V Indicador de madurez en ciberseguridad

OBSERVATORIO DE LA CIBERSEGURIDAD

isms forum
INTERNATIONAL INFORMATION SECURITY COMMUNITY

V Indicador de madurez en ciberseguridad

OBSERVATORIO DE LA CIBERSEGURIDAD

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

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 define 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 sigue siendo el pilar fundamental sobre el que ISMS Forum presenta la quinta 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.

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.

Evaluación de madurez y análisis de riesgos específicos

El estudio de ISMS Forum también incorpora preguntas que varían anualmente y están diseñadas para captar la incidencia de eventos contextuales, como condiciones geopolíticas, macroeconómicas o innovaciones tecnológicas recientes. Además, se incluye una matriz de evaluación del nivel de impacto y probabilidad de ocurrencia, la cual permite a las organizaciones determinar el riesgo residual —o ciberinseguridad— que están asumiendo. Esta matriz complementa el indicador de madurez al ofrecer una visión más clara sobre los riesgos reales que enfrentan las organizaciones, proporcionando una herramienta crítica para la toma de decisiones estratégicas en ciberseguridad.

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 2023, 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

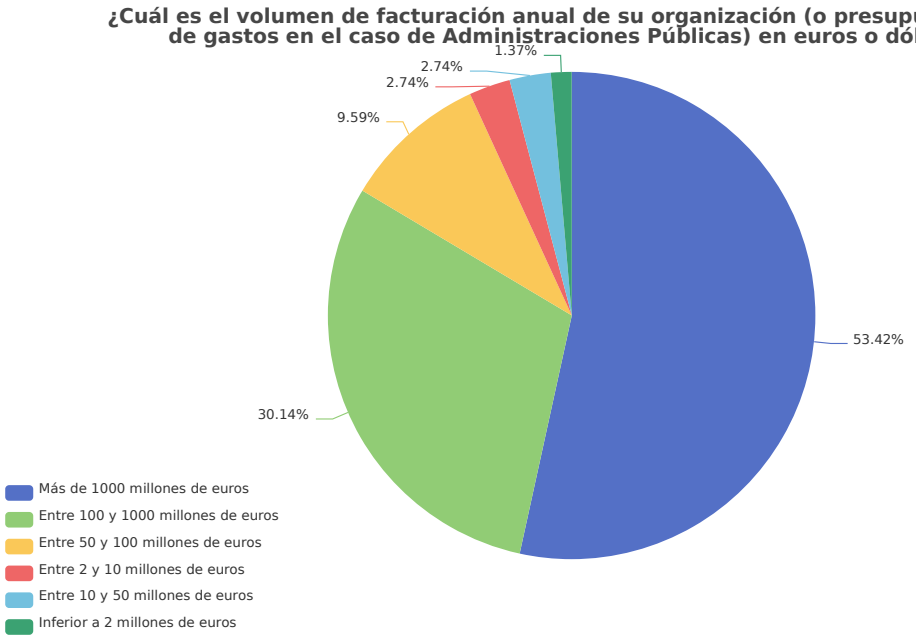


Ilustración 2: Volumen de facturación anual de las empresas participantes

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 mayor parte de las organizaciones (53.42%) tiene un volumen de facturación superior a los 1000 millones de euros, lo cual indica una muestra predominantemente compuesta por empresas grandes o muy grandes. A su vez, el 30.14% de las empresas tienen ingresos entre 100 y 1000 millones de euros. Los restantes segmentos representan valores menores: 9.59% con facturación entre 50 y 100 millones de euros, 2.74% entre 10 y 50 millones, 1.37% entre 2 y 10 millones, y finalmente, solo el 1.37% de las organizaciones tiene un volumen inferior a 2 millones de euros. Esto sugiere que la muestra está principalmente compuesta por grandes corporaciones o entidades con presupuestos significativos.

lustración 3: Puesto de trabajo ocupado por el encuestado.

En la Ilustración 3, se observa el cargo o puesto que ocupan los encuestados dentro de sus organizaciones. La mayoría de los encuestados (86.3%) son directivos o responsables de seguridad de la información, lo que indica que los datos obtenidos provienen de personal con alta responsabilidad en la gestión de la seguridad informática. El resto de los participantes se distribuye entre especialistas en seguridad de la información (5.48%), otros puestos de dirección (5.48%) y, en menor medida, cargos de dirección o responsabilidad de TI (2.74%). Esta distribución sugiere que las respuestas reflejan principalmente la visión de líderes en seguridad dentro de las organizaciones.

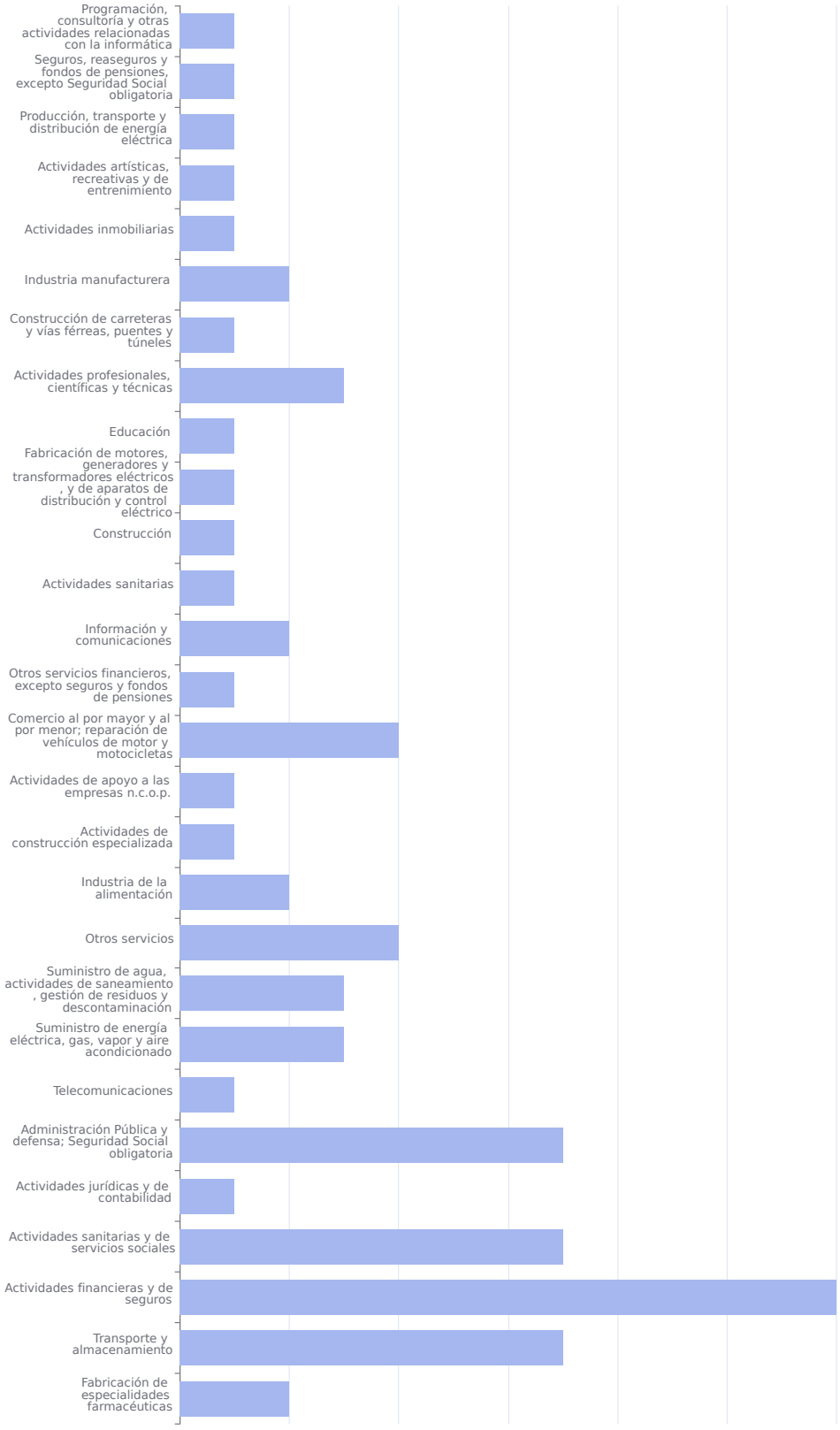


Ilustración 4: Sector de actividad de las empresas participantes.

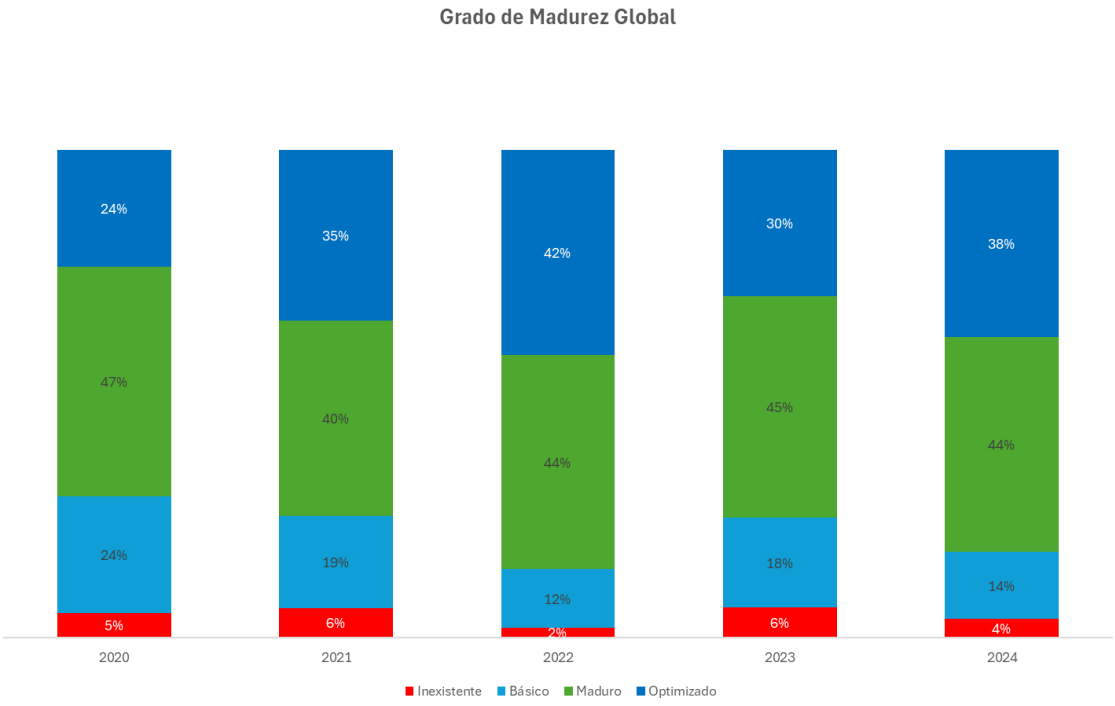
La Ilustración 4 detalla los sectores de actividad de las empresas que participan en el estudio. Los sectores más representados incluyen actividades financieras y de seguros y administración pública y defensa, los cuales concentran una parte significativa de la muestra. Otros sectores importantes son actividades profesionales, científicas y técnicas, así como actividades sanitarias y de servicios sociales. Este amplio rango de sectores indica que la muestra abarca diversas industrias, aunque con un peso considerable de sectores financieros y gubernamentales, lo cual podría influir en las necesidades y desafíos específicos en términos de seguridad de la información.

En resumen, la tipología de la muestra se caracteriza por una predominancia de empresas grandes con alto volumen de facturación, con un enfoque en sectores financieros, gubernamentales y servicios técnicos o científicos. Los encuestados, en su mayoría, son responsables de seguridad de la información, 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

Siguiendo la estructura del NIST Cybersecurity Framework (CSF) 2.0, se ha incorporado el nuevo dominio de Gobierno, que enfatiza la importancia de integrar la ciberseguridad en la gobernanza corporativa de manera estratégica y holística. Esta actualización permite un enfoque más completo sin perder la trazabilidad respecto a años anteriores, ya que CSF 2.0 mantiene la comparabilidad con CSF 1.0 al reorganizar las preguntas sin alterar su esencia. Así, los datos actuales pueden contrastarse con los resultados históricos, facilitando una visión evolutiva de la madurez en ciberseguridad.

En términos generales, los resultados de 2024 muestran una recuperación significativa tras las caídas observadas en 2023. Este año, los niveles optimizados y maduros en los dominios de Identificar, Detectar, Responder, Recuperar y el nuevo dominio Gobierno han alcanzado o incluso superado los valores de 2020, destacando el esfuerzo de las organizaciones para fortalecer sus capacidades. A nivel global, 2024 se posiciona como un año de avance, recuperando y mejorando la madurez en áreas clave de ciberseguridad, en contraste con las limitaciones que se reflejaron el año anterior.



6.1. Dominio 1: Identificar

A lo largo de estos cinco años, el dominio de Identificar ha mostrado una tendencia general de mejora en la gestión de recursos y en los procedimientos de respuesta ante incidentes. Sin embargo, en el aspecto crítico de la Identificación y Documentación de Vulnerabilidades y Amenazas, la regresión en los niveles de madurez sugiere la necesidad de una mayor atención y refuerzo. Este retroceso indica que algunas organizaciones pueden estar experimentando dificultades para mantener el ritmo de los avances necesarios en ciberseguridad, subrayando la importancia de continuar impulsando prácticas sólidas y sostenibles que permitan afrontar los riesgos de forma proactiva y resiliente.

El inventario y la gestión de dispositivos, sistemas, aplicaciones y recursos de información han mostrado una mejora notable en los últimos cinco años. En 2024, el 40% de las organizaciones se encuentran en un nivel maduro y el 33% en un nivel optimizado, lo que refleja una consolidación en este aspecto. Comparativamente, en 2020, solo el 28% estaba en un nivel maduro y el 33% en un nivel optimizado. También se ha reducido la categoría “Inexistente” del 7% en 2020 al 0% en 2024, lo que indica que prácticamente todas las organizaciones han establecido algún nivel de inventario y gestión de sus recursos de ciberseguridad.

En cuanto a los procedimientos de respuesta ante incidentes, también se observa una evolución positiva. En 2024, el 59% de las organizaciones se encuentran en un nivel maduro y el 22% en un nivel optimizado. Esto representa un avance considerable respecto a 2020, cuando solo el 48% estaba en nivel maduro y el 13% en nivel optimizado. La disminución en la categoría “Inexistente”, del 7% en 2020 al 1% en 2024, sugiere que más organizaciones están documentando, actualizando y probando regularmente sus procedimientos de respuesta ante incidentes.

La madurez en la Identificación y Documentación de Vulnerabilidades y Amenazas mostró una tendencia muy positiva hasta 2022. Durante ese período, el porcentaje de organizaciones en un nivel optimizado creció de forma constante, alcanzando su punto máximo en 2022 con un 67%. Sin embargo, a partir de ese año se ha producido un retroceso, y en 2024 los valores han vuelto a niveles similares a los de 2020, con un 47% en nivel optimizado y un 36% en nivel maduro. Además, el porcentaje de organizaciones en la categoría “Inexistente” ha vuelto a aumentar ligeramente, situándose nuevamente en un 4%, el mismo valor registrado en 2020. Este retroceso podría estar vinculado a varios factores, como el aumento en la complejidad de las amenazas y la necesidad de recursos especializados para gestionar adecuadamente las vulnerabilidades. También podría reflejar dificultades en la adaptación de algunas organizaciones a las exigencias de una gestión de riesgos más avanzada y en constante evolución. Esta vuelta a valores de 2020 en

un área tan crítica implica que algunas organizaciones han encontrado obstáculos para mantener la madurez alcanzada en años anteriores, lo que supone una vulnerabilidad potencial frente a ciberamenazas.

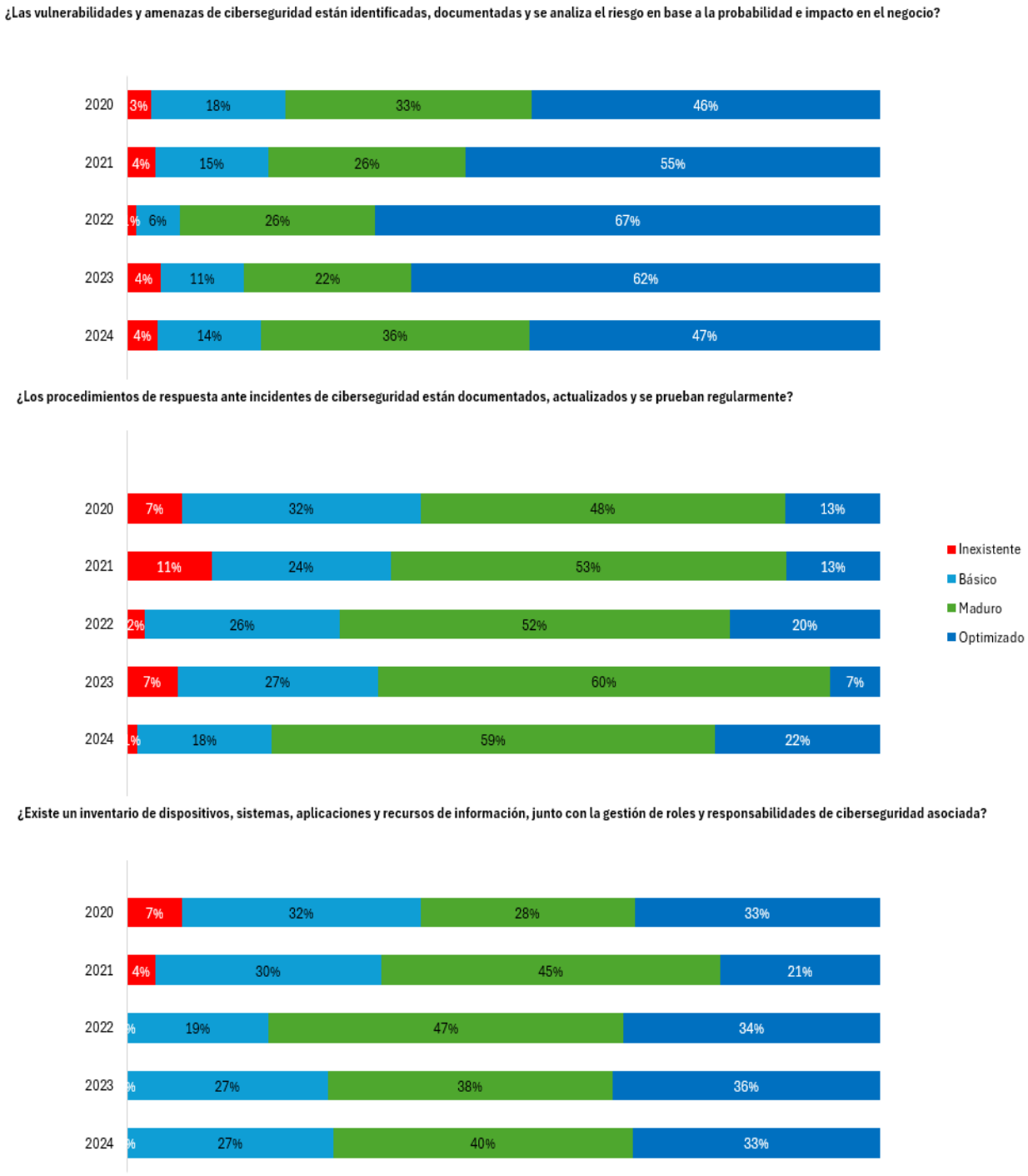


Ilustración 5: Evolución de la tendencia del domino Identificar

Al igual que en el estudio de 2023, las respuestas muestran una **gran variabilidad** en el dominio Identificar (entre 3 y 9), lo que demuestra las enormes diferencias en el grado de implementación de controles cuyo objetivo de la identificación de los riesgos ciber.

En cuanto a la media, en 2024 se establece entorno al 6, lo que se interpreta como que existe un **nivel medio de madurez** en los diferentes sectores, manteniéndose dicho nivel medio estable en relación con los resultados del 2023.

Si tomamos en consideración el tamaño de la muestra, el sector con un mayor índice de madurez es el de **Información y comunicaciones,** que permanece como uno de los sectores líderes al igual que ocurrió en el estudio del año pasado. **Inconsistencia en sectores:** el indicador muestra grandes **inconsistencias en los sectores** de actividades financieras y seguros; actividades sanitarias y de servicios sociales; transporte y almacenamiento y Administración Pública y defensa, lo que indica que existen organizaciones en los citados sectores que tienen alto margen de mejora para alinear su madurez a los de sus respectivos sectores.

Áreas de Mejora: el sector c**on mayor margen de mejora** es el de Fabricación de motores, generadores y transformadores eléctricos, seguido por el sector “otros servicios” que a su vez incluye gran variabilidad en las respuestas, como es normal debido a la naturaleza diversa del mismo.

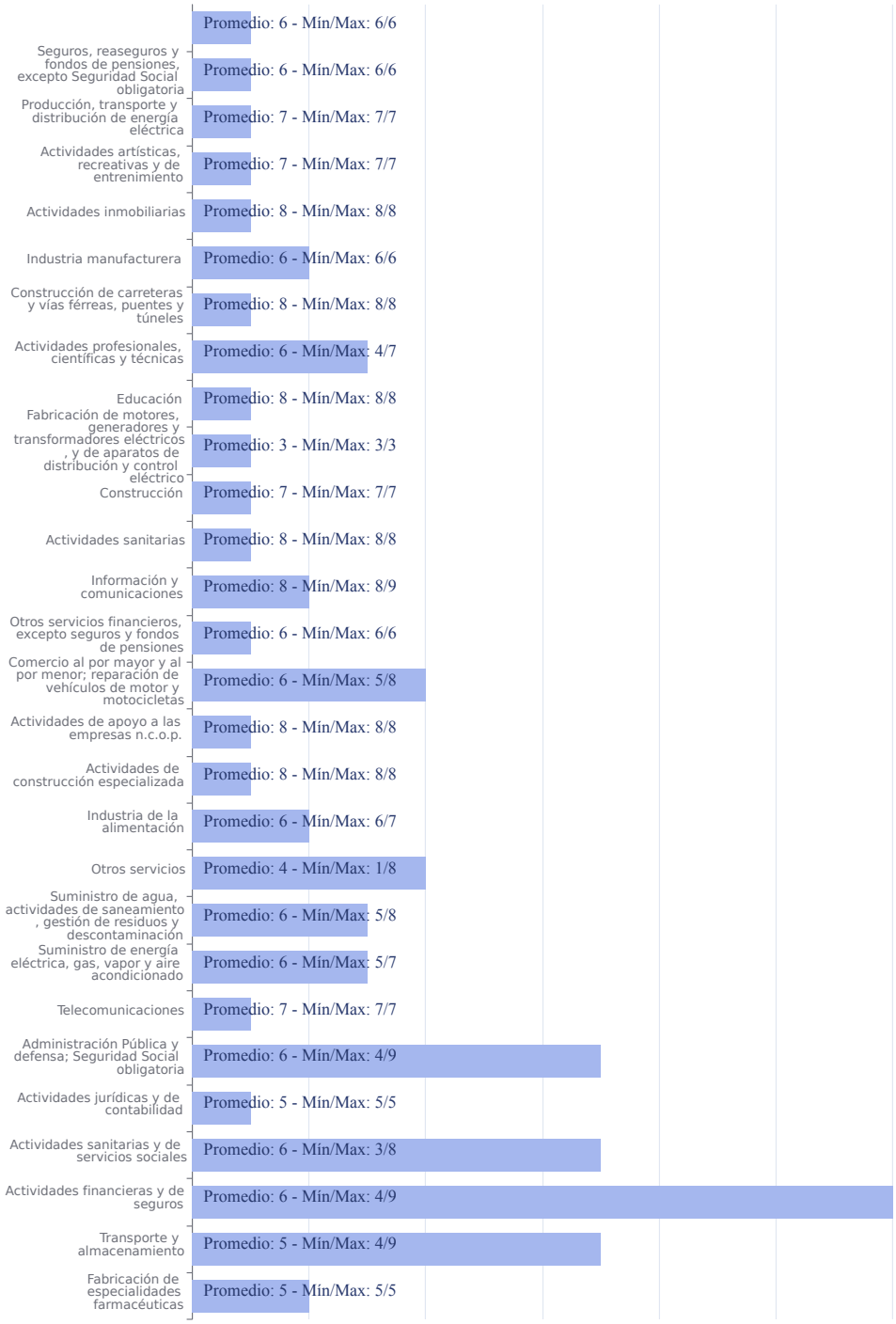


Ilustración 6: Indicador “Identificar” por sector de actividad

6.2. Dominio 2: Proteger

El dominio Identificar ha mostrado en general una tendencia de mejora en los últimos cinco años, con un fortalecimiento notable en la gestión de identidades, la protección de datos y la implementación de medidas de resiliencia técnica. Sin embargo, algunos aspectos, como el mantenimiento de sistemas de control industrial y la gestión del ciclo de vida del dato, presentan variabilidad en los niveles de madurez, con un ligero aumento en las categorías "Inexistente" en 2024. Esto sugiere que, aunque la mayoría de las organizaciones están avanzando en sus prácticas de ciberseguridad, algunas aún enfrentan desafíos específicos en áreas críticas que requieren atención para asegurar una protección uniforme de sus activos e información.

En cuanto a la gestión de identidades y accesos siguiendo el principio de menor privilegio y la segregación de funciones, se observa una tendencia positiva general. En 2024, el 53% de las organizaciones alcanzan un nivel optimizado, lo que representa un incremento desde el 44% de 2020. Además, el porcentaje de "Inexistente" ha disminuido a cero desde 2021, lo que indica que todas las organizaciones han implementado algún nivel de control en este aspecto. La estabilidad en los niveles "Maduro" y "Optimizado" en los últimos años muestra un esfuerzo consistente en consolidar prácticas de control de acceso.

La formación y concienciación de empleados en ciberseguridad ha mostrado mejoras significativas. En 2024, el 48% de las organizaciones se encuentran en un nivel optimizado, y el 42% en un nivel maduro, en comparación con el 26% y 38% respectivamente en 2020. Sin embargo, ha surgido un leve incremento en la categoría “Inexistente” en 2024 (1%), lo que podría indicar que algunas organizaciones nuevas o con menor madurez han sido incluidas en el análisis. En general, el crecimiento en la categoría optimizado desde 2020 refleja un compromiso creciente con la formación continua y la concienciación del personal en temas de ciberseguridad.

En la gestión del ciclo de vida del dato, los resultados han sido variables. En 2024, el 42% de las organizaciones alcanzan el nivel optimizado, y el 48% están en un nivel maduro. Sin embargo, esto representa una disminución en el nivel maduro respecto al pico alcanzado en 2023 (64%). La categoría “Inexistente” se ha mantenido estable en 7% desde 2023, lo que indica una ligera persistencia de organizaciones que aún no implementan esta gestión. La variabilidad en los niveles de madurez refleja fluctuaciones en la capacidad de algunas organizaciones para mantener prácticas consistentes de protección de datos.

La protección de sistemas y activos de información ha mejorado, con un notable incremento en los niveles de madurez. En 2024, el 41% de las organizaciones están en un nivel optimizado, comparado con solo el 23% en 2020. El porcentaje en la categoría "Básico" ha disminuido del 29% en 2023 al 15% en 2024, lo que sugiere una evolución hacia prácticas más avanzadas. Esta mejora puede atribuirse al fortalecimiento de políticas y procedimientos de seguridad que han sido implementados de manera más uniforme en las organizaciones.

En el mantenimiento de sistemas de información y control industrial, la madurez ha mostrado una mejora moderada, aunque se observa cierta inestabilidad. En 2024, el 38% de las organizaciones están en un nivel optimizado, pero la categoría "Inexistente" ha aumentado del 13% en 2023 al 14% en 2024. Este incremento en "Inexistente" puede ser una señal de que algunas organizaciones, especialmente aquellas con menos recursos o experiencia en la gestión de control industrial, están teniendo dificultades para implementar un mantenimiento adecuado de sus sistemas de forma controlada. La variabilidad en este aspecto podría indicar un área de riesgo que requiere atención.

La implementación de medidas técnicas de seguridad ha progresado con una tendencia positiva. En 2024, el 38% de las organizaciones alcanzan el nivel optimizado y el 51% están en un nivel maduro, una mejora respecto al 19% optimizado en 2020. La disminución en la categoría "Básico", de 18% en 2023 a 10% en 2024, sugiere que cada vez más organizaciones están mejorando sus controles técnicos. Sin embargo, el ligero aumento de la categoría "Inexistente" en 2024 (1%) podría señalar desafíos en la implementación de medidas técnicas en ciertas organizaciones con menos madurez.

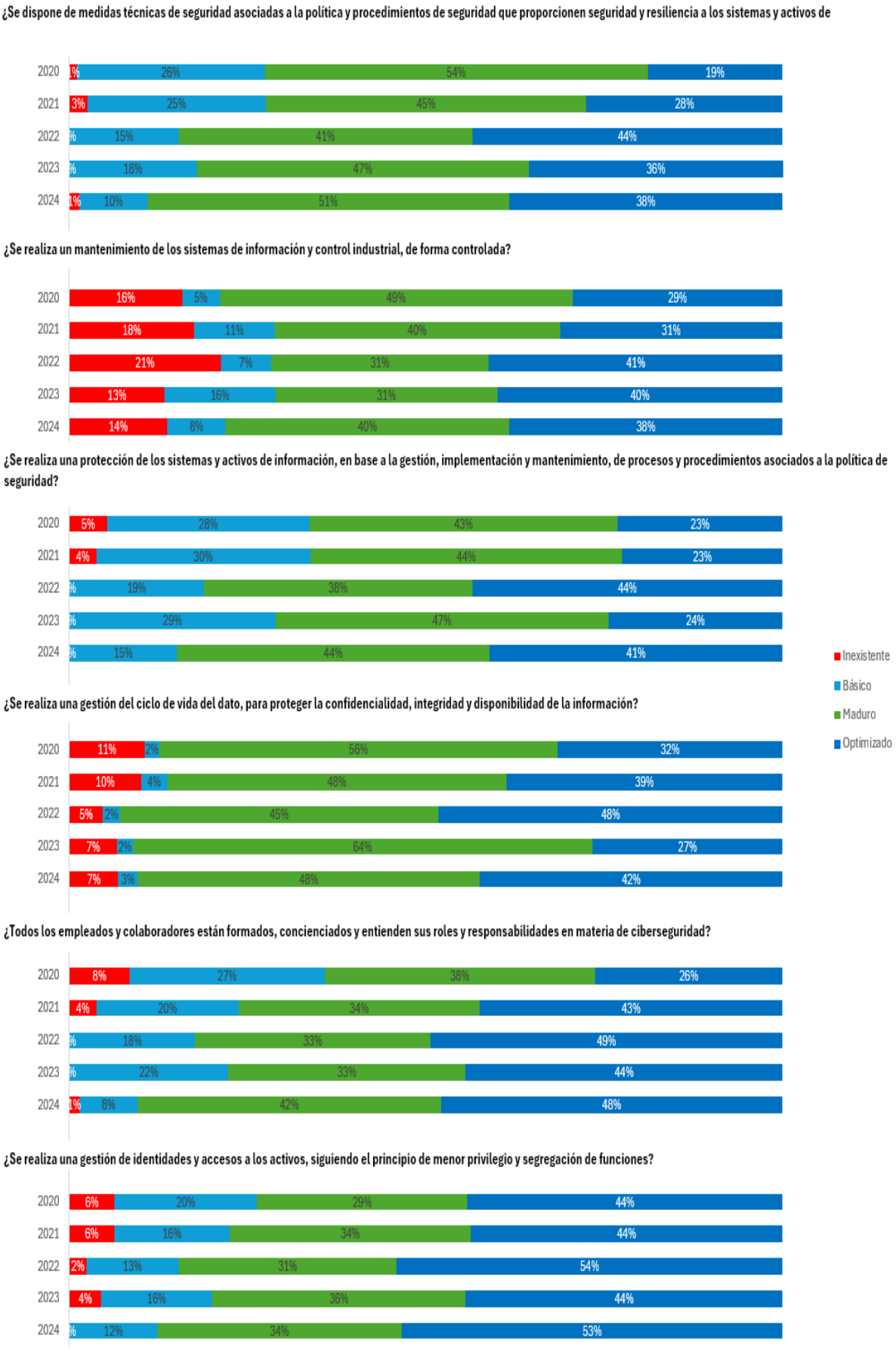


Ilustración 7: Evolución de la tendencia del domino Proteger

La media de las respuestas del dominio proteger es entorno al 14, lo que, además de suponer un avance con respecto al 2023, 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 Actividades profesionales, científicas y técnicas; Información y comunicaciones y Suministro de agua, actividades de saneamiento, gestión de residuos y descontaminación, siendo el sector del suministro de agua el único que sigue destacando con respecto al estudio de 2023.

Inconsistencia en sectores: el indicador muestra grandes inconsistencias en los sectores de Actividades financieras y de seguros; Actividades sanitarias y de servicios sociales; Administración Pública y defensa, Comercio al por mayor y al por menor y Suministro de energía eléctrica, gas, vapor y aire acondicionado, lo que coincide en al menos dos sectores con el dominio identificar, evidenciando otra vez las potenciales mejoras a implantar en las organizaciones de los citados sectores con una madurez más baja que el resto.

Áreas de Mejora: el sector con **mayor margen de mejora** es el de Fabricación de motores, generadores y transformadores eléctricos, seguido por el Otros servicios financieros, excepto seguros y fondos de pensiones

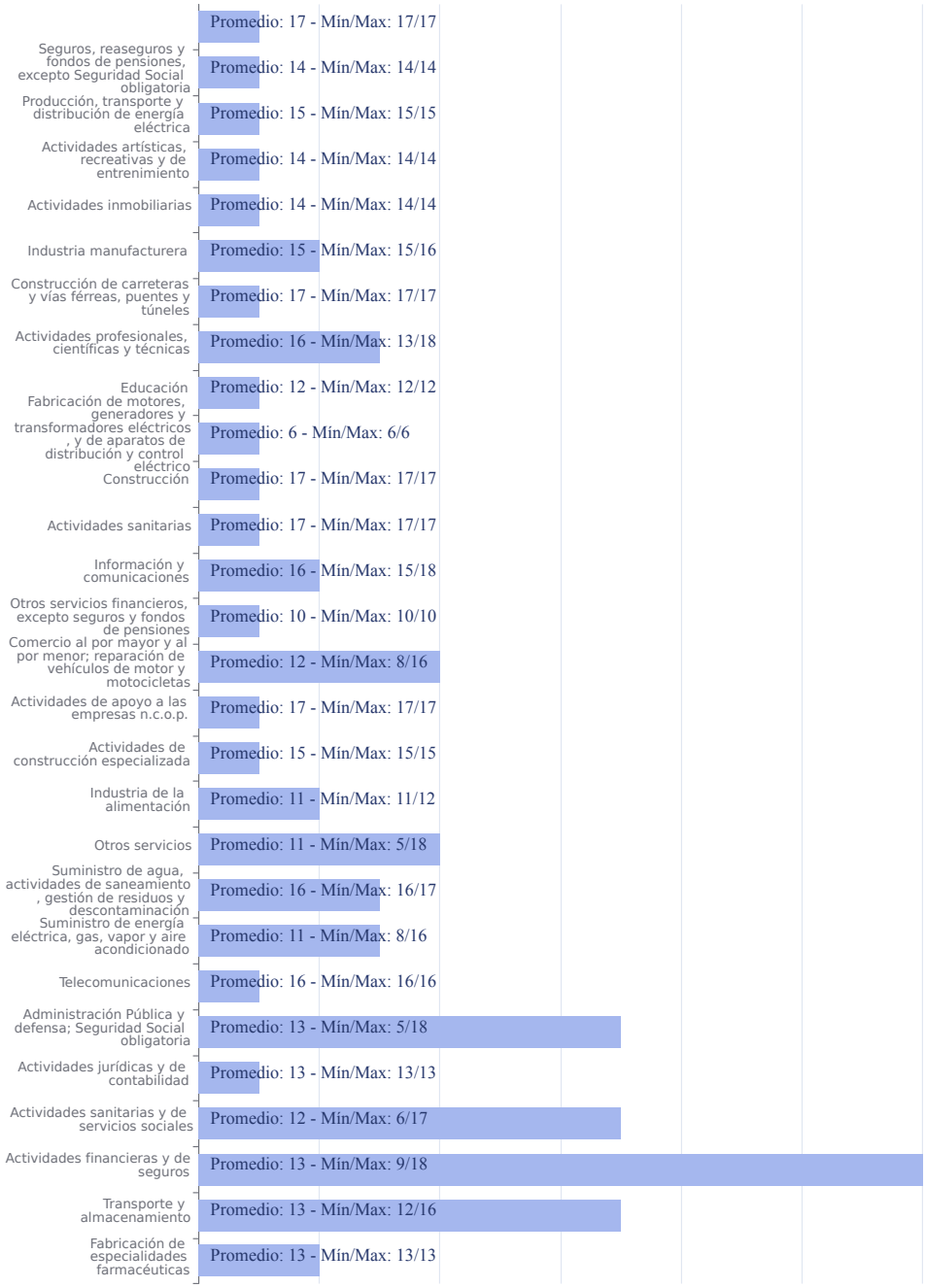


Ilustración 8: Indicador "Proteger" por sector de actividad

6.3. Dominio 3: Detectar

En 2024, el dominio Detectar muestra una notable recuperación y consolidación en varios aspectos críticos de la capacidad de detección de eventos y actividades anómalas. Sin embargo, este repunte positivo contrasta con las caídas generalizadas que se observaron en 2023, lo que aporta un contexto importante sobre el esfuerzo de las organizaciones para restablecer y mejorar sus capacidades de detección.

La disponibilidad de sistemas para la recolección de eventos ha mostrado una clara tendencia de mejora a lo largo de los años a excepción de 2023. En 2020, solo el 26% de las organizaciones se encontraban en un nivel optimizado, mientras que en 2024 este porcentaje ha aumentado hasta el 42%, lo cual es un incremento notable respecto al 18% de 2023. La categoría “Inexistente” también ha disminuido significativamente, rompiendo la tendencia de subida anual desde 2020 para mostrar el valor más bajo en los 5 años (1%). Este cambio sugiere una mayor adopción y madurez en el uso de herramientas de recolección de eventos, lo que refleja un fortalecimiento en la capacidad de detección de incidentes de ciberseguridad.

El análisis para la detección de actividad anómala ha experimentado un crecimiento en el nivel de madurez de las organizaciones. En 2020, solo el 41% de las organizaciones estaban en un nivel optimizado, y este porcentaje ha aumentado hasta el 60% en 2024, frente al 58% en 2023 y el punto máximo de 68% en 2022. Al mismo tiempo, la categoría "Inexistente" ha disminuido del 5% en 2020 al 3% en 2024. En general, el crecimiento en la madurez sugiere una mejora continua en la capacidad de las organizaciones para detectar comportamientos sospechosos de manera proactiva.

La capacidad de monitorización de la actividad de usuarios y proveedores ha experimentado una recuperación en 2024, alcanzando un 51% en el nivel optimizado, comparado con el 44% en 2023. La caída de 2023, en la que el nivel optimizado disminuyó desde un 54% en 2022, sugiere que algunas organizaciones enfrentaron dificultades en la implementación o mantenimiento de herramientas de monitorización avanzado. El rebote en 2024 indica que estas organizaciones han podido restablecer o mejorar sus capacidades de monitorización. Además, la categoría "Inexistente" ha reducido del 7% en 2020 al 1% en 2024, mostrando que prácticamente todas las organizaciones cuentan ahora con algún nivel de monitorización. Este avance en la optimización de la monitorización de usuarios indica una mayor adopción de prácticas de supervisión que ayudan a detectar eventos de ciberseguridad y minimizar riesgos.

La definición y actualización de procedimientos de detección de incidentes ha mostrado un progreso constante. En 2020, solo el 16% de las organizaciones estaban en el nivel optimizado, y en 2024, el 21% de las organizaciones alcanzan un nivel optimizado, superando el 11% de 2023. Este incremento muestra un avance hacia la madurez en la gestión de procedimientos de detección, incluyendo la actualización y prueba regular de los procesos de detección de incidentes. También se ha incrementado la categoría "Maduro", pasando del 48% en 2020 al 64% en 2024, lo que indica una mejora en la formalización de estos procedimientos. Aun así, la categoría "Inexistente" no ha desaparecido completamente y se sitúa en un 3% en 2024.

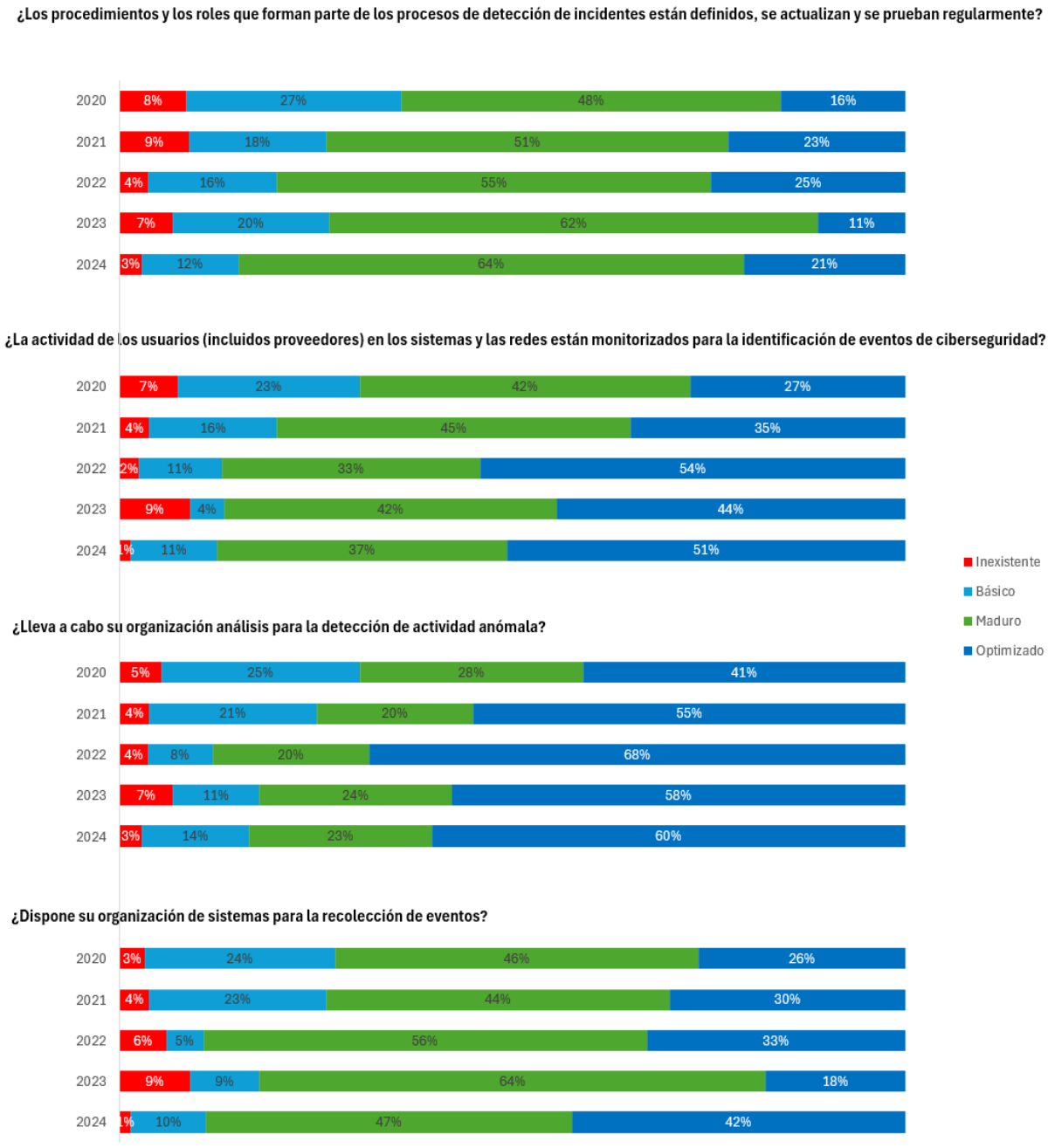


Ilustración 9: Evolución de la tendencia del domino Detectar

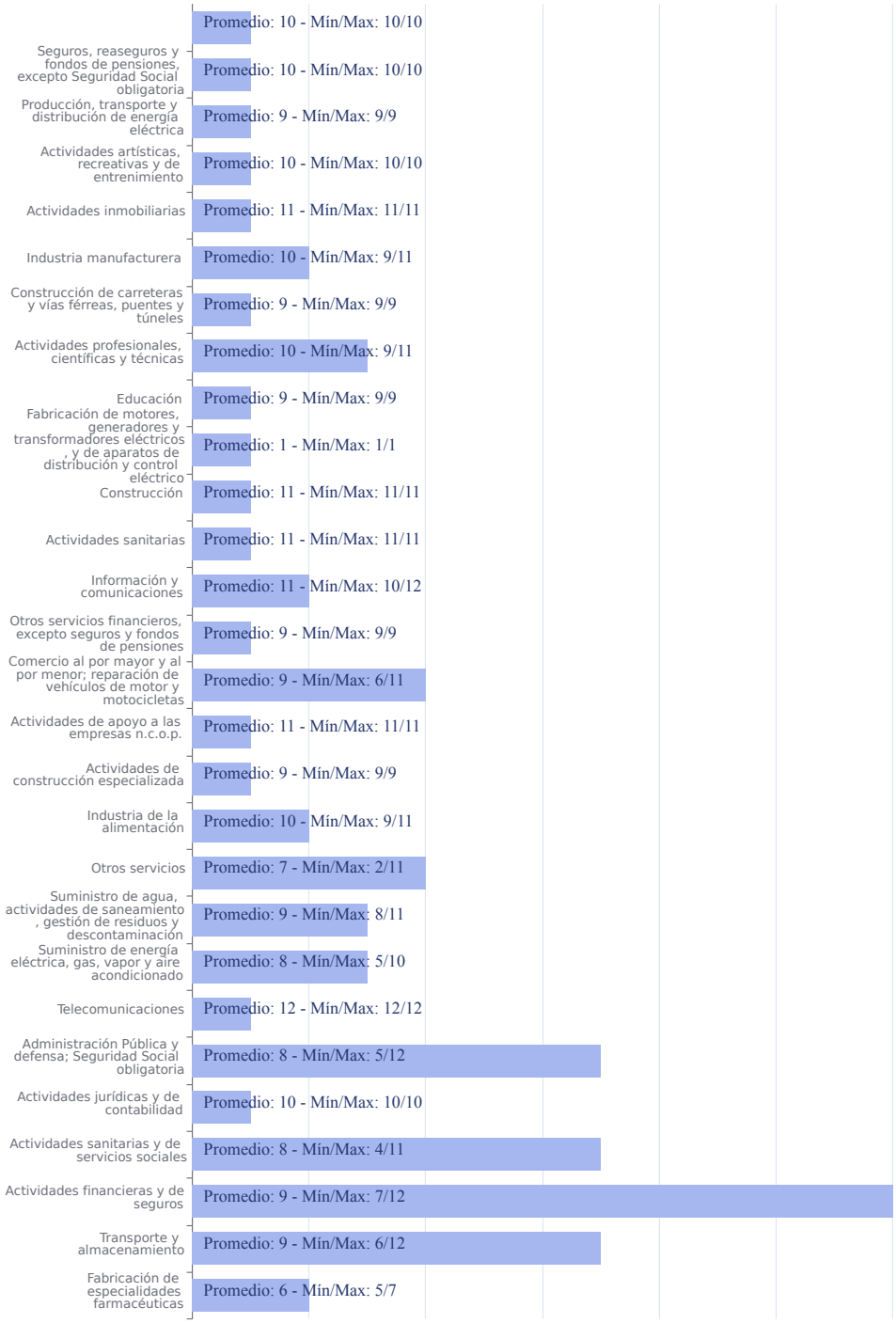


Ilustración 10: Indicador "Detectar" por sector de actividad

Del dominio **DETECTAR**, que se centra en la monitorización de actividad de usuarios, detección de incidentes, el análisis para la detección de actividad anómala y la disponibilidad de sistemas para la recolección de eventos, podemos hacer las siguientes observaciones.

El promedio general para **DETECTAR** es de aproximadamente **9**, un punto por encima respecto al año anterior. Esto indica un **nivel de madurez**

medio/alto en las prácticas de detección de incidentes y eventos de ciberseguridad.

El sector de “Actividades inmobiliarias” al igual que en 2023, vuelve a ser un sector con uno de los promedios más altos. A este se le suman “Telecomunicaciones”, “Construcción”, “Información y comunicaciones”, “Actividades de apoyo a las empresas n.c.o.p.” y “Actividades sanitarias”, como los sectores con promedios más altos, indicando unas **prácticas de detección considerablemente fuertes**.

Inconsistencia en Sectores: El indicador muestra que existe una **gran inconsistencia y variabilidad en los resultados** en sectores como “Actividades sanitarias y de servicios sociales” y “Otros servicios”, demostrando la gran diferencia en el grado de madurez de monitorización, detección y análisis de incidencias dentro de empresas de un mismo sector y evidenciando las potenciales mejoras a implantar en estas con tal de reducir la diferencia. Para el sector de “Otros servicios” cabe destacar que la variabilidad se debe a que en él se agrupan los distintos tipos de organizaciones que no están representadas por el resto de los sectores listados.

Áreas de Mejora: El sector “Fabricación de motores, generadores y transformadores eléctricos y de aparatos de distribución y control eléctrico” es el que menor madurez presenta, así como los sectores de “Fabricación de especialidades farmacéuticas” y “Otros Servicios”, que también muestran un promedio más bajo, dando a entender que podría haber **oportunidades de mejora significativas en la detección de incidentes** para estos sectores.

6.4. Dominio 4: Responder

En 2024, el dominio Responder muestra una recuperación significativa respecto a 2023 en todas las áreas analizadas, alcanzando mayores niveles de madurez y optimización en los procesos de respuesta y mejora continua. La recuperación en 2024 es particularmente notable en aspectos como la investigación de alertas, el análisis forense y la identificación temprana de vulnerabilidades.

En 2024, se observa una mejora significativa en la formalización de los procesos de comunicación ante incidentes, alcanzando un 23% en el nivel optimizado, una gran recuperación desde el 9% en 2023. La categoría "Inexistente" también disminuyó al 3% en 2024 desde el 4% en 2023. Este repunte sugiere que las organizaciones han vuelto a priorizar la formalización y el establecimiento de protocolos claros de comunicación interna y externa en la gestión de incidentes, después de una caída en 2023.

La proporción de organizaciones en el nivel optimizado para la investigación de alertas aumentó al 52% en 2024, en comparación con el 47% de 2023, lo cual representa una recuperación importante tras la caída observada en ese año. El nivel "Inexistente" desaparece en 2024, lo que sugiere que casi todas las organizaciones tienen algún grado de proceso de investigación de alertas en marcha.

La capacidad para realizar análisis forenses ha mostrado fluctuaciones desde 2020. En ese año, solo el 23% de las organizaciones estaban en el nivel optimizado, y esta cifra aumentó a 32% en 2022. Sin embargo, 2023 mostró una disminución al 24% en el nivel optimizado. En 2024, esta cifra se recuperó hasta alcanzar el 37%, lo que sugiere una reactivación de los esfuerzos en análisis detallado post-incidente. La reducción continua de la categoría "Inexistente" de 16% en 2020 a 7% en 2024 muestra que cada vez más organizaciones están avanzando en la implementación de análisis forense.

Desde 2020, este aspecto ha mostrado una tendencia positiva en la madurez de las prácticas de mitigación y contención. En 2020, solo el 19% de las organizaciones estaban en el nivel optimizado. Esta cifra creció al 21% en 2022, pero en 2023 cayó al 11%. En 2024, el nivel optimizado se recupera al

23%, reflejando una mayor capacidad para la identificación temprana y contención de amenazas.

La implementación de procesos formales de mejora continua en la respuesta a incidentes ha mostrado una tendencia de crecimiento desde 2020, cuando únicamente el 8% de las organizaciones estaban en el nivel optimizado. Este porcentaje aumentó gradualmente hasta alcanzar el 12% en 2022. Sin embargo, 2023 fue un año de retroceso, ya que el nivel optimizado se redujo al 11% y la categoría "Inexistente" aumentó al 13%. En 2024, se observó una recuperación con un 18% de las organizaciones alcanzando el nivel optimizado, indicando que las organizaciones han vuelto a fortalecer sus procesos de aprendizaje y mejora tras incidentes.

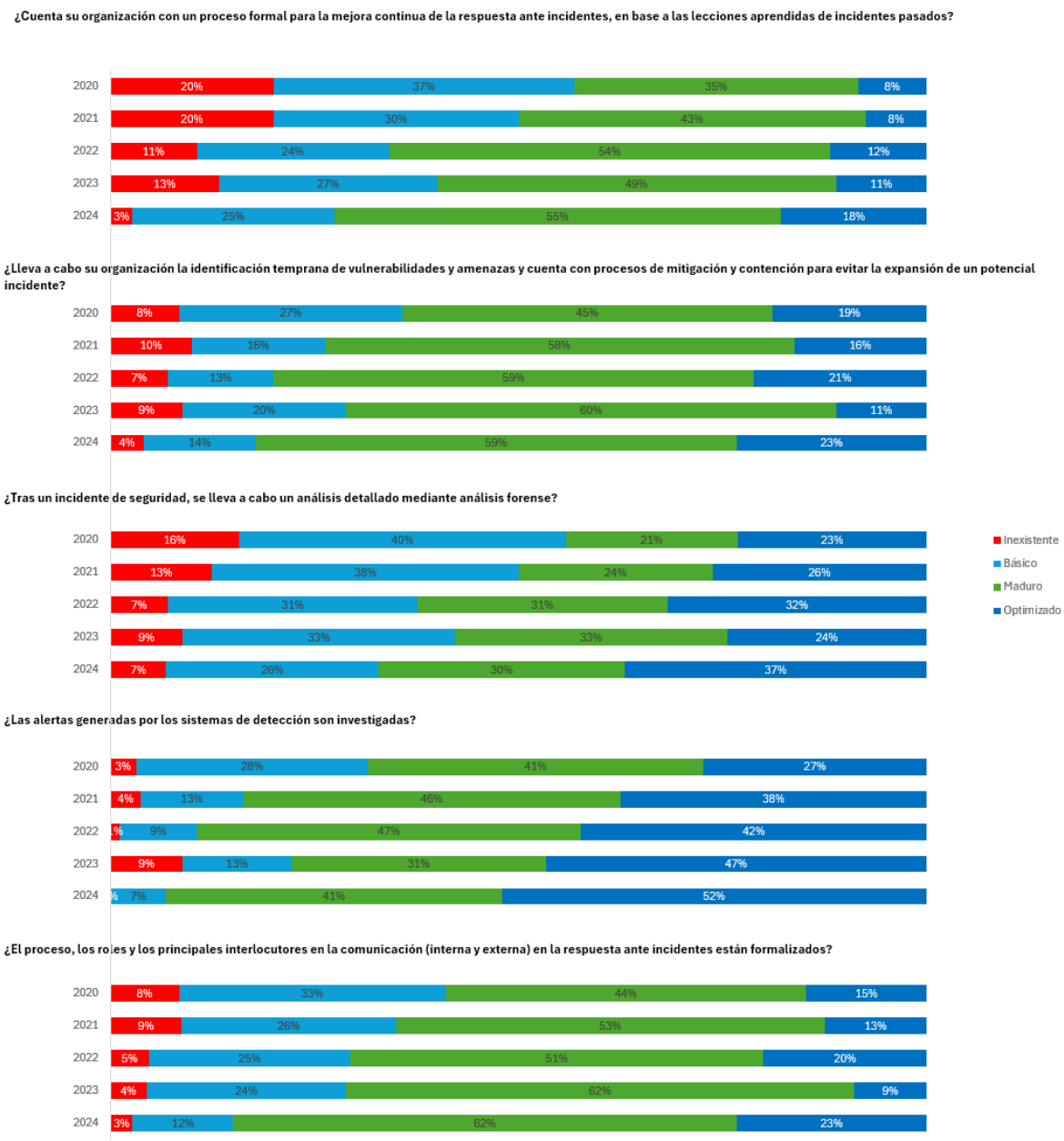


Ilustración 11: Evolución de la tendencia del domino Responder

A continuación, analizamos los datos del dominio **RESPONDER**, centrándonos en la mejora continua de la respuesta ante incidentes, la identificación temprana de vulnerabilidades y amenazas, análisis forense, investigación de alertas, formalización de procesos y comunicación en la respuesta ante incidentes, y la documentación y prueba regular de procedimientos.

El **promedio general** para RESPONDER es de aproximadamente 10. Esto sugiere un nivel medio alto de madurez en las prácticas de respuesta ante incidentes. Sectores como “Información y comunicaciones”, “Actividades artísticas, recreativas y entretenimiento”, “Educación” y “Actividades de apoyo a las empresas n.c.o.p., y de construcción especializada” destacan

con promedios más altos (mayores de 12) indicando prácticas de respuesta relativamente fuertes, y **probablemente** algunas de ellas, **fortalecidas por lecciones aprendidas** de varios incidentes sufridos en sus sectores de actividad**. Especial mención al sector de Educación,** siendo el que más mejora ha mostrado respecto al año anterior.

Consistencia en Muchos Sectores, desde Construcción y manufacturera, pasando por actividades profesionales o sanitarias, hasta suministros o telecomunicaciones. Todas ellas muestran consistencia **con resultados por encima del promedio** de todos los sectores (entre 11 y 12).

Enfoque Específico en "Fabricación de Productos Farmacéuticos", con un **promedio relativamente bajo**, si bien muestra mejoría respecto al año anterior (7 vs 4), **y una nueva industria representada** en la muestra de esta edición, “Fabricación de motores, generadores y transformadores eléctricos , y de aparatos de distribución y control eléctrico” con amplio margen de mejora y atención específica en sus prácticas de respuesta ante incidentes.

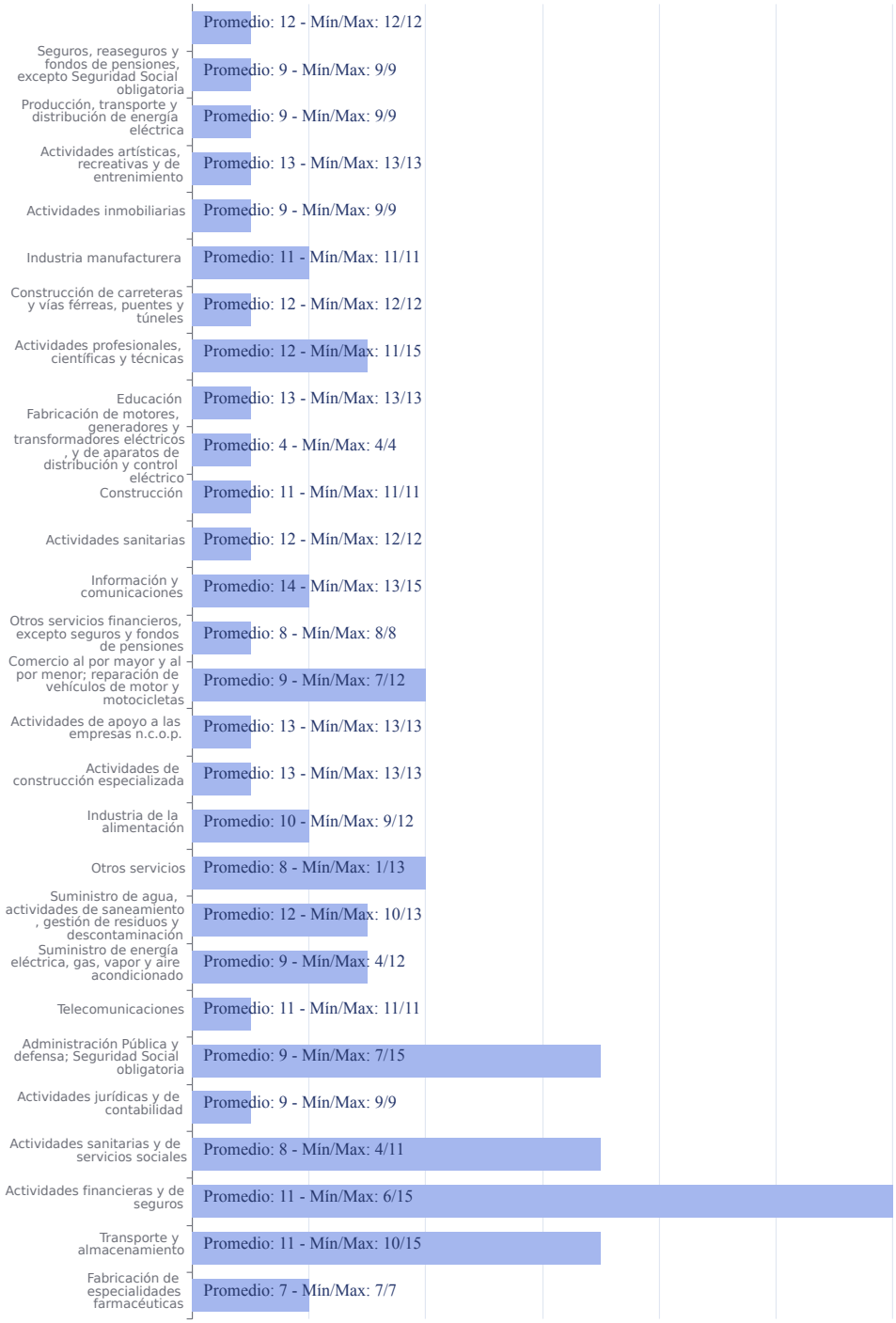


Ilustración 12: Indicador "Responder" por sector de actividad

6.5. Dominio 5: Recuperar

Desde 2020, el dominio Recuperar ha mostrado una tendencia de mejora gradual en la formalización y actualización de los planes de recuperación y en la definición de actividades y roles de comunicación durante estos procesos. Sin embargo, 2023 fue un año de retroceso, donde se observó una caída significativa en los niveles optimizados y un incremento en las categorías más bajas. En 2024, este dominio ha experimentado una notable recuperación, con un aumento en los niveles de madurez y optimización en todos los aspectos evaluados.

En 2024, se observa una mejora significativa en la formalización y prueba regular de los planes de recuperación, con el 12% de las organizaciones alcanzando el nivel optimizado, una notable recuperación desde el 2% en 2023. Además, el nivel maduro también aumentó al 62% en 2024. Comparativamente, en 2020, solo el 9% de las organizaciones estaban en el nivel optimizado, y un 40% en maduro, lo que muestra una tendencia de crecimiento en la madurez de estos planes a lo largo de los años.

La capacidad de actualizar proactivamente los planes de recuperación muestra una recuperación en 2024, con un 12% de las organizaciones en el nivel optimizado y un 63% en maduro, después de haber caído a solo un 2% en optimizado en 2023. En 2020, este aspecto tenía un 11% en optimizado y un 45% en maduro, con un aumento gradual hasta 2022, donde alcanzó un nivel máximo de madurez en el 61%.

En cuanto a la definición de actividades y roles de comunicación durante el proceso de recuperación, el nivel optimizado creció al 30% en 2024, mejorando desde el 22% en 2023. Este aspecto también muestra una tendencia de mejora a lo largo de los años, con solo un 19% en el nivel optimizado en 2020.

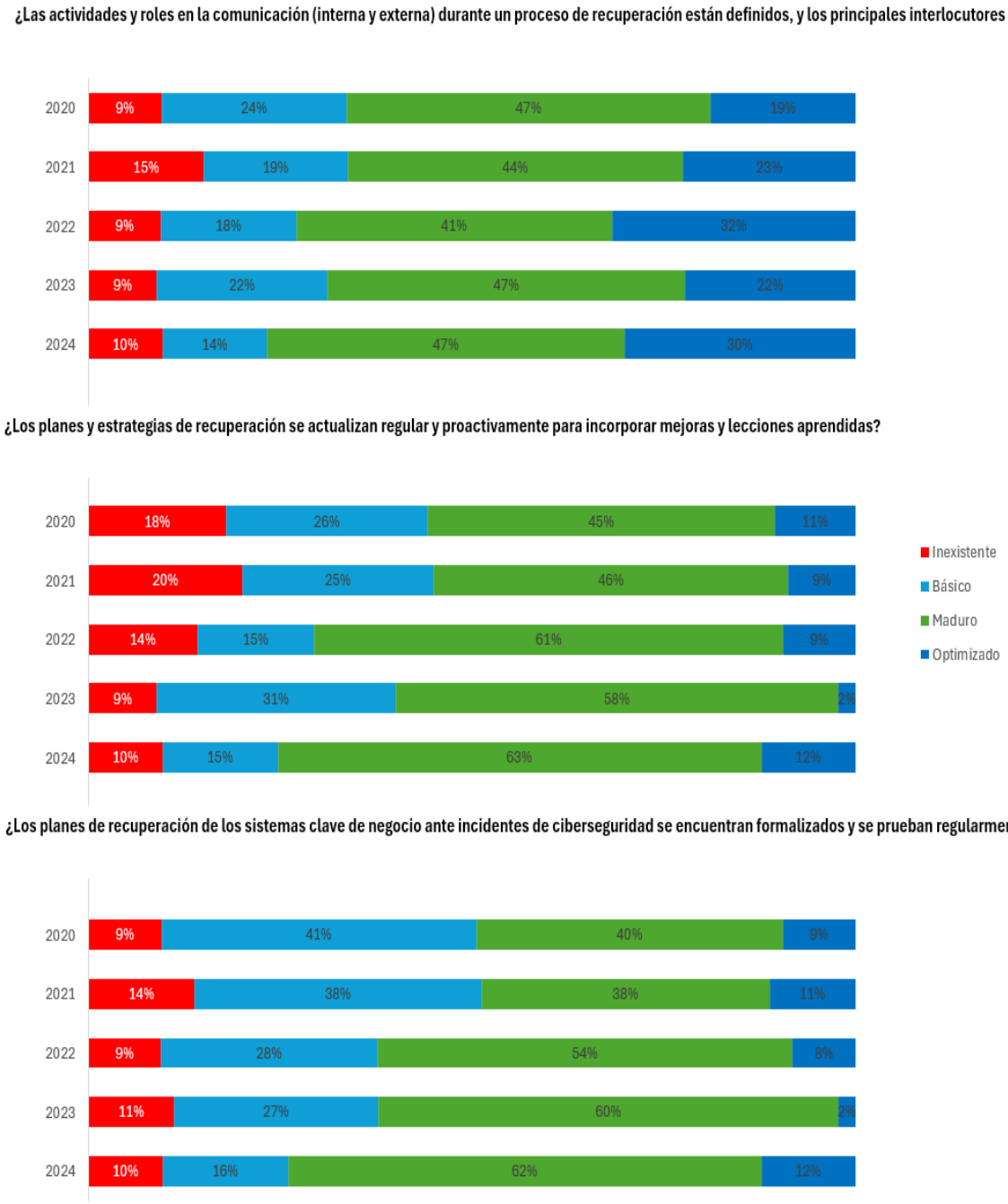


Ilustración 13: Evolución de la tendencia del domino Recuperar

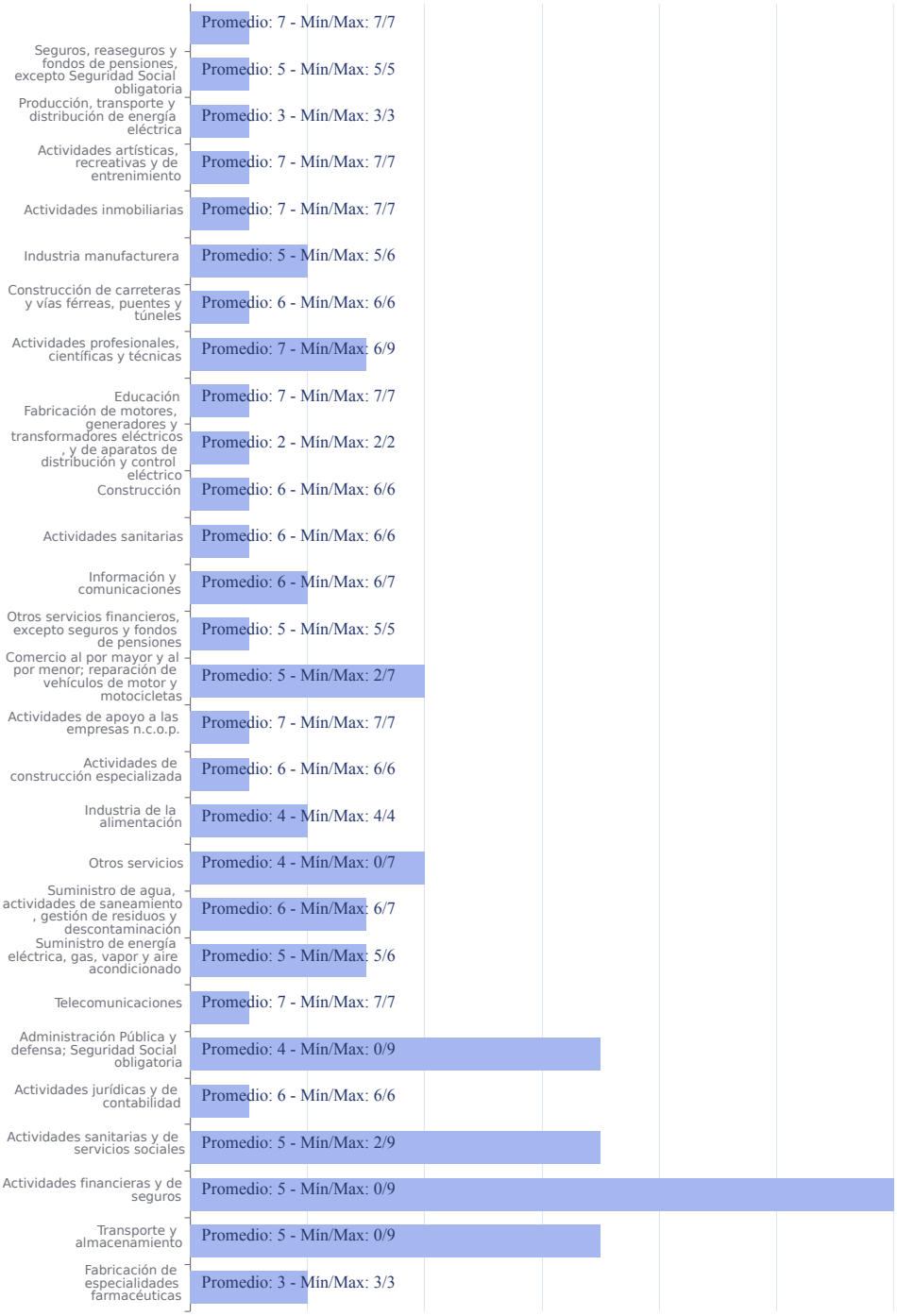
Vamos a analizar los datos en el contexto del dominio ***RECUPERAR***, centrándonos en las actividades y roles en la comunicación durante el proceso de recuperación, la actualización proactiva de planes y estrategias, y la formalización y prueba regular de los planes de recuperación.

El **promedio general** para RECUPERAR es de aproximadamente 5. Esto sugiere un nivel bajo de madurez en las prácticas de recuperación después de incidentes de ciberseguridad, si bien con una clara mejora respecto a los resultados obtenidos en la edición anterior.

Puntos Fuertes por Sector: Sectores como "Actividades artísticas" , “Inmobiliarias”, “Profesionales, científicas y técnicas” o “Educación” destacan con promedios más altos (7), indicando prácticas de recuperación moderadas, y mostrando gran avance respecto a la mejora de sus prácticas en el último año.

Consistencia en Muchos Sectores, desde "Construcción", "Actividades Sanitarias", "Suministros de agua" o “Manufacturera”, muestran consistencia con promedios iguales o superiores a la media de 5.

De nuevo, enfoque Específico en "Fabricación de Productos Farmacéuticos" o “Producción, transporte y distribución de energía eléctrica” con un **promedio bajo** ,**y la nueva industria representada** en la muestra de esta edición, “Fabricación de motores, generadores y transformadores eléctricos , y de aparatos de distribución y control eléctrico” con un margen significativo de mejora y atención específica en sus prácticas de recuperación ante incidentes.



lustración 14: Indicador “Recuperar” por sector de actividad .

6.6. Dominio 6: Gobierno

En este apartado se presentan los datos relativos al dominio de **Gobierno**, nuevo dominio incorporado en la versión 2.0 del NIST CSF, 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 9, lo que indica un nivel de madurez medio en términos de gobernanza en ciberseguridad. Los sectores con los promedios más altos son **Actividades de apoyo a las empresas n.c.o.p.** y **Telecomunicaciones**, ambos con un nivel de madurez consolidado (con valores de 12), lo que sugiere que estos sectores han fortalecido sus estrategias de gobernanza y refleja prácticas de gobernanza sólidas y una integración avanzada de la ciberseguridad en sus estructuras de dirección.

Dispersión en varios sectores: Se observa una notable variabilidad en los resultados en sectores como **Comercio al por mayor y al por menor; reparación de vehículos de motor y motocicletas** (con una dispersión entre 5 y 11), **Administración Pública y Defensa; Seguridad Social obligatoria** (variando de 2 a 12), **Actividades sanitarias y de servicios sociales** (5 a 11) y **Actividades financieras y de seguros** (6 a 12) y **Otros servicios** (con valores entre 3 y 12). Esta amplia dispersión indica 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 motores, generadores y transformadores eléctricos y de aparatos de distribución y control eléctrico**, que presenta el promedio más bajo (5), lo cual pone de manifiesto la necesidad de reforzar la gobernanza en ciberseguridad en este ámbito. Aunque el nivel de madurez en este sector es relativamente bajo, estos resultados pueden ayudar a identificar áreas críticas en las que implementar medidas de gobernanza más robustas.

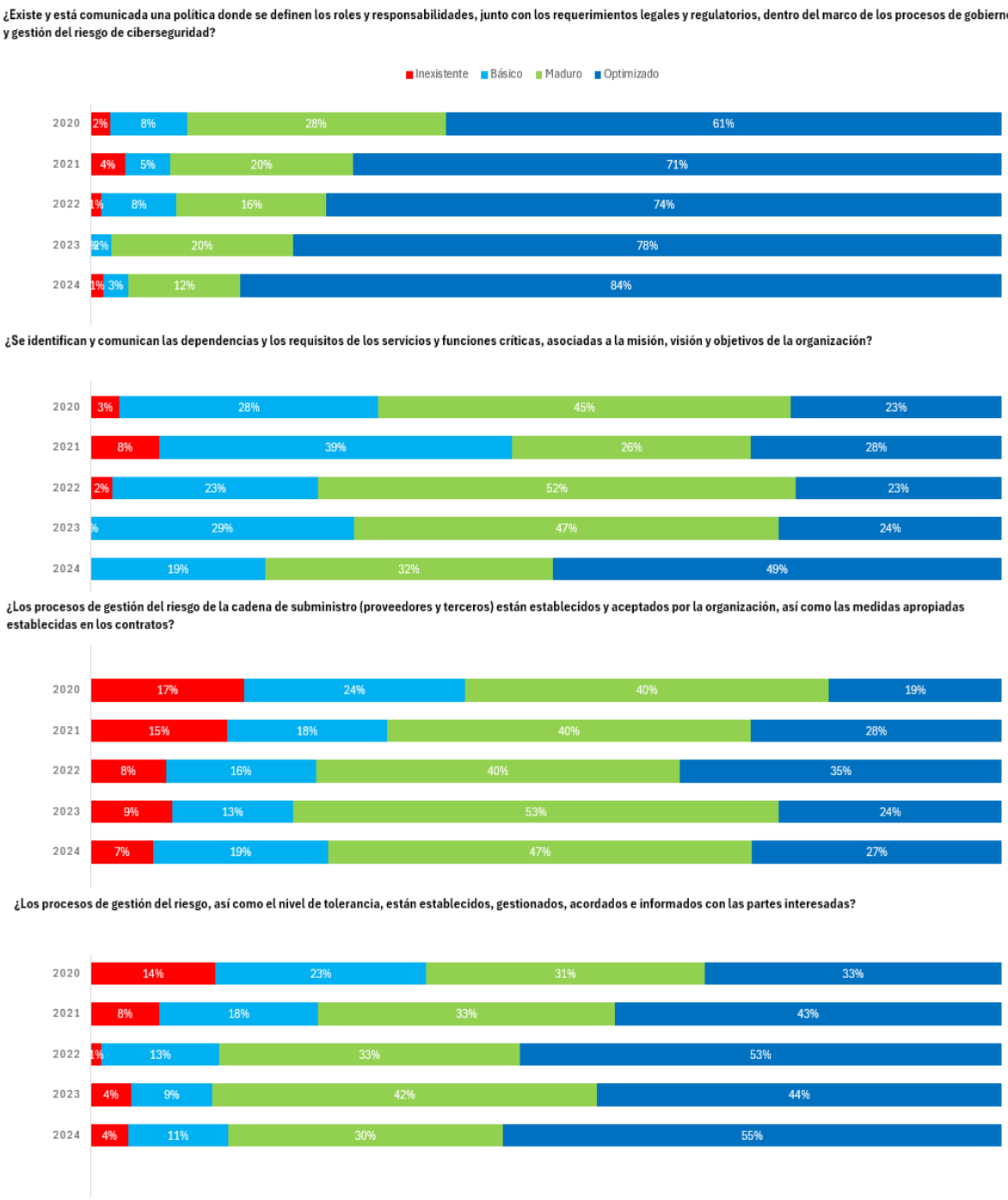


Ilustración 15: Evolución de la tendencia del domino Gobierno

Los datos de los últimos cinco años muestran en general un progreso constante en el dominio de Gobierno. Las organizaciones han 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 un 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.

La madurez en los procesos de gestión del riesgo, incluyendo el establecimiento del nivel de tolerancia y la comunicación con las partes interesadas, ha mostrado un avance significativo. En 2024, el 55% de las organizaciones tienen estos procesos optimizados, un aumento importante desde el 33% en 2020. Al mismo tiempo, la categoría de “Inexistente” ha disminuido del 14% en 2020 al 4% en 2024. Este progreso refleja una mejora en la formalización y transparencia de la gestión del riesgo, con más organizaciones alcanzando niveles altos de madurez.

La gestión de riesgos en la cadena de suministro ha tenido fluctuaciones en sus niveles de madurez. En 2020, solo el 19% de las organizaciones estaban en nivel optimizado, y este porcentaje ha aumentado gradualmente hasta llegar al 27% en 2024, aunque con una ligera baja en 2023 (24%). La categoría "Inexistente" ha reducido su presencia del 17% en 2020 al 7% en 2024, lo que sugiere una mejora en la formalización de prácticas de riesgo con proveedores y terceros. No obstante, la variabilidad observada en los últimos años podría indicar 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 positiva. En 2024, un 49% de las organizaciones han alcanzado un nivel optimizado, en comparación con solo el 23% en 2020. Además, la categoría “Básico” ha disminuido de 28% en 2020 a 19% en 2024. Esto muestra una evolución hacia una mayor integración de la ciberseguridad en la estrategia organizacional, asegurando que las funciones críticas sean identificadas y gestionadas en alineación con la misión y objetivos de la organización.

La madurez en la definición y comunicación de roles, responsabilidades y requisitos regulatorios ha mostrado uno de los mayores avances. En 2024, el 84% de las organizaciones tienen procesos optimizados en este aspecto, un aumento notable desde el 61% en 2020. Este incremento subraya la importancia que las organizaciones han dado a la estructuración y claridad en sus políticas de ciberseguridad, garantizando que los roles y responsabilidades estén claramente definidos y comunicados, lo cual es fundamental para una gobernanza efectiva en ciberseguridad.

Los datos de los últimos cinco años muestran en general un progreso constante en el dominio de Gobierno. Las organizaciones han 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 un 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.

La madurez en los procesos de gestión del riesgo, incluyendo el establecimiento del nivel de tolerancia y la comunicación con las partes interesadas, ha mostrado un avance significativo. En 2024, el 55% de las organizaciones tienen estos procesos optimizados, un aumento importante desde el 33% en 2020. Al mismo tiempo, la categoría de “Inexistente” ha disminuido del 14% en 2020 al 4% en 2024. Este progreso refleja una mejora en la formalización y transparencia de la gestión del riesgo, con más organizaciones alcanzando niveles altos de madurez.

La gestión de riesgos en la cadena de suministro ha tenido fluctuaciones en sus niveles de madurez. En 2020, solo el 19% de las organizaciones estaban en nivel optimizado, y este porcentaje ha aumentado gradualmente hasta llegar al 27% en 2024, aunque con una ligera baja en 2023 (24%). La categoría "Inexistente" ha reducido su presencia del 17% en 2020 al 7% en 2024, lo que sugiere una mejora en la formalización de prácticas de riesgo con proveedores y terceros. No obstante, la variabilidad observada en los últimos años podría indicar 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 positiva. En 2024, un 49% de las organizaciones han alcanzado un nivel optimizado, en comparación con solo el 23% en 2020. Además, la categoría “Básico” ha disminuido de 28% en 2020 a 19% en 2024. Esto muestra una evolución hacia una mayor integración de la ciberseguridad en la estrategia organizacional, asegurando que las funciones críticas sean identificadas y gestionadas en alineación con la misión y objetivos de la organización.

La madurez en la definición y comunicación de roles, responsabilidades y requisitos regulatorios ha mostrado uno de los mayores avances. En 2024, el 84% de las organizaciones tienen procesos optimizados en este aspecto, un aumento notable desde el 61% en 2020. Este incremento subraya la

importancia que las organizaciones han dado a la estructuración y claridad en sus políticas de ciberseguridad, garantizando que los roles y responsabilidades estén claramente definidos y comunicados, lo cual es fundamental para una gobernanza efectiva en ciberseguridad.

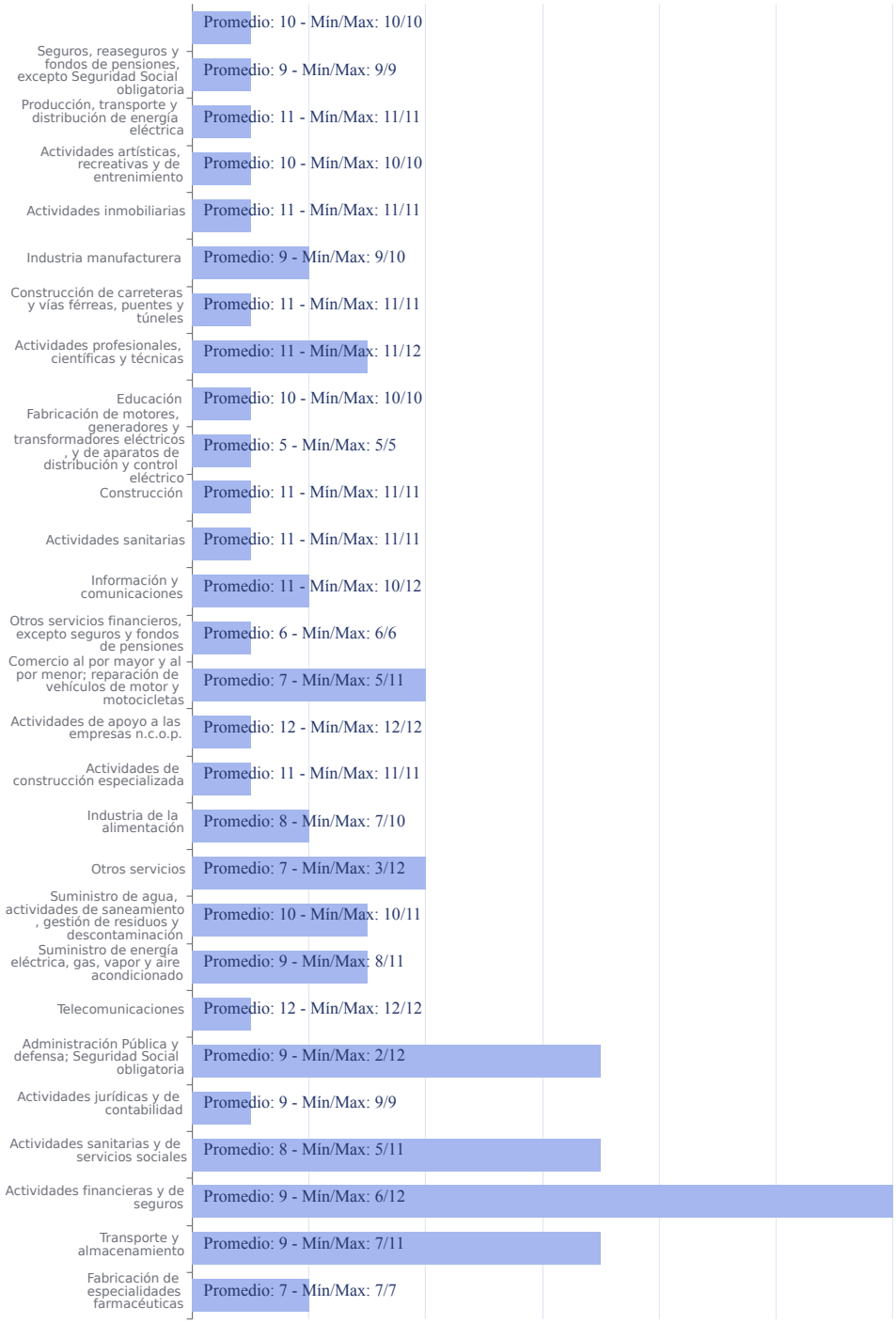


Ilustración 16: Indicador "Gobierno" por sector de actividad .

7. Recursos y Organización

Los datos obtenidos en esta edición permiten analizar la evolución en la distribución de los recursos destinados a ciberseguridad dentro de las organizaciones. Este año se observa una tendencia hacia el incremento en el personal dedicado a ciberseguridad, con una disminución del porcentaje de empresas con menos recursos y un aumento significativo en aquellas con equipos más grandes.

En 2024, un 42,5% de las organizaciones cuentan con entre 1 y 5 personas en el área de ciberseguridad, una reducción notable frente al **64,45% reportado el año anterior.** Asimismo, el **24,7%** de las empresas disponen de entre 5 y 15 personas, **en comparación con el 20% de 2023.** Este cambio también se refleja en el incremento de organizaciones con equipos más amplios: un 21,9% ahora cuenta con entre 15 y 50 personas (frente al 13,33% anterior), y el porcentaje de empresas con más de 50 personas en el área de ciberseguridad ha subido significativamente, alcanzando el **11,0% en 2024 frente al 2,2% del año pasado.**

En cuanto a la operación de la ciberseguridad desde el propio departamento de Ciberseguridad, también se observa un aumento. Este año, un **68,5%** de las empresas analizadas gestionan la ciberseguridad internamente, en comparación con el **57,75% del año pasado**.

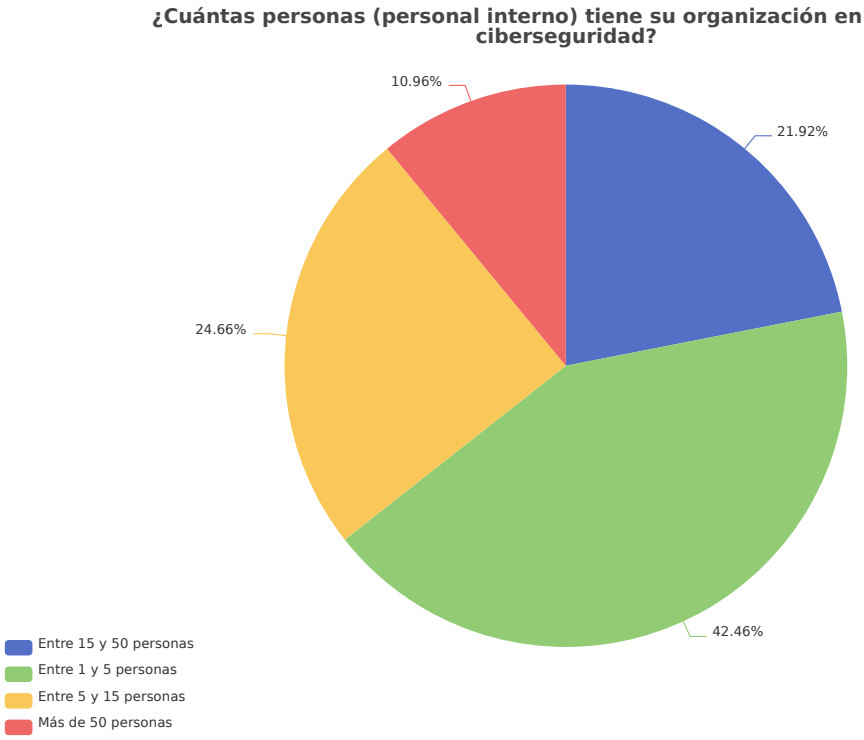


Ilustración 17: Personal interno en ciberseguridad

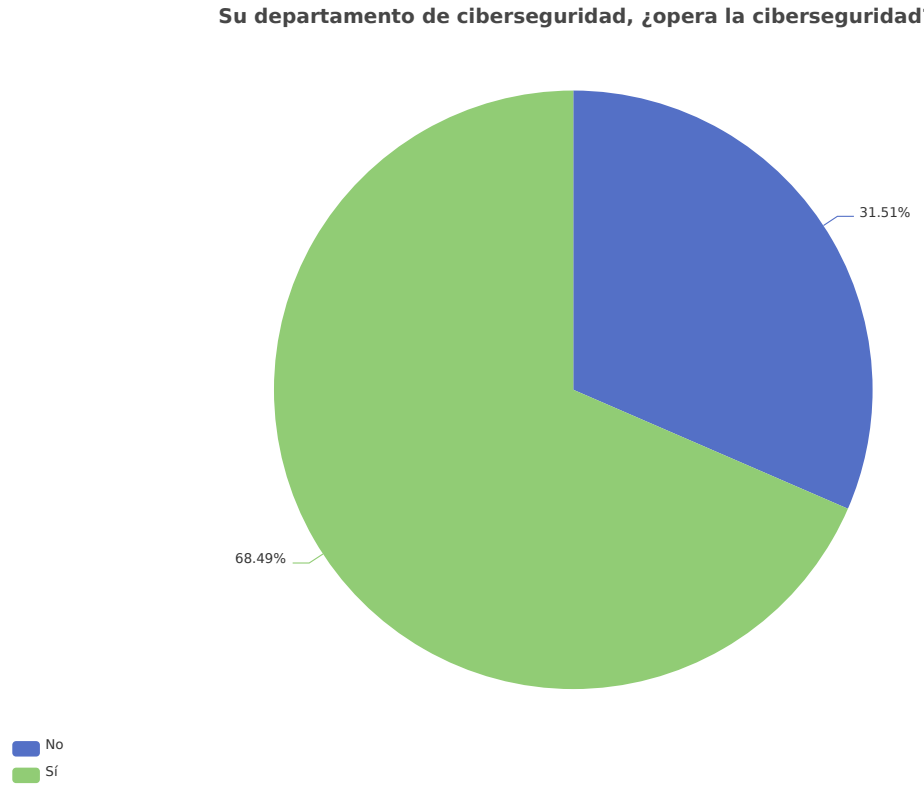


Ilustración 18: Operación de la Seguridad

8. Influencia del contexto actual

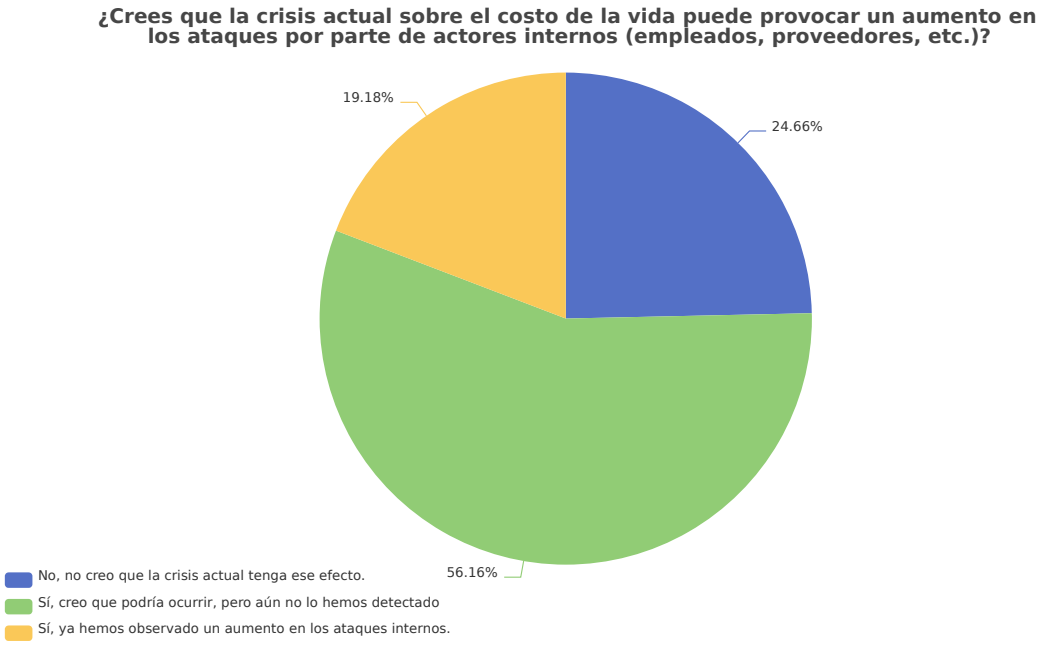


Ilustración 19: Aumento de Ataques internos

De acuerdo a los resultados, existe la percepción generalizada de que el incremento en el costo de la vida podría provocar un aumento en el número de ciberataques cometidos por actores internos. Dos tercios de los encuestados secundan esta afirmación, aunque no han podido detectarlo en la práctica, mientras que casi un 20% de los entrevistados han podido corroborar un incremento de los ataques con origen interno.

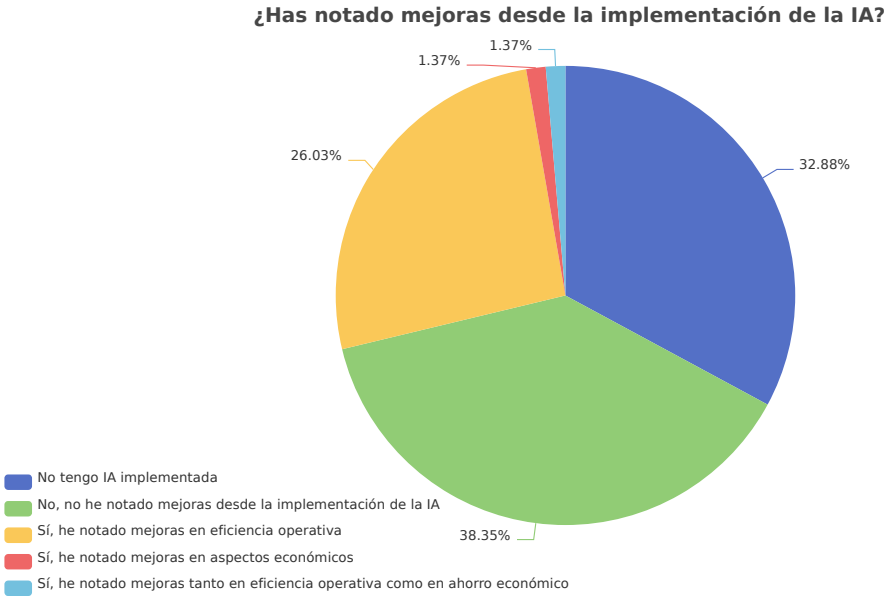


Ilustración 20: Implantación de la IA

Aunque la inteligencia artificial cada vez tiene más presencia en nuestras vidas, aproximadamente un 33% de los encuestados no la han implementado todavía. El 67% restante cuenta con algún tipo de capacidades de IA, pero casi un 40% declara no haber notado ningún tipo de mejora gracias a su utilización. En cuanto a los entrevistados que afirman haber obtenido provecho de la IA, en su mayoría han detectado mejoras relativas a eficiencia operativa, mientras que las mejoras en cuanto a ahorro han sido percibidas de manera muy minoritaria (apenas un 1%).

9. 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, este año se aporta por primera vez la **estimación de probabilidades de ocurrencia de ciberincidentes con distintos niveles de impacto**. Se pretende que este nuevo indicador transmita, 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%.

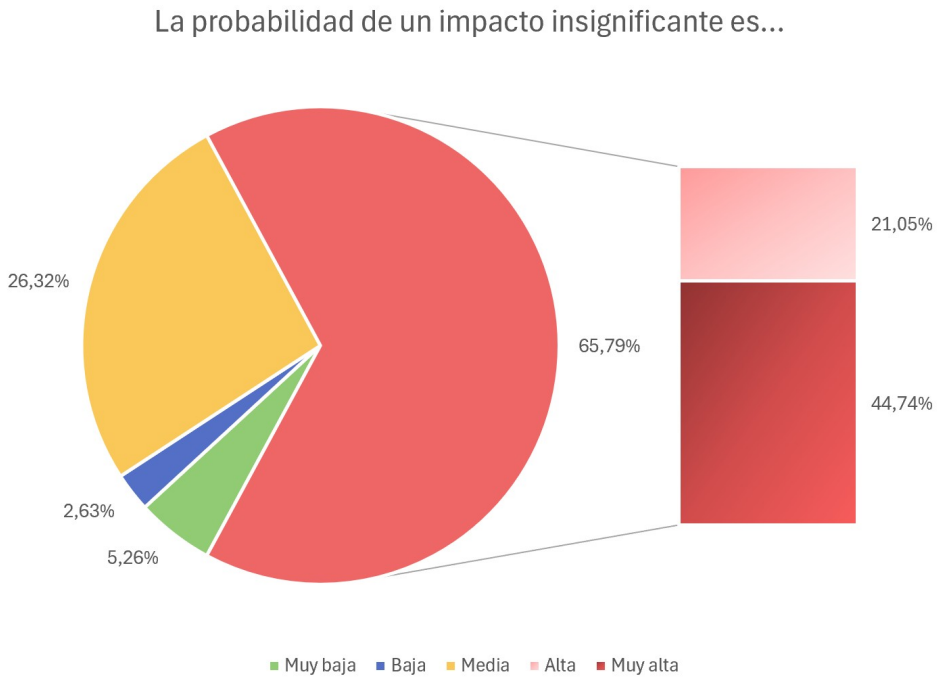


Ilustración 21: Riesgo de ciberinseguridad para impactos insignificantes

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**.

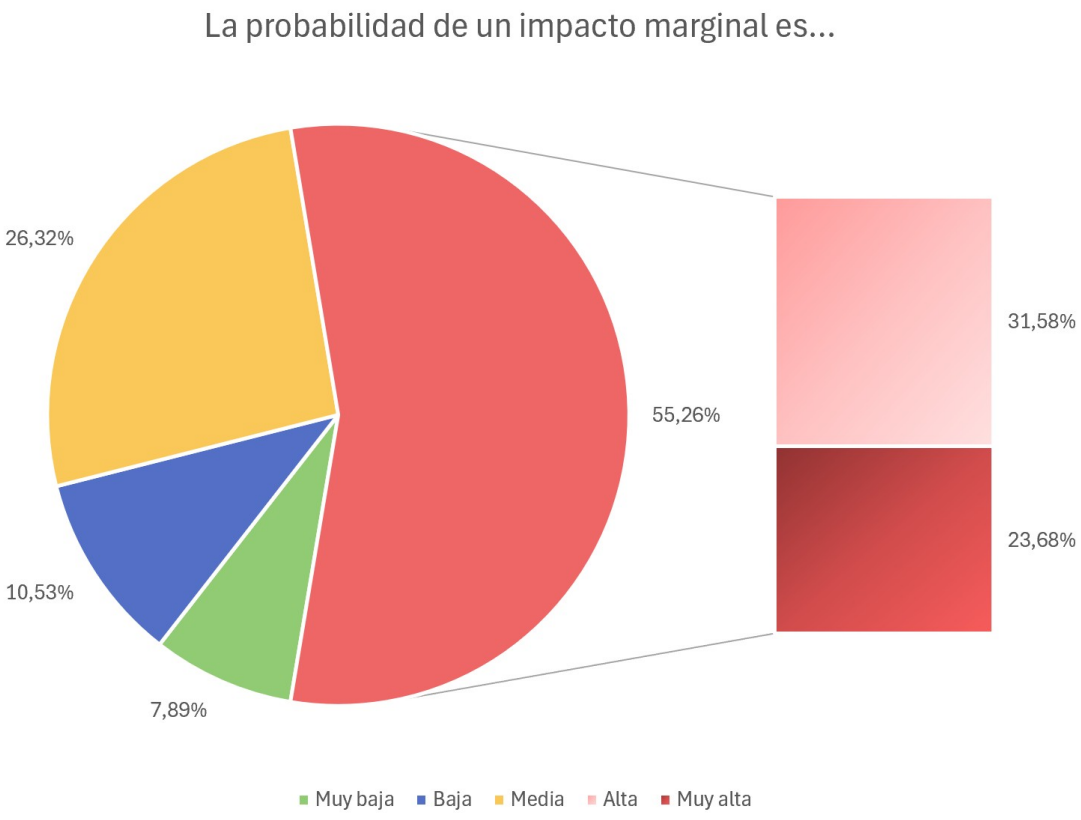


Ilustración 22: Riesgo de ciberinseguridad para impactos marginales

Tal y como muestra la Ilustración 22, **los impactos marginales**, que resultan más dañinos o peligrosos que los insignificantes, **tienen una probabilidad de ocurrencia alta o muy alta para el 55,26% de los encuestados**.

Añadiendo la probabilidad media, un 81,58% considera que este tipo de impactos como normales en su sector, un porcentaje menor que en el caso de los impactos insignificantes, pero claramente mayoritario.

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.

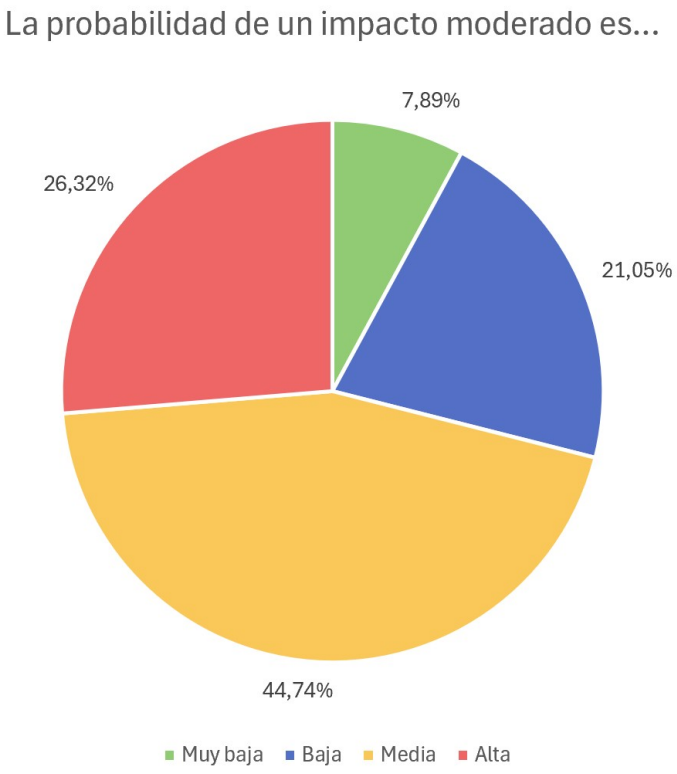


Ilustración 23: Riesgo de ciberinseguridad para impactos moderados

La Ilustración 23 muestra un cambio importante respecto al riesgo de impactos marginales e insignificantes. En concreto, la probabilidad de considerar un impacto moderado desciende hasta el 71% y sólo un 26,32% los considera frecuentes. Ningún encuestado considera un impacto moderado como muy frecuente, y dada la peligrosidad que representan, casi **un 29% de los encuestados considera los ciberincidentes de impacto moderado como eventos de probabilidad baja o muy baja**, demostrando que este tipo de impacto sí merece mayores medidas de ciberseguridad.

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 24. En concreto, el 73,69% de los encuestados les atribuye una probabilidad baja o muy 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 2,63% de los encuestados considera que la probabilidad de sufrir un impacto crítico es alto** (y ningún encuestado lo valora como muy alto).

Ilustración 24: Riesgo de ciberinseguridad para impactos críticos

La probabilidad de un impacto catastrófico es baja o muy baja para el 89,47% de los encuestados, como puede apreciarse en la Ilustración 25. Esto resulta lógico, pues el tipo de ciberincidentes que puedan generar este tipo de daño deben ser el principal foco de las medidas de ciberseguridad. Aunque las probabilidades altas o muy altas son iguales que las de los impactos críticos, hay una diferencia importante entre estos y los catastróficos. Para un impacto crítico, el 23,68% de encuestados atribuye una probabilidad de ocurrencia media, mientras que en el caso de un impacto crítico, este porcentaje se reduce hasta el 7,89%,

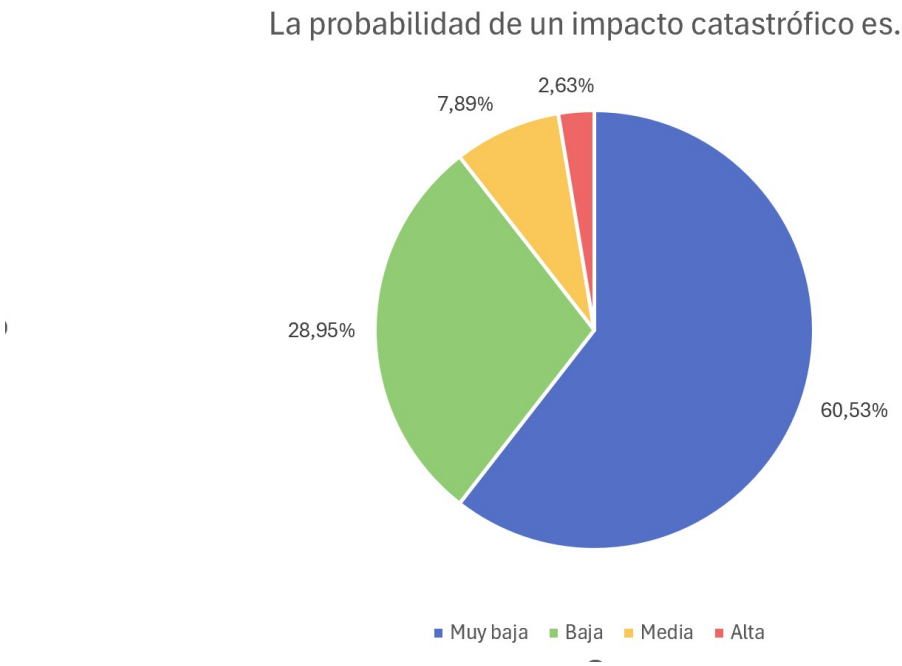


Ilustración 25: Riesgo de ciberinseguridad para impactos catastróficos

Dado que el número de encuestados que completó la parte del cuestionario fue reducido (38), resulta imposible realizar análisis del riesgo de ciberinseguridad por sectores en los que se alcance una representatividad suficiente. No obstante, sí que pueden plantearse algunos cálculos sencillos para aventurar el posible impacto económico de la ciberinseguridad.

La multiplicación del porcentaje de encuestados por las probabilidades asociadas a cada nivel de ocurrencia y el daño estimado para cada tipo de impacto podría dar una estimación económica del coste de la ciberinseguridad. No obstante, este cálculo exigiría asumir que los encuestados son una muestra lo suficientemente representativa de los distintos sectores de la economía española y ponderar posteriormente sus respuestas según la participación de cada sector en el conjunto del PIB nacional.

A pesar de no contar con datos suficientes para ofrecer estimaciones fiables, aprovechamos la ocasión para ofrecer unos cálculos a partir de los datos obtenidos de la encuesta de este año. Así, los impactos insignificantes carecerían de valor económico, los impactos marginales y moderados supondrían un 0,03% de las cifras de negocio respectivamente, los impactos críticos un 0,06% y los impactos catastróficos un 0,38%. Sumando los distintos valores en riesgo por la ciberinseguridad obtendríamos que **el coste aproximado del ciber-riesgo equivaldría a un 0,5% de la cifra de negocio anual**.

Aunque esta cifra pueda parecer baja, es necesario ponerla en contexto. En caso de contar con datos representativos de todos los sectores económicos que componen el PIB español, dado que este, durante el año 2023, ascendió a 1,46 billones de euros, estaríamos hablando de que el coste de la ciberinseguridad en nuestro país podría alcanzar los 73.000 millones de euros.

También establecer comparaciones ayuda a entender la magnitud de estas cifras. Por ejemplo, las estimaciones más pesimistas sobre los efectos macroeconómicos del cambio climático elaboradas por el Fondo Monetario Internacional, indican que España perdería un 0,77 del PIB per cápita para 2030 por esta causa. En caso de materializarse en un solo año los impactos catastróficos por ciberincidentes que se desprenden de nuestra encuesta a nivel nacional (0,38%) se alcanzaría la mitad de daño económico que se espera del peor escenario sobre cambio climático hasta el año 2030.

V Indicador de madurez en ciberseguridad

OBSERVATORIO DE LA CIBERSEGURIDAD

www.ismsforum.es
info@ismsforum.es
(+34) 915 63 50 62

Una iniciativa de

ISMS FORUM
INTERNATIONAL INFORMATION SECURITY COMMUNITY