los promedios más altos son Información y comunicaciones y Transporte terrestre y por tubería, ambos con un nivel de madurez consolidado (con valores de 15), lo que sugiere que estos sectores tienen estrategias y prácticas de gobernanza sólidas, en las que la ciberseguridad se halla integrada en las estructuras de dirección.

Dispersión en varios sectores: Se observa una notable variabilidad en los resultados en sectores como Programación, consultoría y otras actividades relacionadas con la informática (dispersión entre 5 y 12); Actividades profesionales, científicas y técnicas (variado entre 5 y 13), Fabricación de productos farmacéuticos (de 4 a 14); Actividades sanitarias y de servicios sociales (variado de 4 a 11), Comercio al por

mayor y al por menor; reparación de vehículos de motor y motocicletas (7 a 15), Administración pública y defensa; Seguridad Social obligatoria (6 a 12) y Actividades financieras y de seguros (con valores entre 5 y 15).

Estos valores indican que existen organizaciones dentro de estos sectores con un margen considerable de mejora en sus prácticas de gobernanza en ciberseguridad. Sectores con menor madurez: Destaca el sector de Fabricación de especialidades farmacéuticas, que presenta el promedio más bajo (3), lo cual pone de manifiesto la necesidad de reforzar e implementar medidas de gobernanza y ciberseguridad más robustas.

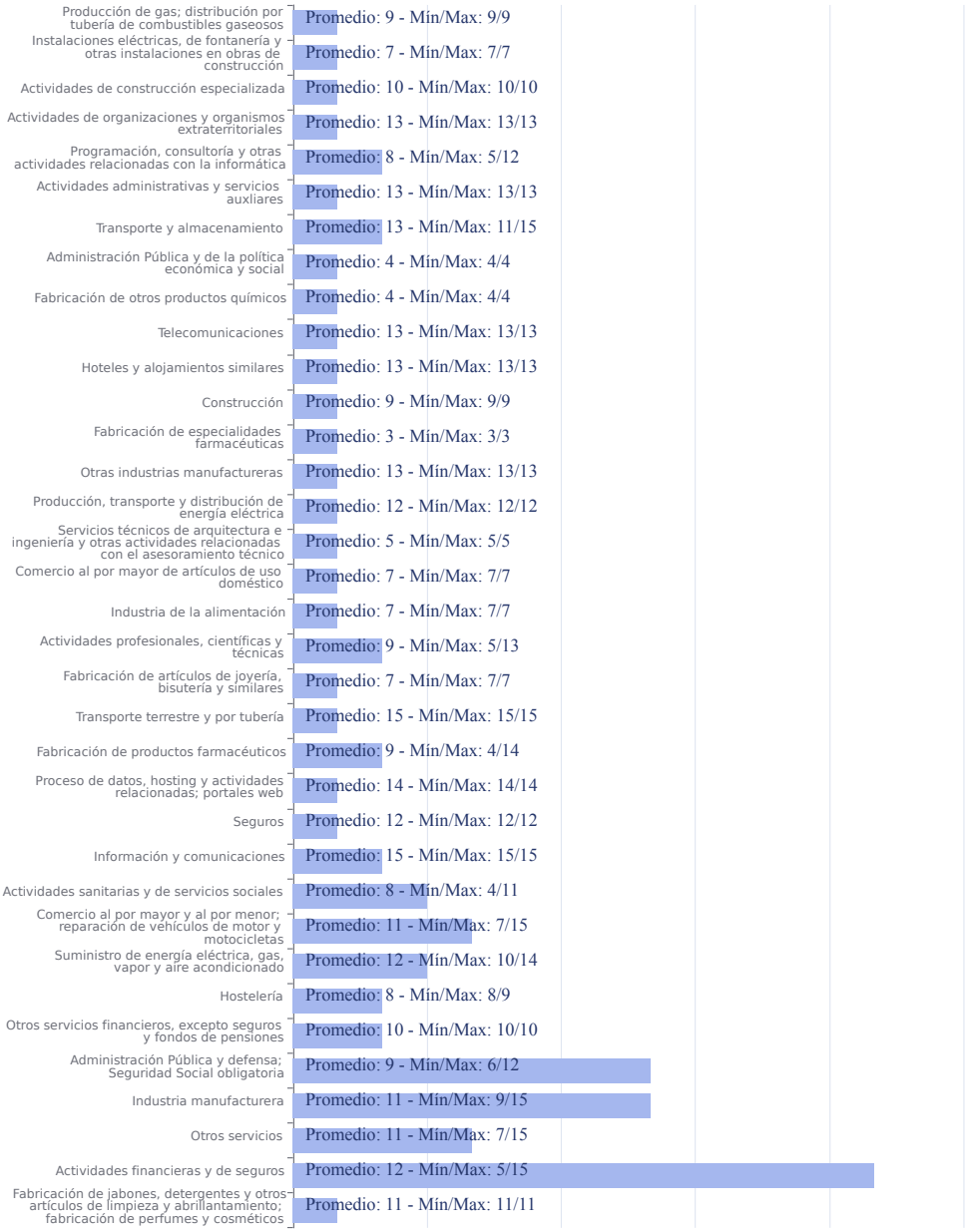


Ilustración 17: Indicador "Gobierno" por sector de actividad.

7. Recursos y Organización

El dimensionamiento de los equipos internos de ciberseguridad constituye un indicador clave para evaluar la madurez organizativa y la capacidad de respuesta ante incidentes.

En esta sección se analizan las tendencias observadas en la composición de dichos equipos.

Rompiendo la tendencia reflejada en el informe de 2024, las respuestas recogidas en esta edición desvelan una **disminución del personal interno** que conforma los equipos de ciberseguridad de las entidades participantes.

En la encuesta de este año, observamos que los equipos más reducidos son los más habituales dentro de las organizaciones: un **57,69% declara contar con un área de ciberseguridad compuesta por entre 1 y 5 empleados** (lo que supone un incremento notable respecto al 42,46% de 2024), mientras que el **21,79% de los encuestados dispone de un equipo conformado por entre 5 y 15 personas** (dato muy similar al 21,92% de 2024). En contrapartida, **las entidades con entre 15 y 50 empleados dedicados a ciberseguridad descienden al 16,67%** (frente al 24,66% del año anterior) y aquellas con los equipos más numerosos, con más de 50 personas, suponen únicamente el 3,85% del total (en comparación con el 10,96% de 2024).

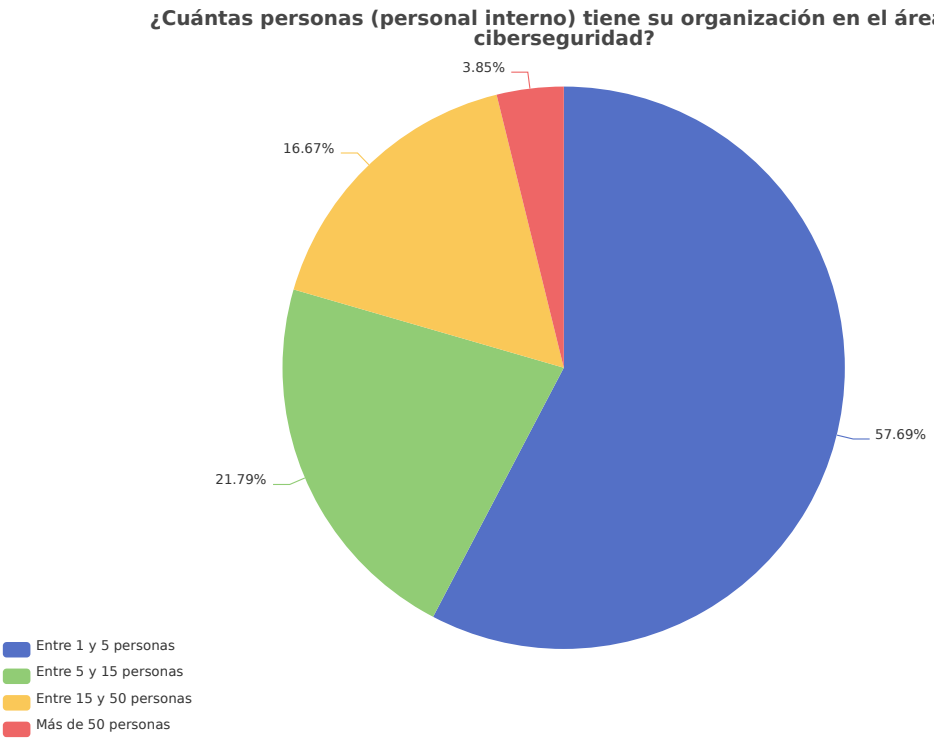


Ilustración 18: Personal interno en ciberseguridad

Este escenario sugiere que las organizaciones están priorizando modelos más ágiles, apoyados en automatización y servicios gestionados, frente a estructuras internas extensas. Esta disminución podría deberse a factores tales como la automatización de ciertas tareas operativas (utilizando tecnologías como SOAR, IA o machine learning) o a una mayor tendencia a la externalización de servicios de ciberseguridad que, a su vez, podría responder a la dificultad de encontrar talento especializado. No obstante, ninguna de estas hipótesis puede corroborarse de manera fehaciente con los datos disponibles de la encuesta.

Además del tamaño del equipo, resulta relevante conocer si el departamento asume la operación directa de la seguridad, aspecto que condiciona la necesidad de recursos internos. En este sentido, **el 74,36% de las organizaciones indica que su departamento de ciberseguridad opera la seguridad**, mientras que **el 25,64% delega esta función en terceros**.

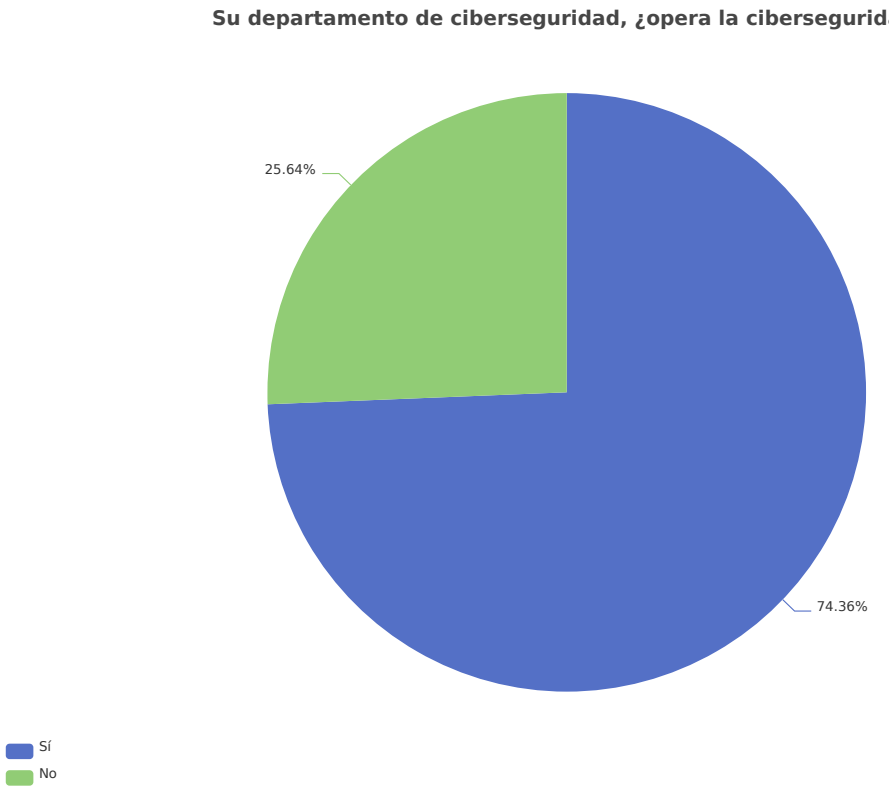


Ilustración 19: Operación de la Seguridad

8. Riesgos y ciberinseguridad

Siguiendo con los objetivos propios del Observatorio de la Ciberseguridad de ISMS de promover el conocimiento e investigación en este ámbito, generando métricas y referencias nacionales, en esta edición se ofrece por segunda vez la estimación de probabilidades de ocurrencia de ciberincidentes con distintos niveles de impacto. Este indicador pretende transmitir, no sólo a los profesionales del sector, sino a instituciones, reguladores, consejos de administración y a la sociedad en general, la magnitud que suponen actualmente los riesgos vinculados al ciberespacio.

Para hacerlo, se busca ofrecer datos de la máxima calidad obtenidos de especialistas, aprovechando el enorme talento y experiencia de la comunidad de CISOs y responsables de seguridad de la información de nuestro país que participan en la elaboración del Indicador de Madurez en Ciberseguridad.

En este particular, se pedía a los encuestados que sus respuestas reflejasen su opinión sobre el conjunto del sector en que opera la organización en la que trabaja, en lugar de la situación de esta en particular. Del mismo modo, las respuestas a esta parte del cuestionario están enfocadas en determinar el riesgo residual, es decir, la probabilidad de materialización de daños, teniendo en cuenta los procesos de gestión y salvaguarda actualmente desplegados por las organizaciones que operan en el sector.

Se asume que cada sector cuenta con un cierto conjunto de salvaguardas desplegadas y una madurez en cuanto a sus procesos de gestión que pretenden conjurar ciertos cíber-riesgos considerados críticos por las organizaciones del sector.

No obstante, puesto que una salvaguarda ideal o perfecta del 100% rara vez (o nunca) se puede alcanzar, los sistemas y organizaciones permanecen en una situación de riesgo denominada residual. Las salvaguardas reducen el riesgo, desde un valor potencial o máximo hasta cierto valor residual. Esa reducción de riesgos es la que se consigue mediante la ciberseguridad de las organizaciones y su grado de madurez, estudiado en el Indicador principal de este informe.

La magnitud de la probabilidad residual o cíber-inseguridad es la proporción que resta entre la eficacia o protección perfecta y la eficacia real o ciberseguridad. Así, el riesgo por ciberinseguridad, en nuestro caso, se define como la probabilidad de materialización de ciberamenazas con distintos niveles de impacto, superando las medidas de ciberseguridad disponibles de acuerdo con el grado de madurez de ciberseguridad de las organizaciones. En particular, los niveles de probabilidad considerados son los siguientes:

- **Muy baja:** Supone una situación muy poco frecuente que, por ejemplo, se produciría una vez cada siglo y a la que se le asignaría una probabilidad de ocurrencia del 0,01%.
- **Baja:** Refleja situaciones poco frecuentes, que pueden suceder una vez cada varios años, con una probabilidad de ocurrencia asignada del 0,1%.
- Media: Recoge situaciones normales, que pueden suceder una vez cada año, con una probabilidad de ocurrencia del 1%.
- **Alta:** Incluye las situaciones que se producen de forma frecuente, por ejemplo, cada mes, con una probabilidad de ocurrencia del 10%.
- **Muy alta:** Supone situaciones muy frecuentes, que se pueden producir diariamente y a las que se asigna una probabilidad de materialización del 100%.

Por su parte, los niveles de impacto o daño que puede producir una ciberamenaza en caso de materializarse, hacen referencia a qué efectos negativos pueden tener sobre activos críticos del sector. Así, la evaluación de riesgos de ciberinseguridad va más allá del análisis técnico (o propio de los sistemas de tecnologías de la información) y debe traducir las consecuencias a términos de negocio. De este modo, a partir de las respuestas de los encuestados, se determina la probabilidad de que las ciberamenazas se materialicen alcanzando distintos niveles de impacto o daño. En concreto, se consideraron los siguientes:

- **Insignificante**: Produce daños menores sobre los activos, que no tendrían consecuencias económicas relevantes o como máximo, estas alcanzarían hasta el 0,01% de la cifra de negocio anual.
- **Marginal:** Representa daños que podrían llegar a considerarse importantes, estando cuantificados en torno al 0,1% de la cifra de negocio anual.
- **Moderado:** Se trataría de un daño que podría considerarse como grave, equivalente al 1% de la cifra de negocio anual.
- **Crítico:** Supone consecuencias de daño muy graves, con una traducción económica cercana al 10% de la cifra de negocio anual.

- **Catastrófico:** Recoge situaciones extremadamente graves o dañinas, que podrían representar un perjuicio económico equivalente al 100% de la cifra de negocio anual.

Como puede apreciarse en la Ilustración 21, el 65,79% de los encuestados considera que la probabilidad de que se produzcan impactos insignificantes vinculados a ciberamenazas es alta o muy alta. Además, aplicando las definiciones anteriores, cabría afirmar que este tipo de impactos se sufren de manera anual o incluso más frecuentemente en un 92,11% de las ocasiones.

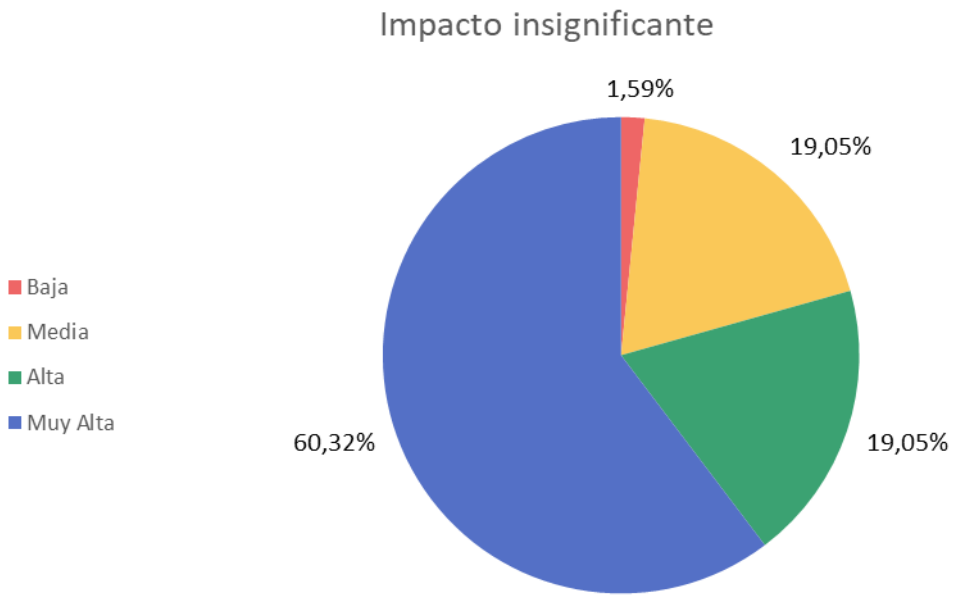


Ilustración 20: Riesgo de ciberinseguridad para impactos insignificantes

Como se muestra en la Ilustración 20, la probabilidad de un impacto alto y muy alto de manera combinada conforman el 79,37% de las respuestas. Este tipo de incidentes sigue siendo frecuentes.

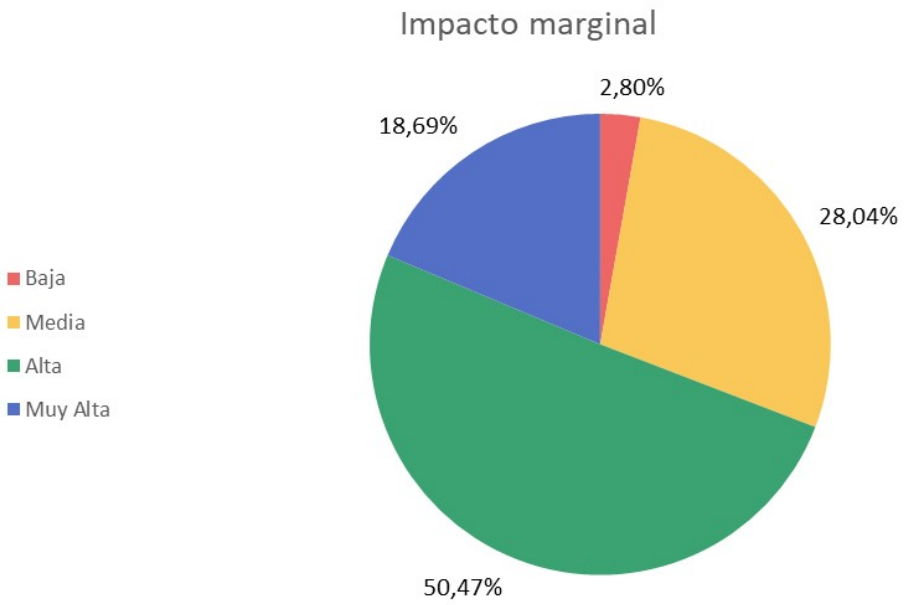


Ilustración 21: Riesgo de ciberinseguridad para impactos marginales

Tal y como muestra la Ilustración 21, los impactos marginales, que resultan más dañinos o peligrosos que los insignificantes, tienen una probabilidad de ocurrencia alta o muy alta para el 69,16% de los encuestados.

Cabe considerar que los daños insignificantes y marginales pueden considerarse como aceptables, dependiendo del apetito al riesgo de cada organización y sector, puesto que su impacto limitado desde el punto de vista económico puede no ser suficiente para justificar inversiones o compromisos adicionales para la mejora de la ciberseguridad.

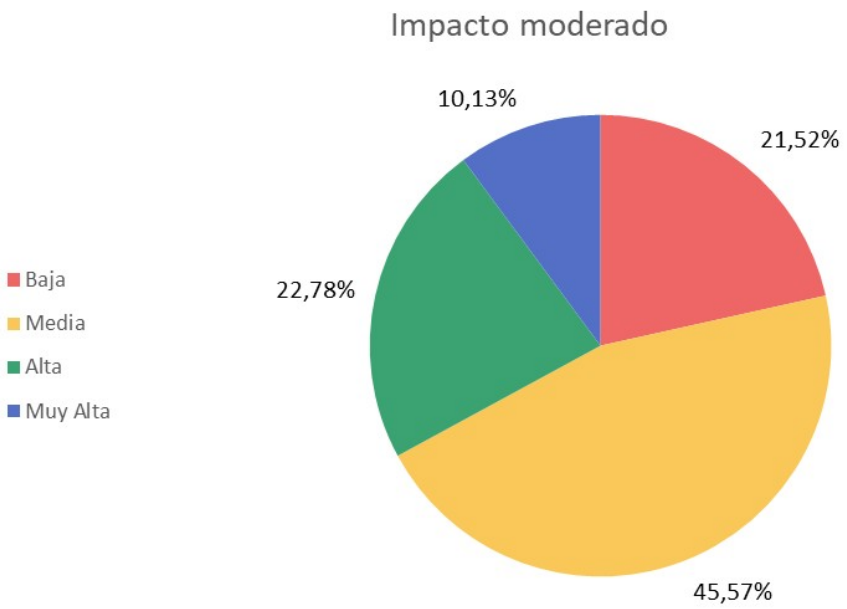


Ilustración 22: Riesgo de ciberinseguridad para impactos moderados

La Ilustración 22 muestra un cambio importante respecto al riesgo de impactos marginales e insignificantes. En concreto, la probabilidad de considerar un impacto moderado como alto y muy alto desciende hasta el 32.91%. Dada la peligrosidad que representan, un 21,52% de los encuestados considera los ciberincidentes de impacto moderado como eventos de probabilidad baja, demostrando que este tipo de impacto sí merece mayores medidas de ciberseguridad a diferencia de los marginales e insignificantes.

El efecto de una mayor atención por la seguridad está especialmente presente en el caso de los ciberincidentes con impacto crítico, tal y como muestra como muestra la Ilustración 23. En concreto, el 87,03% de los encuestados les atribuye una probabilidad media o baja. Esto demuestra que existen salvaguardas y mecanismos habilitados que, en la mayoría de ocasiones, evitan que este tipo de ciberincidentes lleguen a materializarse.

Por el contrario, sólo un 12,97% de los encuestados considera que la probabilidad de sufrir un impacto crítico es alto o muy alto.

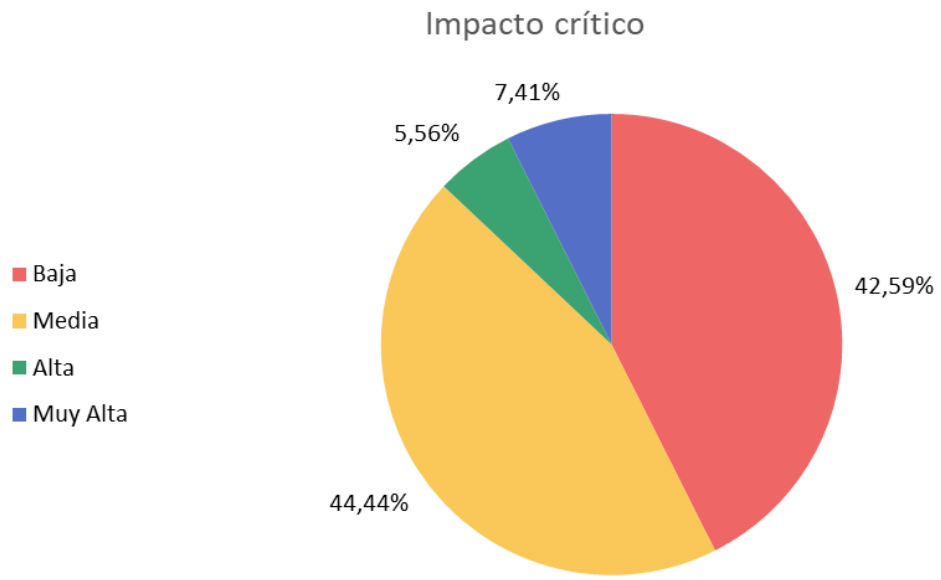


Ilustración 23: Riesgo de ciberinseguridad para impactos críticos

La probabilidad de un impacto catastrófico es media o baja para el 65,52% de los encuestados, como puede apreciarse en la Ilustración 25. Las probabilidades altas o muy altas suben de manera significativa respecto a los impactos críticos, donde para los catastróficos alcanzan el 34,48%.

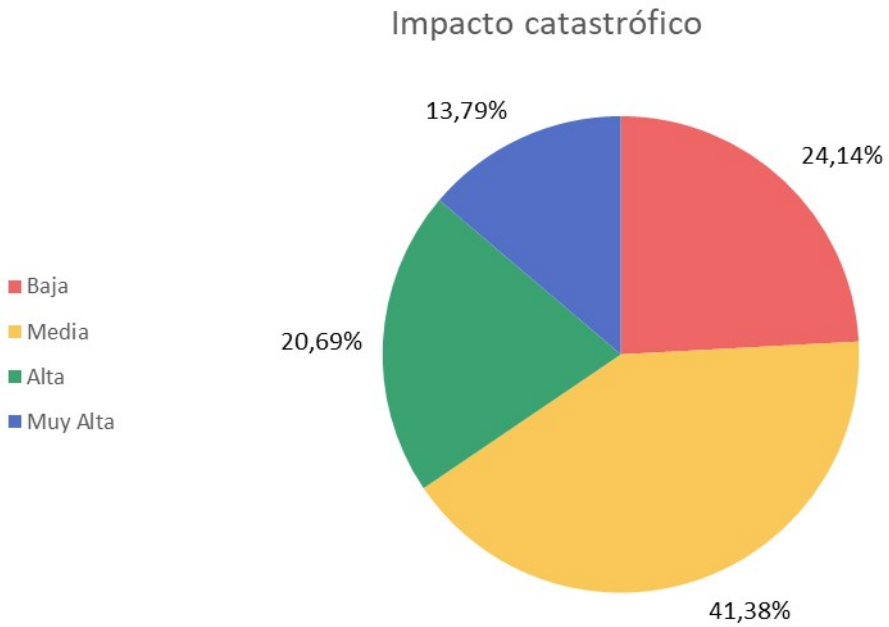


Ilustración 24: Riesgo de ciberinseguridad para impactos catastróficos

El primer dato significativo es que en ninguno de los distintos niveles de impacto se ha valorado como muy baja la probabilidad de ocurrencia. Esto puede tener dos lecturas posibles: un incremento en la percepción de impacto o un incremento en la

probabilidad de ocurrencia. Ambas dan como resultado un incremento del riesgo y de la ciberinseguridad.

Dado que el número de encuestados que completó la parte del cuestionario fue reducido (77), resulta imposible realizar análisis del riesgo de ciberinseguridad por sectores en los que se alcance una representatividad suficiente. No obstante, pueden realizarse estimaciones globales del coste de la ciberinseguridad a partir de la distribución de probabilidades y niveles de impacto.

Asumiendo las equivalencias de daño por nivel de impacto y aplicando las ponderaciones derivadas de las respuestas de esta edición, se estima que:

- Los impactos marginales y moderados suponen aproximadamente un 0,04 % de la cifra de negocio anual.
- Los impactos críticos representarían en torno a un 0,07%.
- Los impactos catastróficos, aunque muy infrecuentes, concentrarían un 0,35% del valor en riesgo.

En conjunto, el coste agregado del ciber-riesgo se estima en torno a un 0,46% de la cifra de negocio anual, lo que, extrapolado al PIB español de 2024 (1,55 billones de euros), equivale a unos 71.300 millones de euros.

Aunque esta cifra puede parecer modesta en términos relativos, resulta ilustrativa al compararla con otros riesgos sistémicos. Por ejemplo, las proyecciones del Fondo Monetario Internacional sitúan la pérdida de PIB per cápita asociada al cambio climático en torno al 0,77% para 2030. Si los impactos catastróficos por ciberincidentes se materializaran en un solo ejercicio, representarían casi la mitad del daño macroeconómico proyectado por el peor escenario climático a medio plazo.

9. Conclusiones

El análisis de la madurez en ciberseguridad que hemos compartido en este informe refleja, desde la perspectiva de quienes lideramos la función, una evolución tangible pero no exenta de retos estructurales. Sin embargo, la foto sectorial sigue mostrando una madurez desigual. Los sectores regulados y críticos —financiero, industrial, infraestructuras— mantienen el liderazgo en la implantación de controles avanzados y en la profesionalización de los equipos, mientras que ámbitos como sanidad, servicios sociales y administración pública siguen arrastrando déficits de inversión, escasez de talento especializado y dificultades para consolidar procesos robustos y sostenibles. Esta brecha, lejos de cerrarse, se amplía en la medida en que la sofisticación de las amenazas y la presión regulatoria aumentan.

En la práctica, la tendencia a la reducción de equipos internos y la externalización de servicios de ciberseguridad es ya una realidad consolidada. La automatización, el uso de plataformas SOAR y la especialización de proveedores permiten ganar eficiencia operativa, pero también introducen nuevos riesgos asociados a la dependencia de terceros y a la gestión de la cadena de suministro. La gestión del talento sigue siendo un reto: la rotación, la escasez de perfiles senior y la presión por mantener la formación continua obligan a repensar los modelos de retención y desarrollo profesional.

El análisis de riesgos confirma lo que muchos CISOs ya intuimos: los incidentes de bajo y medio impacto son recurrentes y suponen un coste agregado relevante, aunque los incidentes críticos y catastróficos se mantienen en niveles de probabilidad controlados gracias a las salvaguardas desplegadas. No obstante, la percepción de riesgo residual sigue creciendo, impulsada por la hiperconectividad, la exposición a terceros y la velocidad de adopción de nuevas tecnologías.

En definitiva, el sector avanza hacia una madurez creciente, pero la resiliencia real dependerá de nuestra capacidad para consolidar la gobernanza, profesionalizar los equipos, invertir en automatización y fortalecer la colaboración sectorial. El reto inmediato es cerrar la brecha entre sectores, anticipar los riesgos emergentes y

mantener la ciberseguridad como un habilitador estratégico, no solo como un centro de coste. La agenda del CISO para los próximos años pasa por ser parte de una transformación segura, con visión de negocio y capacidad de influencia en el comité de dirección.

VI INDICADOR DE MADUREZ EN CIBERSEGURIDAD

Observatorio de la ciberseguridad

Una iniciativa de:

CSC CYBER SECURITY CENTRE

isms forum