INFORME

IV INFORME- RANKING DE TRANSPARENCIA EN CIBERSEGURIDAD DE LAS EMPRESAS DEL IBEX 35

IV ranking - informe de transparencia y buen gobierno de información en ciberseguridad en las empresas del IBEX 35.

Por Javier Huergo

WATCH&ACT
PROTECTION SERVICES

Madrid, noviembre de 2024

INDEPENDENCIA DE NUESTROS INFORMES El presente informe-ranking de transparencia no es financiado por ninguna de las instituciones analizadas en el mismo. Watch&Act Protection Services no recibe contraprestación de ninguna clase por la elaboración de este. Las aclaraciones técnicas en relación con la metodología del informe y el cumplimiento de los indicadores de transparencia podrán ser atendidos conforme a la disponibilidad del personal de Watch&Act Protection Services

Watch&Act Protection Services. Correduría de seguros especialista en seguros de ciberriesgo, de responsabilidad civil, administradores y directivos, riesgos especiales, vida, accidentes y salud. (www.waprotection.com)

Watch&Act International Consulting, Consultora especializada en procesos de transformación digital con foco en las personas. (www.watchandact.eu)

C/ Puerto Rico 8 B

28016 Madrid España

Telf: +34 91 159 17 87

info@watchandact.eu

Índice

1.- Presentación

Presentamos por cuarto año consecutivo los resultados el ***IV informe - ranking de transparencia en ciberseguridad de las empresas del IBEX 35***

En esta edición, hemos añadido al ranking que venimos realizando, la denominación adicional de informe por cuanto que señalamos en el mismo una información que va más allá del ranking de las empresas y que hacen referencia a tendencias, normativas y evolución previsible en materia de ciberseguridad.

Seguimos en un entorno empresarial dinámico. La tecnología es ya parte de nuestras vidas, está en constante evolución creando una mayor dependencia de esta y en consecuencia aumentando los riesgos inherentes de la misma. Este año habrá casi el doble de dispositivos conectados (15 mil millones) que de personas en el mundo. *(1)*

La ciberseguridad ya no puede entenderse como una defensa estática frente a los ataques sino como una estrategia dinámica de protección empresarial y a nivel internacional. Reiteramos un año más, que las amenazas cibernéticas son cada vez más sofisticadas y van siempre por delante de nuestra capacidad de respuesta por lo que estamos obligados de ahora en adelante y más que nunca, a seguir realizando inversiones tanto técnicas como humanas en materia de ciberseguridad que nos protejan y minimicen el impacto económico de cualquier ataque. (Ver recomendaciones clave en materia de ciberseguridad. WEF Davos 2023) *(2)*

La transformación digital con la irrupción de la inteligencia artificial (IA), favorece y facilita la implementación de sistemas de protección a la vez que también da mayores posibilidades a las nuevas amenazas informáticas.

En el presente informe-ranking se han valorado unos indicadores recogidos de la normativa ISO 27001 y otros adicionales que se consideran de interés con el fin de evaluar la mejor transparencia en ciberseguridad publicada en los informes anuales de información no financiera de las empresas del IBEX 35.

Dos nuevos indicadores se han tenido en cuenta en la elaboración de este IV informe – ranking de transparencia que son: la mención de la existencia de una póliza de ciberriesgos y la mención específica de inversiones en materia de seguridad tecnológica o ciberseguridad.

Hay que indicar que esta transparencia de las empresas no solo cumple con las expectativas regulatorias, sino que también establecen un estándar para la excelencia en ciberseguridad, promoviendo así la seguridad y la confianza en el ecosistema empresarial en general.

Seguimos constatando que todavía nos queda mucho camino por recorrer en la transparencia de la información en ciberseguridad y así lo indica La Directiva 2014/95/UE del Parlamento Europeo y del Consejo, de 22 de octubre de 2014, por la que se modifica la Directiva 2013/34/UE en lo que respecta a la divulgación de información no financiera e información sobre diversidad por parte de determinadas grandes empresas y determinados grupos.

Javier Huergo.

Socio Director Watch&Act Protection Services

2.- Introducción al IV informe - ranking

El IV informe- ranking de transparencia en ciberseguridad de las empresas del IBEX 35 analiza y clasifica a las principales empresas españolas en función de su transparencia en la gestión de la ciberseguridad conforme a la información recogida en los:

Informes de sostenibilidad.

Informes integrados.

Informes de gestión consolidados.

Estados de información no financiera.

Informes anuales de gobierno corporativo.

La información recogida en estos informes es crucial para entender cómo las empresas comunican sus esfuerzos y políticas en ciberseguridad a sus accionistas, clientes y otras partes interesadas. El objetivo es identificar riesgos para mejorar la sostenibilidad y aumentar la confianza de los inversores, los consumidores y la sociedad en general y por lo tanto lograr una mayor divulgación de información no financiera. La directiva europea incluye información sobre los procedimientos de diligencia debida aplicados por la empresa, entendiendo por procedimientos de diligencia debida las actuaciones realizadas para identificar y evaluar los riesgos, así como para su verificación y control, incluyendo la adopción de medidas.

La resiliencia operativa digital del sector financiero (DORA), una nueva regulación única en Europa la cual entró en vigor el 17 de enero de 2023 y que será aplicable de forma directa a partir del próximo 17 de enero de 2025 para las entidades financieras y la Directiva NIS2 (Network and Information Systems Directive) para el resto de las empresas en general, le trasladan a estos órganos de administración de las empresas (consejos de administración y comités de dirección) una responsabilidad, vigilancia, control y obligatoriedad de información que les puede llevar a grandes sanciones con perjuicio en su patrimonio personal en caso de incumplimiento.

Con organizaciones de ciberdelincuencia cada vez más sofisticadas y difíciles de prever, la desinformación es un factor de riesgo importante. Con las nuevas normativas a la vista, los consejos de administración deben estar preparados para gestionar los riesgos cibernéticos y tecnológicos a medida que evolucionan. Previsiones sobre ciberriesgos para 2024 de Beazley *(3)*

3. Objetivos y alcance del IV informe – ranking

El objetivo principal del IV informe - ranking es, evaluar el nivel de transparencia de las empresas del IBEX 35 en cuanto a sus prácticas de ciberseguridad. Con este ranking no solo buscamos el mejor cumplimiento con las expectativas de divulgación, sino también fomentar la confianza entre los inversores, clientes, socios comerciales, proveedores y reguladores. La transparencia en ciberseguridad no solo es una muestra de responsabilidad corporativa, sino también un elemento clave para la gestión efectiva de los riesgos tecnológicos, la continuidad del negocio y por ende al valor de la empresa.

Para elaborar el análisis se ha revisado la información disponible en materia de ciberseguridad publicada en las respectivas webs de las empresas correspondiente al ejercicio fiscal 2023.

Este tipo de ranking busca de forma altruista fomentar la transparencia y la rendición de cuentas en el ámbito de la ciberseguridad con los siguientes objetivos específicos:

a) Cumplir con la normativa europea de transparencia.
   La Directiva 2014/95/UE del Parlamento Europeo y del Consejo, de 22 de octubre de 2014

b) Promover la transparencia:
   Fomentar un entorno empresarial donde la transparencia en ciberseguridad sea valorada por los accionistas y prioritaria como forma de gestión empresarial.

c) Reconocer buenas prácticas:
   Identificar y reconocer a las empresas que han implementado prácticas sólidas de ciberseguridad.

d) Incentivar y premiar las buenas prácticas:
   Establecer un reconocimiento a las buenas prácticas en comunicación que puedan tener un impacto directo en el valor y la reputación de la empresa.

e) Establecer un estándar de divulgación:
   Crear un estándar de referencia para la divulgación en ciberseguridad, alentando a las empresas a adoptar mejores prácticas en la comunicación de sus estrategias, políticas y acciones para mitigar riesgos cibernéticos.

f) Promover mejoras continuas:
   Motivar a las organizaciones a mejorar continuamente sus prácticas de ciberseguridad y su capacidad para comunicar de manera efectiva estas mejoras.

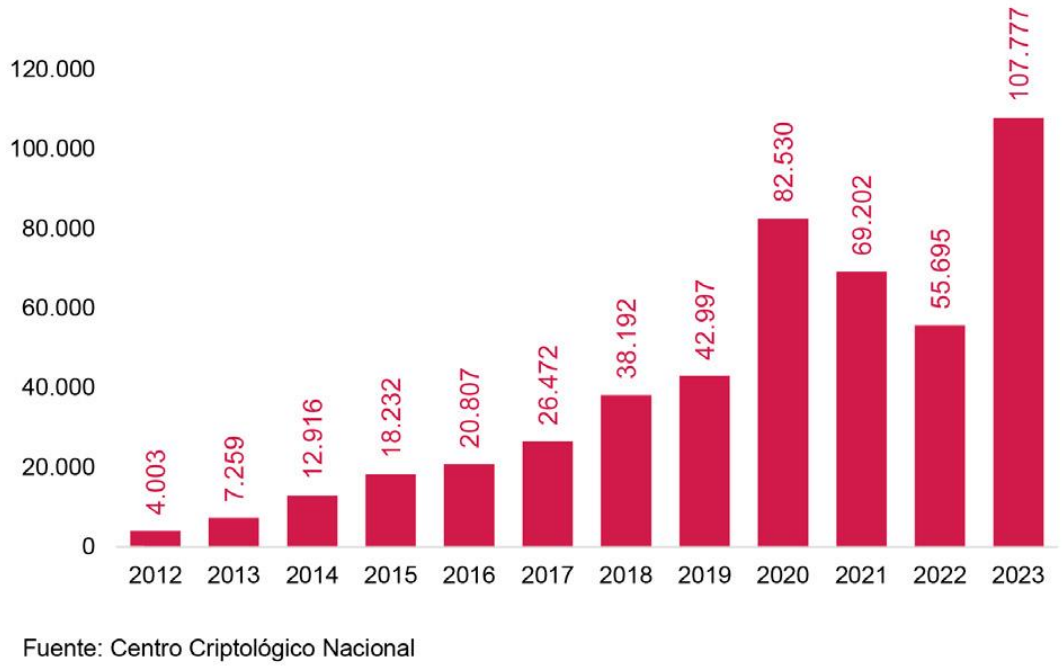
g) Facilitar la toma de decisiones de todos aquellos que son parte interesada de la empresa:
Proporcionar a empleados, inversores, clientes, socios comerciales, proveedores, gobierno y otros terceros una herramienta adicional valiosa para evaluar el cumplimiento de las normas de ciberseguridad y su implicación en el valor, solidez y sostenibilidad de la empresa.

h) Aumentar la conciencia sobre la importancia de la ciberseguridad:
La gran empresa ha de ser un ejemplo de buenas prácticas y promotor para el resto de las empresas de la importancia de la ciberseguridad.

i) Estimular competencia saludable y desarrollo de mejores prácticas:
Fomentar una competencia saludable entre las empresas para mejorar sus medidas de ciberseguridad y comunicar de manera efectiva sus esfuerzos. Esto contribuye al fortalecimiento general del panorama de la ciberseguridad empresarial.

4.- Contexto y tendencias en ciberseguridad

Según el Informe Anual de Seguridad Nacional,*(4)* en 2023 hubo en España un 94% más de ataques que en 2022; y en los primeros meses de 2024 se dio un aumento del 13,5% respecto a enero y febrero de 2023. Los ciberataques recibidos en España y gestionados por el Centro Criptológico Nacional (CNN-CERT) alcanzaron en el 2023 la cifra de 107.777 incidentes con un gran incremento en la criticidad de estos, que supera el 70%. El INCIBE y ESDF-CERT registraron 83.517 y 1.480 ataques respectivamente.



Número de ciber incidentes registrados por el CNN-CERT

El Instituto Nacional de Ciberseguridad (INCIBE), dependiente del Ministerio para la Transformación Digital y de la Función Pública, gestiona la defensa del ciberespacio, pero se centra en los ciberataques a empresas y sorprende ver que registró 83.517 ataques en 2023 que supone un 25% menos que en 2022. Entendemos que este descenso se debe a un menor número de incidencias reportadas por parte de las pequeñas y medianas empresas. Merece la pena destacar que 1.673 ataques tuvieron como objetivo la Red Académica IRIS, la red de comunicación de la comunidad científica y universitaria.

Según las estadísticas, en febrero de 2023, la ciberdelincuencia supuso el 20% de todos los delitos denunciados en España, y el 91,8% de las empresas españolas sufrió un ciberataque en 2022 *(5)* y según el Informe de Ciberpreparación de Hiscox 2024 *(6)* en los últimos 12 meses, el 96% de las empresas españolas ha sido blanco de ciberdelincuentes, ya sea con éxito o intentos fallidos. Además, el 66% de las empresas españolas encuestadas afirman haber visto un incremento en el número de veces que ha sufrido un ciberataque, mientras que solo un 12% ha visto un descenso. Por segundo año consecutivo, la pérdida financiera debido al fraude de desvío de pagos es la principal consecuencia de los ciberataques, afectando al 55% de las empresas españolas encuestadas. Además, la incidencia del ransomware ha aumentado, afectando al 38% de las empresas, en comparación con el 23% del año anterior.

Las estadísticas de ciberataques crecen de año en año y la criticidad de estos también a pesar de las iniciativas e inversiones en ciberseguridad que las empresas vienen realizando de forma creciente año a año. Cada día surgen nuevas amenazas en ciberseguridad y por lo tanto debemos encontrar nuevas formas de defenderse. La Inteligencia Artificial (IA) se postula como un pilar esencial para esa defensa y debe ser considerada como una de las principales iniciativas de aplicación en las empresas en los próximos años.

Fuente: Centro Criptológico Nacional

Criticidad de los ciber incidentes registrados por el CNN-CERT

Los ciberataques más comunes como son entre otros: el ransomware, malware, phishing, denegación de servicio (DDoS), troyanos, ataques de fuerza bruta, fraude al CEO, etc. constituyen amenazas no solo para las grandes empresas, sino también para las pymes. La red de contagio de estas amenazas en las empresas se extiende además por medio de

las empresas que formen parte de su cadena de suministro. Protegerse de los ciberataques es uno de los aspectos más importantes de las empresas conforme se refleja en la gran mayoría de las matrices de materialidad de las empresas del IBEX 35 en donde incluso algunas de ellas llegan a valorar el coste e impacto económico que supondría un ataque en sus sistemas.

Las grandes empresas son conscientes del problema y para ello están destinando cada año mayores presupuestos en soluciones y servicios de seguridad y en la formación en ciberseguridad en sus empresas. La inversión en IA generativa alcanzará los 25.200 millones de dólares en 2023, casi ocho veces más que en 2022. La explosión de la IA está en marcha según indican en la encuesta Risk & Resilience 2024 *(7)* elaborada por Beazley.

Se prevé que el gasto mundial en soluciones y servicios de seguridad sea de 219.000 millones de dólares en 2023, lo que representa un aumento del 12,1% en comparación con 2022, según IDC *(8).* Se espera que las inversiones en hardware, software y servicios relacionados con la ciberseguridad alcancen casi 300.000 millones en 2026, impulsadas por la amenaza continua de los ciberataques, las demandas de proporcionar un entorno de trabajo híbrido seguro y la necesidad de cumplir con los requisitos de gobernanza y privacidad de datos.

El Informe de Riesgos Globales 2023 *(9)* del Foro Económico Mundial (WEF), publicado en enero, situó a la ciberseguridad entre los 10 principales riesgos actuales y futuros a nivel mundial. Se prevé que el coste del cibercrimen a nivel mundial alcance 8 billones de dólares en 2023, según Cybersecurity Ventures *(10)* . Del mismo modo, los analistas de Gartner *(11)* predicen que en los próximos dos años, el 45% de las organizaciones globales se verán afectadas de alguna manera por un ataque a la cadena de suministro.

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) ahora identifica la eliminación de activos de TI *(12)* como un factor crítico a tener en cuenta al planificar la protección de las organizaciones contra ataques a la cadena de suministro de software .

Es de sobra conocido y así lo afirman las estadísticas de ataques reportados por las empresas, que el eslabón más débil de la cadena en materia de ciberseguridad corresponde a los empleados. El 80% de los ciberataques corporativos están dirigidos a los empleados. En un artículo publicado por CybersecurityNews *(13)* señala que Grant Thornton alertó de que, según la compañía, ocho de cada diez ataques cibernéticos que sufren las empresas están dirigidos a empleados, a través malware o phishing.

En este IV informe- ranking no se ha detectado una mejora en la información proporcionada por las empresas en materia de formación a sus empleados. No se ha sido suficientemente específico a la hora de informar el tipo de formación, los grupos de empleados y las horas destinadas a la materia de ciberseguridad.

5. Metodología: IV informe - ranking IBEX 35

La metodología del informe -ranking se basa en un análisis exhaustivo de los informes anuales de las empresas mediante una evaluación de la información disponible públicamente aplicando criterios de accesibilidad, visibilidad, calidad, actualización de la información conforme a los estándares de la ISO 27001 y otros de especial relevancia que creemos aportan claridad en la información debido a la evolución progresiva cambiante y acelerada que presenta el sector de la ciberseguridad.

Es el primer y único ranking que evalúa y puntúa, a partir de la información no financiera publicada, la evidencia de actuaciones que llevan a cabo las empresas con relación a la gestión de los riesgos de ciberseguridad para la protección de los datos sensibles de sus clientes, empleados y otras partes interesadas, así como para garantizar la integridad, confidencialidad y accesibilidad de la información**.**

Además de la accesibilidad, claridad y calidad de la información, se ha valorado muy positivamente la actualización de la información publicada. Es decir, mayor clarificación o aportación de evidencias con nuevas medidas que se han venido realizando durante el año.

Por ello, este año frente a los 12 criterios de evaluación establecidos el año anterior, se han añadido los dos criterios que el año anterior se valoraron en un punto adicional pero que en esta edición pasan a formar parte como criterios de relevancia por la información de especial interés que proporcionan en materia de ciberseguridad. Estos son:

- Mención de póliza de seguros de ciberriesgo.
- Mención de inversiones específicas en tecnología para la protección en ciberseguridad.

Los 14 criterios pueden alcanzar un total de 140 puntos. Cada criterio tiene una escala de puntuación de 0 a 10 con tres valores posibles intermedios de 2.5, 5 y 7 puntos en función de la calidad de la información proporcionada.

Adicionalmente hemos otorgamos un punto adicional a aquellas empresas que destacan por la claridad, accesibilidad y visibilidad de la información como es el caso entre otros de Fluidra (Reconocida por su Informe Anual Int. 2022 con el premio Art of Reporting)

La relación de criterios utilizados en la evaluación y elaboración del ranking son los siguientes:

1. **Responsable de ciberseguridad en la organización** con reporte directo a la alta dirección.

2. **Liderazgo de la alta dirección** con respecto al sistema de gestión de seguridad de la información.

3. **Establecimiento de la política de seguridad de la información** y referencia a procedimientos/protocolos que la desarrollen y que esté accesible en la web de la empresa.

4. **Gestión de los riesgos de ciberseguridad** por la comisión de riesgos que reporta a la alta dirección.

5. **Objetivos y planificación de las actuaciones** en seguridad de la información

6. **Certificación por normas internacionales / auditorías** por terceras partes.

7. **Existencia de un SOC** (Centro de Operaciones de Seguridad) o entidad similar para detectar, analizar, informar y corregir incidentes de seguridad.

8. **Concienciación y capacitación por medio de la formación** a los empleados en ciberseguridad.

9. **Cumplimiento obligaciones legales relativas a la seguridad de la información**

10. **Plan de continuidad de negocio** ante eventos disruptivos relacionados con la seguridad de la información.

11. **Mención de ataques cibernéticos recibidos, número y consecuencias de estos.**

12. **Medidas de control y requisitos en materia de ciberseguridad** exigidos **a proveedores** en la cadena de suministro.

13. **Mención de póliza de seguros de ciberriesgo.**

14. **Mención de inversiones específicas en tecnología para la protección frente a ataques informáticos (ciberseguridad).**

6. Resultados del IV informe -ranking

El resultado de este IV informe – ranking se presenta este año atendiendo a la clasificación de, transparentes, traslúcidas y opacas.

TRANSPARENTES: Este grupo lo integran aquellas empresas que obtienen entre 141 y 127,5 puntos			
1	AENA	141	=
	BANCO DE SANTANDER	141	↑
	BBVA	141	↑
	CAIXABANK	141	↑
	INDITEX	141	=
	TELEFÓNICA	141	=
7	MAPFRE	137,5	=
8	FLUIDRA	136	↑
9	FERROVIAL	135	=
10	ENAGÁS	127,5	↓
TRANSLÚCIDAS: Este grupo lo integran aquellas empresas que obtienen entre 127 y 100 puntos			
11	ENDESA	125	↑
	IBERDROLA	125	↑
	NATURGY	125	↓
14	MELIÁ	123,5	=
15	IAG	120	↓
16	INDRA	117,5	↓
17	GRIFOLS	112,5	↑
	REDEIA	112,5	↑
	REPSOL	112,5	↓
20	UNICAJA	110	↑
21	CELLNEX	107,5	=
22	ACCIONA	100	↑
	ACCIONA ENERGÍA	100	=
	AMADEUS	100	↓
OPACAS: Este grupo lo integran aquellas empresas que obtienen menos de 100 puntos			
25	BANKINTER	97,5	↓
26	BANCO DE SABADELL	96	=
	ACS	95	=
	SACYR	95	↓
29	MERLIN PROPERTIES	92,5	↑
30	COLONIAL	75	↓
31	ACERINOX	72,5	↑
32	LOGISTA	55	↓
	ROVI	55	=
	SOLARIA	55	↓
35	ARCELORMITTAL	0	↓

La muestra del ranking está constituida por las 35 empresas que conforman el índice bursátil IBEX 35 a diciembre de 2023

Es importante volver a aclarar que los resultados obtenidos a través de la evaluación realizada valoran exclusivamente la información publicada por lo que dicha valoración se tiene que utilizar para entender cómo es de transparente una empresa en la gestión relacionada con la ciberseguridad. En ningún caso se pretende hacer una valoración o auditoría de las medidas técnicas adoptadas por la empresa, las cuales entendemos, a la vista de lo que informan, son suficientes.

Los cambios más significativos se han producido en las tres principales entidades financieras que son: El BBVA, BANCO DE SANTANDER y CAIXABANK pasando a liderar el ranking de este año junto con AENA, INDITEX y TELEFÓNICA que continúan manteniendo su posición de cabeza en el ranking de transparencia.

La inclusión de nuevos indicadores junto con la evaluación completa de los añadidos en el año anterior indica una amplia visibilidad y toma de conciencia por parte de estas empresas en cuanto al significado, repercusión e impacto que esta información puede provocar en las cuentas de resultados de estas.

Es precisamente por la incorporación de estos nuevos indicadores por lo que empresas relevantes tales como NATURGY, IAG, INDRA REPSOL y AMADEUS retroceden en el ranking. al no proporcionar información alguna y se enmarcan en la clasificación de empresas translúcidas.

Una mayor información no financiera por parte de las empresas constituye un factor importante a la hora de garantizar un enfoque más a largo plazo, que debe ser fomentado y tenido en cuenta con el objetivo de identificar los riesgos para mejorar la sostenibilidad y aumentar la confianza de los inversores, los consumidores y la sociedad en general.

Por el extremo opuesto de la tabla y dentro de la clasificación de opacidad sigue cerrando un año más ARCELOR MITTAL que junto con LABORATORIOS ROVI y SOLARIA presentan un nivel de transparencia escaso o nulo.

Nos sorprende ver como todavía existen entidades financieras que no terminan de indicar las mejoras en materia de ciberseguridad que sin duda estamos convencidos las tienen y aplican.

La percepción generalizada es que aquellas empresas que han tomado conciencia de que su actividad es crítica y que son conocedores las consecuencias económicas y reputacionales de un ciber ataque han reflejado una mejor información.

En referencia a la clasificación por sectores, las empresas de finanzas y seguros han pasado a una primera posición relegando a un segundo lugar el liderato que tenía el sector de telecomunicaciones. Esto no quiere decir que estos últimos no hayan cumplido las expectativas previstas, sino que las empresas que lideran el ranking este año han proporcionado una mejor información en esta edición.

6.1.- Resultados por criterios

El porcentaje general de cumplimiento por criterios del conjunto de las empresas del IBEX 35 es de un 76% en donde merece la pena destacar:

Los criterios de liderazgo de la alta dirección, establecimiento de la política de seguridad de la información y procedimientos/protocolos y la gestión de los riesgos de ciberseguridad muestran la mayor ratio de cumplimiento frente al resto de indicadores situándose en un rango de entre un 97%-94%.

Es decir, todas las empresas son conscientes de la responsabilidad que se les está trasladando e imponiendo a los consejos de administración y los comités de dirección en la involucración activa y responsabilidad de la gestión de los riesgos de ciberseguridad bajo pena de sanciones y multas administrativas por omisión de ese deber de control. Ello implica de igual forma, el establecimiento de unas políticas claras de gestión y seguridad de la información.

Los nuevos criterios establecidos en el presente año, quizás por su incipiente necesidad, novedad o incluso temor de ser publicado han dado como resultado las peores ratios de cumplimiento. Nos referimos a la mención de póliza de seguros de ciberriesgo y a menciones de inversiones específicas en tecnología para la protección frente a ataques informáticos (ciberseguridad).

La transparencia en cuanto a los incidentes de seguridad con indicaciones específicas a la gravedad de estos sigue siendo baja con carácter general. El Reglamento General de Protección de Datos (RGPD) y las normativas europeas hacen hincapié en ese aspecto. En líneas generales, los departamentos de comunicación de las empresas del IBEX-35 gestionan adecuadamente la comunicación de los ataques relevantes sufridos, si bien la mención en las memorias sigue teniendo mucho margen de mejora.

6.2.- Resultados por sectores

El sector de las finanzas y seguros vuelve a su posición de liderazgo gracias a las buenas puntuaciones obtenidas por las tres principales instituciones financieras y la única aseguradora que cotiza en el IBEX- 35 que es MAPFRE.

Las empresas de telecomunicaciones a excepción de TELEFÓNICA quedan en un segundo lugar por los descensos en el ranking de AMADEUS e INDRA.

El sector de energía se mantiene en su tercera posición por las mejoras de ENDESA, IBERDROLA y REDEIA. Las empresas catalogadas en servicios de consumo también se mantienen en su cuarta posición por la consistencia de AENA y MELIÁ.

Bienes de consumo crece por la buena puntuación un año más de INDITEX

Construcción a pesar de las mejoras de FLUÍDRA, ACCIONA, ACERINOX y FERROVIAL se ve lastrada por caída de SACYR y ARCELORMITTAL

Inmobiliario sigue siendo el furgón de cola a pesar de la mejora de MERLÍN

RESULTADO POR SECTORES 2023

POSICIÓN	SECTOR
1	Finanzas y Seguros
2	Telecomunicaciones
3	Energía
4	Servicios de Consumo
5	Bienes de Consumo
6	Construcción
7	Inmobiliario

7.- Comparativa con informe de año anterior

Este apartado compara los resultados del IV informe con la edición anterior, mostrando la evolución de las empresas en términos de transparencia y destacando mejoras o retrocesos significativos.

La mejora es significativa frente al año anterior dado que a nivel porcentual de cumplimiento global de los indicadores se sitúa en un 83% frente al 76,5%. No obstante, con la inclusión de los dos nuevos indicadores, de la presente edición, hace decrecer el nivel de cumplimiento general hasta situarse a un 75,8%

A nivel de criterios individualizados, el grado de información mejora en todos los criterios con la excepción de la formación que desciende por el detalle de información publicada en las memorias. Hemos observados una menor definición en el número de horas, empleados o categorías profesionales y tipos de formación específica en ciberseguridad.

Comparativa por sectores de los últimos años:

RESULTADO POR SECTORES 2023	
POSICIÓN	SECTOR
1	Finanzas y Seguros
2	Telecomunicaciones
3	Energía
4	Servicios de Consumo
5	Bienes de Consumo
6	Construcción
7	Inmobiliario

RESULTADO POR SECTORES 2022	
POSICIÓN	SECTOR
1	Telecomunicaciones
2	Finanzas y Seguros
3	Energía
4	Servicios de Consumo
5	Construcción
6	Bienes de Consumo
7	Inmobiliario

RESULTADO POR SECTORES 2021	
POSICIÓN	SECTOR
1	Finanzas Seguros
2	Servicios de Consumo
3	Energía
4	Telecomunicaciones
5	Construcción
6	Bienes de Consumo
7	Inmobiliario

RESULTADO POR SECTORES 2020	
POSICIÓN	SECTOR
1	Telecomunicaciones
2	Servicios de Consumo
3	Finanzas Seguros
4	Bienes de Consumo
5	Energía
6	Construcción
7	Inmobiliario

8.- Conclusiones.

Como consecuencia de las crecientes amenazas en ciberseguridad que se viene produciendo desde años atrás, el gobierno español promulgó la Ley 11/2018, que exigía a las empresas del IBEX 35 incluir en sus estados de información no financiera anuales detalles sobre las medidas de ciberseguridad que aplicaban.

Esta ley tenía un doble propósito: aumentar la transparencia y asegurar que las empresas adoptaran prácticas robustas para protegerse contra los ciberataques.

La transparencia en lo que respecta a la divulgación de la información no financiera en los informes anuales en las empresas aparece publicada en la Directiva 2014/95/UE del Parlamento Europeo y del Consejo, de 22 de octubre de 2014 *(14)* y tiene como objetivo identificar riesgos para mejorar la sostenibilidad y aumentar la confianza de los inversores, los consumidores y la sociedad en general. Una mayor información no financiera por parte de las empresas constituye un factor importante a la hora de garantizar un enfoque más a largo plazo, que debe ser fomentado y tenido en cuenta.

Esta directiva afecta a la ciberseguridad de las empresas y se complementa con la necesidad de protección del patrimonio de las empresas, dando lugar a: un reglamento de Resiliencia Operativa Digital (DORA) de la Unión Europea *(15)* y a la Directiva NIS2 *(16)* (Network and Information Systems Directive) es una actualización de la Directiva NIS original.

Entre ambas establecen un marco para la gestión de los riesgos de las tecnologías de la información y la comunicación (TIC) en el sector financiero y unas pautas a seguir para mejorar la ciberseguridad en la Unión Europea ampliando los sectores, tipos de entidad y clasificación de entidades.

Los factores comunes a ambos y de aplicación afectan a:

- Identificación y evaluación de riesgos.
- Gestión de riesgos
- Cadena de suministro TIC
- Respuesta a incidentes
- Notificación de incidentes
- Divulgación coordinada de vulnerabilidades
- Sanciones más estrictas

Este IV Ranking de transparencia en ciberseguridad trata de poner de manifiesto la importancia y relevancia que otorgan las empresas del IBEX-35 a las actuaciones en ciberseguridad que llevan a cabo en sus empresas a tenor de la información publicada en sus informes anuales de información no financiera.

Por ello, destacamos los aspectos clave que en mayor o menor medida se han visto reflejados en la información publicada por estas empresas:

1) En la identificación, evaluación y gestión del riesgo resalta la implicación de los miembros de los Consejos de Administración y de los Comités de Dirección para un conocimiento y cumplimiento de la normativa en ciberseguridad**.** Indican una participación cada vez más activa aportando experiencia y formándose en materia de ciberseguridad**.**

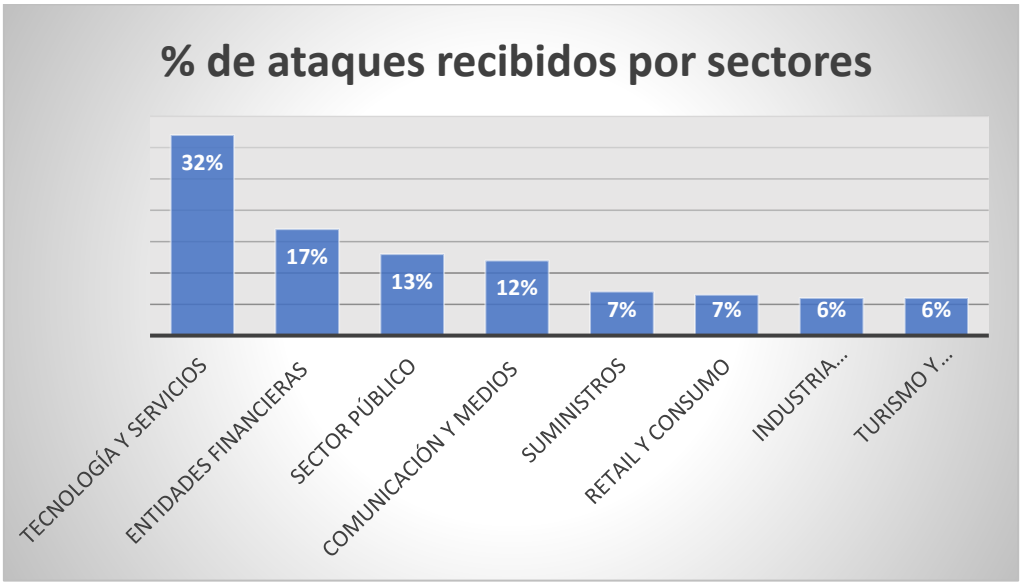
2) El alcance de la protección de la información de las empresas se ha ampliado enormemente. La información referida a las medidas de control en materia de ciberseguridad de terceras partes y en la cadena de suministro mejora frente a años anteriores dadas las posibles repercusiones económicas que ello conlleva

3) La puntuación relativa a la mención de incidentes y la formación**,** que son aspectos esenciales de la transparencia en ciberseguridad, empeora con respecto al año anterior. El nivel de detalle requerido no se ha considerado suficiente transparente. La divulgación coordinada en los reportes de información no financiera es un requisito esencial de las nuevas prácticas a implementar.

En resumen, el informe ofrece recomendaciones para que las empresas mejoren su transparencia en ciberseguridad, subrayando la importancia para la confianza de los inversores, empleados, proveedores y la resiliencia empresarial. Se enfatiza la necesidad de una mejora continua y la adopción de mejores prácticas.

9.- Recomendaciones.

Según el informe "Tendencias en ciberseguridad en España" elaborado por Mastercard *(17)* indica el siguiente porcentaje de ataques por sectores:



Fuente Mastercard

Este informe destaca que la información financiera, el principal objetivo de los ataques. Desde nuestro punto de vista, estos ataques tienen dos repercusiones de importancia:

a) Económicas

- Pérdidas Financieras Directas: Los ciberataques pueden resultar en pérdidas financieras significativas debido a fraudes, como el desvío de pagos. *(18)*.
- Costes de Recuperación: *(19)* Restaurar sistemas y datos afectados puede ser costoso.
- Interrupción de Operaciones

b) Las Reputacionales

- Pérdida de Confianza *(20)* La exposición de datos sensibles puede erosionar la confianza de los clientes y socios comerciales.
- Impacto en la Marca.*(21)*
- Multas y Sanciones

En resumen, un ciberataque no solo afecta las finanzas de una empresa, sino que también puede tener consecuencias duraderas en su reputación y capacidad para operar de manera efectiva. Por eso, es crucial que las empresas inviertan en medidas de ciberseguridad robustas y mantengan una cultura de seguridad proactiva.

"Más del 60% de las empresas españolas han incrementado sus presupuestos de Ciberseguridad. Esta área se afianza como una de las prioridades de las empresas en nuestro país, con un aumento en la inversión y la participación del CISO en el Comité de Dirección", explican desde Logicalis. De igual manera han identificado que el sector bancario ya destina cerca del 10% del gasto tecnológico en ciberseguridad.*(22)*

Por tanto, en esta nueva edición del informe- ranking de transparencia queremos hacer énfasis en dos recomendaciones de especial interés y actualidad:

1) **Un crecimiento significativo que seguiremos viendo con más y nuevas formas de ciberataques** junto con la interacción de la inteligencia artificial (IA) y la irrupción de la computación cuántica, obligará a las empresas a dotar de más medios y recursos económicos intrínsicamente destinados a la ciberseguridad**.**

2) **La búsqueda de alternativas en la transferencia de estos riesgos cibernéticos.**

   Entre las distintas medidas indicadas para como las empresas del IBEX 35 señalan la contratación de los seguros de ciber riesgo.*(23)*

En resumen, el informe ofrece recomendaciones para que las empresas mejoren su transparencia en ciberseguridad, subrayando la importancia para la confianza de los inversores, empleados, proveedores y la resiliencia empresarial. Se enfatiza la necesidad de una mejora continua y la adopción de mejores prácticas.

Referencias

(1) https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/
(2) https://www3.weforum.org/docs/WEF_State_of_the_Connected_World_2023_Edition.pdf Recomendaciones clave en materia de ciberseguridad. WEF Davos 2023)
(3) https://www.beazley.com/es-ES/cyber-services-snapshot/2024-cyber-risk-predictions Previsiones sobre ciberriesgos para 2024 de Beazley
(4) Informe Anual de Seguridad Nacional,
(5) https://www.comparitech.com/blog/information-security/spain-cyber-security-statistics/#:~:text=1.%2091.8%25%20of%20Spanish%20organizations%20were%20compromised%20in,Spanish%20companies%20had%20experienced%20a%20successful%20cyber%20attack.
(6) https://www.hiscox.es/informe-de-ciberpreparacion-de-hiscox-2024
(7) https://www.beazley.com/globalassets/cyber-tech-2024/cybertech_summary_es.pdf
(8) https://www.itdigitalsecurity.es/endpoint/2023/03/el-gasto-en-soluciones-de-ciberseguridad-alcanzara-los-300000-millones-de-dolares-en-2026
(9) https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf
(10) https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/
(11) https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends
(12) https://www.csoonline.com/article/570627/cisa-issues-guidance-on-defending-against-software-supply-chain-attacks.html
(13) Cybersecurity
(14) https://www.boe.es/doue/2014/330/L00001-00009.pdf
(15) https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81962
(16) https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963
(17) https://www.mastercard.com/news/europe/es-es/noticias/notas-de-prensa/es-es/2024/febrero-2024/las-empresas-de-tecnologia-financieras-y-el-sector-publico-concentran-el-62-de-los-ciberataques-en-espana/
(18) https://bigdatamagazine.es/perdida-economica-y-reputacional-principales-consecuencias-de-los-ciberataques/
(19) https://www.deloitte.com/es/es/services/risk-advisory/analysis/impacto-economico-wannacry.html
(20) https://bigdatamagazine.es/perdida-economica-y-reputacional-principales-consecuencias-de-los-ciberataques/
(21) https://www.expansion.com/empresas/banca/2024/08/27/66ccb1ec468aeb0a568b4589.html
(22) https://cybersecuritynews.es/el-sector-bancario-encabeza-la-inversion-en-concienciacion-en-materia-de-ciberseguridad/?utm_source=dmdelivery&utm_medium=email&utm_content=T%C3%ADtulo%20del%20link&utm_campaign=%7B%24mailingName%7D%20URL%20parameter%20pattern
(23) https://www.itdigitalsecurity.es/actualidad/2023/09/los-problemas-de-ciberseguridad-impulsan-la-contratacion-de-polizas-de-seguros

Glosario

AIE	Agencia Internacional de la Energía
ASG	Aspectos ambientales, sociales y de gobernanza
CAPEX	Capital Expenditures. Adquisición de inmovilizado material más activos intangibles
CDP	Carbon Disclosure Project
CHRB	Corporate Human Rights Benchmark
CNMV	Comisión Nacional del Mercado de Valores
COBIT	Control Objectives for Information and related Technology
COSO	Es un sistema de gestión de riesgo y control interno para cualquier organización. Se basa en un marco cuyo objetivo es diagnosticar problemas, generar los cambios necesarios para gestionarlos y evaluar la efectividad de estos.
COSO	Internal Control- Integrated Framework (Committee of Sponsoring Organizations of the Treadway Commission
DPO	Delegado de Protección de datos
ECOVADIS	Soluciones de sostenibilidad
EINF	Estado de Información no financiero Consolidado
EPICS	Edge Protection and Intelligent Control Solution.
EPRA	European Public Real Estate Association
EPRA Net Tangible Assets (NTA)	El cálculo de esta ratio es realizado asumiendo que la entidad compra y vende los activos inmobiliarios netos, materializando así ciertos niveles de pasivo por impuestos diferidos.
ESMA	Directrices de la European Securities Markets Authority
ESRS	(European Sustainability Reporting Standars)
FCA	Autoridad de Conducta Financiera
GRI Standards	Sustainability Reporting Standards. Guía del Global Reporting Initiative
ISO 31000	Señala una familia de normas sobre gestión del riesgo, normas codificadas por la International Organization for Standardization. El propósito de la norma ISO 31000:2009 es proporcionar principios y directrices para la gestión de riesgos y el proceso implementado en el nivel estratégico y operativo
K-ISMS	Es el sistema de gestión de la seguridad de la información de Corea del Sur
MAR	Medidas Alternativas de Rendimiento
MLPS	Es el esquema de protección multinivel. Se trata de un esquema regulatorio diseñado para proteger la ciberseguridad de las redes y sistemas en China
NPS	Net Promoter Score
ODS	Objetivos de Desarrollo Sostenible de Naciones Unidas
PERTE	Proyectos Estratégicos parala Recuperación y Tranformación Económica. i.e. Proyecto Vysinc (Virtual Synchronous compensator)
PRA	Autoridad de Regulación Prudencial
RAF	Instrumento para la implementación de la política de riesgos del Grupo y como una herramienta clave de gestión y control que le permite: formalizar la declaración de propensión al riesgo. UNICAJA

ROCE	Retorno del capital empleado. Del inglés Return on Capital Employed
RSC	Responsabilidad Social Corporativa
SAF	Uso y el suministro de combustible sostenible de aviación
SASB	Sustainability Accounting Standards Board
SCIIF	Sistema de Control Interno sobre la información financiera
TIBER-EU	Marco Europeo para la formación de equipos de respuesta éticos basados en la inteligencia de amenazas
TCFD	Divulgación de Información Financiera relacionada con el clima
TCFD	Task Force on Climate-related Financial Disclosures
WEF	World Economic Forum