II Indicador de madurez en ciberseguridad

OBSERVATORIO DE LA CIBERSEGURIDAD

isms forum INTERNATIONAL INFORMATION SECURITY COMMUNITY

isms BARCELONA INTERNATIONAL INFORMATION SECURITY COMMUNITY

II Estudio sobre el nivel de madurez en ciberseguridad

Con la participación de los siguientes profesionales y organizaciones:

Coordinadores:

David Esteban

Olga Forné

Toni García

Pedro López

David Llorente

Santiago Minguito

Iván Sánchez

Óscar Sánchez

Diseño y maquetación:

Raquel García, Responsable de Comunicación Externa de ISMS Forum

ÍNDICE

ISMS Forum y su nueva 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 ha consolidado 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 da 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 socio-económico 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.

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.

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 EE. UU., 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 ISMS Forum pone a disposición del mercado una herramienta de evaluación a través del indicador nacional de madurez en ciberseguridad, en su segunda edición, con el que las organizaciones puedan determinar el nivel de riesgo que mantienen en comparación con la media establecida, así como evaluar las diferencias respecto a los resultados de la primera edición.

El Estudio sobre el nivel de madurez en ciberseguridad de la empresa española es el primer análisis que establece el Observatorio de la Ciberseguridad de ISMS Forum 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 fenómenos.

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.

En esta segunda edición del Observatorio se han añadido dos indicadores adicionales al del nivel de madurez mencionado anteriormente. El primero está relacionado con los recursos y organización de la ciberseguridad en la Empresa Española, con el objetivo de analizar recursos, presupuesto y tipología de operación de la ciberseguridad. Por último,

un indicador temporal para analizar la influencia de la pandemia COVID-19, en cuanto a evolución de las ciberamenazas, impacto en recursos dedicados a ciberseguridad, efecto del teletrabajo y concienciación de la alta dirección.

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 80 directores de seguridad de la información que operan en el ámbito territorial nacional, tanto en empresas multinacionales como nacionales. No se ha recopilado información de empresas proveedoras de servicios de ciberseguridad.

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

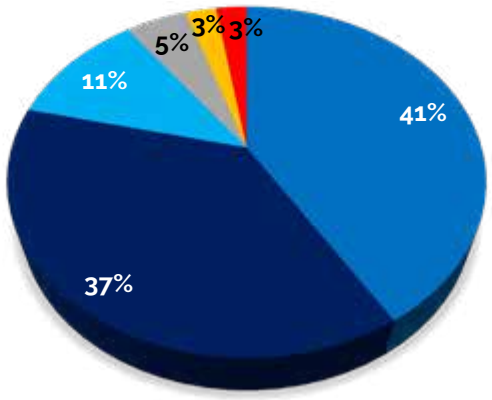
Planificación de recuperación, Mejoras y Comunicaciones.

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.

Tipología de la muestra

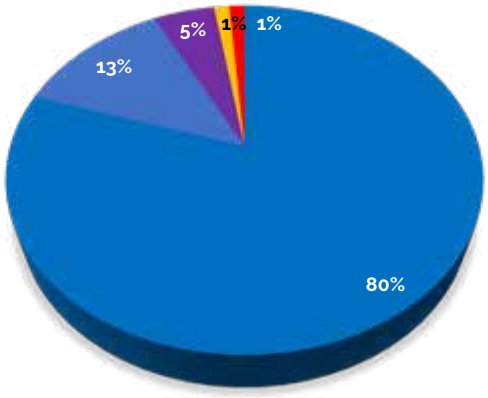
En la presente edición, hemos contado con la participación de 80 empresas, de las cuales un 37% facturan más de 1.000 millones de Euros y el 41% más de 100. El 93% de los encuestados ocupan puestos de responsabilidad o son especialistas de seguridad de la información. Dado que el orden de comentario es inverso al de los gráficos, sugiero cambiar uno de ellos.

¿Cuál es el volumen de facturación anual de su organización?



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

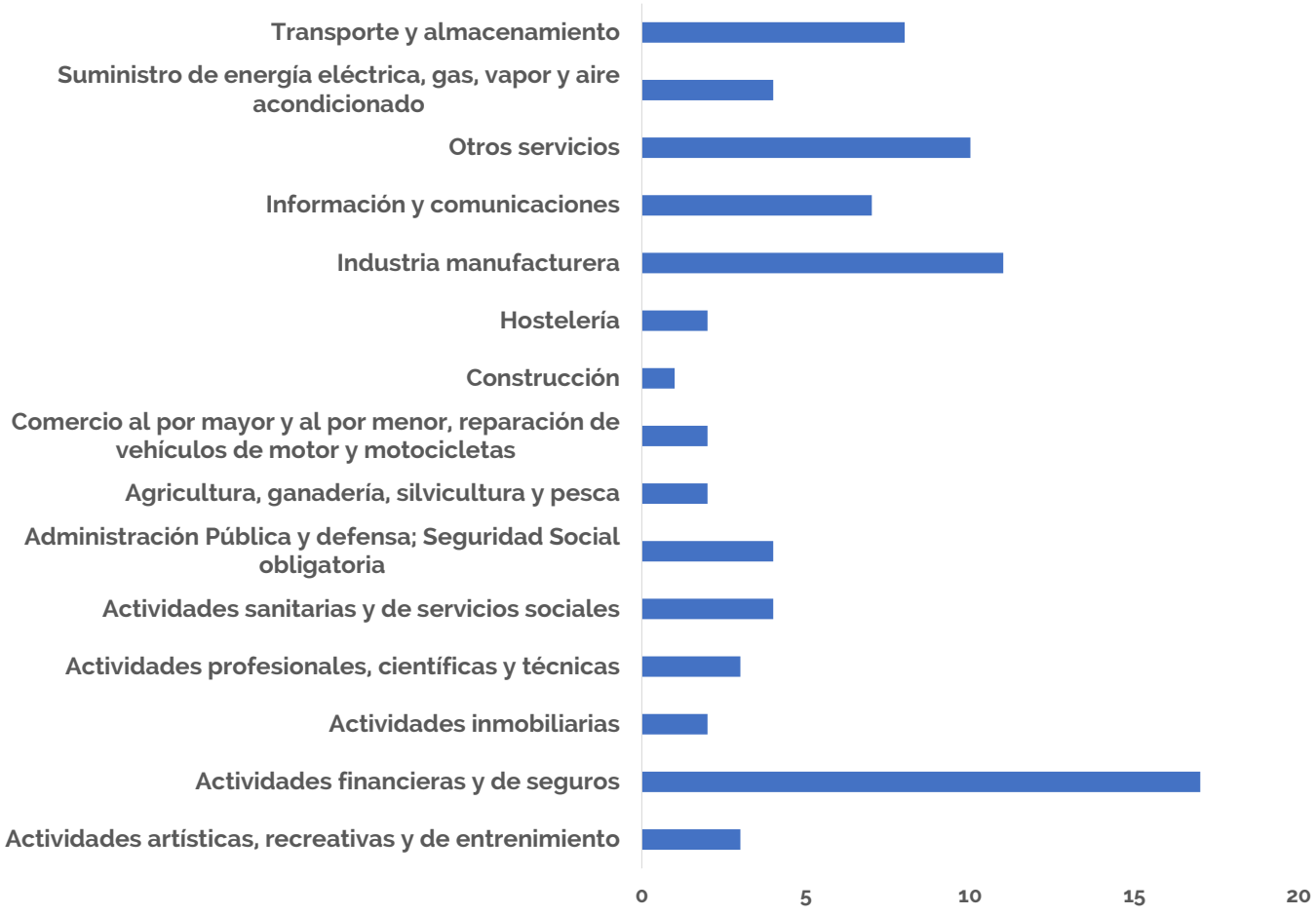
¿Qué puesto ocupa en su organización?



- Dirección/Responsable de la Seguridad de la información
- Especialista en Seguridad de la información
- Dirección/Responsable de TI
- Otro puesto de Dirección
- Especialista en TI

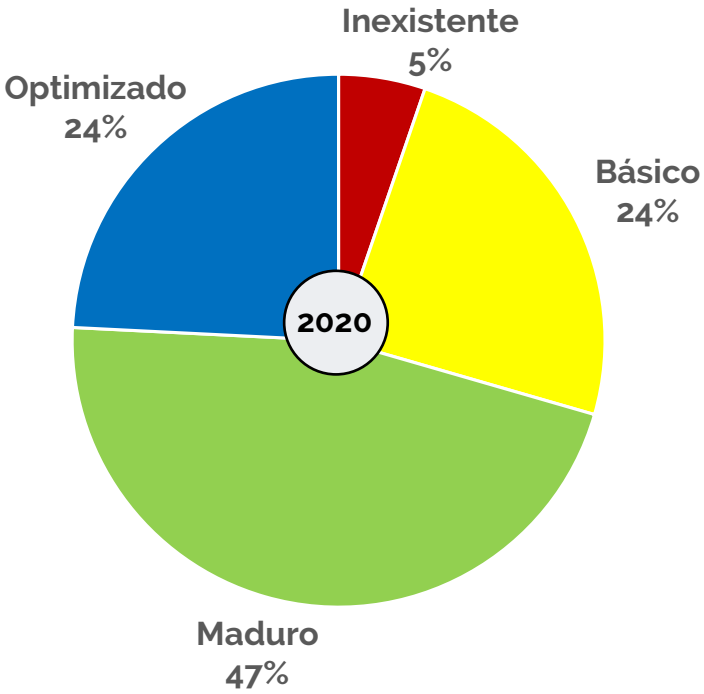
Se ha obtenido una alta representatividad en los sectores Financiero y Seguros, Industria Manufacturera, Transporte y Almacenamiento, e Información y Comunicaciones.

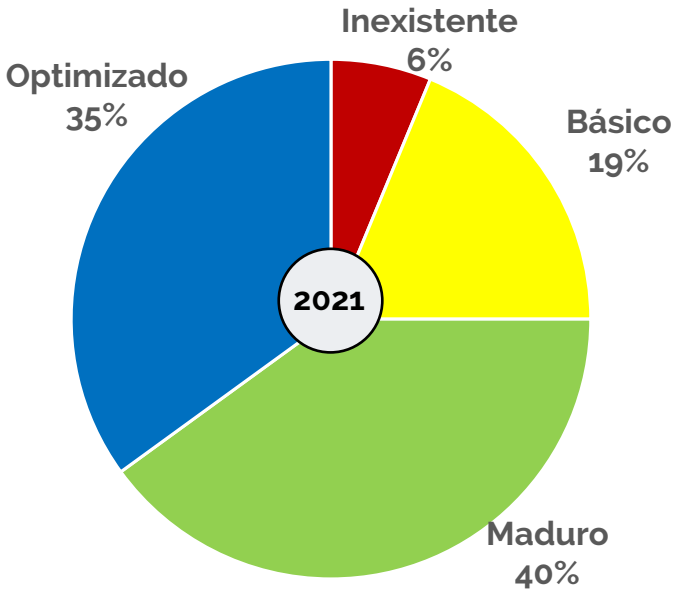
Sector



Principales indicadores

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



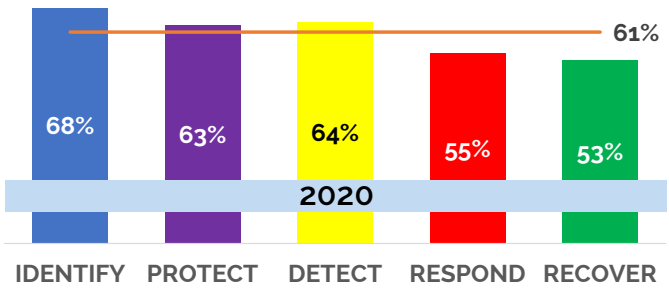


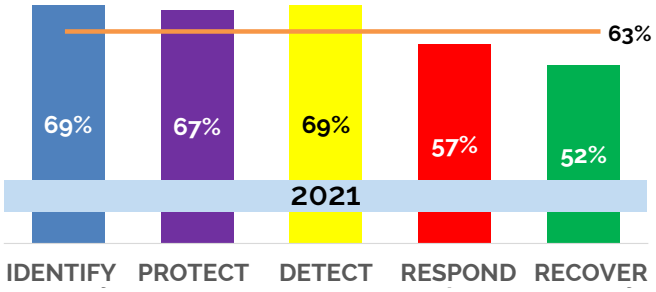
Se observa una evolución de los niveles de madurez, con una mejora considerable en el grado de madurez "optimizado", donde en el año 2020, el 24% de las empresas encuestadas se consideraban incluidas en este segmento, y en el año en curso obtenemos 35%. Así mismo, la evolución positiva observada se extiende al hecho de que el conjunto de empresas con niveles elevados de madurez en ciberseguridad (maduro u optimizado) se ha incrementado hasta el 75%, respecto al 71% del año 2020.

Consecuentemente se han reducido los porcentajes en los niveles "maduro" y "básico". En cuanto al nivel "inexistente", tenemos 4 empresas incluidas en esta edición, respecto a 3 empresas en la edición anterior.

Nivel de Madurez por Dominio NIST

Sector	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER	Nivel de madurez
Construcción	100%	67%	92%	83%	56%	79%
Actividades financieras y de seguros	82%	81%	79%	70%	67%	76%
Información y comunicaciones	81%	78%	77%	67%	65%	74%
Suministro de energía eléctrica, gas, vapor y aire acondicionado	78%	74%	79%	60%	61%	70%
Comercio al por mayor y al por menor, reparación de vehículos de motor y motocicletas	72%	75%	75%	53%	56%	66%
Actividades inmobiliarias	83%	72%	67%	47%	56%	65%
Industria manufacturera	66%	71%	76%	57%	43%	63%
Transporte y almacenamiento	65%	67%	61%	59%	57%	62%
Otros servicios	63%	58%	65%	58%	43%	57%
Actividades artísticas, recreativas y de entrenimiento	57%	59%	50%	50%	52%	54%
Actividades profesionales, científicas y técnicas	59%	50%	53%	50%	56%	54%
Actividades sanitarias y de servicios sociales	60%	57%	54%	42%	42%	51%
Administración Pública y defensa; Seguridad Social obligatoria	50%	49%	52%	43%	22%	43%
Agricultura, ganadería, silvicultura y pesca	42%	47%	58%	28%	28%	41%
Hostelería	36%	36%	50%	25%	6%	31%



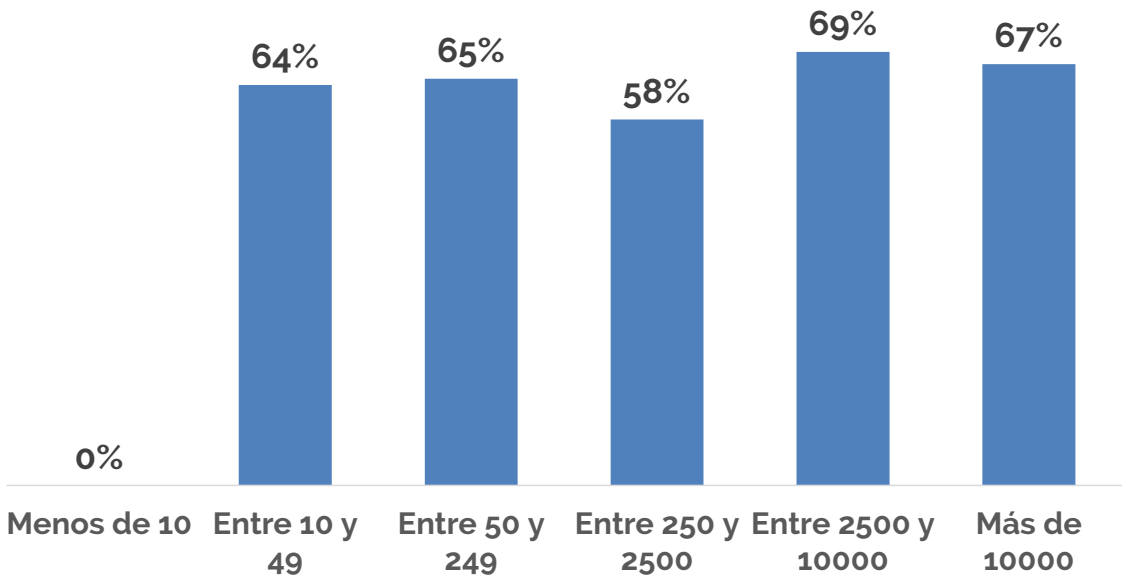


Al igual que en la edición anterior, el promedio de todos los dominios se sitúa en la franja alta de madurez básica, con una ligera mejora de dos puntos porcentuales.

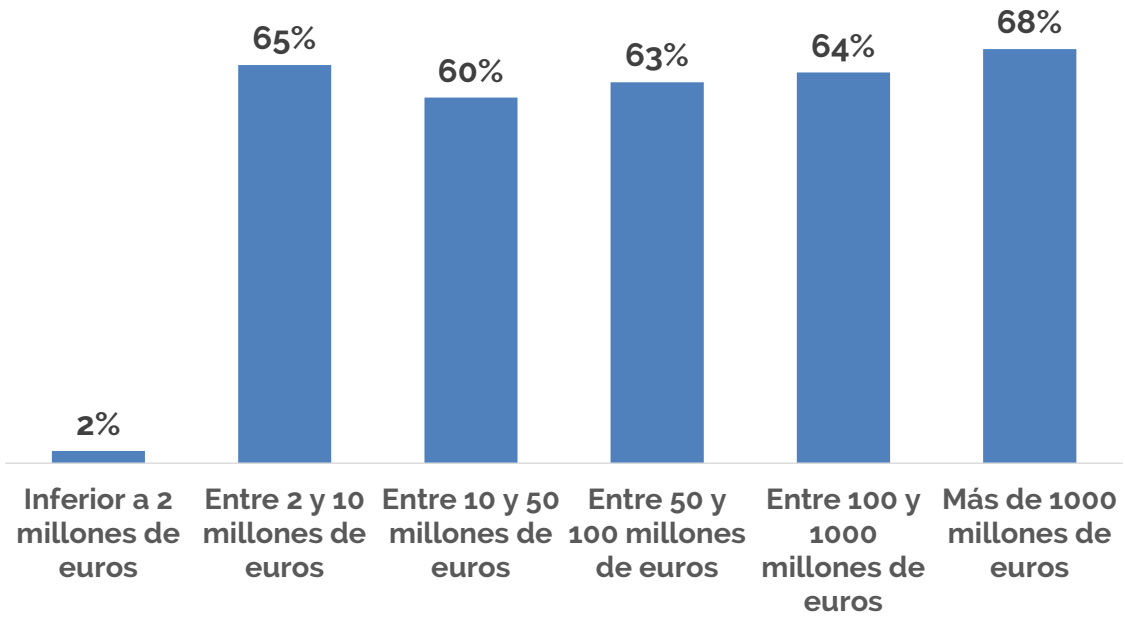
Sin embargo, se observa una mejora significativa en los ámbitos de Protect and Detect con un incremento de 4 y 5 puntos porcentuales respectivamente.

Respond y Recover siguen siendo los dominios que muestran una necesidad de mejora, mostrando el último un ligero retroceso respecto al año anterior.

Grado de madurez por número de empleados

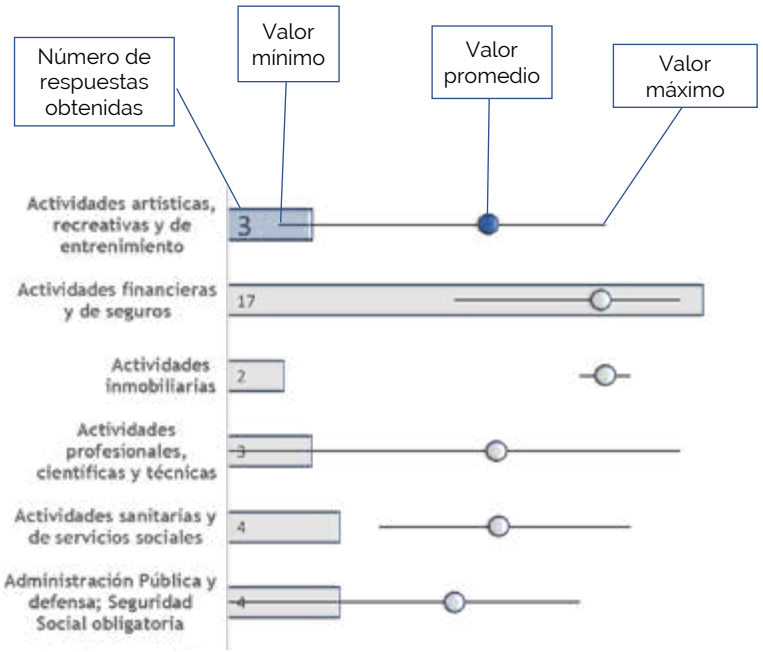


Grado de madurez por facturación

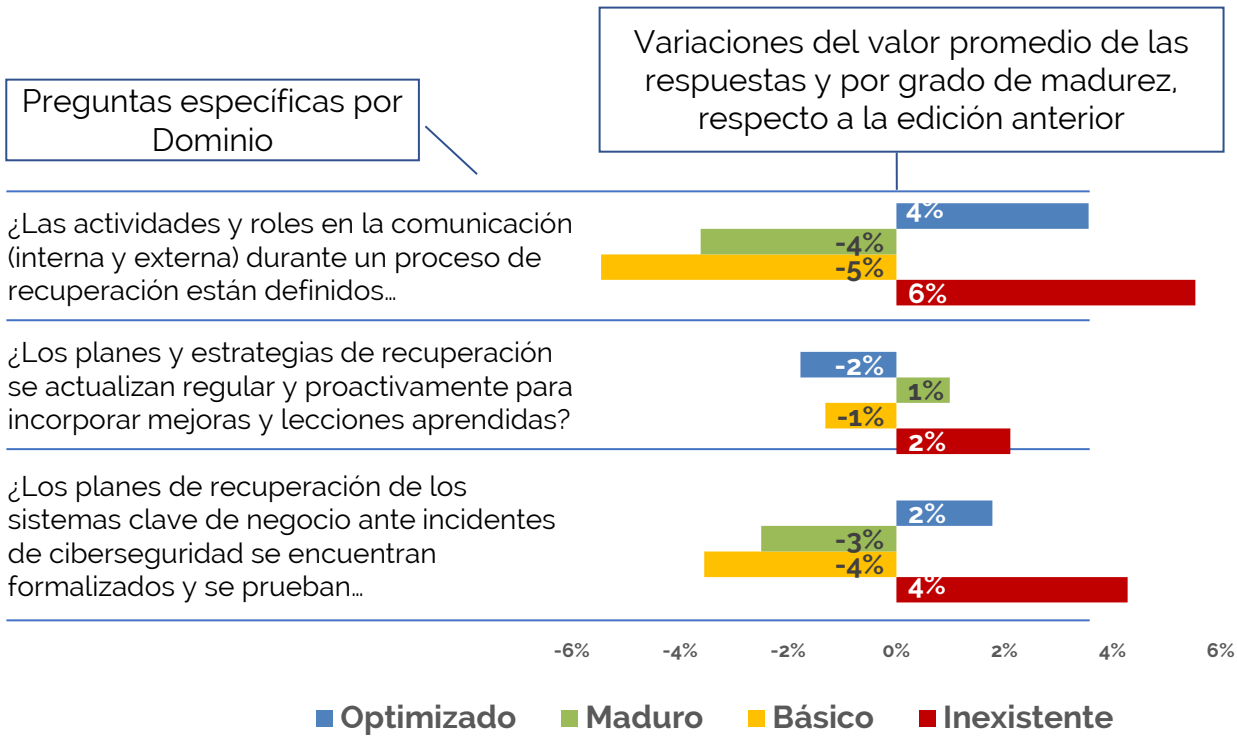


Grado de madurez por Dominio NIST y Sector Empresarial

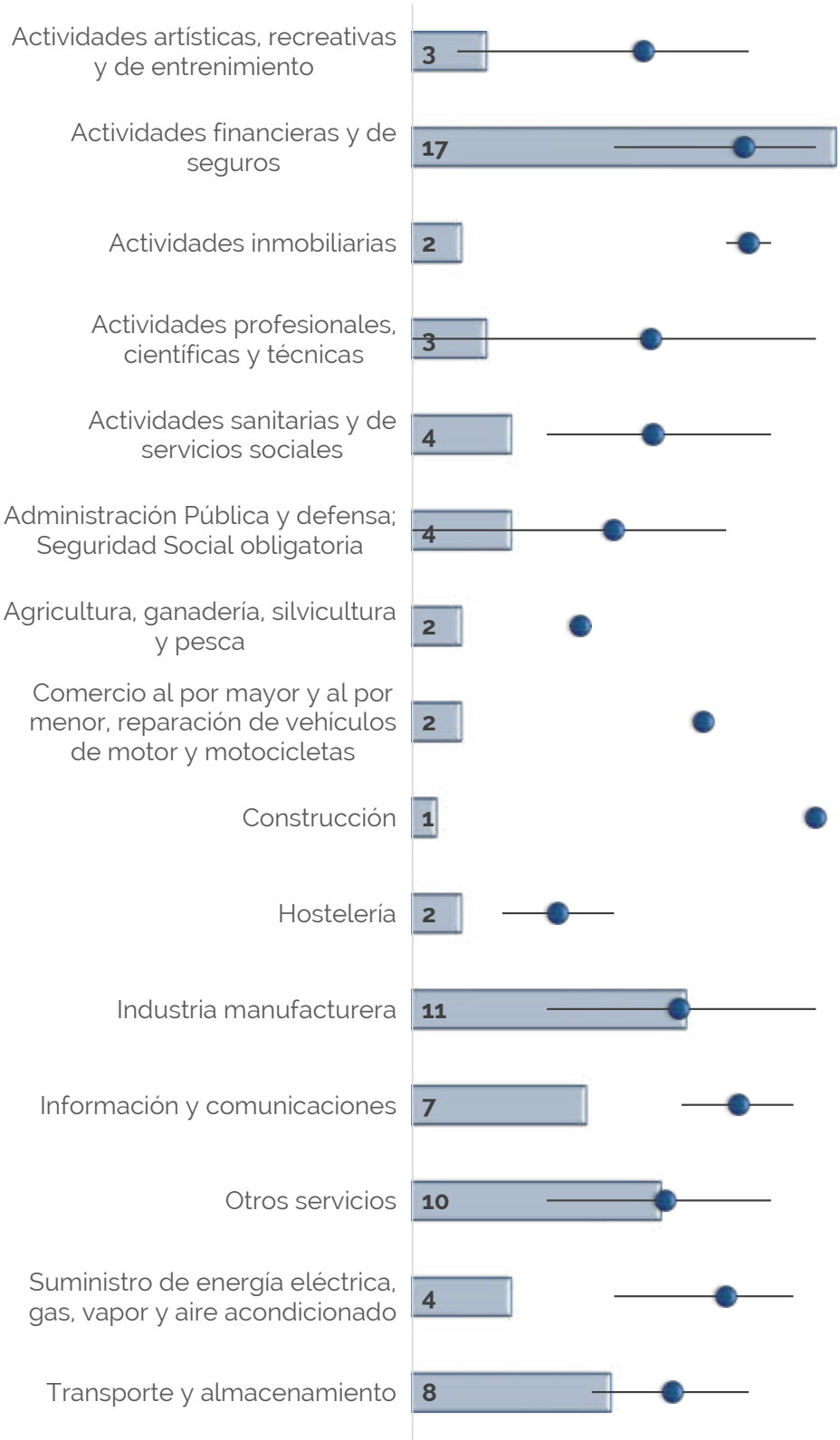
A continuación, se muestran los resultados obtenidos para cada uno de los Dominios del NIST, y por Sector Empresarial. En el gráfico de barras, se especifican el número de empresas que han cumplimentado la encuesta para cada uno de los Sectores representados. El gráfico de stock superpuesto al de barras,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



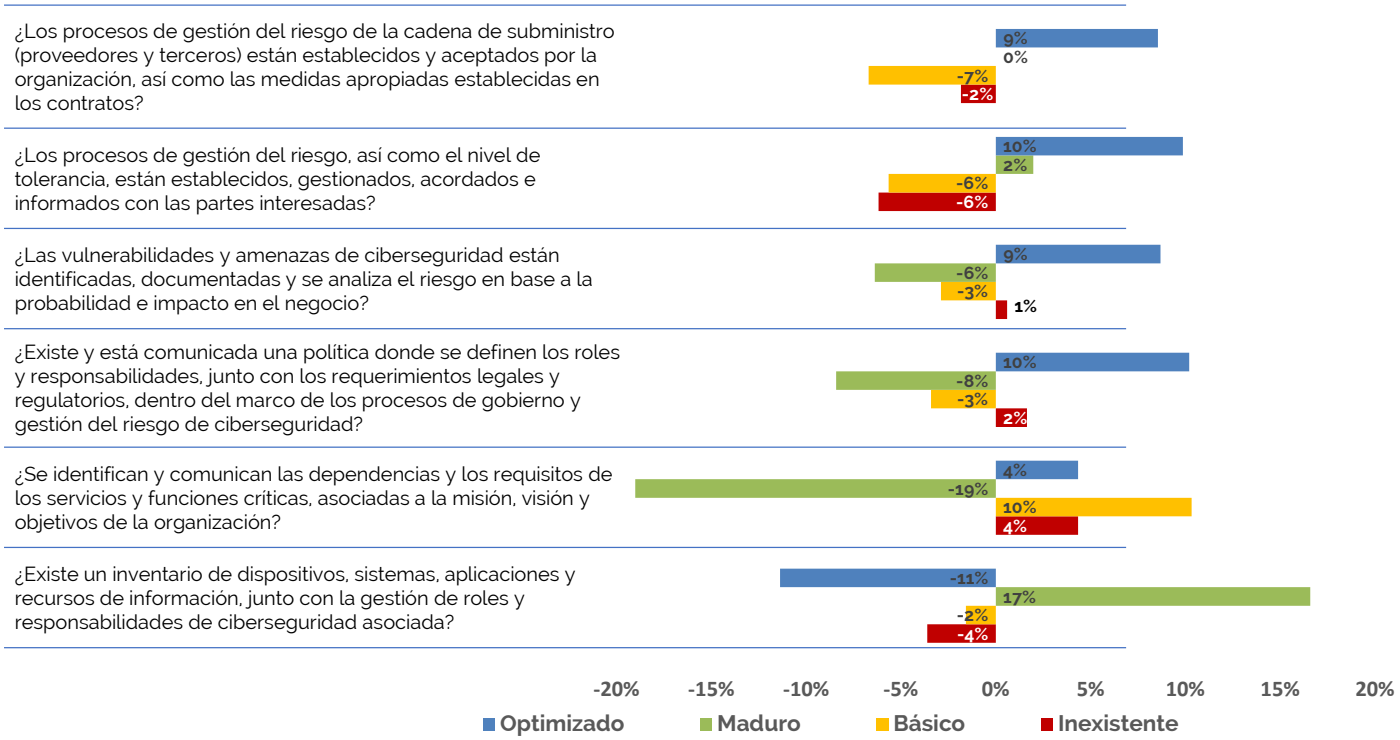
Se muestran también las diferencias obtenidas en los niveles de madurez para cada una de las preguntas respecto a la edición anterior. De este modo se analizan a nivel granular las tendencias para cada una de las áreas tratadas por Dominio NIST.



DOMINIO 1: IDENTIFICAR



Los sectores Financiero, Inmobiliario, Comercio, Información y Comunicaciones, y Utilities muestran mayor madurez, teniendo en cuenta la representación de la muestra. Cabe destacar la dispersión de la respuesta en los sectores de Actividades profesionales, científicas y técnicas, así como en la Administración Pública.



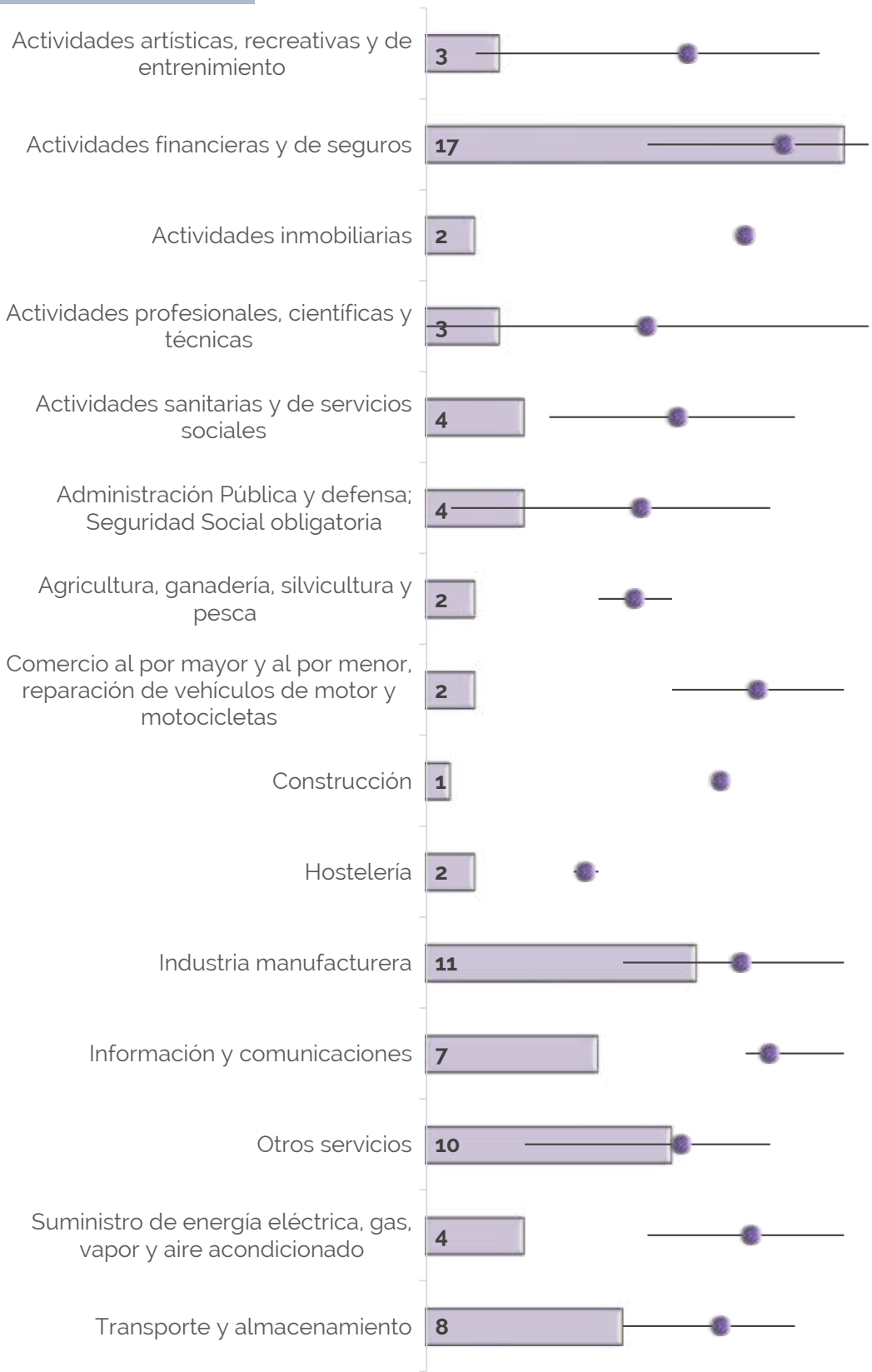
En comparación con el estudio de la primera edición, destaca la mejora en los procesos de gestión del riesgo y el nivel de tolerancia de los mismos, siendo éstos establecidos, gestionados, acordados e informados con las partes interesadas, en un 43% de la muestra, suponiendo un incremento del 10%. Asimismo, más del 70% de las empresas cuentan con 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, suponiendo también un incremento del 10% respecto a la edición anterior.

Se observa una mejora del 9% hacia el nivel optimizado, en cuanto a las empresas que mantienen identificadas y documentadas las vulnerabilidades y amenazas de ciberseguridad, y analizan el riesgo en base a la probabilidad e impacto en el negocio, llegando en esta edición al 55% de la muestra.

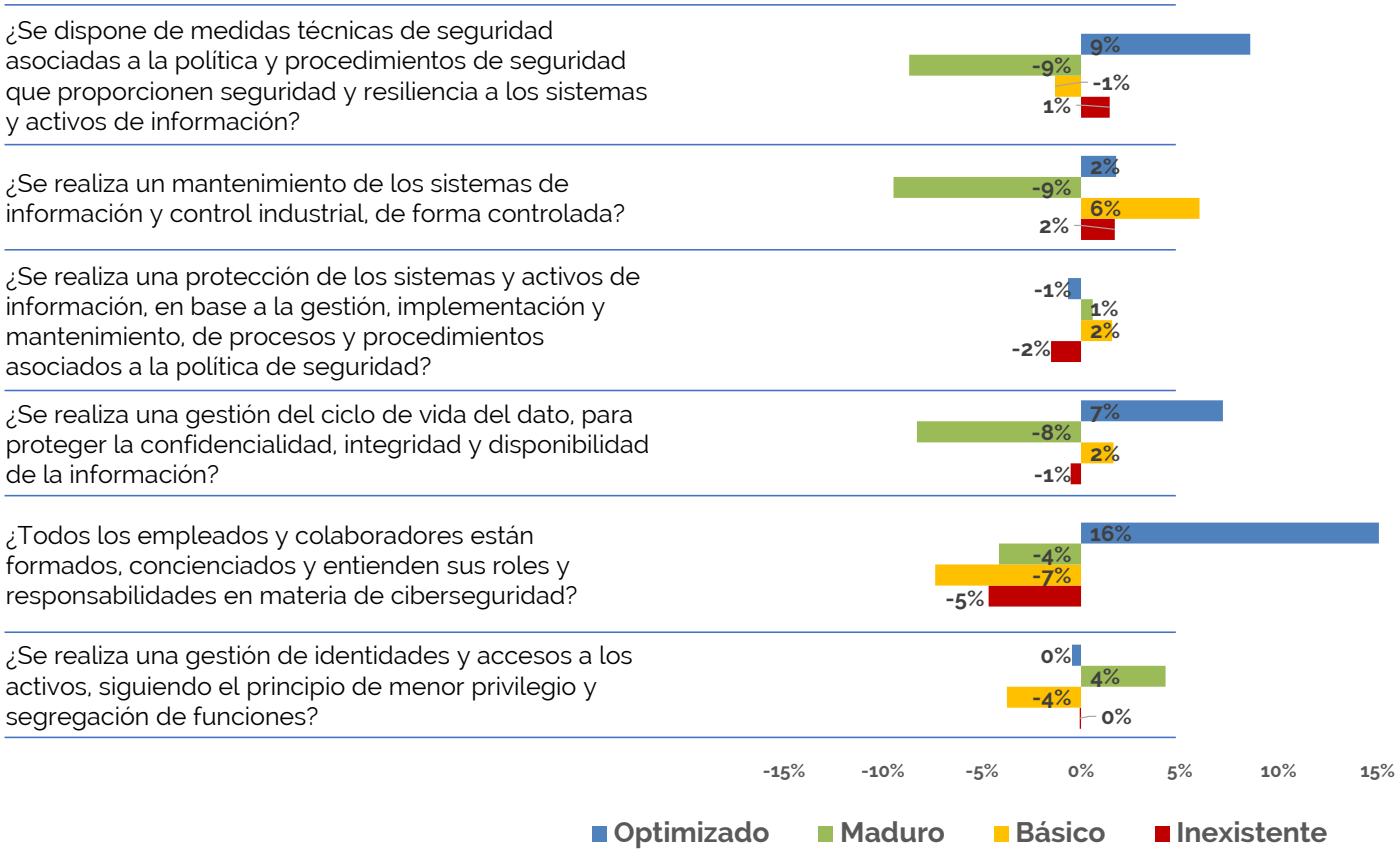
En el apartado de inventario de dispositivos, sistemas, aplicaciones y recursos de información, y gestión de roles y responsabilidades, se observa una convergencia de las respuestas hacia el grado de madurez "maduro", desde el "optimizado", "básico" e "inexistente", con un 45% de la muestra, respecto al 28% de la edición anterior.

Sin embargo se identifica una divergencia desde el maduro, hacia niveles colindantes, para las empresas que identifican y comunican las dependencias y los requisitos de los servicios y funciones críticas, asociadas a la misión, visión y objetivos de la organización, con un 26% de las mismas, lo que supone una reducción del 19% a la edición anterior.

DOMINIO 2: PROTEGER



El Sector Financiero y Seguros lideran el dominio, seguidos del manufacturero, otros servicios, transporte y almacenamiento. Destacar la dispersión de la respuesta en los sectores de Actividades Artísticas, recreativas, profesionales, científicas y técnicas, así como Administración Pública.



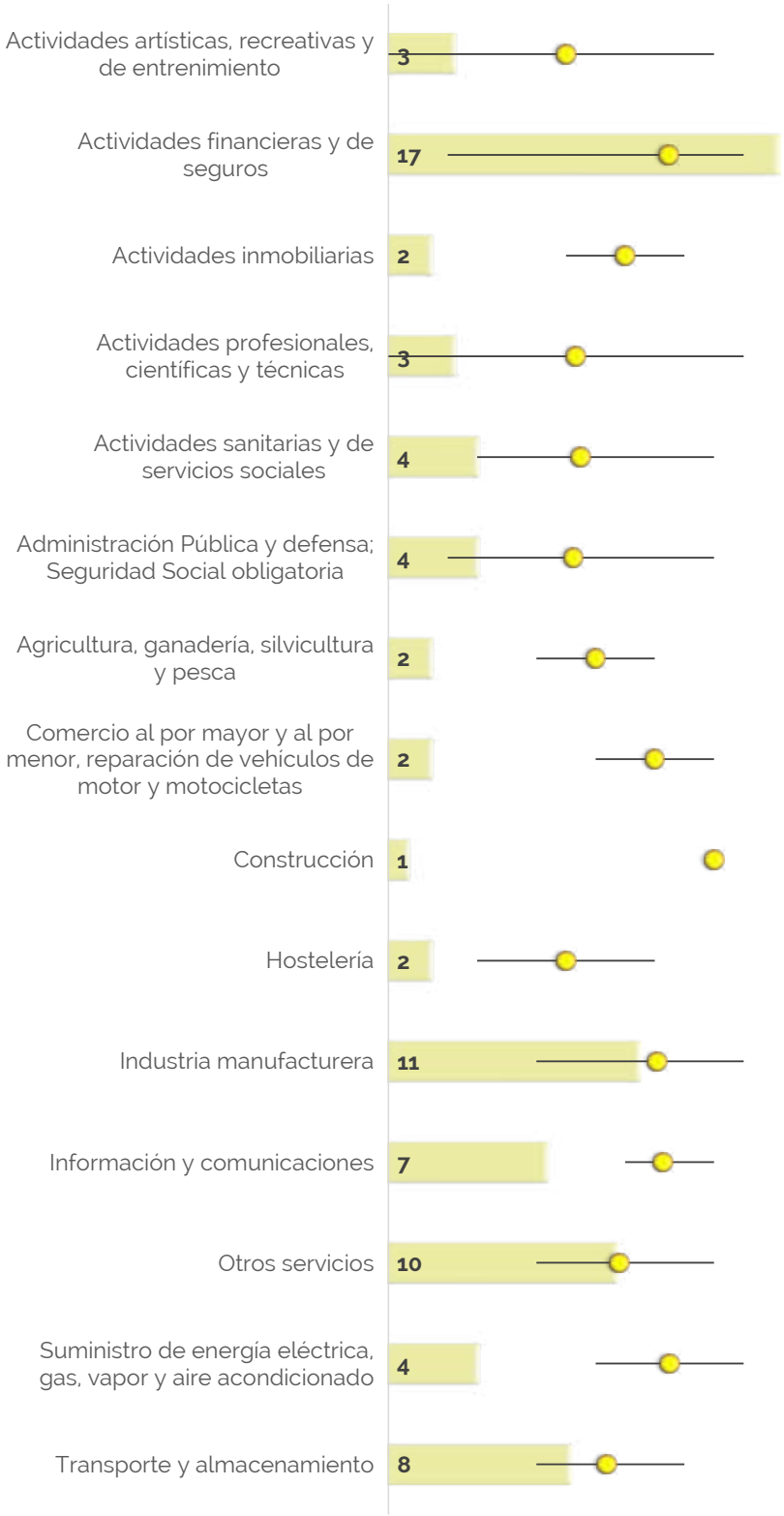
En comparación con el estudio de la primera edición, destaca la mejora en la formación y concienciación de empleados y colaboradores, siendo el proceso asociado establecido en un nivel óptimo para el 43% de la muestra, suponiendo un incremento del 16%. Asimismo, el 28% de las empresas cuentan con medidas técnicas completas incluyendo registros de bitácora, suponiendo también un incremento del 9% respecto a la edición anterior.

Se observa una mejora del 7% hacia el nivel optimizado, en cuanto a las empresas que realizan una gestión del ciclo de vida del dato, para proteger la confidencialidad, integridad y disponibilidad de la información, llegando en esta edición al 39% de la muestra.

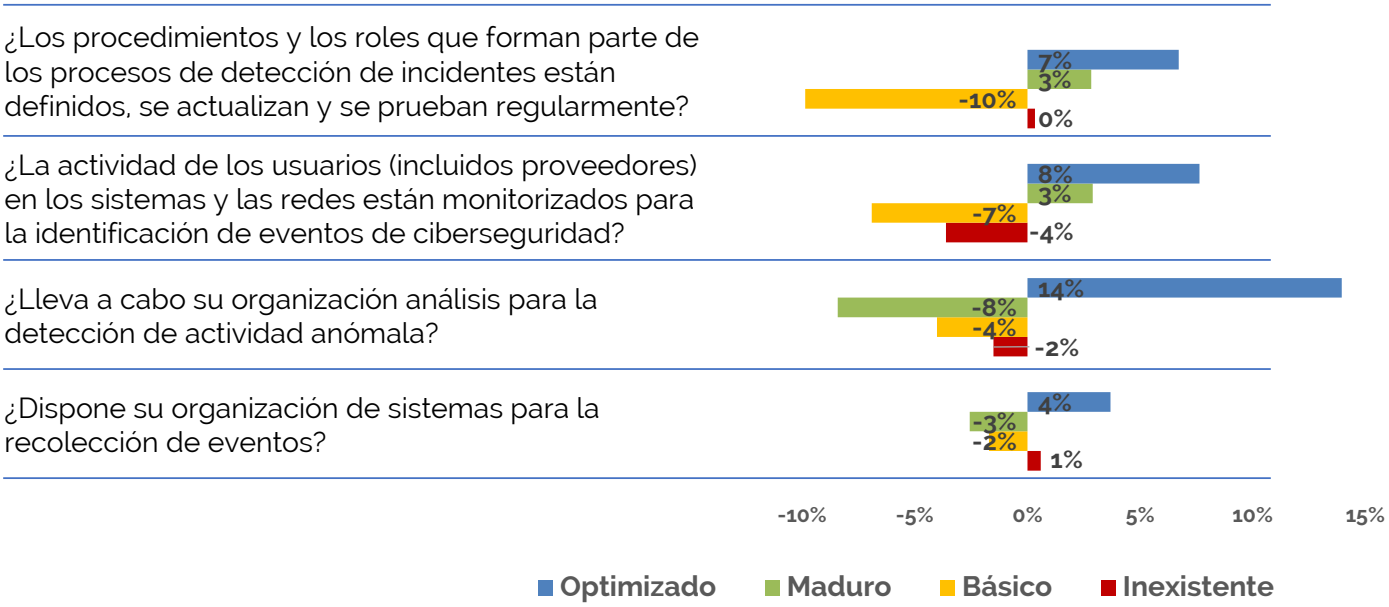
En el apartado de gestión de identidades y accesos, se observa una mejora del 4% desde el nivel de madurez básico, siendo ya el 78% de las empresas las que disponen de dicho proceso.

Por último, en el apartado de protección de los sistemas en base a la gestión, implementación y mantenimiento de procesos y procedimientos asociados a la política de seguridad, se observa una ligera convergencia de las respuestas hacia los grados de madurez "básico" y "maduro", desde el "optimizado" e "inexistente", con un 74% de la muestra, respecto al 72% de la edición anterior.

DOMINIO 3: DETECTAR



El Sector Financiero y Seguros lideran el dominio, seguidos del manufacturero, otros servicios, transporte y almacenamiento. Destacar la dispersión de la respuesta en los sectores de Actividades Artísticas, recreativas, profesionales, científicas y técnicas, así como Financiero y Seguros.

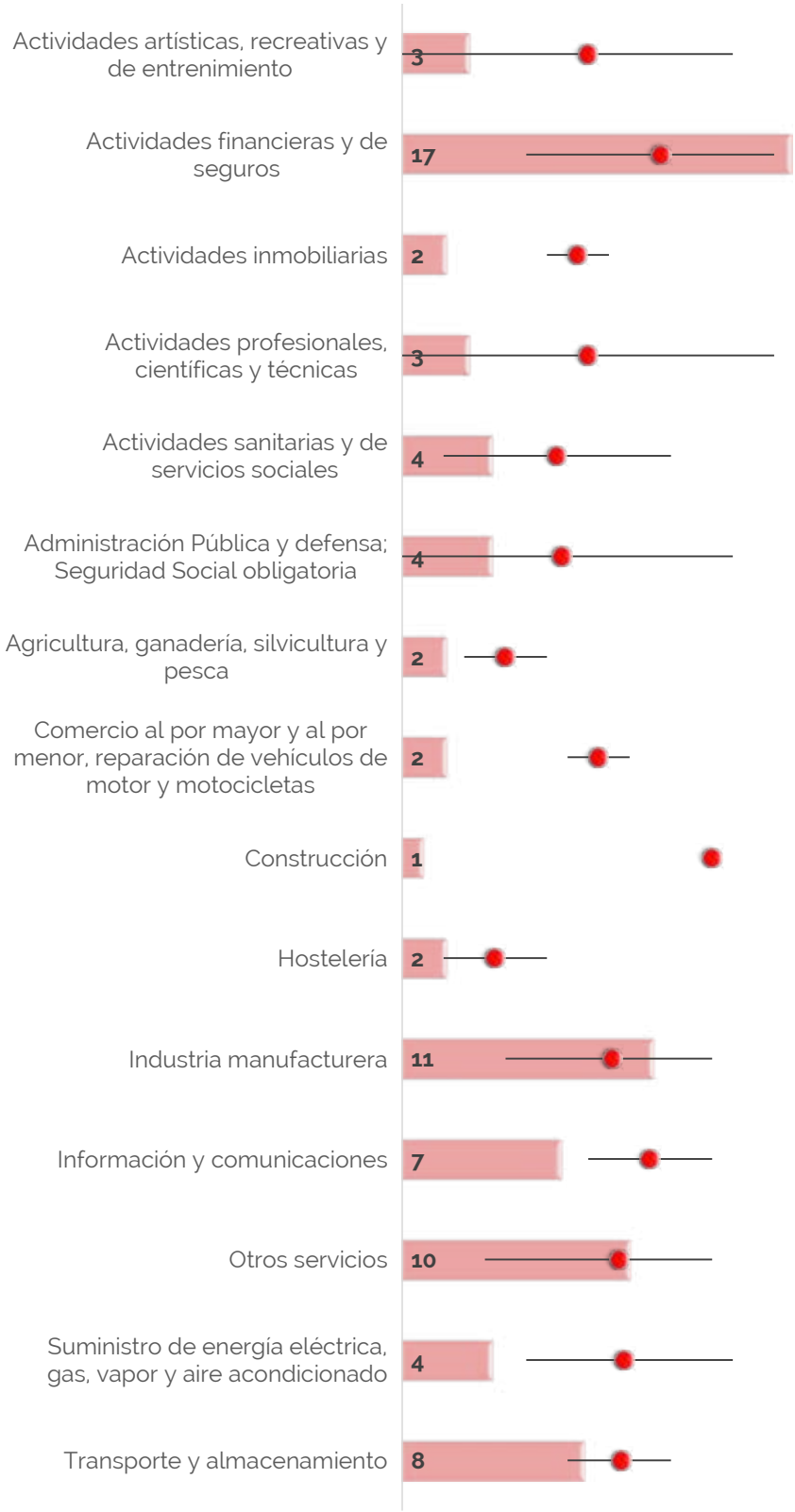


El dominio de "Detectar" mejora en todos los ámbitos en comparación con el estudio de la primera edición. Destaca de forma significativa la detección de actividad anómala, mediante la realización de análisis de comportamiento con métodos automáticos en función de umbrales definidos, en el 55% de la muestra, suponiendo un incremento del 14%.

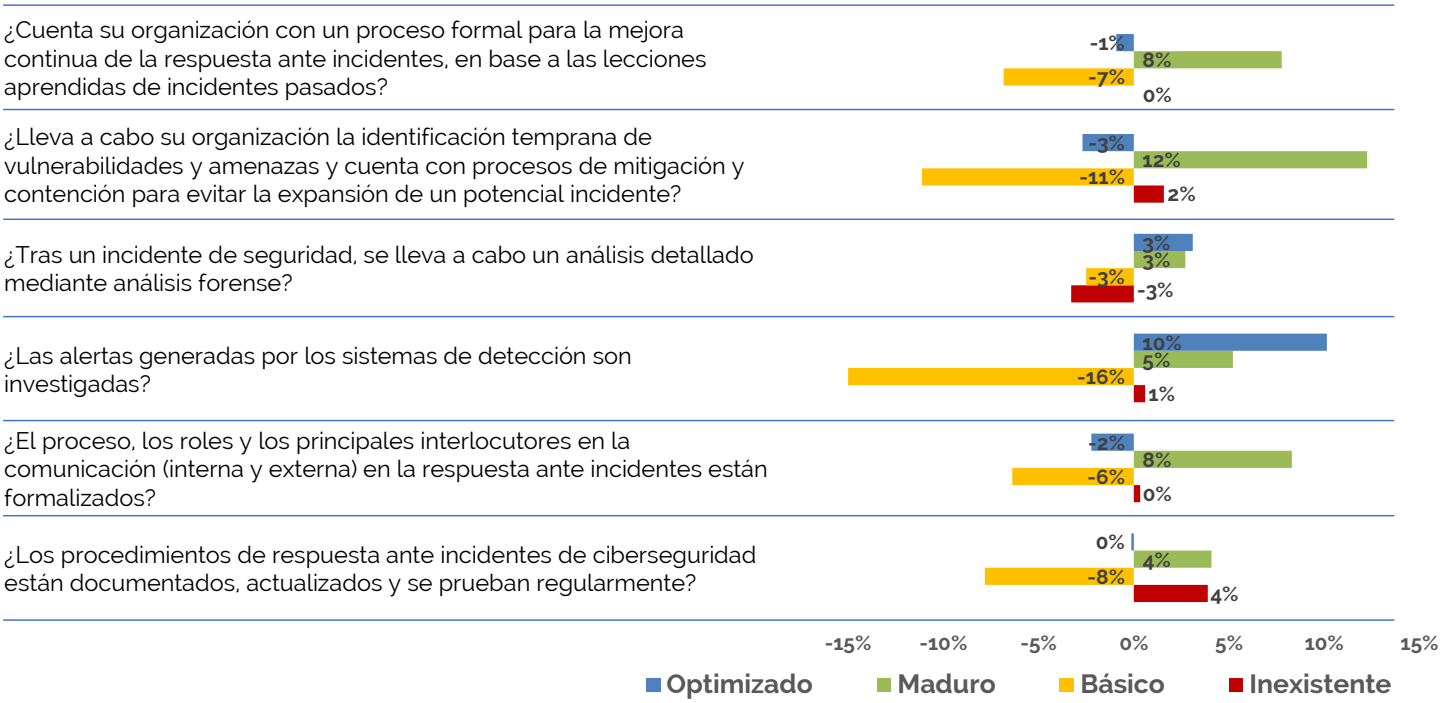
Asimismo, se observan incrementos entorno al 10% en grado de madurez en los apartados de monitorización de actividad de los usuarios, y procedimientos y procesos de detección de incidentes.

El apartado de recolección de eventos, si bien es el que menos crece con un 4%, muestra que el 96% de las empresas encuestadas disponen ya de sistemas de recolección y recogen eventos en mayor o menor medida.

DOMINIO 4: RESPONDER



El Sector Financiero y Seguros lideran el dominio, seguidos del manufacturero, otros servicios, transporte y almacenamiento. Destacar la dispersión de la respuesta en los sectores de Actividades Artísticas, recreativas, profesionales, científicas y técnicas, así como Administración Pública.

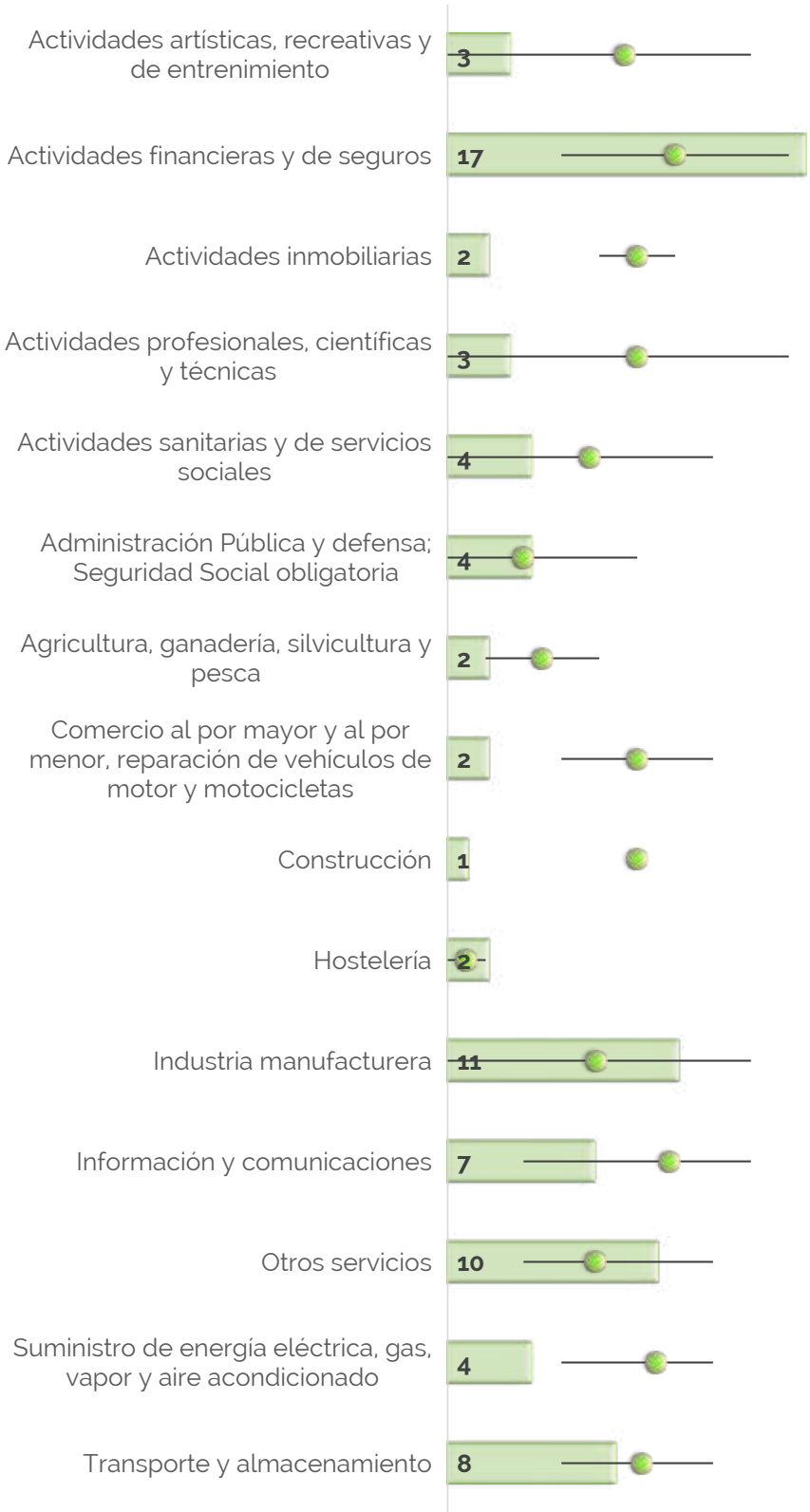


En comparación con el estudio de la primera edición, destaca de forma significativa la investigación de las alertas generadas por los sistemas de detección, con un incremento del 15%, siendo ya el 84% de las empresas, las que se encuentran en un grado maduro u optimizado. Asimismo, el 74% de las empresas realizan la identificación temprana de vulnerabilidades mediante procesos y/o sistemas automáticos, suponiendo también un incremento del 10% respecto a la edición anterior.

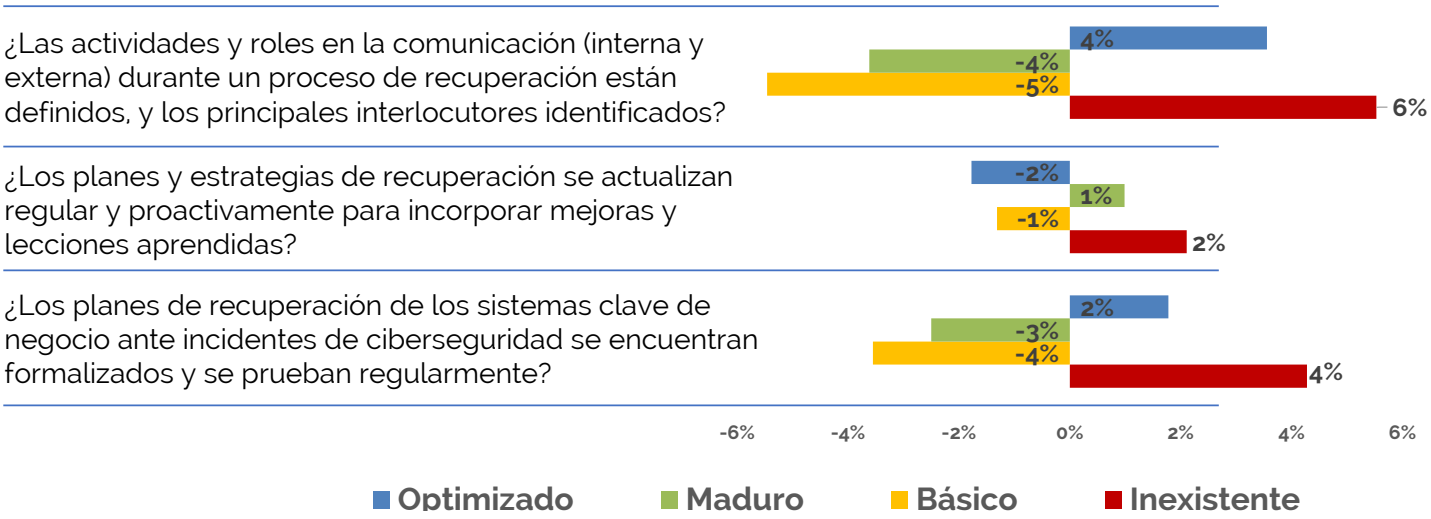
Del mismo modo, se observa una mejora del 8%, en cuanto a las empresas que disponen de planes de respuesta ante incidentes, y que los revisan como mínimo una vez al año, llegando en esta edición al 43% de la muestra. Mejora también la realización de análisis forenses después de un incidente de seguridad, con una mejora del 6%.

El único apartado que no muestra mejora, es el de procedimientos de respuesta, documentados, actualizados y probados, donde se observa una divergencia de las respuestas desde el grado de madurez "básico", hacia el "inexistente" y "maduro", con un 45% de la muestra, respecto al 28% de la edición anterior.

DOMINIO 5: RECUPERAR



El Sector Financiero y Seguros lideran el dominio, seguidos del manufacturero, otros servicios, transporte y almacenamiento. Destacar la dispersión de la respuesta en los sectores de Actividades Artísticas, recreativas, profesionales, científicas y técnicas, así como Manufacturera.



En general los resultados obtenidos en el dominio de "Recuperar" han empeorado respecto a la edición anterior. Se puede observar que si bien hay una mejora del 2% en cuanto las empresas que disponen de planes de recuperación y son seguidos paso a paso, hasta un 14% de la muestra aún no disponen de dichos planes de recuperación, suponiendo un decremento de 4 puntos porcentuales.

Respecto a la actualización de los planes de recuperación con el objetivo de incluir mejoras y lecciones aprendidas, se observan pequeñas variaciones de uno o dos puntos porcentuales entre grados de madurez.

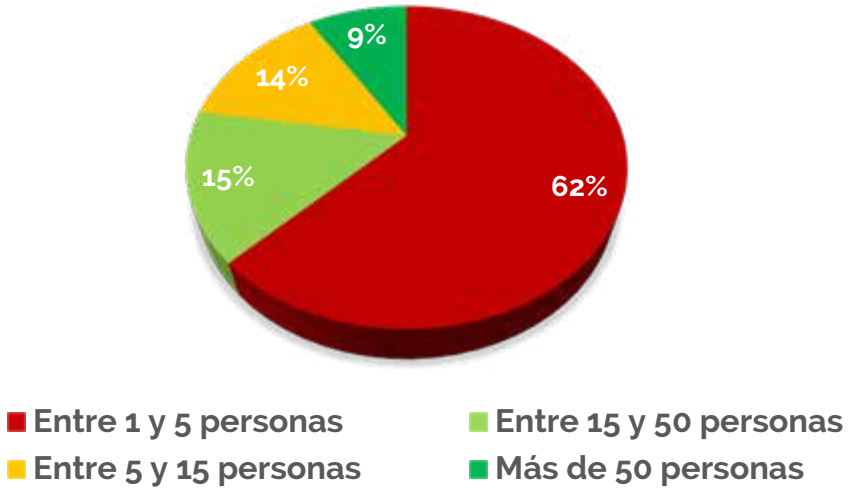
Por último, los resultados obtenidos para las actividades y roles de comunicación interna y externa, durante un proceso de recuperación, muestra una divergencia de las respuestas desde los grados de madurez "básico" y "maduro", hacia el "inexistente" y "optimizado".

Recursos y Organización

Recursos y Personal Interno

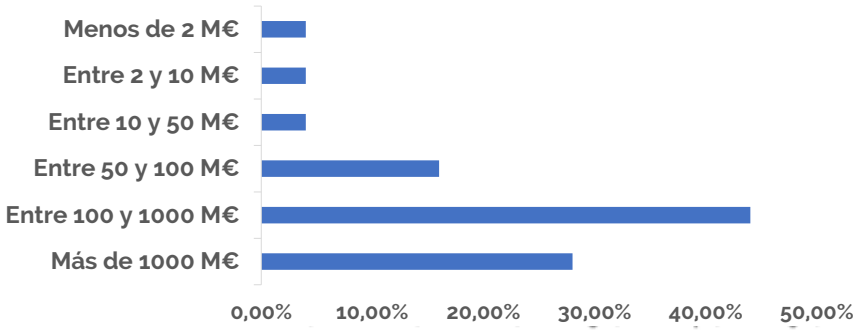
Los datos obtenidos permiten analizar la distribución de los recursos destinados a ciberseguridad. Más de un 60% de las organizaciones analizadas disponen de entre 1 y 5 personas en el área de ciberseguridad, un 14% tienen entre 5 y 15 personas, un 15% entre 15 y 50 personas y menos de un 10% tienen más de 50 personas en el área de ciberseguridad .

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



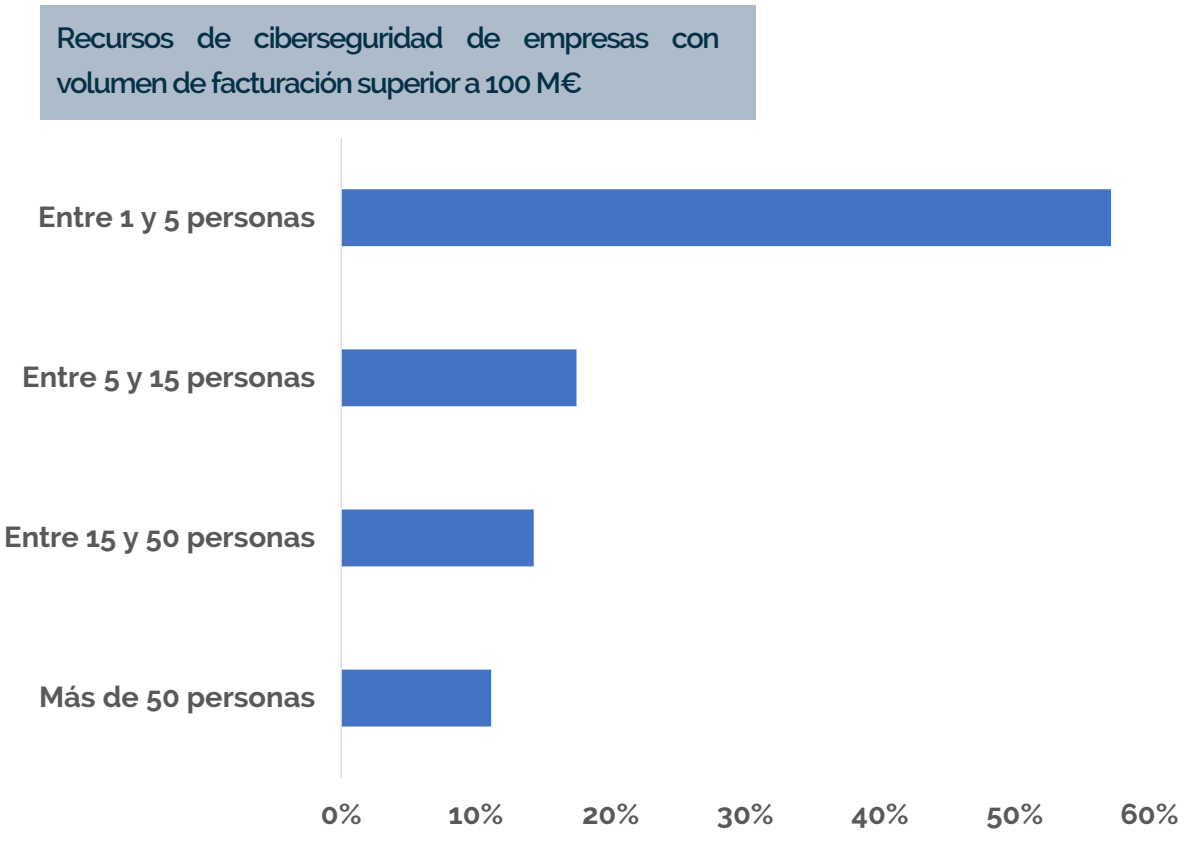
Si entramos en detalle, un 72% de las empresas con entre 1 y 5 recursos de ciberseguridad (un 45% del total de la muestra) se corresponde a empresas con una facturación superior a 100 millones de euros:

Volumen de facturación de empresas con entre 1 y 5 recursos de ciberseguridad



Recursos ciberseguridad	Volumen facturación	Total
Entre 1 y 5 personas	Menos de 2 M€	2,5%
	Entre 2 y 10 M€	2,5%
	Entre 10 y 50 M€	2,5%
	Entre 50 y 100 M€	10,0%
	Entre 100 y 1000 M€	27,5%
	Más de 1000 M€	17,5%
Entre 5 y 15 personas	Entre 100 y 1000 M€	6,3%
	Más de 1000 M€	7,5%
Entre 15 y 50 personas	Entre 10 y 50 M€	2,5%
	Entre 50 y 100 M€	1,3%
	Entre 100 y 1000 M€	5,0%
	> 1000 M€	6,3%
Más de 50 personas	Entre 100 y 1000 M€	2,5%
	> 1000 M€	6,3%

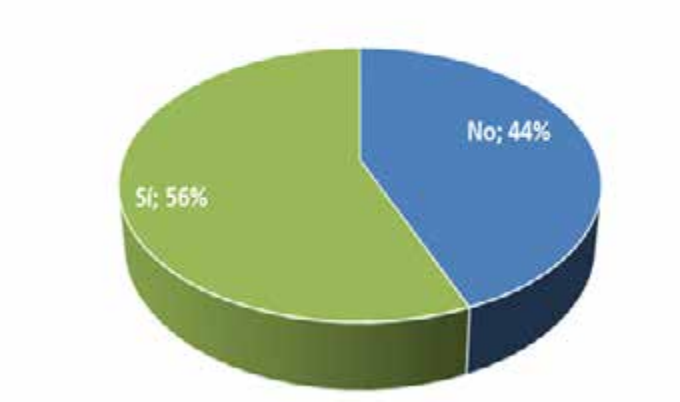
Si correlamos los datos tomando como criterio principal el volumen de facturación, se observa que un 57 % de las empresas con facturación superior a 100 millones de euros tienen entre 1 y 5 personas en el área de ciberseguridad.



Operación de la Seguridad

Del total de las empresas analizadas, un 56% operaban la ciberseguridad desde el propio departamento de Ciberseguridad.

Su departamento de ciberseguridad, ¿opera la ciberseguridad?



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

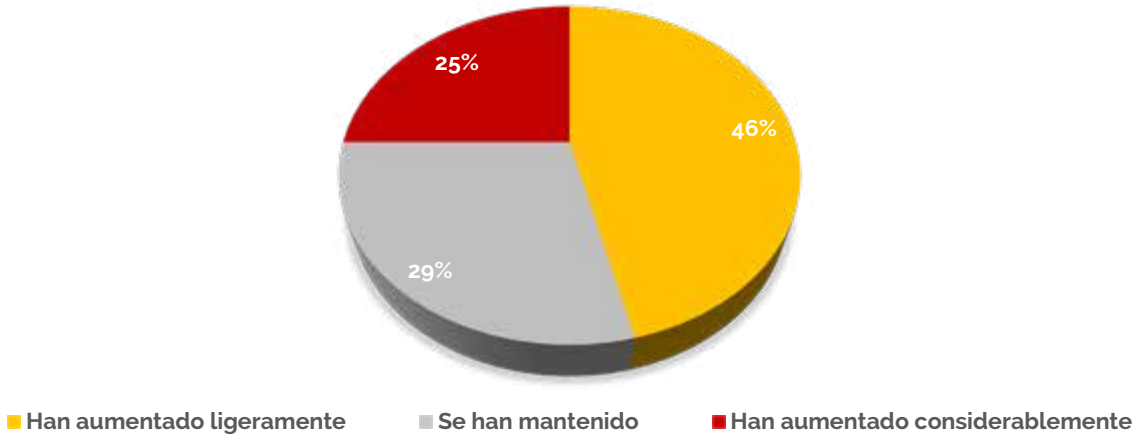
- Un 25% de las empresas que han respondido facturan más de 100 millones de € y con un máximo de 5 personas gestionan la seguridad, pero no la operan.
- Un 20% de las empresas que han respondido facturan más de 100 millones de € y con un máximo de 5 personas gestionan y operan la seguridad.
- Todas las empresas con facturación menor de 10 millones de € operan la seguridad desde el departamento seguridad con menos de 5 personas.

Influencia de la Pandemia COVID-19

Evolución ciberamenazas y recursos

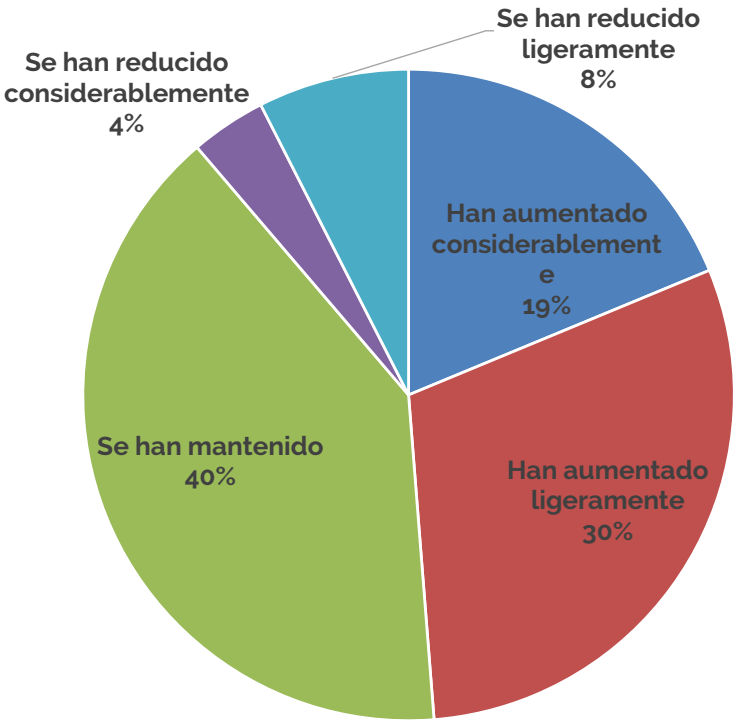
Durante el periodo de pandemia, la mayoría de los encuestados, un 46%, han considerado que las ciberamenazas han aumentado ligeramente. El resto han apreciado que han aumentado considerablemente (un 25%) o que se han mantenido (un 29%). Ninguno de los encuestados ha considerado que las ciberamenazas se hayan reducido durante el periodo.

Durante el periodo de pandemia, ¿qué evolución han tenido las ciberamenazas que ha recibido su organización?



Los datos analizados también permiten concluir que casi un 50% de las empresas han aumentado los recursos dedicados a ciberseguridad durante la pandemia , pero más de un 10% de las empresas han reducido recursos durante la pandemia (véase Figura 6).

Presupuesto post-pandemia



Si analizamos la evolución de los recursos teniendo en consideración la percepción de evolución de las amenazas, más de 40% de las empresas consideran que han aumentado las amenazas durante la pandemia y además han incrementado recursos. En el otro extremo, cerca de un 25% de las empresas han identificado que han aumentado las amenazas pero no han incrementado recursos.

Evolución de recursos durante pandemia	Evolución de amenazas durante pandemia	Total
Los recursos han aumentado	Las amenazas han aumentado considerablemente	16,3%
	Las amenazas han aumentado ligeramente	25,0%
	Las amenazas se han mantenido	7,5%
Los recursos se han mantenido	Las amenazas han aumentado considerablemente	7,5%
	Las amenazas han aumentado ligeramente	16,3%
	Las amenazas se han mantenido	16,3%
Los recursos se han reducido	Las amenazas han aumentado considerablemente	1,3%
	Las amenazas han aumentado ligeramente	5,0%
	Las amenazas se han mantenido	5,0%

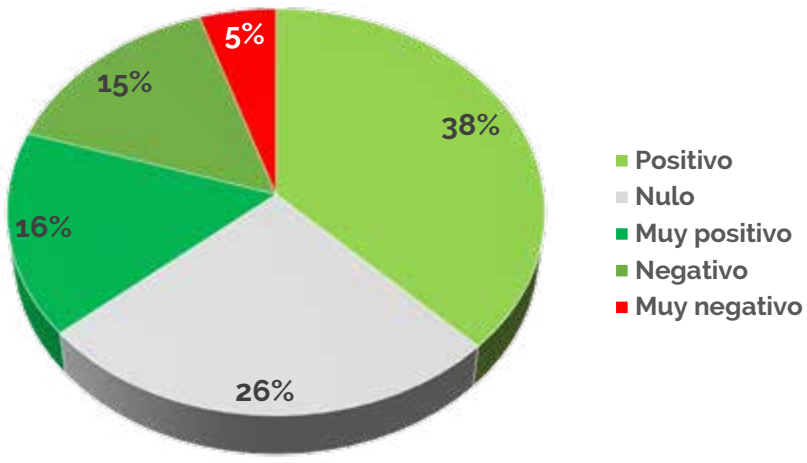
Durante el periodo de pandemia, la mayoría de los encuestados, un 46%, han considerado que las ciberamenazas han aumentado ligeramente. El resto han apreciado que han aumentado considerablemente (un 25%) o que se han mantenido (un 29%). Ninguno de los encuestados ha considerado que las ciberamenazas se hayan reducido durante el periodo.

Recursos de ciberseguridad	Evolución de recursos durante pandemia	Total
Entre 1 y 5 personas	Han aumentado considerablemente	11,3%
	Han aumentado ligeramente	18,8%
	Se han mantenido	25,0%
	Se han reducido ligeramente	3,8%
	Se han reducido considerablemente	3,8%
Entre 5 y 15 personas	Han aumentado considerablemente	3,8%
	Han aumentado ligeramente	3,8%
	Se han mantenido	6,3%
Entre 15 y 50 personas	Han aumentado ligeramente	2,5%
	Se han mantenido	8,8%
	Se han reducido ligeramente	3,8%
Más de 50 personas	Han aumentado considerablemente	3,8%
	Han aumentado ligeramente	5,0%

Efecto Teletrabajo

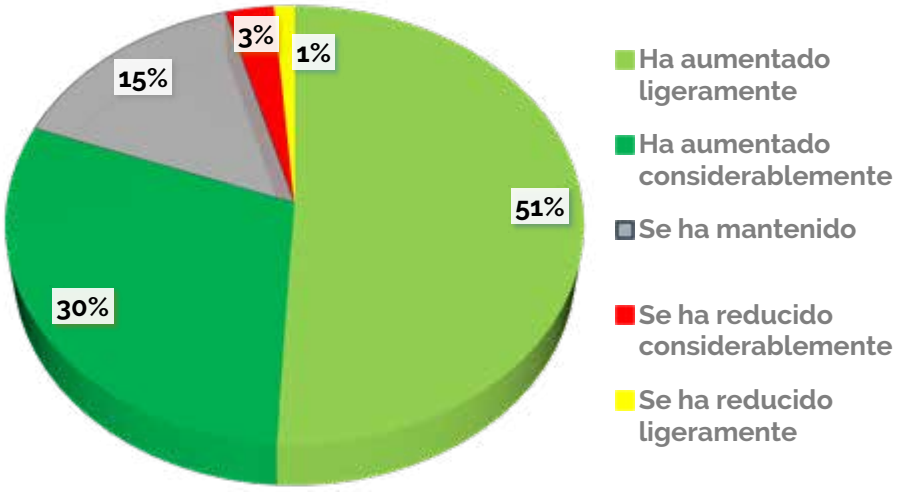
Más de un 50% de las Empresas considera que el efecto del teletrabajo ha provocado un efecto positivo o muy positivo sobre la ciberseguridad mientras que un 20% piensa que el efecto ha sido negativo o muy negativo.

Presupuesto post-pandemia



Interés Alta Dirección durante la Pandemia

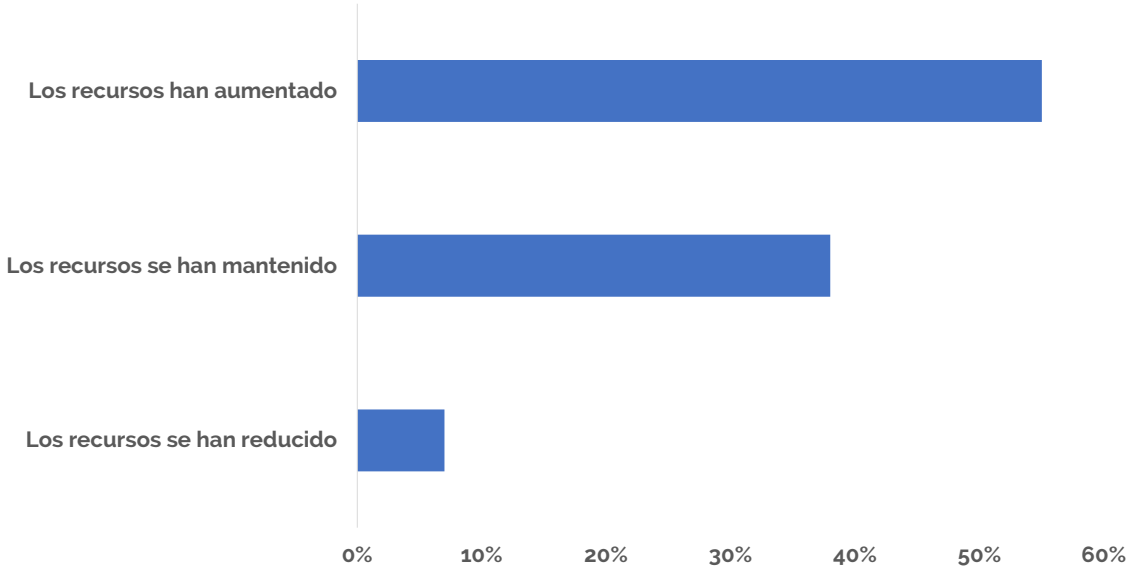
Durante el periodo de pandemia, ¿qué evolución ha tenido el interés de la alta dirección de su organización por la ciberseguridad?



Más de un 80% de las empresas considera que el interés de la alta dirección por la ciberseguridad ha aumentado, y de estos, un 55% han aumentado recursos (un 45% del total de las empresas encuestadas).

Evolución interés alta dirección durante pandemia	Evolución de recursos durante pandemia	Evolución de amenazas durante pandemia	Total
El interés de la alta dirección ha aumentado	Los recursos han aumentado	Las ciberamenazas han aumentado	**39%**
		Las ciberamenazas se han mantenido	6%
	Los recursos se han mantenido	Las ciberamenazas han aumentado	20%
		Las ciberamenazas se han mantenido	11%
	Los recursos se han reducido	Las ciberamenazas han aumentado	4%
		Las ciberamenazas se han mantenido	1%
El interés de la alta dirección se ha mantenido	Los recursos han aumentado	Las ciberamenazas han aumentado	1%
		Las ciberamenazas se han mantenido	1%
	Los recursos se han mantenido	Las ciberamenazas han aumentado	3%
		Las ciberamenazas se han mantenido	5%
	Los recursos se han reducido	Las ciberamenazas han aumentado	3%
		Las ciberamenazas se han mantenido	3%
El interés de la alta dirección se ha reducido	Los recursos han aumentado	Las ciberamenazas han aumentado	1%
	Los recursos se han mantenido	Las ciberamenazas han aumentado	1%
	Los recursos se han reducido	Las ciberamenazas se han mantenido	1%

Evolución de recursos de seguridad de empresas con aumento de interés de alta dirección



Un enfoque complementario sobre las dimensiones

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 exploratorio con el que determinar en qué ámbitos específicos se estructura la madurez de las organizaciones que han formado parte de la muestra del estudio.

En este sentido, dos de los dominios NIST, en concreto los de Protección y Recuperación, se consideran claros, mostrando una única dimensión, en la que las organizaciones tomarán valores altos, medios o bajos entre los extremos de un continuo. Todas las cuestiones a las que hacen referencia las preguntas del cuestionario propias de estos dos dominios, tienden a responderse en una misma dirección, por lo que puede considerarse que los indicadores de "protección" y "recuperación" son relativamente sencillos de interpretar.

No obstante, los otros tres dominios NIST (Identificación, Detección y Respuesta) presentan diversas dimensiones o ámbitos, por lo que no es fácil considerar 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 de la "Gestión de riesgo y requerimientos legales" y el de la "Operativa y documentación". Una organización tendrá una elevada o reducida madurez en Identificación si cuenta con valores altos o bajos simultáneamente en "Gestión de riesgo y requerimientos legales" y en "Operativa y documentación". 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.

En lo que respecta a la Detección, encontramos también dos dimensiones, aunque una

de ellas se corresponde de manera bastante clara con lo esperado para este dominio y reúne a la mayoría de las preguntas planteadas en el cuestionario con este propósito. Esta dimensión principal se ha denominado "Actividades de detección", mientras que la segunda se ha caracterizado como "Documentación de la detección". La documentación de la detección se corresponde con la disponibilidad de sistemas para la recolección de eventos y es independiente de las restantes "Actividades de detección". Así, se pueden observar organizaciones que destaquen en ambas cuestiones, en ninguna, que tengan valores intermedios en las dos, o que bien dominen una de ellas, pero tengan amplio margen de mejora en la otra.

De acuerdo al análisis realizado, el dominio NIST de "Respuesta" es el más complejo de todos. En él observamos un espacio tridimensional en cuanto a los ejes del "Enfoque basado en la comunicación y las responsabilidades", las "Rutinas de prueba, documentación y actualización de los procedimientos de respuesta" y la "Cultura preventiva/ reactiva". Existen múltiples configuraciones del grado de madurez de una organización de acuerdo a estas dimensiones. Así, puede adoptarse un "Enfoque basado en la comunicación y las responsabilidades" u optar, como alternativa o extremo contrario, con una profusa investigación de las alertas generadas por los sistemas de detección. A su vez, la utilización de las "Rutinas de prueba, documentación y actualización de los procedimientos de respuesta" aparecen como una alternativa al análisis forense. Y la adopción de culturas preventivas o reactivas tiene, en un extremo, la identificación temprana de vulnerabilidades (y procesos de mitigación y contención), y en el contrario, la elaboración de planes de respuesta en base a las lecciones aprendidas de incidentes pasados, de acuerdo con un proceso formal de mejora continua.

Por último, merece la pena destacar que el dominio "Recuperar", aunque sólo plantea una única dimensión, muestra ciertas peculiaridades a la hora de poder interpretar la madurez en el mismo. Esta dimensión, de acuerdo a los resultados del análisis factorial, sugiere que las organizaciones se posicionan entre dos extremos, caracterizados por el desarrollo de la respuesta desde el área funcional de ciberseguridad, y la adopción de un enfoque de respuesta más holístico o corporativo, respectivamente.

Anexo

Análisis Factorial Exploratorio para los dominios NIST

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 pretende aplicar 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 recomendables contemplar más dimensiones, factores y facetas a la hora de analizar las actividades de identificación, protección, detección, respuesta y recuperación.

Conviene tener en cuenta que 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 80 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 80:6 para los dominios de identificación (NIST1), protección (NIST2) y respuesta (NIST4), de 80:4 para detección (NIST3) y de 80:3 para recuperación (NIST5).

Igualmente, para realizar un análisis factorial es recomendable, aunque no obligatorio, que las variables a tratar sean normales, puesto que mejora los resultados obtenidos. Este hecho no se cumple en este estudio, debido a que el número de respuestas obtenidas puede considerarse escaso desde el punto de vista estadístico. Una muestra de mayor tamaño seguramente habría permitido trabajar con variables que siguiesen una distribución normal.

Análisis factorial exploratorio Dominio NIST 1: IDENTIFICAR

Estadísticos descriptivos

	Media	Desv. Desviación	N de análisis
NIST101	2,84	,803	80
NIST102	2,74	,951	80
NIST103	3,59	,758	80
NIST104	3,33	,868	80
NIST105	3,10	,949	80
NIST106	2,80	1,011	80

Matriz de correlaciones[a]

		NIST101	NIST102	NIST103	NIST104	NIST105	NIST106
Correlación	NIST101	1,000	,325	,013	-,268	,022	-,072
	NIST102	,325	1,000	,269	-,079	-,013	,353
	NIST103	,013	,269	1,000	,553	,111	,238
	NIST104	-,268	-,079	,553	1,000	,482	,536
	NIST105	,022	-,013	,111	,482	1,000	,390
	NIST106	-,072	,353	,238	,536	,390	1,000
Sig. (unilateral)	NIST101		,002	,454	,008	,425	,264
	NIST102	,002		,008	,242	,456	,001
	NIST103	,454	,008		,000	,164	,017
	NIST104	,008	,242	,000		,000	,000
	NIST105	,425	,456	,164	,000		,000
	NIST106	,264	,001	,017	,000	,000	
a. Determinante = ,166							

Prueba de KMO y Bartlett

Medida Kaiser-Meyer-Olkin de adecuación de muestreo		**,440**
Prueba de esfericidad de Bartlett	**Aprox. Chi-cuadrado**	**136,881**
	gl	**15**
	Sig.	**,000**

Comunalidades

	Inicial	**Extracción**
NIST101	1,000	,596
NIST102	1,000	,770
NIST103	1,000	,450
NIST104	1,000	,856
NIST105	1,000	,413
NIST106	1,000	,622

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	2,251	37,517	37,517	2,251	37,517	37,517
2	1,454	24,228	61,744	1,454	24,228	61,744
3	,946	15,770	77,515			
4	,773	12,879	90,394			
5	,405	6,758	97,152			
6	,171	2,848	100,000			
Método de extracción: análisis de componentes principales.						

Matriz de componente[a]

	Componente	
	1	**2**
NIST104	,872	
NIST106	,772	
NIST103	,641	
NIST105	,629	
NIST102		,839
NIST101		,758
Método de extracción: análisis de componentes principales.		
a. 2 componentes extraídos.		

Dado que el índice KMO es demasiado bajo, sería recomendable descartar la realización del análisis factorial. No obstante, dado que el test de esfericidad de Bartlett es altamente significativo, se procede a su realización. La solución propuesta por el análisis factorial exploratorio se inclina por dos factores, que explican sólo un 62% de la varianza total. El análisis de la varianza explicada muestra que la extracción de un tercer factor (cuyo autovalor está muy próximo al nivel de corte de 1) aumentaría la explicación hasta el 78%. No obstante, se mantiene el nivel de corte estándar, exigiendo autovalores superiores a la unidad, y dando como resultado dos factores. Uno contiene las preguntas NIST103, NIST104*, NIST105 y NIST106, y el segundo incluye las preguntas NIST101 y

NIST102* (los asteriscos indican el indicador dominante a la hora de determinar el contenido del factor obtenido).

A la vista de los resultados obtenidos, identificar parece tener una doble naturaleza. Por una parte, se observa un componente de "gestión de riesgo y requerimientos legales", en el que se incluye la identificación, documentación y análisis de riesgo de vulnerabilidades y amenazas, los procesos de gestión del riesgo de la cadena de suministro, contratos, política de roles y responsabilidades, gestión del riesgo de ciberseguridad y los niveles de tolerancia establecidos.

Por otra parte, puede apreciarse cierto componente de "operativa y documentación", con la identificación y comunicación de dependencias y requisitos de los servicios y funciones críticas (asociadas a la misión, visión y objetivos de la organización) y el inventario de dispositivos, sistemas, aplicaciones y recursos de información, y la gestión de roles y responsabilidades de ciberseguridad.

En definitiva, a la vista del análisis realizado, identificar tiene una vertiente legal y de gestión de riesgos, y otra operativa y de documentación. De este modo, para que una empresa pueda alcanzar la excelencia en este domino deberá dominar ambos tipos de actividades.

Análisis Factorial Exploratorio Dominio NIST 2: PROTEGER

Estadísticos descriptivos

	Media	Desv. Desviación	N de análisis
NIST201	3,15	,915	80
NIST202	3,15	,873	80
NIST203	3,15	,901	80
NIST204	2,85	,813	80
NIST205	2,85	1,057	80
NIST206	2,98	,795	80

Matriz de correlaciones[a]

		NIST201	NIST202	NIST203	NIST204	NIST205	NIST206
Correlación	NIST201	1,000	,764	,739	,609	,272	,649
	NIST202	,764	1,000	,824	,853	,587	,881
	NIST203	,739	,824	1,000	,722	,529	,765
	NIST204	,609	,853	,722	1,000	,548	,915
	NIST205	,272	,587	,529	,548	1,000	,598
	NIST206	,649	,881	,765	,915	,598	1,000
Sig. (unilateral)	NIST201		,000	,000	,000	,007	,000
	NIST202	,000		,000	,000	,000	,000
	NIST203	,000	,000		,000	,000	,000
	NIST204	,000	,000	,000		,000	,000
	NIST205	,007	,000	,000	,000		,000
	NIST206	,000	,000	,000	,000	,000	
a. Determinante = ,002							

Prueba de KMO y Bartlett

Medida Kaiser-Meyer-Olkin de adecuación de muestreo		,854
Prueba de esfericidad de Bartlett	Aprox. Chi-cuadrado	468,265
	gl	15
	Sig.	,000

Comunalidades

	Inicial	Extracción
NIST201	1,000	,618
NIST202	1,000	,916
NIST203	1,000	,793
NIST204	1,000	,827
NIST205	1,000	,441
NIST206	1,000	,881
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	4,475	74,590	74,590	4,475	74,590	74,590
2	,753	12,552	87,142			
3	,386	6,428	93,571			
4	,206	3,432	97,003			
5	,100	1,664	98,667			
6	,080	1,333	100,000			
Método de extracción: análisis de componentes principales.						

Matriz de componente[a]

	Componente
	1
NIST202	,957
NIST206	,939
NIST204	,909
NIST203	,890
NIST201	,786
NIST205	,664
Método de extracción: análisis de componentes principales.	
a. 1 componentes extraídos.	

El KMO tiene un valor ideal para la realización del análisis factorial (superior a 0,8 e inferior a 0,9). La solución que ofrece concuerda con lo esperado y deriva en un único factor, que reúne todas las preguntas planteadas en la encuesta para este dominio NIST, y explica un 75% de la varianza total. El análisis de la protección de acuerdo con la batería de preguntas planteada en el cuestionario puede considerarse validado.

En conclusión, todas las actividades dedicadas a la protección que se han analizado son convergentes, por lo que el concepto y tareas involucradas en la protección resultan claros. Esto facilita su planificación y gestión, reduciendo el riesgo de ambigüedades, tal y como se verá que puede suceder en otros dominios propuestos por el marco NIST.

Análisis Factorial Exploratorio Dominio NIST 3: DETECTAR

Estadísticos descriptivos

	Media	Desv. Desviación	N de análisis
NIST301	3,00	,827	80
NIST302	3,26	,924	80
NIST303	3,11	,811	80
NIST304	2,88	,862	80

Matriz de correlaciones[a]

		NIST301	NIST302	NIST303	NIST304
Correlación	NIST301	1,000	-,232	-,019	-,337
	NIST302	-,232	1,000	,855	,788
	NIST303	-,019	,855	1,000	,726
	NIST304	-,337	,788	,726	1,000
Sig. (unilateral)	NIST301		,019	,434	,001
	NIST302	,019		,000	,000
	NIST303	,434	,000		,000
	NIST304	,001	,000	,000	
a. Determinante = ,072					

Prueba de KMO y Bartlett

Medida Kaiser-Meyer-Olkin de adecuación de muestreo		,665
Prueba de esfericidad de Bartlett	Aprox. Chi-cuadrado	201,743
	gl	6
	Sig.	,000

Comunalidades

	Inicial	Extracción
NIST301	1,000	,983
NIST302	1,000	,908
NIST303	1,000	,916
NIST304	1,000	,845
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	2,651	66,263	66,263	2,651	66,263	66,263
2	1,001	25,023	91,286	1,001	25,023	91,286
3	,230	5,746	97,032			
4	,119	2,968	100,000			
Método de extracción: análisis de componentes principales.						

Matriz de componente[a]

	Componente	
	1	2
NIST302	,948	
NIST304	,915	
NIST303	,897	
NIST301		,935
Método de extracción: análisis de componentes principales.		
a. 2 componentes extraídos.		

En este caso, el KMO tiene un valor cercano a lo recomendado para el análisis factorial exploratorio (0,7). Sin embargo, la solución, al contrario de lo esperado, deriva en dos factores, que conjuntamente explican un 91% de la varianza total de los datos. El primer factor incluye las preguntas NIST302*, NIST303 y NIST304 y supone un 66% de la varianza total. En el segundo factor sólo está recogida la pregunta NIST 301, que representa un 25% de la varianza total.

Los resultados del análisis factorial realizado sugieren que los análisis para la detección de actividades anómalas están vinculados con procedimientos y roles para la detección de incidentes y la monitorización de usuarios en sistemas y redes. Sin duda estas son claramente "actividades de detección" y se corresponden con lo esperado para este dominio. No obstante, los sistemas de recolección de eventos parecen ser una tarea de naturaleza diferente a las anteriores, más vinculada a la "documentación de la detección", que parece no conducirse de manera integrada con las anteriores.

Análisis Factorial Exploratorio Dominio NIST 4: RESPONDER

Estadísticos descriptivos

	Media	Desv. Desviación	N de análisis
NIST401	2,66	,841	80
NIST402	2,69	,805	80
NIST403	3,18	,792	80
NIST404	2,64	1,009	80
NIST405	2,80	,833	80
NIST406	2,38	,891	80

Matriz de correlaciones[a]

		NIST401	NIST402	NIST403	NIST404	NIST405	NIST406
Correlación	NIST401	1,000	,160	-,062	-,638	-,080	,087
	NIST402	,160	1,000	-,747	-,157	-,057	,112
	NIST403	-,062	-,747	1,000	-,141	,303	-,076
	NIST404	-,638	-,157	-,141	1,000	-,163	-,255
	NIST405	-,080	-,057	,303	-,163	1,000	-,341
	NIST406	,087	,112	-,076	-,255	-,341	1,000
Sig. (unilateral)	NIST401		,078	,292	,000	,242	,223
	NIST402	,078		,000	,082	,309	,160
	NIST403	,292	,000		,106	,003	,251
	NIST404	,000	,082	,106		,075	,011
	NIST405	,242	,309	,003	,075		,001
	NIST406	,223	,160	,251	,011	,001	
a. Determinante = ,124							

Prueba de KMO y Bartlett

Medida Kaiser-Meyer-Olkin de adecuación de muestreo		,413
Prueba de esfericidad de Bartlett	Aprox. Chi-cuadrado	159,179
	gl	15
	Sig.	,000

Comunalidades

	Inicial	Extracción
NIST401	1,000	,728
NIST402	1,000	,881
NIST403	1,000	,913
NIST404	1,000	,878
NIST405	1,000	,751
NIST406	1,000	,694
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	1,975	32,922	32,922	1,975	32,922	32,922
2	1,660	27,675	60,597	1,660	27,675	60,597
3	1,208	20,135	80,732	1,208	20,135	80,732
4	,732	12,196	92,928			
5	,261	4,344	97,272			
6	,164	2,728	100,000			
Método de extracción: análisis de componentes principales.						

Matriz de componente[a]

Matriz de componente[a]			
	Componente		
	1	**2**	**3**
NIST402	,794		,427
NIST403	-,744	,548	
NIST404	-,405	-,841	
NIST401	,515	,676	
NIST406	,444		-,692
NIST405	-,407		,691
Método de extracción: análisis de componentes principales.			
a. 3 componentes extraídos.			

Como sucedía para el Dominio NIST 1, en el NIST 3, el KMO resulta demasiado bajo, lo que desaconsejaría realizar el análisis factorial. No obstante, la prueba de esfericidad de Bartlett sí que resulta significativa, por lo que se procede al análisis. La solución propuesta llevaría a un total de tres factores que, aunque juntos explican un 81% de la varianza total, muestran cargas no del todo nítidas en la matriz de componentes. El primero de estos factores contiene las preguntas NIST402* y, con efecto inverso, NIST403. El segundo factor recoge las preguntas NIST404* (con efecto inverso) y NIST401. El tercer factor reúne las preguntas NIST406 (con carga inversa) y NIST405.

A pesar de la dificultad que este análisis factorial presenta para ofrecer conclusiones

robustas, sí que parece observarse que la tarea de responder ante las amenazas es especialmente compleja. Podría haber indicios de que responder es una cuestión de qué responsabilidades se consideran críticas, qué peso se otorga a las rutinas de prueba, documentación y actualización de procedimientos, y si prima una filosofía reactiva o preventiva. Cada empresa puede adoptar decisiones diferentes en estos tres parámetros, lo que hace complicado definir una estrategia óptima y/o única con el fin de responder con éxito ante un incidente.

La formalización del proceso, roles e interlocutores para la comunicación (interna y externa) y la investigación de las alertas generadas por los sistemas de detección (primer factor) parecen estar relacionados estrechamente, pero de manera inversa. Esto sugiere que adoptar un "enfoque basado en la comunicación y las responsabilidades" es una alternativa a la investigación de alertas. Las habilidades requeridas en una u otra actividad son distintas, plantean un perfil diferente para la persona responsable de las mismas, y hacen que las organizaciones puedan cargar las tintas en uno u otro de estos extremos.

Por otra parte, el análisis forense tras un incidente de seguridad y la documentación, actualización y prueba de los procedimientos de respuesta ante incidentes parecen mostrar una naturaleza diferente a los elementos anteriores, quizás por requerir un mayor componente técnico. En concreto, y dada la relación entre variables propuesta por el análisis factorial, podría deducirse que cuando se disponen de "rutinas de prueba, documentación y actualización de los procedimientos de respuesta" ante incidentes, no son necesarios análisis forenses tan detallados como cuando se carece de estas rutinas.

Por último, los procesos formales de mejora continua para la respuesta ante incidentes (en base a las lecciones aprendidas de incidentes pasados) están inversamente relacionados con la identificación temprana de vulnerabilidades y amenazas y los procesos de mitigación y contención para evitar la expansión de un potencial incidente. Esto sugiere dos filosofías contrapuestas, que se corresponderían con la "respuesta preventiva" y la "respuesta reactiva" respectivamente.

Análisis Factorial Exploratorio Dominio NIST 5: RECUPERAR

Estadísticos descriptivos

	Media	Desv. Desviación	N de análisis
NIST501	2,46	,871	80
NIST502	2,44	,912	80
NIST503	2,74	,978	80

Matriz de correlaciones[a]

		NIST501	NIST502	NIST503
Correlación	NIST501	1,000	-,322	-,227
	NIST502	-,322	1,000	,116
	NIST503	-,227	,116	1,000
Sig. (unilateral)	NIST501		,002	,021
	NIST502	,002		,152
	NIST503	,021	,152	
a. Determinante = ,848				

Prueba de KMO y Bartlett

Medida Kaiser-Meyer-Olkin de adecuación de muestreo		,553
Prueba de esfericidad de Bartlett	Aprox. Chi-cuadrado	12,704
	gl	3
	Sig.	,005

Comunalidades

	Inicial	Extracción
NIST501	1,000	,623
NIST502	1,000	,500
NIST503	1,000	,332

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	1,454	48,473	48,473	1,454	48,473	48,473
2	,892	29,722	78,195			
3	,654	21,805	100,000			

Método de extracción: análisis de componentes principales.

Matriz de componente[a]

	Componente
	1
NIST501	-,789
NIST502	,707
NIST503	,576

Método de extracción: análisis de componentes principales.

a. 1 componentes extraídos.

Como sucedía para los dominios NIST 1 y NIST 3, en el análisis del NIST 5 encontramos que el KMO es bajo, y sólo está ligeramente por encima del valor mínimo exigible. Esto, además de la falta de significatividad del Test de Bartlett, indica que la realización del análisis factorial no es adecuada en este caso. De hecho, aunque la solución obtenida está de acuerdo con lo esperado, y muestra un único factor que reúne todas las preguntas de la encuesta relativas a este dominio, sólo recoge un 48% de la varianza total de los datos de la muestra. Todo lo anterior exige la máxima cautela a la hora de extraer conclusiones de este análisis.

Aparentemente, recuperar es una tarea que se puede definir con claridad a través de las actividades analizadas en las preguntas recogidas en el cuestionario utilizado. No obstante, llama la atención el hecho de que cuando no se formalizan y prueban regularmente los planes de recuperación de los sistemas clave de negocio es porque los planes y estrategias de recuperación se actualizan de manera regular y proactiva, y se dispone de una definición e identificación de actividades, roles e interlocutores para la comunicación. Esto parece sugerir que las empresas podrían optar por dos posiciones, cuyos extremos estarían en un enfoque holístico o corporativo, u otro más centrado en las responsabilidades específicas propias de un área funcional. Así, el factor obtenido podría definirse como "recuperación desde el área funcional de ciberseguridad".

915 63 50 62

info@ismsforum.es

Calle Segre 29, 1B
28002, Madrid, Spain

@ISMSForum

ISMS Forum