

Desinformación sobre empresas e instituciones y sus estrategias de respuesta: análisis longitudinal de verificaciones en España (2023–2025)

Disinformation targeting companies and institutions and their response strategies: a longitudinal analysis of fact-checking in Spain (2023–2025)

Rodríguez-Fernández, L., Robles Marquez, I., y Rodríguez de Austria Giménez de Aragón, A. M.



Leticia Rodríguez-Fernández. Universidad de Cádiz (España).

Profesora titular en el Departamento de Marketing y Comunicación de la Universidad de Cádiz. Ejerce como vocal de la Conferencia de Rectores y Rectoras de las Universidades Españolas (CRUE) en el Foro contra las Campañas de Desinformación en el ámbito de la Seguridad Nacional. Investigadora Principal del Grupo de Investigación Comunicación estratégica e influencia en la sociedad digital (COMINDI).

<https://orcid.org/0000-0002-7472-5472>, leticia.rodriguez@uca.es



Isabel Robles Márquez. Universidad de Cádiz (España).

Doctoranda en el programa de Comunicación de la Universidad de Cádiz, Máster en Dirección Estratégica e Innovación en Comunicación y Graduada en Publicidad y Relaciones Públicas y en Marketing e Investigación de Mercados. Sus líneas de investigación se centran en la comunicación estratégica, comunicación deportiva, la divulgación científica y el estudio de la desinformación.

<https://orcid.org/0009-0004-5977-0525>, Isa.roblesmarquez@alum.uca.es



Alfonso M. Rodríguez de Austria Giménez de Aragón. Universidad de Cádiz (España).

Doctor en Comunicación por la Universidad de Sevilla. Profesor del Departamento de Marketing y Comunicación de la Facultad de Ciencias Sociales y de la Comunicación de la Universidad de Cádiz. Sus líneas de trabajo giran en torno a los procesos de influencia masiva, propaganda, retórica, y desinformación.

<https://orcid.org/0000-0003-4597-4944>, alfonso.rodriguezdeaustralia@uca.es

Recibido: 03-09-2025 – Aceptado: 05-02-2026

<https://doi.org/10.26441/RC-2025.1-2026-4171>

RESUMEN: Propósito. Este trabajo analiza la desinformación que busca afectar a organizaciones en España a partir de un análisis de contenido, con enfoque longitudinal, de las verificaciones publicadas por Maldita.es, EFE Verifica, Newtral y RTVE Verifica. **Metodología.** La muestra incluye 630 verificaciones correspondientes al año 2023 y al segundo trimestre de 2024 y 2025, que hacen referencia a 549 entidades y generan un total de 730 menciones a empresas, instituciones y figuras públicas. **Resultados y conclusiones.** Los resultados evidencian una presencia constante de desinformación a lo largo del tiempo, sin variaciones estacionales significativas, siendo las empresas, especialmente de los sectores retail y bancario, las organizaciones más afectadas. No obstante, el análisis muestra que las instituciones públicas concentran un mayor número de menciones acumuladas por una misma organización, lo que las convierte en objetivos recurrentes de las campañas de desinformación. Se observa, además, una creciente convergencia entre desinformación y ciberdelincuencia, que se materializa en prácticas como el phishing, la suplantación de identidad corporativa e institucional y el uso de tecnologías basadas en inteligencia artificial, como los deep fakes, para legitimar ciberdelitos. **Aportes originales.** Si bien la desinformación es un riesgo y una amenaza que afecta tanto a empresas como a

instituciones, y para la cual han de estar prevenidas y tener capacidad de actuación y respuesta, solo en el 52,6% de las verificaciones se documentó la existencia de una respuesta ofrecida por la organización. Estas respuestas se caracterizan por su carácter mayoritariamente reactivo, fragmentado y centrado en redes sociales y páginas web corporativas, con una escasa implantación de estrategias preventivas.

Palabras clave: desinformación; comunicación estratégica; relaciones públicas; ciberseguridad; ciberdelitos; empresas; instituciones; verificación, fake news.

ABSTRACT: Purpose. This study analyses disinformation targeting organisations in Spain through a longitudinal content analysis of fact-checks published by Maldita.es, EFE Verifica, Newtral and RTVE Verifica. **Methodology.** The sample comprises 630 fact-checks corresponding to the year 2023 and the second quarter of 2024 and 2025, referring to 549 entities and generating a total of 730 mentions of companies, institutions and public figures. **Results and conclusions.** The results reveal a constant presence of disinformation over time, with no significant seasonal variations, with companies—particularly in the retail and banking sectors—being the most affected organisations. However, the analysis shows that public institutions accumulate a higher number of mentions per single organisation, making them recurrent targets of disinformation campaigns. Additionally, an increasing convergence between disinformation and cybercrime is observed, materialised in practices such as phishing, corporate and institutional identity impersonation, and the use of artificial intelligence-based technologies, such as deepfakes, to legitimise cybercriminal activities. **Original contributions.** Although disinformation represents a risk and a threat affecting both companies and institutions, which therefore need to be prepared and capable of responding, only 52,6% of the fact-checks document the existence of a response by the affected organisation. These responses are predominantly reactive, fragmented, and focused on social media and corporate websites, with limited implementation of preventive strategies.

Keywords: disinformation; strategic communication; public relations; cybersecurity; cybercrime; companies; institutions; verification; fake news.

1. Introducción

La digitalización ha transformado los modelos comunicativos y ha puesto en evidencia que la desinformación es el mal endémico de nuestro tiempo. La crisis de desinformación es una crisis de desconfianza. Según *Edelman Trust Barometer* (2024), el 63% de las personas encuestadas en 28 países (n=32.000) no confía en los líderes políticos, el 61% no cree en los líderes empresariales, y el 64% presenta el mismo sentimiento hacia periodistas y reporteros. La desconfianza ha crecido, en todos los casos, entre uno y tres puntos respecto a la misma encuesta realizada el año anterior.

Un escenario de crisis que podría agravarse con el consumo y distribución de contenidos generados con inteligencia artificial. Según el *Global Risk Report* (2024) publicado por el Foro Económico Mundial, los próximos años estarán marcados principalmente por el clima extremo, la desinformación generada por inteligencia artificial y la polarización social. Si bien, la ciudadanía parece ser consciente de esta situación, como se observa en la encuesta realizada por Ipsos (2023) en 29 países (n=21.816), en la que los encuestados consideran que la inteligencia artificial hará que la desinformación sea peor y contribuirá en la generación de contenidos falsos. Una preocupación que se enmarca en la propia naturaleza de la inteligencia artificial, pues los algoritmos aprenden en base a los patrones y contenidos que obtienen del ecosistema digital. Como observan García-Marín y Murolo (2023: 74), “los algoritmos en los medios digitales tienen que ver con desarrollos de la ingeniería y de la informática, pero su implementación tiene implicaciones sociales”.

En este contexto, la generación de contenidos con IA conlleva numerosos riesgos, como el fenómeno “slop”, traducido como “bazofia”, término que hace referencia a los contenidos basura que la IA produce y difunde en la red. Una vez estos entran en los ecosistemas digitales, las redes sociales aumentan su difusión y alcance, alimentando un bucle de aprendizaje cuyo

resultado son contenidos falsos con alta visibilidad. Sirva como ejemplo el caso de difusión de imágenes falsas creadas con IA de crías de pavos reales cuyo alcance terminó posicionando en buscadores y convirtiéndolas en fuente principal frente a las imágenes reales (Castillo, 2024).

En este sentido, y como señala Harari (2024: 72), “las redes sociales han aprendido a usar la información para mantener un orden social más sólido entre poblaciones mayores, al emplear no solo relatos veraces, sino también ficciones, fantasías, propaganda y -en ocasiones- mentiras en toda regla”.

2. Marco teórico

2.1. Cuando la desinformación erosiona la confianza y la reputación de las organizaciones

Desde hace varios años las organizaciones que representan el sector de la comunicación estratégica y las relaciones públicas se muestran preocupadas por los efectos que la desinformación tendrá sobre la comunicación y reputación de las organizaciones, así como en la propia profesión. En 2024, la Organización Internacional de Consultores de Comunicación (ICCO) la destacaba en su informe anual como una de las principales preocupaciones en materia de ética profesional. Según su encuesta global (n=268), el 78% de los profesionales afirmaba haber rechazado a algún cliente por razones éticas, mientras que el 13% no lo había hecho y un 9% no estaba seguro. Entre los principales desafíos para las agencias de relaciones públicas para el siguiente año, el 43% señaló la falta de consecuencias para aquellas empresas que actúan de manera poco ética o trabajan con clientes cuestionables, seguido del 39%, que destacó la desinformación como un problema clave. También los códigos éticos del sector han ido adecuándose a esta coyuntura, rechazando como se observa en la Declaración de Helsinki, el uso del *astroturfing* o de las *fake news* (International Communications Consultancy Organisations, 2014). Preocupación que también se extiende de manera particular a los profesionales, que detectan una carencia de estrategias para anticipar y neutralizar ataques de desinformación y demandan más iniciativas de alfabetización mediática para ayudar a la ciudadanía a ser más crítica, resaltando la importancia de profesionalizar el sector y evitar el intrusismo laboral (Rodríguez-Fernández y Establés, 2023; Lambert, Ewing y Hassan, 2024).

Estudios anteriores han ahondado en cómo la desinformación puede afectar a las organizaciones, señalando a las instituciones como principales afectadas e identificando prácticas tales como creación de noticias falsas en supuestos medios digitales o clonados, uso de noticias humorísticas/satíricas que tratan de pasar como información real, alteración de imágenes con montajes, uso de vídeos o imágenes descontextualizadas, falsas declaraciones y falsas conversaciones o interacciones desde redes sociales, entre otras (Rodríguez-Fernández, 2019; Gomes Gonçalves *et al.*, 2025). No obstante, y dado que este tipo de trabajos parte de las verificaciones recogidas por los fact-checkers, estas tendrían a su vez relación con los propios acontecimientos mediáticos, así como con las agendas y prioridades de los verificadores. Se observa así que un año después de la pandemia casi una cuarta parte de los contenidos falsos analizados (n=255) tenían como protagonista al Gobierno de España, a gobiernos autonómicos y a otras instituciones (Almansa *et al.*, 2022) o como cada plataforma de verificación de datos aplica también su propia agenda de verificación en ámbitos como la salud, con un compromiso más o menos significativo (Costa *et al.*, 2023).

No menos preocupante resulta el hecho de que algunas empresas hayan decidido hacer de la influencia negativa su negocio, incluyendo el *astroturfing*, los discursos negacionistas, el *greenwashing* y otras técnicas de desinformación como parte de su estrategia de comunicación o de su catálogo de servicios, también conocidos como *Dark PR* (Ennis, 2023; Rodríguez-Fernández, 2024). Un mercado que ha encontrado en los países del sur, como Filipinas, oportunidades para ensayar y perfeccionar estas estrategias insidiosas sin apenas supervisión ni restricciones (Gaw, 2025) y cuyas motivaciones son principalmente intereses económicos y/o de imagen de marca (Mirza *et al.*, 2023).

La desinformación, además, también suele ser empleada como recurso para el robo de datos y otras series de ciberdelitos que se han incrementado notablemente en los últimos años. Durante el último semestre de 2023, España se posicionó como el país europeo con mayor número de ciberataques, ocupando el tercer lugar a nivel mundial (ESET, 2023). Una circunstancia permanente en 2024, pues numerosas empresas españolas se han visto afectadas por ciberataques, demostrando tanto su vulnerabilidad como compañías como de la de los usuarios que tienen su confianza depositada en las mismas. Según el informe extraordinario elaborado por el equipo de inteligencia de S2 Grupo, en los primeros meses de 2024 se habían recogido 27 publicaciones de filtraciones y robos de datos que afectan directamente a entidades españolas, tanto instituciones como empresas de primer nivel, que a priori, deberían contar con buenos sistemas de ciberseguridad. Se encuentran entre ellos Orange, el Ayuntamiento de Calvià (Mallorca), Douglas, FIATC, El Confidencial, la Universidad Complutense de Madrid, Banco Santander, Telefónica o Iberdrola, entre otros (Cabrera, 2024).

2.2. Cómo las empresas y las instituciones enfrentan la desinformación: estrategias y respuestas

Se recogen pocos trabajos que hayan abordado el estudio de tácticas y estrategias para luchar o contrarrestar la desinformación desde el enfoque de la comunicación de las organizaciones. Desde el lado de las asociaciones y patronales representativas, en 2018 el *European Communication Monitor* encuestó a 3.100 profesionales de 48 países, recogiendo que, solo en el mes empleado para el estudio, el 22.5% de las organizaciones se habían visto afectadas por desinformación, pero solo el 12% había establecido rutinas avanzadas para identificarla. También en la edición 2018-2019 del *Latin American Communication Monitor* (n=1.165) apenas el 26% de las organizaciones había implementado pautas y rutinas formales para enfrentarse a la desinformación, y solo el 7,2% ha instalado tecnologías y sistemas específicos para identificarla (Silveira, *et al.*, 2020).

El *prebunking* y el *debunking* son otras de las tácticas que se erigen como potenciales soluciones. Tomando como referencia el trabajo “125 términos sobre la desinformación” del Foro contra las campañas de desinformación en el ámbito de la Seguridad Nacional (Arce *et al.*, 2024) entendemos por *prebunking* el “conjunto de medidas preventivas orientadas a inmunizar o alertar anticipadamente a la ciudadanía ante mensajes falsos”. En esta misma línea, se incorpora también el término inoculación, que busca la prevención a través de la incorporación temprana de mensajes preventivos que permitan contrarrestar los efectos de la desinformación.

Por su parte, *debunking* haría alusión a la “acción de demostrar la falsedad o inexactitud de un contenido presumiblemente desinformativo utilizando estrategias y técnicas de verificación”. A diferencia de la verificación, el *debunking* no solo se centra en revelar la exactitud de la información o los datos, además desmiente la desinformación revelando las prácticas empleadas. Ambas técnicas son complementarias, pues el *debunking* se centra en corregir afirmaciones falsas que ya circulan en el discurso popular, y el *prebunking* busca fortalecer la resistencia psicológica de las personas frente a afirmaciones engañosas antes de que las encuentren.

Ambas técnicas comienzan a ser englobadas en el estudio de la comunicación estratégica, fundamentalmente para ahondar en sus efectos frente a los discursos negacionistas promovidos por determinadas industrias. Amazeen *et al.* (2025) realizaron un estudio experimental (n=1.045) mostrando a los participantes publicidad desinformativa de ExxonMobil, algunas con revelaciones y otras precedidas de mensajes de inoculación. Los resultados mostraron que el anuncio influía eficazmente en las creencias, pero que la divulgación ayudaba a los participantes a reconocer el contenido como publicidad, y que los mensajes de inoculación reducían la susceptibilidad, aunque no del todo. Se añaden los trabajos de Castellani y Berton (2017) que recogen el uso de estrategias de defensa como campañas de comunicación destinadas a informar a sus partes interesadas, o de Boman y Scheneider (2021), que observaron que la anticipación y la publicación de refutación simultánea (*prebunking*) es la técnica más efectiva. Otros autores proponen también el desarrollo de protocolos de crisis proactivos que

permitan responder con celeridad a la desinformación para minimizar su impacto (Vázquez y Paniagua, 2022). En esta misma línea, Mirza *et al.* (2023) aluden a los “equipos de mitigación” recogiendo sobre las potenciales fórmulas de mitigación “denunciar cuentas y contenidos para su eliminación”, “esperar temporalmente a que los incidentes pequeños o nuevos se desarrollen más antes de intervenir” e incluso “no hacer nada” mientras se continúa con la monitorización del incidente emergente, para evitar propagar o amplificarlo inadvertidamente, “cuando de otro modo podría simplemente desaparecer por sí solo”.

Si bien otras investigaciones han explorado cómo las organizaciones deberían responder a la desinformación, también han analizado en qué medida la autoridad del emisor influye en su impacto persuasivo. Entre las conclusiones se observa que el emisor de las correcciones es menos importante que el encuadre, y que las correcciones narrativas resultaban mucho más eficaces para mejorar la percepción del consumidor que las correcciones objetivas. Estos resultados sugieren que las organizaciones deben desarrollar estrategias de gestión de riesgos o de crisis como las mencionadas anteriormente, en las que se detallen cómo deben transmitirse a los consumidores las correcciones de las noticias falsas, prestando especial atención al encuadre del mensaje (Kropf, Wood y Parsons, 2023).

Por otro lado, las empresas tecnológicas, conscientes de su responsabilidad en el ecosistema digital, han adoptado algunos compromisos en aras de mejorar la resiliencia de la sociedad. En 2024, veinte compañías, incluyendo Microsoft, Meta, Google y Amazon, firmaron un acuerdo para combatir la desinformación durante los procesos electorales desarrollados durante ese año en 70 países de todo el mundo, prestando especial atención a aquella generada con inteligencia artificial (EFE, 2024). Se añade la adopción de políticas educativas en torno a la alfabetización mediática y digital.

Sin embargo, el liderazgo en la promoción de acciones destinadas a contrarrestar la desinformación parece recaer fundamentalmente en las instituciones. La pandemia de COVID-19 hizo aún más necesario el flujo de información por parte de fuentes institucionales y organismos internacionales (Ferreira Caceres *et al.*, 2022). Así, la Organización Mundial de la Salud (OMS) ha adoptado distintas acciones y colaboraciones tanto a través de sus medios propios como de terceros tales como con Wikipedia (Fidalgo, 2020) o recientemente con Tik Tok (WHO, 2024) para ofrecer información sanitaria fiable y frenar la desinformación. De forma paralela, la Unión Europea ha desarrollado políticas destacadas en este ámbito (Rúas-Araújo *et al.*, 2025), incorporando el *Big Data*, la ciencia de datos y la inteligencia artificial (Moreno Espinosa *et al.*, 2024). Una labor que requiere de un importante juego de equilibrios entre la confianza y la desconfianza institucional pues como señalan Rodríguez-Pérez y Canel (2022), “algo de desconfianza institucional ayuda a mantener una actitud de alerta y conciencia de la propagación de información falsa e incrementa los niveles de resiliencia” (p.862).

Asimismo, resulta especialmente relevante el trabajo desarrollado desde la Academia, pues la búsqueda de soluciones frente a la desinformación se ha convertido en la temática más frecuente en las investigaciones publicadas entre 2016 y 2020 (García-Marín, 2021). Esta preocupación ha posicionado a España como el tercer país mundial con mayor producción de artículos científicos en este campo, solo por detrás de EE.UU. y Reino Unido, y el primero en habla hispana (Rodríguez-Fernández *et al.*, 2023).

3. Objetivos y metodología

Esta investigación tiene como objetivo principal identificar cuáles son las empresas e instituciones que pueden verse más afectadas por la desinformación y explorar si están proporcionando respuestas para contrarrestarla. Aunque investigaciones previas han realizado una aproximación inicial al fenómeno (Rodríguez-Fernández, 2019; Gomes Gonçalves *et al.*, 2025), no existen estudios que profundicen en las respuestas ofrecidas.

Así, como objetivo secundario, se busca cuantificar y clasificar las respuestas emitidas, con el fin de identificar tendencias en el comportamiento de las organizaciones frente a la información falsa.

Para alcanzar estos objetivos se ha propuesto una investigación de carácter exploratorio, realizando una primera revisión del marco conceptual que ha contribuido notablemente en el diseño de la segunda parte de la investigación, basada en el análisis de contenido. Dado que la desinformación es un fenómeno fragmentado, se propone analizar las verificaciones emitidas por las organizaciones especializadas, pues estas suelen seleccionar los contenidos falsos más relevantes por su impacto y difusión. En este caso, se han recopilado todas las verificaciones relacionadas con empresas, instituciones y personajes públicos desde enero a diciembre de 2023 emitidas por Maldita, Newtral, EFE Verifica y RTVE Verifica. Esta primera selección nos ha permitido tener una fotografía de interés sobre los principales tipos de desinformación que buscan afectar a organizaciones. No obstante, y para dotar de profundidad al trabajo, se ha seleccionado el trimestre con mayor volumen de verificaciones recogidas (abril, mayo y junio) y se han recogido datos sobre los mismos meses en 2024 y 2025. Con ellos se busca dar un enfoque longitudinal al trabajo que permita abrir una ventana de comparación, contraste y evolución.

La selección de estos cuatro verificadores se basa en su relevancia en el ámbito de la verificación de información. *EFE Verifica*, *Maldita* y *Newtral* fueron elegidos debido a que son tres de los cuatro verificadores españoles que forman parte de la organización *International Fact-Checking Network* (IFCN). Se excluyó a *Verificat*, ya que su ámbito de actividad está limitado a Cataluña. Además, se incluyó a *RTVE Verifica*, dado que se trata de un área especializada dentro de la Corporación de Radio y Televisión Española (RTVE), empresa pública española con alcance estatal.

Las verificaciones se recopilaron manualmente mediante una ficha de registro en la que se consignaba: la fecha de publicación, el titular del contenido, la organización mencionada, el enlace al contenido, el tipo de estafa o engaño, observaciones y la respuesta emitida por la organización. La extracción de la información fue realizada por dos codificadores con roles complementarios. El primero se encargó de recopilar todos los datos de manera sistemática, siguiendo criterios estandarizados para asegurar la coherencia y uniformidad en el registro. El segundo codificador asumió la revisión y validación exhaustiva de la información recopilada, verificando, detectando posibles errores u omisiones y asegurando que todas las entradas cumplieran con los parámetros metodológicos definidos. Se garantiza así la fiabilidad y consistencia de la base de datos, minimizando sesgos y aumentando la calidad de los resultados finales.

El registro de verificaciones se centró exclusivamente en referencias a empresas, instituciones y figuras públicas, excluyendo los partidos políticos con el fin de realizar un análisis especializado en comunicación corporativa e institucional, y evitar el enfoque político. Para los fines de este estudio, hemos recogido como institución organizaciones gubernamentales, educativas, culturales y financieras, así como corporaciones privadas con reconocimiento formal, excluyendo entidades políticas de carácter partidario, movimientos sociales sin estructura formal y actores individuales.

En relación con las figuras públicas, se incluyeron únicamente aquellas alusiones a personalidades políticas cuando estas se vinculan con timos o estafas que involucraron a alguna marca, siguiendo el mismo criterio aplicado a otras figuras públicas. De este modo, se recopilaron contenidos que utilizan la imagen, voz o identidad de una persona reconocida para legitimar inversiones fraudulentas, promociones inexistentes, estafas económicas o engaños tecnológicos mediante *deepfakes*, vídeos manipulados, citas falsas o clonación de identidad. Dentro de esta categoría también se incluyen alusiones directas a empresarios y/o directivos de organizaciones. Por el contrario, se excluyeron verificaciones relacionadas con contenido falsos cuyo objetivo principal era afectar la reputación o credibilidad de políticos o autoridades religiosas.

En el caso de Maldita, la búsqueda se limitó a las entradas etiquetadas como 'timo'. En la web de Newtral, se analizaron dos tipos de publicaciones dentro de la sección 'Zona de verificación': por un lado, los artículos, y por otro, las entradas de 'Fakes', utilizando las etiquetas 'Phishing' y 'Estafa'. Para RTVE, las entradas seleccionadas se basaron en las etiquetas temáticas del medio, específicamente 'Estafa', 'Verifica RTVE Ciberdelitos' y 'Ciberdelitos'. Finalmente, en EFE Verifica, la búsqueda se centró en las publicaciones agrupadas bajo la denominación 'Verificaciones'.

Para recopilar las respuestas emitidas por las organizaciones, se revisó detalladamente el contenido de las verificaciones, dado que los cuatro verificadores registran si las empresas o instituciones han tomado medidas para desmentir la desinformación, indicando además las acciones desarrolladas. En aquellos casos en los que no se obtuvo este dato, se realizó una comprobación posterior mediante búsquedas en Google, con el objetivo de localizar contenido indexado, revisando además los medios propios de las correspondientes organizaciones para complementar la primera revisión y garantizar la precisión y exhaustividad de la información recopilada.

En total, se recogieron 630 contenidos, 456 correspondientes al año 2023, y 88 y 86 correspondientes al trimestre de análisis de 2024 y 2025. Los contenidos fueron analizados manualmente, excluyendo algunas repeticiones de resúmenes que revisaban las mismas verificaciones ya recogidas individualmente. Posteriormente, se clasificó la información según el mes de publicación, el tipo de organización (empresas, instituciones, personajes famosos o sociedad en general), el nombre y la actividad de la organización, y el número de menciones, ya que una organización puede aparecer en distintas verificaciones.

Las respuestas ofrecidas por las organizaciones se clasificaron según el tipo de herramienta utilizada, que se limitó a: redes sociales, página web corporativa, comunicados de prensa, correos electrónicos a afectados y/o declaraciones de portavoces de la organización o de su departamento de comunicación. La base de datos empleada para este trabajo, así como los archivos de Excel que contienen las clasificaciones de verificaciones y respuestas han sido depositados para su consulta en Zenodo y pueden ser recuperadas en el siguiente enlace: (<https://zenodo.org/records/15033285>).

Finalmente, y con el objetivo de profundizar en los tipos de desinformación y las respuestas ofrecidas por las organizaciones, y sobre el análisis y clasificación manual de las 630 verificaciones realizadas previamente, se cruzaron todos los datos con herramientas de inteligencia artificial. En concreto, se recurrió a ChatGPT, asistente de inteligencia artificial creado por OpenAI, y Gemini, asistente de IA de Google, para la elaboración de una tabla sintética que relaciona los principales tipos de desinformación identificados con las respuestas observadas desde las organizaciones. Sobre los resultados obtenidos se realizaron los ajustes necesarios en las denominaciones y categorías analíticas con el fin de garantizar la coherencia y validez del análisis, como, por ejemplo, la sustitución del término “desinformación institucional” por “desinformación contra las instituciones”, una formulación más precisa y correcta para el presente trabajo. También a través de este procedimiento se ha obtenido un gráfico con las organizaciones más mencionadas en las verificaciones, lo que permite diferenciar las organizaciones más afectadas por impacto extensivo e intensivo.

4. Resultados

4.1. Cómo afecta la desinformación a empresas e instituciones: análisis de las verificaciones recogidas en 2023

A través del estudio de las verificaciones realizadas a lo largo de un año, se han identificado patrones de actividad, tanto en términos de volumen como de distribución temporal, así como los principales sectores empresariales e instituciones protagonistas de piezas de desinformación

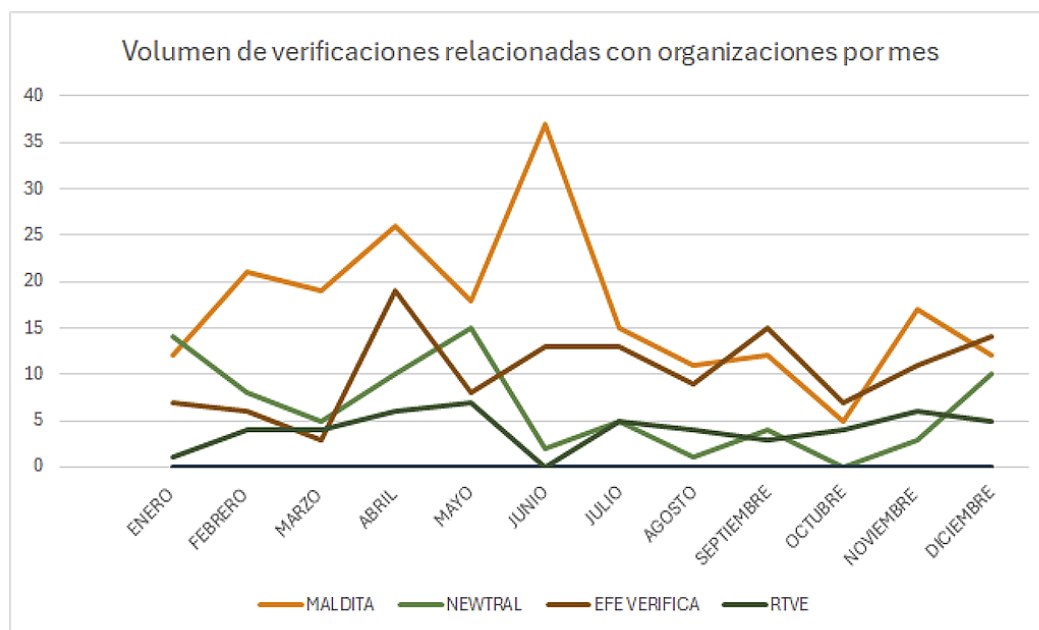
y de la posterior verificación por organizaciones independientes. Además, el análisis transversal del trimestre más fecundo en verificaciones (abril-junio) de los años 2023 a 2025 permite introducir variables temporales y tendencias incipientes tanto en el tipo de las empresas afectadas por la desinformación como en las respuestas para hacerle frente.

El estudio se centra en el trabajo desarrollado por *Maldita*, *Newtral*, *Efe Verifica* y *RTVE Verifica*, destacando el número de verificaciones realizadas por cada una de estas entidades y su evolución a lo largo del tiempo. Además, se analizan las entidades que han sido objeto de verificaciones, diferenciando entre empresas, instituciones y figuras públicas, y se identifican los sectores económicos más afectados por la desinformación, con especial atención a aquellas compañías que han sido mencionadas con mayor frecuencia en los procesos de verificación.

A partir de estos datos, se busca ofrecer una visión detallada sobre la naturaleza y el alcance de la desinformación en el ámbito empresarial e institucional, así como la respuesta de las entidades verificadoras en la lucha contra la propagación de noticias falsas. Los resultados obtenidos permiten comprender mejor las dinámicas de la desinformación en distintos sectores y la importancia de los esfuerzos de verificación y de la propia respuesta de las organizaciones afectadas para mitigar su impacto en la sociedad.

Como se observa en el gráfico 1, *Maldita* es el verificador que presenta la mayor cantidad de contenidos relacionados con organizaciones, con un total de 205 verificaciones registradas en 2023. Le sigue *EFE Verifica* con 125 contenidos, mientras que *Newtral* y *RTVE Verifica* muestran un menor volumen de estas informaciones, con 77 y 49 verificaciones respectivamente.

Gráfico 1. Volumen de verificaciones relacionadas con organizaciones durante 2023



Fuente: elaboración propia.

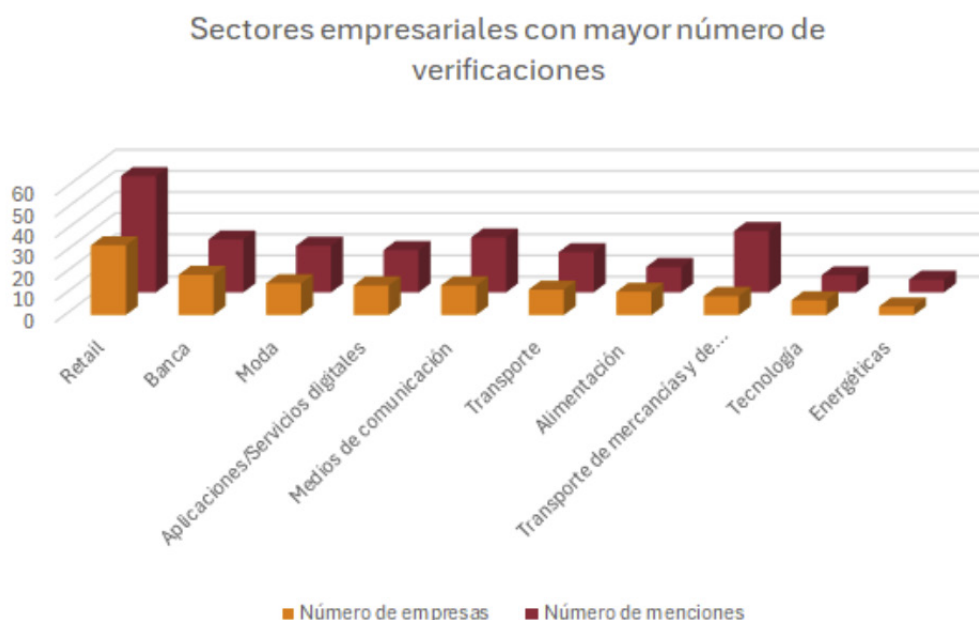
Se ha identificado una distribución estable en la cantidad de verificaciones relacionadas con organizaciones a lo largo del año 2023, sin una reducción significativa en los meses de verano. Los meses con mayor número de contenidos relacionados fueron abril, mayo y junio (este segundo trimestre del año ha sido por ello el escogido para realizar un análisis de tendencias en la verificación de la desinformación), mientras que octubre fue el mes con menor número de verificaciones, alcanzando aproximadamente un 25% de la actividad registrada en abril. Sorprendentemente, agosto no fue el mes con menos verificaciones, ya que se documentaron 25 publicaciones que aludían a organizaciones, en comparación con la media mensual de 38. Estos datos sugieren que las campañas de desinformación que pueden afectar a organizaciones son constantes y permanentes, sin que en este análisis se hayan identificado diferencias significativas en campañas como navidad o periodos vacacionales.

En total se han recogido por tanto 456 verificaciones que realizan 506 menciones a 326 empresas, instituciones y personajes públicos. En el global de las entidades objeto de las verificaciones destacan las organizaciones empresariales. Se ha encontrado un total de 156 empresas que han protagonizado al menos una verificación, algunas de ellas varias, hasta llegar a un total de 244 menciones entre todas estas empresas. Destacan por número de verificaciones protagonizadas las empresas Correos, con 22 menciones repartidas entre las cuatro verificadoras, y Amazon, con nueve menciones, aunque en este caso todas las publicaciones pertenecen al mismo verificador, Maldita.

Los contenidos relacionados con instituciones y con personas famosas fueron relativamente similares en número, con 83 verificaciones para instituciones y 87 para figuras públicas. Sin embargo, al considerar el número total de menciones, las instituciones acumularon 148 referencias, mientras que las personas famosas registraron 114. Este dato sugiere que, aunque la cantidad de verificaciones individuales es comparable, las instituciones son objeto de desinformación con una mayor recurrencia. Dentro de este grupo, la Agencia Tributaria destacó con 15 verificaciones registradas, distribuidas entre Maldita, Newtral y RTVE Verifica. Estas además se enmarcan temporalmente durante los meses en los que se desarrolla la campaña de la declaración de la renta, motivando que el engaño o fraude pueda tener mayor efectividad en la ciudadanía.

Dado que las empresas han sido las entidades más mencionadas en las verificaciones y, por lo tanto, las más afectadas por la desinformación, se ha llevado a cabo una categorización por sectores. El objetivo es identificar si hay industrias que se pueden ver más afectadas por su tipo de actividad por la desinformación.

Gráfico 2. Volumen de empresas y menciones según el sector empresarial



Fuente: elaboración propia.

En el gráfico 2 se muestra cómo el sector de las empresas *retail* o comercio minorista están a la cabeza en el número tanto de organizaciones mencionadas como en el número de estas menciones. Se han detectado 55 menciones a 33 empresas distintas del sector. Las empresas más mencionadas entre las verificaciones analizadas son Amazon, Mercadona, Lidl, Ikea, El Corte Inglés o Carrefour.

El sector bancario también ocupó un lugar destacado en términos de verificaciones. Empresas como BBVA, Unicaja, Ibercaja y Banco Santander fueron objeto de informaciones falsas que motivaron verificaciones por parte de las entidades analizadas. Además de estos sectores, también se identificaron verificaciones frecuentes en empresas de moda, servicios digitales, medios de comunicación, transporte y alimentación, todos ellos con más de diez menciones en el período evaluado.

Dentro del sector de transporte de mercancías y mensajería, se identificaron nueve empresas que fueron objeto de verificaciones, con un total de 29 menciones. Correos destacó ampliamente en este ámbito, acumulando 22 verificaciones, lo que la convierte en la empresa, en este caso pública, con mayor número de menciones dentro de su sector. Esto indica que la compañía ha sido un blanco frecuente de desinformación, lo que podría estar relacionado con su carácter público y su vinculación con los procesos electorales y la desinformación sobre el voto por correo, pues en julio de 2023 se celebraron las elecciones generales en España.

Es necesario destacar que se han recogido verificaciones sobre informaciones falsas que utilizan tecnologías basadas en Inteligencia Artificial para elaborar *deepfakes*. Uno de los objetivos principales de estas piezas es la estafa, como se comprueba en los contenidos falsos protagonizados por Elon Musk, Carlos Slim o el presidente de Repsol, Antonio Brufau, en las que supuestamente promocionan inversiones rentables en criptomonedas o en sus propias empresas. Para la elaboración de estas piezas se utiliza la IA, el montaje de vídeo y la clonación de la voz, tecnologías que se desarrollan rápidamente y que permiten la elaboración de *deepfakes* cada vez más difíciles de detectar.

4.2. Resultados: análisis longitudinal de los años 2023-2025

El análisis de la totalidad de las verificaciones recopiladas en 2023 ha permitido obtener una primera fotografía de referencia sobre los tipos de desinformación orientados a afectar a las organizaciones. No obstante, con el objetivo de dotar al estudio de una dimensión longitudinal, se incorporaron también datos trimestrales correspondientes a los años 2024 y 2025. Para ello, se tomó como periodo de referencia el trimestre comprendido entre abril y junio, al tratarse de los meses que concentraron el mayor volumen de verificaciones en 2023.

En 2024 se recogieron un total de 88 verificaciones (Maldita 35, Newtral 25, RTVE 13, EFE Verifica 15) que hacían alusión a 140 entidades, con un total de 127 menciones. Mientras que en 2025 se obtuvieron 86 contenidos (Maldita 34, Newtral 24, RTVE 18 y EFE Verifica 10) que aludían a 83 organizaciones con 87 menciones. Se observa así una disminución en el volumen total de verificaciones, pasando de un total de 130 en 2023 a 86 en 2025. Esta disminución puede tener relación con las propias agendas de los verificadores, si bien RTVE Verifica incrementa el total de contenidos y Maldita mantiene un número similar de contenidos, siendo EFE Verifica el que presenta un descenso más pronunciado, bajando de 40 verificaciones.

Observamos así que en el trimestre de 2023 analizado el foco era el robo masivo de datos con campañas dirigidas a la Agencia Tributaria y Correos, mientras que en 2024 se recogen más fraudes de inversión (criptomonedas) que utilizan la imagen de personajes famosos. En el trimestre analizado en 2025 se observa que un mismo contenido falso puede afectar a 5 o 6 marcas distintas del mismo sector. Es el caso de las empresas Primor, Vorwerk, Pandora y Decathlon, que son empleadas bajo el fraude de regalo de productos por liquidación o cese de actividad. En estos casos los ciberdelincuentes usan un solo servidor que cambia el logo y los colores según el enlace, para probablemente optimizar costes. El uso de estas plantillas permite que, si una marca desmiente el contenido falso, los atacantes simplemente cambien el nombre de la empresa afectada en segundos.

A la hora de disgregar los datos por tipo de organización, encontramos que las empresas siguen siendo las organizaciones más afectadas por la desinformación. 38 empresas fueron objeto de verificación en el segundo trimestre de 2024, y 50 en 2025, mientras que las instituciones fueron objeto de verificación en 25 y 22 ocasiones, y los personajes públicos lo fueron en 14 y 11 ocasiones. Se da sin embargo la circunstancia de que en estos años la mayor concentración de menciones sobre un mismo elemento (empresa, institución u organización) se han llevado a cabo sobre determinadas instituciones y personajes, como la Organización Mundial de la Salud (hasta en 9 ocasiones), la Agencia Tributaria (8), la Dirección General de Tráfico (8), o el doctor Pedro Cavadas (4). Volviendo a las empresas, resulta reseñable que en 2024 todas las empresas fueron mencionadas una sola vez, y en 2025 hubo 58 menciones de 50 empresas, destacando como la empresa más afectada el banco BBVA (5 menciones) y la empresa aseguradora Mapfre (3 menciones). Otras empresas afectadas fueron Amazon, Lidl, Telefónica y Mahou.

En cuanto a los sectores empresariales más afectados por la desinformación, la tendencia de los trimestres analizados de los años 2024 y 2025 es continuista sobre el año 2023. El sector más afectado es el minorista o retail (13 menciones), siendo también destacado el sector de la banca con 10 verificaciones. Las empresas de aplicaciones y servicios digitales fueron objeto de verificación hasta en 11 ocasiones, y los medios de comunicación en 9. Los servicios de mensajería y transporte de mercancías pasan a ser objeto de 7 menciones, descendiendo acusadamente con respecto a la representación que tenía en 2023, motivada principalmente por la empresa Correos fue objeto de múltiples informaciones falsas.

Los resultados de este estudio evidencian que la desinformación dirigida a organizaciones no es un fenómeno errático, sino una actividad persistente y altamente estratégica que encuentra en el sector corporativo, especialmente en el retail y la banca, su principal objetivo. La recurrencia de ataques contra entidades como Correos o la Agencia Tributaria en periodos críticos —como procesos electorales o campañas fiscales— demuestra que los agentes desinformadores aprovechan ventanas de oportunidad institucional para maximizar la credibilidad y el impacto de sus narrativas. Esta sistematicidad sugiere que la desinformación ha dejado de ser una crisis coyuntural para convertirse en un riesgo reputacional y operativo constante que requiere una vigilancia permanente por parte de las organizaciones afectadas.

Por otro lado, se observa una evolución crítica en la sofisticación de los ataques, caracterizada por la convergencia entre la inteligencia artificial y la suplantación de autoridad. El uso de *deepfakes* y clonación de voz para orquestar estafas financieras no solo representa un salto tecnológico, sino una explotación deliberada del capital simbólico de figuras públicas y sectores clave como el bancario y el retail. La diversificación de estos engaños —donde personajes de la política o la realeza se vinculan a criptomonedas, mientras que figuras del ámbito sanitario se utilizan para validar productos médicos fraudulentos— demuestra una segmentación estratégica del fraude. En última instancia, la desinformación está logrando mimetizar los canales de comunicación oficiales y la imagen de marca de sectores críticos, lo que dificulta la detección por parte del ciudadano y exige una respuesta defensiva mucho más proactiva por parte de las organizaciones afectadas. Destaca en este sentido el caso de RTVE que a pesar de tener incluso un verificador propio se ha convertido en 2025 en uno de los principales suplantados (usando la marca de sus programas estrella).

La utilización de *deepfakes* de personas famosas como reclamo para estafas de supuestas plataformas de inversiones en bolsa y especialmente en criptomonedas es una constante relevante de los trimestres de 2024 y 2025 analizados. Los datos arrojan que las figuras públicas más utilizadas en este tipo de estafas durante los segundos trimestres del trienio 2023-2025 son el doctor Pedro Cavadas, que aparece en cuatro ocasiones, e Isabel Díaz Ayuso, presidenta de la Comunidad de Madrid, que aparece mencionada en tres verificaciones. Curiosamente, Isabel Díaz Ayuso aparece ligada a las plataformas de inversión en criptomonedas, mientras que, de una forma más coherente, el doctor Cavadas aparece recomendando productos farmacéuticos falsos con efectos supuestamente milagrosos. Otras figuras presentes, relacionadas con la inversión en criptomonedas y el juego online son el rey Felipe VI, la reina Letizia y la cantante Rosalía.

4.3. Comunicación estratégica: cuál es la respuesta de las empresas e instituciones a la desinformación

De las 456 verificaciones analizadas correspondientes al año 2023, se identificaron 160 contenidos en los que se documenta algún tipo de respuesta emitida por empresas e instituciones frente a contenidos falsos o engañosos, lo que representa únicamente el 35 % del total de verificaciones referidas a organizaciones. Este porcentaje constituye una línea base relevante para el análisis longitudinal. Al contrastar estos resultados con los datos correspondientes al segundo trimestre de 2024 y 2025, se detecta que la proporción de verificaciones que incluyen respuesta organizacional aumenta notablemente, alcanzando el 66,9%. Por tanto, y sobre el total de verificaciones analizadas (n=630) se registran respuestas en el 52,6% de los casos.

En relación con el tipo de actor que emite la respuesta, en 2023 las empresas concentraron aproximadamente dos tercios de las intervenciones registradas (107 de 160), frente a un tercio

correspondiente a instituciones (53). Esta relación se reproduce de forma consistente en los datos del segundo trimestre de 2024 y 2025, en los que las respuestas emitidas por empresas siguen siendo mayoritarias en términos absolutos (78 intervenciones), frente a las registradas por instituciones (54), pese a que estas últimas presentan una mayor tasa de respuesta relativa cuando son objeto de desinformación.

La publicación de mensajes en redes sociales se mantiene como la estrategia dominante en los tres periodos analizados. En 2023, este canal concentró cerca del 40 % de las respuestas identificadas, y los datos correspondientes al segundo trimestre de 2024 y 2025 confirman una proporción equivalente. Las redes sociales funcionan como espacios de respuesta inmediata y de contacto directo con los usuarios, especialmente en casos de estafas virales. Un ejemplo paradigmático lo constituyen las respuestas emitidas por las empresas cerveceras Mahou y Estrella de Galicia ante la difusión de un contenido falso muy similar que circuló tanto en redes sociales como en aplicaciones de mensajería, en el que se anunciaba falsamente una promoción consistente en el sorteo de una “mininevera” a través de un enlace fraudulento. A pesar de tratarse de estafas independientes, ambas utilizaban el mismo producto como reclamo, lo que apunta a la reutilización de narrativas y formatos por parte de los estafadores y a la necesidad de respuestas reiteradas por parte de las marcas afectadas.

En algunos casos, estas intervenciones en redes sociales se ven reforzadas por otros canales de comunicación. Así ocurre, por ejemplo, con la Dirección General de Tráfico (DGT), que confirmó a Verifica RTVE que “no tiene nada que ver” con una página web que promovía ilegalmente la venta de distintivos ambientales bajo el nombre de DGT Online. Del mismo modo, la Embajada de Italia en España confirmó a EFE Verifica la falsedad de una información que afirmaba que Italia había eliminado el género no binario de sus documentos de identidad oficiales, aclarando que dicha opción nunca ha estado contemplada en su sistema documental. Estos casos ilustran una combinación de respuesta reactiva y aclaración institucional que se mantiene tanto en 2023 como en los periodos analizados de 2024 y 2025.

La publicación de contenidos explicativos en páginas web corporativas constituye de forma estable la segunda estrategia más empleada. En 2023, esta modalidad representó aproximadamente una cuarta parte del total de respuestas, y los datos del segundo trimestre de 2024 y 2025 muestran una proporción similar, con una ligera intensificación en sectores especialmente afectados por fraudes digitales. Empresas como Amazon, Banco Sabadell, BBVA, Caixabank, Coca-Cola, Correos, Mercadona o Netflix recurren de manera recurrente a este tipo de comunicados, al igual que instituciones como la Agencia Tributaria. La relevancia de esta estrategia radica en su carácter explicativo y en su capacidad para permanecer accesible a largo plazo mediante la indexación en buscadores, facilitando que los usuarios encuentren el desmentido oficial al buscar información sobre el contenido falso.

Imagen 1. Ejemplo de contenido en página web corporativa explicando la usurpación de identidad de Mercadona en una estafa



Fuente: <https://info.mercadona.es/>

En determinados casos, la función de alerta recae en medios o páginas web especializadas vinculadas al entorno informativo de la empresa, más que en la propia organización. Este es el caso de Apple, donde páginas como [applesfera.com](https://www.applesfera.com) y [genbeta.com](https://www.genbeta.com) advirtieron sobre un correo electrónico fraudulento dirigido a usuarios de iCloud que anunciaba un inexistente programa de fidelización. Aunque Apple negó la veracidad del mensaje tras ser consultada por los verificadores, no emitió un comunicado público específico, lo que evidencia una delegación parcial de la respuesta en actores externos

Imagen 2. Ejemplo de correo electrónico falso enviado a usuarios de iCloud.



Fuente: <https://www.applesfera.com>

Las declaraciones emitidas por portavoces o departamentos de comunicación, generalmente tras consultas de los verificadores, continúan representando en torno a una cuarta parte de las respuestas documentadas en los tres periodos analizados. Este tipo de intervención mantiene un carácter eminentemente reactivo y raramente se traduce en comunicaciones preventivas dirigidas al público general, lo que refuerza la dependencia de la actividad de verificación como detonante de la respuesta organizacional.

Un elemento que muestra continuidad y cierta consolidación es la coordinación interinstitucional en la respuesta a campañas de desinformación recurrentes. Los fraudes vinculados a la Agencia Tributaria durante el periodo de presentación de la renta constituyen un ejemplo significativo, tanto en 2023 como en los datos parciales de 2024 y 2025. En estos casos, la Agencia publicó avisos de seguridad en su página web, mientras que la Policía Nacional y el Instituto Nacional de Ciberseguridad (INCIBE) difundieron advertencias complementarias en redes sociales y en sus portales oficiales. De forma similar, la suplantación de identidad de la Guardia Civil mediante correos electrónicos que acusaban falsamente a ciudadanos de delitos graves fue denunciada tanto por este cuerpo como por la Policía Nacional, reforzando el mensaje preventivo mediante una respuesta coordinada.

Por el contrario, el uso de comunicados de prensa y el contacto directo con las personas afectadas siguen siendo estrategias claramente marginales. En 2023, ambas modalidades representaron menos del 5 % del total de respuestas, y los datos correspondientes al segundo trimestre de 2024 y 2025 confirman su carácter excepcional. El caso del Ayuntamiento de Madrid, que emitió un comunicado para alertar sobre multas de tráfico falsas colocadas en parabrisas, o el de Air Europa, que contactó directamente con sus clientes tras un ciberataque para recomendar la anulación de tarjetas bancarias, se mantienen como excepciones asociadas a contextos de especial gravedad o a fraudes que trascienden el entorno digital.

En conjunto, la incorporación de los datos del trimestre más prolífico de los años 2024 y 2025 refuerza la conclusión de que las estrategias de respuesta frente a la desinformación presentan una notable estabilidad longitudinal. Los ejemplos empíricos y los indicadores cuantitativos muestran que no se ha producido un incremento significativo ni en la frecuencia

ni en la diversidad de las respuestas organizacionales. La reacción sigue siendo minoritaria, predominantemente empresarial, concentrada en las redes sociales y en las páginas web corporativas, y activada de forma reactiva, generalmente tras la intervención de los verificadores.

Cabe destacar finalmente la evolución identificada en las verificaciones que podría contribuir positivamente a la alfabetización digital de la ciudadanía. Así, de las verificaciones analizadas en 2023 a 2025 que ya no mencionan solo a la empresa o institución, sino al procedimiento de estafa, con titulares que tienden a describir el procedimiento más que a centrarse en las organizaciones. Si bien, en 2023 se recogían contenidos bajo el titular "Amazon no regala móviles" estas evolucionan hacia "verificaciones de marca blanca" como "La estafa del paquete no entregado: cómo roban tus datos" o "Las empresas de retail nunca piden pagos por SMS" que sirve tanto para esta compañía como para otras. Igualmente se tiende a la multi verificación agrupando a distintas organizaciones que se ven afectadas por el mismo ciberdelito, facilitando el recuerdo de las actuaciones frente a la organización que se emplea en el proceso.

4.4. Relación entre tipo de desinformación y respuesta de las organizaciones

Cabe destacar en primer lugar, y sobre el conjunto total de verificaciones analizadas, los tipos dominantes de desinformación que afectan a empresas, instituciones y figuras públicas y que aparecen de forma recurrente. Se observa así:

- **Estafas económicas y fraudes como phishing administrativo (renta, multas) o phishing bancario (SMS, vishing).** Su principal objetivo es obtener un beneficio económico directo mediante el engaño empleando para ello falsas inversiones, premios inexistentes, cobros fraudulentos o solicitudes de información sensible.
- **Suplantación de identidad corporativa o institucional:** uso fraudulento de la identidad de una empresa, institución o persona pública para dotar de credibilidad a un ciberdelito. Puede tener como finalidad la estafa, pero el elemento central es la apropiación de la marca o imagen.
- **Falsos comunicados oficiales:** Contenidos que imitan a comunicados oficiales, notas de prensa o avisos operativos, atribuidos falsamente a instituciones o empresas, normalmente del servicio público. Es frecuentemente empleada contra sectores como el del transporte.
- **Manipulación o invención de declaraciones:** consiste en alterar, sacar de contexto o inventar declaraciones atribuidas a personas públicas o portavoces institucionales. Para ello se emplean frases que están fuera de contexto, titulares engañosos o contenidos audiovisuales editados. Al igual que en la técnica de suplantación de identidad corporativa e institucional la finalidad puede ser la estafa, pero en el proceso se sirve de la imagen y reputación del portavoz.
- **Desinformación contra instituciones:** Narrativas falsas que afectan a instituciones públicas, organismos internacionales o políticas públicas, con un alto componente ideológico. Se enmarcan en esta categoría tantas narrativas conspirativas, contenidos falsos sobre organismos internacionales, de información climática o contra normativa.
- **Desinformación contra el ámbito sanitario:** Información falsa o engañosa relacionada con la salud, tratamientos, vacunas o alertas sanitarias. Suele apelar al miedo y a la urgencia y se sirve para ello de falsos consejos médicos, del alarmismo sanitario, las narrativas pseudocientíficas o los rumores virales y los contenidos descontextualizados. Por extensión puede afectar tanto a empresas o instituciones relacionadas.

Se observa, además, y gracias a este cruce de datos, que los tipos de desinformación no solo se diferencian por su contenido, sino por su finalidad y el riesgo percibido, factores que condicionan directamente la estrategia de respuesta adoptada por las organizaciones. Se recoge en la siguiente tabla 1 esta relación de forma estructurada

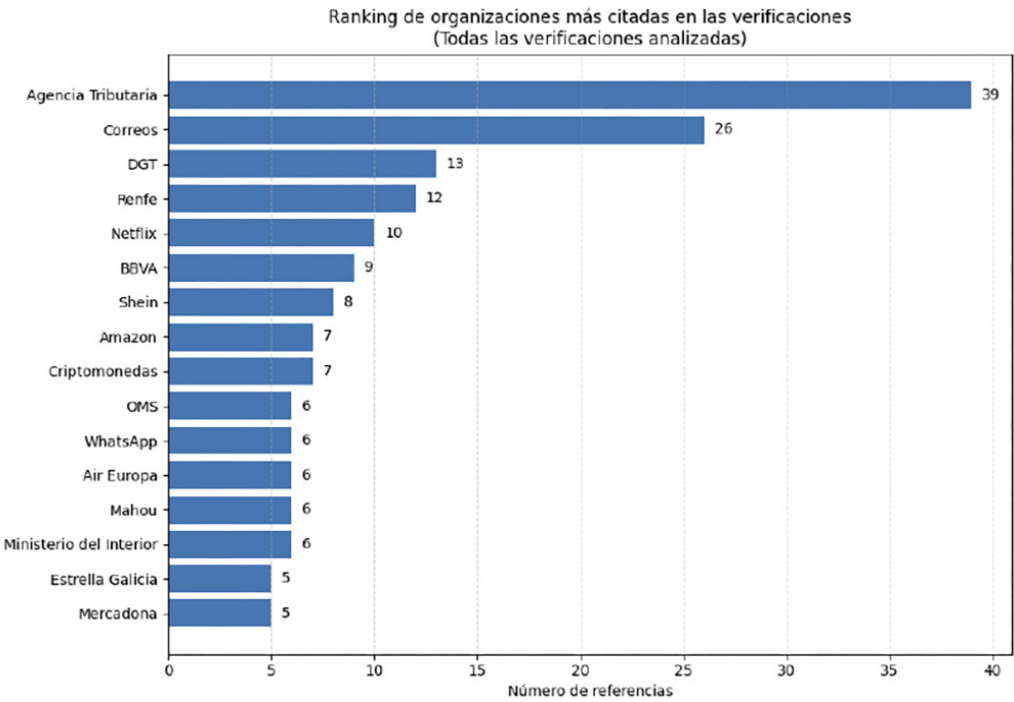
Tabla 1. Relación entre tipos de desinformación, riesgo percibido y estrategias de respuesta de las organizaciones

Tipo de desinformación	Ámbito afectado	Finalidad dominante	Riesgo percibido	Estrategia de respuesta
Estafas económicas	Empresas / usuarios	Económica	Muy alto	Reactiva y preventiva
Suplantación de identidad	Empresas / instituciones / famosos	Reputacional	Alto	Defensiva
Falsos comunicados y alertas	Empresas e instituciones	Confusión social	Medio	Institucional contenida
Manipulación de declaraciones	Famosos / portavoces	Reputacional	Medio	Selectiva
Desinformación contra instituciones	Instituciones públicas y organismos	Política / institucional	Variable	Silencio estratégico o comunicado general
Desinformación contra el ámbito sanitario	Salud pública / ciudadanía	Salud pública	Alto	Pedagógica y preventiva
Rumores virales y descontextualización	Transversal	Viralidad	Bajo	No respuesta

Fuente: Elaboración propia a partir del análisis y la categorización manual previa de los datos, complementados posteriormente mediante el cruce y la sistematización con herramientas de inteligencia artificial (Gemini y ChatGPT).

Finalmente, el Gráfico 3 presenta las organizaciones más mencionadas en relación con el volumen total de contenidos analizados. Cabe destacar que las cuatro primeras corresponden a instituciones y empresas públicas.

Gráfico 3. Ranking de organizaciones más citadas en las verificaciones analizadas.



Fuente: Elaboración propia a partir del análisis y la categorización manual previa de los datos, complementados posteriormente mediante el cruce y la sistematización con herramientas de inteligencia artificial (Gemini y ChatGPT).

5. Discusión y conclusiones

En primer lugar, resulta relevante destacar que la desinformación dirigida a organizaciones constituye un riesgo reputacional específico que, en numerosos casos, converge con dinámicas propias de la ciberdelincuencia. Tal y como se recoge en la categorización de los tipos de desinformación desarrollada en este trabajo, varias de las técnicas identificadas tienen como finalidad el fraude económico o el robo de datos personales, y se apoyan en fórmulas de engaño como la suplantación de identidad corporativa o institucional para dotar de verosimilitud a los contenidos falsos.

El impacto extensivo de la desinformación afecta de manera predominante a las empresas, especialmente a aquellas pertenecientes a los sectores retail y bancario. Estas organizaciones concentran un elevado número de verificaciones distribuidas entre un gran volumen de empresas distintas, generalmente mediante patrones de engaño y fraude que se replican de forma sistemática. En este sentido, se aprecia que un mismo contenido falso puede llegar a afectar simultáneamente a cinco o seis marcas de un mismo sector, lo que evidencia un riesgo ya compartido para determinados sectores empresariales.

Por el contrario, el impacto intensivo de la desinformación se manifiesta con mayor claridad en el ámbito de las instituciones públicas. Del total de las 630 verificaciones analizadas, las tres organizaciones más mencionadas corresponden a la Agencia Tributaria, Correos y la DGT, que acumulan un elevado volumen de menciones a lo largo del tiempo. Esta exposición acumulativa podría estar vinculada a su condición de autoridades públicas, a la instrumentalización de la desinformación con fines ideológicos o, en algunos casos, a intereses relacionados con la seguridad nacional y la confianza en los servicios públicos.

Pese a la relevancia de estos impactos, la respuesta de empresas e instituciones frente a la desinformación continúa siendo mayoritariamente reactiva, con una media de respuesta del 52,6% sobre el total de verificaciones analizadas. No obstante, en los trimestres correspondientes a 2024 y 2025 se observa un incremento de dicha respuesta, lo que podría interpretarse como una mayor concienciación por parte de las organizaciones sobre la necesidad de desmentir activamente los contenidos falsos. Asimismo, las redes sociales corporativas e institucionales se consolidan como el canal más utilizado para la difusión de estos desmentidos. En este contexto, resulta especialmente relevante la coordinación observada entre instituciones públicas en la denuncia de este tipo de prácticas, un refuerzo que, junto con la comunicación desarrollada por las propias empresas, contribuye a mejorar la visibilidad del problema y a reforzar la prevención frente a estas modalidades de desinformación y fraude.

No obstante, y como limitaciones de este estudio conviene recordar que representa una visión parcial, al basarse exclusivamente en los contenidos verificados y difundidos por las organizaciones de *fact-checking* analizadas. Si bien estas entidades desempeñan un papel fundamental en la identificación de la desinformación, sus verificaciones no abarcan la totalidad de los contenidos falsos o engañosos que circulan en los entornos digitales y que pueden afectar a las organizaciones. En este sentido, futuras líneas de investigación podrían ampliar el alcance del análisis mediante estudios comparativos que incorporen tanto verificadores internacionales como otros mecanismos de detección de desinformación, con el objetivo de ofrecer una visión más completa y transversal del fenómeno y de sus implicaciones para la gestión reputacional y la comunicación estratégica de organizaciones públicas y privadas.

Finalmente, desde una perspectiva de comunicación estratégica, resulta necesario profundizar en el estudio de la desinformación dirigida a organizaciones, atendiendo tanto a su impacto como a las respuestas que éstas articulan frente a dichos contenidos. Al mismo tiempo, los resultados ponen de relieve la conveniencia de que empresas e instituciones avancen en el fortalecimiento de estrategias preventivas, en la cooperación entre actores públicos y privados y en la integración de la gestión de la desinformación dentro de sus políticas de comunicación, gestión de crisis y seguridad.

6. Financiación

Este artículo forma parte del Proyecto de Investigación “Comunicación estratégica ante el reto de la desinformación, desafíos, innovación y respuestas (COMDESIR)” FEDER-UCA-2024-B1-01 cofinanciado por el Programa Operativo FEDER Andalucía 2021-2027 y por la Consejería de Universidad, Investigación e Innovación de la Junta de Andalucía.

7. Contribuciones

Roles	Autor 1	Autor 2	Autor 3
Conceptualización	x		
Análisis formal	x	x	x
Obtención de fondos	x		
Administración del proyecto	x		
Investigación	x	x	x
Metodología	x		
Tratamiento de datos	x	x	x
Recursos	x		
Software	x	x	x
Supervisión	x		
Validación	x	x	x
Visualización de resultados		x	x
Redacción-borrador original	x	x	x
Redacción-Revisión y edición	x	x	x

Bibliografía

Agencia Tributaria (2023). *Relación de fraudes detectados*. <https://bit.ly/3YtnC3J>

Almansa-Martínez, A., Fernández-Torres, M. J. y Rodríguez-Fernández, L. (2022). Desinformación en España un año después de la COVID-19. Análisis de las verificaciones de Newtral y Maldita. *Revista Latina de Comunicación Social*, 80, 183-200. <https://doi.org/10.4185/RLCS-2022-1538>

Arce García, S., Rodríguez Fernández, L., Establés Heras, M. J., García Marín, D., Marín García, B., Martín Jiménez, V., Pérez Curiel, C., Said Hung, E., Salaverría Aliaga, R. y Wagner, A. (2024). 125 términos sobre desinformación. En: Presidencia del Gobierno, *Trabajos del Foro contra las campañas de desinformación. Iniciativas 2024*. (pp. 9-39). Gobierno de España. Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática.

Boman, C. y Schneider, E. (2021). Finding an antidote: Testing the use of proactive crisis strategies to protect organizations from astroturf attacks. *Public Relations Review*, 47(1). <https://doi.org/10.1016/j.pubrev.2020.102004>

Cabrera, J. (2024). *Principales ciberataques en España en 2024*. Channel Partner: <https://bit.ly/3zhKYAs>

Castellani, P. y Berton, M. (2017). *Fake news and corporate reputation: what strategies do companies adopt against false information in the media?* 20th Excellence in Service International Conference. Conference Proceedings. <https://bit.ly/3aOcdwH>

Castillo, C. (2024, 14 de octubre). *¿Sabes cómo es un pavo real bebé? La inteligencia artificial no y es un problema grave para Internet (Do you know what a baby peacock looks like? Artificial intelligence doesn't and it's a serious problem for the Internet)*. El Diario. <https://bit.ly/4spXG73>

Costa-Sánchez, C.; Vizoso, Á.; López-García, X. Fake News in the Post-COVID-19 Era? The Health Disinformation Agenda in Spain. *Societies* 2023, 13, 242. <https://doi.org/10.3390/soc13110242>

Diario de Madrid (2022). *Alerta: falsedad documental en fotocopias que simulan ser multas de tráfico colocadas en los parabrisas de algunos vehículos de la capital*. <https://bit.ly/3LARrIV>

Edelman (2024). *Edelman Trust Barometer 2024*. Edelman.com. <https://bit.ly/3XpxFpK>

EFE (2024, 16 de febrero). *Las grandes tecnológicas se comprometen a luchar contra la desinformación electoral*. <https://bit.ly/3LuF2dr>

Ennis, G. (2023). *Dark PR: How Corporate Disinformation Harms Our Health and the Environment*. Daraja Press.

ESET (2023). *ESET Threat Report H2 2023*. <https://bit.ly/3B5I5TU>

Ferreira Caceres, M. M., Sosa, J. P., Lawrence, J. A., Sestacovschi, C., Tidd!Johnson, A., Rasool, M. H. U., Gadamidi, V. K., Ozair, S., Pandav, K., Cuevas!Lou, C., Parrish, M., Rodriguez, I. y Fernandez, J. P. (2022). The impact of misinformation on the COVID-19 pandemic. *AIMS Public Health*, 9(2), 262–277. <https://doi.org/10.3934/publichealth.2022018>

Fidalgo, P. (2020, November 11). *WHO and Wikipedia team up against 'fake news' about coronaviruses*. El Plural. <https://bit.ly/4pvEmT7>

Foro Económico Mundial (2024). *Global Risks Report 2024*. weforum.org. <https://bit.ly/4guj0ST>

García-Marín, D. (2021). Agenda temática, metodologías e impacto de la investigación sobre desinformación. Revisión sistemática de la literatura (2016-2020). *Doxa Comunicación. Revista Interdisciplinar De Estudios De Comunicación Y Ciencias Sociales*, 33, 321-346. <https://doi.org/10.31921/doxacom.n33a854>

García-Marín, D., & Murolo, L. (2023). Plataformas, ficción y medios de comunicación: El algoritmo como cultura. In J. A. Gabelas-Barroso, D. García-Marín, & R. Aparici (Eds.), *La invasión del algoritmo* (pp. 291–293). Editorial Gedisa.

Gaw, F. (2025). Disinformation promotion on social media. In L. Edwards, C. Bourne, J. A. Cabañes, G. Castro (Eds.) *Disinformation promotion on social media* (Vol. 0, pp. -). Sage Publications Ltd, <https://doi.org/10.4135/9781529674583>

INCIBE (2023). *Suplantación de la Agencia Tributaria vía SMS durante el periodo de presentación de la renta 2023*. <https://bit.ly/4qETVIZ>

International Communications Consultancy Organisations (2014). *Helsinki Declaration*. ICCO. <https://iccopr.com/helsinki-declaration/>

Kropf, B., Wood, M., Parsons, K. (2023). Message matters: Correcting organisational fake news, *Computers in Human Behavior*, 144, <https://doi.org/10.1016/j.chb.2023.107732>.

Harari, Y. N. (2024). *Nexus*. Debate.

Lambert, C.A., Ewing, M.E. y Hassan, T. (2024). Watchful waiting: public relations strategies to minimize and manage a fake news crisis, *Journal of Communication Management*, 28(3), 459-481. <https://doi.org/10.1108/JCOM-05-2022-0064>

Mirza, S. Begum, L., Niu, L., Pardo, S., Abouzied, A., Papotti, P., & Pöpper, C. (2023). Tactics, Threats & Targets: Modeling Disinformation and its Mitigation. Proceedings 2023 Network and Distributed System Security Symposium. Network and Distributed System Security Symposium, San Diego, CA, USA. <https://doi.org/10.14722/ndss.2023.23657>

Moreno Espinosa, P., Abdulsalam Alsarayreh, R. A., & Figueero Benítez, J. C. (2024). El Big Data y la inteligencia artificial como soluciones a la desinformación. *Doxa Comunicación. Revista Interdisciplinar de Estudios de Comunicación y Ciencias Sociales*. <https://doi.org/10.31921/doxacom.n38a2029>

Rodríguez-Fernández, L. (2019). Desinformación y comunicación organizacional: estudio sobre el impacto de las fake news. *Revista Latina de Comunicación Social*, 74, 1714-1728. <https://doi.org/10.4185/RLCS-2019-1406>

Rodríguez-Fernández, L. y Establés, M. J. (2023). Impacto de la desinformación en las relaciones públicas: aproximación a la percepción de los profesionales (The impact of misinformation on public relations: an approach to practitioners' perceptions). *Estudios sobre el Mensaje Periodístico* 29(4), 843-853. <https://doi.org/10.5209/esmp.88661>

Rodríguez-Fernández, L. (2023). Desinformación y relaciones públicas. Aproximación a los términos Black PR y Dark PR (Disinformation and public relations. Approach to the terms Black PR and Dark PR). *ICONO 14. Revista Científica De Comunicación Y Tecnologías Emergentes*, 21(1). <https://doi.org/10.7195/ri14.v21i1.1920>

Rodríguez-Fernández, L. (Coord.), Aguado Terrón, J. M., Almansa Martínez, A., Arce García, S., Blanco Alfonso, I., Burguera Ameave, L., Campos Domínguez, E., Cantón Correa, J., Establés Heras, M. J., García Marín, D., Gómez García, S., Puebla Martínez, B., Rementería Núñez, M. J., Rodríguez Virgili, J., Salaverría Aliaga, R., & Wagner, A. (2023). Mapa de las capacidades de investigación en materia de desinformación en las universidades y centros de investigación. En *Foro contra las campañas de desinformación en el ámbito de la Seguridad Nacional. Trabajos 2023* (pp. 116–167). Gobierno de España, Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática.

- Rodríguez-Pérez, C., & Canel, M. J. (2022). La resiliencia a la desinformación como un recurso intangible asociado a los países. Análisis de España. *Estudios sobre el Mensaje Periodístico*, 28(4), 855-865. <https://doi.org/10.5209/esmp.82723>
- Rúas-Araújo, J., Quintas-Froufe, N., Dragomir, M., & Dos-Santos-Monteiro-Marinho, S. C. (2025). El impacto de la desinformación en la comunicación política, institucional y empresarial [Editorial. *Revista Mediterránea de Comunicación/Mediterranean Journal of Communication*, 16(2), e30103. <https://doi.org/10.14198/MEDCOM.30103>
- Silveira, A., Álvarez-Nobell, A. y Sadi, G. (2020). Fake news y relaciones públicas en América Latina. *In Mediaciones de la Comunicación*, (15), 1, 25-40.
- Vázquez Almendros, P y Paniagua Rojano, F. J. (2022). La labor de verificación de noticias desde el departamento de comunicación. Estudio de casos en el sector agroalimentario. *Revista de Ciencias de la Comunicación e Información*, 27, 1-23. <https://doi.org/10.35742/rcci.2022.27.e238>
- WHO. (2024, September 24). *WHO TikTok collaboration to generate more science!based information on health and wellness*. <https://bit.ly/45A55GT>
- Zerfass, A., Tench, R., Verhoeven, P., Vercic, D. y Moreno, A. (2018). *European Communication Monitor. Communication Director*. <https://bit.ly/45HRKMF>

