



¿QUÉ INFORMACIÓN RECIBEN LOS ACCIONISTAS DE LOS CIBERRIESGOS A LOS QUE ESTÁN EXPUESTAS LAS EMPRESAS COTIZADAS?

Un análisis comparado de las empresas del Ibex-35 y el Dow Jones en el periodo 2015-2017

Este trabajo ha contado con el patrocinio de

C L I F F O R D
C H A N C E

INFORMÁTICA

El Corte Inglés

AUTORES

Patricia Sánchez

*Directora Adjunta del Centro de Investigación
de Seguros de IE*
patricia.sanchez@ie.edu

José Esteves, PhD

*Profesor de Sistemas de Información y Decano Asociado
de los Programas MBA de IE Business School*
Jose.esteves@ie.edu

Laura Núñez, PhD

*Directora del Centro de Investigación
de Seguros y Profesora de Finanzas
de IE Business School*
Laura.nunez@ie.edu





TABLA DE CONTENIDOS

1. INTRODUCCIÓN	7
1.1 La información pública sobre riesgos -incluidos los cibernéticos- de las empresas cotizadas	8
1.1.1 Empresas cotizadas en el Ibex-35	8
1.1.2 Empresas cotizadas en el Dow Jones	10
1.2 Guía de la SEC para la elaboración del reporte de los riesgos de ciberseguridad.	10
2. METODOLOGÍA	13
2.1 Creación de la base de datos documental: recogida y pre-procesamiento de documentos.	14
2.2 Análisis cualitativo de contenido: estudio basado en conceptos mediante el uso del software de análisis semántico Leximancer.	17
2.3 Análisis cuantitativo de contenido: creación de un diccionario de palabras clave y extracción de la frecuencia de uso de las mismas con la ayuda de los softwares Text Analyst, KH Coder y SPSS.	18
3. RESULTADOS	21
3.1. Análisis cualitativo de contenidos: conceptualización del mensaje sobre ciberriesgos que las empresas del Ibex-35 y el DJ trasladan a los inversores o accionistas.	22
3.2 Análisis cuantitativo de contenido: terminología con la que las empresas del Ibex-35 y el DJ hablan de ciberseguridad a los inversores o accionistas.	26
3.2.1 Terminología empleada al hablar de ciberriesgos	26
3.2.2 El uso de los términos “ciber” y “seguridad de la información”	30
4. CONCLUSIONES Y RECOMENDACIONES	39
5. BIBLIOGRAFÍA	43
6. ANEXOS	45

”

Los accionistas tienen derecho a recibir información fiel de la situación de la empresa, incluidos los principales riesgos a los que se enfrenta, que deben contemplar aquellos relacionados con la ciberseguridad.

INTRODUCCIÓN

A día de hoy, la ciberseguridad es un problema que afecta prácticamente a todas las empresas. El Informe de Riesgos Globales 2019, elaborado por el Foro Económico Mundial, sitúa los ciberataques y el fraude masivo de datos en el top 5 de los riesgos globales con mayor probabilidad de ocurrencia¹.

Asimismo, el Barómetro de Riesgos de Allianz, que se publica anualmente, refleja desde hace años ya, la preocupación creciente de las empresas por el impacto que los ciberriesgos pueden tener en su negocio. Este informe recoge datos sobre la importancia que las empresas otorgan a diversos riesgos globales. En el informe de 2019², basado en 2415 encuestas a directivos de 86 países, los eventos de ciberseguridad se sitúan a la cabeza, junto con la interrupción del negocio, como las dos mayores amenazas según los encuestados. Con relación a la interrupción del negocio, los encuestados declaran que los incidentes de ciberseguridad son el detonante más temido.

En el caso de las empresas cotizadas, los accionistas tienen derecho a recibir información fiel de la situación de la empresa, la evolución de sus negocios, y la descripción de los principales riesgos e incertidumbres a los que se enfrenta, incluidos los relacionados con la ciberseguridad, con la razonable limitación de no hacer pública aquella información sensible que pudiera perjudicar a la propia empresa en el sentido de hacerla más vulnerable. Los supervisores de los mercados son los encargados de velar por el cumplimiento de estos principios que la regulación establece.

El **objetivo** del presente trabajo es analizar y comparar, en dos mercados bursátiles con diferente marco legal e institucional, el norteamericano y el español, **la información que reciben los accionistas sobre los ciberriesgos**, a los que están expuestas, las empresas cotizadas, la gestión que de los mismos hacen y el potencial impacto que pueden tener en sus negocios.

Para ello, se seleccionan dos de los índices representativos de dichos mercados, el **Ibex-35** y el **Dow Jones** y se examinan los documentos que las empresas que forman parte de dichos índices están obligadas a hacer públicos a sus accionistas, analizando específicamente aquellos apartados relacionados con la exposición a riesgos y gestión de los mismos.

¹ *The Global Risks Report (2019). World Economic Forum. 14th edition*

² *Allianz Risk Barometer 2019*

LA INFORMACIÓN PÚBLICA SOBRE RIESGOS -INCLUIDOS LOS CIBERNÉTICOS- DE LAS EMPRESAS COTIZADAS

1.1.1 Empresas cotizadas en el Ibex-35

Las empresas cotizadas en el mercado español tienen obligación de publicar anualmente, antes de la celebración de la junta de accionistas, el informe financiero auditado (que comprende el informe de gobierno corporativo, las cuentas anuales y las notas a las mismas, y el informe de gestión) de manera que los accionistas puedan analizar toda la información con anterioridad a la celebración de la junta de accionistas, y en su caso exigir explicaciones sobre las actuaciones llevadas a cabo por la empresa.

No es fácil delimitar en qué parte concreta de estos documentos publicados por las sociedades del Ibex-35 podemos encontrar información sobre los riesgos tecnológicos y/o ciberriesgos a los que están expuestas las compañías, su potencial impacto en el negocio, y la gestión de los mismos que llevan a cabo.

Por un lado, el informe anual de gobierno corporativo incluye dos secciones en su formulario de obligado cumplimiento sobre la gestión de riesgos: (i) la E "Sistemas de control y gestión del riesgo"; y (ii) y la F "Sistemas internos de control y gestión de riesgos en relación con el proceso de emisión de la información financiera". Los subapartados de ambas secciones están detallados en el Anexo A.

Por otro lado, la regulación contable también exige describir los riesgos a los que se enfrenta la empresa en las notas a las cuentas anuales, así como en el informe de gestión. El informe de gestión es el documento que acompaña a las cuentas para explicar la labor efectuada por la dirección de la empresa durante el ejercicio económico, pero no está normalizado, por lo que el contenido del mismo es muy dispar entre unas y otras empresas, y como Gonzalo Angulo y Garvey (2015) indican, su calidad no siempre es la deseada³.

La CNMV publicó durante el 2013 una guía para la elaboración del informe de gestión de las compañías cotizadas, que constituye un marco de referencia voluntario. La guía contiene un listado de riesgos que se pueden presentar, tanto operativos, como financieros. La guía enumera los siguientes riesgos operativos a modo de ejemplo: "accidentes o ataques dirigidos hacia la compañía o su personal; fallos de control interno; existencia de barreras de entrada; prohibiciones para operar; fraude o apropiación indebida; concentración de compras en un número limitado de proveedores; fallos y colapsos de los sistemas de información; riesgos relativos a nuevas inversiones; riesgo país; riesgos relativos a la reputación". La guía de la CNMV incluye sugerencias sobre el contenido deseable de información respecto a los riesgos que pueden afectar a las empresas, así como indicaciones sobre la descripción a hacer referente a la política de gestión y las estrategias de mitigación del impacto de los mismos, permitiendo que en otros documentos se haga referencia a esta parte de la información sobre riesgos. La guía comienza el apartado de "Riesgos e incertidumbre" con el siguiente texto: "Al redactar este apartado la entidad seleccionará, en el contexto de sus objetivos y estrategias, las principales fuentes de riesgo a las que se enfrente [esta mención incluye aquellos riesgos que puedan tener un impacto material], sean éstas de tipo operativo o financiero, para

³ Gonzalo Angulo y Garvey (2015). *Revista de Contabilidad y Dirección*, V 20, pp21-63. Pág. 23: "Es justo decir que hay honrosas excepciones, pero el panorama de la calidad conseguida en casi treinta años de informes de gestión es, cuando menos, sombrío para la generalidad de las sociedades que deben presentarlo".

explicar y valorar adecuadamente cuáles son, o pueden ser, sus efectos en la rentabilidad y la situación financiera”. Como curiosidad podemos comentar que en las 179 páginas que conforman la guía para elaborar el informe de gestión, la palabra ciber no aparece, ni para hablar de ciberriesgos ni para hablar de ciberseguridad, aunque como se observa en una de las citas anteriores, sí se contemplan riesgos o fallos de los sistemas de información.

En palabras de Gonzalo Angulo y Garvey (2015), “El informe de gestión cumpliría la misión de exponer la estrategia y la política, y si fuera posible la descripción de los resultados de estas a largo plazo, mientras que en las notas a las cuentas y el informe anual de gobierno corporativo se ofrecerían detalles más propios de la gestión llevada a cabo en el ejercicio”⁴. Por otro lado, los mismos autores señalan que el hecho de que el informe de gestión deba ser obligatoriamente suscrito por los administradores, haciéndoles responsables directos de su contenido, fomenta que en ocasiones se cubra la responsabilidad de informar, mediante la inclusión de referencias vagas y genéricas que pueden servir para cualquier entidad. Por ello, muchas empresas ofrecen información más amplia en informes adicionales que no tienen las implicaciones legales que tiene el informe de gestión, como son la memoria de sostenibilidad y el informe integrado, que generalmente describe el modelo de negocio de la empresa, incluyendo datos sobre riesgos. Pero ciertamente, la información dada en estos informes adicionales cuenta con una limitación fundamental, su falta de verificación por un organismo independiente ajeno a la empresa. Por ello, el presente estudio limita su análisis a los documentos contenidos en **el informe financiero anual auditado (cuentas y memoria de notas que las acompaña, informe de gestión e informe de gobierno corporativo)**.

Para hacernos una idea de lo inabarcable que puede resultar en ocasiones esta información para los accionistas, es suficiente señalar que el informe financiero de las compañías cotizadas tiene una extensión que en muchas ocasiones supera las 500 páginas. A la dificultad de la extensión le tenemos que añadir la falta de homogeneidad entre las distintas compañías en la presentación de la información del informe financiero: (i) Algunas incluyen en el documento, el informe de gobierno corporativo, mientras que otras no, haciendo referencia únicamente a la dirección web en la que este está disponible; (ii) Tampoco todas las empresas presentan el mismo detalle en el índice de los contenidos del informe financiero, incluso algunas no incluyen un índice; (iii) Las secciones en los informes de las compañías no son homogéneas, por ejemplo algunas incluyen en el informe de gestión un apartado sobre innovación y/o tecnología (BBVA apartado 8 del informe)⁵, mientras que otras no; (iv) La extensión con la que cada empresa trata el contenido de una misma sección es muy distinta, por ejemplo en la sección 4 de gestión de riesgos del informe de gestión, el BBVA incluye solo dos líneas referenciando dicha información a la nota 5 de las cuentas anuales en la que trata con mayor extensión los riesgos (43 páginas), mientras en el informe de gestión de la empresa ACCIONA, que tiene una extensión superior a las 50 páginas, gran parte de su contenido se refiere a la gestión de riesgos de la empresa.

⁴ Así lo reconoce también la guía publicada por la CNMV para elaborar el informe de gestión en la que comenta en su página 143 que las informaciones sobre “la gestión de los principales riesgos e incertidumbres se ofrecen tanto en las notas a las cuentas anuales como en el informe de gestión y en el informe anual de gobierno corporativo. El criterio para decidir qué parte de la información se incluye en una nota y qué otra se inserta en el informe de gestión será el de informar de la política, objetivos y estrategias en este último, mientras que los datos concretos de actividad son más propios de las notas o del informe anual de gobierno corporativo.”

⁵ Dentro del apartado 8 “Innovación y Tecnología” del informe de gestión 2017 del BBVA se incluye un sub-apartado “gestión de riesgos operativos y protección del cliente” con una extensión de una página en la que se aborda el tema de las amenazas relativas a los ciberriesgos y las actuaciones de la empresa relativas a la gestión de los mismos.

En este contexto de complejidad, hemos delimitado qué secciones o apartados, de los documentos que comprende el informe financiero, van a constituir la base de nuestro estudio sobre la información reportada por las empresas cotizadas de los ciberriesgos a los que están expuestas, a los siguientes:

1. Los apartados del informe de gobierno corporativo mencionados anteriormente: el relativo al punto E sobre sistemas de control y gestión del riesgo; y el referente al punto F sobre sistemas internos de control y gestión de riesgos en relación con el proceso de emisión de la información financiera.
2. Los apartados que hacen referencia a la gestión de riesgos, o a la innovación o tecnología, en el informe de gestión de las empresas.
3. Los apartados que hacen referencia a la gestión de riesgos en las notas que acompañan las cuentas anuales consolidadas.

1.1.2 EMPRESAS COTIZADAS EN EL DOW JONES

Con relación al mercado americano, esta complejidad de documentos se reduce sustancialmente, ya que es un único documento el exigido por el supervisor, la US Securities and Exchange Commission (la SEC) como documento de referencia para los inversores - el denominado **"Form 10-K"** - que incluye las cuentas auditadas de la compañía y una serie de contenidos explicativos sobre las mismas y sobre la evolución de la empresa y los riesgos a los que está expuesta. La SEC tiene la obligación de supervisar periódicamente la información presentada en este documento.

Uno de los apartados del informe 10-K hace referencia, en concreto, a los riesgos a los que la empresa está expuesta (Part I: Item 1.A Risk Factors). Es este apartado el que seleccionamos para analizar, en el caso de las empresas cotizadas del Dow Jones (DJ), la información que dichas empresas reportan sobre los ciberriesgos que pueden afectarles.

1.2

GUÍA DE LA SEC PARA LA ELABORACIÓN DEL REPORTE DE LOS RIESGOS DE CIBERSEGURIDAD

La SEC publicó en el año 2011 una guía para las empresas cotizadas, de carácter voluntario, con indicaciones sobre cómo reportar la información relativa a los riesgos de ciberseguridad, los ciber incidentes y su impacto en las operaciones⁶. Dicha guía, actualizada en el año 2018, justifica su publicación en base a la creciente dependencia tecnológica de todas las empresas, lo que las hace más vulnerables a los riesgos asociados con la ciberseguridad. Cabe destacar que en España no existe una guía parecida que indique a las empresas cómo deben reportar los riesgos de ciberseguridad, su gestión y su posible incidencia en el negocio.

⁶ <https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>

Algunas de las recomendaciones más destacadas, sobre la información que se debe dar a los accionistas de los ciber riesgos potenciales o sufridos por las empresas, que incluye la guía de la SEC en su versión de 2011 son las siguientes:

- Información sobre la naturaleza de los riesgos materiales y cómo cada riesgo afecta a la compañía.
- Aspectos del negocio que pueden dar lugar a riesgos materiales en ciberseguridad, así como sus potenciales costes y consecuencias.
- Funciones externalizadas afectadas y cómo los riesgos para estas funciones son abordados.
- Riesgos relativos a ciberriesgos que pueden permanecer inadvertidos por un periodo de tiempo prolongado.
- Cobertura de seguros relevante.
- Incidentes materiales ocurridos a nivel individual o agregado, incluyendo los costes y consecuencias.
- La propiedad robada.
- El efecto del ciberataque en las operaciones de la compañía, su liquidez y su condición financiera.
- Si futuras operaciones o la futura condición financiera se verán afectadas por el ataque.
- Información relacionada con los procedimientos legales afectados por el ciber incidente.

En 2018, la SEC actualizó la guía e incluyó recomendaciones adicionales, como por ejemplo:

- Establecer y mantener controles y procedimientos de comunicación apropiados y efectivos que permitan el reporte preciso y puntual de los eventos materiales, incluidos aquellos relacionados con la ciberseguridad.
- Reportar riesgos e incidentes de ciberseguridad que son importantes para los inversores y que pueden afectar a las acciones regulatorias llevadas a cabo por autoridades estatales/federales y autoridades externas a EEUU.
- Notificar puntualmente cualquier incidente de ciberseguridad.
- Corregir información previamente reportada que la compañía considere incorrecta u omitida.

Sin duda, en un campo novedoso como es el de los ciberriesgos y la ciberseguridad, en el que las experiencias previas son limitadas, y que está en continua evolución dada su relación con la tecnología, una guía como la de la SEC puede ser un instrumento de gran utilidad para las empresas, que en ocasiones todavía no han experimentado o se enfrentan por primera vez a episodios específicos de ciberataques y que deben anticipar qué mecanismos son los más adecuados para protegerse y cómo informar en este campo tan delicado a los accionistas.

”

Dada la ingente cantidad de información examinada en este estudio, más de 500 documentos de texto, la metodología empleada se ha basado en el análisis textual mediante el uso de softwares semánticos.

METODOLOGÍA

Dada la ingente cantidad de información que vamos a examinar en este estudio, a pesar del limitado número de empresas seleccionado, la metodología elegida está basada en el análisis textual mediante el empleo de softwares semánticos. A través de estos softwares se realizará un examen de la información sobre riesgos reportada por las empresas cotizadas del Ibex-35 y el Dow Jones en sus informes públicos.

Estudios previos han analizado ya mediante esta metodología la información recogida en los informes publicados para los accionistas. Por ejemplo, Narasimhan (2013) analiza los informes 10-K, mediante el análisis de contenido, para determinar el tono del discurso. Martin & Rice (2007)⁷, por otro lado, analizan los riesgos de cuatro empresas tecnológicas, reportados durante un periodo de 10 años, en los apartados 1A sobre factores de riesgos de los informes 10-K, apartado que se analiza también en este estudio.

No obstante, para poder aplicar estos softwares es necesario realizar previamente un trabajo importante de pre-procesamiento de los textos que son seleccionados como base del análisis, ya que es necesario realizar una conversión a texto de gráficos y tablas.

A continuación, describimos con más detalle la base de datos textual construida como plataforma de nuestros análisis, las características de los softwares empleados y el enfoque de los análisis.

¹ *The Global Risks Report (2019)*. World Economic Forum. 14th edition

² *Allianz Risk Barometer 2019*

2.1

CREACIÓN DE LA BASE DE DATOS DOCUMENTAL: RECOGIDA Y PRE-PROCESAMIENTO DE DOCUMENTOS

Para analizar la información sobre ciberriesgos que las empresas cotizadas en España y en Estados Unidos reportan a los accionistas, se han seleccionado las compañías cotizadas en dos de los índices más representativos de los mercados bursátiles de ambos países, el Ibex-35 y el Dow Jones (DJ). La tabla 1 muestra las empresas agrupadas por sectores, que están representadas en ambos índices. Los Anexos B.1 y B.2 presentan el listado de las empresas, junto a su capitalización bursátil, del Ibex-35 y del DJ respectivamente.

Con objeto de conformar la base de datos documental a analizar, se identifican y seleccionan, para las compañías de la muestra pertenecientes al Ibex-35, los informes financieros anuales auditados (**cuentas y memoria de notas que las acompaña, informe de gestión e informe de gobierno corporativo**) de los años 2015, 2016 y 2017 (315 documentos). Para las empresas del Dow Jones en nuestra muestra se selecciona **el informe 10-K** correspondiente a los mismos años, 2015, 2016 y 2017 (90 documentos).

De dichos documentos se localizan y seleccionan manualmente los apartados relacionados con riesgos, innovación y tecnología, que se han mencionado anteriormente con detalle, y se convierten a archivos TXT. Para ello es necesario realizar un ingente trabajo de búsqueda visual de los apartados, revisión de los mismos y conversión manual de texto, tablas y gráficos a formato TXT, para que dichos contenidos puedan posteriormente ser analizados. La conversión de las tablas y gráficos a formato TXT es especialmente intensiva en horas de trabajo, por lo que estas se convierten solo si su contenido es relevante con relación al objeto del trabajo. En la Tabla 2 se desglosa el total de documentos recogidos para cada empresa de la muestra.



TABLA 1. EMPRESAS ANALIZADAS POR SECTOR

SECTORES	IBEX-35 ⁹	DOW JONES
Petróleo y energía	Enagás Endesa Gas Natural (Naturgy) Iberdrola R.E.C. Repsol	Chevron Exxon
Materiales básicos, Industria y Construcción	Acciona Acerinox ACS ArcelorMittal Ferrovial Siemens Gamesa Técnicas Reunidas	3M Boeing Caterpillar Dow DuPont General Electric United Technologies
Bienes y Servicios de consumo	Abertis Aena Dia Grifols IAG Inditex Mediaset Melia Viscofan	CocaCola Walt Disney The Home Depot Johnson & Johnson McDonalds Merck Nike Pfizer Procter & Gamble United Health Gr. Walmart
Servicios financieros	Banco Sabadell Bankia Bankinter BBVA Caixabank Mapfre Santander	American Express Goldman Sachs JP Morgan Travelers Visa
Tecnología y telecomunicaciones	Amadeus Cellnex Indra Telefonica	Apple Cisco IBM Intel Microsoft Verizon
Servicios inmobiliarios	Inmobiliaria Colonial Merlin Properties	

⁹ Empresas pertenecientes al IBEX-35 en 2017

TABLA 2. DOCUMENTOS SELECCIONADOS DE LAS EMPRESAS OBJETO DE ANÁLISIS

DOW JONES¹⁰	
Ítem 1.A del informe 10-K	Año 2015: 31 archivos Año 2016: 31 archivos Año 2017: 31 archivos
Total: 93 archivos de texto	
IBEX-35¹¹	
Apartado E del Informe Anual de Gobierno Corporativo:	Año 2015: 34 archivos Año 2016: 34 archivos Año 2017: 34 archivos
Apartado F del Informe Anual de Gobierno Corporativo: <i>"Sistemas internos de control y gestión de riesgos en relación con el proceso de emisión de la información financiera (SCIF)"</i>	Año 2015: 34 archivos Año 2016: 34 archivos Año 2017: 34 archivos
Nota de las Cuentas Anuales Consolidadas relativa a los riesgos de la empresa.	Año 2015: 34 archivos Año 2016: 34 archivos Año 2017: 34 archivos
Sección del Informe de Gestión Consolidado, relativa a los riesgos de la empresa, o a la innovación y tecnología.	Año 2015: 34 archivos Año 2016: 34 archivos Año 2017: 34 archivos
Total: 408 archivos de texto	
Total de documentos analizados: 501 archivos de texto	

¹⁰ Las compañías Dow Chemical y DuPont se fusionaron en 2017, creando Dow DuPont, empresa que cotiza actualmente en el Dow Jones. Para el presente trabajo se han analizado los textos de las dos empresas por separado, haciendo un total de 31 archivos para las 30 empresas del Dow Jones.

¹¹ Se excluye de los análisis la empresa Arcelormittal debido a no encontrarse disponibles los archivos correspondientes en la página web de la Comisión Nacional del Mercado de Valores (<https://www.cnmv.es/portal/home.aspx>).

2.2

ANÁLISIS CUALITATIVO DEL CONTENIDO: ESTUDIO BASADO EN CONCEPTOS MEDIANTE EL USO DEL SOFTWARE DE ANÁLISIS SEMÁNTICO LEXIMANCER

Leximancer es un software de análisis y minería de textos (*text mining*) que utiliza técnicas de *machine learning*, entre ellas la teoría estadística Bayesiana y estadísticas de co-ocurrencia de palabras. El programa realiza, de forma automática, el análisis de contenido de una gran cantidad de textos, con la ventaja de eliminar la subjetividad de los análisis, al basarse directamente en los textos y no en la visión de los investigadores. Para realizar el análisis Leximancer usa “bloques de texto” como unidades de análisis. En este estudio se utilizó la configuración estándar de dos oraciones por bloque. El proceso de análisis de Leximancer se describe en profundidad en Smith y Humphreys (2006), conjuntamente con su validez y pruebas de fiabilidad. Para analizar los documentos recogidos en este estudio, utilizamos el software Leximancer (Versión 4.0, Leximancer Pty Ltd., Brisbane, Australia).

Leximancer utiliza la frecuencia de palabras y los datos de co-ocurrencia con otras palabras para identificar familias de términos que tienden a usarse juntos en el texto y a partir de estas, y mediante una serie de algoritmos, identifica los conceptos más relevantes en el texto. De esta manera, tal y como se describe en la guía de uso del software, los conceptos son “conjuntos de palabras que generalmente viajan juntas a lo largo del texto” (Leximancer User Guide, 2018). Para poder desarrollar este análisis es necesario eliminar palabras altamente frecuentes en los textos, pero de escaso valor semántico, como “y”, “o”, “sí”, “no”, etc. Estas palabras están incluidas en el propio software en una lista denominada “stop list” que el investigador puede modificar añadiendo palabras que considere poco relevantes.

Debido a que el número de conceptos que se obtiene de un texto suele ser grande, estos se agrupan por proximidad en grupos, que son denominados tópicos. Es decir, los conceptos que se atraen y se relacionan, se agrupan en tópicos. Los tópicos adquieren su nombre del concepto más prominente en el grupo de conceptos interconectados. Para cada tópico, el software calcula el número de “hits”, que se refiere al número de extractos de texto asociados a cada tópico.

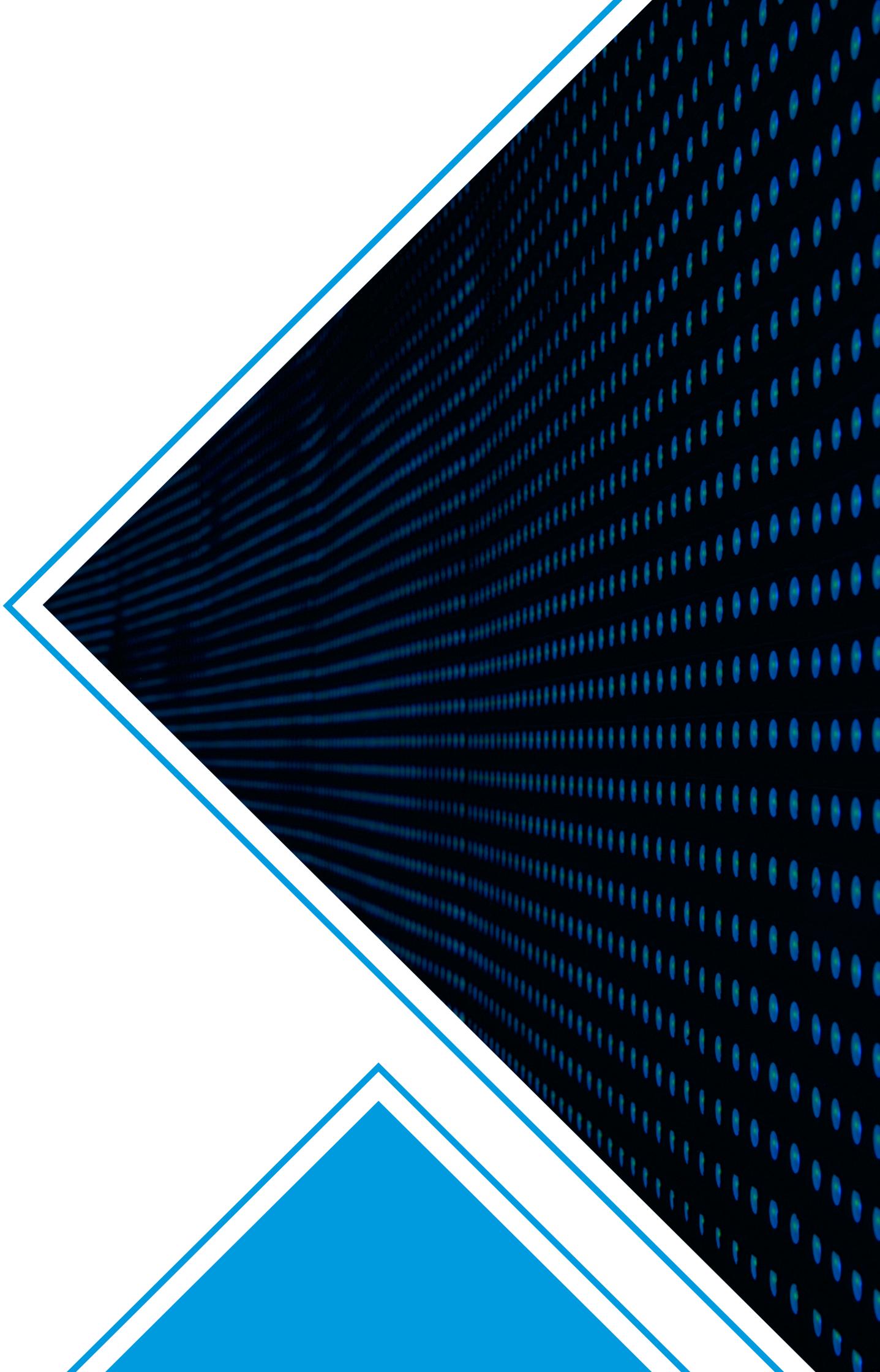
Aplicando este software de análisis semántico, **Leximancer**, a los documentos de la base de datos textual construida, se llevará a cabo una recuperación de conceptos semánticos de (1) los riesgos de negocio reportados por las empresas de ambos índices, y (2) de los riesgos de ciberseguridad que mencionan, así como de los aspectos de los mismos de los que hablan. Con el objetivo de poder comparar los resultados obtenidos para las empresas del Dow Jones y del Ibex-35, se analizará en esta fase únicamente el apartado 1.A de los Informes 10-K de las empresas del Dow Jones, y el apartado E de los Informes de Gobierno Corporativo de las empresas del Ibex-35. El resto de los documentos recogidos para el Ibex-35 se excluyen de este bloque de análisis, si bien sí serán empleados en el examen cuantitativo posterior de textos.

2.3

ANÁLISIS CUANTITATIVO DEL CONTENIDO: CREACIÓN DE UN DICCIONARIO DE PALABRAS CLAVE Y EXTRACCIÓN DE LA FRECUENCIA DE USO DE LAS MISMAS CON LA AYUDA DE LOS SOFTWARES TEXT ANALYST, KH CODER Y SPSS

El primer paso para abordar el análisis cuantitativo de los contenidos de los documentos que conforman la base de datos es crear un diccionario de términos relacionados con ciberseguridad y ciberriesgos. Para ello se utiliza el software Text Analyst, que es un programa que utiliza algoritmos matemáticos basados en redes neuronales para determinar la importancia relativa de los conceptos, analizando sus conexiones con otros conceptos del texto. De esta forma, el software analiza los textos determinando qué conceptos (ya sean palabras o combinaciones de palabras) son las más importantes en el contexto del texto investigado (Megaputer Intelligence, 2000). Con este software se analizan todos los textos recogidos referentes a las compañías cotizadas en el Dow Jones y se extrae un listado de las palabras más usadas. A continuación, se seleccionaron aquellas palabras que tienen relación con los riesgos cibernéticos para crear un diccionario. La selección de las palabras se hizo en base al criterio de dos miembros del equipo de investigación. Dicho diccionario se tradujo al español para poder emplearlo también en el análisis de los informes recopilados para las empresas del Ibex-35.

El segundo paso es crear una base de datos que recoja las palabras clave, contempladas en el diccionario de riesgos cibernéticos, de los documentos de las diferentes empresas de la muestra en cada uno de los tres años estudiados. En este bloque de análisis se incluyen todos los archivos recopilados para el Dow Jones (Item 1A del Informe 10K) y para el Ibex-35 (los dos apartados del Informe de Gobierno Corporativo, y los apartados correspondientes de las Cuentas Anuales Consolidadas y del Informe de Gestión Consolidado). Para recoger los términos cibernéticos que contempla el diccionario creado de los informes corporativos se emplea el software **KH Coder**. Se confecciona de esta manera una base de datos con dichos términos. Una vez creada la base de datos, se realizan análisis de frecuencias y se extraen estadísticos descriptivos (mínimo, máximo, suma y media) de las palabras clave de interés mediante el software **IBM SPSS Statistics v.20**.



”

El mensaje que las empresas del Dow Jones trasladan a los inversores se refiere a los riesgos específicos que tienen que gestionar y su posible impacto en los stakeholders, mientras que las del Ibex-35 lo enfocan a las medidas de seguridad, especialmente a la cobertura con seguros.

RESULTADOS

Siguiendo la metodología comentada, analizamos los documentos de la base de datos textual que se ha elaborado a partir de los informes financieros públicos elaborados por las compañías cotizadas en el Dow Jones y el Ibex-35, y a través de los cuales se informa a los accionistas o inversores de la actividad de la empresa durante el ejercicio económico y de los planes a futuro.

Primero, en el apartado 3.1, exponemos los resultados del examen cualitativo realizado, en el que se analizan los conceptos y tópicos más empleados por

las empresas en el mensaje que envían a los accionistas, que en definitiva son los propietarios de las empresas cotizadas, sobre los riesgos que les afectan y en particular examinamos qué importancia relativa dan en dicho mensaje a los ciberriesgos, y qué aspectos de los mismos les preocupan más.

A continuación, en el apartado 3.2, presentamos los resultados obtenidos en el análisis cuantitativo, a través del cual examinamos el vocabulario con el que expresan el mensaje, relativo a los ciberriesgos y la gestión que de los mismos hacen, que trasladan a los accionistas. Mientras que el primer análisis enmarca la comunicación que las empresas hacen de los ciberriesgos en el conjunto de riesgos que mencionan en sus informes financieros, proporcionando una visión relativa del grado de importancia que dan a los mismos, el segundo análisis nos permite ahondar en el vocabulario específico que se emplea al hablar de ciberriesgos, ofreciendo una medida absoluta de la frecuencia de uso de dicho vocabulario.

3.1

ANÁLISIS CUALITATIVO DE CONTENIDOS: CONCEPTUALIZACIÓN DEL MENSAJE SOBRE CIBERRIESGOS QUE LAS EMPRESAS DEL IBEX-35 Y EL DJ TRASLADAN A LOS ACCIONISTAS

¿Cuáles son los riesgos a los que se enfrentan las empresas? ¿Se encuentran los ciberriesgos entre los riesgos de negocio que las empresas reconocen afrontar? Y si es así, ¿qué faceta o aspecto de los ciberriesgos les preocupa más? Para tratar de responder a estas preguntas, analizamos el contenido de los mensajes que las empresas cotizadas envían a sus accionistas utilizando el software de análisis semántico Leximancer. Dado el mayor número de informes de los que se dispone para las empresas del Ibex-35, con el objetivo de que sean comparables los resultados para ambos mercados, el americano y el español, este análisis comparativo se limita en las empresas del Ibex-35 al informe anual de gobierno corporativo, que es el documento más apropiado para reportar la gestión realizada durante el ejercicio económico, y en concreto al apartado E “Sistemas de control y gestión del riesgo”, cuyo contenido se compara con el del apartado 1.A. “Risk factors” de los informes 10-K de las empresas del Dow Jones.

Primero se examina qué importancia relativa dan las empresas a los ciberriesgos dentro de la información sobre “riesgos de negocio” que trasladan a los inversores, y posteriormente se investiga sobre qué aspectos de la “ciberseguridad” les alertan.

Análisis de Riesgos de Negocio.

El conjunto de empresas cotizadas en el DJ centra su mensaje sobre “riesgos de negocio” durante el periodo analizado 2015-2017, en torno a cuatro tópicos: producción/productos, financiero/mercados, ciber y regulación. Curiosamente, las empresas del Ibex-35 ponen el foco en temas muy diferentes al hablar a sus accionistas de los principales riesgos que pueden afectarles, centrándose sobre todo en dos tópicos: control/gestión/administración, y actividad/operaciones. La tabla 3 muestra los conceptos con los que las empresas relacionan dichos tópicos



TABLA 3. TÓPICOS SOBRE RIESGOS DE NEGOCIO Y CONCEPTOS CON LOS QUE ESTOS SE RELACIONAN, MÁS MENCIONADOS POR LAS EMPRESAS DEL DJ Y EL IBEX-35 EN LA INFORMACIÓN TRASLADADA A LOS ACCIONISTAS

TOPICOS	HITS*	CONCEPTOS ASOCIADOS
Dow Jones		
Producción/productos	6090	servicios / clientes / desarrollo / acceso / uso
Financiero/mercados	5203	condiciones económicas / precios / exterior / ventas
Ciber	3744	Información / seguridad/ tecnología / datos / proveedores / uso / terceros / servicios / amenazas / ataques / derechos de propiedad / propiedad intelectual
Regulación	3647	leyes / requisitos / normativa / gubernamental / acciones
Ibex-35		
Control / gestión	4564	sistemas / funciones / información / políticas / auditoria / cumplimiento / procesos
Actividad/operaciones	1755	desarrollo / exposición / sector

* El número de "hits" se refiere al número de extractos de texto asociados a cada tópico.

Como puede observarse, al menos en lo que se refiere a los informes de gobierno corporativo, las empresas españolas no mencionan mucho los ciberriesgos al hablar de la gestión de riesgos realizada durante el ejercicio económico, a diferencia de las americanas que sí lo hacen. De hecho, las empresas del DJ hablan de los ciberriesgos o la ciberseguridad asociándolos con multitud de conceptos, desde información y datos, hasta tecnología, pasando por ataques y amenazas, o por derechos de propiedad y propiedad intelectual, o hasta por proveedores y servicios.

Si ciertamente el informe normalizado de gobierno corporativo no incluye ningún sub-apartado específico destinado a informar sobre ciberriesgos, sí solicita que las empresas informen de los "planes de respuesta y supervisión para los principales riesgos de la entidad", por lo que estos, los ciberriesgos, dada la relevancia de los mismos en el contexto actual, deberían ser tratados en dicho apartado del informe. Quizá el hecho de que el apartado sobre sistemas de control y gestión del riesgo del informe de gobierno corporativo recuerde continuamente a las empresas que deben incluir también los riesgos de materia fiscal, esté sesgando la percepción de que este apartado debe contemplar sobre todo riesgos de índole financiera y fiscal. De hecho, el tercer tópico en prevalencia en las empresas del Ibex-35 cuando hablan de riesgos es el de "fiscalidad", no incluido en la tabla 3 por el sesgo que el propio formato oficial con el que las empresas tienen que elaborar el apartado E induce sobre el mismo. El Anexo A incluye el desglose de puntos que el apartado E exige cumplimentar a las empresas sobre riesgos.

Análisis de Riesgos de Ciberseguridad

A continuación pasamos a examinar los conceptos que cubren las empresas al informar a los accionistas sobre “ciberseguridad” o “seguridad”. Añadimos la palabra “seguridad” dado que en el análisis anterior hemos detectado el escaso uso, si es que se hace alguno, de la palabra “ciber” por parte de las compañías del Ibex-35 en el apartado E “sistemas de control y gestión del riesgo” del informe de gobierno corporativo. La tabla 4 muestra los conceptos con los que las empresas a ambos lados del atlántico relacionan los tópicos de ciberseguridad o seguridad de la información agrupados en torno a diferentes temas. Podemos observar por tanto a partir de dicha tabla cuáles son los temas con los que las empresas relacionan la ciberseguridad en sus informes y analizar las notables diferencias que encontramos en las empresas del DJ frente a las del Ibex-35.

TABLA 4. CONCEPTOS SOBRE “CIBERSEGURIDAD O SEGURIDAD DE LA INFORMACIÓN” MÁS MENCIONADOS POR LAS EMPRESAS DEL DJ Y EL IBEX-35 EN LA INFORMACIÓN TRASLADADA A LOS ACCIONISTAS

EMPRESAS	CONCEPTOS ASOCIADOS
Dow Jones	riesgos / amenazas / ataques información / datos / acceso servicios / producción – productos / uso-procesos tecnología / desarrollo clientes / proveedores / terceras partes / empleados / compañía regulación / leyes / derecho de propiedad intelectual/ litigios financiera /requerimientos / pagos
Ibex-35	riesgos Información / sistemas servicios / gestión- procesos / negocio / operaciones / actividad / mercados seguros clientes / consejo administración normativa / fiscalidad / auditoria / control financiera / crédito / tipo de cambio / moneda

El primer concepto que muestra la tabla 4 relacionado con la ciberseguridad sería la propia mención a los “riesgos”, tanto en las empresas cotizadas en el DJ como en el Ibex-35. Sin embargo, una diferencia notable entre ambos grupos de empresas es que las del DJ introducen en su vocabulario términos adicionales al de “riesgo”, que es bastante general, y que tienen una connotación más grave y específica, tales como “amenazas” y “ataques”. Estos términos son incorporados por las mismas solo en 2017, no apareciendo ni en 2016 ni en 2015, mostrando por tanto una evolución en el lenguaje que no han experimentado todavía las empresas españolas.

Un segundo grupo de conceptos con el que se relaciona la ciberseguridad es el relativo a la información y los datos. En este caso la diferencia entre el DJ y el Ibex-35, es que el primero pone más énfasis en el “acceso”, mientras que el segundo lo hace en “los sistemas” al mencionar estos riesgos a los accionistas.



El mensaje sobre ciberseguridad también está relacionado en ambos conjuntos de compañías con los servicios, productos, procesos y actividad. Sin embargo, el foco de las empresas del DJ se concentra sobre todo en servicios y productos, mientras que las compañías del Ibex-35 reflejan menor preocupación por los outputs y mayor por variables como los mercados, las operaciones, o los negocios, que de alguna manera están menos controladas por la propia compañía que su producción.

Sorprende en gran medida, que en las compañías españolas no aparezca el concepto de “tecnología” entre los ligados a la seguridad. Ni tan siquiera aparece el de desarrollo. De la misma manera sorprende enormemente que en las empresas del DJ no aparezca el concepto de “seguros” ligado a la ciberseguridad, concepto que sí mencionan las empresas del Ibex-35.

Otra diferencia notable entre las empresas de ambos mercados es la referencia que hacen a los *stakeholders* cuando hablan de ciberseguridad. Las americanas mencionan a un número amplio de los mismos, clientes, proveedores, terceras partes, y empleados, y también a la propia compañía, mientras que las españolas, no mencionan ni proveedores, ni terceras partes, ni empleados, *stakeholders* que tienen una importancia fundamental en la ciberseguridad de las compañías.

Es también interesante la divergencia entre ambos grupos de empresas en su mensaje sobre la ciberseguridad relacionada con la regulación: mientras en España el foco se pone en los procesos de control, auditoría y fiscalidad, en EEUU el enfoque se centra en los derechos de propiedad intelectual y los litigios, probablemente derivados de estos riesgos.

Finalmente, ambos grupos de empresas relacionan la seguridad con la función financiera, pagos, requerimientos (las del DJ), créditos, moneda y tipo de cambio (las del Ibex-35).

Nuestra percepción es que el mensaje que las empresas trasladan a los inversores en el mercado americano (basado en un lenguaje más consciente de los riesgos “amenazas y ataques”, más centrado en sus outputs concretos “productos y servicios” que en los mercados, o actividades, ligado a la “tecnología”, implicando a todos los *stakeholders*, incluidos “proveedores, empleados y terceras partes”, y mostrando una preocupación por “la propiedad intelectual”) es más específico y adecuado que el usado por las empresas españolas representadas en el Ibex-35, que construyen su comunicación con términos menos específicos, sin mencionar apenas a los *stakeholders*, y refiriéndose en mayor medida a seguros externos que puedan mitigar los efectos de posibles eventos de seguridad.

3.2

ANÁLISIS CUANTITATIVO DEL CONTENIDO: TERMINOLOGÍA CON LA QUE LAS EMPRESAS DEL IBEX-35 Y EL DJ HABLAN DE CIBERSEGURIDAD A LOS ACCIONISTAS

Tras el análisis anterior sobre el marco conceptual en el que las mayores empresas españolas y americanas cotizadas en sus respectivos mercados encuadran su comunicación a los accionistas sobre los ciberriesgos a los que están expuestas y cómo los gestionan, pasamos ahora a realizar un examen cuantitativo de los contenidos de sus mensajes. En este apartado se examina el conjunto de secciones seleccionadas de todos los documentos que conforman la base de datos textual - informe 10-K de las empresas del DJ e informe financiero (anotaciones a las cuentas, informe de gestión e informe de gobierno corporativo) de las empresas del Ibex-35 - para realizar un estudio cuantitativo de la terminología empleada al hablar de ciberriesgos.

3.2.1 TERMINOLOGÍA EMPLEADA AL HABLAR DE CIBERRIESGOS

Como primer paso de este análisis elaboramos un diccionario de los términos usados por las empresas al hablar de ciberseguridad. La lista de los términos más empleados en los documentos elaborados por las compañías del Dow Jones y del Ibex-35 para cada uno de los tres años estudiados al hablar de ciberseguridad, se presenta en las tablas 5 y 6 respectivamente. Para cada palabra se indica la frecuencia (Frec.) de aparición en el conjunto de los textos analizados. Por tanto, las frecuencias hacen referencia al número de veces que aparecen dichas palabras en los documentos recogidos para el total de las empresas de cada índice bursátil de la muestra.

Respecto a las empresas del Dow Jones (tabla 5) es interesante observar cómo los primeros siete términos empleados por el conjunto de empresas permanecen invariables en el ranking durante los tres años examinados, siendo las frecuencias muy similares en los tres años. Dichos términos son por orden de mayor a menor prevalencia “sistemas” e “información”, con frecuencias siempre superiores a las 300 apariciones (lo que no sorprende al ser términos muy generales), seguidos de “reputación”, “datos” y “propiedad intelectual” con frecuencias en torno de las 200-250 apariciones, y finalmente de “seguridad” y “software” con frecuencias en torno a 150 apariciones el primero y en torno a 100 el segundo. Llama la atención la aparición del término “reputación” tantas veces y además su evolución creciente en el tiempo, con 228, 250 y 258 apariciones en 2015, 2016 y 2017 respectivamente. Ello indica que existe una preocupación importante en las empresas del DJ por el riesgo de reputación, o al menos eso es lo que están trasladando a sus accionistas. El avance del término “datos” desde las 186 apariciones en 2015 a las casi 240 del 2017 es también notable, reflejando bien cierta inquietud hacia la protección o pérdida de los datos, bien las mayores exigencias de las regulaciones que se han ido implantando durante estos años con relación a la protección de datos. También destaca la atención que ponen las empresas americanas en los riesgos relativos a la “propiedad intelectual”, muy superior por ejemplo a la referida a la “privacidad”. Otro aspecto destacable es el fuerte incremento en la frecuencia de uso del término “ciber ataque” cuya aparición en los informes 10-K crece un 60% a lo largo de los tres años analizados, pasando de 55 (año 2015) a 88 (año 2017) apariciones, situándose en 2017 como el octavo concepto más empleado al hablar de ciberriesgos por las empresas del DJ.

TABLA 5. FRECUENCIA DE USO DE LAS PALABRAS CLAVE SOBRE CIBERSEGURIDAD EN LAS EMPRESAS DEL DOW JONES

2015	Frec.	2015	Frec.	2015	Frec.
System	454	System	451	System	462
Information	305	Information	316	Information	333
Reputation	228	Reputation	250	Reputation	258
Datum/data	186	Datum/data	200	Datum/data	239
Intellectual property	184	Intellectual property	199	Intellectual property	195
Security	149	Security	165	Security	160
Software	86	Software	88	Software	103
Privacy	62	Cyber attack(s)	66	Cyber attack(s)	88
Cyber attack(s)	55	Breach	59	Privacy	65
Computer	54	Privacy	56	Breach	60
Breach	49	Computer	46	Information technology system	50
Information technology system	42	Information technology system	44	Cyber security	50
Security breach	40	Security breach	39	Computer	47
Hardware	35	Hardware	35	Confidential information	41
Confidential information	31	Cyber security	33	Data protection	41
Personal information	30	Data protection	32	Security breach	38
Cyber security	28	Confidential information	31	Hardware	37
Data protection	24	Information security	26	Personal information	33
Information security	22	Personal information	23	Update	23
Hacker	21	Confidentiality	19	Personal datum/data	23
Update	19	Personal datum/data	18	Data security	23
Data breach	18	Hacker	18	Confidentiality	19
Confidentiality	17	Update	17	Hacker	18
Personal datum/data	16	Data security	16	Information security	17

TABLA 6. FRECUENCIA DE USO DE LAS PALABRAS CLAVE SOBRE CIBERSEGURIDAD EN LAS EMPRESAS DEL IBEX-35

2015	Frec.	2015	Frec.	2015	Frec.
Información	3407	Información	3561	Información	3606
Sistema	2126	Sistema	2156	Sistema	2184
Seguridad	457	Seguridad	474	Seguridad	526
Reputación	296	Reputación	317	Reputación	351
Datos	254	Datos	266	Datos	264
Seguridad de la información	85	Seguridad de la información	112	Seguridad de la información	111
Confidencialidad	80	Confidencialidad	77	Confidencialidad	78
Actualizar	68	Actualizar	77	Actualizar	72
Ciber seguridad	45	Ciber seguridad	56	Ciber seguridad	63
Protección de datos	33	Sistema informático	35	Protección de datos	38
Sistema informático	29	Protección de datos	35	Sistema informático	34
Software	28	Software	29	Software	32
Ciber ataque	18	Ciber ataque	24	Ciber ataque	30
Ordenador	13	Privacidad	21	Ciber riesgo	19
Datos personales	13	Hardware	14	Privacidad	17
Ciber	11	Ordenador	12	Ordenador	14
Privacidad	10	Ciber riesgo	12	Hardware	12
Incidente(s) de seguridad	9	Contraseña	10	Incidente(s) de seguridad	12
Hardware	8	Incidente(s) de seguridad	10	Contraseña	10
Ciber riesgo	7	Datos personales	9	Ciber crimen	6
Contraseña	7	Ciber	4	Datos personales	6
Información confidencial	4	Intrusión/ intromisión	4	Datos confidenciales	5
Filtración	3	Información sensible	4	Ciber	5
Ciber crimen	3	Ciber crimen	3	Información confidencial	4
Ciber incidente	3	Ciber incidente	3	Intrusión	4

En el caso de las compañías del Ibex-35 (tabla 6) las siete palabras usadas con más frecuencia al hablar de ciberriesgos permanecen también invariables en el ranking a lo largo del periodo analizado. A la cabeza se sitúan los mismos términos generales que aparecían en las empresas del DJ, “información” y “sistemas”, al que se añade el de “seguridad”. Es interesante observar cómo de nuevo los términos “reputación” y “datos” adquieren protagonismo, al aparecer en la cuarta y quinta posición con una evolución creciente. Así pues, parece que estas preocupaciones no son exclusivas de las empresas del DJ, sino que son compartidas por las compañías españolas que forman parte del Ibex-35. En efecto, si comparamos la información reportada por las empresas españolas con la reportada por las empresas del Dow Jones (tablas 6 y 5) vemos que hay muchas similitudes en cuanto a las palabras que son empleadas con más frecuencia para hablar de ciberriesgos. Pero también hay algunas discrepancias notables entre ellas que merecen un análisis.

Una de estas diferencias es el uso por parte de las cotizadas del Ibex-35, de la palabra “confidencialidad” que aparece en séptima posición en el ranking, con una frecuencia en torno a 80, mientras que en las empresas del DJ este término no es demasiado prevalente. De hecho, las empresas españolas utilizan en mayor medida el término “confidencialidad” que “privacidad”, mientras las compañías americanas hacen un mayor uso del término “privacidad” que del término “confidencialidad” (ver palabras en azul en tablas 5 y 6). Hay un matiz importante que diferencia ambos términos, dado que la confidencialidad se refiere principalmente a información sensible para la empresa que debe ser protegida de accesos no autorizados, mientras que la privacidad hace referencia a la información relativa a las personas, a la que por motivo de su operativa las empresas pueden tener acceso (bancos, aseguradoras de salud, etc.) y cuyo secreto constituye un derecho reconocido y legislado. Así pues, las empresas españolas trasladan a sus accionistas una gran preocupación por la confidencialidad, mientras que las americanas lo hacen por la privacidad.

Otra diferencia se refiere al uso del término “propiedad intelectual” con una frecuencia de aparición cercana a 200 menciones y el quinto puesto en el ranking de las empresas del DJ, y que ni siquiera aparece en el vocabulario empleado por las empresas del Ibex-35 al hablar de ciberriesgos. Interpretamos este hecho como una cuestión cultural que refleja la mayor importancia que en el mundo anglosajón se le da a la propiedad intelectual, con respecto a nuestro país, en el que no existe dicha cultura y por tanto las empresas no hablan de ello. Quizá el uso de este término de “propiedad intelectual” está supliendo de alguna forma el uso que no hacen las empresas del DJ, tal y como hemos comentado en el párrafo anterior, del término confidencialidad con el que guarda cierta relación.

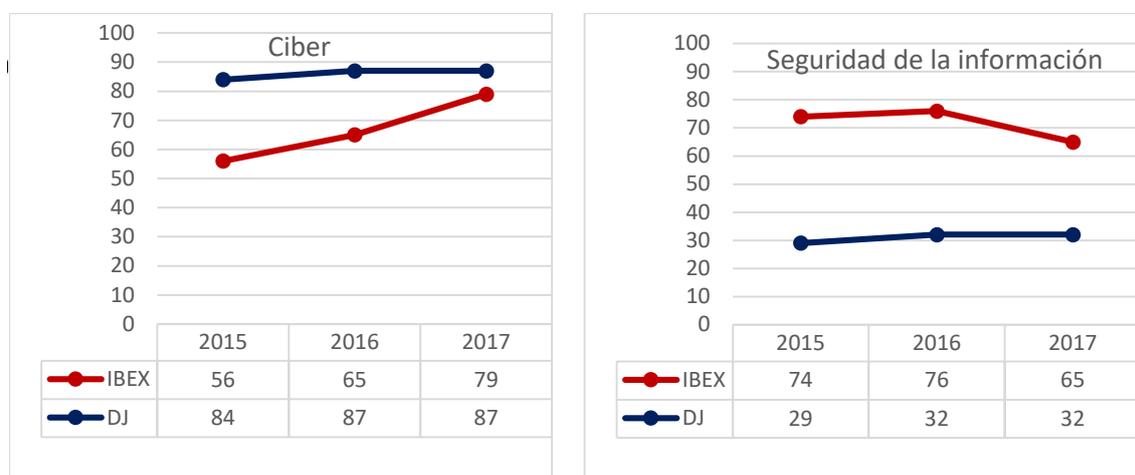
Finalmente es interesante señalar una diferencia que tiene un matiz importante por el contraste en el tono del mensaje que transmite. Nos referimos al hecho de que en las empresas del DJ se habla más de ciber-ataques que de ciber-seguridad (el doble), mientras que en las del Ibex-35 por el contrario, se habla más de ciber-seguridad que de ciber-ataques (también el doble) – ver palabras en rojo de las tablas 5 y 6. Ello implica que el mensaje que se le está enviando al accionista a ambos lados del atlántico es muy diferente, mientras las empresas americanas ponen el foco en alertar sobre los riesgos de un ciber-ataque, las empresas españolas lo ponen en las medidas de ciberseguridad

3.2.2 EL USO DE LOS TÉRMINOS “CIBER” Y “SEGURIDAD DE LA INFORMACIÓN”

Dada la relevancia de la palabra “ciber” en este estudio y el hecho de que se emplea habitualmente de forma combinada con otras palabras (“ciber-riesgo”, “ciber-seguridad”, “ciber-ataque”, “ciber-crimen”, “ciber-incidente”, etc.), realizamos un examen específico de las compañías que lo usan y de su frecuencia de aparición en los documentos de las compañías cotizadas en ambos mercados. Dicha frecuencia incluye por tanto todas las palabras combinadas que contienen dicho término. En paralelo, analizamos también el uso de las palabras “seguridad de la información”, ya que ha sido el término comúnmente utilizado históricamente para tratar temas de ciber-seguridad, cuando esta no era todavía una preocupación generalizada. Los gráficos 1 y 2 presentan estos análisis.

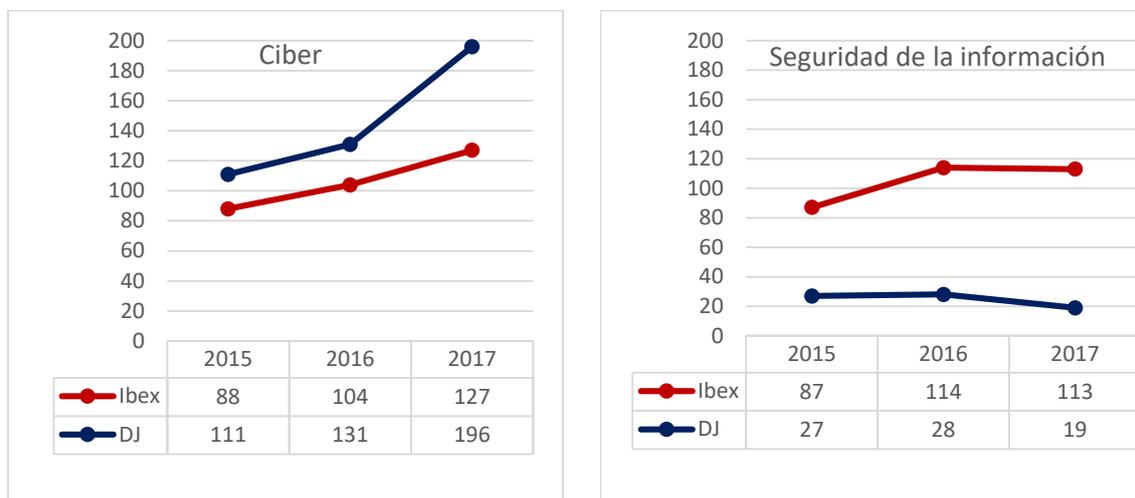
Entendemos que “seguridad de la información” denota de alguna forma un lenguaje de una etapa previa a la actual, mientras que “ciber” hace referencia a la etapa actual, siendo también un término de alcance más amplio. El análisis de la frecuencia con la que las empresas emplean ambos términos nos da una idea de hasta qué punto el mensaje que trasladan a los accionistas está adaptado al momento actual en el que hablar de ciberriesgos es lo habitual.

GRÁFICO 1. PORCENTAJE DE EMPRESAS DEL IBEX-35 Y DEL DOW JONES QUE UTILIZAN LOS TÉRMINOS “CIBER” Y “SEGURIDAD DE LA INFORMACIÓN” EN ALGUNA OCASIÓN EN LOS DOCUMENTOS ANALIZADOS



El gráfico 1 muestra el porcentaje de empresas en el Ibex-35 y el DJ, que utiliza en alguna ocasión el término “ciber” y “seguridad de la información”. Aunque en 2015 el primer término era más empleado por las empresas americanas y menos usado por las españolas, en el 2017 se produce ya una convergencia hacia un uso mayoritario de “ciber”, también por parte de las compañías españolas (el 79% de las mismas lo usa, así como un 87% de las del DJ). Por el contrario, con el paso del tiempo el término “seguridad de la información” va quedando relegado (el 65% de las empresas del Ibex-35 lo usó en 2017 frente a un 74% en 2015, y tan solo el 30% de las del DJ lo usa en 2017).

GRÁFICO 2. FRECUENCIA DE USO DE LOS TÉRMINOS "CIBER" Y "SEGURIDAD DE LA INFORMACIÓN"

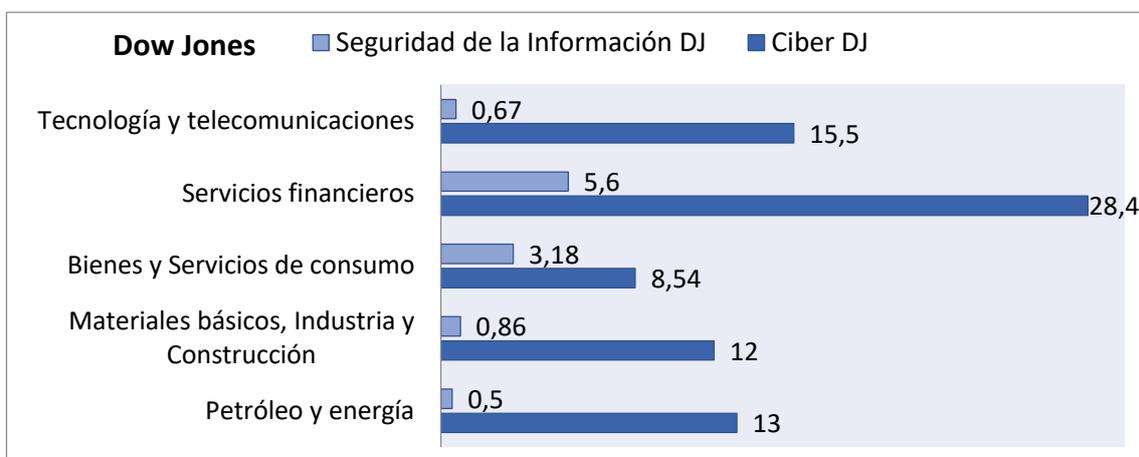
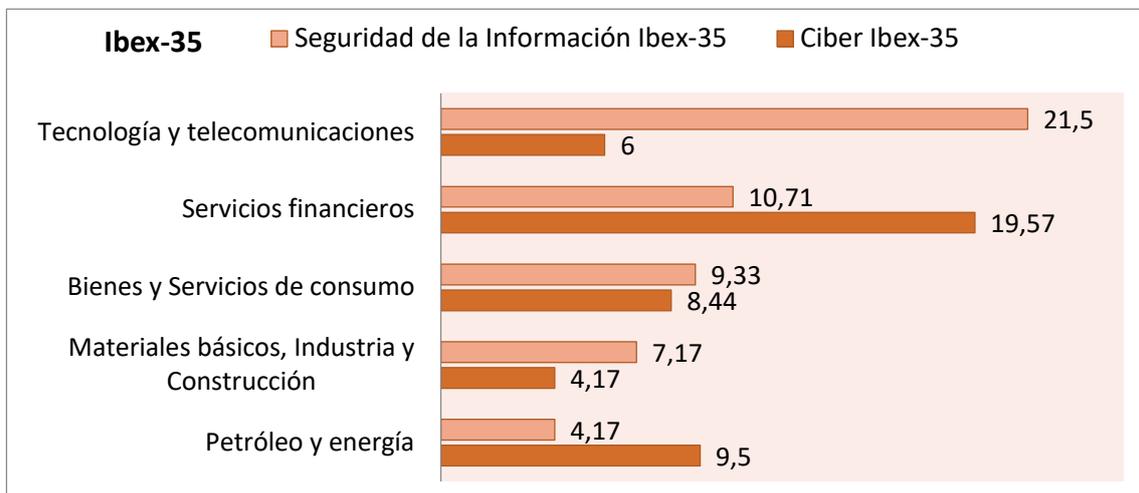


El análisis de la frecuencia con la que dichos términos aparecen en estas empresas, mostrado en el gráfico 2, corrobora los resultados anteriores. La frecuencia de uso de "ciber" registra un crecimiento notable entre 2015 y 2017 en ambos mercados, mientras que el uso de "seguridad de la información" permanece estable o decrece.

Por tanto, los resultados del análisis indican que las empresas americanas emplean de forma generalizada el término "ciber", tendencia que está comenzando a manifestarse en las empresas españolas también. Nuestra interpretación de esta tendencia es que a medida que las empresas son más conscientes de los ciberriesgos, muestran una mayor propensión a emplear un vocabulario más adaptado a los mismos. En este sentido, las empresas americanas llevan una ventaja clara sobre las españolas, si bien en los últimos años la distancia entre ambas se ha acortado enormemente. En cuanto al término seguridad de la información, su uso entre las empresas del Ibx-35 está decayendo, apoyando nuestra interpretación anterior, siendo muy escaso desde hace ya más tiempo su empleo por parte de las empresas americanas.

Para profundizar en el detalle de esta información, analizamos la frecuencia con la que aparecen las palabras ciber y seguridad de la información por sectores, tanto en las empresas del Ibex-35 como del Dow Jones. La información completa se presenta en el Anexo C y un resumen de la misma agrupada para el conjunto de los tres años considerados en el estudio, en el gráfico 3, que muestra la frecuencia media por año y por sector para ambos mercados, con la que aparecen ambos términos, “ciber” y “seguridad de la información”, en la información reportada a los accionistas. Se ha omitido el sector de servicios inmobiliarios en el gráfico debido a la nula presencia de empresas americanas en el mismo, y a que tan solo hay dos representantes de este sector en el Ibex-35. No obstante, el Anexo C sí lo incluye.

GRÁFICO 3. FRECUENCIA MEDIA POR EMPRESA DE LOS TÉRMINOS “CIBER” Y “SEGURIDAD DE LA INFORMACIÓN” EN EL IBEX-35 Y EL DOW JONES EN EL PERIODO 2015-2017



Centrándonos en la información que proporciona el gráfico 3, observamos que el sector financiero es el que menciona en mayor medida cuestiones relativas a “ciber” tanto en las empresas americanas como españolas (28,4 y 19,6 respectivamente es la frecuencia media de uso del término por empresa). Otro de los sectores en ambos mercados donde el uso de “ciber” prevalece sobre el de “seguridad de la información” es el de petróleos y energía. No cabe duda, de que estos sectores se encuentran entre los más globalizados a nivel mundial, y la homogeneidad entre las empresas que los conforman es alta, por lo que parece lógico esperar que las tendencias en el uso de terminología específica al hablar de riesgos sean convergentes entre las empresas que pertenecen a los mismos en ambos índices.

En el resto de sectores del Ibex-35, donde la heterogeneidad de las empresas que los conforman es más alta, se emplea más el término “seguridad de la información” al hablar de los riesgos que pueden afectar a la empresa y de su gestión, a pesar de ser un término mucho más limitado en cuanto a alcance de significado. Lo contrario ocurre en el Dow Jones, en cuyas empresas se menciona siempre, independientemente del sector, con mayor frecuencia media, el término “ciber” que “seguridad de la información”.

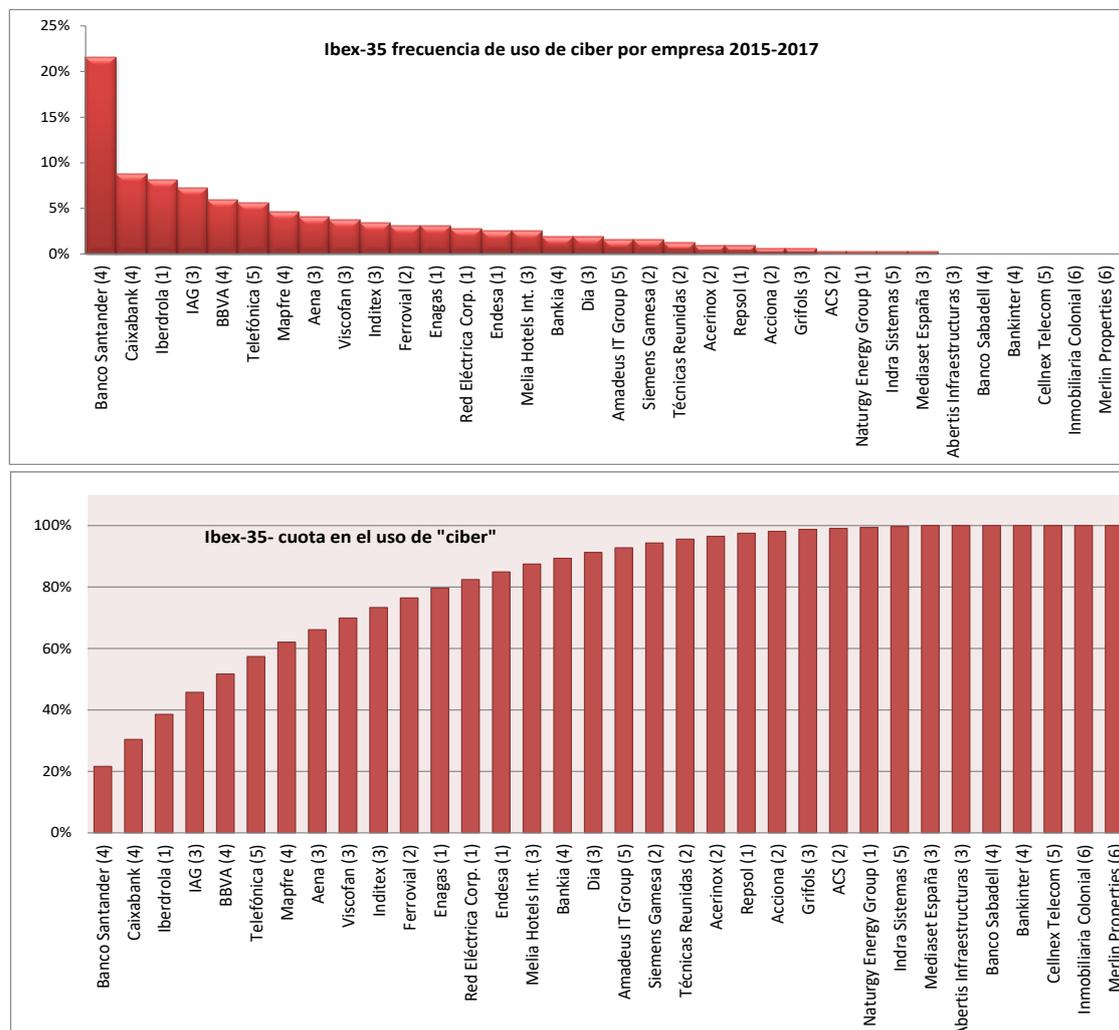
Un caso que llama la atención es el de la industria de tecnología y telecomunicaciones, en el que contrariamente a lo que podría esperarse, las empresas españolas que cotizan en el Ibex-35 hablan en mucha mayor medida de “seguridad de la información” que de “ciber” (21,5 y 6 respectivamente en media por empresa). Si algún sector debiera estar familiarizado con los ciberriesgos en mayor medida es precisamente este, por lo que este resultado sorprende, ya que lo natural sería usar el lenguaje más adaptado a los mismos, tal y como hacen las empresas americanas, salvo que se quiera evitar hablar de ellos directamente.

Dados estos resultados que denotan diferencias importantes por sectores, especialmente en el conjunto de cotizadas en el Ibex-35, en cuanto al uso de un lenguaje más o menos adaptado al entorno actual, resulta de interés investigar si también existen diferencias importantes en cuanto al uso del lenguaje entre las empresas de cada sector, es decir, si unas están más adaptadas al tiempo actual que otras. El gráfico 4 presenta, para cada empresa del Ibex-35, la cuota en la frecuencia de utilización, o número de menciones, del término “ciber” en el conjunto de los tres años estudiados, sobre el conjunto de las empresas del Ibex-35, mientras que el gráfico 5 presenta esta misma información para las empresas del Dow Jones. Dicha información se encuentra detallada también en el Anexo D.1.



Podemos observar que en el caso del Ibex-35 es una empresa financiera, Banco Santander, la que utiliza este término con mayor frecuencia a bastante distancia de la siguiente empresa, también perteneciente al sector financiero, Caixabank. Es importante destacar que el 50% de las menciones de la palabra ciber en el periodo 2015-2017 proceden de tan solo 5 empresas, 3 de ellas financieras (se añade BBVA), una energética (Iberdrola) y una de infraestructuras (IAG). También vemos como solo 12 empresas reúnen el 80% de las menciones de "ciber" hechas en el periodo. Estas 12 empresas representan todos los sectores, salvo el de servicios inmobiliarios (Telefónica, Mapfre, Aena, Viscofan, Inditex, Ferrovial, Enagás). Son dos las conclusiones que obtenemos de este detallado análisis. En primer lugar, que los resultados por sectores están condicionados por un número limitado de empresas y no por todas, incluso en los sectores que anticipábamos más globales como el financiero. Prueba de ello es por ejemplo que dos empresas del sector financiero no mencionan ni una sola vez la palabra "ciber" en los documentos analizados a lo largo de los tres años considerados, 2015-2017. También el hecho de que las 15 empresas del Ibex-35 que menos mencionan el término ciber (apenas alcanzan entre las 15 el 5% del uso del mismo) representan todos los sectores analizados sin excepción. La segunda conclusión es que el uso de este lenguaje más "moderno" o actualizado al hablar de los ciberriesgos se concentra en un número bastante reducido de las empresas del índice representativo del mercado español.

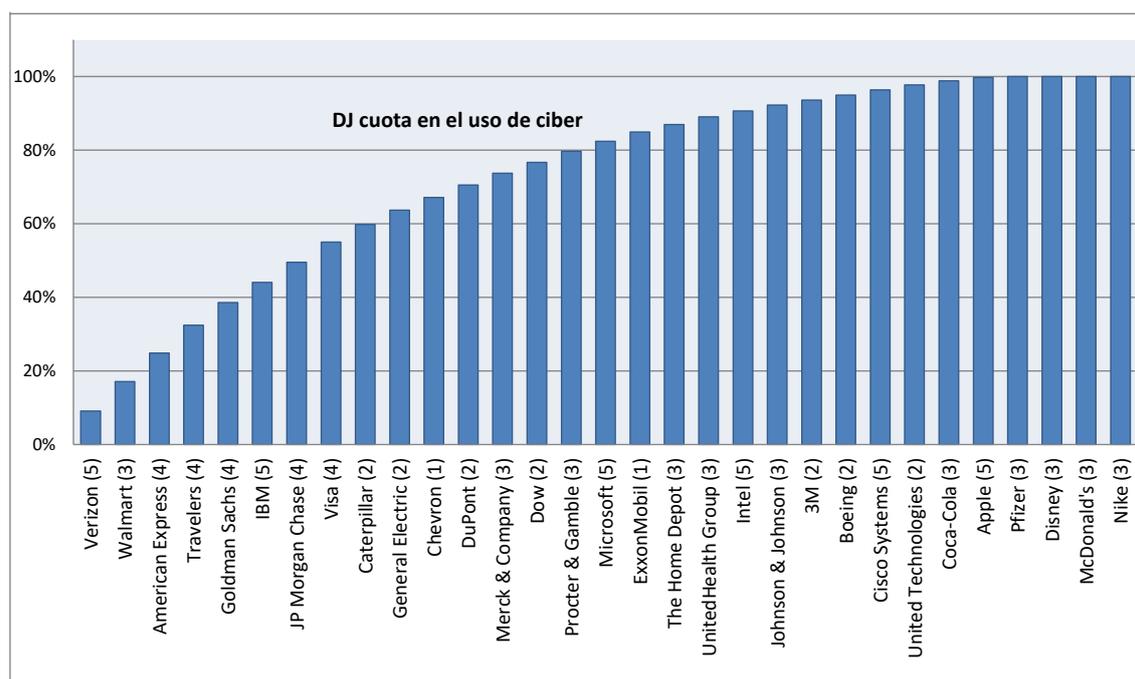
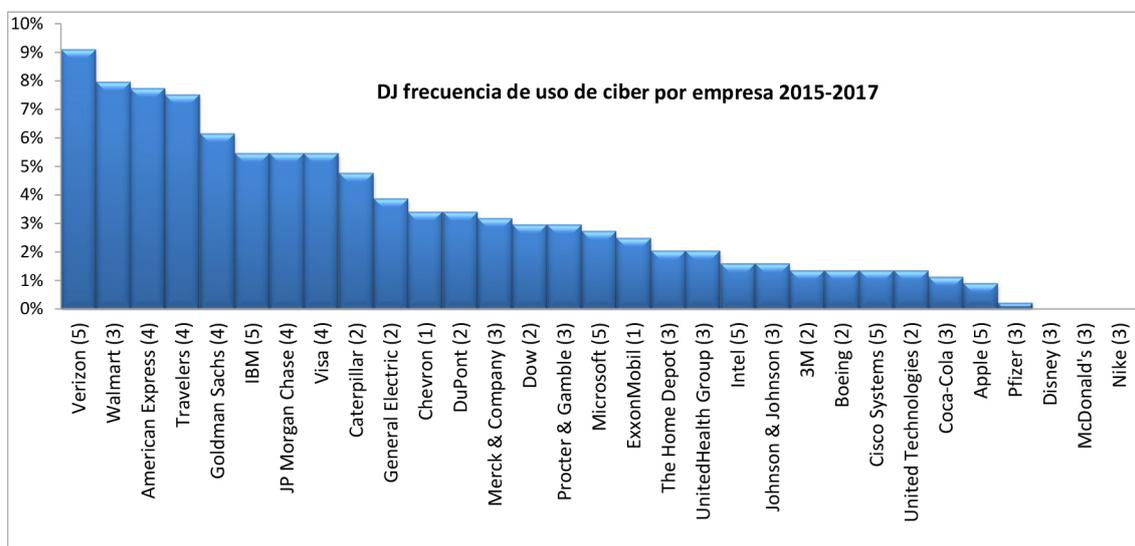
GRÁFICO 4. CUOTA DE CADA EMPRESA EN EL TOTAL DE MENCIONES DE "CIBER" DEL IBEX-35 DURANTE EL PERÍODO 2015-2017



Nota. Sectores: 1: Petróleo y energía; 2: Materiales básicos, Industria y Construcción; 3: Bienes y Servicios de consumo; 4: Servicios financieros; 5: Tecnología y telecomunicaciones; 6: Servicios inmobiliarios

En el caso del Dow Jones, la empresa que más menciona “ciber” es Verizon, una empresa de telecomunicaciones, seguida por Walmart, del sector bienes y servicios de consumo. Una de las primeras observaciones que podemos hacer es que el uso de este lenguaje que emplea la palabra ciber se encuentra mucho menos concentrado en un grupo reducido de empresas tal y como se percibe en el gráfico 5. Respecto al sector financiero, cabe destacar que todas las empresas del Dow Jones de dicho sector se encuentran en el top 10 de las empresas que más hablan de “ciber” en sus informes financieros. Es interesante destacar que solo hay 3 empresas del DJ que no mencionan en los tres años la palabra ciber y son todas del sector bienes y servicios de consumo (en comparación con las 8 empresas del Ibex-35 que no la mencionan que pertenecen a 4 sectores, bienes y servicios de consumo, tecnología y telecomunicaciones, financiero y servicios inmobiliarios).

GRÁFICO 5. CUOTA POR EMPRESA EN EL TOTAL DE MENCIONES DE “CIBER” DEL DOW JONES DURANTE 2015-2017



Nota. Sectores: 1: Petróleo y energía; 2: Materiales básicos, Industria y Construcción; 3: Bienes y Servicios de consumo; 4: Servicios financieros; 5: Tecnología y telecomunicaciones; 6: Servicios inmobiliarios

En cuanto al término “seguridad de la información”, cuyo análisis detallado se incluye en el Anexo D.2, vemos que 17 empresas del Dow Jones no lo mencionan en ningún momento en los apartados de factores de riesgo de sus informes financieros durante los años estudiados, mientras que han sido solo 3 las empresas americanas que en dicho periodo no han usado el término ciber. Curiosamente, las dos empresas americanas que con más frecuencia han empleado “seguridad de la información” (conjuntamente alcanzan el 40% de las menciones) son American Express y Walmart, dos de las empresas que más usan también el término ciber. Por tanto, en el mercado americano, el uso de las palabras seguridad de la información está muy concentrado en un número reducido de empresas y además convive en estas con el uso de la palabra ciber. No es este el caso de las empresas españolas, en el que solo 7 no han empleado dicho término, y en el que solo la mitad de las empresas que más uso hacen del mismo emplean también con frecuencia ciber, mientras que la otra mitad no ha empleado ciber o lo ha hecho de forma marginal. De hecho, en el Ibex-35, las dos empresas que más utilizan “seguridad de la información” son dos empresas tecnológicas, Amadeus e Indra, que mencionan el término 41 y 38 veces frente a la mención que hacen de ciber, 5 veces y 1 vez respectivamente. En contraste, ninguna de las seis empresas tecnológicas del Dow Jones, con excepción de Microsoft que lo emplea 5 veces, utiliza el término “seguridad de la información” a lo largo de los tres años del estudio.

Finalmente, debido a que se recogió información de distintos informes financieros españoles, en dicho mercado podemos analizar la ubicación de estos términos (ver Tabla 5). A este respecto, cabe destacar que casi el 50% de las menciones de “ciber” aparece en los Informes de Gestión, mientras que alrededor del 80% de las menciones de “seguridad de la información” se encuentra en los apartados F de los Informes de Gobierno Corporativo.

TABLA 5. FRECUENCIA DE UTILIZACIÓN DE LOS TÉRMINOS “CIBER” Y “SEGURIDAD DE LA INFORMACIÓN” (SI) EN LOS DISTINTOS DOCUMENTOS RECOGIDOS DE LOS INFORMES FINANCIEROS ESPAÑOLES

Informe	CIBER		SI	
	N	%	N	%
Cuentas Anuales Consolidadas	63	20	11	4
Apartado E del IGC	82	26	27	9
Apartado F del IGC (con relación a la emisión de info. financiera)	22	7	258	82
Informe de Gestión Consolidado	152	48	18	6
		100%		100%



”

El principal factor de preocupación con relación a los ciberataques es la reputación, tanto para las empresas del Ibex-35 como para las del Dow Jones.



CONCLUSIONES Y RECOMENDACIONES

En los últimos años cada vez se han hecho más frecuentes los ataques cibernéticos, y la ciberseguridad se ha convertido en una cuestión estratégica para las empresas. La preocupación que suscitan todas las cuestiones relativas a los ciberriesgos queda patente, año tras año, en los diversos informes que se publican, como pueden ser el Barómetro de Riesgos de Allianz o el Informe de Riesgos Globales elaborado por el Foro Económico Mundial, ya mencionados en la introducción de este informe, y que se basan en encuestas realizadas a directivos de empresas de distintos países. Sin embargo, esta preocupación no parece haberse trasladado aún a los informes financieros que las grandes empresas cotizadas, en este caso las españolas y norteamericanas, han de publicar anualmente para informar a sus accionistas. Si bien es cierto que un número importante de empresas, especialmente del mercado americano, sí mencionan los riesgos cibernéticos y cuestiones relacionadas con la ciberseguridad en sus empresas, la información facilitada es generalmente bastante superficial. Efectivamente, cuando se comenta alguno de los posibles riesgos cibernéticos a los que las empresas han de hacer frente, se detalla muy poco en qué consiste, o factores como su criticidad o su amplitud.

Por otro lado, el análisis comparado entre la información que las empresas del Dow Jones y las del Ibex-35 trasladan a sus accionistas sobre ciberriesgos y ciberseguridad, muestra como las empresas españolas están a bastante distancia de las americanas en el reporte de información sobre los mismos. Una cuestión que llama la atención es, sin embargo, la mayor mención sobre seguros externos para cubrir ciberriesgos hecha por las empresas españolas, mención que prácticamente está ausente en los informes de las empresas americanas. Parece por tanto, que las empresas españolas se ampararían en mayor medida que las americanas en el uso de "ciberseguros" para gestionar los ciberriesgos, a tenor de lo reportado en los informes de ambos conjuntos de compañías. Una segunda interpretación que cabría de este hecho, estaría basada en el conocido dicho español de "echar balones fuera".

Cuando las empresas hablan de riesgos en general, en el mercado americano los ciberriesgos están presentes (son el tercer tipo de riesgo más mencionado en los informes) mientras que en la conversación que las empresas españolas mantienen con sus accionistas están prácticamente ausentes. Además en las pocas ocasiones que las empresas del Ibex hablan de ellos, el tono del mensaje y el propio mensaje difiere al dado por las del DJ. Las empresas americanas emplean un lenguaje más específico y consciente de la gravedad de los riesgos cibernéticos a los que se enfrentan, emplean con frecuencia palabras como “amenazas y ataques”, además su mensaje, y por tanto su preocupación, está más centrado en sus outputs concretos “productos y servicios”, que en la generalidad de los mercados, y va ligado a la “tecnología”, implicando a todos los *stakeholders*, incluidos “proveedores, empleados y terceras partes”, y mostrando en bastantes ocasiones cierta preocupación por “la propiedad intelectual”. Es un lenguaje más específico y, en nuestra opinión, más adecuado que el usado por las empresas españolas representadas en el Ibex-35, que construyen su comunicación al hablar de ciberseguridad o ciberriesgos con términos más generales, sin mencionar apenas a los *stakeholders*, la tecnología, o la propiedad intelectual, y haciendo más referencias en cambio a procesos de control, auditoría, o financieros en relación con la ciberseguridad. Por el contrario destaca en el estudio la coincidencia sobre la relevancia que las empresas a ambos lados del atlántico dan a la reputación, ya que sus informes están llenos de referencias a la misma con relación a los riesgos cibernéticos.

Este retraso en cuanto al reporte de ciberriesgos por parte de las empresas españolas cotizadas podría estar inducido no tanto, o no solo, por una menor concienciación de las mismas frente a las americanas, acerca de la importancia de los ciberriesgos, sino también por una regulación que pone el foco, por un lado, más en los sistemas de gestión de los riesgos que en el detalle o especificación de los propios riesgos (criticidad, alcance, etc.), y por otro, en los riesgos financieros y fiscales sobre otro tipo de riesgos. Por ejemplo, el apartado E del informe anual de gobierno corporativo de obligado cumplimiento para las empresas cotizadas españolas, se centra en el propio sistema de control y gestión de riesgos más que en los riesgos en sí mismos, haciendo además hincapié en todos sus subapartados en la inclusión de los riesgos fiscales (véase Anexo A). Asimismo el apartado F, también analizado en este estudio y detallado en el mismo anexo, que junto con el apartado E conforman la sección en la que las empresas reportan los riesgos y su gestión en el Informe de gobierno corporativo, hace referencia explícita a la gestión de los riesgos relacionados con el proceso de emisión de la información financiera.

Este sesgo de la normativa, que probablemente responda a justificaciones adecuadas por el diferente contexto sectorial o cultural en el que desarrollan su actividad las empresas españolas, y que no contempla ninguna mención explícita a la ciberseguridad, puede estar de alguna forma condicionando la información que las empresas cotizadas españolas trasladan a sus accionistas.

Una posibilidad para corregir este “sesgo” en las empresas españolas relativo al reporte de los riesgos que las afectan y la gestión que de los mismos hacen, podría ser seguir el ejemplo de la US Securities and Exchange Commission, que como ya se ha mencionado en este estudio, ha editado una guía para ayudar a las empresas a elaborar la información que deben trasladar a los accionistas acerca de los riesgos cibernéticos a los que están expuestas, su desglose, su alcance, su criticidad, etc. y la gestión que de los mismos están haciendo. En un área tan delicada, como es la de la ciberseguridad, el reporte de información debe ser suficientemente amplio para garantizar el derecho de los accionistas a estar informados sobre la situación y riesgos de las empresas en las que invierten, pero a su vez, esta información que se les da a los accionistas, en una empresa cotizada es pública, por lo que hay que mantener un equilibrio razonable para no poner en una situación de vulnerabilidad a la propia empresa, lo que iría a su vez en detrimento de

los propios accionistas. Sin duda este equilibrio es delicado, y una guía del organismo supervisor sería bien recibida tanto por parte de las empresas como de los accionistas. En nuestra opinión esta sencilla solución contribuiría a que existiese mayor transparencia en este sentido en el mercado español, garantizando mejor los derechos de los accionistas a estar informados de la situación de las empresas en las que están invirtiendo. También sería de utilidad para las propias empresas, ya que les ayudaría en el proceso interno de análisis y gestión de los riesgos cibernéticos, un campo todavía desconocido y en continua evolución.

Curiosamente, a pesar de la ventaja que sacan las empresas americanas a las españolas en materia de reporte de riesgos de ciberseguridad, la propia SEC es consciente del camino que queda por recorrer, como muestra el hecho, no solo de que haya editado un guía para que las empresas cotizadas elaboren el reporte de los ciberriesgos, sino que además en 2018 la haya actualizado solicitando a las compañías que detallen en mayor medida dichos riesgos cibernéticos. El presidente de la SEC, Jay Clayton, ha declarado recientemente: “The Commission is focused on identifying and managing cybersecurity risks and ensuring that market participants—including issuers, intermediaries, investors and government authorities—are actively and effectively engaged in this effort and are appropriately informing investors and other market participants of these risks” (Rossi et al. 2018).

No obstante, hay que mencionar que la falta de contenido sobre ciberseguridad y ciberriesgos en los informes de las cotizadas no se da por igual en todas las empresas, especialmente en el caso español, donde hay compañías que sí tienen más presente, como muestra el análisis realizado, la gravedad y relevancia de este tipo de riesgos y trasladan mucha más información sobre los mismos y su gestión a los accionistas, el caso más destacado es el del Banco Santander, pero también otras empresas, Caixabank, Iberdrola, IAG, BBVA, Telefónica o Mapfre informan, aunque en menor medida, de los ciberriesgos a sus accionistas. Sin embargo, en general, el grueso de las compañías cotizadas españolas tiene todavía mucho camino por recorrer para garantizar el derecho de los accionistas a estar informados sobre estos riesgos.

Finalmente, una última conclusión o implicación de este estudio, se refiere al potencial existente para las empresas aseguradoras a la hora de ofrecer coberturas relacionadas con la ciberseguridad, especialmente en el mercado español, en el que las empresas consideran estos seguros como un complemento importante en su gestión de ciberriesgos a la luz de las referencias que hacen a los mismos en sus informes. A tener en cuenta en este sentido, destaca la inquietud que las compañías muestran con respecto al riesgo de reputación asociado a los ciberriesgos, así como de protección de la información, ya sea “confidencial” o “privada”.

Es importante a la hora de interpretar los resultados que se presentan en este estudio, señalar las limitaciones que, como cualquier investigación, tiene. Siendo dos las más importantes. En primer lugar es fundamental tener en cuenta que los análisis realizados no pueden ser exhaustivos debido a la ingente cantidad de información elaborada por las empresas en sus informes financieros, especialmente en el mercado español. En este sentido quizá ayudaría, que los organismos supervisores españoles proveyesen de una guía normalizada de obligado seguimiento para el reporte financiero (cuentas e informe de gestión), al igual que se hace en el mercado americano (informe 10-k). No podemos olvidar que la mejor forma de “des-informar es sobre-informar”. Una segunda limitación se refiere al uso de softwares semánticos empleados para hacer los análisis. Si bien estos tienen la ventaja de presentar una visión objetiva del análisis del texto, también tienen limitaciones en cuanto a la comprensión semántica de las oraciones y análisis de los contenidos, al estar basados en algoritmos que no siempre pueden captar la riqueza de los matices o interpretar con exactitud los términos.



BIBLIOGRAFÍA

Baugh, N., McNallen, A., & Frazelle, M. (2014). *Concept Mapping as a Data Collection and Analysis Tool in Historical Research. The Qualitative Report, 19(13), 1-10.*

Butler-Kisber, L., & Poldma, T. (2010). *The Power of Visual Approaches in Qualitative Inquiry: The Use of Collage Making and Concept mapping in Experiential Research. Journal of Research Practice, 6(2), 1-17.*

Cretchley, J., Gallois, C., Chenery, H., & Smith, A. (2010). *Conversations Between Carers and People with Schizophrenia: a Qualitative Analysis using Leximancer. Qualitative Health Research, 20(12), 1611-1628.*

Hayes, A. F., & Krippendorff, K. (2007). *Answering the call for a standard reliability measure for coding data. Communication Methods and Measures, 1, 77-89.*

Megaputer Intelligence, Inc. (2000). *Tutorial: Text Analyst Introduction. Case Study.*

Rossi, M., Richman, L., & Burke, M. (2018). *SEC concerns on cybersecurity. The corporate board, september/october 2018, 20-24.*

Smith, A. E. y Humphreys, M. S. (2006). *Evaluation of unsupervised semantic mapping of natural language with Leximancer concept mapping. Behavior Research Methods, 38(2), 262-279.*



ANEXOS

A.A

ANEXO A. DESGLOSE DE SUBAPARTADOS DE LAS SECCIONES E Y F DEL INFORME DE GOBIERNO CORPORATIVO.

E. Sistemas de control y gestión del riesgo

- E.1 Explique el alcance del Sistema de Gestión de Riesgos de la sociedad, incluidos los de materia fiscal.
- E.2 Identifique los órganos de la sociedad responsables de la elaboración y ejecución del Sistema de Gestión de Riesgos, incluido el fiscal.
- E.3 Señale los principales riesgos, incluidos los fiscales, que pueden afectar a la consecución de los objetivos de negocio.
- E.4 Identifique si la entidad cuenta con un nivel de tolerancia al riesgo, incluido el fiscal.
- E.5 Indique qué riesgos, incluidos los fiscales, se han materializado durante el ejercicio.
- E.6 Explique los planes de respuesta y supervisión para los principales riesgos de la entidad, incluidos los fiscales.

F. Sistemas internos de control y gestión de riesgos en relación con el proceso de emisión de la información financiera

- F.1 Entorno de control de la entidad
 - F.1.1. Qué órganos y/o funciones son los responsables de: (i) la existencia y mantenimiento de un adecuado y efectivo SCIF; (ii) su implantación; y (iii) su supervisión.
 - F.1.2. Si existen, especialmente en lo relativo al proceso de elaboración de la información financiera, los siguientes elementos:
 - Departamentos y/o mecanismos encargados: (i) del diseño y revisión de la estructura organizativa; (ii) de definir claramente las líneas de responsabilidad y autoridad, con una adecuada distribución de tareas y funciones; y (iii) de que existan procedimientos suficientes para su correcta difusión en la entidad.
 - Código de conducta, órgano de aprobación, grado de difusión e instrucción, principios y valores incluidos (indicando si hay menciones específicas al registro de operaciones y elaboración de información financiera), órgano encargado de analizar incumplimientos y de proponer acciones correctoras y sanciones.
 - Canal de denuncias, que permita la comunicación al comité de auditoría de irregularidades de naturaleza financiera y contable, en adición a eventuales

incumplimientos del código de conducta y actividades irregulares en la organización, informando en su caso si éste es de naturaleza confidencial.

- Programas de formación y actualización periódica para el personal involucrado en la preparación y revisión de la información financiera, así como en la evaluación del SCIIF, que cubran al menos, normas contables, auditoría, control interno y gestión de riesgos.

F.2 Evaluación de riesgos de la información financiera. Informe, al menos, de:

F.2.1. Cuáles son las principales características del proceso de identificación de riesgos, incluyendo los de error o fraude, en cuanto a:

- Si el proceso existe y está documentado.
- Si el proceso cubre la totalidad de objetivos de la información financiera, (existencia y ocurrencia; integridad; valoración; presentación, desglose y comparabilidad; y derechos y obligaciones), si se actualiza y con qué frecuencia.
- La existencia de un proceso de identificación del perímetro de consolidación, teniendo en cuenta, entre otros aspectos, la posible existencia de estructuras societarias complejas, entidades instrumentales o de propósito especial.
- Si el proceso tiene en cuenta los efectos de otras tipologías de riesgos (operativos, tecnológicos, financieros, legales, reputacionales, medioambientales, etc.) en la medida que afecten a los estados financieros.
- Qué órgano de gobierno de la entidad supervisa el proceso.

F.3 Actividades de control. Informe, señalando sus principales características, si dispone al menos de:

F.3.1. Procedimientos de revisión y autorización de la información financiera y la descripción del SCIIF, a publicar en los mercados de valores, indicando sus responsables, así como de documentación descriptiva de los flujos de actividades y controles (incluyendo los relativos a riesgo de fraude) de los distintos tipos de transacciones que puedan afectar de modo material a los estados financieros, incluyendo el procedimiento de cierre contable y la revisión específica de los juicios, estimaciones, valoraciones y proyecciones relevantes.

F.3.2. Políticas y procedimientos de control interno sobre los sistemas de información (entre otras, sobre seguridad de acceso, control de cambios, operación de los mismos, continuidad operativa y segregación de funciones) que soporten los procesos relevantes de la entidad en relación a la elaboración y publicación de la información financiera.

F.3.3. Políticas y procedimientos de control interno destinados a supervisar la gestión de las actividades subcontratadas a terceros, así como de aquellos aspectos de evaluación, cálculo o valoración encomendados a expertos independientes, que puedan afectar de modo material a los estados financieros.

F.4 Información y comunicación. Informe, señalando sus principales características, si dispone al menos de:

F.4.1. Una función específica encargada de definir, mantener actualizadas las políticas contables (área o departamento de políticas contables) y resolver dudas o conflictos derivados de su interpretación, manteniendo una comunicación fluida

con los responsables de las operaciones en la organización, así como un manual de políticas contables actualizado y comunicado a las unidades a través de las que opera la entidad.

- F.4.2. Mecanismos de captura y preparación de la información financiera con formatos homogéneos, de aplicación y utilización por todas las unidades de la entidad o del grupo, que soporten los estados financieros principales y las notas, así como la información que se detalle sobre el SCIIF.
- F.5 Supervisión del funcionamiento del sistema. Informe, señalando sus principales características, al menos de:
 - F.5.1. Las actividades de supervisión del SCIIF realizadas por el comité de auditoría, así como si la entidad cuenta con una función de auditoría interna que tenga entre sus competencias la de apoyo al comité en su labor de supervisión del sistema de control interno, incluyendo el SCIIF. Asimismo, se informará del alcance de la evaluación del SCIIF realizada en el ejercicio y del procedimiento por el cual el encargado de ejecutar la evaluación comunica sus resultados, si la entidad cuenta con un plan de acción que detalle las eventuales medidas correctoras, y si se ha considerado su impacto en la información financiera.
 - F.5.2. Si cuenta con un procedimiento de discusión mediante el cual, el auditor de cuentas (de acuerdo con lo establecido en las NTA), la función de auditoría interna y otros expertos puedan comunicar a la alta dirección y al comité de auditoría o administradores de la entidad las debilidades significativas de control interno identificadas durante los procesos de revisión de las cuentas anuales o aquellos otros que les hayan sido encomendados. Asimismo, informará de si dispone de un plan de acción que trate de corregir o mitigar las debilidades observadas.
- F.6 Otra información relevante
- F.7 Informe del auditor externo. Informe de:
 - F.7.1. Si la información del SCIIF remitida a los mercados ha sido sometida a revisión por el auditor externo, en cuyo caso la entidad debería incluir el informe correspondiente como anexo. En caso contrario, debería informar de sus motivos.

ANEXO B. LISTADO DE EMPRESAS, SECTOR Y CAPITALIZACIÓN BURSÁTIL DE LAS EMPRESAS ESTUDIADAS

ANEXO B.1 – Empresas del Ibex-35

EMPRESA	SECTOR	CAPITALIZACIÓN BURSÁTIL ^{12,13}
Abertis Infraestructuras	Bienes y Servicios de consumo	18.183 ¹⁴
Acciona	Materiales básicos, Industria y Construcción	4.786
Acerinox	Materiales básicos, Industria y Construcción	2.680
ACS	Materiales básicos, Industria y Construcción	11.668
Aena	Bienes y Servicios de consumo	23.152
Amadeus IT Group	Tecnología y telecomunicaciones	30.252
Arcelor Mittal	Materiales básicos, Industria y Construcción	20.739
Banco Sabadell	Servicios financieros	5.366
Bankia	Servicios financieros	7.975
Bankinter	Servicios financieros	6.243
BBVA	Servicios financieros	34.886
Caixabank	Servicios financieros	18.142
Cellnex Telecom	Tecnología y telecomunicaciones	5.683
Dia	Bienes y Servicios de consumo	387
Enagas	Petróleo y energía	5.873
Endesa	Petróleo y energía	23.091
Ferrovial	Materiales básicos, Industria y Construcción	14.821
Naturgy Energy Group	Petróleo y energía	23.836
Grifols	Bienes y Servicios de consumo	10.184
IAG	Bienes y Servicios de consumo	14.904
Iberdrola	Petróleo y energía	47.612
Inditex	Bienes y Servicios de consumo	79.536
Indra Sistemas	Tecnología y telecomunicaciones	1.702
Inmobiliaria Colonial	Servicios inmobiliarios	4.446
Mapfre	Servicios financieros	7.619
Mediaset España	Bienes y Servicios de consumo	2.156
Melia Hotels International	Bienes y Servicios de consumo	2.029
Merlin Properties	Servicios inmobiliarios	5.391
Red Eléctrica Corporación	Petróleo y energía	10.232
Repsol	Petróleo y energía	23.703
Banco Santander	Servicios financieros	79.537
Siemens Gamesa	Materiales básicos, Industria y Construcción	9.240
Técnicas Reunidas	Materiales básicos, Industria y Construcción	1.310
Telefónica	Tecnología y telecomunicaciones	38.620
Viscofan	Bienes y Servicios de consumo	2.426

¹² Datos extraídos el 20/02/2019 de la web <http://www.expansion.com/mercados/indices.html>

¹³ En millones de euros

¹⁴ Dato hasta el 3/8/2018. En la actualidad no cotiza en la Bolsa de Madrid

ANEXO B.2 – Empresas del Dow Jones

EMPRESA	SECTOR	CAPITALIZACIÓN BURSÁTIL ^{12,13}
3M	Materiales básicos, Industria y Construcción	119.830
American Express	Servicios financieros	90.215
Apple	Tecnología y telecomunicaciones	944.198
Boeing	Materiales básicos, Industria y Construcción	237.475
Caterpillar	Materiales básicos, Industria y Construcción	79.373
Chevron	Petróleo y energía	230.057
Cisco Systems	Tecnología y telecomunicaciones	249.222
Coca-Cola	Bienes y Servicios de consumo	191.868
Dow DuPont	Materiales básicos, Industria y Construcción	81.543
ExxonMobil	Petróleo y energía	333.028
General Electric	Materiales básicos, Industria y Construcción	87.851
Goldman Sachs	Servicios financieros	73.651
The Home Depot	Bienes y Servicios de consumo	216.429
IBM	Tecnología y telecomunicaciones	124.823
Intel	Tecnología y telecomunicaciones	241.908
Johnson & Johnson	Bienes y Servicios de consumo	364.266
JP Morgan Chase	Servicios financieros	345.007
McDonald's	Bienes y Servicios de consumo	138.987
Merck & Company	Bienes y Servicios de consumo	206.340
Microsoft	Tecnología y telecomunicaciones	841.777
Nike	Bienes y Servicios de consumo	106.631
Pfizer	Bienes y Servicios de consumo	243.300
Procter & Gamble	Bienes y Servicios de consumo	247.919
Travelers	Servicios financieros	34.212
UnitedHealth Group	Bienes y Servicios de consumo	259.037
United Technologies	Materiales básicos, Industria y Construcción	110.890
Verizon	Tecnología y telecomunicaciones	229.700
Visa	Servicios financieros	252.270
Walmart	Bienes y Servicios de consumo	287.185
Walt Disney	Bienes y Servicios de consumo	169.442

ANEXOC. ANÁLISIS DE LAS FRECUENCIAS DE UTILIZACIÓN DE LOS TÉRMINOS “CIBER” Y “SEGURIDAD DE LA INFORMACIÓN”

C.1. Estadísticos descriptivos de las frecuencias de utilización de los términos “ciber” y “seguridad de la información” (SI), por año y por sector de actividad en el conjunto de empresas analizadas de los dos índices bursátiles

En las siguientes tablas se muestran algunos estadísticos descriptivos sobre las frecuencias de uso de los términos “ciber” y “seguridad de la información”. Siendo la frecuencia el número de menciones de los términos en cada empresa, el mínimo y el máximo se refieren, respectivamente, al número **mínimo** y **máximo** de veces que se menciona el término en el conjunto de empresas del sector. La suma se refiere al total de veces que se mencionan “ciber” o “seguridad de la información” en cada sector. Finalmente, la **media** representa el número medio de veces que las empresas de cada sector mencionan dichos términos

Sector	N	Año	Ciber				SI			
			Min.	Max.	S	M	Min.	Max.	S	M
Petróleo y energía	8	2015	0	5	14	1,75	0	4	10	1,25
		2016	0	9	28	3,5	0	4	9	1,13
		2017	1	12	41	5,13	0	3	7	0,88
		Total	1	26	83	10,38	0	11	26	3,25
Materiales básicos, Industria y Construcción	13	2015	0	6	28	2,15	0	6	16	1,23
		2016	0	7	31	2,38	0	6	14	1,08
		2017	1	8	50	3,85	0	9	19	1,46
		Total	1	21	109	8,38	0	21	49	3,77
Bienes y Servicios de consumo	20	2015	0	10	39	1,95	0	8	33	1,65
		2016	0	12	54	2,7	0	11	42	2,1
		2017	0	15	76	3,8	0	10	44	2,2
		Total	0	35	169	8,45	0	27	119	5,95
Servicios financieros	12	2015	0	28	84	7	0	9	33	2,75
		2016	0	22	84	7	0	9	41	3,42
		2017	0	21	111	9,25	0	9	29	2,42
		Total	0	69	279	23,25	0	26	103	8,58
Tecnología y telecomunicaciones	10	2015	0	13	34	3,4	0	13	22	2,2
		2016	0	13	38	3,8	0	16	35	3,5
		2017	0	14	45	4,5	0	17	33	3,3
		Total	0	40	117	11,7	0	41	90	9
Servicios inmobiliarios	2	2015	0	0	0	0	0	0	0	0
		2016	0	0	0	0	0	1	1	0,5
		2017	0	0	0	0	0	0	0	0
		Total	0	0	0	0	0	1	1	0,5

Nota. N = número de empresas. Min = mínimo. Max = máximo. S = suma. M = media.

C.2. Estadísticos descriptivos de las frecuencias de utilización de los términos “ciber” y “seguridad de la información” (SI) por sector de actividad en las empresas del IBEX y del Dow Jones, en el conjunto de años estudiados.

Sector Total	IBEX									DOW JONES								
	N	Ciber				SI				N	Ciber				SI			
		Min	Max	S	M	Min	Max	S	M		Min	Max	S	M	Min	Max	S	M
Petróleo y energía	6	1	26	57	9,5	0	11	25	4,17	2	11	15	26	13	0	1	1	0,5
Materiales básicos, Industria y Construcción	6	1	10	25	4,17	0	21	43	7,17	7	6	21	84	12	0	5	6	0,86
Bienes y Servicios de consumo	9	0	23	76	8,44	0	27	84	9,33	11	0	35	93	8,54	0	13	35	3,18
Servicios financieros	7	0	69	137	19,6	1	26	75	10,7	5	24	34	142	28,4	0	19	28	5,6
Tecnología y telecomunicaciones	4	0	18	24	6	3	41	86	21,5	6	4	40	93	15,5	0	4	4	0,67
Servicios inmobiliarios	2	0	0	0	0	0	1	1	0,5	-	-	-	-	-	-	-	-	-

Nota. N = número de empresas. Min = mínimo. Max = máximo. S = suma. M = media aritmética.

ANEXO D. FRECUENCIAS DE USO DE “CIBER” Y “SEGURIDAD DE LA INFORMACIÓN” POR EMPRESA

D.1. Total de menciones de “ciber” durante el período 2015-2017

EMPRESAS IBEX (SECTOR)	MENCIONES “CIBER”
Banco Santander (4)	69
Caixabank (4)	28
Iberdrola (1)	26
IAG (3)	23
BBVA (4)	19
Telefónica (5)	18
Mapfre (4)	15
Aena (3)	13
Viscofan (3)	12
Inditex (3)	11
Ferrovial (2)	10
Enagas (1)	10
Red Eléctrica Corporación (1)	9
Endesa (1)	8
Melia Hotels International	8
Bankia (4)	6
Dia (3)	6
Amadeus IT Group (5)	5
Siemens Gamesa (2)	5
Técnicas Reunidas (2)	4
Acerinox (2)	3
Repsol (1)	3
Acciona (2)	2
Grifols (3)	2
ACS (2)	1
Naturgy Energy Group (1)	1
Indra Sistemas (5)	1
Mediaset España (3)	1
Abertis Infraestructuras (3)	0
Banco Sabadell (4)	0
Bankinter (4)	0
Cellnex Telecom (5)	0
Inmobiliaria Colonial (6)	0
Merlin Properties (6)	0

EMPRESAS IBEX (SECTOR)	MENCIONES “CIBER”
Verizon (5)	40
Walmart (3)	35
American Express (4)	34
Travelers (4)	33
Goldman Sachs (4)	27
IBM (5)	24
JP Morgan Chase (4)	24
Visa (4)	24
Caterpillar (2)	21
General Electric (2)	17
Chevron (1)	15
DuPont (2)	15
Merck & Company (3)	14
Dow (2)	13
Procter & Gamble (3)	13
Microsoft (5)	12
ExxonMobil (1)	11
The Home Depot (3)	9
UnitedHealth Group (3)	9
Intel (5)	7
Johnson & Johnson (3)	7
3M (2)	6
Boeing (2)	6
Cisco Systems (5)	6
United Technologies (2)	6
Coca-Cola (3)	5
Apple (5)	4
Pfizer (3)	1
Disney (3)	0
McDonald's (3)	0
Nike (3)	0

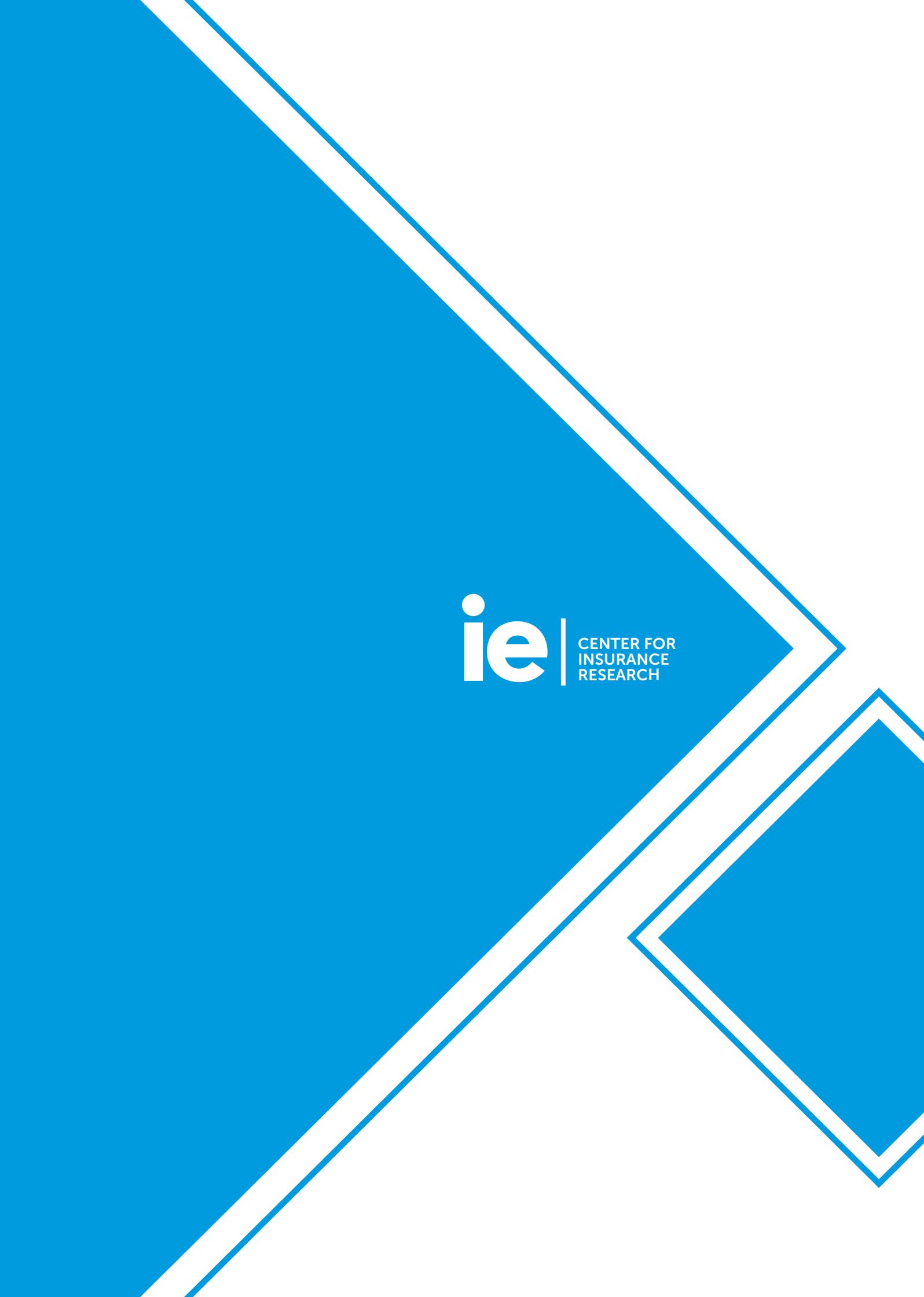
Nota. Sectores: 1: Petróleo y energía; 2: Materiales básicos, Industria y Construcción; 3: Bienes y Servicios de consumo; 4: Servicios financieros; 5: Tecnología y telecomunicaciones; 6: Servicios inmobiliarios

D.2. Total de menciones de “seguridad de la información” durante el período 2015-2017

EMPRESAS IBEX (SECTOR)	MENCIONES “CIBER”
Amadeus IT Group (5)	41
Indra Sistemas (5)	38
Inditex (3)	27
Bankia (4)	26
IAG (3)	21
Ferrovial (2)	21
Mapfre (4)	18
Caixabank (4)	14
Técnicas Reunidas (2)	12
Red Eléctrica Corporación (1)	11
Aena (3)	10
Dia (3)	9
Endesa (1)	9
Bankinter (4)	9
Abertis Infraestructuras (3)	7
Grifols (3)	6
Acerinox (2)	6
Telefónica (5)	4
Melia Hotels International (3)	4
Siemens Gamesa (2)	4
Banco Sabadell (4)	4
Banco Santander (4)	3
Enagas (1)	3
Cellnex Telecom (5)	3
Naturgy Energy Group (1)	2
BBVA (4)	1
Merlin Properties (6)	1
Iberdrola (1)	0
Repsol (1)	0
Acciona (2)	0
ACS (2)	0
Mediaset España (3)	0
Viscofan (3)	0
Inmobiliaria Colonial (6)	0

EMPRESAS IBEX (SECTOR)	MENCIONES “CIBER”
American Express (4)	19
Walmart (3)	13
The Home Depot (3)	6
Pfizer (3)	6
Procter & Gamble (3)	5
Caterpillar (2)	5
Visa (4)	5
Goldman Sachs (4)	4
Microsoft (5)	4
Johnson & Johnson (3)	2
UnitedHealth Group (3)	2
Nike (3)	1
General Electric (2)	1
ExxonMobil (1)	1
Chevron (1)	0
JP Morgan Chase (4)	0
Travelers (4)	0
3M (2)	0
Boeing (2)	0
Dow (2)	0
DuPont (2)	0
United Technologies (2)	0
Apple (5)	0
Cisco Systems (5)	0
IBM (5)	0
Intel (5)	0
Verizon (5)	0
Coca-Cola (3)	0
Disney (3)	0
McDonald's (3)	0
Merck & Company (3)	0

Nota. Sectores: 1: Petróleo y energía; 2: Materiales básicos, Industria y Construcción; 3: Bienes y Servicios de consumo; 4: Servicios financieros; 5: Tecnología y telecomunicaciones; 6: Servicios inmobiliarios



ie | CENTER FOR
INSURANCE
RESEARCH