Revista de Comunicación de la SEECI, nº 48, 15 marzo 2019 -15 julio 2019, 149-171
ISSN: 1576-3420

INVESTIGACIÓN http://doi.org/10.15198/seeci.2019.48.149-171
Recibido: 14/08/2018 --- **Aceptado**: 09/01/2019 --- **Publicado**: 15/03/2019

LA TRANSPARENCIA COMO VARIABLE REPUTACIONAL DE LA COMUNICACIÓN DE CRISIS EN EL CONTEXTO MEDIÁTICO DEL CIBERATAQUE WANNACRY

TRANSPARENCY AS A REPUTATIONAL VARIABLE OF THE CRISIS COMMUNICATION IN THE MEDIA CONTEXT OF WANNACRY CYBERATTACK

Luis Mañas-Viniegra[1]: Universidad Complutense de Madrid. España.
lmanas@ucm.es

José Ignacio Niño González: Universidad Complutense de Madrid. España.
josenino@ucm.es

Luz Martínez Martínez: Universidad Rey Juan Carlos. España.
luz.martinez@urjc.es

RESUMEN

Esta investigación analiza el contexto mediático del ciberataque WannaCry en relación con la comunicación de crisis llevada a cabo por Telefónica con respecto a la ejercida en el sector de Telecomunicaciones, aplicando en dos intervalos del ciberataque la teoría fundamentada o *grounded theory* al discurso mediático de la prensa. A pesar de la mejorable reputación de las marcas corporativas en el sector de Telecomunicaciones, la reacción inmediata, la transparencia informativa ejercida, la colaboración con los organismos públicos y otros afectados y una rápida solución al ciberataque son las categorías fundamentales sobre las que se ha construido una reputación más sólida que la de su competencia directa durante la comunicación de crisis, trasladando la tradicional portavocía oficial a las redes sociales de uno de sus directivos. El sentimiento negativo del 14% que emerge del discurso mediático durante la primera oleada del ciberataque coincide con el 12% mostrado por la ciudadanía en Twitter, por lo que la opinión publicada es coherente con la opinión de los públicos. A pesar de ello, se observa una mayor incidencia del enfoque negativo en los diarios digitales "confidenciales", menos expuestos a la presión publicitaria de las grandes marcas corporativas y más a la pérdida de valores periodísticos aludida en la literatura científica.

---

[1]Luis Mañas-Viniegra: Doctor en Comunicación Audiovisual y Publicidad, profesor asociado en la Universidad Complutense de Madrid y miembro del grupo de investigación Complutense "Gestión de las Marcas y Procesos de Comunicación".
lmanas@ucm.es

PALABRAS CLAVE: WannaCry – análisis mediático – comunicación de crisis – reputación – marca corporativa – transparencia – redes sociales.

ABSTRACT

This piece of research analyzes the media context of the WannaCry cyberattack in relation to the crisis communication carried out by Telefónica with respect to that exercised in the Telecommunications sector, applying, in two intervals of the cyberattack, the *grounded theory* to the media discourse of the press. Despite the improvable reputation of the corporate brands in the Telecommunications sector, the immediate reaction, the informative transparency exerted, the collaboration with public bodies and others affected and a quick solution to the cyberattack are the fundamental categories on which a stronger reputation than that of its direct competition has been built during the crisis communication, transferring the traditional official spokesperson to the social networks of one of its directors. The negative feeling of 14% that emerges from the media discourse during the first wave of cyberattack coincides with the 12% shown by citizens on Twitter, so the published opinion is consistent with the opinion of the public. Despite this, there is a greater incidence of the negative approach in the "confidential" digital newspapers, less exposed to the advertising pressure of the large corporate brands and more to the loss of journalistic values alluded to in the scientific literature.

KEY WORDS: WannaCry – media analysis – crisis communication – reputation – corporate brand – transparency – social networks.

A TRANSPARÊNCIA COMO VARIÁVEL REPUTACIONAL DA COMUNICAÇÃO DE CRISES NO CONTEXTO MEDIÁTICO DO CIBER ATAQUE WANNACRY

RESUME

Esta investigação analisa o contexto mediático do ciber ataque WannaCry em relação com a comunicação de crises levada a cabo por Telefônica com respeito a exercida no setor de Telecomunicações, aplicando em dois intervalos de ciber ataque a teoria fundamentada ou *grounded theory* ao discurso mediático da imprensa. Apesar da melhorável reputação das marcas coorporativas no setor de Telecomunicações, a reação imediata, a transparência informativa exercida, a colaboração com os organismos públicos e outros afetados e uma rápida solução ao ciber ataque são as categorias fundamentais sobre as que foram construídas uma reputação mais solida que a de sua concorrente direta durante a comunicação de crises, trasladando a tradicionais porta vozes oficial as redes sociais de um de seus diretivos. O sentimento negativo de 14% que emerge do discurso mediático durante a primeira oleada de ciber ataque coincide com 12% mostrado pela cidadania em Twitter, pelo qual a opinião publicada é coerente com a opinião dos públicos. Apesar disso, se observa uma maior incidência do enfoque negativo nas notícias digitais "confidenciais",

menos expostos a pressão publicitaria das grandes marcas coorporativas e mais a perda de valores jornalísticas aludida na literatura cientifica.

PALAVRAS CHAVE: WannaCry – analises mediática – comunicação de crises – reputação – marcas coorporativas – transparência – redes sociais.

Cómo citar el artículo:

Mañas-Viniegra, L.; Niño González, J. L., y Martínez Martínez, L. (2019). La transparencia como variable reputacional de la comunicación de crisis en el contexto mediático del ciberataque WannaCry. [Transparency as a reputational variable of the communication in the media context of WannaCry cyberattack]. Revista de Comunicación de la SEECI, 48, 149-171. doi: http://doi.org/10.15198/seeci.2019.48.149-171 Recuperado de http://www.seeci.net/revista/index.php/seeci/article/view/549

1. INTRODUCCIÓN

Los medios de comunicación influyen notablemente en la interpretación que los públicos realizan de una crisis, especialmente las previas al ecosistema digital. En función de la selección de los temas que integran la *agenda-setting* (Shaw, 1979; Wolf, 1994), cada día se decide por los *gatekeepers* el bloqueo o no de determinadas informaciones (Barzilai-Nahon, 2008). Junto a los efectos del encuadre desde el que se observa la realidad o *framing* (Hanggli & Kriesi, 2012) y la exposición selectiva (Rubin, 1996), pueden provocar una correlación positiva entre el número de noticias publicadas y una mayor preocupación por parte de la ciudadanía (Igartua, Otero, Muñiz, Cheng, & Gómez, 2007).

Sin embargo, la pérdida de valores que ha sufrido una parte de la profesión periodística, entre los que destacan "el contraste, el rigor, la honestidad y la calidad" (Gómez-Mompart, Gutiérrez-Lozano, & Palau-Sampio, 2015, p. 147) y una escasa independencia política y económica (Asociación de la Prensa de Madrid, 2014), han provocado que la información publicada sobre las empresas en situaciones de crisis no se corresponda en ocasiones con la interpretación de la situación que realizan el resto de públicos y que expresan habitualmente en las redes sociales. Esta paradoja provoca que la opinión publicada no siempre se corresponda con la opinión de los públicos, que es precisamente una de las cuestiones que esta investigación trata de aclarar en relación con el caso de estudio. No podemos obviar en relación a esa independencia económica que Telefónica es el undécimo mayor anunciante en España (Sánchez-Revilla, 2017), en línea con otros grandes operadores del sector de las telecomunicaciones, ya que tanto Vodafone como Orange se encuentran en el *top* 10 de los anunciantes.

Las grandes organizaciones han pasado de competir como marcas producto a configurarse como marcas corporativas (Olins, 2009) disociadas de los productos y orientadas hacia sus públicos de interés o *stakeholders* (Freeman, 1984) a partir de modelos de conducta que proyectan a la sociedad, convirtiéndose algunas en

referentes para ella (Benavides-Delgado, 2015), donde la reputación, transparencia, responsabilidad social y un buen gobierno corporativo son componentes esenciales. La reputación se fundamenta en la percepción (Gaine-Ross, 2003), el reconocimiento (Ferguson, Deephouse, & Ferguson, 2000) o la participación (Aaker, 1996) de los *stakeholders*, quienes evalúan la personalidad o identidad corporativa, con un carácter estructural que permite unos efectos duraderos (Villafañe, 2012). El enfoque sistémico de las organizaciones propugna, además, unas relaciones recíprocas entre la organización y sus públicos (Xifra, 2005), de modo que se establezca un modelo simétrico bidireccional (Grunig & Hunt, 1984) en la comunicación.

A pesar de la variedad de crisis que pueden afectar a una organización, existen elementos que se reiteran, como la ausencia de previsión, una información inicial insuficiente ante acontecimientos que suceden rápidamente y a los que hay que responder con urgencia, o el interés de los medios de comunicación, encontrándose afectadas la imagen y la reputación de los diferentes públicos: las víctimas, los empleados, los clientes, los poderes públicos, la audiencia de los medios o la propia organización, entre otros externos e internos (Cervera-Fantoni, 2008; Castillo-Esparcia, 2010), considerando que es necesario armonizar los intereses de la organización con los de sus públicos (Costa, 2004).

El escenario de incertidumbre que conlleva cualquier crisis provoca un incremento de la presión informativa por parte de los medios de comunicación, los ciudadanos y los propios empleados que afecta negativamente a la relación entre la empresa y sus *stakeholders* (Van-der-Meer, Verhoeven, Beentjes, & Vliegenthart, 2017). Es esa tensión la que habitualmente lleva a la precipitación y a cometer errores en la comunicación de crisis y, por ello, el Director General o CEO de la empresa continúa siendo el portavoz que mayor credibilidad puede despertar cuando se dispone de la reputación adecuada (Kim & Park, 2017), aunque siempre en coordinación con el *dircom* (Grunig, Grunig, & Dozier, 2002), que en el caso de Telefónica reporta directamente a la Presidencia (Recalde & Gutiérrez-García, 2017). A pesar de estas tensiones, es imprescindible para proteger la reputación que las primeras declaraciones de la empresa se produzcan con rapidez, sean transparentes, ofrezcan información precisa y tranquilicen a los públicos que pudieran verse afectados (Woods, 2016), prestando una atención adecuada a las evaluaciones que realicen los medios de comunicación, la ciudadanía y el resto de *stakeholders* (Romero-Rodríguez, Torres-Toukoumidis, & Pérez-Rodríguez, 2017).

La llegada de las redes sociales influyeron de manera determinante en la relación asimétrica que existía entre las empresas y los públicos de interés o *stakeholders* en la comunicación de crisis, permitiendo que éstos accediesen a información que los primeros acostumbraban a ocultar cuando podían prever que perjudicaría su imagen (Castillo-Esparcia & Ponce, 2015). Precisamente la pérdida de credibilidad, confianza y reputación son consecuencias de una gestión de crisis inadecuada (Capriotti, 1999; Villafañe, 2008).

La hostilidad comunicativa (Castillo-Esparcia & Ponce, 2015) es un comportamiento negativo hacia la organización que afecta a su credibilidad y

reputación al centrarse la atención de la opinión pública en un aspecto concreto de la situación que ha originado la crisis, surgida en muchas ocasiones a partir de la publicación de una información que se desconocía o de la propia respuesta que da la organización al hecho que inicia la crisis. Que las marcas en redes sociales habitualmente respondan de manera rápida a las menciones que reciben (Aced, 2013), implica el riesgo de que el equipo de *community managers* proporcione información o emita una respuesta sin haber considerado que se encuentra en una situación de crisis, a pesar de la necesidad de responder a una crisis 2.0 con rapidez, visibilidad y credibilidad (Bollero, 2008). En cualquier caso, la comunicación de crisis en el ecosistema digital implica un cambio continuo que implica una revisión de las teorías y taxonomías existentes (García-Ponce & Smolak-Lozano, 2013).

En una situación de comunicación de crisis actual, tanto la *agenda-setting* como el *framing* de los medios debe contrastarse con las opiniones expresadas por los *stakeholders* en redes sociales para evaluar cómo evoluciona la percepción de los públicos sobre la situación, de modo que se adapten las respuestas de la organización de cara a preservar su reputación (Coombs, 2007; Coombs, & Holladay, 2012; Bowen & Zheng, 2015).

La importancia de la crisis generada por el ciberataque WannaCry radica en la alteración de algunos los principios rectores de la gestión de la comunicación que tradicionalmente se han seguido por parte de las organizaciones (Westphalen & Piñuel, 1993; Luecke, 2005): llevar la iniciativa en la comunicación con un único portavoz designado que evite la formación de rumores, ofrecer detalles de lo sucedido sin proporcionar información falsa ni eludir la responsabilidad que corresponda, manteniendo la credibilidad con disculpas públicas por lo sucedido e iniciando medidas concretas para paliar sus efectos y evitar que se pueda volver a repetir en un futuro.

1.1. El contexto de la organización

En 1924 se crea la Compañía Telefónica Nacional de España (Telefónica) para prestar un servicio de telefonía que ejercerá en régimen de monopolio, encabezando en los años 70 una internacionalización sin precedentes entre las empresas españolas y comenzando a cotizar en la Bolsa de Nueva York en 1987 (Calvo-Calvo, 2010). Sin embargo, las directivas de liberalización de la hoy denominada Unión Europea, dirigidas a disolver los monopolios en los servicios básicos, propiciaron que Telefónica se privatizase y tuviese que competir en libre concurrencia a partir de 1998 con nuevas compañías que surgieron en pleno auge de la telefonía móvil e Internet (Bel & Trillas, 2005). La consecuencia fue una cruenta guerra comercial que se extendió durante más de una década y que derivó en una notable pérdida de reputación por parte Telefónica (Calzada & Estruch, 2011) y, en general, de todo el sector de Telecomunicaciones. Fue en ese momento cuando la Compañía comprendió la necesidad de innovar y educar en innovación para convertirse en el actual operador integrado de telecomunicaciones, mejorar la satisfacción del cliente y desarrollar una decidida política de responsabilidad social corporativa (Palacios-Marqués & Devece-Caranana, 2013), decisiones que han permitido su conversión en una auténtica corporación multinacional (Clifton, Comin, & Díaz-Fuentes, 2011).

Para ello, la entidad emprendió una reestructuración de su arquitectura de marcas que permitiese la paulatina recuperación de su reputación corporativa, simplificando una maraña de marcas cuyo origen fueron las adquisiciones y fusiones llevadas a cabo con anterioridad a la crisis de las *puntocom* en el año 2000. De este modo, se reducían las marcas de producto a Movistar, O2 y Vivo, disociándolas de la marca corporativa Telefónica y centrando ésta en unos valores corporativos coherentes con "el respeto, la calidad y la transparencia" (Telefónica, 2016), su responsabilidad social y una buena organización del gobierno corporativo en la búsqueda de una mayor relación con la ciudadanía y la obtención de una mejor reputación.

A pesar de que la marca de producto Movistar ocupa el puesto 43 a nivel mundial, con una valoración de más de 22.000 millones de dólares (Kantar MillwardBrown, 2017), la marca corporativa Telefónica no se encuentra entre las 50 empresas con mejor reputación en España (RepTrak, 2017) ni entre las 100 primeras del mundo (RepTrak, 2017a), por lo que la cuestión reputacional continúa siendo vulnerable en su gestión estratégica. De igual modo, el propio sector de las Telecomunicaciones es el que peor reputación obtiene de todos, con 56,0 puntos, que RepTrak considera débil sin necesidad de comparación con otros sectores.

1.2. El ciberataque WannaCry

El 12 de mayo de 2017 comenzaba un ciberataque mundial con un *software* malicioso o *malware*, llamado WannaCry, que afectaba a varias empresas españolas bloqueando sus redes de comunicaciones y pidiendo un rescate para su liberación, de ahí la denominación de *ransomware*. La noticia, que apareció inicialmente en los medios de comunicación sin una confirmación oficial, pronto incorporó a Telefónica como la principal afectada tras la ratificación efectuada por fuentes internas, mientras otras compañías que se citaban como atacadas lo negaban rotundamente, como Vodafone, BBVA o Capgemini. Un tercer grupo de empresas, como Iberdrola o Gas Natural, sólo reconocían haber apagado sus equipos como medida de prevención. El Centro de Respuesta a Incidentes de Seguridad e Industria (CERTSI), dependiente del Ministerio de Interior y del Ministerio de Industria, confirmó oficialmente que España había sufrido el ciberataque de WannaCry, aunque sin mencionar a las empresas afectadas.

El ciberataque WannaCry ha suscitado el interés de los investigadores, aunque limitado hasta ahora a cuestiones como su análisis tecnológico (Krunal & Kumar, 2017; Mourle & Patil, 2017; Woods, Agrafiotis, & Jason, 2017), la propuesta de utilización de la tecnología Blockchain, que envía y encripta la información separada por bloques, la consideración de la ciberseguridad como un derecho humano (Shackelford, 2017), las consecuencias que ha tenido para los pacientes del servicio británico de salud o NHS (Clarke & Youngstein, 2017; Ehrenfeld, 2017) o las responsabilidades penales que pudieran derivarse desde la perspectiva del *compliance* (Cain et al., 2017).

Este tipo de ciberataques no son nuevos y su efecto inmediato para las corporaciones es conocido tras los precedentes sufridos por Google en 2010 (Jacobs

& Helft, 2010) o por Sony Pictures en 2014 (Barnes & Cieply, 2014): la parálisis de su sistema informático y la petición del pago de un rescate. Sin embargo, más allá de los efectos meramente económico-financieros y de parada técnica de los procesos de las empresas, de duración efímera, las crisis reputacionales que pudieran derivarse son el auténtico problema al que se enfrentan. Una mala gestión de la comunicación de crisis suele ser el detonante de una crisis reputacional.

Es habitual que las empresas hagan públicos estos ciberataques días después de haberlos sufrido, mostrando el control de la situación y minimizando las consecuencias. Es por ello que habitualmente sus *stakeholders* reclaman una mayor transparencia, puesto que los datos personales de los clientes, proveedores o los propios empleados pueden haber estado expuestos, hecho que se omite en muchas ocasiones. Así sucedió en el caso de Google citado, que supuso una lección aprendida para informar expresamente sobre esta cuestión al sufrir un nuevo ciberataque al año siguiente. En otro ataque sufrido por Sony en 2011, la Compañía tardó seis días en comunicar que los datos personales de 77 millones de usuarios habían quedado expuestos, incluyendo los registros de sus tarjetas de crédito (Delclós, 2011).

En este sentido, la confirmación oficial por parte de Telefónica se producía la misma mañana del ataque a través de un escueto comunicado aséptico de 5 líneas en su sala de prensa online en la que se afirmaba haber

> detectado un incidente de ciberseguridad que ha afectado los PCs de algunos empleados de la red corporativa interna de la compañía. De forma inmediata, se ha activado el protocolo de seguridad para este tipo de incidencias con la intención de que los ordenadores afectados funcionen con normalidad lo antes posible. (Telefónica, 2017).

Telefónica era la primera empresa que reconocía el ataque, lo comunicó con transparencia y colaboró con los organismos públicos en la solución del ransomware, hecho que fue reconocido en nota de prensa por el propio Instituto Nacional de Ciberseguridad (INCIBE) y con la condecoración de la medalla blanca de la Guardia Civil al Chief Data Officer (CDO) de Telefónica por su colaboración.

En el ciberataque WannaCry sufrido por Telefónica, la portavocía la asumió informalmente a través de su cuenta en Twitter su CDO, única persona de la Compañía que hizo algún tipo de declaración identificada, aunque sorprendentemente fue para indicar que "la seguridad interna de telefónica no es una de mis responsabilidades directas. Pero todos somos parte de la seguridad en la casa. Las noticias son exageradas". Las críticas no se hicieron esperar en los medios de comunicación y en medios sociales, puesto que en la propia web de Telefónica se indica su dependencia jerárquica de la Presidencia y sus funciones como "responsable de la ciberseguridad global y de la seguridad de los datos". Añadió, además, que se encontraba de vacaciones, aunque ayudando en remoto.

Son numerosas las crisis en las que, equivocadamente, el líder culpa de la misma a la negligencia de sus empleados (Volkswagen y sus emisiones tóxicas), la invención

de los medios de comunicación (Donald Trump) o las propias víctimas (crisis del Ébola en España), estrategias típicas defensivas (Coombs & Holladay, 2010). Sin embargo, es insólita la situación en la que el portavoz lleva a cabo un ejemplo de transparencia anunciando una crisis que afecta a la marca corporativa para, a continuación, eludir cualquier tipo de responsabilidad aun siendo el máximo responsable de su prevención, iniciando la posibilidad de que se produzca una crisis reputacional dentro de la comunicación de crisis.

El 19 de mayo, el CDO de Telefónica publicó una entrada en su blog personal en la que aclaraba sus responsabilidades, vacaciones, aciertos y errores en la gestión del ciberataque, en un nuevo alarde de transparencia y naturalidad en la comunicación de la crisis desconocidas en otras crisis previas al ecosistema digital.

2. OBJETIVOS

Esta investigación analiza cuantitativamente y cualitativamente la comunicación de crisis de Telefónica con motivo de la infección de sus sistemas informáticos por el ciberataque WannaCry, comparando el enfoque de las informaciones publicadas por la prensa española con el sentimiento de sus públicos en Twitter.

Los objetivos específicos son:

- Identificar las informaciones publicadas en la prensa nacional sobre la organización durante el ciberataque.
- Analizar el contenido y el discurso de las informaciones para identificar el enfoque positivo, negativo o neutro utilizado.
- Identificar los elementos novedosos de la comunicación de crisis de Telefónica con influencia en su reputación.
- Realizar un análisis de sentimiento de Telefónica en Twitter durante el ciberataque.
- Determinar si la opinión publicada coincide con la opinión de los públicos.

3. METODOLOGÍA

Para la consecución de los objetivos se emplea como metodología la teoría fundamentada (Glaser & Strauss, 1967; Strauss & Corbin, 1990; Glaser, 1992; Locke, 2001; Douglas 2004; Blythe, 2007) o *grounded theory* por su carácter explicativo de las conductas en las organizaciones y de los discursos sociales, partiendo sin hipótesis que pueda condicionar los resultados antes de saturar las categorías en la identificación de los conceptos redundantes en el análisis del discurso (Benavides-Delgado, 2005).

Se analizan las dos oleadas en la comunicación de crisis de Telefónica con motivo del ciberataque WannaCry. La primera abarca desde el 12 hasta el 18 de mayo de 2017, es decir, desde que se produce la infección del *ransomware* WannaCry hasta que los efectos en España desaparecen por completo, que es la semana de la crisis reputacional. La segunda se inicia el 19 de mayo, tras entrada publicada en su *blog* por el CDO de Telefónica, hasta que concluye el mes de mayo.

Por un lado, se analizan cuantitativa y cualitativamente las informaciones publicadas al respecto por la prensa con el soporte del software Atlas.ti v.6.2. La muestra está formada por tres grupos de medios impresos. Un primer grupo lo integran las cinco principales cabeceras de prensa nacional diaria: El País, La Vanguardia, El Mundo, ABC y La Razón. El segundo grupo lo compone toda la prensa económica: Expansión, Cinco Días y El Economista. Un tercer grupo lo forman los cinco principales diarios digitales que habitualmente se centran en informaciones "confidenciales": El Confidencial, Ok Diario, Libertad Digital, Eldiario.es y Voz Populi. Se accedió a sus versiones digitales por disponer de mayor profusión de noticias que la versión impresa y se eliminaron las informaciones en las que apareciesen las palabras clave "ransomware", "WannaCry" o "ciberataque" sin que estuviera presente Telefónica, puesto que su contenido era meramente tecnológico.

El diseño muestral está basado en la selección realizada a partir los datos de difusión del año 2016 (OJD, 2017) de los cinco principales diarios nacionales y toda la prensa económica.

Tabla 1. *Promedio de difusión año 2016 de diarios nacionales y prensa económica en España.*

Información general	**Promedio difusión**
El País	194.005
La Vanguardia	114.960
El Mundo	108.386
ABC	91.159
La Razón	77.129
Información económica	**Promedio difusión**
Expansión	23.992
Cinco Días	21.205
El Economista	11.661

Fuente: Elaboración propia a partir de OJD (2017).

En el caso de los diarios digitales confidenciales, la selección de los cinco diarios se realiza partir de los datos de visitantes únicos al cierre de marzo de 2017 (Comscore, 2017):

Tabla 2. *Usuarios únicos año 2016 de diarios digitales "confidenciales".*

Diario	**Visitantes únicos (000)**
Elconfidencial.com	10.368
Eldiario.es	6.578

Elespanol.com	6.499
Okdiario.com	5.541
Libertaddigital.com	2.987

Fuente: Elaboración propia a partir de Comscore MMX (2017).

En el primer intervalo (i^1) se registran 173 informaciones válidas (93,51% del total), frente a las 12 (6,49%) del segundo intervalo (i^2), conforme a la siguiente distribución:

Tabla 3. *Distribución del número de informaciones publicadas por intervalo.*

Diario	i^1	i^2	Total
El País	16	3	19
La Vanguardia	7	1	8
El Mundo	18	3	21
ABC	25	0	25
La Razón	17	0	17
Expansión	8	0	8
Cinco Días	12	1	13
El Economista	17	0	17
Elconfidencial.com	8	0	8
Eldiario.es	10	2	12
Elespanol.com	15	0	15
Okdiario.com	15	1	16
Libertaddigital.com	5	1	6
Total	**173**	**12**	**185**

Fuente: Elaboración propia.

El contenido se catalogó en 3 familias: reputación positiva, neutra y negativa, que, a su vez, se ordenan en unidades hermenéuticas para cada intervalo. El sistema de codificación empleado ha sido inductivo o *bottom-up*, partiendo de los datos para llegar a los códigos.

Por otro lado, se realiza un análisis de sentimiento de la marca Telefónica en comparación con la de su competidor Vodafone -implicado en el ciberataque sin un reconocimiento oficial- a partir del contenido de los tweets publicados, evaluado por pares por los autores con el objetivo de contrastar la opinión publicada por la prensa con la de otros stakeholders, que se amplían al conjunto de la sociedad con presencia en Twitter, a menudo la más crítica. El análisis de sentimiento se realiza con el soporte tecnológico de la API de Twitter a partir de los tweets publicados el 12 de mayo de 2017, por ser éste el primer día de la crisis y el de mayor virulencia para

la marca, aislando así el efecto de su transparencia y la portavocía ejercida en redes sociales en el escenario más negativo posible con respecto al resto de días de la gestión de la comunicación de crisis.

4. DISCUSIÓN

La unidad hermenéutica i[1], la principal, permitió establecer tres familias en función del enfoque adoptado mayoritariamente por cada información en la que se citaba expresamente a Telefónica en relación con el ciberataque: enfoque positivo (34 informaciones, el 19,65% del total), neutro (119, 68,79%) y negativo (20, 11,56%). Hay que considerar que sufrir un ciberataque es, *per se*, un hecho negativo, pero se ha considerado el tono general de cada información y la predominancia de unos elementos sobre otros, ya sean negativos o positivos. Además, se observa claramente en el siguiente gráfico cómo las informaciones con enfoque negativo tienen mayor frecuencia en los diarios digitales "confidenciales", que presentan una menor dependencia de los ingresos publicitarios de las grandes marcas como Telefónica.

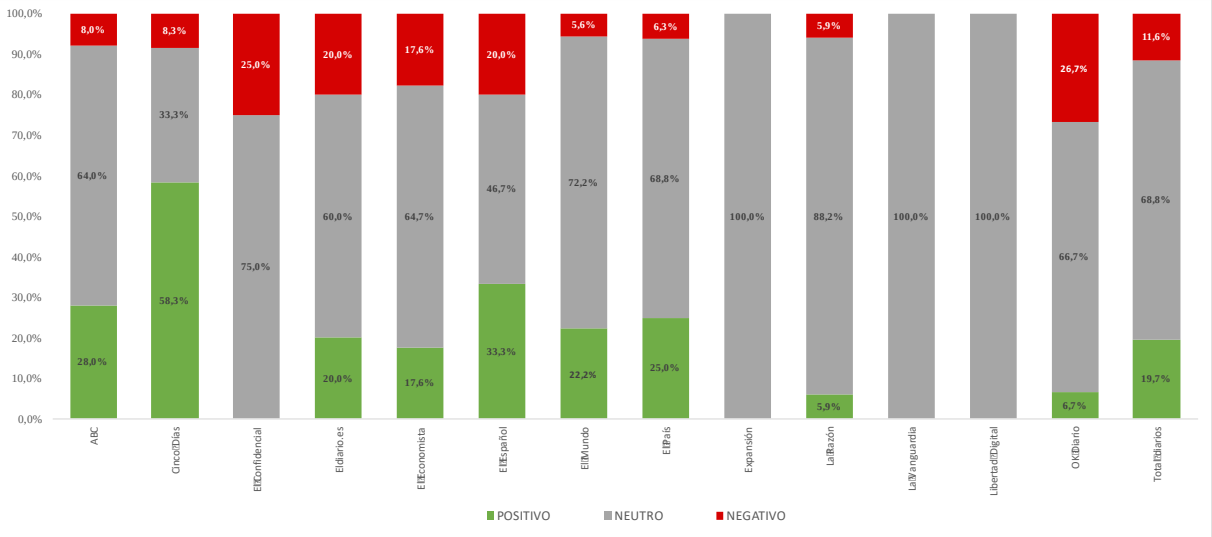

Figura 1. *Tipos de discursos por diarios y en total en intervalo i[1].*
Fuente: Elaboración propia.

Dentro de la primera familia, la del enfoque positivo, el análisis del contenido ha permitido codificar tres categorías que construyen un discurso positivo. La primera de ellas es la colaboración de Telefónica con INCIBE y con otras empresas para encontrar una solución al ciberataque en España, con 29 menciones. La segunda es el discurso informativo de control de la situación, que en la mayoría de las informaciones van ligadas a la solución de la infección, con 67 menciones. En tercer lugar, existe un reconocimiento, y en ocasiones un elogio, de la transparencia mostrada por la Compañía, avisando del ataque y reconociéndolo públicamente desde el primer momento, al contrario que el resto de las empresas españolas afectadas, que aseguraban haber apagado sus equipos por mera precaución. Tan sólo Renault a nivel mundial actuó con la misma transparencia en su comunicación de crisis. La transparencia aparece reflejada en 114 menciones.

El enfoque neutro constituye la segunda familia, detectándose dos categorías a partir de la codificación de las informaciones en las que se cita expresamente a Telefónica: "ciberataque", con 248 menciones que representan el 69% de las informaciones, hace referencia a un enfoque de las informaciones en el que se relatan los hechos acaecidos sin una opinión expresa sobre la actuación o la vulnerabilidad de la Compañía. La segunda categoría menciona en 196 ocasiones a otras empresas u organismos afectados, otorgándoles en la mayoría de las ocasiones más espacio que a Telefónica, especialmente en el caso del NHS por su repercusión internacional y mayor incidencia para los ciudadanos.

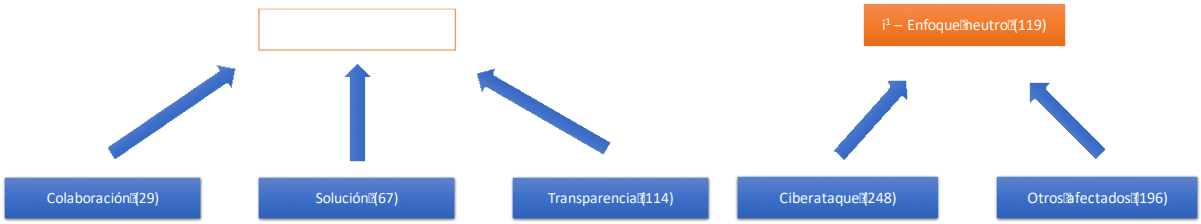

Figura 2. *Diagrama de relación i¹-positivo y enfoque neutro.*
Fuente: Elaboración propia.

El enfoque negativo apenas aparece en 20 informaciones, el 12% del total, dato que refleja por sí mismo una adecuada gestión de la comunicación de crisis, al menos en su relación con la prensa. Las informaciones estrictamente negativas adoptan un enfoque crítico, en ocasiones cercano a la sátira, a la actitud del CDO de Telefónica (16 menciones) por eludir responsabilidades en su cuenta de Twitter, la debilidad que implica en plena era digital anunciar por megafonía a todos los empleados que apaguen los ordenadores y dejen de trabajar hasta nueva orden (58 menciones), más allá de que una empresa de tal magnitud resulte infectada, y, en último lugar, la focalización de la crisis en la irresponsabilidad de un empleado que abrió el correo electrónico que contenía el virus, únicamente con 4 menciones.

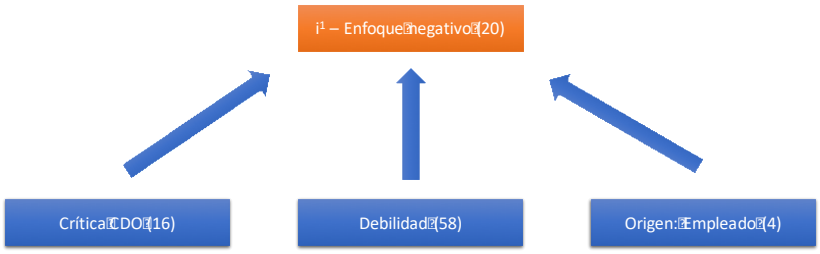

Figura 3. *Diagrama de relación i¹-enfoque negativo.*
Fuente: Elaboración propia.

La unidad hermenéutica i^2 refleja claramente cómo el interés informativo decae y se aleja de Telefónica con sólo 12 informaciones, de las que únicamente una (8%) es negativa, como consecuencia de la debilidad mostrada por una empresa de su magnitud. No aparece ya ningún código sobre las críticas al CDO, que han quedado neutralizadas con sus explicaciones. El enfoque neutro vuelve a predominar con 7 informaciones y el positivo representa el 33% de las informaciones de este segundo

periodo, destacando de nuevo la transparencia, con seis menciones, sólo por detrás de los códigos que pertenecen al enfoque neutro: "ciberataque" (9 menciones) y "otros afectados" (5).

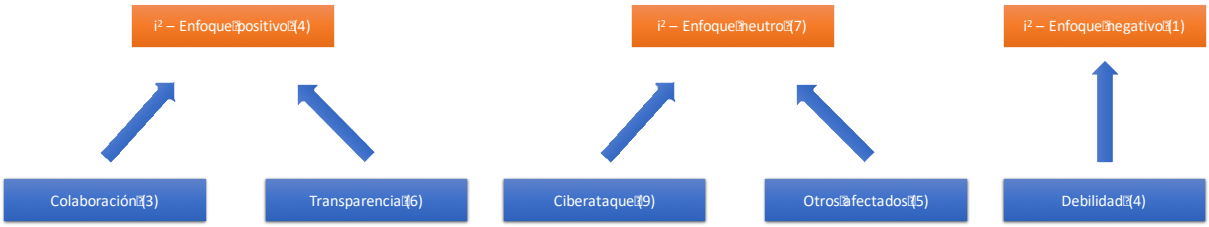

Figura 4. *Diagrama de relación i².*
Fuente: Elaboración propia.

En cuanto a la reiteración total de los códigos en las informaciones, los códigos neutros representan el 60,34% sobre el total, los positivos, un 28,85% y los negativos, tan sólo un 10,80%. Los códigos preeminentes son "ciberataque" (33,86%), "otros afectados" (26,48%) y "transparencia" (15,81%). Los datos vuelven a confirmar la importancia de la rápida comunicación y asunción del ciberataque por parte de Telefónica en la gestión de la crisis, evitando una incidencia reputacional en las informaciones publicadas.

Tabla 4. *Frecuencia de los códigos en informaciones publicadas por intervalo.*

Códigos	i^1	i^2	Total	%
Ciberataque	248	9	257	33,86%
Colaboración	29	3	32	4,22%
Crítica CDO	16	0	16	2,11%
Debilidad	58	4	62	8,17%
Origen: empleado	4	0	4	0,53%
Otros afectados	196	5	201	26,48%
Solución	67	0	67	8,83%
Transparencia	114	6	120	15,81%
Total	**732**	**27**	**759**	**100,00**

Fuente: Elaboración propia.

Agotar el análisis de la comunicación de crisis llevada a cabo con motivo del ciberataque sufrido en la prensa supondría limitar la importancia del resto de *stakeholders* en el refuerzo o el deterioro de esa reputación aún frágil de la marca corporativa Telefónica.

El análisis de sentimiento en Twitter del día del ciberataque, realizado con los mismos criterios del análisis de las informaciones, confirma cómo efectivamente el alarde de transparencia y colaboración llevado a cabo ha servido para neutralizar los

efectos negativos en la opinión pública de la debilidad o la actitud inicial del CDO a la hora de eludir responsabilidades. El 3,8% de los *tweets* refleja un sentimiento positivo, un 82,4% neutro y un 13,7% negativo. La puntuación de sentimiento, que se calcula dividiendo exclusivamente los *tweets* positivos entre la suma de los positivos y negativos, es 21.

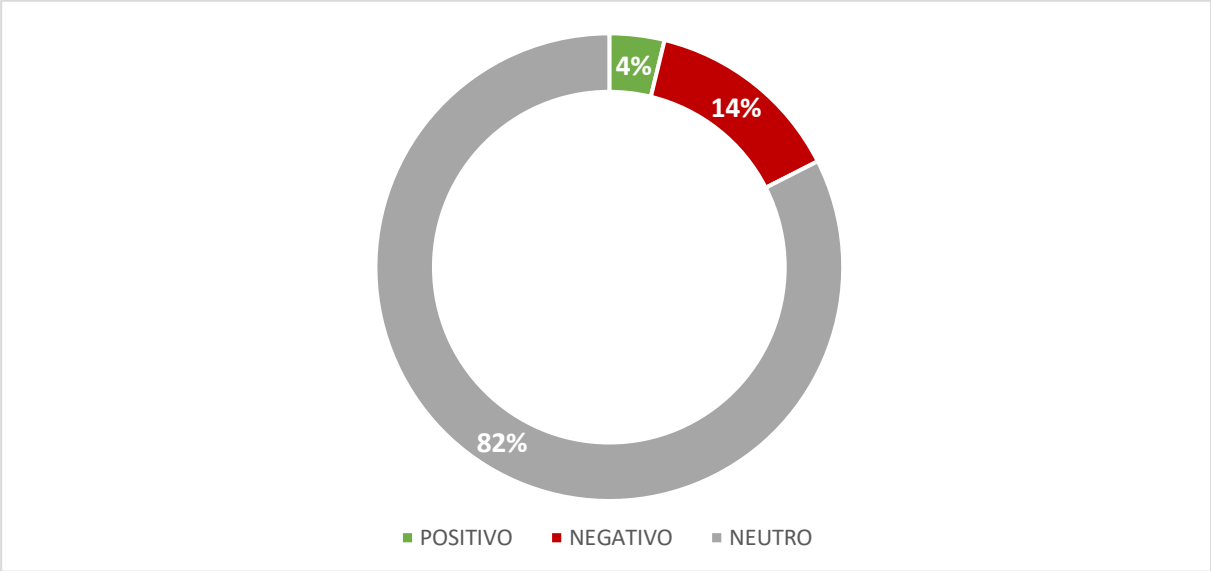

Figura 5. *Análisis de sentimiento de Telefónica durante el ciberataque.*
Fuente: Elaboración propia.

Ya advertimos en el estado de la cuestión los problemas reputacionales que Telefónica arrastra como consecuencia de la feroz competencia vivida por el sector de las telecomunicaciones durante más de una década. Por ello, y aun habiendo disociado sus marcas de producto de su marca corporativa, aún hoy se aprecian críticas de los consumidores de Movistar en sus *tweets* haciendo alusión a Telefónica, por lo que aún es necesario un mayor periodo de tiempo para que todos los públicos aprecien esta diferencia. Hay que considerar, de igual modo, que Telefónica es una empresa que cotiza en Bolsa y que las alzas o bajas en su cotización diaria también afectan a los *tweets* que se publican sobre ella, no como marca, sino como empresa cotizada de cuya evolución depende el patrimonio de millones de accionistas.

Precisamente porque, aun contemplando todos estos condicionantes, pudiera parecer que el 13,7% de sentimiento negativo es muy elevado reputacionalmente en términos absolutos, hay que realizar una comparativa con su competencia y con otras marcas reputadas pertenecientes a otros sectores no afectados por el ciberataque.

Hay que recordar que Telefónica no se encuentra entre las marcas más reputadas a nivel internacional ni en España, cuestión fundamental a la hora de afrontar una crisis con fortaleza. De este modo, frente al 13,7% de sentimiento negativo de Telefónica, Renault presenta sólo un 2,7% negativo y un 8,4% positivo, cifras mucho más sólidas reputacionalmente que las de Telefónica, especialmente teniendo en

cuenta que Renault fue la otra gran marca que reconoció el sufrir el ataque desde el primer momento y que partía de la posición 87 a nivel mundial en el Global RepTrak 2017 (Reputation Institute, 2017). Sin embargo, al comparar el análisis de sentimiento de Telefónica con respecto a su competencia el día del ciberataque, comprobamos que presenta el menor sentimiento negativo, a pesar de ser el principal protagonista en España del ciberataque en todos los medios de comunicación, un hecho que por sí mismo es negativo. Como consecuencia lógica, presenta también el menor sentimiento positivo el día del ataque, que mejora conforme la crisis se va solucionando, y también el mayor sentimiento neutro.

Vodafone, su principal competidor, no reconoció en ningún momento haber sufrido el ataque, a pesar de que todos los medios de comunicación así lo afirmaban por fuentes no oficiales. Esta actitud tiene un claro reflejo de deterioro reputacional no recogido por la prensa, pero sí por el análisis de sentimiento realizado en Twitter, con un 26,8% de sentimiento negativo, casi el doble del experimentado por Telefónica. Ni Orange ni Más Móvil sufrieron el ciberataque, mostrando ambos un comportamiento dispar. Así mientras el sentimiento positivo experimentado por Orange ascendía hasta el 28,8%, el mayor de todos, los datos de Más Móvil eran peores que los de Telefónica, explicados por la débil reputación de todo el sector de Telecomunicaciones como consecuencia de los conflictos permanentes que experimentan con sus clientes y que ya han sido mencionados.

Tabla 5. *Análisis de sentimiento durante el ciberataque.*

Empresa	Sentimiento Positivo	Sentimiento Neutro	Sentimiento Negativo	Puntuación Sentimiento
Más Móvil	3,4%	78,2%	18,4%	15
Orange	28,8%	54,8%	16,4%	63
Telefónica	3,8%	82,4%	13,7%	21
Vodafone	9,3%	63,9%	26,8%	25

Fuente: Elaboración propia.

En definitiva, parece existir una coherencia entre la agenda y el *framing* de la prensa y el análisis de sentimiento de los públicos en Twitter, a pesar de que la información publicada por los diarios "confidenciales", menos afectados por la presión publicitaria de los grandes grupos y más permeables a esa pérdida de valores aludidos en la revisión de la literatura científica, es considerablemente más negativa. Ni en las informaciones ni en las redes sociales se centra el discurso en los clientes como posibles afectados, lo que corrobora la importancia de la marca corporativa sobre la de producto actualmente en las grandes organizaciones. En relación a la gestión de la comunicación de crisis llevada a cabo, la organización ha reforzado su reputación, escasa en el sector, con un ejercicio de reacción inmediata, transparencia y colaboración conforme a las directrices clásicas del estado de la cuestión. Sin embargo, la gran aportación del caso es la transferencia de la portavocía oficial a las redes sociales y a uno de sus directivos tras un escueto

comunicado oficial sobre la situación, con un discurso ágil, transparente y de colaboración, sin ocultar información que se había producido sobre un hecho del que todavía no se tenía el control y que, por otra parte, ya habían filtrado los empleados a través de sus redes sociales sin reparar en las consecuencias, convirtiéndose en la primera fuente de información para los medios y reforzando la falta de previsión y el carácter de urgencia en la respuesta que la literatura científica ha puesto de manifiesto de manera habitual en el inicio de la comunicación de crisis.

5. CONCLUSIONES

Una sólida reputación corporativa es el mejor intangible para afrontar una situación de crisis. Sin embargo, la reputación de las marcas corporativas en el sector de las telecomunicaciones es deficiente y ello implica una mayor vulnerabilidad ante el ciberataque WannaCry sufrido, que ha adquirido una notable dimensión informativa y ha captado el interés de los *stakeholders*.

Las crisis son imprevistas por su propia esencia y, el día antes de producirse, Telefónica anunciaba un incremento en su beneficio del 42% con respecto al año anterior y su marca de producto Movistar comunicaba a sus clientes el fin de los cargos adicionales por *roaming* en sus viajes por Europa. Sin embargo, estas informaciones positivas desaparecieron de la agenda de los medios en el momento en el que una crisis de tal magnitud afectaba a la Compañía.

A pesar de la discutida independencia de los medios en relación a los grandes anunciantes que financian su actividad, entre los que se encuentra Telefónica, ésta se erigió en protagonista de las informaciones sobre el ciberataque en España, destacando el enfoque neutro en el 69% de las informaciones publicadas en el primer intervalo, el de mayor magnitud, y el enfoque positivo en el 20% de los casos. A pesar del reducido número de informaciones negativas (11% en el primer intervalo y 8% en el segundo), mientras la prensa de información general opta mayoritariamente por el tono neutro, en los diarios "confidenciales" hay una mayor incidencia del tono negativo.

Los elementos positivos en la comunicación de crisis ejercida han sido la transparencia, una rápida solución al ciberataque y la colaboración mostrada con todos los agentes implicados. Entre los elementos negativos, destacan la debilidad mostrada por una gran empresa tecnológica y la actitud inicial del portavoz eludiendo sus responsabilidades profesionales, que posteriormente fueron aclaradas en un nuevo ejercicio de transparencia y que provocó que Telefónica desapareciese de la agenda de los medios rápidamente en relación con el ciberataque, con una contribución a la literatura científica sobre la comunicación de crisis basada en la ruptura de la portavocía oficial única y la gestión principal a través de las redes sociales de manera ágil, transparente y colaborativa.

Como consecuencia de todo ello, el resultado ha sido un sentimiento negativo similar en las informaciones publicadas en prensa (14%) con respecto al expresado por los públicos en Twitter (12%), mostrando una posición de mayor solidez con

respecto al resto de marcas corporativas del sector de las telecomunicaciones, especialmente con Vodafone, quien negó sufrir el ciberataque, a pesar de que todos los medios la contradecían aludiendo a fuentes internas, elevando su sentimiento negativo en Twitter hasta el 26,8%.

6. REFERENCIAS

Aaker, D.A. (1996). Measuring brand equity across products and markets. *California Management Review*, *38*(3), 102-120.

Aced, C. (2013). *Relaciones públicas 2.0. Cómo gestionar la comunicación corporativa en el entorno digital*. Barcelona: UOC.

Asociación de la Prensa de Madrid (2014). *Informe anual de la profesión periodística*. Madrid: Asociación de la Prensa de Madrid. Recuperado de http://www.apmadrid.es/wp-content/uploads/2009/02/Informe profesion_2014_def_baja.pdf

Barnes, B., & Cieply, M. (2014, 29 de noviembre). Intrusion on Sony Unit Prompts a Shutdown of Messaging Systems. *New York Times*. Recuperado de https://www.nytimes.com/2014/11/30/business/media/intrusion-on-sony-unit-prompts-a-shutdown-of-messaging-systems.html?action=click&contentCollection=Media&module=RelatedCoverage&region=EndOfArticle&pgtype=article

Barzilai-Nahon, K. (2008). Toward a theory of network gatekeeping: A framework for exploring information control. *Journal of the Association for Information Science and Technology*, *59*(9), 1493-1512. doi: https://doi.org/ 10.1002/asi.20857

Bel, G., & Trillas, F. (2005). Privatization, corporate control and regulatory reform: the case of Telefónica. *Telecommunications Policy*, *29*(1), 25-51. doi: https://doi.org/10.1016/j.telpol.2004.09.003

Benavides-Delgado, J. (2015). La publicidad, la marca y la ética en la construcción de los valores sociales. En J. Benavides, & A. Monfort (Coords.). *Comunicación y empresa responsable* (pp. 45-58). Pamplona: EUNSA.

Benavides-Delgado, J. (2005). Nuevas propuestas para el análisis del lenguaje en los medios, en *Questiones publicitarias*, *10*(1), 13-33. doi: https://doi.org/10.5565/rev/qp.154

Blythe, J. (2007). Advertising creatives and brand personality: a grounded theory perspective, en *Brand Management*, *14*(4), 284-294. doi: https://doi.org/ 10.1057/palgrave.bm.2550071

Bollero, D. (2008). Comunicación de crisis: El plan web en una crisis. *Revista de Comunicación*, 6, 44-48.

Bowen, S. A. (2008). Frames of terrorism provided by the news media and potential communication responses. En H. D. O'Hair *et al*. (eds.), Terrorism: Communication and rhetorical perspectives (pp. 337–358). New Jersey, NY: Hampton.

Cain, C. C. *et al*. (2017). Global ransomware attack: preparation is key. *Journal of Health Care Compliance*, *19*(3), 37-40.

Calvo-Calvo, A. (2010). *Historia de Telefónica: 1924-1975. Primeras décadas: tecnología, economía y política*. Barcelona: Ariel-Fundación Telefónica.

Calzada, J., & Estruch, A. (2011). Telefonía móvil en España: regulación y resultados. *Cuadernos Económicos de ICE*, 81, 39-70. Recuperado de http://www.revistasice.com/CachePDF/CICE_81_39-70__4D2E26DCC881483187872FE9A63999E2.pdf

Capriotti, P. (1999). *Planificación estratégica de la imagen corporativa*. Barcelona: Ariel.

Castillo-Esparcia, A., & Ponce, D. G. (2015). *Comunicación de Crisis 2.0*. Madrid: Fragua.

Castillo-Esparcia, A. (2010). *Introducción a las Relaciones Públicas*. Málaga: Instituto de Investigación en Relaciones Públicas.

Cervera-Fantoni, A. L. (2008). *Comunicación total*. Madrid: ESIC.

Clarke, R., & Youngsteing, T. (2017). Cyberattack on Britain's National Health Service - A wake-up call for modern medicine. *The New England Journal of Medicine*, *377*(5), 409-411. doi: https://doi.org/10.1056/NEJMp1706754

Clifton, J., Comin, F., & Díaz-Fuentes, D. (2011). From national monopoly to multinational corporation: How regulation shaped the road towards telecommunications internationalisation. *Business History*, *53*(5), 761-781. doi: https://doi.org/10.1080/00076791.2011.599588

Comscore (2017). *Informe Comscore MMX marzo 2017*.

Coombs, T. W. (2007). Attribution theory as a guide for post-crisis communication research. *Public Relations Review*, *33*(2), 135–139. doi: https://doi.org/10.1016/j.pubrev.2006.11.016

Coombs, W. T., & Holladay, S. J. (2012). The paracrisis: The challenges created by publicly managing crisis prevention. *Public Relations Review*, *38*(3), 408–415. doi: https://doi.org/10.1016/j.pubrev.2012.04.004

Coombs, W. T., & Holladay, S. J. (Eds.) (2010). *The handbook of crisis communication*. Massachusetts: Wiley-Blackwell. doi: https://doi.org/10.1002/9781444314885

Costa, J. (2004). *La imagen de marca. Un fenómeno social*. Barcelona: Paidós.

Delclós, T. (2011, 28 de abril). Sony tarda seis días en avisar de una colosal brecha de seguridad. *El País*. Recuperado de https://elpais.com/diario/2011/04/28/sociedad/1303941603_850215.html?rel=mas

Douglas, D. (2004). Grounded theory and the 'and' in entrepreneurship research. *Electronic Journal of Business Research Methods*, 2, 59-68.

Ehrenfeld, J. M. (2017). WannaCry, cybersecurity and health information technology: a time to act. *Journal of Medical Systems*, 41, 104. doi: https://doi.org/10.1007/s10916-017-0752-1

Ferguson, T. D., Deephouse, D. L., & Ferguson, W. L. (2000). Do strategic groups differ in reputation? *Strategic Management Journal*, *21*(12), 1195-1214. doi: https://doi.org/10.1002/1097-0266(200012)21:12<1195::AID-SMJ138>3.0.CO;2-R

Freeman, R. E. (1984). *Strategic Management: A stakeholder approach*. Massachusetts: Harpercollins.

Gaine-Ross, L. (2003). *CEO capital: a guide to building CEO reputation and company success*. New Jersey, NY: Wiley & Sons.

García-Ponce, D., & Smolak-Lozano, E. (2013). Comunicación de crisis: Compilación y revisión de teorías y taxonomías prácticas desde una perspectiva cualitativa. *Vivat Academia*, 124, 51-67. doi: https://doi.org/10.15178/va.2013.124.51-67

Glaser, B. G. (1992). *Basics of grounded theory analysis: emergence vs. forcing*. California, CA: Sociology Press.

Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: strategies for qualitative research*. New York, NY: Aldine.

Gómez-Mompart, J. L., Gutiérrez-Lozano, J. F., & Palau-Sampio, D. (2015). Los periodistas españoles y la pérdida de la calidad de la información: el juicio profesional. *Comunicar*, *23*(45), 143-150. doi: https://doi.org/10.3916/C45-2015-15

Grunig, L. A., Grunig, J. E., & Dozier, D. M. (2002). Excellent public relations and effective organizations. *A study of communication management in three countries*. Mahwah: Laurence Erlbaum Associates.

Grunig, J., & Hunt, T. (1984). *Dirección de Relaciones Públicas*. Madrid: Gestión 2000.

Hanggli, R., & Kriesi, H. (2012). Frame construction and frame promotion (strategic framing choices). *American Behavioral Scientist*, *56*(3), 260-278. doi: https://doi.org/10.1177/0002764211426325

Igartua, J. J., Otero, J. A., Muñiz, C., Cheng, L., & Gómez, J. (2007). *Efectos* cognitivos y afectivos de los encuadres noticiosos de la inmigración. En J. J. Igartua, & C. Muñiz (Eds.), *Medios de comunicación, inmigración y sociedad* (pp. 197-232). Salamanca: Universidad de Salamanca.

Jacobs, A., & Helft, M. (2010, 12 de enero). Google, citing attack, threatens to exit China. *New York Times*. Recuperado de http://www.nytimes.com/2010/01/13/world/asia/13beijing.html?ref=technology

Kantar MillwardBrown (2017). *Brandz Top 100 most valuable global brands 2017*. Recuperado de http://brandz.com/admin/uploads/files/BZ_Global_2017_Report.pdf

Kim, Y., & Park, H. (2017). Is there still a PR problem online? exploring the effects of different sources and crisis response strategies in online crisis communication via social media. *Corporate Reputation Review*, *20*(1), 76-104. Doi: https://doi.org/10.1057/s41299-017-0016-5

Krunal, A. G., & Kumar, P. D. (2017). Survey on ransomware: a new era of cyber attack. *International Journal of Computer Applications*, *168*(3), 38-41. doi: https://doi.org/10.5120/ijca2017914446

Locke, K. (2001). *Grounded theory 1984-1994*. California, CA: Sociology Press.

Luecke, R. (2005). *Gestión de crisis: Convertirlas en oportunidades*. Barcelona: Deusto.

Mourle, S., & Patil, M. (2017). A brief study of Wannacry threat: Ransomware attack 2017. *International Journal of Advance Research in Computer Science*, *8*(5), 1938-1940. doi: http://dx.doi.org/10.26483/ijarcs.v8i5.4021

OJD (2017). *Buscador de publicaciones. Promedio de difusión año 2016*. Recuperado de https://www.ojd.es/buscador.

Olins, W. (2009). *El libro de las marcas*. Barcelona: Océano.

Palacios-Marqués, D., & Devece-Caranana, C. A. (2013). Policies to support Corporate Social Responsibility: The case of Telefonica. *Human Resource Management*, *52*(1), 145-152. doi: https://doi.org/10.1002/hrm.21510

Recalde, M., & Gutiérrez-García, E. (2017). Dirección de comunicación y sector de telecomunicaciones: estudio de caso. *Doxa Comunicación*, 24, 77-101.

Recuperado de http://dspace.ceu.es/bitstream/10637/8453/1/Direccion_MonicaRecalde%26ElenaGutierrez_Doxa_2017.pdf

RepTrak (2017). *RepTrak España 2017*. Recuperado de https://www.reputationinstitute.com/CMSPages/GetAzureFile.aspx?path=~\media\media\documents\reptrak_espana_2017.pdf&hash=0f8b030d657a228a8d691f26769a0453ff71d6d604f8f7c92639f610aac0e6e3&ext=.pdf

RepTrak (2017a). 2017 *Global Reptrak 100*. Recuperado de https://www.reputationinstitute.com/CMSPages/GetAzureFile.aspx?path=~\media\media\documents\global_reptrak_2017.pdf&hash=7cde2bdcf25beb53df447672be60dbf7318a9d5e9ef7ace6b7648c23136a1d7c&ext=.pdf

Romero-Rodríguez, L. M., Torres-Toukoumidis, A. T., & Pérez-Rodríguez, A. (2017). Gestión comunicacional de crisis: Entre la agenda corporativa y mediática. Estudio de caso Volkswagen. *Revista Internacional de Relaciones Públicas*, *7*(13), 83-100. doi: https://doi.org/10.5783/RIRP-13-2017-06-83-100

Rubin, A. M. (1996). Usos y efectos de los media: una perspectiva uso-gratificación. En B. Jennings, & D. Zillman (Eds.), *Los efectos de los medios de comunicación. Investigaciones y teorías* (pp. 555-582). Barcelona: Paidós.

Sánchez-Revilla, M. A. (2017). *Estudio Infoadex de la inversión publicitaria en España 2017*. Madrid: Infoadex.

Shackelford, S. (2017). Exploring the 'Shared Responsibility' of cyber peace: Should Cybersecurity be a human right? *Bloomington: Indiana University Kelley School of Business Research,* Working Paper nº 17-55. Recuperado de https://ssrn.com/abstract=3005062

Shaw, E. (1979). Agenda-setting and mass communication theory. *Gazette International Journal for Mass Communication Studies*, *25*(2), 96-105.

Strauss, A. L., & Corbin, J. (1990). *Basics of qualitative research: grounded theory, procedures and techniques*. Newbury Park: Sage.

Telefónica (2016). *Elige todo*. Recuperado de http://www.eligetodo.com/

Telefónica (2017). *Incidencia ciberseguridad*. Recuperado de https://www.telefonica.com/es/web/sala-de-prensa/detalle-noticia/-/asset_publisher/O34kxJNk5Exu/content/incidencia-ciberseguridad?redirect=https%3A%2F%2Fwww.telefonica.com%2Fes%2Fweb%2Fsala-de-prensa%2Fnoticias

Van-der-Meer, T. G. L. A., Verhoeven, P., Beentjes, H. W. J., & Vliegenthart, R. (2017). Communication in times of crisis: The stakeholder relationship under

pressure. *Public Relations Review*, *43*(2), 426-440. doi: https://doi.org/10.1016/j.pubrev.2017.02.005

Villafañe, J. (2012). *La buena empresa. Propuesta para una teoría de la reputación corporativa*. Madrid: Pearson.

Villafañe, J. (2008). *La gestión profesional de la imagen corporativa*. Madrid: Pirámide.

Westphalen M. H., & Piñuel, J. L. (1993). *La Dirección de Comunicación. Prácticas profesionales. Diccionario técnico*. Madrid: Ediciones del Prado.

Wolf, M. (1994). *Los efectos sociales de los media*. Barcelona: Paidós.

Woods, C. L. (2016). When more than reputation is at risk: How two hospitals responded to Ebola. *Public Relations Review*, *42*(5), 893-902. doi: https://doi.org/10.1016/j.pubrev.2016.10.002

Woods, D., Agrafiotis, I., & Jason, R. C. (2017). Mapping the coverage of security controls in cyber insurance proposal forms. *Journal of Internet Services and Applications*, *8*(8), 1-13. https://doi.org/10.1186/s13174-017-0059-y

Xifra, J. (2005*). Planificación estratégica de las relaciones públicas*. Barcelona: Paidós.

AUTORES

Luis Mañas-Viniegra
Profesor asociado en el Departamento de Ciencias de la Comunicación Aplicada de la Universidad Complutense de Madrid. Doctor en Comunicación Audiovisual y Publicidad, es Licenciado en Periodismo y en Publicidad y Relaciones Públicas. Ha sido profesor en la Universidad Carlos III de Madrid, Universidad Rey Juan Carlos y Universidad de Valladolid. Es miembro del grupo de investigación Complutense de Gestión de las Marcas y Procesos de Comunicación, siendo actualmente IP del Proyecto de Innovación Docente "Mapa visual de orientación profesional para el Grado en Publicidad y Relaciones Públicas".
lmanas@ucm.es
Orcid ID: https://orcid.org/0000-0001-9129-5673

José Ignacio Niño González
Doctor en Publicidad y Relaciones Públicas por la Universidad Complutense de Madrid, y Máster en Administración de Empresas por el Instituto de Empresa de Madrid. Actualmente es Secretario de la Comisión Académica del Programa de Doctorado en Comunicación, Audiovisual, Publicidad y Relaciones Públicas que se imparte en la Facultad de Ciencias de la Información (UCM). En la actualidad trabaja en dos proyectos de investigación, uno de carácter tecnológico ligado a la Innovación

Docente y otro en el ámbito del consumo mediático multipantalla. Es Subdirector del laboratorio de Neuromarketing "NeurolabCenter" perteneciente al Departamento de Teorías y Análisis de la Comunicación de la Facultad de Ciencias de la Información (UCM).
josenino@ucm.es
Orcid ID: https://orcid.org/0000-0001-6940-2399

Luz Martínez Martínez
Doctora en Comunicación Audiovisual por la Universidad Complutense de Madrid. Profesora asociada en el Grado de Comunicación Audiovisual de la Universidad Rey Juan Carlos de Madrid e Investigadora de la Cátedra de Comunicación y Salud del departamento de Teorías y Análisis de la Comunicación (UCM). Actualmente está integrada como investigadora en el laboratorio de Neuromarketing "NeurolabCenter" perteneciente al Departamento de Teorías y Análisis de la Comunicación de la Facultad de Ciencias de la Información (UCM). Sus líneas de investigación se centran en el análisis de la creación y efectos psicosociales y culturales del discurso audiovisual en diferentes soportes, su aplicación en el edu-entretenimiento y el estudio de su eficacia a través de metodologías innovadoras, neuromarketing.
luz.martinez@urjc.es
Orcid ID: http://orcid.org/0000-0001-8582-724X