IV Indicador de madurez en ciberseguridad

OBSERVATORIO DE LA CIBERSEGURIDAD

isms forum INTERNATIONAL INFORMATION SECURITY COMMUNITY

isms BARCELONA INTERNATIONAL INFORMATION SECURITY COMMUNITY

IV Indicador de madurez en ciberseguridad

OBSERVATORIO DE LA CIBERSEGURIDAD

AUTORES

PARTICIPANTES

David Esteban

Daniel García

David Llorente

Iván Sánchez

Olga Forné

Óscar Sánchez

Pedro López

Santiago Minguito

Toni García

GESTIÓN DE PROYECTOS

Beatriz García

Índice

ISMS Forum y su iniciativa: el Observatorio de la Ciberseguridad

ISMS Forum es una organización sin ánimo de lucro que se fundó en enero de 2007 con el propósito de fomentar el desarrollo, el conocimiento y la cultura de la Seguridad de la Información en España, además de actuar en beneficio de la comunidad involucrada en este sector. Con una vocación inclusiva y abierta, se erige como el principal foro especializado a nivel nacional en el que empresas, organizaciones públicas y privadas, investigadores y profesionales pueden colaborar, compartir experiencias y estar al tanto de los últimos avances en materia de Seguridad de la Información. Todos sus esfuerzos se rigen por valores fundamentales, como la transparencia, la independencia, la objetividad y la neutralidad.

ISMS Forum comenzó su trayectoria como el Capítulo Español de ISMS International User Group (IUG), una organización que promovía el conocimiento y la implementación de Sistemas de Gestión de la Seguridad de la Información en todo el mundo, siguiendo la familia de estándares ISO 27000. En la actualidad, la Asociación mantiene una representación global unificada y centralizada en España bajo la marca denominada International Information Security Community.

La Asociación organiza diversas iniciativas que abordan, desde una perspectiva global o especializada, el campo de la Seguridad de la Información. Estas iniciativas incluyen Jornadas Internacionales, Data Privacy Institute, Cloud Security Alliance, Cyber Security Center, IoT Security Center, talleres sobre temas específicos y formación especializada en protección de datos y ciberseguridad. Además, gestionan certificaciones como Certified Data Privacy Professional (CDPP), Certificación de Delegado de Protección de Datos (CDPD), Certified Cyber Security Professional (CCSP) y promueven el Certificate Of Cloud Security Knowledge (CCSK).

En 2020, el marco asociativo de ISMS Forum se consolidó como la comunidad más grande de expertos y organizaciones con intereses y responsabilidades en seguridad de la información en España. Esto se logró promoviendo la formación y excelencia de sus miembros, facilitando la comunicación con las autoridades de control y fomentando el intercambio de conocimientos entre los principales actores y expertos en el sector para impulsar y contribuir a la mejora de la ciberseguridad en España.

Además, la Asociación dio un paso adicional en su objetivo de crear conciencia sobre la necesidad de formar y sensibilizar sobre los riesgos asociados a la dependencia de la sociedad de las Tecnologías de la Información y la Comunicación (TIC), un aspecto crucial para garantizar el desarrollo socioeconómico del país.

Para cumplir con la misión anteriormente descrita, la Asociación identifica la necesidad de ser un referente y ofrecer una plataforma para el desarrollo de indicadores que permitan el análisis y la discusión de las áreas de mayor preocupación, así como los riesgos y desafíos más relevantes en el campo de la ciberseguridad. De esta manera, se establece el primer Observatorio de la Ciberseguridad para empresas y profesionales del sector.

Objetivos del Observatorio de la Ciberseguridad

Los objetivos del Observatorio de la Ciberseguridad son:

- Brindar una plataforma para el análisis del nivel de madurez, evolución y los nuevos fenómenos en el ámbito de la seguridad de la información.
- Generar indicadores nacionales sobre el estado de la ciberseguridad en empresas y entidades tanto privadas como públicas.
- Promover el conocimiento y la investigación en el campo de la ciberseguridad.
- Crear métricas y referencias nacionales para evaluar y mejorar la ciberseguridad.
- Colaborar y establecer un diálogo con instituciones y reguladores en materia de ciberseguridad.

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

Según la definición de gestión de riesgos proporcionada por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos, se trata de un proceso continuo que implica la identificación, evaluación y respuesta a los riesgos. Para gestionar adecuadamente los riesgos, las organizaciones deben comprender la probabilidad de que ocurra un evento y los posibles impactos que podrían derivarse de él. Esta premisa es la base sobre la cual el Observatorio de Ciberseguridad de ISMS Forum presenta la tercera edición de su estudio. Su objetivo es proporcionar claridad acerca del estado actual de la ciberseguridad en las empresas nacionales y ofrecer información valiosa tanto para las empresas como para los profesionales. El estudio busca generar un indicador anual que permita una mejor interpretación de la evolución interanual de los riesgos cibernéticos y su relación con otros factores y fenómenos.

El indicador de nivel de madurez en ciberseguridad se basa en el marco metodológico establecido por el Instituto Nacional de Estándares y Tecnología (NIST) en 2013. Este marco se ha utilizado ampliamente a nivel global por organizaciones de diversos sectores y tamaños. Sirve como referencia para aquellas organizaciones que aplican los principios y las mejores prácticas para medir y mejorar sus capacidades en las áreas de Identificación, Protección, Detección, Respuesta y Recuperación. Es importante destacar que NIST ofrece un marco de políticas de ciberseguridad que no son de cumplimiento obligatorio y que cada organización debe adaptar según sus necesidades, regulaciones aplicables y su propia naturaleza.

En esta cuarta edición del Observatorio, se ha analizado la influencia del uso de herramientas de inteligencia artificial como indicador temporal para comprender su impacto en el contexto actual. El estudio, realizado por ISMS Forum, se centra en la aplicación del marco desarrollado por NIST en una muestra de 45 organizaciones que operan a nivel nacional. Esta muestra incluye tanto empresas multinacionales como nacionales, y no recopila información de empresas proveedoras de servicios de ciberseguridad.

2. Aplicación de los dominios establecidos por el NIST

Identificar – (Gestión de activos, Entorno de negocios, Gobernanza, Evaluación de riesgos y Estrategia de gestión de riesgos).
Desarrollar una comprensión organizacional para administrar el riesgo de ciberseguridad para sistemas, personas, activos, datos y capacidades.

Proteger – (Gestión de identidad y control de acceso, Conciencia y entrenamiento, Seguridad de datos, Procesos y procedimientos de protección de la información, Mantenimiento y Tecnología de protección).
Desarrollar e implementar medidas de seguridad adecuadas para garantizar la entrega de servicios críticos. La función Proteger admite la capacidad de limitar o contener el impacto de un posible evento de ciberseguridad.

Detectar – (Anomalías y eventos, Monitoreo continuo de seguridad y Procesos de detección).
Desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad. La Función Detectar permite el descubrimiento oportuno de eventos de ciberseguridad.

Responder – (Planificación de respuesta, Comunicaciones, Análisis, Mitigación y Mejoras).
Desarrollar e implementar actividades apropiadas para tomar medidas con respecto a un incidente detectado de ciberseguridad.

Recuperar – (Planificación de recuperación, Mejoras y Comunicaciones).
Desarrollar e implementar actividades apropiadas para mantener los planes de resiliencia y restablecer cualquier capacidad o servicio que se haya visto afectado debido a un incidente de ciberseguridad.

3. Tipología de muestra

En la presente edición, hemos contado con la participación de 45 empresas, de las cuales un 31% facturan más de 1.000 millones de Euros y el 17% más de 100. El 95% de los encuestados ocupan puestos de responsabilidad o son especialistas de seguridad de la información.

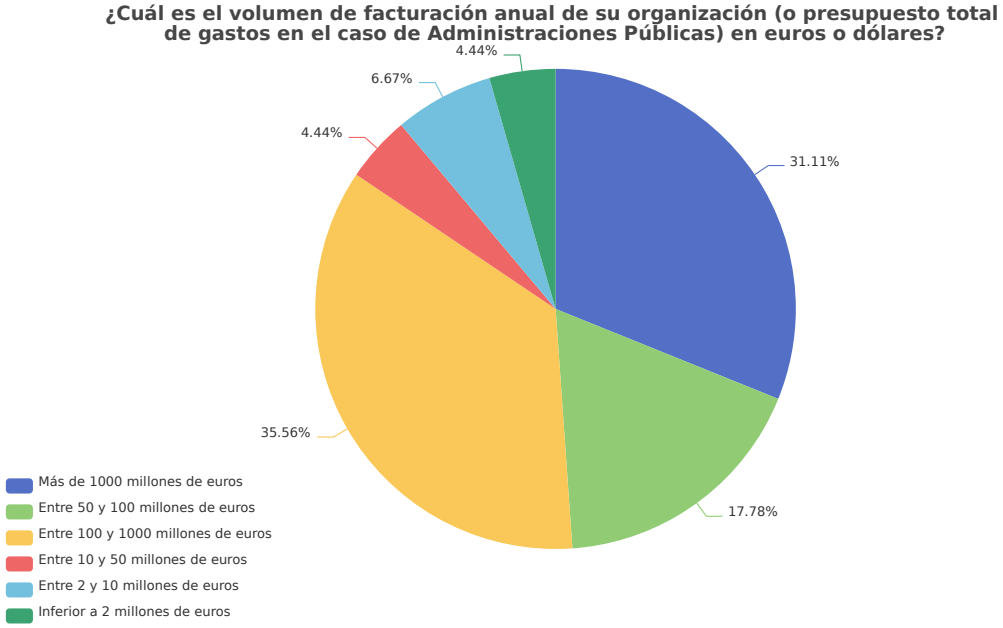


Ilustración 1: Volumen de facturación anual de las empresas participantes

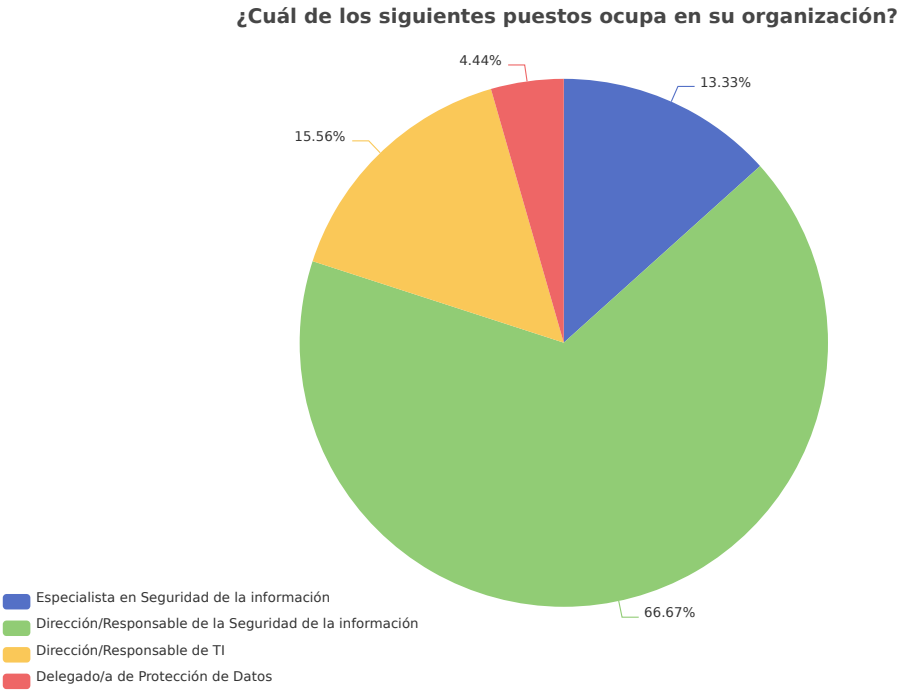


Ilustración 2: Puesto de trabajo ocupado por el encuestado.

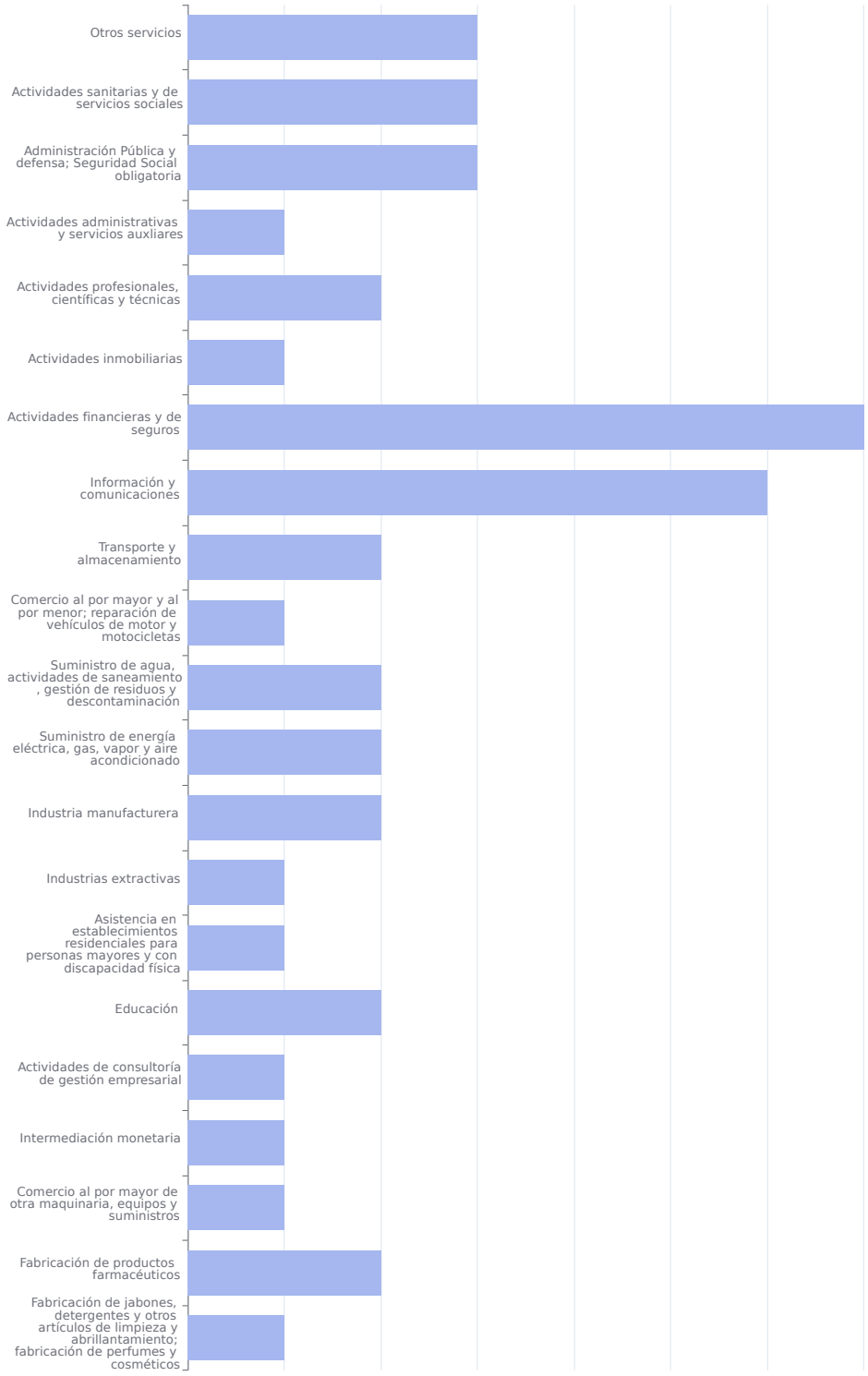


Ilustración 3: Sector de actividad de las empresas participantes.

4. Nivel de madurez

Dominio 1: Identificar

Este análisis global proporciona una visión panorámica de la situación de las empresas españolas en términos de identificación de riesgos cibernéticos. Observando los resultados en su conjunto, podemos destacar algunas tendencias y patrones generales en la madurez del dominio 1.

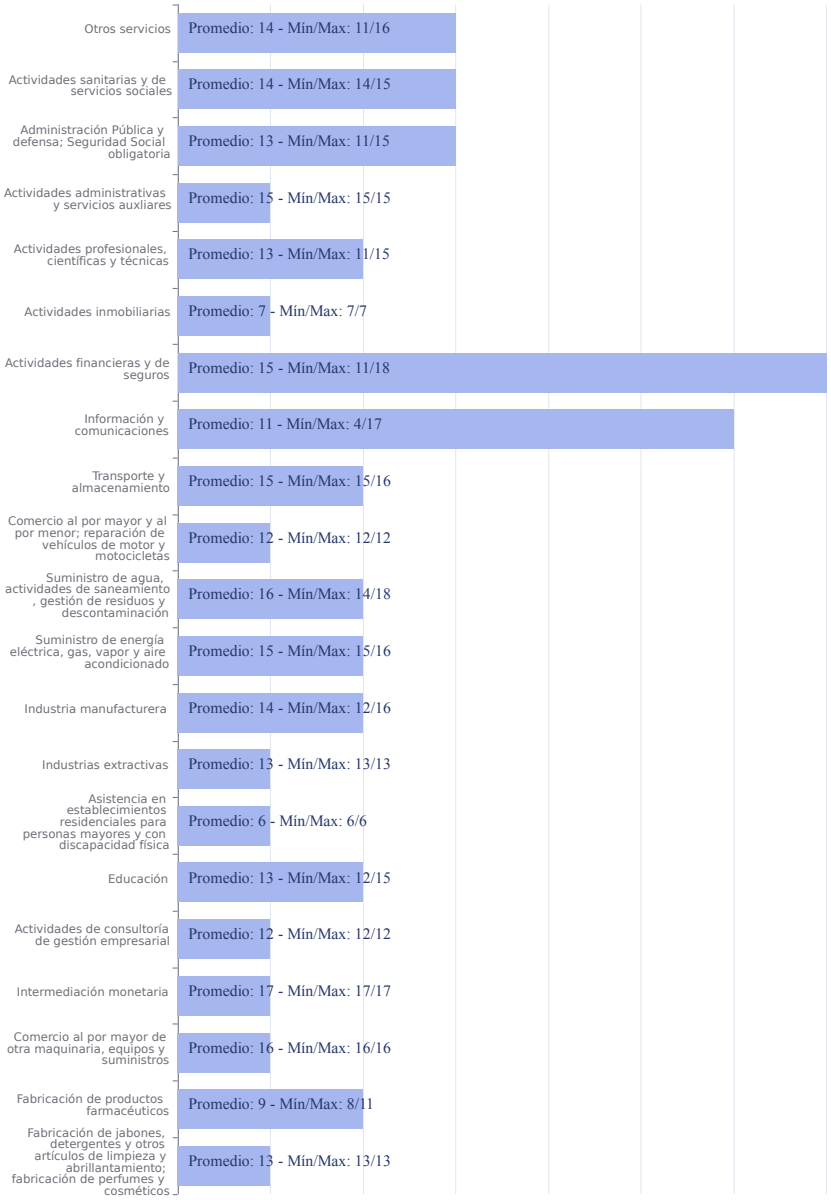


Ilustración 4: Indicador "Identificar" por sector de actividad .

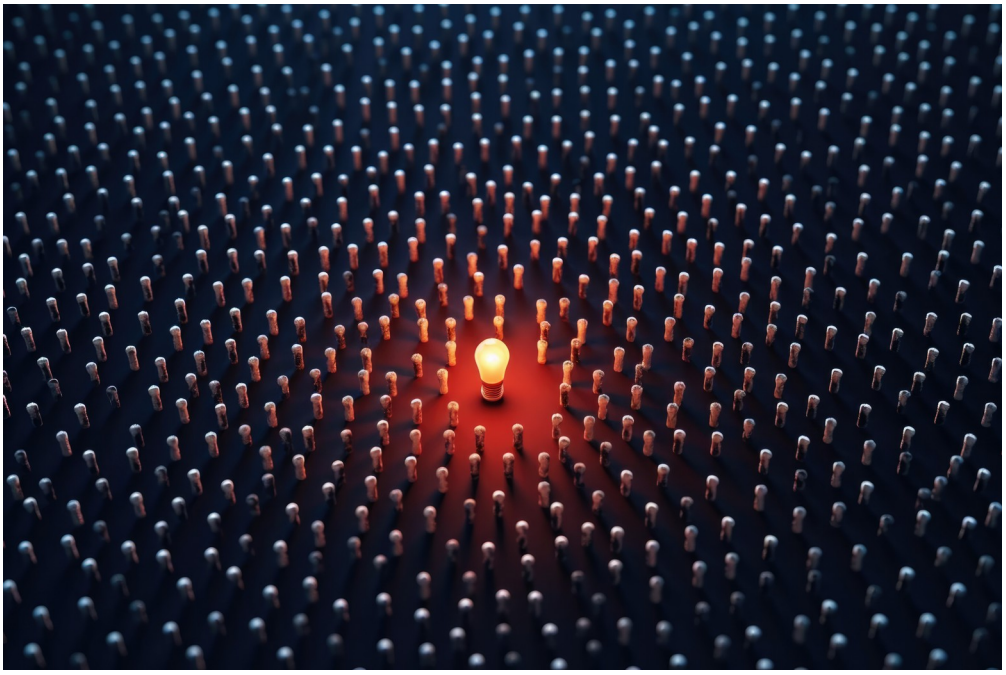
El **promedio general** de todas las respuestas es aproximadamente 13. Este valor puede interpretarse como un nivel medio de madurez en la identificación de riesgos cibernéticos.

El **rango mínimo/máximo** varía desde 4 hasta 18, indicando una amplia variabilidad en la madurez de la identificación de riesgos entre las diferentes empresas y sectores evaluados.

Fortalezas: Sectores como "Actividades Administrativas y Servicios Auxiliares," "Transporte y Almacenamiento," "Suministro de Agua, Actividades de Saneamiento, Gestión de Residuos y Descontaminación," y "Intermediación Monetaria" destacan por tener promedios altos y rangos estrechos, sugiriendo una identificación de riesgos fuerte y consistente.

Áreas de Mejora: Sectores como "Actividades Inmobiliarias," "Asistencia en Establecimientos de Personas Mayores y con Discapacidad Física," presentan promedios más bajos y/o rangos más amplios, señalando áreas que podrían necesitar mejoras en la identificación de riesgos cibernéticos.

Consistencia en Algunos Sectores: Algunos sectores muestran una consistencia en la identificación de riesgos, indicando que las empresas dentro de esos sectores están aplicando prácticas más uniformes y están por encima de la media.



Dominio 2: Proteger

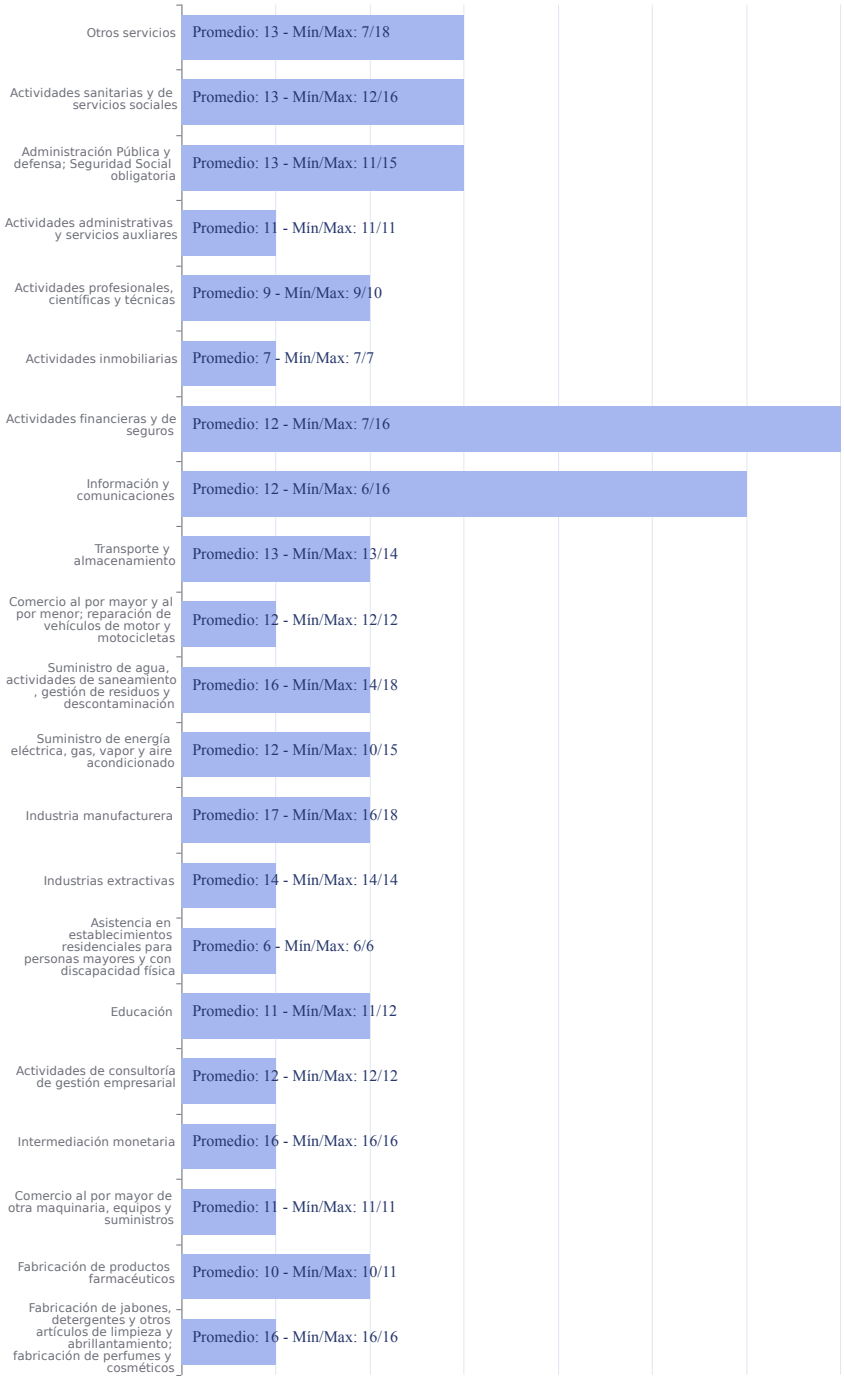


Ilustración 5: Indicador "Proteger" por sector de actividad .

Del dominio PROTEGER, centrado en 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 y accesos, podemos destacar:

El **promedio general** para PROTEGER es de aproximadamente 12, lo que indica un nivel medio de madurez en las prácticas de protección de la información y ciberseguridad.

Fortalezas por Sector: Sectores como "Industria Manufacturera" (Promedio: 17) y "Suministro de Agua, Actividades de Saneamiento, Gestión de Residuos y Descontaminación" (Promedio: 16) destacan por tener promedios más altos, indicando fuertes prácticas de protección.

Áreas de Mejora por Sector: Sectores como "Asistencia en Establecimientos de Personas Mayores y con Discapacidad Física" (Promedio: 6) y "Actividades Profesionales, Científicas y Técnicas" (Promedio: 9) muestran áreas que podrían necesitar mejoras en sus prácticas de protección.

Dominio 3: Detectar

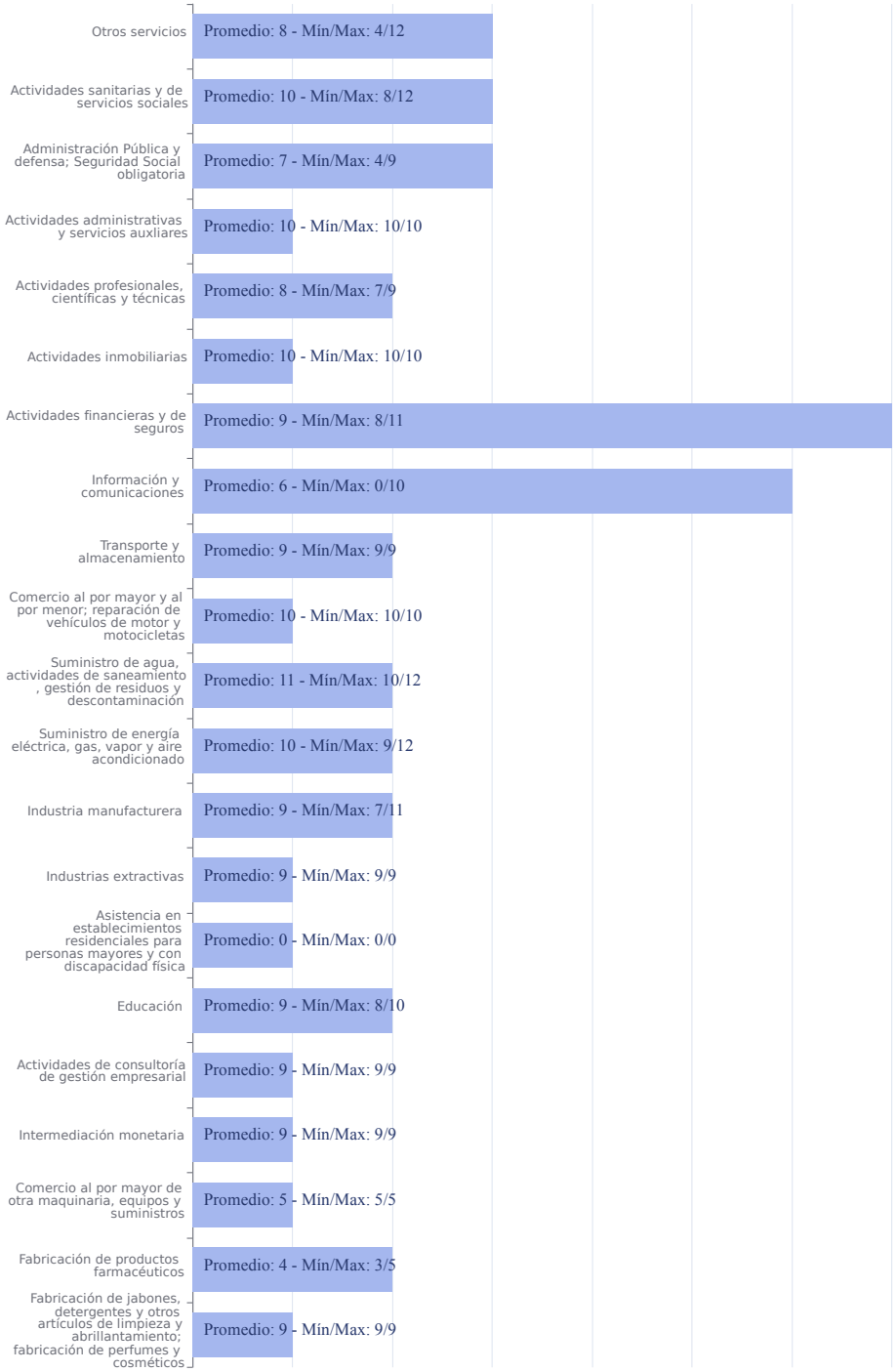


Ilustración 6: Indicador "Detectar" por sector de actividad .

Del dominio DETECTAR, centrado en la detección de incidentes, la monitorización de la actividad de usuarios, el análisis para la detección de actividad anómala y la disponibilidad de sistemas para la recolección de eventos, hacemos algunas observaciones:

El **promedio general** para DETECTAR es de aproximadamente 8. Esto sugiere un nivel medio alto de madurez en las prácticas de detección de incidentes y eventos de ciberseguridad.

Sectores como "Suministro de Agua, Actividades de Saneamiento, Gestión de Residuos y Descontaminación" y "Actividades Inmobiliarias" destacan con promedios más altos, indicando **prácticas de detección relativamente fuertes**.

Mientras que Sectores como "Asistencia en Establecimientos de Personas Mayores y con Discapacidad Física" tienen un promedio de 0, indicando que podría haber **oportunidades significativas de mejora** en la detección de incidentes.

Dominio 4: Responder

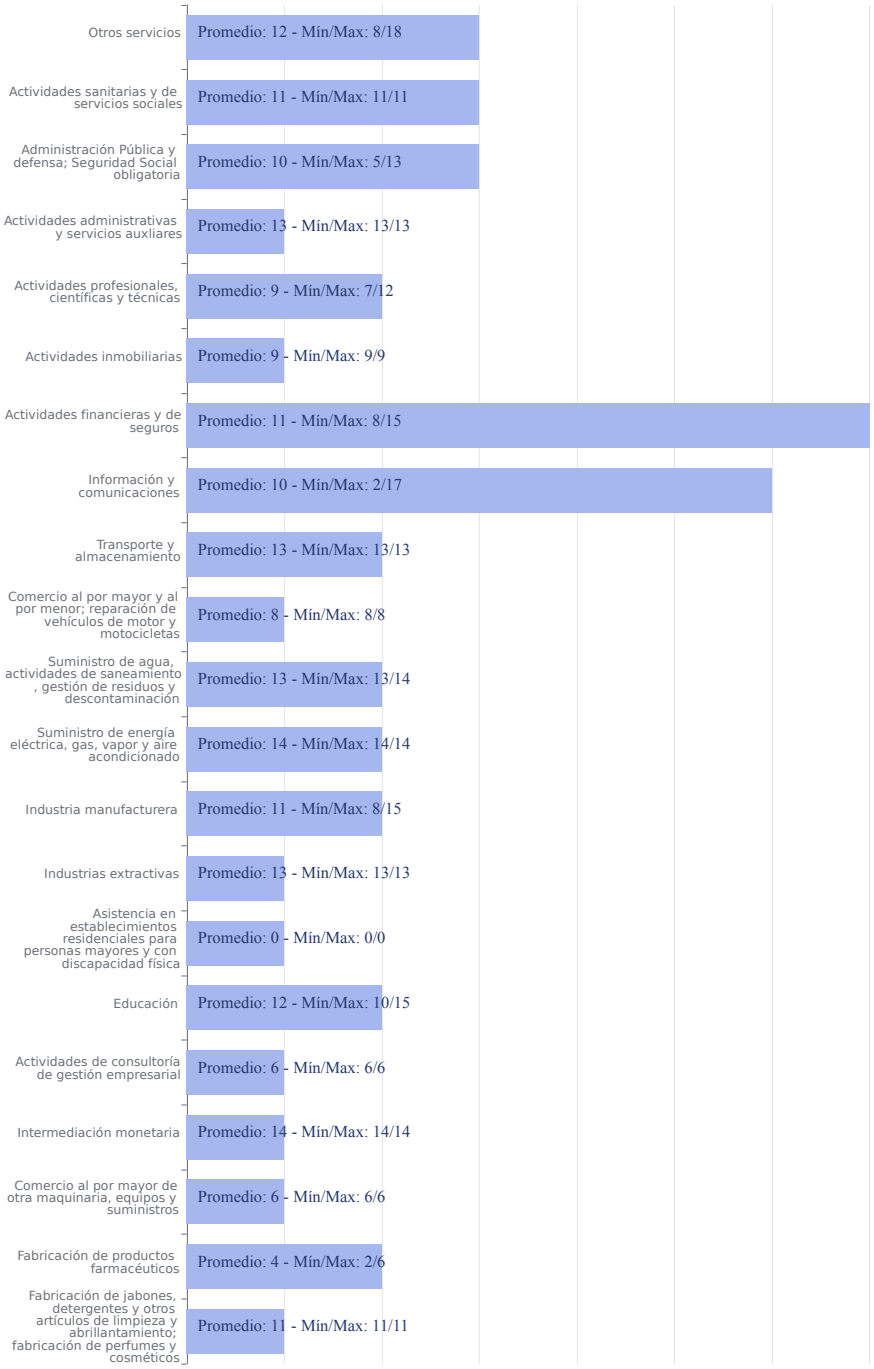


Ilustración 7: Indicador "IResponder" por sector de actividad .

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 "Suministro de Energía Eléctrica, Gas, Vapor y Aire Acondicionado," "Industrias Extractivas," y "Transporte y Almacenamiento" destacan con promedios más altos, indicando prácticas de **respuesta relativamente fuertes.**

Consistencia en Algunos Sectores: Sectores como "Actividades Administrativas y Servicios Auxiliares" y "Suministro de Agua, Actividades de Saneamiento, Gestión de Residuos y Descontaminación" muestran consistencia con promedios iguales en el rango.

Enfoque Específico en "Educación" y "Fabricación de Productos Farmacéuticos": Estos sectores tienen **promedios relativamente bajos**, lo que sugiere que podrían necesitar una atención específica en sus prácticas de respuesta ante incidentes.

Dominio 5: Recuperar

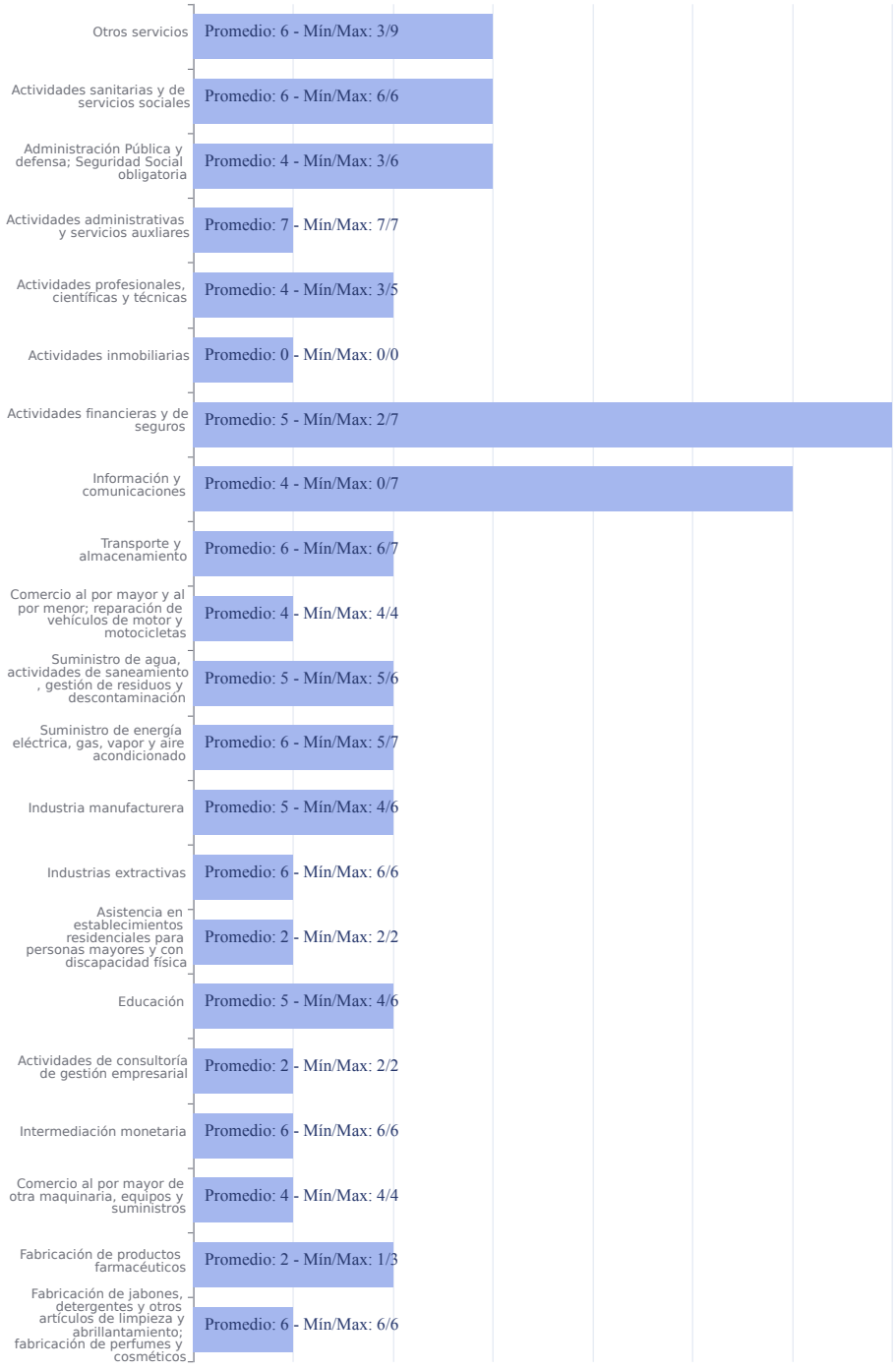


Ilustración 8: Indicador "Recuperar" por sector de actividad .

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 4. Esto sugiere un nivel bajo de madurez en las prácticas de recuperación después de incidentes de ciberseguridad.

Puntos Fuertes por Sector: Sectores como "Actividades Sanitarias y de Servicios Sociales" y "Asistencia en Establecimientos de Personas Mayores y con Discapacidad Física" destacan con promedios más altos, indicando prácticas de recuperación relativamente fuertes.

Áreas de Mejora por Sector: Sectores como "Actividades Inmobiliarias," "Educación," "Actividades de Consultoría de Gestión Empresarial," y "Fabricación de Productos Farmacéuticos" tienen promedios más bajos, lo que sugiere oportunidades significativas de mejora en las prácticas de recuperación.

Consistencia en Algunos Sectores: Sectores como "Industrias Extractivas," "Intermediación Monetaria," y "Fabricación de Jabones, Detergentes y Otros Artículos de Limpieza y Abrillantamiento; Fabricación de Perfumes y Cosméticos" muestran consistencia con promedios iguales en el rango.

5. Recursos y Organización

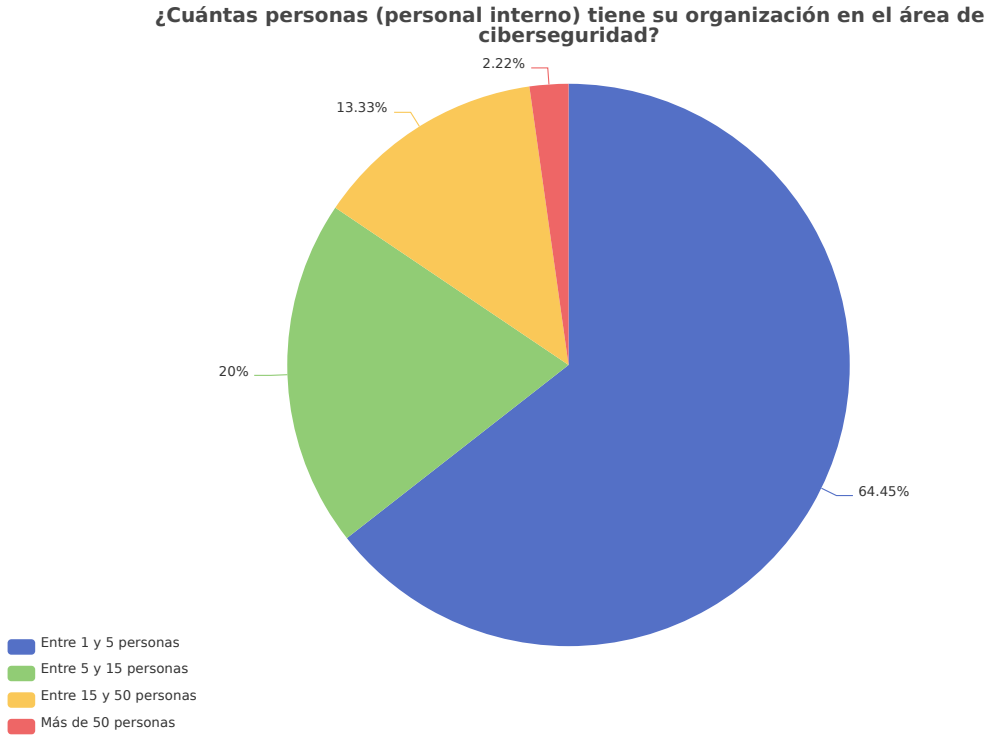


Ilustración 4: Personal interno en ciberseguridad

Los datos obtenidos permiten analizar la distribución de los recursos destinados a ciberseguridad. Un 64,45% de las organizaciones analizadas disponen de entre 1 y 5 personas en el área de ciberseguridad, un 20% tienen entre 5 y 15 personas, un 13,33% entre 15 y 50 personas. Únicamente encontramos un 2,2% de empr empresas con más de 50 personas en el área de ciberseguridad.

Operación de la Seguridad

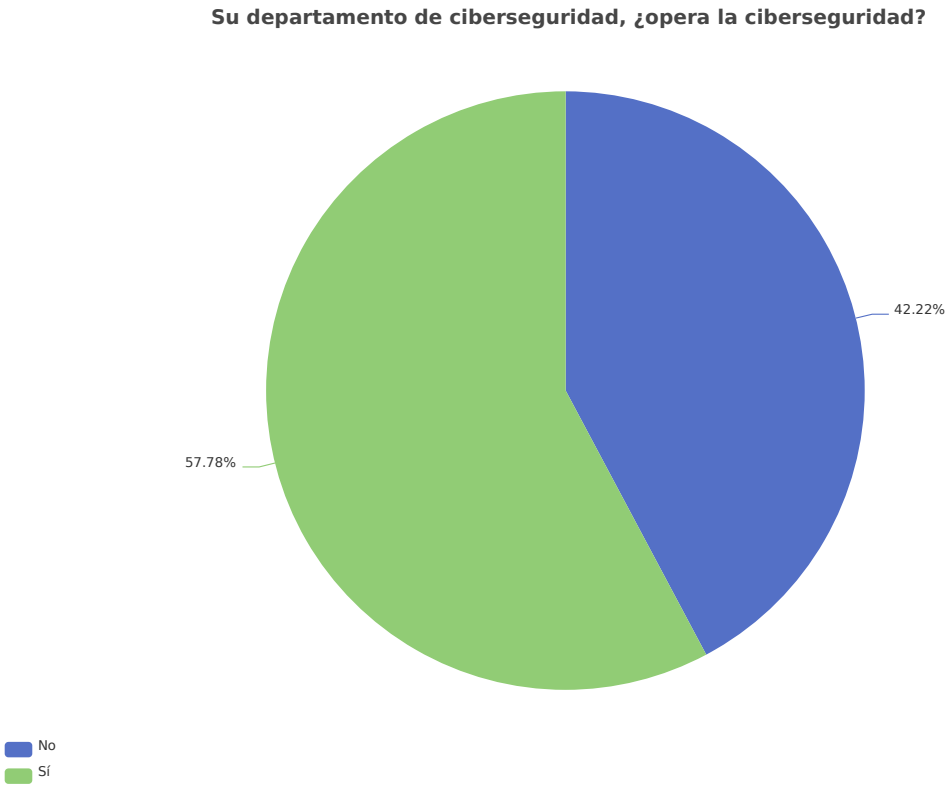


Ilustración 5: Operación de la Seguridad

Del total de las empresas analizadas, un 57,75% operaban la ciberseguridad desde el propio departamento de Ciberseguridad.

6. Influencia del contexto actual

IA: nuevas amenazas de seguridad

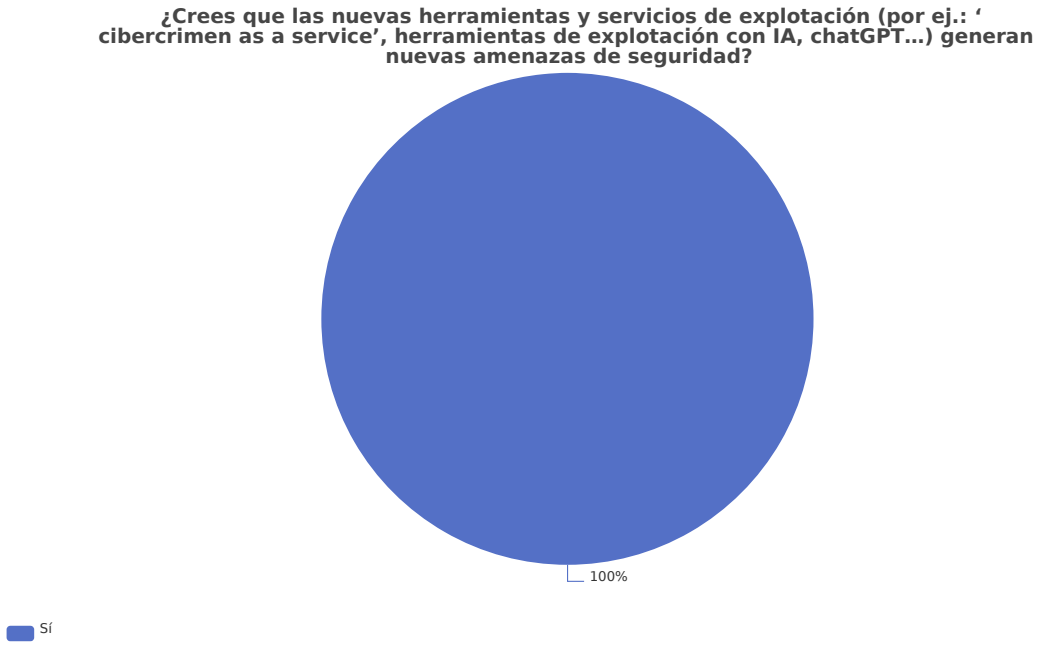


Ilustración 6: Nuevas amenazas de seguridad por herramientas de IA

Incremento de ataques por la crisis actual

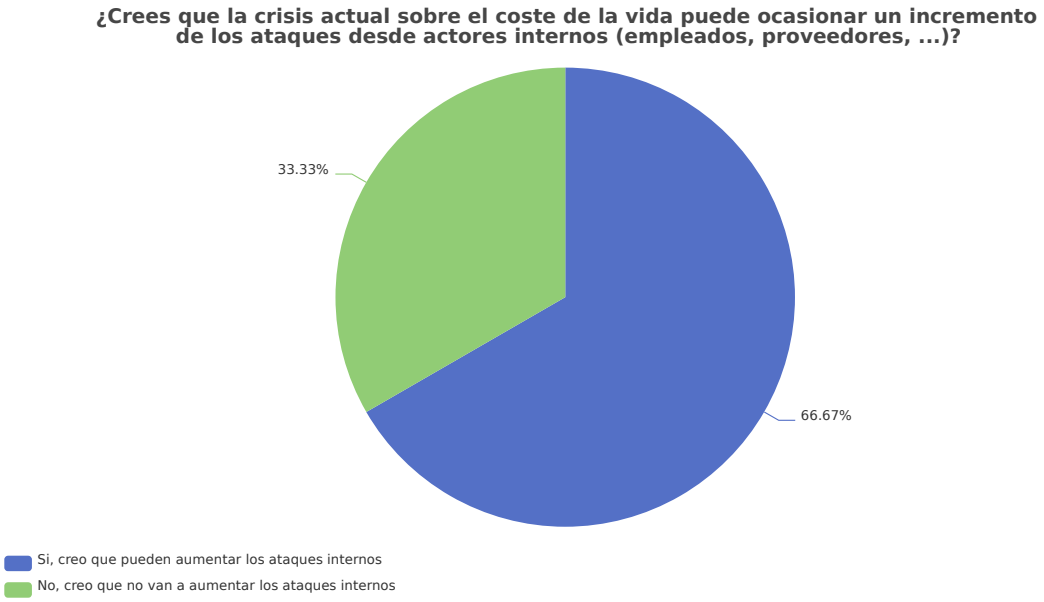


Ilustración 7: Incremento de ataques por la crisis actual

Los resultados la gráfica nos muestran como dos tercios de los encuestados percibe un aumento de los riesgos, lo que sugiere que existe una preocupación significativa en la comunidad de seguridad de la información.
Existen varias razones por las cuales los profesionales de seguridad podrían percibir un aumento en los riesgos internos durante una crisis económica: **Desesperación financiera:** Los empleados que enfrentan dificultades económicas pueden ser más propensos a considerar actividades ilícitas, como el robo de datos o la venta de información confidencial. **Insatisfacción laboral:** La presión financiera puede aumentar la insatisfacción laboral, lo que podría llevar a comportamientos desleales o incluso a la participación en actividades maliciosas. **Aumento de la vulnerabilidad interna:** En momentos de crisis económica, las empresas a menudo se ven obligadas a reducir costos, lo que podría afectar negativamente a las medidas de seguridad interna, haciendo que sea más fácil para los empleados o proveedores llevar a cabo acciones maliciosas. **Mayor dependencia de proveedores externos:** Las empresas a menudo dependen de proveedores externos para diversos servicios. Durante una crisis, la presión financiera en estos proveedores podría aumentar, lo que podría llevar a comportamientos riesgosos o incluso maliciosos.

Calidad de los servicios

Estos hallazgos indican que, si bien la mayoría de las organizaciones parecen estar gestionando eficazmente el impacto de la inflación en la calidad de sus servicios, hay un segmento notable que experimenta una disminución. Esto resalta la importancia crítica de equilibrar la gestión de costos con la provisión de servicios de alta calidad, especialmente en contextos económicos desafiantes. Es esencial que las organizaciones adopten un enfoque proactivo en la identificación y mitigación de riesgos que puedan comprometer la excelencia en la entrega de sus servicios.

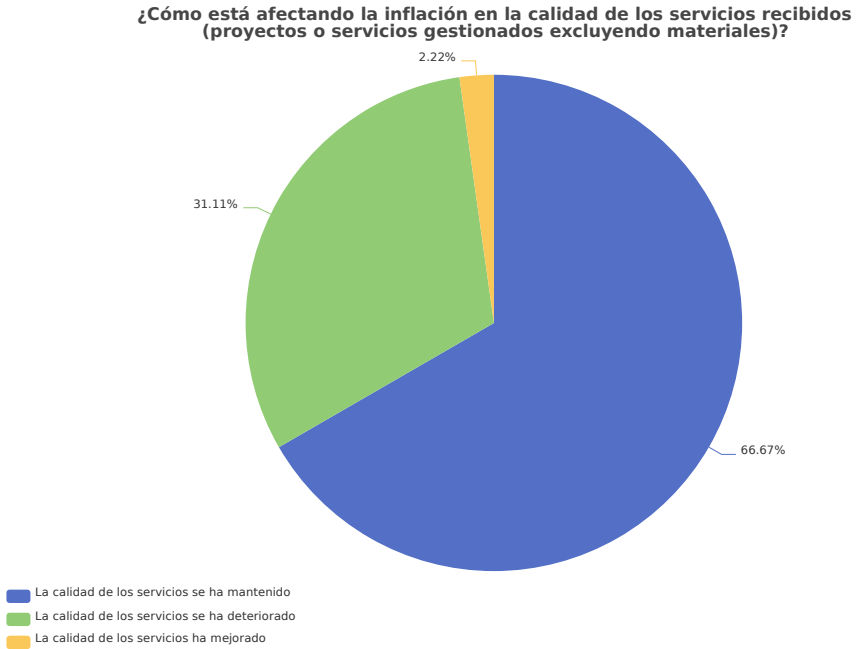


Ilustración 8: Calidad de los servicios

Variación de los presupuestos

En general, estos resultados sugieren una diversidad de enfoques en la gestión de presupuestos de seguridad en el contexto de la inflación. La asignación de recursos para la seguridad puede depender de la percepción de riesgos específicos, la cultura organizacional, y las estrategias generales de gestión financiera. Es esencial que las organizaciones encuentren un equilibrio adecuado entre la inversión en seguridad y la gestión eficiente de los recursos financieros.

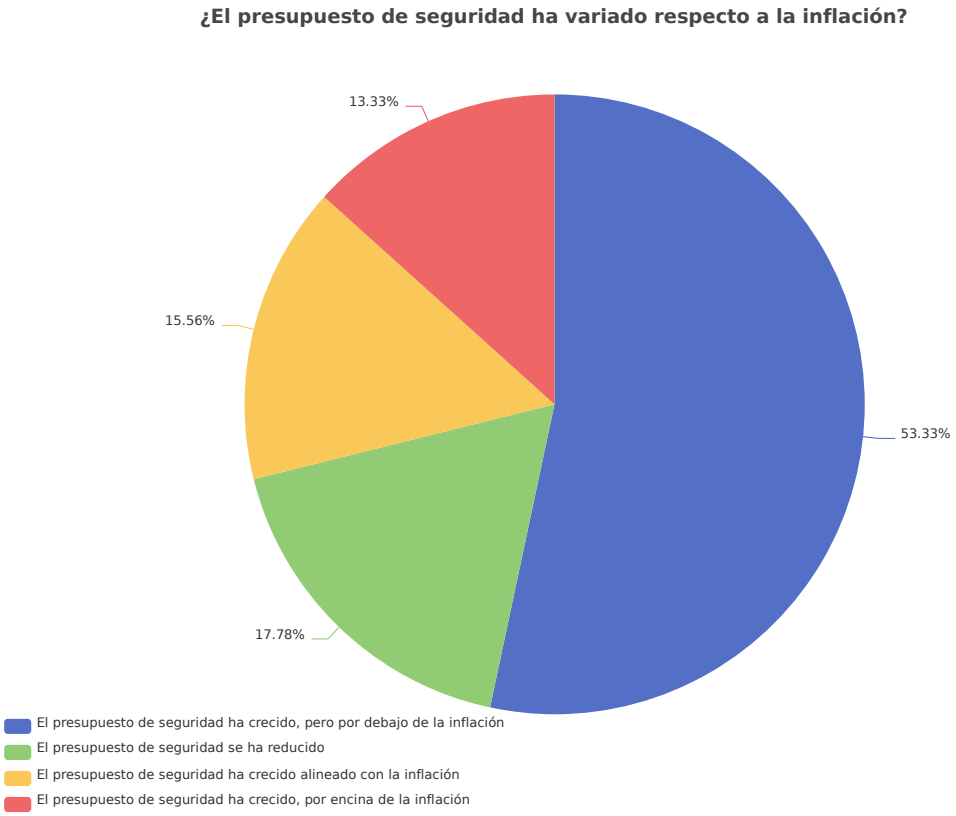


Ilustración 9: Variación de los presupuestos

IV 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

isms BARCELONA INTERNATIONAL INFORMATION SECURITY COMMUNITY