www.ismsforum.es

III Indicador de madurez en ciberseguridad

OBSERVATORIO DE LA CIBERSEGURIDAD

Una iniciativa de

isms forum

isms BARCELONA

Noviembre 2022

III 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
DISEÑO/MAQUETACIÓN	Cynthia Rica

CONTENIDOS

Introducción

ISMS Forum y su iniciativa: el Observatorio de la Ciberseguridad

ISMS Forum es una organización sin ánimo de lucro fundada en enero de 2007 para promover el desarrollo, conocimiento y cultura de la Seguridad de la Información en España y actuar en beneficio de toda la comunidad implicada en el sector. Creada con una vocación plural y abierta, se configura como el principal foro nacional especializado de debate para empresas, organizaciones públicas y privadas, investigadores y profesionales donde colaborar, compartir experiencias y conocer los últimos avances y desarrollos en materia de Seguridad de la Información. Toda su actividad se desarrolla en base a los valores de transparencia, independencia, objetividad y neutralidad.

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

La Asociación organiza su actividad a través de distintas iniciativas, que abordan desde una perspectiva global o especializada la Seguridad de la Información: Jornadas Internacionales, Data Privacy Institute, Cloud Security Alliance, Cyber Security Center, IoT Security Center, workshops sobre materias concretas y formación especializada en protección de datos y ciberseguridad. Además gestiona las certificaciones Certified Data Privacy Professional (CDPP), Certificación de Delegado de Protección de Datos (CDPD), Certified Cyber Security Professional (CCSP) y promueve el Certificate Of Cloud Security Knowledge (CCSK).

En 2020, el marco asociativo de ISMS Forum se consolidó como la mayor comunidad de expertos y organizaciones con interés y responsabilidades en materia de seguridad de la información, promoviendo la formación y excelencia de sus asociados, facilitándoles cauces de interlocución con las administraciones y autoridades de control, y fomentando el intercambio de conocimientos entre los principales actores y expertos implicados en el sector para impulsar y contribuir a la mejora de la ciberseguridad en España.

Unido a lo anterior, la Asociación dio un paso más con el objetivo crear un estado de conciencia sobre la necesidad de formar y sensibilizar, aportando indicadores que permitan gestionar los riesgos derivados de la dependencia actual de la sociedad respecto a las Tecnologías de la Información y la Comunicación (TIC), siendo un aspecto clave para asegurar el desarrollo socioeconómico del país.

Para alcanzar la misión anteriormente descrita, la Asociación identifica la necesidad de actuar como referente y ofrecer una plataforma para el desarrollo de indicadores que permita la puesta en común y el análisis de aquellas áreas que generan mayor preocupación y, en general, de los riesgos y retos más relevantes. Se constituye de esta manera el primer Observatorio de la Ciberseguridad para empresas y profesionales del sector.

> “Se constituye de esta manera el primer Observatorio de la Ciberseguridad para empresas y profesionales del sector.

Objetivos del Observatorio de la Ciberseguridad

- **Plataforma para el análisis del nivel de madurez, evolución y nuevos fenómenos en el ámbito de la seguridad de la información.**
- **Generación de indicadores nacionales sobre el estado de la Ciberseguridad en empresas y entidades privadas y públicas.**
- **Promoción de conocimiento e investigación.**
- **Generación de métricas y referencias nacionales.**
- **Colaboración e interlocución con instituciones y reguladores.**

1 ESTUDIO SOBRE EL NIVEL DE MADUREZ EN CIBERSEGURIDAD DE LA EMPRESA ESPAÑOLA

Según define la gestión de riesgos el Instituto Nacional de Estándares y Tecnología (NIST) de EEUU, se trata del proceso continuo de identificación, evaluación y respuesta al riesgo; y para gestionar el riesgo, las organizaciones deben comprender la probabilidad de que ocurra un evento y los posibles impactos resultantes.

Esta es la premisa con la que el Observatorio de la Ciberseguridad de ISMS Forum pone a disposición del mercado la tercera edición de su estudio, con la finalidad de generar claridad sobre el estado del arte de la ciberseguridad empresarial nacional y para facilitar información de utilidad para empresas y profesionales con la generación de un indicador anual que permita interpretar de una mejor manera la evolución interanual de los riesgos cibernéticos y su relación con terceros factores y fenómeno.

El indicador de nivel de madurez en ciberseguridad utiliza el marco metodológico basado en el estándar creado por el Instituto Nacional de Estándares y Tecnología (NIST) en 2013. Dicho marco ha sido globalmente utilizado por organizaciones de cualquier sector o tamaño, sirviendo de referencia a las organizaciones que apliquen los principios y buenas prácticas para medir y mejorar sus capacidades de Identificación, Protección, Detección, Respuesta y Recuperación. Cabe aclarar que NIST proporciona un marco de políticas de orientación de ciberseguridad no vinculantes, que cada organización deberá adaptar a sus necesidades, regulación aplicable y naturaleza propias.

> “
>
> (...) ISMS Forum pone a disposición del mercado una herramienta de evaluación a través del indicador nacional de madurez en ciberseguridad derivados de la dependencia actual de la sociedad respecto a las Tecnologías de la Información y la Comunicación.

En esta tercera edición del Observatorio se ha añadido un indicador adicional a los analizados en ediciones anteriores. Un indicador temporal para analizar la influencia del contexto actual, en cuanto a evolución de las ciberamenazas, impacto en recursos dedicados a ciberseguridad, volumen de trabajo en el área de ciberseguridad, así como, sus efectos en la cadena de suministro.

Como elemento de valor añadido en la evaluación de los resultados obtenidos en la encuesta, se ha realizado un análisis factorial para detectar patrones similares en las respuestas que muestren cómo se estructura la toma de decisiones en ciberseguridad en las empresas españolas.

El estudio realizado por ISMS Forum ha tenido por objeto la aplicación del Marco elaborado por NIST en una muestra formada por 85 organizaciones que operan en el ámbito territorial nacional, contando tanto con empresas multinacionales como nacionales. No se ha recopilado 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

(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.

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 LA MUESTRA

En la presente edición, hemos contado con la participación de 85 empresas, de las cuales un 38% facturan más de 1.000 millones de Euros y el 32% más de 100. El 91% de los encuestados ocupan puestos de responsabilidad o son especialistas de seguridad de la información.

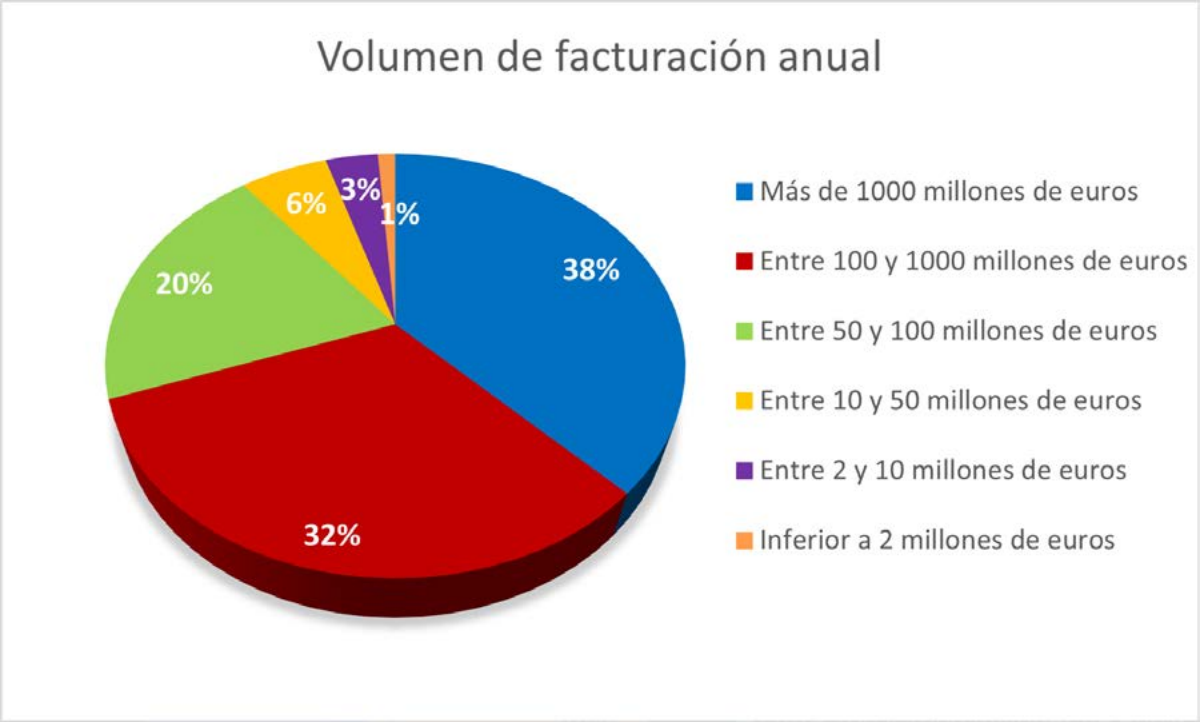


Ilustración 1: Volumen de facturación anual de las empresas participantes.

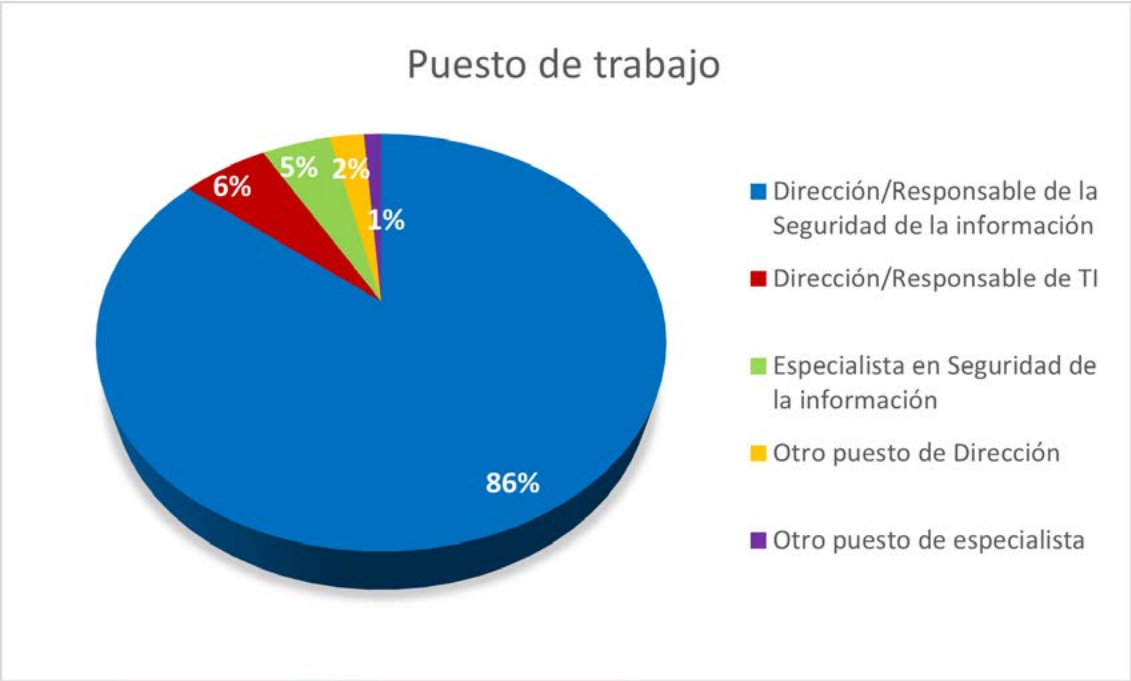


Ilustración 2: Puesto de trabajo ocupado por el encuestado .

Ilustración 3: Sector de actividad de las empresas participantes.

4 NIVEL DE MADUREZ

Principales Indicadores

Se inicia la exposición de resultados del presente Estudio con el análisis del grado de madurez global reflejado en el indicador.

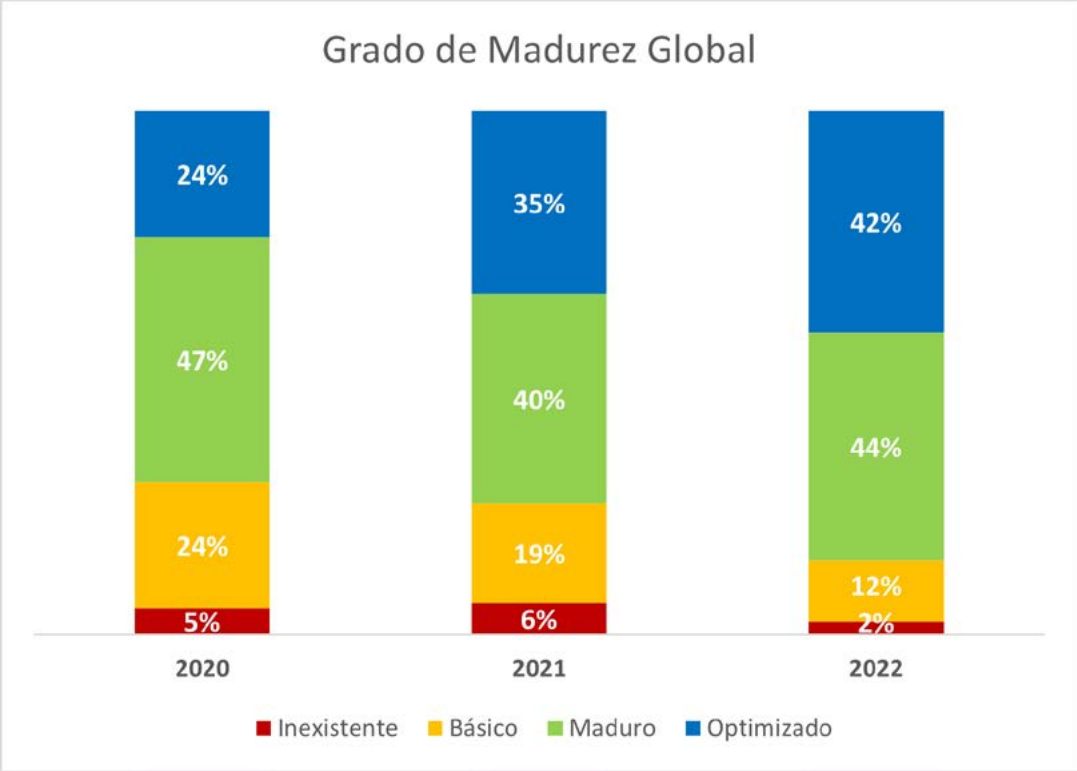


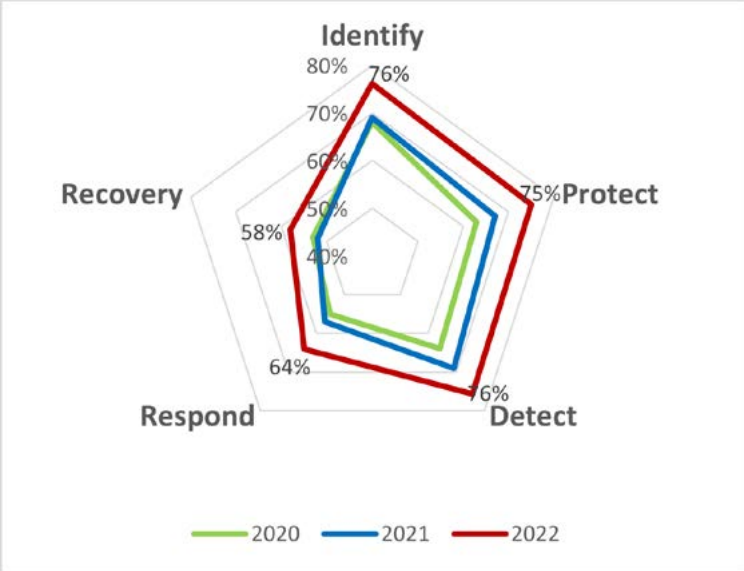
Ilustración 4: Evolución del grado de madurez .

La primera conclusión que podemos extraer es la de una mejora generalizada de los niveles de madurez de los controles, que sigue la tendencia iniciada en 2021. Se observa un incremento de los controles en niveles "optimizado" (+7%) y "maduro" (+4%) que se traduce en un 42% y 44% global, respectivamente. Así mismo, si los consideramos de forma agrupada, la evolución en estos dos niveles de madurez más elevados se observa que el incremento es superior al observado en la anterior edición, con un 86%, respecto al 75% del año 2021.

Consecuentemente se han reducido los porcentajes de controles en niveles "básico" (-7%) e "inexistente" (-4%). En este último nivel se encuentran únicamente 2 empresas, respecto a 4 empresas en la edición anterior.

Nivel de Madurez por Dominio NIST

Sector	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER	Nivel de madurez
Actividades administrativas y servicios auxiliares	94,44%	91,67%	91,67%	86,11%	83,33%	89,44%
Agricultura, ganadería, silvicultura y pesca	88,89%	77,78%	100,00%	88,89%	66,67%	84,44%
Suministro de energía eléctrica, gas, vapor y aire acondicionado	86,67%	93,33%	93,33%	77,78%	71,11%	84,44%
Suministro de agua, actividades de saneamiento, Gestión de Residuos y Descontaminación	92,59%	92,59%	86,11%	79,63%	70,37%	84,26%
Actividades financieras y de seguros	82,68%	80,72%	82,84%	73,20%	69,28%	77,75%
Transporte y almacenamiento	82,41%	85,19%	81,94%	63,89%	57,41%	74,17%
Industrias Extractivas	72,22%	77,78%	75,00%	72,22%	66,67%	72,78%
Actividades inmobiliarias	72,22%	66,67%	75,00%	66,67%	66,67%	69,44%
Información y comunicaciones	78,40%	72,22%	70,37%	62,96%	62,96%	69,38%
Construcción	77,78%	75,00%	75,00%	63,89%	38,89%	66,11%
Actividades sanitarias y de servicios sociales	75,93%	81,48%	62,50%	54,63%	55,56%	66,02%
Industria manufacturera	60,56%	67,22%	80,00%	62,78%	48,89%	63,89%
Comercio al por mayor y por menor; Reparación de vehículos de motor y motocicletas	73,33%	57,78%	73,33%	52,22%	48,89%	61,11%
Actividades artísticas, recreativas y de entretenimiento	59,72%	54,17%	72,92%	59,72%	55,56%	60,42%
Administración pública y defensa	76,19%	78,57%	55,95%	48,41%	42,86%	60,40%
NS/ NC	66,67%	62,96%	63,89%	53,70%	44,44%	58,33%
Actividades profesionales, científicas y técnicas	83,33%	55,56%	58,33%	38,89%	33,33%	53,89%
Otros Servicios	55,56%	38,89%	41,67%	55,56%	77,78%	53,89%
Hostelería	38,89%	38,89%	83,33%	50,00%	0,00%	42,22%



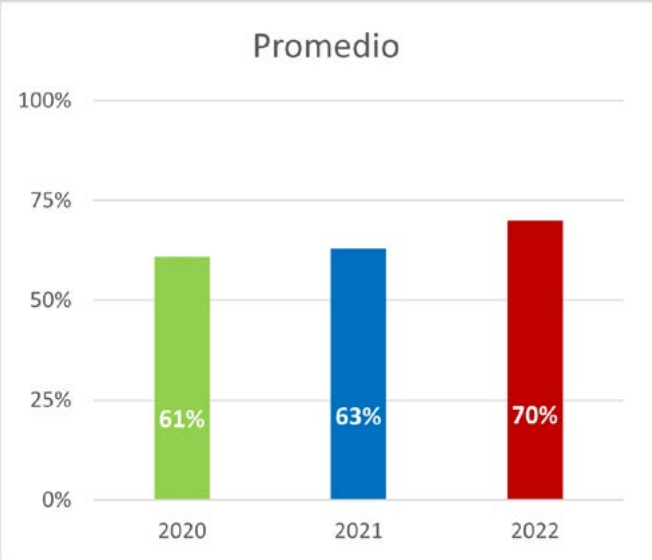


Ilustración 5 y 6: Evolución y promedio de los indicadores de madurez.

En la presente edición se observa una mejora significativa en todos los ámbitos analizados, con un incremento de 7 puntos porcentuales respecto a los resultados de la edición anterior.

El ámbito de Protect es el que más crece con un 8%, seguido de Identify, Detect y Respond con un 7%. Por último Recovery ha mejorado también respecto al año anterior, con un 6% de incremento en su grado de madurez promedio.

Aún con dichos incrementos, Respond y Recover siguen siendo los dominios que muestran una necesidad de mejora.

Grado de madurez por número de empleados

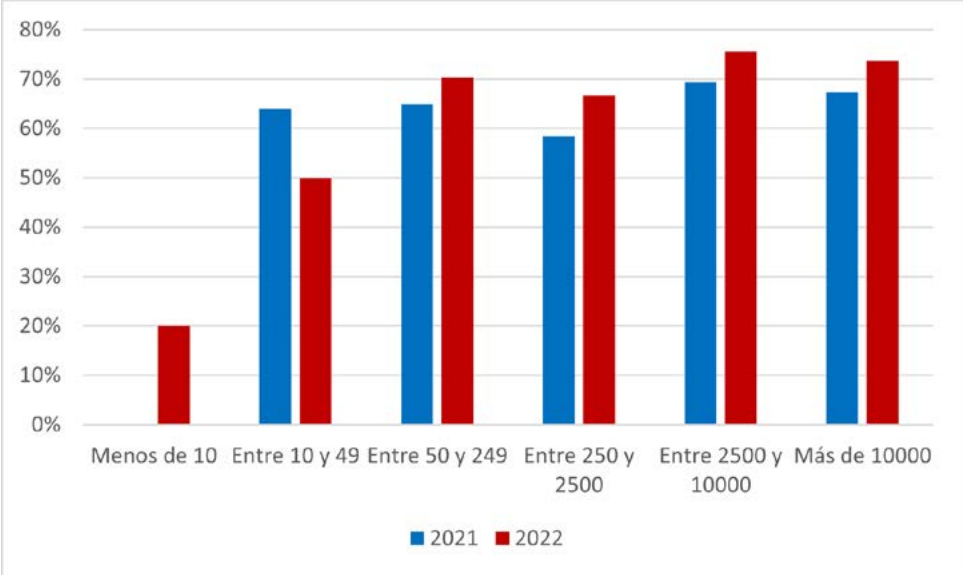


Ilustración 7: Evolución del grado de madurez en relación con el tamaño de las empresas.

Grado de madurez por facturación

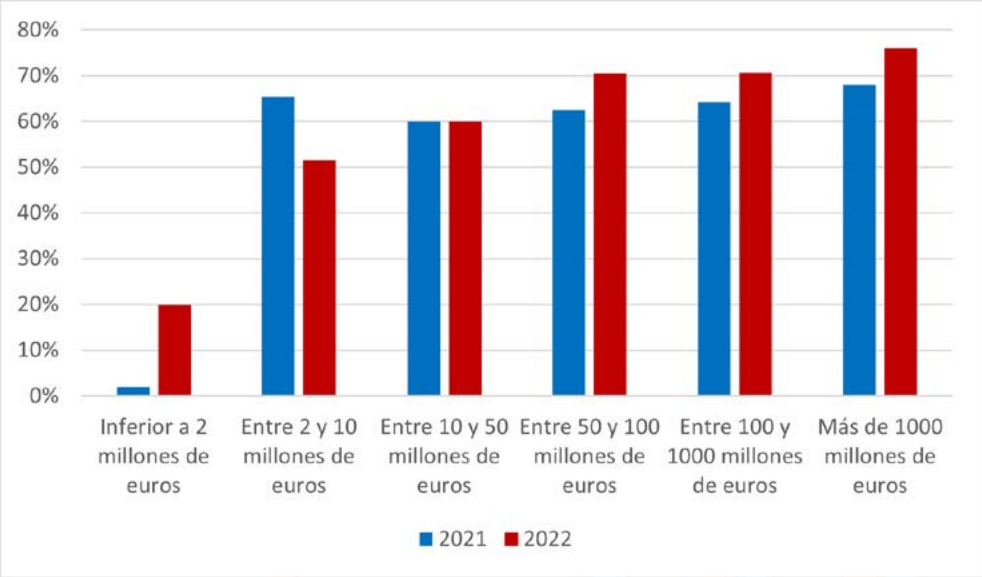
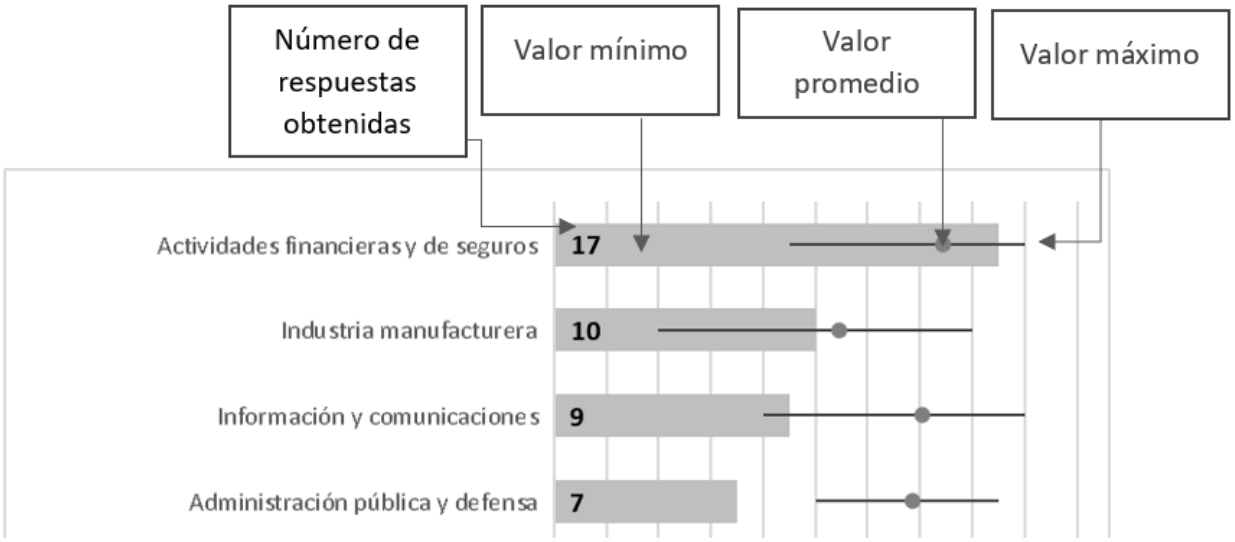


Ilustración 8: Evolución del grado de madurez en relación con la facturación anual.

Grado de madurez por Dominio NIST y Sector Empresarial

A continuación, se muestran los resultados obtenidos para cada uno de los Dominios del NIST, y por Sector Empresarial. En el gráfico de barras, se especifican el número de empresas que han cumplimentado la encuesta para cada uno de los Sectores representados. El gráfico de stock superpuesto al de barras, se representa la dispersión en las respuestas con los valores mínimos y máximos, así como la media aritmética de las mismas mediante las esferas.



Se muestran también las diferencias obtenidas en los niveles de madurez para cada una de las preguntas respecto a las ediciones anteriores. De este modo se analizan a nivel granular las tendencias para cada una de las áreas tratadas por Dominio NIST.

DOMINIO 1: IDENTIFICAR

DOMINIO 2: PROTEGER

DOMINIO 3: DETECTAR

DOMINIO 4: RESPONDER

DOMINIO 5: RECUPERAR

DOMINIO 1: IDENTIFICAR

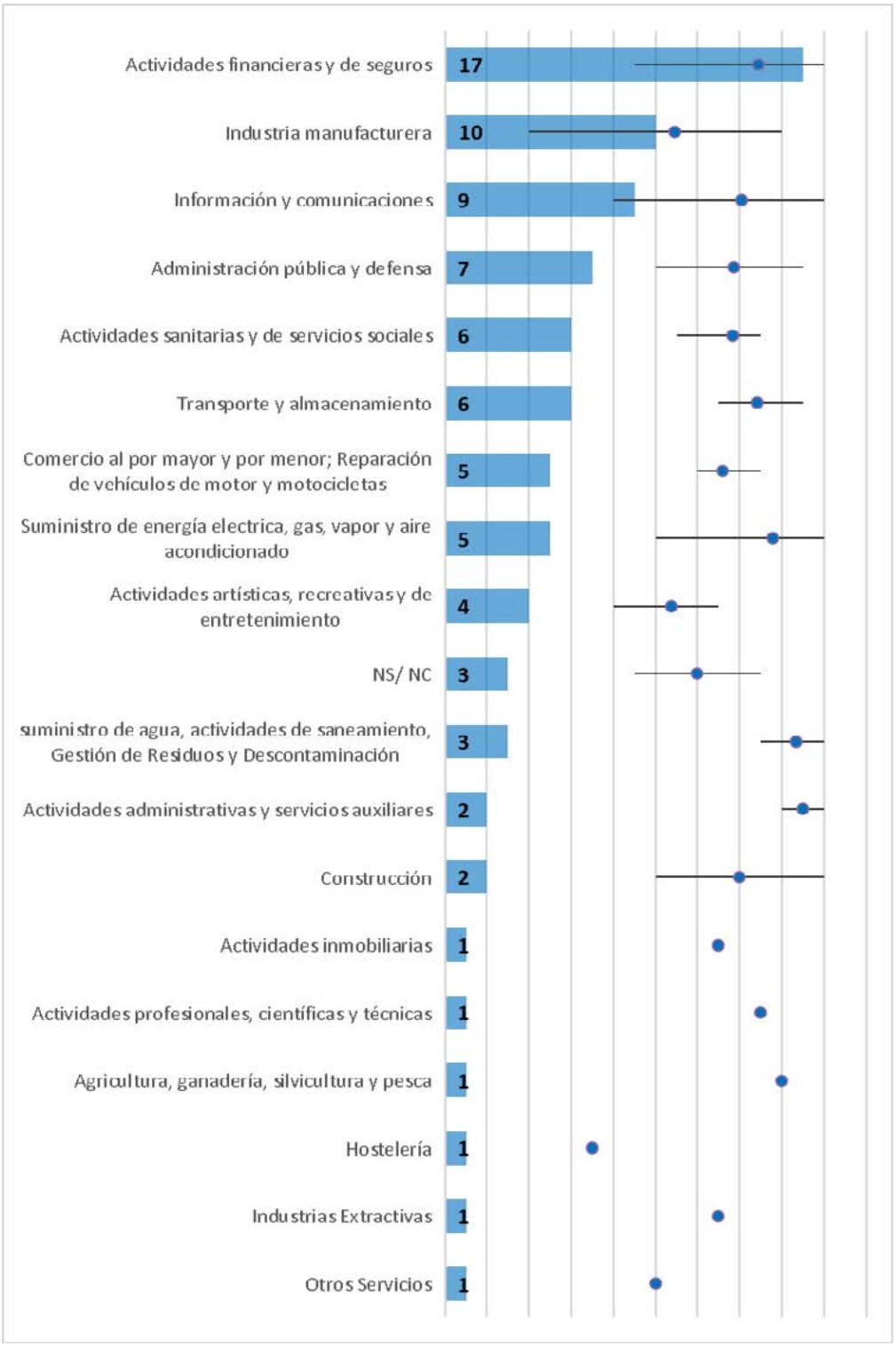


Ilustración 9: Indicador "Identificar" por sector de actividad.

Los sectores Financiero y Seguros, Información y Comunicaciones, Administración Pública y Defensa muestran mayor madurez en el dominio "identificar", teniendo en cuenta la representación de la muestra. Cabe destacar la dispersión de la respuesta en los sectores Manufacturero e Información y Comunicaciones.

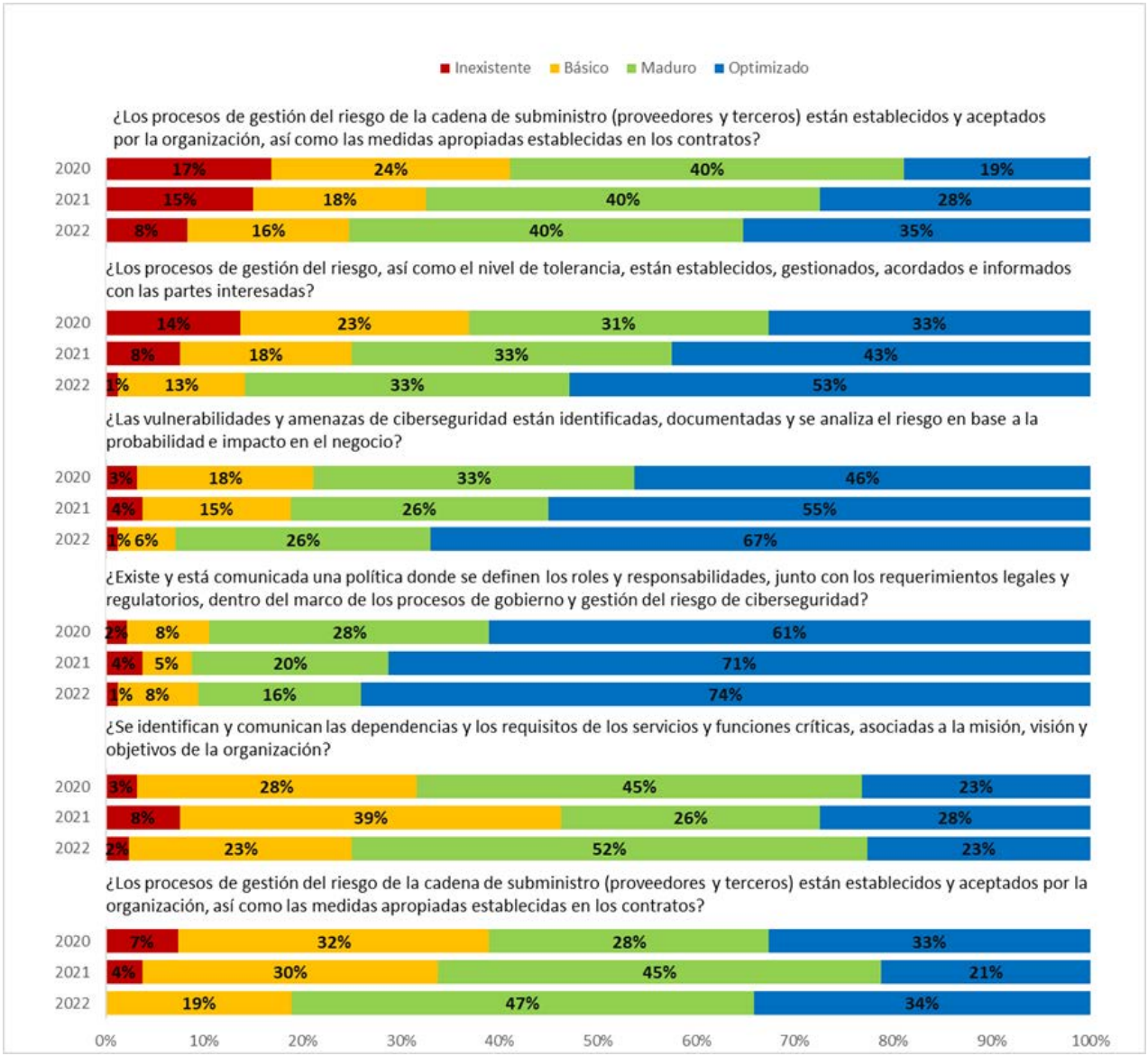


Ilustración 10: Evolución del grado de madurez de "Identificar".

El dominio "Identificar" es uno de los que mayores mejoras ha alcanzado respecto al Estudio anterior, con un 7% de mejora. Desde el I Estudio de Madurez ha pasado de una madurez global del 68% en 2020, al 69% en 2021 y hasta el 76% alcanzado en la presente Edición, situándose a la par con el Dominio de "Detectar" y "Responder".

La principal mejora proviene de las organizaciones que identifican las vulnerabilidades y amenazas y analizan su riesgo asociado, alcanzando un 26% de organizaciones un nivel Maduro y un 67% de ellas un nivel optimizado.

Del mismo modo, las organizaciones que cuentan procesos de gestión del riesgo tanto interno como en relación con terceros, mejoran en general respecto a ediciones anteriores.

DOMINIO 2: PROTEGER

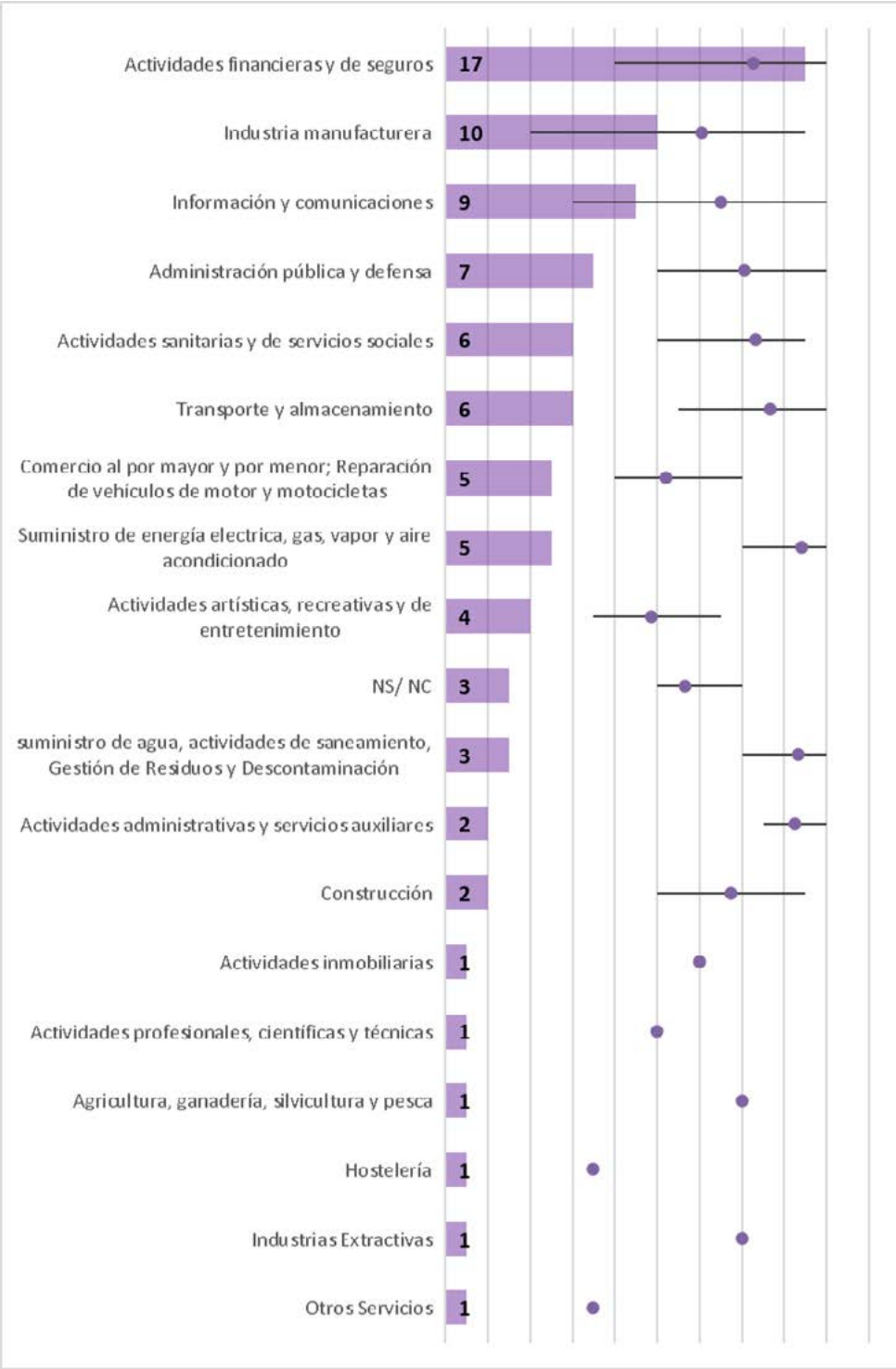


Ilustración 11: Indicador "Proteger" por sector de actividad.

En esta ocasión el dominio de "Proteger" lo lidera de Los sectores Financiero y Seguros, Suministro de energía, Transporte y Actividades Sanitarias, teniendo en cuenta la representación de la muestra. Cabe destacar también la dispersión de la respuesta en los sectores Manufacturero e Información y Comunicaciones.

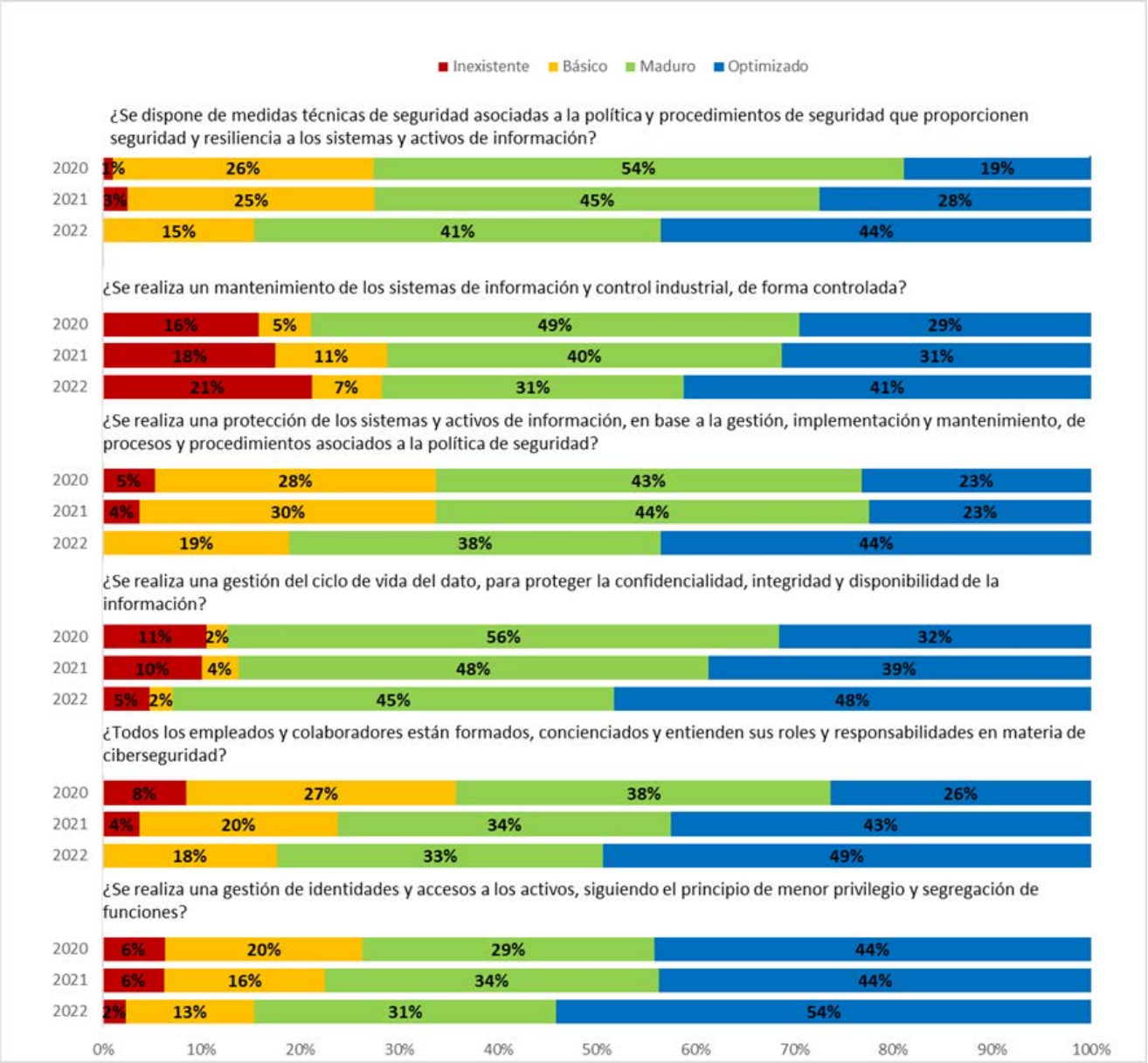


Ilustración 12: Evolución del grado de madurez de "Proteger".

El dominio "Proteger" es el que lidera el grupo que mayores mejoras ha alcanzado respecto al Estudio anterior, con un 8%. Desde el I Estudio de Madurez ha pasado de una madurez global del 63% en 2020, al 67% en 2021 y hasta el 75% alcanzado en la presente Edición.

La principal mejora proviene de las organizaciones que realizan una protección de los sistemas y activos de información, alcanzando un 38% de organizaciones un nivel Maduro y un 44% de ellas un nivel optimizado.

En cambio el apartado de mantenimiento de los sistemas de información y control industrial sufre un ligero retroceso en el nivel de madurez "Inexistente" pasando del 18% al 21%.

DOMINIO 3: DETECTAR

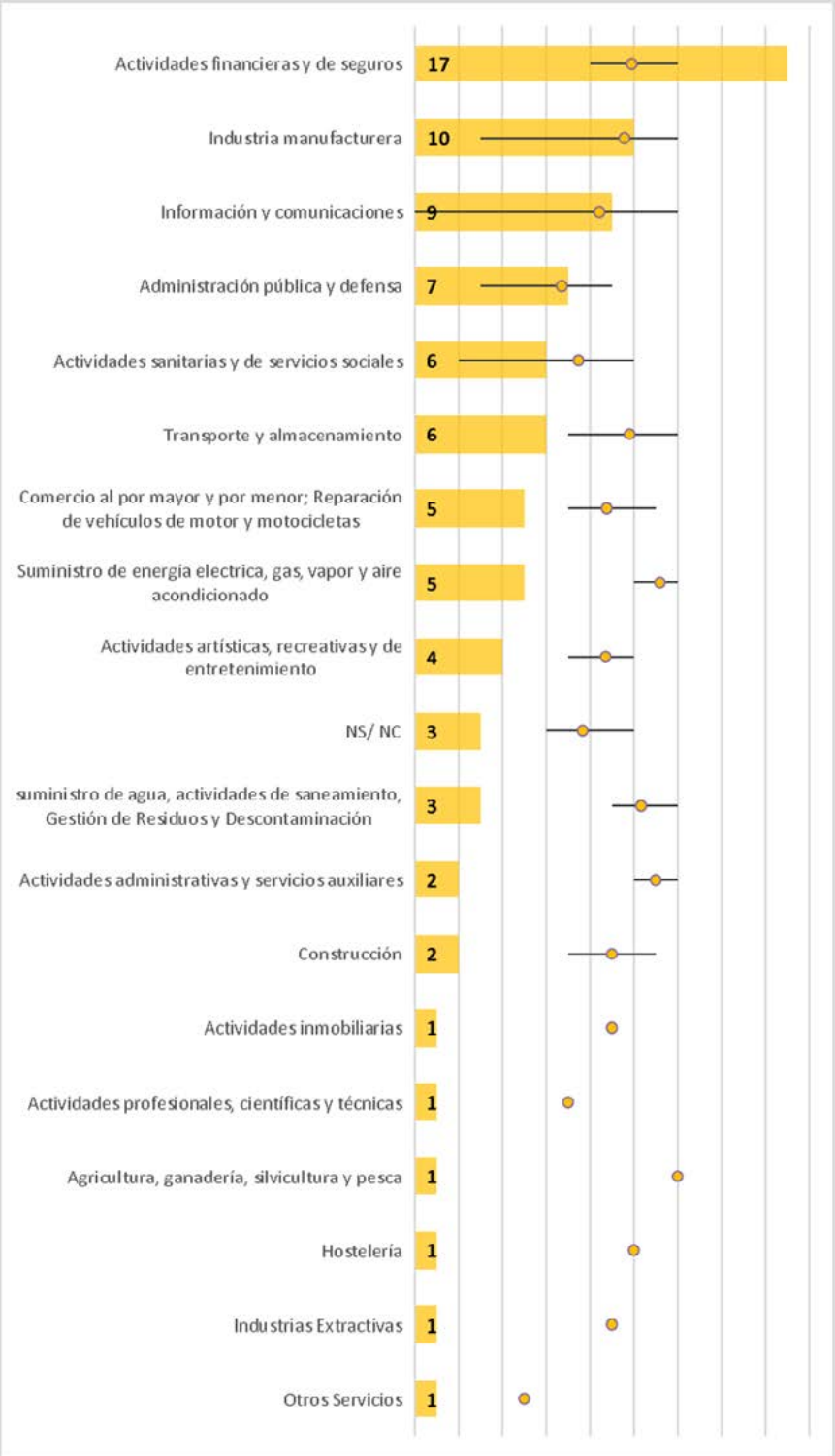


Ilustración 13: Indicador "Detectar" por sector de actividad.

De nuevo el Sector Financiero y de Seguros lidera el dominio por número absoluto de respuestas, alcanzando además un elevado valor promedio de madurez, con una baja dispersión. Sectores como la Industria Manufacturera o de Información y Comunicaciones alcanzan igualmente un alto nivel de madurez pero, sin embargo, la dispersión de sus resultados es muy elevada.

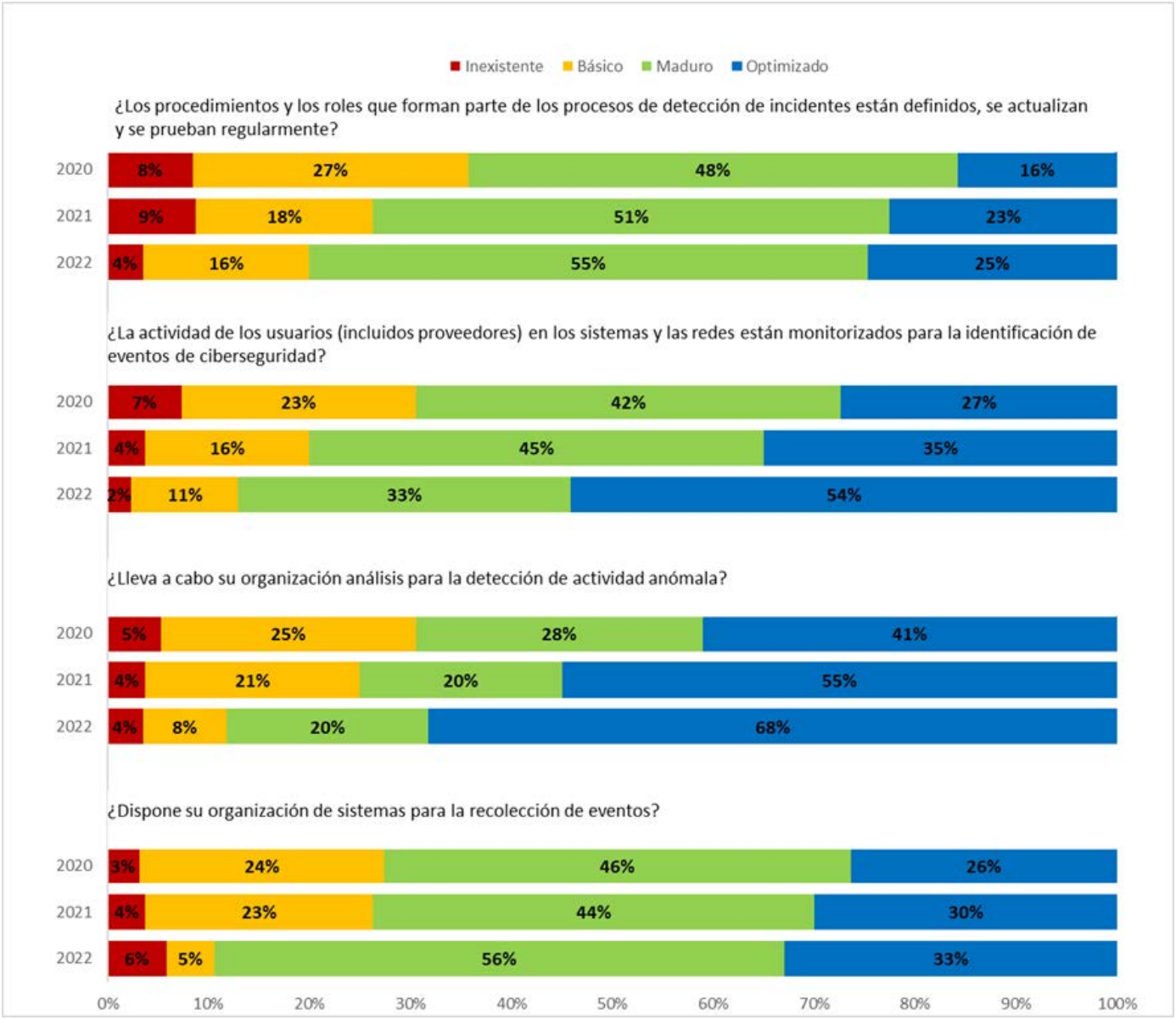


Ilustración 14: Evolución del grado de madurez de "Detectar".

El dominio "Proteger" es el que lidera el grupo que mayores mejoras ha alcanzado respecto al Estudio anterior, con un 8%. Desde el I Estudio de Madurez ha pasado de una madurez global del 63% en 2020, al 67% en 2021 y hasta el 75% alcanzado en la presente Edición.

La principal mejora proviene de las organizaciones que realizan una protección de los sistemas y activos de información, alcanzando un 38% de organizaciones un nivel Maduro y un 44% de ellas un nivel optimizado.

En cambio el apartado de mantenimiento de los sistemas de información y control industrial sufre un ligero retroceso en el nivel de madurez "Inexistente" pasando del 18% al 21%.

DOMINIO 4: RESPONDER

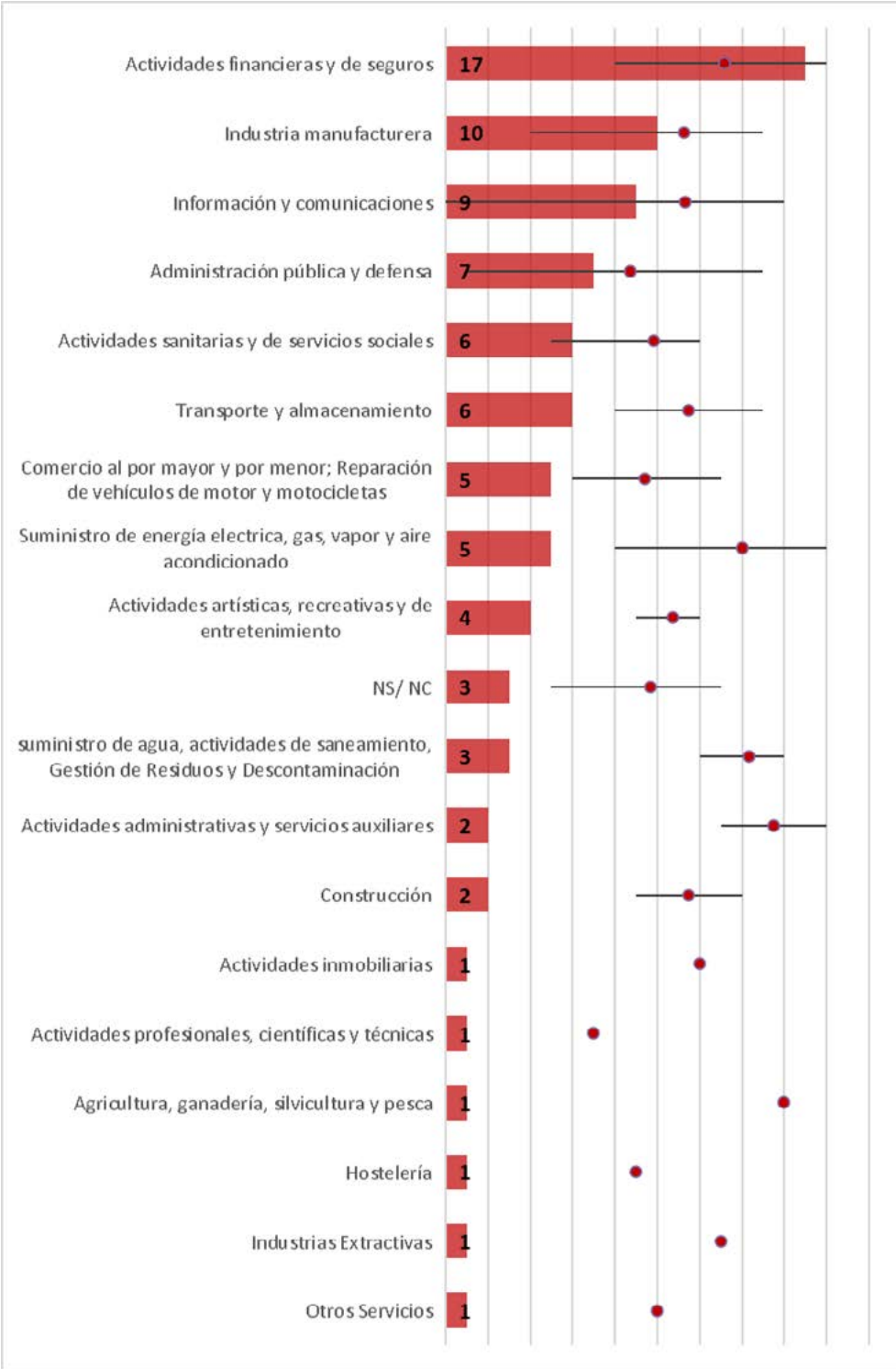


Ilustración 15: Indicador "Responder" por sector de actividad.

El dominio de "Responder" presenta en general un nivel de dispersión muy elevado entre las respuestas de organizaciones del mismo sector. Esto indica diferentes grados de madurez, lo que es consistente con resultados de años anteriores. Destaca el alto grado de madurez promedio de las organizaciones del sector de suministro energético y gas.

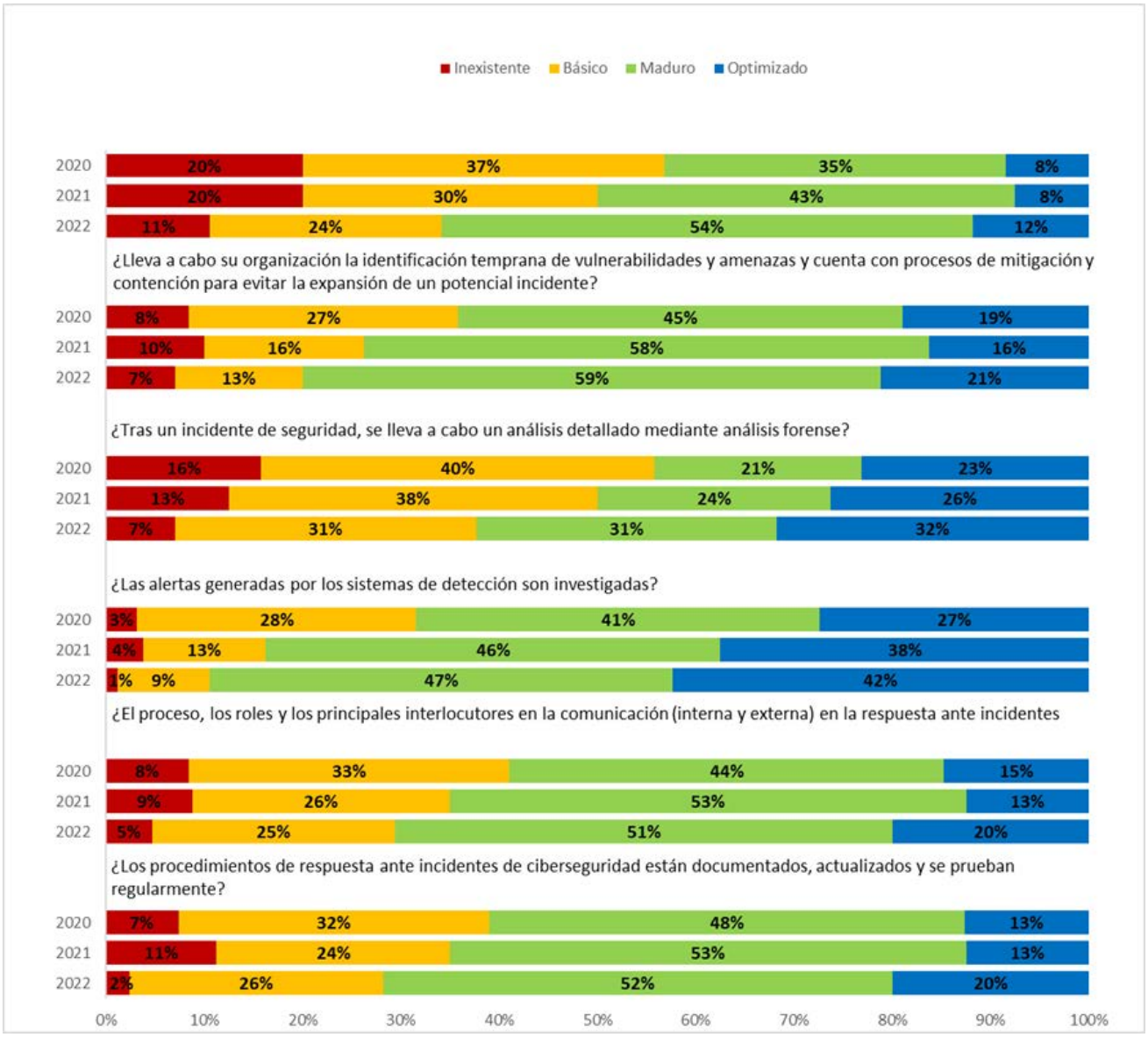


Ilustración 16: Evolución del grado de madurez de "Responder".

De manera consistente con Estudios anteriores, el dominio "Responder" presenta un nivel de madurez promedio menor que dominios precedentes. Sin embargo, la mejora alcanzada en la madurez promedio en este III Estudio sobre estudios anteriores es significativa, siendo de un 64%, sobre un 57% de madurez global en 2021 y un 55% 2020.

La principal mejora proviene de las organizaciones que tras un incidente de seguridad llevan a cabo un análisis forense, alcanzando un 31% de organizaciones un nivel Maduro y un 32% de ellas un nivel optimizado.

Del mismo modo, las organizaciones que cuentan con un proceso formal para la mejora continua de la respuesta ante incidentes en base a lecciones aprendidas de incidentes pasados han aumentado considerablemente, estando en este III Estudio un 54% de ellas en un nivel Maduro (sobre el 43% de 2021).

El único apartado donde la mejoría no es significativa es en lo relativo a las alertas generadas por los sistemas de información y si estas son investigadas, aumentando un 1% el nivel de madurez "Maduro" y un 4% el nivel de madurez "Optimizado".

DOMINIO 4: RESPONDER

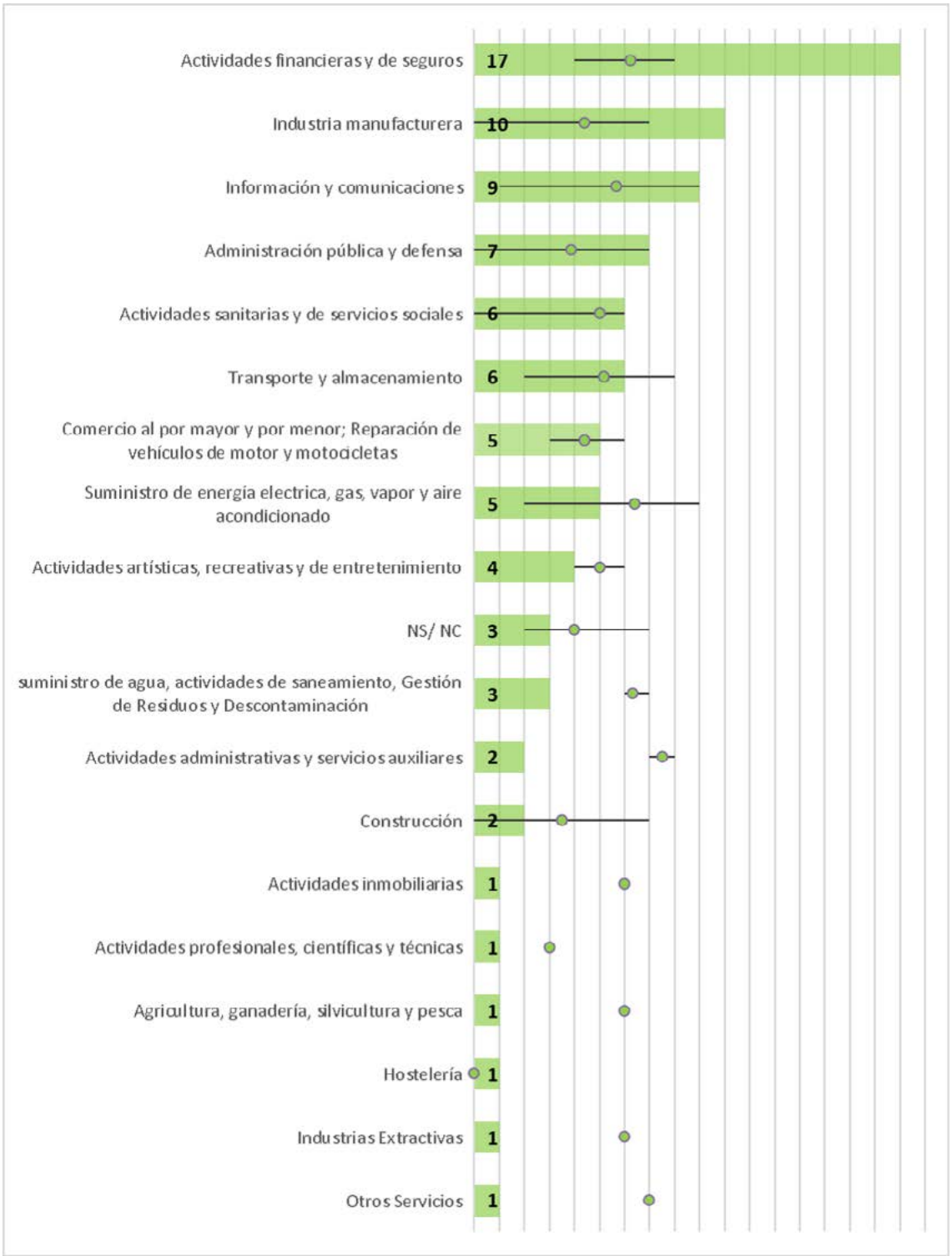


Ilustración 17: Indicador "Recuperar" por sector de actividad.

El dominio de "Recuperar" presenta un nivel de madurez más bajo que el resto de los dominios, si bien el grado de dispersión general no es elevado, a excepción de sectores como la industria Manufacturera o de Información y Comunicaciones.

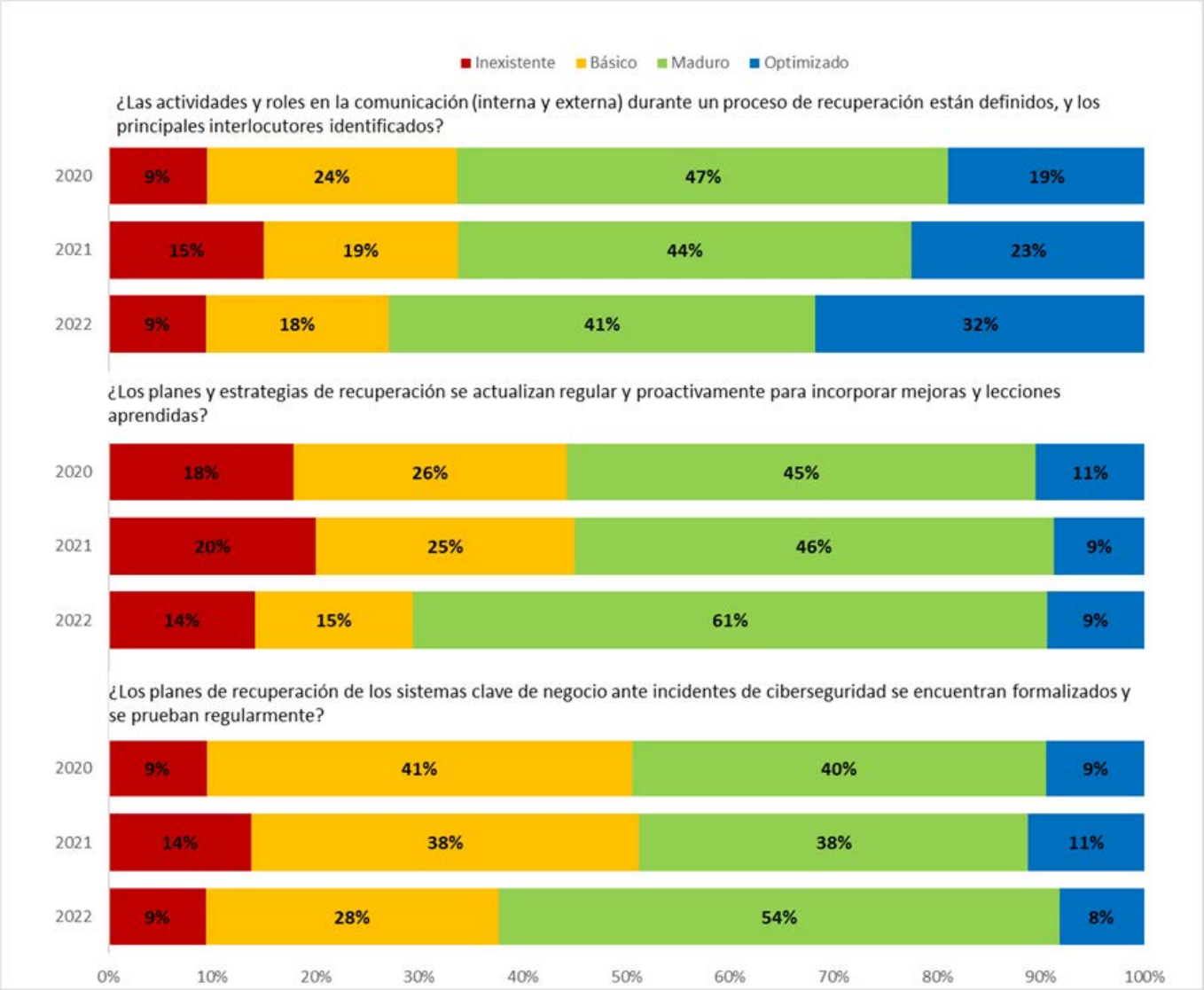


Ilustración 18: Evolución del grado de madurez de "Recuperar".

De nuevo, de manera consistente con Estudios anteriores, el dominio "Recuperar" tiene el nivel de madurez promedio más bajo de los 5 dominios analizados. Ello tiene sentido puesto que el orden de cada uno de los dominios sigue una lógica de madurez; es decir, las organizaciones trabajan inicialmente en dominios con Identificar o Proteger antes de pasar a dominios más centrados en la Respuesta y la Recuperación. Sin embargo, hay que destacar que en este III Estudio, el grado de madurez global del dominio de Recuperar es del 58%, lo que supone una mejora del 6%, sobre un 52% alcanzado en 2021.

La principal mejora se concentra en las organizaciones que han definido actividades y roles durante el proceso de recuperación, donde ya un 32% de organizaciones declaran un nivel "Optimizado". También se aprecian mejoras en las organizaciones que actualizan regular y proactivamente los planes y estrategias de recuperación, incorporando lecciones aprendidas, donde hasta un 61% de organizaciones declaran un nivel "Maduro" (+15% comparado con 2021)

El resto de las cuestiones planteadas en el dominio no presentan mejoras muy significativas, aunque el avance es positivo en todas ellas.

5 RECURSOS Y ORGANIZACIÓN

Recursos y Personal Interno

Los datos obtenidos permiten analizar la distribución de los recursos destinados a ciberseguridad. Un 60% de las organizaciones analizadas disponen de entre 1 y 5 personas en el área de ciberseguridad, un 19% tienen entre 5 y 15 personas, un 15% entre 15 y 50 personas y únicamente un 6% tienen más de 50 personas en el área de ciberseguridad.

Ilustración 19: Personal interno en ciberseguridad.

Si entramos en detalle, un 58% de las empresas con entre 1 y 5 recursos de ciberseguridad (un 35% del total de la muestra) se corresponde a empresas con una facturación superior a 100 millones de euros. Este porcentaje ha disminuido con respecto a 2021 en el que los datos mostraban que un 72% de las empresas con entre 1 y 5 recursos de ciberseguridad tenían una facturación superior a 100 millones de euros:

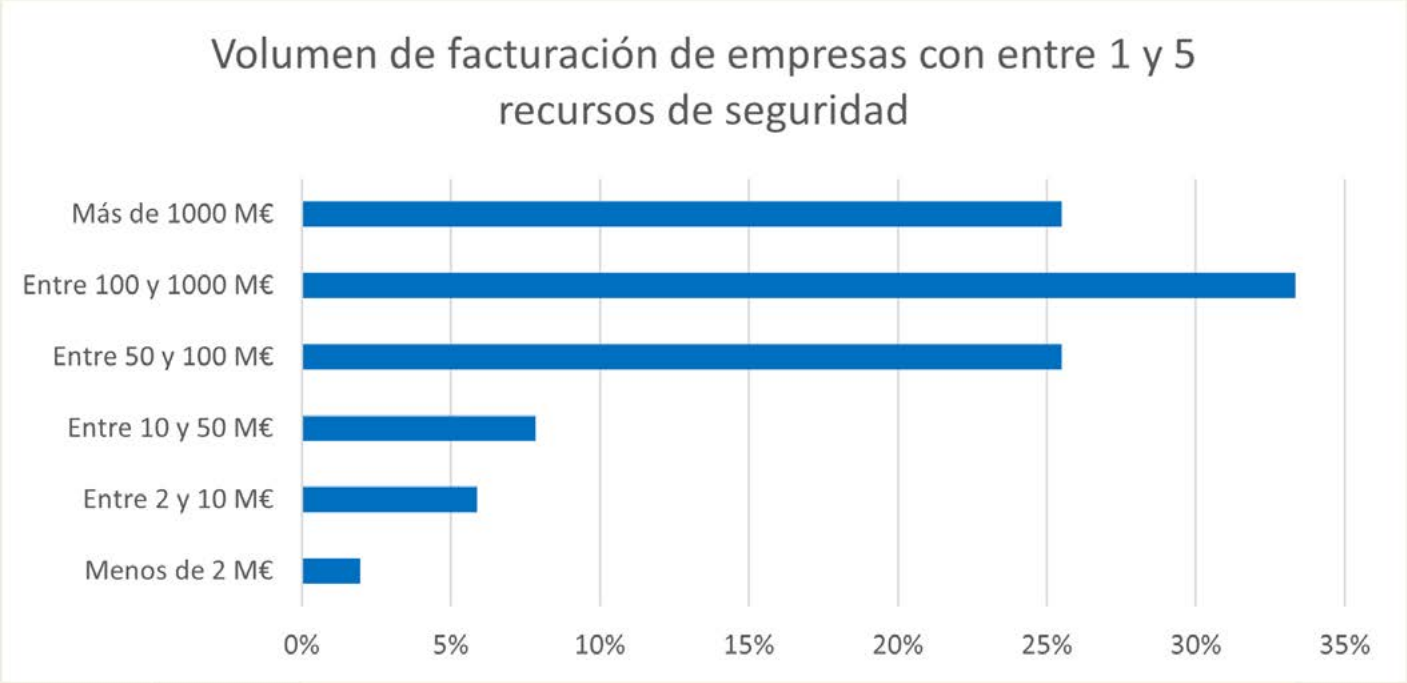


Ilustración 20: Volumen de facturación de empresas de 1 a 5 recursos en seguridad.

Recursos ciberseguridad	Volumen facturación	Total 2021	Total 2022
Entre 1 y 5 personas	Menos de 2 M€	3%	1%
	Entre 2 y 10 M€	3%	4%
	Entre 10 y 50 M€	3%	5%
	Entre 50 y 100 M€	10%	15%
	Entre 100 y 1000 M€	28%	20%
	Más de 1000 M€	18%	15%
Entre 5 y 15 personas	Entre 10 y 50 M€	0%	1%
	Entre 50 y 100 M€	0%	2%
	Entre 100 y 1000 M€	6%	5%
	Más de 1000 M€	8%	7%
Entre 15 y 50 personas	Entre 10 y 50 M€	3%	0%
	Entre 50 y 100 M€	1%	2%
	Entre 100 y 1000 M€	5%	6%
	Más de 1000 M€	6%	7%
Más de 50 personas	Entre 100 y 1000 M€	3%	1%
	Más de 1000 M€	6%	5%

Si correlacionamos los datos tomando como criterio principal el volumen de facturación, se observa que un 50 % de las empresas con facturación superior a 100 millones de euros tienen entre 1 y 5 personas en el área de ciberseguridad.

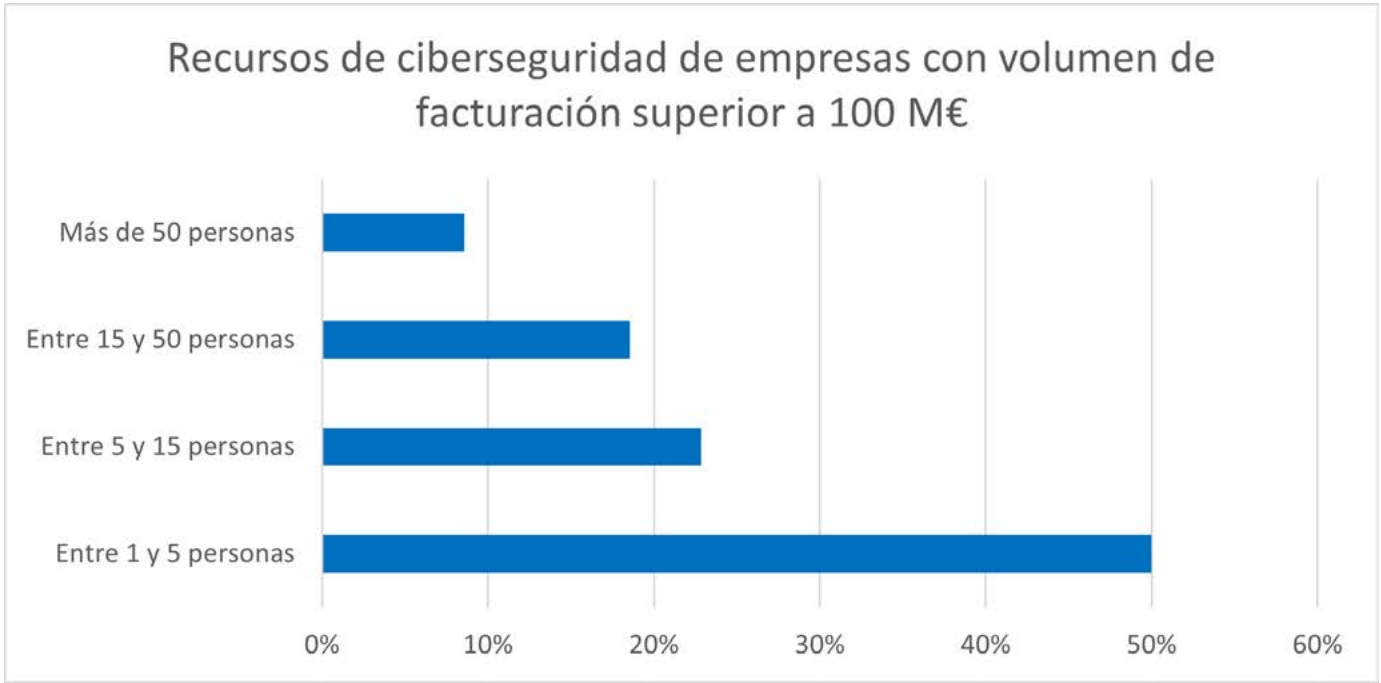


Ilustración 21: Volumen de facturación de empresas de 1 a 5 recursos en seguridad.

Operación de la Seguridad

Del total de las empresas analizadas, un 67% operaban la ciberseguridad desde el propio departamento de Ciberseguridad.

Ilustración 22: Volumen de facturación de empresas de 1 a 5 recursos en seguridad.

Si analizamos estos datos de forma conjunta con la información de facturación proporcionada y con el número de recursos disponibles para ciberseguridad, obtenemos los siguientes datos:

- Un 10% de las empresas que han respondido facturan más de 100 millones de € y con un máximo de 5 personas gestionan la seguridad, pero no la operan.
- Un 25% de las empresas que han respondido facturan más de 100 millones de € y con un máximo de 5 personas gestionan y operan la seguridad.
- Todas las empresas con facturación menor de 10 millones de € operan la seguridad desde el departamento seguridad con menos de 5 personas.

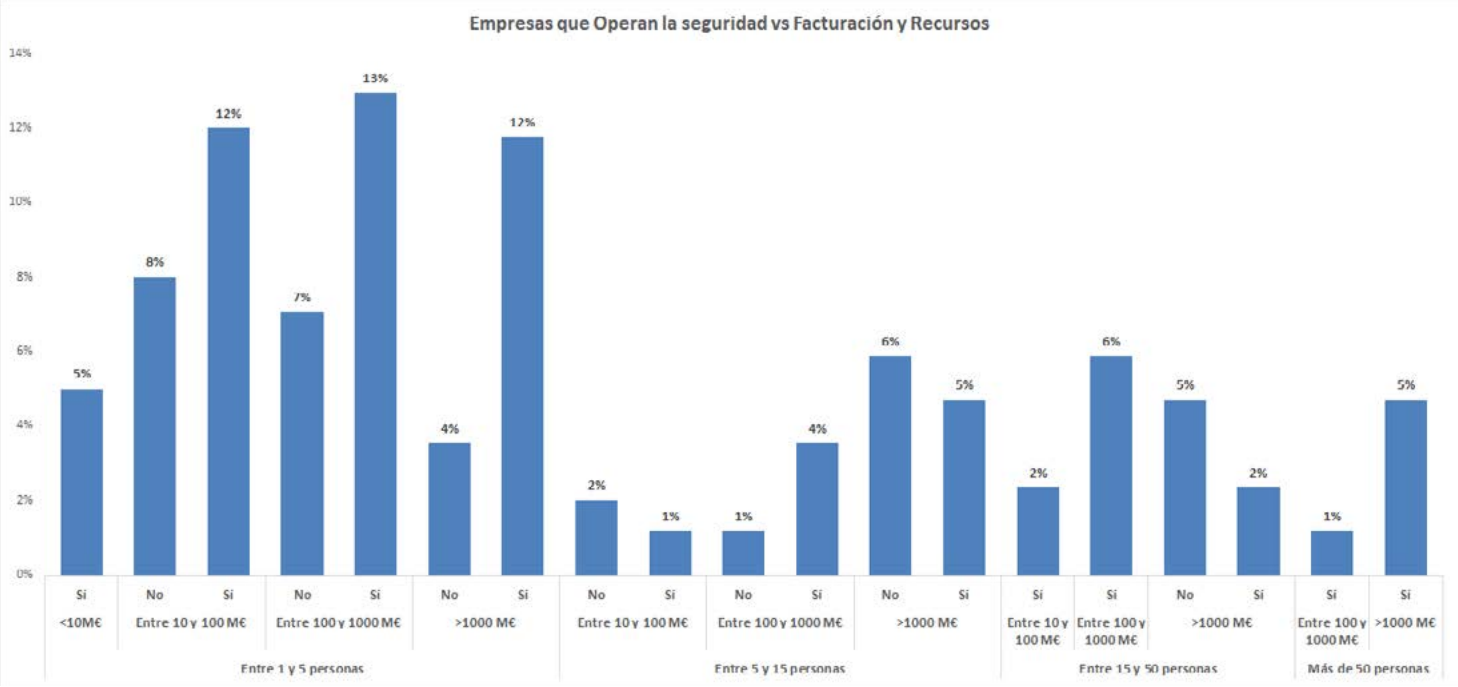


Ilustración 23: Empresas que operan en seguridad versus facturación y recursos.

6 INFLUENCIA DEL CONTEXTO ACTUAL

Evolución de las ciberamenazas y los recursos

Durante el último año, tomando en consideración el contexto sociopolítico actual, la mayoría de los encuestados (más de un 75%), considera que el volumen de ciberamenazas han aumentado.

Por otro lado, un 15% de los encuestados percibe que el nivel de ciberataques se mantiene, mientras que un 10% percibe que éste ha disminuido (5% considerablemente y 5% ligeramente).

Contrastan estos valores con los obtenidos en el estudio del año anterior, donde el nivel de percepción sobre el aumento de ciberataques era ligeramente inferior (71%). Al mismo tiempo, ninguno de los encuestados entonces, indicó no tener la percepción de que el número de ciberataques hubiera disminuido.

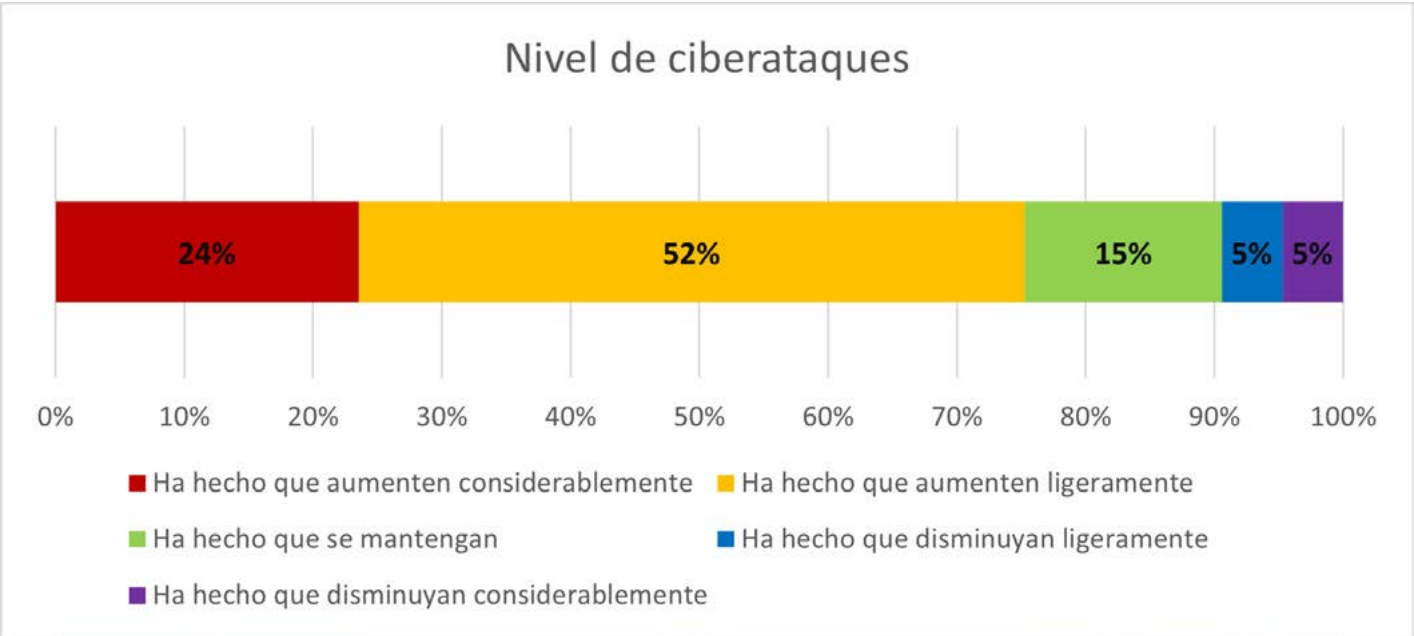


Ilustración 24: Nivel de ciberataques en el contexto actual.

En cuanto al nivel de estrés de los recursos de ciberseguridad, se confirma un impacto altamente significativo del contexto en la carga/presión/estrés.

Prácticamente la totalidad de los encuestados tiene una percepción de que ha aumentado carga/presión/estrés de los miembros del equipo de ciberseguridad (concretamente, el 66% de los encuestados perciben que el aumento es considerable y un 29% que ha percibido un ligero aumento).

Por otro lado, un porcentaje muy minoritario (2%) no percibe variación del nivel de carga/presión/estrés, e incluso un número similar de los encuestados indica que su nivel de estrés ha disminuido en el último año.

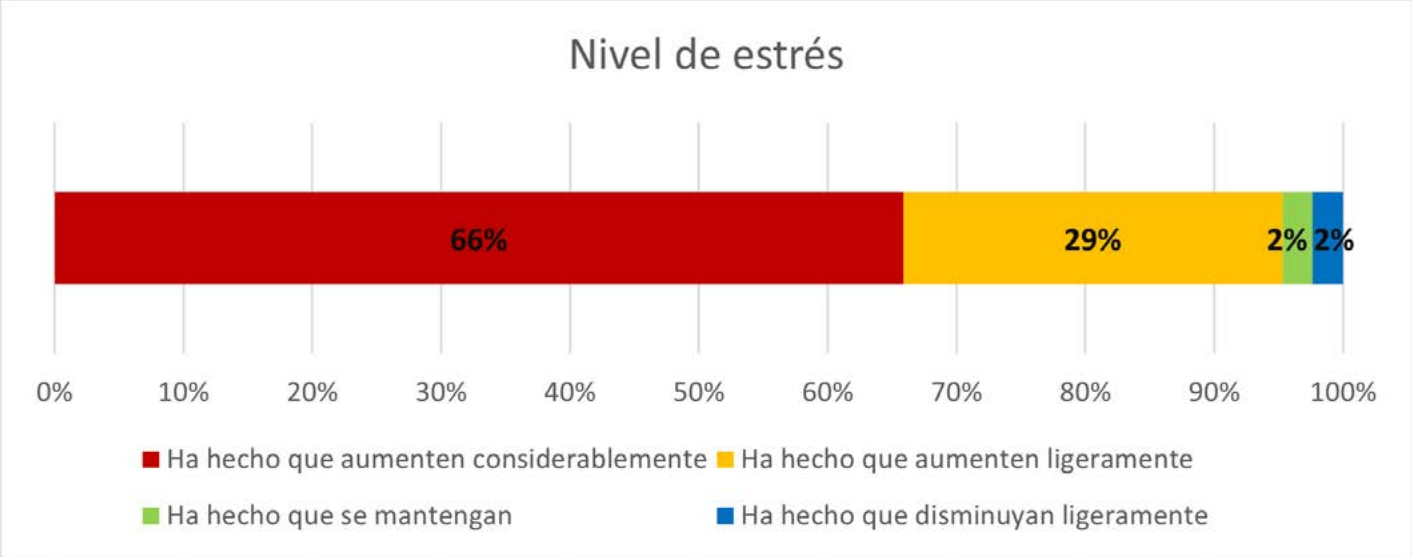


Ilustración 25: Nivel de estrés en los equipos de ciberseguridad.

Respecto a acciones realizadas por las distintas empresas encuestadas ante el conflicto de Ucrania, destaca el refuerzo de la monitorización de los eventos de seguridad, así como la actualización de los análisis de riesgos, incorporando nuevas amenazas o parámetros de riesgo, con un 54% y 49% respectivamente. Sin embargo, únicamente el 12% de los encuestados han realizado simulacros de incidentes. No sorprenden estos resultados, si relacionamos dichas acciones con el grado de madurez de los dominios NIST, siendo los dominios de "Identificar" y "Detectar" los más maduros con un 76%, en contraste con el de "Recuperar" con un 58%.

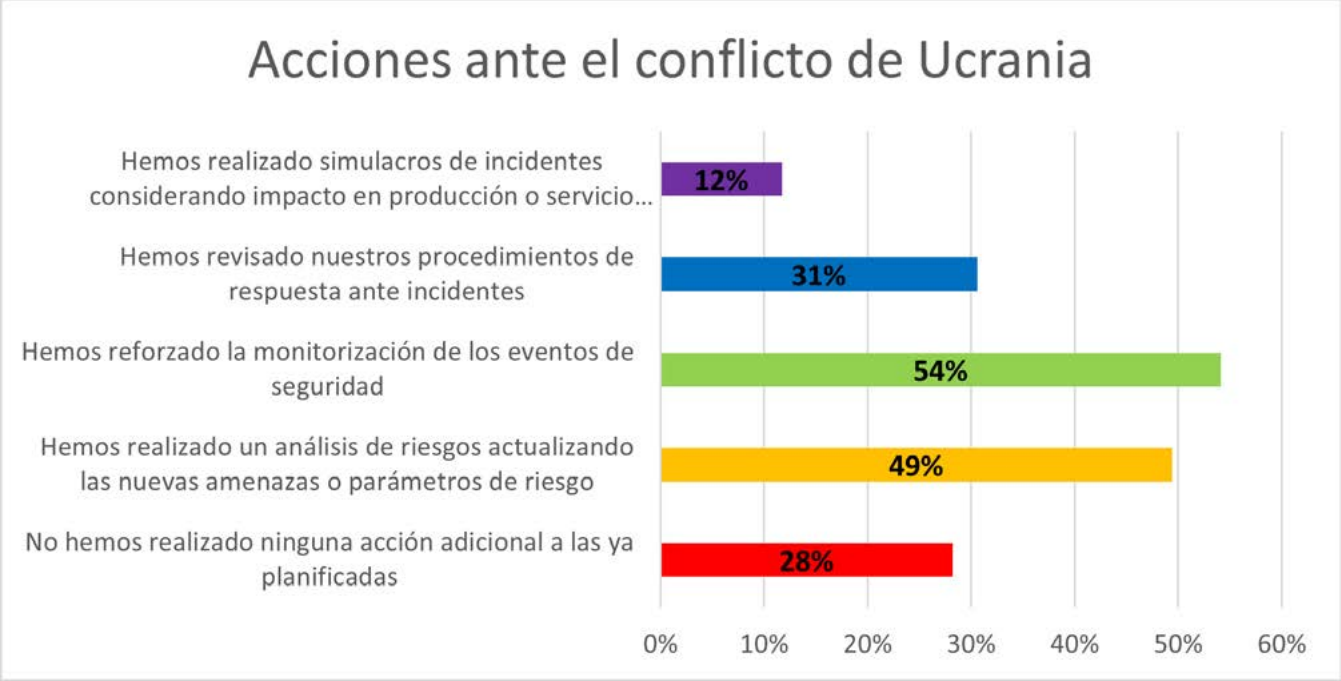


Ilustración 26: Acciones realizadas en materia de ciberseguridad a raíz del conflicto de Ucrania.

Efectos en la cadena de suministro y el plan de ciberseguridad

Según se desprende de los resultados de la encuesta, un 38% de los consultados percibieron que los ciberataques recibidos no tuvieron un impacto significativo en la cadena de suministro. Es un porcentaje relativamente elevado, que puede indicar que en términos generales, hay poca dependencia, o bien las características de la muestra, en la que predominan las empresas de servicios, reduce esta dependencia. Aún así, el 61% de los encuestados ha visto algún impacto de los ciberataques sobre su cadena de suministro.

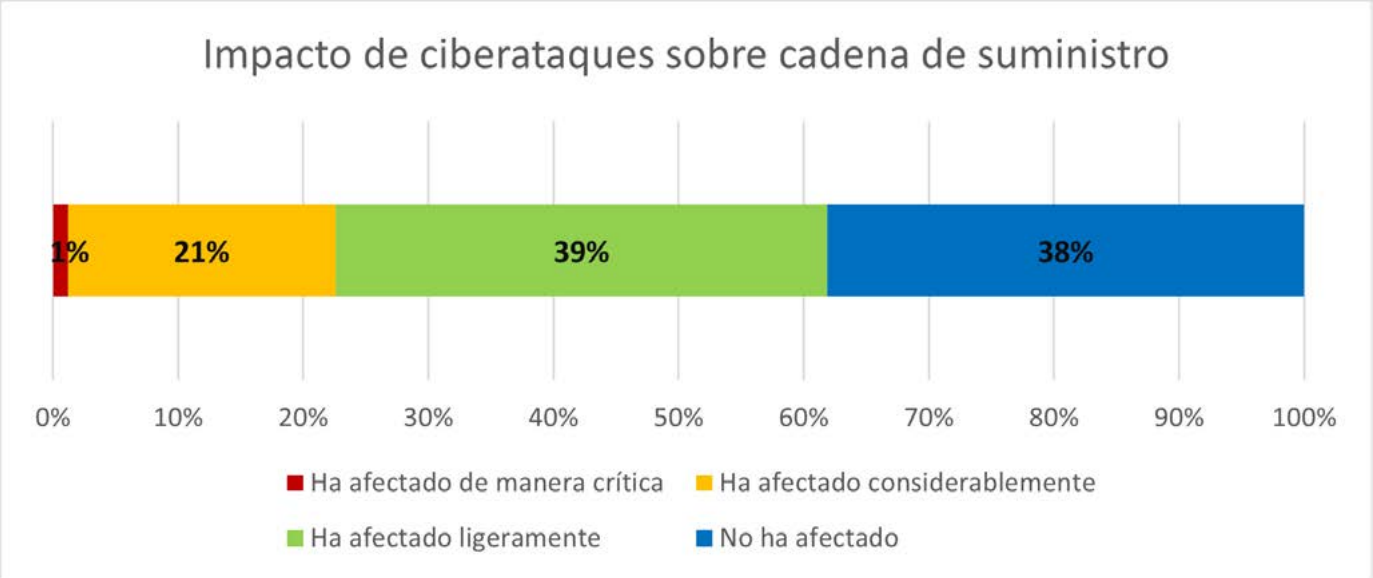


Ilustración 27: Impacto de los ciberataques en la cadena de suministro.

Si se realiza un análisis más detallado teniendo en cuenta la correlación entre sector empresarial y el impacto de los ciberataques, se observa que dicho impacto se concentra en 9 de los 19 sectores de actividad. Destaca la industria manufacturera, comercio, construcción o suministros, como los sectores con más impacto.

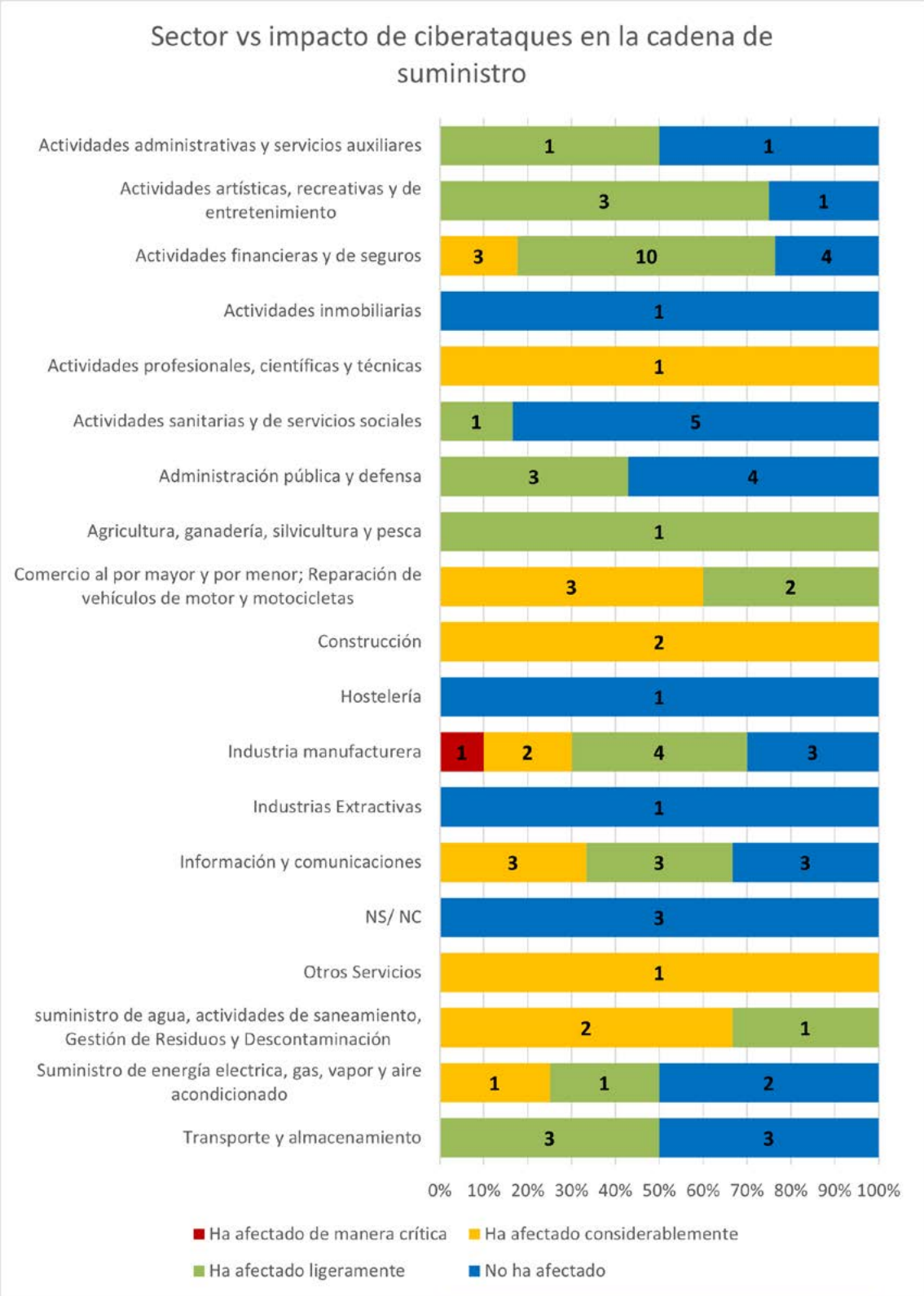


Ilustración 28: Correlación entre el sector de actividad y el impacto de ciberataques sobre cadena de suministro.

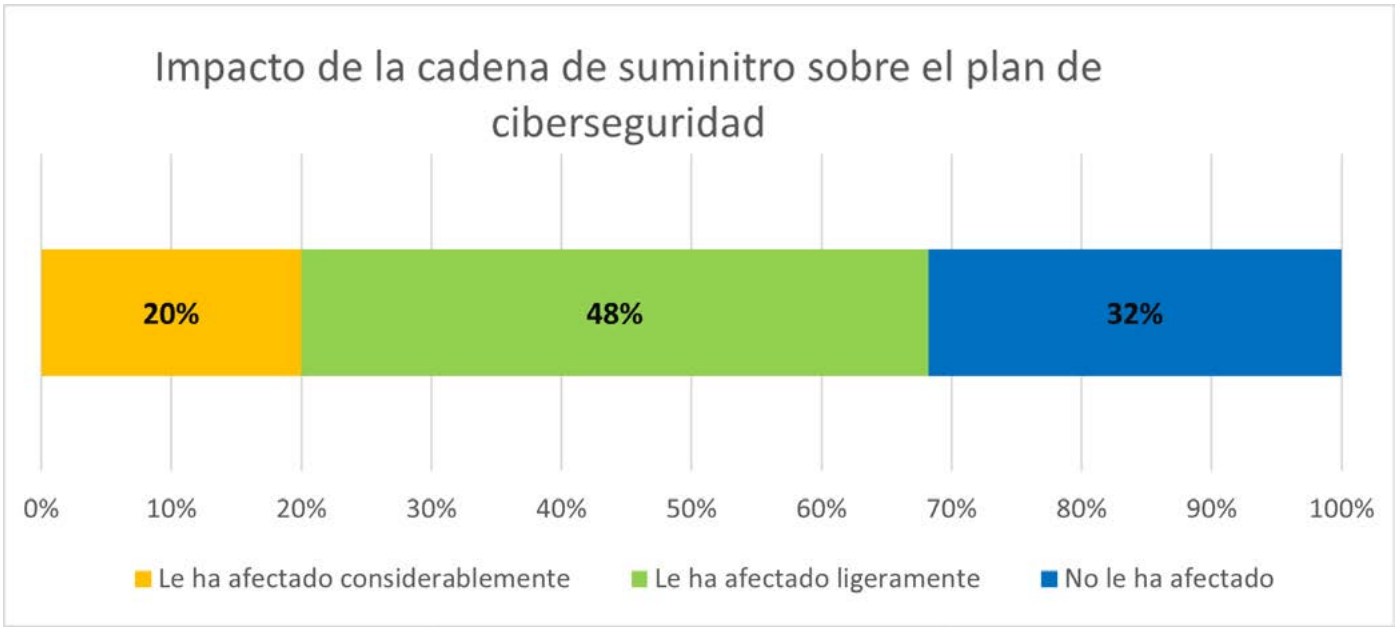


Ilustración 29: Impacto de la cadena de suministro sobre el plan de ciberseguridad de la organización.

Por otro lado, cuando se reformula la pregunta y evaluamos el impacto de la crisis en la cadena de suministro sobre el plan de ciberseguridad, el número de respuestas que indican que el impacto de esta sí les ha afectado, lo que da a entender que una incidencia en la cadena de suministro puede tener efectos significativos y por lo tanto, se requiere establecer planes de contingencia o soluciones multiproveedor en cuanto a la cadena de suministro, para reducir el riesgo.

7 UN ENFOQUE COMPLEMENTARIO SOBRE LAS DIMENSIONES DE LA MADUREZ EN CIBERSEGURIDAD

A lo largo del informe se han planteado los indicadores de madurez concediendo la misma importancia a todas las preguntas del cuestionario y estableciendo valoraciones medias para cada una de ellas y por cada uno de los dominios NIST. Sin embargo, en este apartado se ofrece, como visión complementaria y para la reflexión, un análisis factorial para detectar patrones similares en las respuestas con el fin de mostrar cómo se estructura la toma de decisiones en ciberseguridad.

En esta tercera edición del informe, vemos como dos de los dominios NIST: Detección y Recuperación, son dominios unidimensionales. ¿Qué significa esto? Que la interpretación de estos dos dominios se realiza en base a una única variable, a un único valor para su evaluación y esto nos indica que ambos dominios son relativamente sencillos de interpretar.

Por otro lado, tenemos el resto de los dominios del NIST: **Identificación, Protección y Respuesta** que presentan diversas dimensiones o ámbitos, por lo que su evaluación es menos trivial y sencilla que los dominios anteriormente mencionados y las respuestas no son tan fácilmente considerables como que la posición de una organización es alta, media o baja de una manera inequívoca.

Así, de acuerdo con los resultados del análisis factorial realizado y que se detalla posteriormente, la **Identificación** muestra dos ámbitos: el del **"análisis y gestión del riesgo de ciberseguridad"** y el de la "operativa para la identificación". Una organización tendrá una elevada o reducida madurez en Identificación si cuenta con valores altos o bajos simultáneamente en **"análisis y gestión del riesgo de ciberseguridad" y en "operativa para la identificación"**. Sin embargo, al tener dos dimensiones o ámbitos para la Identificación, pasaríamos a tener un plano de soluciones en el que valores intermedios en ambas dimensiones no resultaría equivalente a contar con una posición destacada en una de ellas y lo contrario en la otra.

> "Detección y Recuperación, son dominios unidimensionales, (...) mientras que Identificación, Protección y Respuesta presentan diversas dimensiones o ámbitos.

En lo que respecta a la **Protección**, este año encontramos que se representa también con dos dimensiones, introduciendo la dimensión **"control industrial"** a la ya existente de **"protección"** que ya reúne todas las preguntas propias del cuestionario para este dominio. Así en esta edición, para contar con una madurez elevada en este dominio se requiere un dominio de las dos dimensiones: la tradicional y la asociada al control industrial o IoT.

Finalmente, de acuerdo con el análisis realizado, el dominio NIST de **"Respuesta"** también se muestra en dos dimensiones que este año se han simplificado respecto al anterior. En esta edición hemos trabajado con las dimensiones: **"respuesta proactiva"** y **"respuesta reactiva"**. Las capacidades de **"respuesta proactiva"** son anticipatorias y se desarrollan antes de la detección, pudiendo generar una automatización de la respuesta por parte de las organizaciones más maduras. En la dimensión de la "respuesta reactiva" se mantienen las capacidades de respuestas concretas que vienen de la investigación de alertas o de vulnerabilidades, del análisis forense, de la mitigación o la contención de amenazas. Al igual que los otros dos dominios bidimensionales, para que una organización sea plenamente madura en este domino ha de dominar las dos dimensiones simultáneamente.

8 LECCIONES APRENDIDAS EN LA ELABORACIÓN DEL INFORME

Este es el tercer informe que se elabora con la intención de reflejar la realidad de las empresas de una manera rigurosa y con la mayor fiabilidad posible a partir de la información de que se dispone.

Nuestro punto de partida para recoger información es el cuestionario. La revisión de las respuestas de los años anteriores, en múltiples ocasiones nos lleva a considerar cómo hacemos las preguntas del cuestionario, y este análisis nos impulsa a introducir mejoras en las siguientes versiones.

El análisis del conjunto de preguntas, respuestas y resultados nos da la confianza de que este cuestionario ha quedado validado para analizar la madurez de la ciberseguridad de acuerdo con los dominios NIST. Como herramienta básica de aproximación a la realidad de las empresas a través de los encuestados, creemos que consigue reflejar fielmente la complejidad de las casuísticas representadas. Esta sólida base es la que nos permite medir de una manera objetiva el estado de madurez según el marco de referencia de los dominios NIST.

La retroalimentación de nuestra experiencia sobre el análisis en todas sus fases nos ayuda a ir elevando la calidad de los indicadores de una edición respecto a la siguiente. Es un objetivo fundamental, el ofrecer indicadores de calidad y precisos que describan lo más fidedignamente posible cuál es el estado de madurez, y que posteriormente permitan al lector establecer su propio marco de comparación respecto a su sector o situación.

Las distintas ediciones del informe nos van proporcionando una visión histórica de la evolución de los indicadores. Este histórico lo utilizamos de dos maneras, para enriquecer la posterior edición del informe, por un lado desarrollamos conocimiento del propio proceso de elaboración de conclusiones. Este conocimiento redunda en una mejor capacidad de entendimiento de las diferencias en las respuestas. Por otro lado, el histórico nos permite ver que existe una coherencia en el conjunto de preguntas, respuestas y resultados.

Por último, la metodología que seguimos para analizar los datos es más sofisticada. La adopción de mejoras en nuestra capacidad analítica nos da confianza en el resultado que ofrecemos. Esta metodología se describe ampliamente en el apartado posterior "Anexo I".

ANEXO I

Análisis Factorial Exploratorio para los dominios NIST

El presente informe presenta los indicadores de madurez en ciberseguridad concediendo la misma importancia a todas las preguntas del cuestionario para cada uno de los dominios NIST y estableciendo valoraciones medias para cada una de ellas. Sin embargo, el análisis factorial exploratorio puede permitir identificar en qué ámbitos específicos se estructura la madurez de las organizaciones que han formado parte de la muestra del estudio.

El análisis factorial es una técnica de análisis multivariante de reducción de datos. Su objetivo es transformar un conjunto de variables o indicadores en un nuevo (y menor) número de variables, denominadas factores, que expliquen la mayoría de la información contenida en el conjunto inicial, es decir, que expliquen la mayor parte de la varianza común.

El análisis factorial exploratorio se emplea para facilitar la comprensión de fenómenos complejos, que resulta difícil medir a través de una única variable. Por ejemplo, a partir de un cuestionario con diferentes características personales, el análisis factorial exploratorio podría detectar patrones similares en las respuestas sobre nivel de ingresos, nivel educativo y ocupación, lo que ofrecería un factor como solución, el cual podría interpretarse y "etiquetarse" como "estatus social".

En el caso que nos ocupa, la encuesta del Observatorio de la Ciberseguridad emplea 25 preguntas adaptadas del marco NIST (Marco para la mejora de la seguridad cibernética en infraestructuras críticas), organizadas en torno a cinco dominios, dimensiones principales, o factores: Identificar, proteger, detectar, responder y recuperar. Así, se aplica el análisis factorial exploratorio a cada bloque de preguntas planteadas por el marco NIST para cada uno de los dominios señalados. Este procedimiento permitirá comprobar si la definición de la madurez de la ciberseguridad de la empresa española puede abordarse desde cinco factores o dimensiones que se corresponden nítidamente con los dominios del marco NIST, o si resulta más recomendable contemplar más dimensiones, factores y facetas a la hora de analizar las actividades de identificación, protección, detección, respuesta y recuperación.

La aplicación del análisis factorial exige tener una ratio lo más elevada posible entre el número de observaciones y el número de variables (preguntas en este caso) a procesar. Así, resulta recomendable una ratio de 20:1 y no trabajar nunca con ratios inferiores a 5:1. En el caso que nos ocupa, dado que se obtuvieron 85 respuestas para cada una de las preguntas planteadas en la encuesta, de cara a la valorar la robustez de las conclusiones ofrecidas, conviene tener en cuenta que las ratios obtenidas fueron de 85:6 para los dominios de identificación (NIST1), protección (NIST2) y respuesta (NIST4), de 85:4 para detección (NIST3) y de 85:3 para recuperación (NIST5).

En el informe del pasado año se introdujo esta técnica como enfoque complementario y prospectivo al estudio principal realizado por el Observatorio de la Ciberseguridad. No obstante, los resultados de fiabilidad de las pruebas estadísticas realizadas no eran especialmente adecuados salvo para dos de los dominios NIST estudiados. Por el contrario, en el estudio realizado este año, dada la cantidad y calidad de los datos recogidos, todos los análisis factoriales realizados resultan aceptables, lo que sí que permite extraer conclusiones a partir de los mismos con cierta confianza.

Resumen de los resultados alcanzados

Como resumen de los resultados obtenidos del análisis factorial, más allá de su idoneidad de aplicación para el presente estudio, cabe destacar que detección y recuperación son dominios unidimensionales, mientras que los dominios de identificación, protección y respuesta son bidimensionales. Así, la identificación, protección y respuesta son cuestiones con múltiples facetas que, para ser desarrolladas con éxito, pueden requerir distintas destrezas a aplicar en dos ámbitos diferenciados.

Cuando se habla de fenómenos o dominios NIST unidimensionales se hace referencia al hecho de que puede sintetizarse toda la información de las preguntas del cuestionario propias de estos dos dominios en lo que sería una única variable de "detección" y otra de "recuperación". Esto indica que los indicadores considerados para evaluar la "detección" y la "recuperación" son relativamente sencillos de interpretar y recogen actividades que están clara y estrechamente conectadas entre sí. Así, las dimensiones de "detección" y "recuperación" obtenidas mediante los respectivos análisis factoriales permitirían valorar las capacidades de una organización para cada uno de estos dominios NIST como altas, medias o bajas, utilizando un simple eje para ello.

Por su parte, como el año pasado, el dominio NIST dedicado a la identificación muestra dos dimensiones o factores. Estas dimensiones son el "análisis y gestión del riesgo de ciberseguridad" y la "operativa para la identificación". Por tanto, para considerar a una organización como excelente en el dominio NIST de identificación, debe contar con altas capacidades que conjuguen los aspectos legales y de gestión de riesgos, y simultáneamente con las capacidades operativas necesarias relacionadas los inventarios, gestión de roles y responsabilidades, y definición de las dependencias y requisitos críticos para el sistema de objetivos de la organización. Representar el grado de preparación en identificación de una organización concreta no podría hacerse en un eje, sino que requeriría un espacio de soluciones de doble eje en el que evaluar sus capacidades de "análisis y gestión del riesgo de ciberseguridad" y de "operativa para la identificación"

En la pasada edición de este informe, el dominio NIST de protección mostraba una estructura unidimensional. Sin embargo, este año se representa mayoritariamente por una dimensión que se ha seguido denominando "protección" y que reúne todas las preguntas del cuestionario propias de este dominio salvo una, que representa una nueva dimensión denominada "control industrial". Este factor, además de la "protección", se convierte en un requisito con tratamiento necesariamente diferenciado de esta para aquellas empresas que estén intentando aprovechar los avances del internet de las cosas (IoT) con sistemas de control de activos dispersos geográficamente, sistemas de control distribuido y sistemas con controladores lógicos programables para controlar sus procesos. La identificación de esta dimensión de "control industrial" por parte del análisis factorial indica que supone una nueva forma de protección, dedicada al denominado "perímetro inteligente", diferente de la tradicional. Así, un grado de madurez elevado en el dominio de protección requiere dominar sus dos dimensiones, la tradicional y la IoT.

Finalmente, el dominio NIST dedicado a la respuesta también resulta bidimensional. En concreto, a través del análisis factorial se han encontrado dos factores de respuesta, calificados como "respuesta proactiva" y "respuesta reactiva". La "respuesta proactiva" supone un conjunto de actuaciones que mejoran las capacidades de respuesta de la organización de manera preventiva, sin necesidad de enfrentarse directamente a ningún evento de ciberseguridad. Por su parte, la "respuesta reactiva" se centra en las actuaciones que demuestran capacidades de respuesta ante eventos de ciberseguridad concretos, como la investigación de alertas, el análisis forense, la identificación de vulnerabilidades y amenazas o los procesos de mitigación y contención. De manera similar a lo que sucedía para la identificación y protección, para que una organización consiga un grado de madurez elevado en el dominio de respuesta, debe lograr un rendimiento excelente en las actividades de "respuesta proactiva" y "respuesta reactiva" simultáneamente.

1. Análisis factorial exploratorio para la identificación

El KMO tiene un valor ideal para la realización del análisis factorial (superior a 0,8 e inferior a 0,9). En concreto, alcanza la cifra de 0,824. Al mismo tiempo, el test de esfericidad de Bartlett es altamente significativo. Ambos resultados hacen adecuado y recomendable utilizar el análisis factorial exploratorio para reducir la dimensionalidad de las preguntas del cuestionario relativas a la identificación.

La solución obtenida del análisis muestra dos factores diferenciados, que explican un 64,45% de la varianza total contenida en los datos originales. El primero de estos dos factores o variables, el más relevante a la hora de entender la identificación, recoge casi un 40% de la varianza total, y reúne las siguientes preguntas del cuestionario (se indican en el orden de su relevancia para la construcción e interpretación del factor resultante): ID4, ID5, ID3 e ID6. El segundo factor, por su parte, supone cerca del 25% de la varianza, y agrupa a las preguntas ID1 e ID2.

Cabe destacar que los resultados de agrupación de preguntas en dos factores son idénticos a los obtenidos el pasado año, lo que parece corroborar que la estructura de actividades extraída del análisis factorial para la identificación resulta consistente.

El primer factor ha sido denominado "análisis y gestión del riesgo de ciberseguridad", puesto que es precisamente todas las preguntas que agrupa tienen el riesgo como elemento común. En concreto, el "análisis y gestión del riesgo de ciberseguridad" es la dimensión de la identificación que incluye:

- **La identificación, documentación y análisis de riesgo de las vulnerabilidades y amenazas de ciberseguridad, según la probabilidad e impacto en el negocio (ID4).**
- **Los procesos de gestión del riesgo y niveles de tolerancia establecidos, gestionados, acordados e informados (ID5).**
- **Una política de roles y responsabilidades, requerimientos legales y regulatorios, integrada con los procesos de gobierno y gestión del riesgo de ciberseguridad (ID3).**
- **El establecimiento de procesos de gestión del riesgo de la cadena de suministro (proveedores y terceros) y medidas apropiadas en los contratos asociados (ID6).**

El segundo elemento de la identificación se ha denominado "operativa para la identificación", e incluye las actividades relativas a:

- **Inventarios (de dispositivos, sistemas, aplicaciones y recursos de información), gestión de roles y responsabilidades asociadas (ID1).**
- **Identificación y comunicación de dependencias y requisitos de los servicios y funciones críticas, de acuerdo con el sistema de objetivos de la organización (ID2).**

A la vista del análisis realizado, identificar tiene una vertiente con un importante componente legal y de gestión de riesgos, y otra más operativa e instrumental. Así, una organización que busque optimizar sus capacidades de identificación deberá desarrollar competencias tanto para el "análisis y gestión del riesgo de ciberseguridad" como para la "operativa para la identificación".

Matriz de correlaciones[a]							
		ID1	ID2	ID3	ID4	ID5	ID6
Correlación	ID1	1,000	,308	,304	,178	,236	,381
	ID2	,308	1,000	,318	,351	,396	,404
	ID3	,304	,318	1,000	,476	,540	,441
	ID4	,178	,351	,476	1,000	,503	,421
	ID5	,236	,396	,540	,503	1,000	,544
	ID6	,381	,404	,441	,421	,544	1,000
Sig. (unilateral)	ID1		,002	,002	,052	,015	<,001
	ID2	,002		,002	,001	,000	,000
	ID3	,002	,002		,000	,000	,000
	ID4	,052	,001	,000		,000	,000
	ID5	,015	,000	,000	,000		,000
	ID6	,000	,000	,000	,000	,000	
a. Determinante = ,199							

Prueba de KMO y Bartlett		
Medida Kaiser-Meyer-Olkin de adecuación de muestreo		,824
Prueba de esfericidad de Bartlett	Aprox. Chi-cuadrado	129,316
	gl	15
	Sig.	<,001

Comunalidades		
	Inicial	Extracción
ID1	1,000	,851
ID2	1,000	,466
ID3	1,000	,590
ID4	1,000	,662
ID5	1,000	,693
ID6	1,000	,606
Método de extracción: análisis de componentes principales.		

Varianza total explicada									
Componente	Autovalores iniciales			Sumas de cargas al cuadrado de la extracción			Sumas de cargas al cuadrado de la rotación		
	Total	% de varianza	% acumulado	Total	% de varianza	% acumulado	Total	% de varianza	% acumulado
1	2,970	49,504	49,504	2,970	49,504	49,504	2,378	39,626	39,626
2	,897	14,949	64,452	,897	14,949	64,452	1,490	24,826	64,452
3	,685	11,410	75,862						
4	,551	9,181	85,043						
5	,503	8,390	93,433						
6	,394	6,567	100,000						
Método de extracción: análisis de componentes principales.									

Matriz de componente[a]		
	Componente	
	1	2
ID1	,524	,759
ID2	,646	,222
ID3	,746	-,183
ID4	,709	-,398
ID5	,791	-,260
ID6	,771	,108
Método de extracción: análisis de componentes principales.		
a. 2 componentes extraídos.		

Matriz de componente rotado[a]		
	Componente	
	1	2
ID1	,037	,922
ID2	,427	,533
ID3	,728	,244
ID4	,812	,043
ID5	,807	,203
ID6	,593	,504
Método de extracción: análisis de componentes principales. Método de rotación: Varimax con normalización Kaiser[a]		
a. La rotación ha convergido en 3 iteraciones.		

Matriz de transformación de componente		
Componente	1	2
1	,845	,535
2	-,535	,845
Método de extracción: análisis de componentes principales. Método de rotación: Varimax con normalización Kaiser.		

2. Análisis factorial exploratorio para la protección

En este caso, el KMO tiene un valor de 0,777, superior a lo recomendado para el análisis factorial exploratorio (0,7) y cercano a sus rangos ideales. Del mismo modo, la prueba de esfericidad de Bartlett resulta altamente significativa, por lo que la aplicación del análisis factorial exploratorio es adecuada y recomendable para comprender qué dimensiones o factores encierran las preguntas del cuestionario relativas a la protección.

El año pasado, la solución ofrecida por el análisis factorial ofrecía un único factor, que reunía todas las preguntas planteadas en la encuesta para este dominio NIST, y explica un 75% de la varianza total. Este año, la capacidad explicativa de la solución llega al 67% de la varianza total contenida en los datos originales, pero con dos factores. No obstante, de estos dos factores, el primero reúne el 45% de la varianza explicada y el segundo sólo un 22%, teniendo este último un único indicador de los originalmente planteados en el cuestionario (PR5).

El primer factor, por su alto poder explicativo sobre la protección, y por reunir cinco de las seis preguntas recogidas en la encuesta, se ha denominado precisamente "protección", incluyendo las siguientes actividades (se muestran ordenadas según su relevancia para la construcción e interpretación del factor resultante):

- **Protección de sistemas y activos de información, en base a la gestión, implementación y mantenimiento de procesos y procedimientos asociados a la política de seguridad (PR4).**
- **Gestión del ciclo de vida del dato, para proteger la confidencialidad, integridad y disponibilidad de la información (PR3).**
- **Gestión de identidades y accesos a los activos, según el principio de menor privilegio y segregación de funciones (PR1).**
- **Formación, concienciación y comprensión de roles y responsabilidades en materia de ciberseguridad por parte de todos los empleados y colaboradores (PR2).**
- **Medidas técnicas de seguridad asociadas a la política y procedimientos de seguridad para proporcionar seguridad y resiliencia a los sistemas y activos de información (PR6).**

El segundo factor de la protección se ha calificado como "control industrial", pues únicamente incluye el mantenimiento controlado de los sistemas de información y control industrial (PR5). La separación o independencia de este factor del resto de actividades de protección puede obedecer a la distinción entre empresas industriales y de servicios, o a la creciente importancia que está cobrando el despliegue de sistemas vinculados al internet de las cosas (IoT).

A la vista de los resultados obtenidos, todo tipo de organización, independientemente de su sector de actividad, debe vigilar la "protección". No obstante, la dimensión de "control industrial" cobra una especial relevancia a la hora de llevar a cabo una protección integral en el caso de las empresas que tengan sistemas de información para controlar procesos como la fabricación, la manipulación de productos, la producción y la distribución, sistemas de control de supervisión y adquisición de datos para controlar activos dispersos geográficamente, sistemas de control distribuido y sistemas con controladores lógicos programables para controlar procesos localizados (NIST SP 800-39).

Matriz de correlaciones[a]

		PR1	PR2	PR3	PR4	PR5	PR6
Correlación	PR1	1,000	,454	,468	,540	,342	,503
	PR2	,454	1,000	,399	,443	,274	,708
	PR3	,468	,399	1,000	,489	,185	,314
	PR4	,540	,443	,489	1,000	,160	,507
	PR5	,342	,274	,185	,160	1,000	,287
	PR6	,503	,708	,314	,507	,287	1,000
Sig. (unilateral)	PR1		<,001	<,001	<,001	<,001	<,001
	PR2	,000		,000	,000	,006	,000
	PR3	,000	,000		,000	,045	,002
	PR4	,000	,000	,000		,072	,000
	PR5	,001	,006	,045	,072		,004
	PR6	,000	,000	,002	,000	,004	

a. Determinante = ,131

Prueba de KMO y Bartlett		
Medida Kaiser-Meyer-Olkin de adecuación de muestreo		,777
Prueba de esfericidad de Bartlett	Aprox. Chi-cuadrado	164,797
	gl	15
	Sig.	<,001

Comunalidades		
	Inicial	Extracción
PR1	1,000	,612
PR2	1,000	,624
PR3	1,000	,557
PR4	1,000	,687
PR5	1,000	,866
PR6	1,000	,648
Método de extracción: análisis de componentes principales.		

Varianza total explicada										
Componente	Autovalores iniciales			Sumas de cargas al cuadrado de la extracción			Sumas de cargas al cuadrado de la rotación			
	Total	% de varianza	% acumulado	Total	% de varianza	% acumulado	Total	% de varianza	% acumulado	
1	3,089	51,485	51,485	3,089	51,485	51,485	2,693	44,881	44,881	
2	,905	15,079	66,564	,905	15,079	66,564	1,301	21,684	66,564	
3	,783	13,057	79,621							
4	,534	8,898	88,519							
5	,424	7,065	95,584							
6	,265	4,416	100,000							
Método de extracción: análisis de componentes principales.										

Matriz de componente[a]		
	Componente	
	1	2
PR1	,782	,003
PR2	,788	,058
PR3	,663	-,343
PR4	,754	-,345
PR5	,458	,810
PR6	,801	,086
Método de extracción: análisis de componentes principales.		
a. 2 componentes extraídos.		

Matriz de componente rotado[a]		
	Componente	
	1	2
PR1	,706	,335
PR2	,688	,388
PR3	,746	-,028
PR4	,829	,008
PR5	,069	,928
PR6	,688	,419
Método de extracción: análisis de componentes principales.		
Método de rotación: Varimax con normalización Kaiser.		
a. La rotación ha convergido en 3 iteraciones.		

Matriz de transformación de componente		
Componente	1	2
1	,905	,426
2	-,426	,905
Método de extracción: análisis de componentes principales.		
Método de rotación: Varimax con normalización Kaiser.		

3. Análisis factorial exploratorio para la detección

Como sucedía para la protección, en el caso de la detección el KMO tiene un valor de 0,773, superior a lo recomendado para el análisis factorial exploratorio (0,7) y cercano a sus rangos ideales. También la prueba de esfericidad de Bartlett resulta altamente significativa, así que la aplicación del análisis factorial exploratorio es adecuada y recomendable también en este caso, y permitirá entender la dimensionalidad de las preguntas del cuestionario relativas a la protección (DE1, DE2, DE3 y DE4).

La solución obtenida se basa en un único factor o dimensión, de acuerdo con lo esperado, y que lógicamente se ha etiquetado como "detección". Este factor permite representar el 65% de la varianza explicada y reúne todas las preguntas de la encuesta relativas a este dominio. Así, las actividades propias de la "detección", indicadas según su peso para esta variable, son las siguientes:

- **Contar con sistemas para la recolección de eventos de ciberseguridad (DE1).**
- **Monitorizar la actividad de usuarios (incluidos proveedores) en sistemas y redes para detectar eventos de ciberseguridad (DE3).**
- **Análisis de detección de actividad anómala (DE2).**
- **Definición, actualización y prueba de los procedimientos y roles implicados en los procesos de detección de incidentes (DE4).**

Matriz de correlaciones[a]					
		DE1	DE2	DE3	DE4
Correlación	DE1	1,000	,576	,652	,576
	DE2	,576	1,000	,572	,390
	DE3	,652	,572	1,000	,424
	DE4	,576	,390	,424	1,000
Sig. (unilateral)	DE1		<,001	<,001	<,001
	DE2	,000		,000	,000
	DE3	,000	,000		,000
	DE4	,000	,000	,000	
a. Determinante = ,229					

Prueba de KMO y Bartlett		
Medida Kaiser-Meyer-Olkin de adecuación de muestreo		,773
Prueba de esfericidad de Bartlett	Aprox. Chi-cuadrado	120,741
	gl	6
	Sig.	<,001

Comunalidades		
	Inicial	Extracción
DE1	1,000	,773
DE2	1,000	,619
DE3	1,000	,687
DE4	1,000	,526
Método de extracción: análisis de componentes principales.		

Varianza total explicada						
Componente	Autovalores iniciales			Sumas de cargas al cuadrado de la extracción		
	Total	% de varianza	% acumulado	Total	% de varianza	% acumulado
1	2,605	65,130	65,130	2,605	65,130	65,130
2	,648	16,198	81,328			
3	,436	10,912	92,241			
4	,310	7,759	100,000			
Método de extracción: análisis de componentes principales.						

Matriz de componente[a]	
	Componente
	1
DE1	,879
DE2	,787
DE3	,829
DE4	,726
Método de extracción: análisis de componentes principales.	
a. 1 componentes extraídos.	

4. Análisis factorial exploratorio para la respuesta

En el caso del dominio NIST relativo a la respuesta, las pruebas para evaluar la idoneidad de la realización del análisis factorial exploratorio resultan también claramente favorables. Así, el KMO asciende a un valor de 0,806, dentro de los rangos ideales para aplicar esta técnica (superior a 0,8 e inferior a 0,9). Y también la prueba de esfericidad de Bartlett resulta altamente significativa.

La solución que ofrece el análisis apunta a la existencia de dos factores o dimensiones diferenciadas en la respuesta, que alcanzan a explicar un 72% de la varianza total contenida en los datos originales. La primera de estas dimensiones recoge un 41% de la varianza total, mientras que la segunda explica otro 31%.

El primer factor de la respuesta se ha denominado "respuesta proactiva", puesto que reúne actuaciones que no se ejecutan ante la presencia de un evento de ciberseguridad, pero que contribuyen a la mejora de las capacidades de respuesta. En concreto, la "respuesta proactiva" agrupa las siguientes actividades (reseñadas según su relevancia para la construcción e interpretación de esta variable):

- **Documentación, actualización y prueba de procedimientos de respuesta ante incidentes (RS1).**
- **Proceso formal de mejora continua de la respuesta ante incidentes, en base a incidentes pasados (RS6).**
- **Formalización del proceso, roles e interlocutores en la comunicación (interna y externa) de incidentes (RS2).**

El segundo factor o dimensión de la respuesta se ha bautizado como "respuesta reactiva", pues recoge actuaciones relacionadas directamente con las fases iniciales, de desarrollo y posteriores a un evento de ciberseguridad. En particular, la "respuesta reactiva" incluye las actividades de:

- **Investigación de alertas generadas por los sistemas de detección (RS3).**
- **Análisis forense tras incidentes de seguridad (RS4).**
- **Identificación temprana de vulnerabilidades y amenazas y procesos de mitigación y contención (RS5).**

Matriz de componente rotado[a]		
	Componente	
	1	2
RS1	,905	,124
RS2	,788	,336
RS3	,079	,843
RS4	,241	,723
RS5	,506	,664
RS6	,841	,214
Método de extracción: análisis de componentes principales. Método de rotación: Varimax con normalización Kaiser.		

Matriz de correlaciones[a]							
		RS1	RS2	RS3	RS4	RS5	RS6
Correlación	RS1	1,000	,708	,250	,302	,476	,685
	RS2	,708	1,000	,386	,373	,558	,588
	RS3	,250	,386	1,000	,370	,490	,243
	RS4	,302	,373	,370	1,000	,497	,387
	RS5	,476	,558	,490	,497	1,000	,555
	RS6	,685	,588	,243	,387	,555	1,000
Sig. (unilateral)	RS1		<,001	,010	,002	<,001	<,001
	RS2	,000		,000	,000	,000	,000
	RS3	,010	,000		,000	,000	,013
	RS4	,002	,000	,000		,000	,000
	RS5	,000	,000	,000	,000		,000
	RS6	,000	,000	,013	,000	,000	
a. Determinante = ,080							

Prueba de KMO y Bartlett		
Medida Kaiser-Meyer-Olkin de adecuación de muestreo		,806
Prueba de esfericidad de Bartlett	Aprox. Chi-cuadrado	204,719
	gl	15
	Sig.	<,001

Comunalidades		
	Inicial	Extracción
RS1	1,000	,834
RS2	1,000	,734
RS3	1,000	,718
RS4	1,000	,581
RS5	1,000	,697
RS6	1,000	,753
Método de extracción: análisis de componentes principales.		

Varianza total explicada									
Componente	Autovalores iniciales			Sumas de cargas al cuadrado de la extracción			Sumas de cargas al cuadrado de la rotación		
	Total	% de varianza	% acumulado	Total	% de varianza	% acumulado	Total	% de varianza	% acumulado
1	3,334	55,562	55,562	3,334	55,562	55,562	2,467	41,119	41,119
2	,983	16,386	71,948	,983	16,386	71,948	1,850	30,829	71,948
3	,647	10,785	82,733						
4	,433	7,211	89,944						
5	,361	6,017	95,961						
6	,242	4,039	100,000						
Método de extracción: análisis de componentes principales.									

Matriz de componente[a]		
	Componente	
	1	2
RS1	,794	-,451
RS2	,830	-,211
RS3	,575	,622
RS4	,631	,428
RS5	,805	,220
RS6	,798	-,340
Método de extracción: análisis de componentes principales.		
a. 2 componentes extraídos.		

Matriz de componente rotado[a]		
	Componente	
	1	2
RS1	,905	,124
RS2	,788	,336
RS3	,079	,843
RS4	,241	,723
RS5	,506	,664
RS6	,841	,214
Método de extracción: análisis de componentes principales. Método de rotación: Varimax con normalización Kaiser.		
a. La rotación ha convergido en 3 iteraciones.		

Matriz de transformación de componente		
Componente	1	2
1	,795	,607
2	-,607	,795
Método de extracción: análisis de componentes principales. Método de rotación: Varimax con normalización Kaiser.		

5. Análisis factorial exploratorio para la recuperación

Como sucedía para la protección y la detección, en el caso de la recuperación el KMO tiene un valor de 0,741, superior a lo recomendado para el análisis factorial exploratorio (0,7). Esto, junto con una prueba de esfericidad de Bartlett altamente significativa, aconseja la aplicación del análisis factorial exploratorio para entender la dimensionalidad de las tres preguntas del cuestionario relativas a la recuperación (RE1, RE2 y RE3).

El análisis factorial ofrece como solución un único factor o dimensión, lo que está de acuerdo con lo esperado, y que en consecuencia se ha denominado "recuperación". Así, recuperar es un cometido que se puede describir con claridad de manera convergente a través de las actividades analizadas en las preguntas recogidas en el cuestionario empleado por el Observatorio de la Ciberseguridad.

Este factor permite representar el 83% de la varianza explicada y reúne todas las preguntas de la encuesta relativas a este dominio. Así, las cuestiones propias de la "recuperación", indicadas según su peso en la construcción de esta variable, son las siguientes:

- **Actualización regular y proactiva de planes y estrategias de recuperación para incorporar mejoras y lecciones aprendidas (RE2).**
- **Formalización y prueba regular de los planes de recuperación de los sistemas clave de negocio ante incidentes de ciberseguridad (RE1)**
- **Definición de actividades, interlocutores y roles en la comunicación (interna y externa) durante el proceso de recuperación (RE3).**

Matriz de correlaciones[a]				
		RE1	RE2	RE3
Correlación	RE1	1,000	,803	,714
	RE2	,803	1,000	,721
	RE3	,714	,721	1,000
Sig. (unilateral)	RE1		<,001	<,001
	RE2	,000		,000
	RE3	,000	,000	
a. Determinante = ,152				

Prueba de KMO y Bartlett		
Medida Kaiser-Meyer-Olkin de adecuación de muestreo		,741
Prueba de esfericidad de Bartlett	Aprox. Chi-cuadrado	154,663
	gl	3
	Sig.	<,001

Comunalidades		
	Inicial	Extracción
RE1	1,000	,850
RE2	1,000	,855
RE3	1,000	,788
Método de extracción: análisis de componentes principales.		

Varianza total explicada						
Componente	Autovalores iniciales			Sumas de cargas al cuadrado de la extracción		
	Total	% de varianza	% acumulado	Total	% de varianza	% acumulado
1	2,493	83,095	83,095	2,493	83,095	83,095
2	,310	10,348	93,443			
3	,197	6,557	100,000			
Método de extracción: análisis de componentes principales.						

Matriz de componentea	
	Componente 1
RE1	,922
RE2	,925
RE3	,888
Método de extracción: análisis de componentes principales.	
a. 1 componentes extraídos.	

ANEXO II

Encuesta Observatorio de la Ciberseguridad

Salir

III Estudio del nivel de madurez en ciberseguridad de la empresa española

1. ¿Cuál de los siguientes puestos ocupa en su organización?

- ◯ Dirección/Responsable de la Seguridad de la información
- ◯ Dirección/Responsable de TI
- ◯ Delegado/a de Protección de Datos
- ◯ Otro puesto de Dirección
- ◯ Especialista en Seguridad de la información
- ◯ Especialista en TI
- ◯ Otro puesto de especialista
- ◯ Consultoría de Seguridad de la Información, Consultoría de TI o similar

2. ¿Es usted la persona con la máxima (única) responsabilidad del área de ciberseguridad en su organización?

- ◯ Sí
- ◯ No

3. En caso de que la respuesta anterior sea no, ¿cuántos niveles existen hasta la máxima (última) responsabilidad para el área de ciberseguridad?

4. ¿Qué porcentaje del presupuesto de TI dedica su organización específicamente a ciberseguridad?

- ◯ Entre el 1% y el 3%
- ◯ Entre el 3% y el 5%
- ◯ Entre el 5% y el 7%
- ◯ Más del 7%

5. ¿Cuántas personas (personal interno) tiene su organización en el área de ciberseguridad?

- ◯ Entre 1 y 5 personas
- ◯ Entre 5 y 15 personas
- ◯ Entre 15 y 50 personas
- ◯ Más de 50 personas

6. Su departamento de ciberseguridad, ¿opera la ciberseguridad?

- ◯ Sí
- ◯ No

* 7. ¿Cuál de los siguientes sectores describe mejor su principal actividad de negocio?'

[ ]

* 8. ¿Cuántos empleados tiene su organización?

- ◯ Menos de 10
- ◯ Entre 10 y 49
- ◯ Entre 50 y 249
- ◯ Entre 250 y 2500
- ◯ Entre 2500 y 10000
- ◯ Más de 10000

* 9. ¿Cuál es el volumen de facturación anual de su organización (o presupuesto total de gastos en el caso de Administraciones Públicas) en euros o dólares?

- ◯ Inferior a 2 millones de euros
- ◯ Entre 2 y 10 millones de euros
- ◯ Entre 10 y 50 millones de euros
- ◯ Entre 50 y 100 millones de euros
- ◯ Entre 100 y 1000 millones de euros
- ◯ Más de 1000 millones de euros

* 10. Indique el año de constitución de su organización

[ ]

11. ¿Forma su organización parte de un grupo internacional?

- ◯ Sí
- ◯ No

* 12. En caso de que la respuesta anterior sea sí, ¿se concentra la función de ciberseguridad para todas la empresas del grupo?"

- ◯ Sí
- ◯ No

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

- ◯ No existe inventario
- ◯ Existe un inventario parcial y se actualiza manualmente de manera puntual sin gestión de roles
- ◯ Existe un inventario completo no asociado a la gestión de roles y responsabilidades
- ◯ Existe un inventario completo y actualizado donde se revisan los roles y responsabilidades de manera periódica

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

- ◯ No existe misión, visión, ni objetivos
- ◯ Existe misión, visión y objetivos, pero no se aplican sobre las funciones y servicios críticos
- ◯ Existe misión, visión y objetivos para los servicios y funciones críticas
- ◯ Existe misión, visión y objetivos para todos los servicios y funciones de la organización

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

- ◯ No existe una política de seguridad
- ◯ Existe una política de seguridad no aprobada por dirección
- ◯ Existe una política de seguridad aprobada por dirección pero sin gobierno ni gestión del riesgo
- ◯ Existe una política de seguridad aprobada por dirección y conocida por toda la compañía, con un gobierno y gestión del riesgo

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

- ◯ No se identifican las vulnerabilidades ni amenazas
- ◯ Se identifican de manera parcial las vulnerabilidades y amenazas
- ◯ Se identifican las vulnerabilidades y amenazas pero no se analiza el riesgo de negocio
- ◯ Se identifican las vulnerabilidades y amenazas, y se analiza el riesgo de negocio

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

- ◯ No existe un proceso de gestión del riesgo
- ◯ Existe un proceso de gestión del riesgo pero no se define el nivel de tolerancia
- ◯ Existe un proceso de gestión del riesgo y un nivel de tolerancia pero no es conocido ni acordado por todas partes interesadas
- ◯ Existe un proceso de gestión del riesgo y se han establecido los niveles de tolerancia en base a los acuerdos entre las partes interesadas

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

- ◯ No existe un proceso de gestión de riesgos de la cadena de suministro
- ◯ No existe un proceso de gestión del riesgo pero se establecen los requisitos en los contratos
- ◯ Existe un proceso de gestión del riesgo de terceros y se establecen las medidas en los contratos, pero no se auditan
- ◯ Existe un proceso de gestión del riesgo de terceros y se establecen las medidas necesarias en los contratos, así como los procesos para medir su cumplimiento

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

- ◯ No existe la gestión de identidades ni accesos a los activos de la organización
- ◯ Existe una gestión de identidades parcial pero no se cruza con el acceso físico a los activos
- ◯ Existe una gestión de identidades y accesos, pero no se establecen los controles para garantizar el menor privilegio y la segregación de funciones
- ◯ Existe una gestión de identidades y accesos en base al principio de menor privilegio y segregación de funciones

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

- ◯ No existe un proceso de formación y concienciación
- ◯ Existe un proceso de formación y concienciación parcial pero no todos los usuarios están incluidos
- ◯ Existe un proceso de formación y concienciación conocido que se realiza anualmente
- ◯ Existe un proceso de formación y concienciación medible y repetible, para todos los empleados y colaboradores

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

- ◯ No están identificados los datos y no se protegen
- ◯ Están identificados los datos pero no se protegen
- ◯ Están identificados los datos pero se protegen de manera parcial
- ◯ Los datos están identificados y protegidos independiente de su estado y entorno para garantizar la confidencialidad, integridad y disponibilidad

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

- ◯ No existen procesos y procedimientos de seguridad
- ◯ Existen procesos y procedimientos que cubren parcialmente los ámbitos definidos en la política de seguridad
- ◯ Los procesos y procedimientos están documentados, pero no todos están implementados
- ◯ Todos los procesos y procedimientos están implementados y se revisan de forma periódica

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

- ◯ No se controlan los mantenimientos
- ◯ Se controlan los mantenimientos in situ pero no los remotos
- ◯ Se controlan los mantenimientos in situ y remotos, pero no se auditan los accesos
- ◯ Se controlan los mantenimientos in situ y remotos, y se auditan los accesos a los sistemas

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

- ◯ No existen medidas técnicas
- ◯ Existen medidas técnicas que cubren parcialmente los requerimientos de seguridad
- ◯ Existen medidas técnicas que cubren los requerimientos de seguridad
- ◯ Existen medidas técnicas completas incluyendo registros de bitácora para asegurar el correcto funcionamiento de las mismas

* 25. ¿Dispone su organización de sistemas para la recolección de eventos?

- ◯ No existen sistemas para la recolección de eventos
- ◯ Existen sistemas para la recolección de eventos pero únicamente para un porcentaje menor de los sistemas y redes
- ◯ Existen sistemas para la recolección de eventos que cubren los sistemas y redes clave del negocio
- ◯ Existen sistemas para la recolección de eventos que cubren todos los sistemas y redes de mi organización

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

- ◯ No se lleva a cabo el análisis de eventos
- ◯ Se analizan los eventos de forma reactiva
- ◯ Se realiza análisis de actividad anómala ad-hoc mediante métodos manuales
- ◯ Se realiza análisis de comportamiento mediante métodos automáticos en función de umbrales definidos

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

- ◯ No se monitoriza la actividad de los usuarios o dispositivos en los sistemas y redes de la organización
- ◯ La monitorización de la actividad de los usuarios o dispositivos es muy limitada, y no permite la detección de eventos de ciberseguridad. No se llevan a cabo escaneos de seguridad
- ◯ Se monitoriza la actividad de los usuarios o dispositivos en los sistemas críticos de negocio. Se llevan a cabo escaneos de seguridad a demanda
- ◯ Toda la actividad de los usuarios y los dispositivos está monitorizada. Se llevan a cabo escaneos de seguridad de manera regular

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

- ◯ No están definidos los procedimientos o roles para los procesos de detección de incidentes
- ◯ Existen procedimientos de detección si bien no se encuentran formalmente definidos y documentados. Los roles y responsabilidades no están asignados
- ◯ Los procedimientos de detección están definidos, aunque no todas las responsabilidades se encuentran asignadas. Se llevan a cabo pruebas 1 vez al año
- ◯ Los procedimientos de detección están definidos, y todos los roles y responsabilidades asignados. Se prueban y actualizan 2 veces al año

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

- ◯ No están definidos los procedimientos de respuesta ante incidentes
- ◯ Existen procedimientos de respuesta ante incidentes si bien no se encuentran documentados. No se llevan a cabo pruebas de manera regular
- ◯ Los procedimientos de respuesta ante incidentes están documentados y se llevan a cabo pruebas anuales
- ◯ Los procedimientos de respuesta ante incidentes están formalmente documentados y actualizados y se llevan a cabo pruebas 2 pruebas al año

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

- ◯ Los procesos, roles e interlocutores para la respuesta ante incidentes no están identificados
- ◯ Únicamente los procesos clave de respuesta ante incidentes están identificados. Los roles e interlocutores no están definidos formalmente
- ◯ Los principales procesos, roles e interlocutores están identificados. Se les forma y capacita de manera regular (1 vez al año). La comunicación y coordinación es ad-hoc
- ◯ Todos los procesos, roles e interlocutores están identificados. Se les forma y capacita de manera regular (2 veces al año). La comunicación y coordinación se realiza de acuerdo a procedimientos definidos

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

- ◯ No se analizan las alertas de los sistemas de detección
- ◯ Únicamente un conjunto de alertas se investigan, pero sin SLAs formalizados
- ◯ Las alertas más relevantes se investigan de acuerdo a un proceso definido, pero sin SLAs formalizados
- ◯ La totalidad de las alertas se investigan de acuerdo a un proceso definido con SLAs formalizados

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

- ◯ La organización no lleva a cabo análisis forenses.
- ◯ Se lleva a cabo un análisis forense de un número limitado de eventos detectados (inferior al 10% de las detecciones).
- ◯ Se lleva a cabo un análisis forense de los eventos detectados mas relevantes (inferior al 25% de las detecciones).
- ◯ Se lleva a cabo un análisis forense de un elevado conjunto de los eventos mas relevantes detectados (superior al 50% de las detecciones).

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

- ◯ No existen sistemas o procesos para la identificación temprana de vulnerabilidades
- ◯ La identificación temprana de vulnerabilidades se realiza mediante procesos manuales. Los procesos de contención y mitigación son manuales
- ◯ La identificación temprana de vulnerabilidades se realiza mediante procesos automáticos. Los procesos de contención y mitigación son manuales
- ◯ La identificación temprana de vulnerabilidades se realiza mediante sistemas automatizados, y los procesos de contención y mitigación son automáticos

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

- ◯ No hay un proceso formal para la revisión y mejora de los procesos de respuesta ante incidentes
- ◯ Existen planes de respuesta pero éstos se revisan de manera ad-hoc
- ◯ Los planes de respuesta se revisan como mínimo 1 vez al año, e incorporan algunas lecciones aprendidas de incidentes pasados
- ◯ Los planes de respuesta se revisan como mínimo 2 veces al año, y existe un proceso para la incorporación de lecciones aprendidas

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

- ◯ No se dispone de planes formalizados para la recuperación de los sistemas ante incidentes de ciberseguridad
- ◯ Se dispone de planes de recuperación, si bien no son seguidos paso a paso por la organización. Los planes se revisan de manera ad-hoc
- ◯ Se dispone de planes de recuperación, si bien pueden no ser seguidos paso a paso por la organización. Cualquier desviación relevante sobre el plan se aprueba y documenta. Los planes se revisan 1 vez al año
- ◯ Se dispone de planes de recuperación y estos son seguidos paso a paso por la organización. Cualquier desviación sobre el plan se aprueba y documenta. Los planes se revisan 2 veces al año

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

- ◯ Los planes o estrategias de recuperación no se actualizan regularmente
- ◯ Los planes de recuperación se revisan de manera ad-hoc y no se incorporan lecciones aprendidas de incidentes pasados
- ◯ Los planes de recuperación se revisan de manera regular (1 vez al año), e incorporan alguna lección aprendida de incidentes pasados
- ◯ Los planes de recuperación se revisan de manera regular (2 veces al año), y existe un proceso para incorporar lecciones aprendidas

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

- ◯ No están definidos los roles en la comunicación para los procesos de recuperación ante incidentes de seguridad
- ◯ Algunos roles de comunicación y coordinación en la recuperación están definidos. No hay canales formalmente definidos para la comunicación
- ◯ Los principales roles de comunicación y coordinación en la recuperación están definidos. Existen canales informales para la comunicación
- ◯ Todos roles de comunicación y coordinación en la recuperación están formalmente definidos. Existen canales formales para la comunicación y no se usan canales alternativos

38. El contexto actual, ¿Cómo ha afectado a las ciberamenazas que ha recibido su organización?

- ◯ Ha hecho que aumenten considerablemente
- ◯ Ha hecho que aumenten ligeramente
- ◯ Ha hecho que se mantengan
- ◯ Ha hecho que disminuyan ligeramente
- ◯ Ha hecho que disminuyan considerablemente

39. El contexto actual, acumulado en los últimos años, ¿Cómo ha afectado a la carga de trabajo, nivel de presión y estrés de su equipo de ciberseguridad?

- ◯ Ha hecho que aumenten considerablemente
- ◯ Ha hecho que aumenten ligeramente
- ◯ Ha hecho que se mantengan
- ◯ Ha hecho que disminuyan ligeramente
- ◯ Ha hecho que disminuyan considerablemente

40. ¿Ha realizado su empresa alguna acción adicional en materia de ciberseguridad a raíz del conflicto de Ucrania? *(marque tantas respuestas como sea necesario)*

- ☐ No hemos realizado ninguna acción adicional a las ya planificadas
- ☐ Hemos realizado un análisis de riesgos actualizando las nuevas amenazas o parámetros de riesgo
- ☐ Hemos reforzado la monitorización de los eventos de seguridad
- ☐ Hemos revisado nuestros procedimientos de respuesta ante incidentes
- ☐ Hemos realizado simulacros de incidentes considerando impacto en producción o servicio ofrecido a raíz de un evento generado por el conflicto

41. El contexto actual, ¿en qué medida ha afectado mediante ciberataques a la cadena de suministros de su organización?

- ◯ No ha afectado
- ◯ Ha afectado ligeramente
- ◯ Ha afectado considerablemente
- ◯ Ha afectado de manera crítica

42. ¿En qué medida ha afectado la crisis global de suministros al plan de ciberseguridad de su organización (retrasos, adaptaciones y cambios en el mismo)?

- ◯ No le ha afectado
- ◯ Le ha afectado ligeramente
- ◯ Le ha afectado considerablemente
- ◯ Le ha afectado de manera crítica

43. Por último, si desea que le hagamos llegar los resultados del estudio a su finalización, indíquenos una dirección de correo electrónico. Su dirección se utilizará exclusivamente para el envío del estudio.

Listo

III Indicador de madurez en ciberseguridad

OBSERVATORIO DE LA CIBERSEGURIDAD

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

@ISMSForum

ISMS Forum

Una iniciativa de

ISMS FORUM