INFORME

V INFORME - RANKING DE TRANSPARENCIA EN CIBERSEGURIDAD IBEX 35 - 2024

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

Por Javier Huergo

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

El **V informe - ranking de transparencia en ciberseguridad del IBEX 35** constituye una iniciativa pionera y de referencia en el análisis de la transparencia corporativa en materia de ciberseguridad de las principales empresas españolas cotizadas.

En un contexto global marcado por el incremento exponencial de las amenazas cibernéticas y la evolución acelerada del panorama regulatorio, la transparencia en ciberseguridad ha adquirido una dimensión estratégica fundamental para las organizaciones. Este quinto informe anual no solo mantiene su compromiso con el análisis riguroso y objetivo, sino que incorpora importantes novedades metodológicas y temáticas que reflejan las tendencias emergentes en el sector.

Las principales novedades del V Informe 2024 incluyen:

- Ampliación del marco de evaluación de 14 a 16 criterios de análisis.
- Incorporación de un nuevo criterio específico sobre el uso de Inteligencia Artificial ciberseguridad.
- Indicación o mención del cumplimiento de la nueva regulación europea: NIS2, DORA y la Ley de Ciberresiliencia
- Análisis de la dotación de recursos humanos en departamentos de ciberseguridad

La metodología se mantiene fundamentada en el análisis exhaustivo de la información no financiera publicada por las empresas del IBEX 35, garantizando la objetividad y comparabilidad de los resultados. El informe continúa siendo el único ranking en España que evalúa específicamente la transparencia en ciberseguridad basándose exclusivamente en información pública corporativa.

La ciberseguridad se ha convertido en un factor crítico no solo para la protección de los activos digitales de la compañía, sino también para la estabilidad financiera y la reputación corporativa.

Los indicadores de ciberseguridad ponen de manifiesto las medidas de protección y alertan de los posibles costes financieros derivados de incidencias y brechas de seguridad.

Entendemos por tanto que estos indicadores han de formar parte del reporte y seguimiento que realizan los órganos de gobierno responsables en esta materia.

Las empresas deben exigir a sus directivos y empleados un compromiso sólido en gestión de la ciberseguridad con el objetivo de proteger los activos del negocio y mitigar riesgos financieros que afecten al valor de las empresas.

Finalmente he de indicar que este informe se dirige a múltiples audiencias: directivos y consejos de administración que buscan benchmarking sectorial, inversores que requieren información para la toma de decisiones, las propias empresas analizadas que les permite acceder a ventajas competitivas de financiación en el supuesto de correcto cumplimiento, reguladores interesados en el cumplimiento normativo y la comunidad académica y profesional especializada en ciberseguridad.

Javier Huergo.

Socio Director Watch&Act Protection Services

2.- Introducción al V informe - ranking

El V informe-ranking de transparencia en ciberseguridad de las empresas del IBEX 35 constituye la evolución natural de una metodología consolidada que ha demostrado su valor como herramienta de análisis y benchmarking durante cinco ediciones consecutivas. Este informe analiza y clasifica a las principales empresas españolas en función de su transparencia en la gestión de la ciberseguridad, basándose en la información divulgada públicamente a través de sus informes corporativos.

La información objeto de análisis se obtiene de los siguientes documentos corporativos correspondientes al ejercicio fiscal 2024:

- Informes de sostenibilidad y ESG
- Informes integrados anuales
- Informes de gestión consolidados
- Estados de información no financiera
- Informes anuales de gobierno corporativo
- Memorias anuales y documentos de registro universal

La relevancia de esta información radica en su capacidad para reflejar el compromiso real de las empresas con la transparencia en ciberseguridad ante sus grupos de interés. Estos documentos constituyen el canal oficial de comunicación corporativa hacia accionistas, inversores, reguladores, clientes y la sociedad en general, siendo por tanto el medio más fidedigno para evaluar el nivel de divulgación en materia de ciberseguridad.

El V informe incorpora importantes evoluciones metodológicas que responden a los cambios del entorno regulatorio y tecnológico:

- Ampliación del marco de evaluación: Se han incorporado dos nuevos criterios que elevan el total de 14 a 16 criterios de análisis, aumentando la puntuación máxima de 140 a 160 puntos.
- Adaptación regulatoria: El marco de evaluación se ha actualizado para reflejar el cumplimiento de las nuevas normativas europeas NIS2, DORA y la Ley de Ciberresiliencia de la UE, así como la actualización de la Estrategia Nacional de Ciberseguridad 2024.
- Enfoque en tendencias emergentes: Se han añadido criterios específicos para evaluar la adopción de inteligencia artificial en ciberseguridad y la transparencia en la dotación de recursos humanos especializados.

Esta evolución metodológica mantiene la comparabilidad histórica mientras incorpora los desarrollos más relevantes del ecosistema de ciberseguridad empresarial, garantizando que el ranking continúe siendo una herramienta de referencia para la evaluación de la transparencia en ciberseguridad.

3.- Objetivos y alcance del V informe - ranking

El objetivo principal del V informe-ranking es evaluar de manera objetiva y sistemática el nivel de transparencia de las empresas del IBEX 35 en cuanto a sus prácticas de ciberseguridad. Este ranking trasciende la mera clasificación para constituirse en una herramienta integral que fomenta la transparencia, la responsabilidad corporativa y la excelencia en la comunicación de aspectos críticos para la sostenibilidad empresarial.

La metodología aplicada se fundamenta en la revisión exhaustiva de la información disponible públicamente en materia de ciberseguridad, publicada por las empresas correspondiente al ejercicio fiscal 2024, garantizando la objetividad y comparabilidad de los resultados obtenidos.

Objetivos Específicos

Objetivo	Descripción
Promoción de transparencia	Fomentar un entorno empresarial donde la transparencia en ciberseguridad sea valorada por los accionistas y constituya una prioridad estratégica en la gestión empresarial.
Reconocimiento de buenas prácticas	Identificar y reconocer públicamente a las empresas que han implementado y comunicado de manera efectiva prácticas sólidas de ciberseguridad.
Incentivo a la excelencia	Establecer un sistema de reconocimiento que genere un impacto positivo directo en el valor y la reputación empresarial, incentivando la mejora continua.
Establecimiento de estándares	Crear un marco de referencia para la divulgación en ciberseguridad, promoviendo la adopción de mejores prácticas en la comunicación de estrategias, políticas y acciones.
Mejora continua	Motivar a las organizaciones a perfeccionar continuamente sus prácticas de ciberseguridad y su capacidad de comunicación efectiva.
Facilitar toma de decisiones	Proporcionar a empleados, inversores, clientes, proveedores, reguladores y accionistas una herramienta valiosa para evaluar el cumplimiento y la solidez empresarial.
Concienciación sectorial	Posicionar a la gran empresa como ejemplo y promotor de la importancia de la ciberseguridad en el tejido empresarial español.
Competencia saludable	Estimular una competencia constructiva entre las empresas para mejorar sus medidas de ciberseguridad y comunicar efectivamente sus esfuerzos.

Alcance y limitaciones

Universo de análisis: Las 35 empresas que componen el índice IBEX 35 a fecha de cierre del ejercicio 2024.

Fuentes de información: Exclusivamente documentos de información pública corporativa oficial publicados por las empresas en sus portales web y registros oficiales.

Período de análisis: Información correspondiente al ejercicio fiscal 2024, con fecha límite de recopilación a 31 de diciembre de 2024.

Criterios de evaluación: 16 criterios específicos de ciberseguridad con puntuación de 0 a 10 puntos cada uno, totalizando 160 puntos máximos.

Limitaciones: El análisis se circunscribe a la información divulgada públicamente, no evaluando las capacidades reales de ciberseguridad ni la efectividad de las medidas implementadas, sino exclusivamente la transparencia en su comunicación.

4.- Contexto y tendencias en ciberseguridad

El panorama de la ciberseguridad empresarial ha experimentado una transformación acelerada durante los últimos años, caracterizada por la convergencia de múltiples factores: la evolución de las amenazas cibernéticas, la revolución de la inteligencia artificial, los cambios regulatorios europeos y la consolidación de nuevos modelos de trabajo. Este contexto dinámico configura un escenario complejo que requiere de las empresas una adaptación continua de sus estrategias de seguridad y transparencia.

Evolución del panorama regulatorio europeo

El año 2024 marca un hito en la regulación europea de ciberseguridad con la entrada en vigor de marcos normativos que redefinen las obligaciones empresariales:

NIS2 (Directiva UE 2022/2555): Fecha de aplicación: octubre 2024. Amplía significativamente el alcance de la regulación de ciberseguridad, incorporando nuevos sectores y estableciendo requisitos más estrictos para la gestión de riesgos, notificación de incidentes y responsabilidades directivas. Su transposición al ordenamiento nacional español implica nuevas obligaciones de reporte y transparencia.

DORA (Reglamento UE 2022/2554): Fecha de aplicación: enero 2025. Específico para el sector financiero, establece un marco integral de resiliencia operativa digital que incluye requisitos detallados de gestión de riesgos de TIC, pruebas de resiliencia y supervisión de terceros críticos.

Ley de Ciberresiliencia de la UE: Fecha de aplicación: 2024 – 2027 gradual. En fase de implementación, esta regulación establecerá requisitos de ciberseguridad para productos con elementos digitales, impactando en las cadenas de suministro y la gestión de terceros.

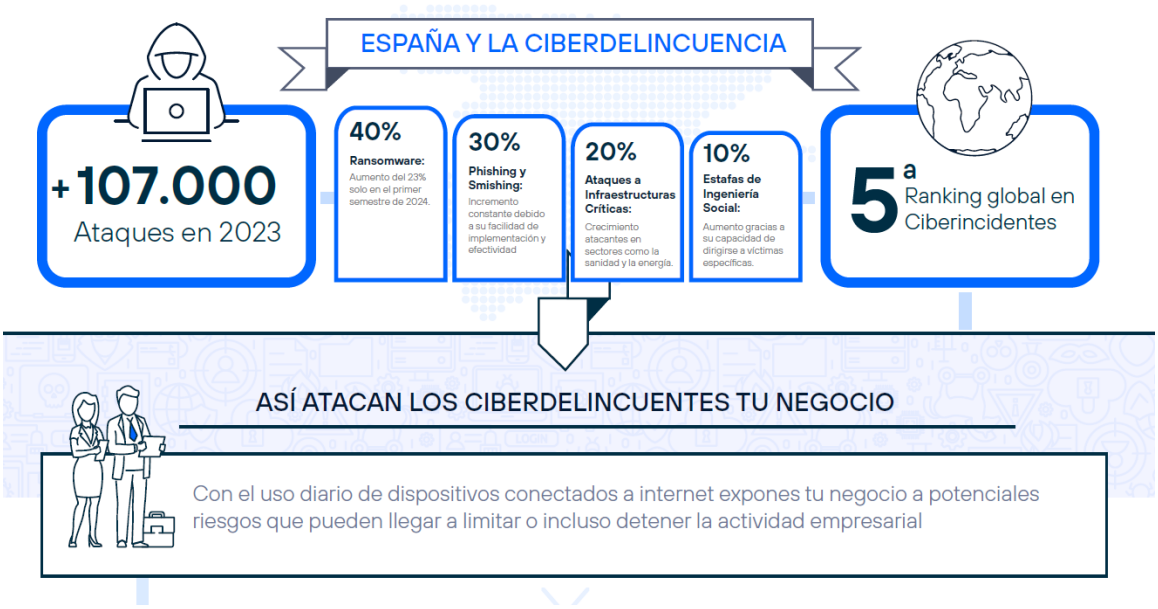
Estrategia Nacional de Ciberseguridad 2024: La actualización de la estrategia nacional española incorpora nuevos objetivos de transparencia y colaboración público-privada, alineándose con las directrices europeas.

Estas regulaciones no solo establecen nuevos requisitos de cumplimiento, sino que elevan las expectativas de transparencia y reporte, elementos centrales en la evaluación del presente ranking.

Amenazas emergentes y tendencias tecnológicas

Según indica el informe de Control Risks para la aseguradora QBE (1) revela que "los **ciberataques significativos y exitosos aumentaron un 42% en Europa y Norteamérica** entre 2023 y 2024, impulsados por factores geopolíticos como la guerra en Ucrania. A nivel mundial, los ciberataques estratégicamente disruptivos se duplicaron, pasando de 103 en 2020 a 196 en 2024, y se prevé que aumenten aproximadamente un 20 %, hasta alcanzar los 233, para finales de 2025.

Conforme publicación de Seguros News de junio de 2025 (2) el **52% de las empresas con entre 100 y 2.000 empleados sufrió un ciberataque** durante el último año. Para una de cada siete (14%), el ciberataque provocó una interrupción de un día laboral o más.

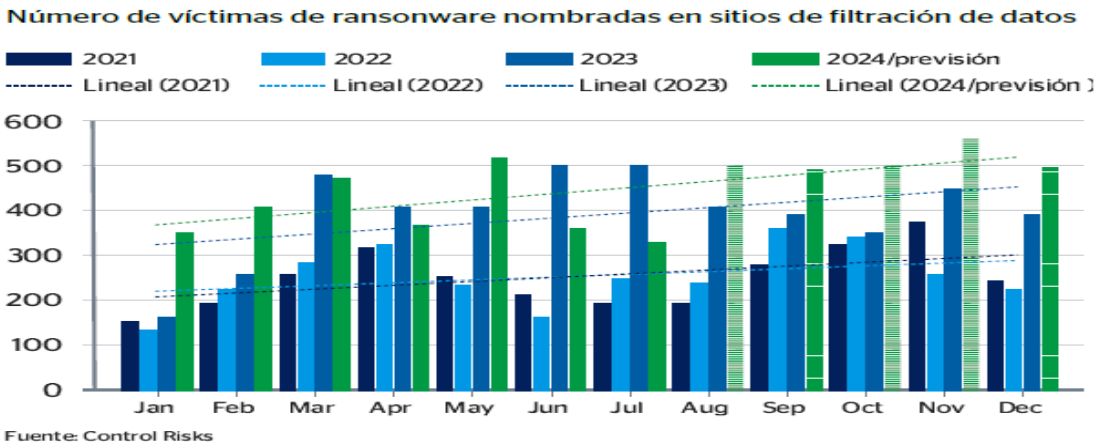


Fuente: Instituto Nacional de Ciberseguridad (INCIBE), Centro de Respuesta a Incidentes de Seguridad e Industria (CERTSI), Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC),

En el caso de **España**, el porcentaje aumenta hasta el **53%.**, aunque cae hasta el 9% el porcentaje de las empresas que dicen haber sufrido la interrupción laboral de un día o más. Entre quienes sufrieron ciberataques, tres de cada cinco (59%) afirmaron que al menos uno de ellos estaba **vinculado a un proveedor**, y casi la mitad (49%) sufrió una **pérdida de ingresos.** Señalar a modo de ejemplo los datos que publica Health-ISAC (3) donde señala que en el último año, el 92% de las organizaciones sanitarias sufrieron al menos un incidente, con más de **276 millones de registros médicos comprometidos en todo el mundo**.

El ecosistema de amenazas ha evolucionado hacia formas más sofisticadas y dirigidas:

Ransomware como servicio (RaaS): La industrialización del ransomware ha democratizado el acceso a herramientas avanzadas, incrementando el número y la sofisticación de los ataques. En el 2023 crecieron un 74% respecto a 2022



Número de víctimas nombradas públicamente por grupos de extorsión de *ransomware* y filtración de datos

2021	2022	2023	2024 (previsión)	2025 (previsión)
2964	2981	4698	4800	5200

Fuente: Control Risk

Ataques a la cadena de suministro: Los incidentes como SolarWinds han evidenciado la vulnerabilidad de las cadenas de suministro digitales, elevando la importancia de la gestión de terceros.

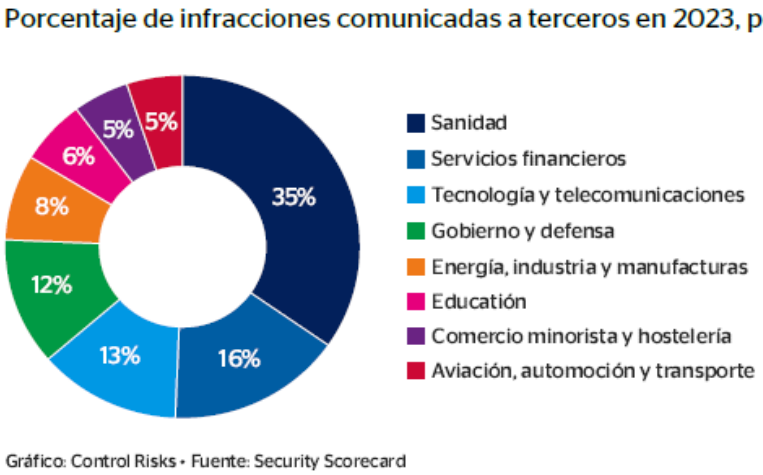


Gráfico: Control Risks • Fuente: Security Scorecard

Deepfakes y manipulación de IA: La utilización maliciosa de tecnologías de IA genera nuevos vectores de ataque, desde campañas de desinformación hasta fraudes financieros sofisticados.

Fuente: Telefónica Seguros

Ataques a infraestructuras críticas: El incremento de ataques dirigidos a infraestructuras esenciales ha elevado la conciencia sobre la ciberseguridad nacional y sectorial.

Criptominería maliciosa: La proliferación de ataques dirigidos a la instalación de software de minería de criptomonedas en sistemas empresariales.

Estas tendencias requieren de las empresas una adaptación continua de sus estrategias defensivas y una comunicación transparente sobre las medidas adoptadas para mitigar estos riesgos emergentes.

Fuente: Telefónica Seguros

Fuente: Global Corporate IT Security Risk survey, B2B International with Kaspersky Lab, Eset,

5.- Metodología: V informe - ranking IBEX 35

La metodología del V informe-ranking se fundamenta en un análisis exhaustivo y sistemático de los informes anuales y documentos corporativos de las empresas del IBEX 35. Este enfoque garantiza la objetividad, reproducibilidad y comparabilidad de los resultados, basándose exclusivamente en información de carácter público y oficial.

El V informe representa una evolución metodológica significativa respecto a ediciones anteriores, incorporando las lecciones aprendidas durante cinco años de análisis y adaptándose a los cambios del entorno regulatorio y tecnológico. La metodología se caracteriza por su rigor analítico, transparencia en los criterios de evaluación y enfoque integral de la ciberseguridad empresarial.

Principios metodológicos

El marco metodológico se sustenta en los siguientes principios fundamentales:

- **Objetividad**: La evaluación se basa exclusivamente en evidencias documentales disponibles públicamente, eliminando la subjetividad en la valoración.
- **Transparencia**: Todos los criterios de evaluación, escalas de puntuación y procedimientos de análisis son públicos y replicables.
- **Comparabilidad**: La metodología permite la comparación tanto entre empresas como la evolución temporal de cada organización.
- **Exhaustividad**: El análisis abarca múltiples dimensiones de la ciberseguridad empresarial, desde la gobernanza hasta la implementación operativa.
- **Actualización continua**: La metodología se actualiza anualmente para incorporar las mejores prácticas y cambios regulatorios relevantes.
- **Accesibilidad**: Los resultados se presentan de manera comprensible para múltiples audiencias, desde especialistas técnicos hasta inversores y reguladores.

Fuentes de información

La evaluación se basa en el análisis de los siguientes documentos corporativos oficiales correspondientes al ejercicio fiscal 2024:

- Informes Integrados Anuales: Informes que combinan información financiera y no financiera, proporcionando una visión holística de la gestión empresarial.
- Informes de Gestión Consolidados: Documentos que acompañan a las cuentas anuales consolidadas, incluyendo información sobre riesgos y medidas de control.
- Estados de Información No Financiera: Documentos específicos requeridos por la normativa europea para empresas de gran dimensión.
- Informes de Sostenibilidad y ESG: Documentos específicos de sostenibilidad que incluyen información sobre ciberseguridad como componente de la gestión de riesgos ESG
- Informes Anuales de Gobierno Corporativo: Documentos que detallan las estructuras de gobierno y control interno, incluyendo aspectos de ciberseguridad.
- Memorias Anuales y Documentos de Registro Universal: Información completa sobre la actividad empresarial y sus riesgos asociados.

Criterios de inclusión: Se consideran válidos únicamente los documentos oficiales publicados por las empresas en sus portales web corporativos, registros oficiales o comunicaciones a organismos reguladores.

Período de referencia: Información correspondiente al ejercicio fiscal 2024.

Marco de Evaluación: 16 Criterios del V Informe

El V informe incorpora un marco de evaluación ampliado que consta de 16 criterios específicos, organizados en cuatro categorías temáticas que abarcan de manera integral los aspectos más relevantes de la ciberseguridad empresarial. Esta estructura permite una evaluación sistemática y equilibrada de diferentes dimensiones de la transparencia en ciberseguridad.

Estructura de criterios por categorías

Categoría	Criterios	Descripción	Puntos
A: GOBERNANZA Y LIDERAZGO	1-4	Estructura organizacional, liderazgo directivo, políticas corporativas y gestión integrada de riesgos	40
B: ESTRATEGIA Y OPERACIONES	5-8	Planificación estratégica, certificaciones, capacidades operativas y formación	40
C: CUMPLIMIENTO Y CONTINUIDAD	9-10	Cumplimiento normativo y planes de continuidad de negocio	20
D: TRANSPARENCIA E INNOVACIÓN	11-16	Comunicación de incidentes, gestión de terceros, inversiones, seguros, IA y recursos humanos	60

Sistema de puntuación

El sistema de puntuación del V informe se basa en una escala granular que permite capturar diferentes niveles de calidad y exhaustividad en la información divulgada:

Puntuación máxima total: 160 puntos (16 criterios × 10 puntos)
Escala por criterio: 0 - 2.5 - 5 - 7 - 10 puntos

Criterios de puntuación:

• 0 puntos: Ausencia total de información sobre el criterio evaluado
• 2.5 puntos: Mención básica o información muy limitada
• 5 puntos: Información presente pero incompleta o poco detallada
• 7 puntos: Información adecuada con algunos aspectos detallados
• 10 puntos: Información completa, detallada y de alta calidad

Clasificación final de empresas:

- TRANSPARENTES: 130-160 puntos
- TRANSLÚCIDAS: 100-129 puntos
- OPACAS: <100 puntos

Novedades Metodológicas del V Informe 2024

El V informe incorpora importantes innovaciones metodológicas que reflejan la evolución del ecosistema de ciberseguridad:

Nuevos criterios incorporados:

Criterio 15 - Mención del uso de Inteligencia Artificial en ciberseguridad: Evalúa la transparencia en la comunicación sobre la implementación de tecnologías de IA para la mejora de las capacidades de ciberseguridad, incluyendo sistemas de detección automática, análisis predictivo y respuesta automatizada a incidentes.

Criterio 16 - Mención del número de personas que trabajan en el departamento de ciberseguridad:
Valora la divulgación de información cuantitativa sobre los recursos humanos dedicados específicamente a ciberseguridad, reflejando el compromiso organizacional con esta área estratégica.

Esta evolución metodológica garantiza que el V informe mantenga su relevancia como herramienta de análisis y benchmarking en un entorno regulatorio y tecnológico en constante evolución.

6.- Resultados del V Ranking 2024

El V Ranking de Transparencia en Ciberseguridad del IBEX 35 presenta resultados que reflejan tanto la evolución progresiva de la transparencia corporativa en España como los desafíos que persisten en la comunicación efectiva de las estrategias de ciberseguridad. Los resultados obtenidos en esta edición 2024 evidencian un panorama diversificado, con empresas que han alcanzado niveles de excelencia en transparencia, mientras otras mantienen oportunidades significativas de mejora.

IV RANKING DE TRANSPARENCIA EN CIBERSEGURIDAD

TRANSPARENTES: Este grupo lo integran aquellas empresas que obtienen entre 160 y 130 puntos			
1	CAIXABANK	160	=
1	FERROVIAL	160	↑
1	FLUIDRA	160	↑
1	INDITEX	160	=
2	MAPFRE	152,5	=
2	INDRA	150	↑
3	BBVA	147,5	↓
4	B. SANTANDER	145	↓
4	ENAGAS	145	↑
4	MELIÁ	145	↑
5	AENA	140	↓
5	TELEFÓNICA	140	↓
6	REDEIA	137,5	↑
7	CELLNEX	135	↑
7	NATURGY	135	↓
8	ACS	130	↑
8	AMADEUS	130	↑
8	GRIFOLS	130	↑
TRANSLÚCIDAS: Este grupo lo integran aquellas empresas que obtienen entre 127,5 y 100 puntos			
9	B. SABADELL	127,5	↑
10	ACCIONA ENERGÍA	122,5	↑
10	BANKINTER	122,5	↑
11	REPSOL	115	↓
12	ACCIONA	112,5	↑
14	MERLIN PR	107,5	↑
15	IAG	105	↓
16	UNICAJA	100	↓
16	IBERDROLA	100	↓
OPACAS: Este grupo lo integran aquellas empresas que obtienen menos de 100 puntos			
17	SOLARIA	95	↑
18	ENDESA	75	↓
19	COLONIAL IN	72,5	↓
20	ACERINOX	62,5	↓
21	LOGISTA	50	↓
22	ROVI	40	↓
23	SACYR	25	↓
24	PUIG BRANDS	20	=

El análisis se basa en la evaluación de 16 criterios específicos aplicados a las 35 empresas del IBEX 35, utilizando información pública correspondiente al ejercicio fiscal 2024. La puntuación total posible de 160 puntos permite una clasificación granular que distingue entre empresas transparentes (160-130 puntos), translúcidas (129-100 puntos) y opacas (<100 puntos).

Merece la pena destacar en el presente ranking el liderazgo mantenido un año más por CAIXABANK e INDITEX y los ascensos de FERROVIAL y FLUIDRA al pódium de los mejores.

MAPFRE se mantiene un año más en la segunda posición y señalamos mejoras significativas en INDRA y ACS que, junto con ENAGÁS, MELIÁ, REDEIA Y CELLNEX mejoran su posicionamiento en el ranking con respecto al año anterior.

En resumen, observamos un equilibrio competitivo en dónde es el mismo número de empresas las que mejoran frente a las que retroceden. Preocupa la alta volatilidad de algunas de ellas, en donde encontramos empresas que han perdido liderazgo e incluso han sufrido retrocesos severos.

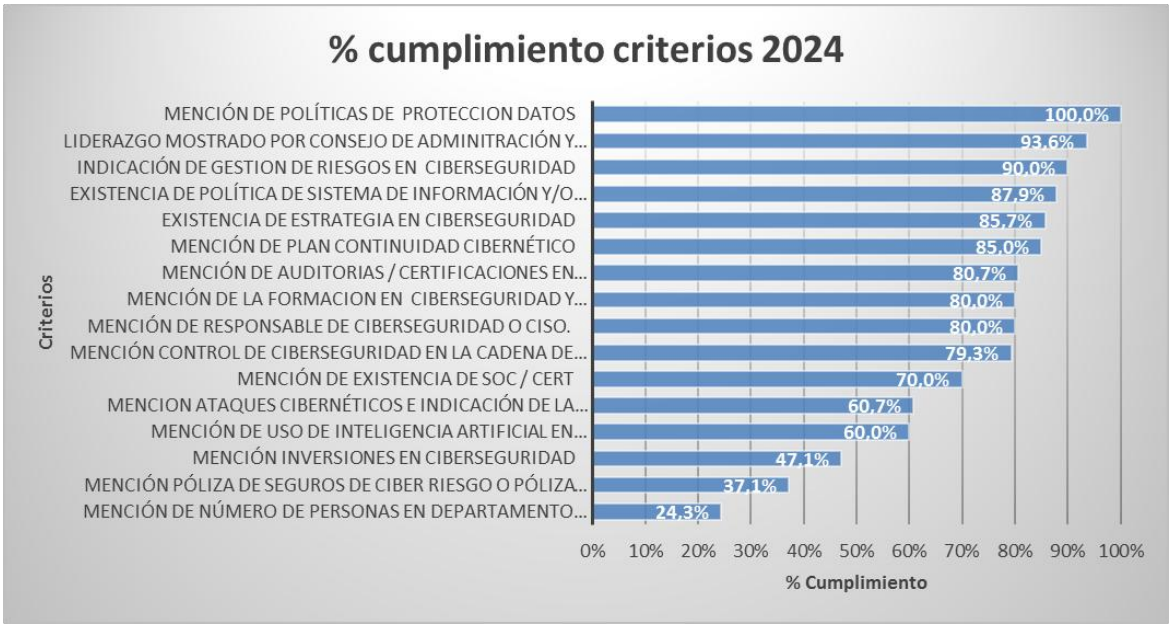
Los resultados de esta edición reflejan un entorno muy dinámico en donde el impacto de las nuevas exigencias regulatorias, la incorporación de tecnologías emergentes como la inteligencia artificial, y la creciente concienciación sobre la importancia estratégica de la ciberseguridad en el entorno empresarial español obliga a una mejora continua para mantener posiciones de transparencia.

6.1.- Análisis de resultados por criterios

El análisis por criterios revela patrones significativos en la transparencia de las empresas del IBEX 35, identificando fortalezas consolidadas y áreas que requieren atención prioritaria. La evaluación de los 16 criterios específicos proporciona una radiografía detallada del estado de la transparencia en ciberseguridad en el mercado español.

Criterios con mayor nivel de transparencia

Los análisis identifican varios criterios donde las empresas del IBEX 35 demuestran niveles elevados de transparencia:

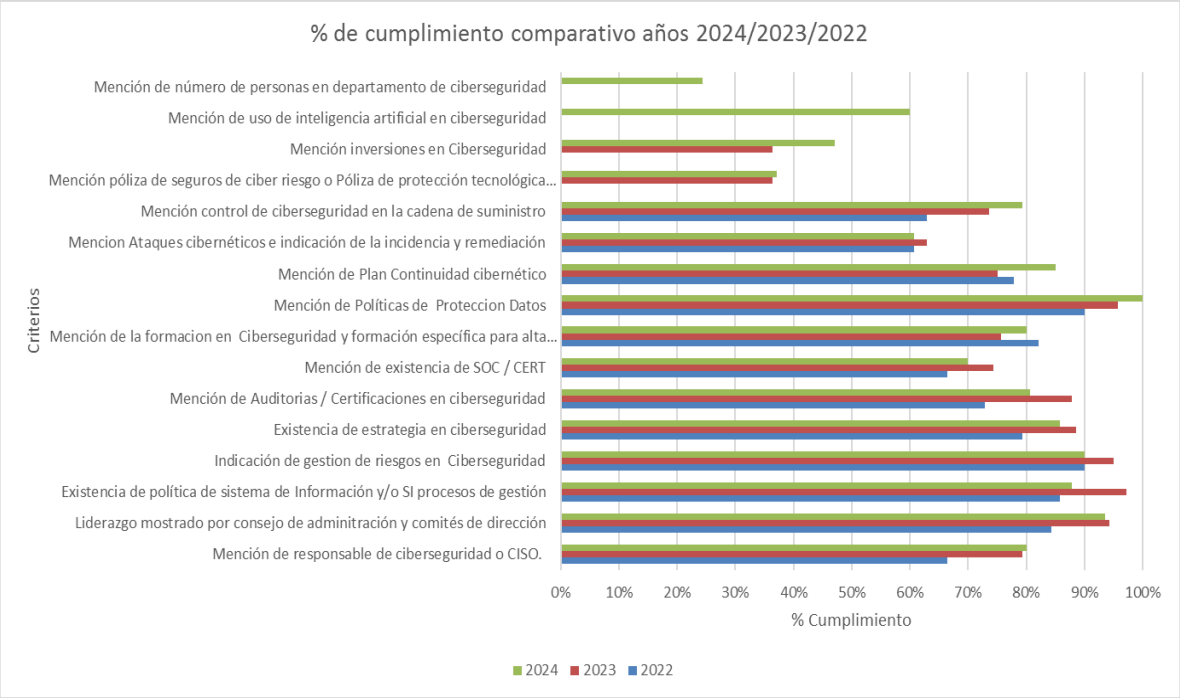


Criterio 2 – Liderazgo de la alta dirección. El 93,6% de las empresas son conscientes de la importancia del cumplimiento de este criterio y así lo reflejan de forma mayoritaria. La nueva normativa en ciberseguridad es muy exigente en el cumplimiento de este criterio.

Criterio 3 - Política de Seguridad de la Información: El 87,9% de las empresas analizadas publican alguna forma de política de seguridad, aunque la calidad y detalle varía significativamente. Las empresas del sector financiero lideran esta categoría con políticas comprehensivas y actualizadas.

Criterio 4 – Gestión de riesgos de ciberseguridad: El 90% de las empresas analizadas hacen referencia de forma específica en el capítulo de gestión de riesgos globales de la empresa a la ciberseguridad.

Criterio 9 - Cumplimiento de Obligaciones Legales: El 100% de las empresas mencionan explícitamente el cumplimiento del RGPD., aunque la referencia a otras normativas como NIS2 o DORA es aún limitada, lo que representa una oportunidad de mejora significativa.



Criterios con oportunidades de mejora

Varios criterios evidencian oportunidades significativas de mejora en transparencia:

Criterio 6 - Certificaciones y Cumplimiento Normativo: El 80,7% de las empresas reportan certificaciones específicas de ciberseguridad, siendo ISO 27001 la más prevalente, aunque insistimos que la referencia a otras normativas como NIS2 o DORA es aún limitada, lo que representa una oportunidad de mejora significativa. La transparencia en este criterio ha mostrado una mejora sostenida durante los últimos tres años.

Criterio 11 - Transparencia en incidentes de seguridad: Solo el 60,7% de las empresas comunican de manera proactiva incidentes de ciberseguridad. Esta baja transparencia contrasta con las mejores prácticas internacionales y las expectativas de los clientes, accionistas, proveedores, inversores y empleados.

Criterio 13 - Seguros de ciberriesgo: El 37,1% de las empresas mencionen la contratación de pólizas específicas de ciberriesgo, y aunque somos conocedores de la concienciación que tienen las empresas del IBEX 35 sobre la transferencia de estos riesgos cibernéticos, la gran mayoría no son transparentes en este criterio por temores infundados de efecto llamada para ciberdelincuentes.

Criterio 15 - Uso de inteligencia artificial en ciberseguridad (NUEVO): Únicamente el 60% de las empresas mencionan específicamente el uso de IA en sus estrategias de ciberseguridad, a pesar de la creciente adopción de estas tecnologías en el sector.

Criterio 16 - Recursos Humanos en Ciberseguridad (NUEVO): Solo el 24,3% de las empresas divulgan información cuantitativa sobre su dotación de personal especializado en ciberseguridad, limitando la capacidad de evaluación de los inversores sobre los recursos destinados a esta área crítica.

Impacto de las nuevas regulaciones

No se ha incluido ningún criterios específico-relacionados con las nuevas regulaciones europeas (NIS2, DORA, Ley de Ciberresiliencia) pero se revela en a información publicada un panorama de adaptación progresiva.

Preparación para NIS2: El 34% de las empresas potencialmente afectadas mencionan específicamente la preparación para el cumplimiento de NIS2, evidenciando una concienciación creciente pero aún parcial.

Cumplimiento DORA (Sector Financiero): Las entidades financieras muestran un 67% de referencias específicas a la preparación para DORA, reflejando una mayor madurez en la adaptación regulatoria sectorial.

Ley de Ciberresiliencia: Solo el 8% de las empresas hacen referencia específica a esta regulación, lo que sugiere una oportunidad de mejora en la preparación ante futuras obligaciones normativas.

Estos resultados indican que, aunque existe concienciación sobre el cambio regulatorio, la comunicación específica sobre las medidas de adaptación requiere mayor desarrollo.

6.2.- Análisis de Resultados por Sectores

El análisis sectorial del V Ranking revela diferencias significativas en los niveles de transparencia en ciberseguridad entre los distintos sectores representados en el IBEX 35.

Esta segmentación permite identificar patrones sectoriales, mejores prácticas transferibles y oportunidades de benchmarking entre industrias.

La evaluación sectorial considera tanto la puntuación absoluta como la puntuación ponderada por número de empresas, proporcionando una visión equilibrada del desempeño relativo de cada sector.

RESULTADO POR SECTORES 2024

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

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

Sectores con mejor desempeño en transparencia

Sector Telecomunicaciones (4 empresas - Puntuación promedio: 138.75): Se sitúa nuevamente en la primera posición del ranking y demuestra liderazgo en la adopción y comunicación de tecnologías emergentes. Las empresas de este sector destacan especialmente en los nuevos criterios relacionados con IA y dotación de recursos humanos especializados.

Sector Financiero y Seguros (7 empresas - Puntuación promedio: 136.43): Las entidades financieras demuestran madurez en la comunicación de aspectos como certificaciones internacionales, cumplimiento normativo e inversiones específicas en ciberseguridad. La regulación sectorial específica (DORA) ha incentivado una mayor transparencia preventiva.

Sector Energético (8 empresas - Puntuación promedio: 115.63): Muestra una transparencia sólida, especialmente en aspectos relacionados con la gestión de infraestructuras críticas y planes de continuidad de negocio. La exposición a riesgos cibernéticos específicos del sector impulsa una mayor comunicación sobre medidas preventivas.

Sectores con oportunidades de mejora

Sector Servicios de Consumo (4 empresas – Puntuación promedio: 110.00): Presenta el menor crecimiento interanual y evidencia oportunidades significativas de mejora. La transparencia en ciberseguridad parece no ser prioritaria en la comunicación corporativa, a pesar de la creciente importancia de la protección de datos de clientes.

Sector Construcción (6 empresas - Puntuación promedio: 108.33): A pesar del crecimiento significativo en puntuación ponderada, la puntuación absoluta promedio sugiere oportunidades de mejora en la sistematización de la comunicación sobre ciberseguridad.

Sector Inmobiliario (2 empresas - Puntuación promedio: 90.00): Aunque muestra crecimiento positivo (+7.46%), mantiene niveles de transparencia por debajo del promedio del índice. La digitalización acelerada del sector requiere una comunicación más robusta sobre las medidas de ciberseguridad adoptadas.

Sector Bienes de Consumo (4 empresas - Puntuación promedio: 87.50): Sufre una gran caída lastrada por empresas en donde la transparencia en ciberseguridad no ha calado en sus informes.

Telecomunicaciones y Finanzas y Seguros, lideran de forma recurrente el ranking sectorial con una transparencia consolidada y sistemática.

Tendencias sectoriales emergentes

El análisis sectorial identifica varias tendencias emergentes relevantes**:**

Convergencia regulatoria: Los sectores con mayor exposición regulatoria (financiero, energético, telecomunicaciones) muestran una convergencia progresiva en los niveles de transparencia, sugiriendo un efecto normalizador de la regulación**.**

Digitalización como catalizador: Los sectores en proceso de transformación digital acelerada demuestran mejores tasas de crecimiento en transparencia, evidenciando que la digitalización impulsa la concienciación sobre ciberseguridad**.**

Especialización temática: Cada sector desarrolla fortalezas específicas en diferentes criterios de transparencia, creando oportunidades de aprendizaje cruzado e intercambio de mejores prácticas**.**

Brecha de adaptación: Se observa una brecha creciente entre sectores altamente regulados y aquellos con menor presión regulatoria específica en ciberseguridad.

Estas tendencias sugieren la necesidad de enfoques sectoriales diferenciados en las estrategias de mejora de transparencia, aprovechando las fortalezas específicas de cada industria**.**

7.- Evolución y comparativa con ranking anterior (2023)

La comparativa entre el V Ranking 2024 y el IV Ranking 2023 revela una evolución dinámica en la transparencia de ciberseguridad de las empresas del IBEX 35. El análisis longitudinal permite identificar tendencias consolidadas, mejoras significativas y cambios en el posicionamiento relativo de las empresas, proporcionando información valiosa sobre la dirección del mercado español en materia de transparencia en ciberseguridad.

La metodología de comparación se basa en el análisis de 35 empresas que participaron en ambos rankings, manteniendo la comparabilidad metodológica y ajustando las diferencias derivadas de la ampliación del marco de criterios de 14 a 16 elementos de evaluación.

Tendencias generales de evolución

Estancamiento agregado de transparencia: La puntuación total agregada del índice sin la ampliación de criterios experimentó un estancamiento en la transparencia en donde se ha evidenciado una volatilidad en las posiciones obtenidas en el ranking con caídas significativas por parte de empresas que ocupaban puestos de liderazgo.

Estabilidad en el liderazgo: Las empresas líderes del ranking mantienen posiciones destacadas, con CAIXABANK e INDITEX conservando posiciones de liderazgo. Sin embargo, se observa una mayor competencia en las posiciones superiores, con FERROVIAL emergiendo a las posiciones de liderazgo.

Dinamismo competitivo: El análisis revela alta volatilidad posicional: 16 empresas mejoran sus posiciones, 16 retroceden y solo 3 mantienen posiciones idénticas. Esta distribución evidencia un mercado altamente dinámico donde las mejoras en transparencia generan ventajas competitivas tangibles.

Casos destacados de evolución

Mejoras más significativas:

ACS: Logra el mayor ascenso (8 posiciones), pasando de la posición 16 a la 8. Esta mejora se atribuye principalmente a la publicación de información detallada sobre el uso de la IA en ciberseguridad a través de la política de inteligencia artificial publicada y la implementación de un SOC especializado.

INDRA: Asciende 7 posiciones (de 9 a 2), consolidándose en el pódium gracias a la mejora sustancial en la comunicación sobre el uso de IA en ciberseguridad y la transparencia en la dotación de recursos humanos especializados

Retrocesos significativos**:**

ENDESA: Experimenta el mayor retroceso (12 posiciones, de 6 a 18), principalmente debido a la reducción en la granularidad de la información publicada sobre certificaciones y la gestión de terceros.

IBERDROLA: Desciende 10 posiciones (de 6 a 16), afectada por cambios en la estructura de reporte que redujeron la visibilidad de información específica sobre ciberseguridad.

Impacto de los nuevos criterios

Los dos nuevos criterios incorporados en el V Ranking (IA en ciberseguridad y recursos humanos) han tenido un impacto diferencial significativo.

Criterio 15 - IA en ciberseguridad: Solo el 54% de las empresas obtuvieron puntuaciones significativas en este criterio, evidenciando una oportunidad de diferenciación competitiva. Las empresas del sector tecnológico y telecomunicaciones lideran esta categoría, mientras que sectores tradicionales muestran menor desarrollo.

Criterio 16 - Recursos humanos en ciberseguridad: La transparencia sobre dotación de personal especializado es aún menor (17% de empresas con información relevante), sugiriendo que este aspecto se considera información sensible o competitiva por parte de las organizaciones.

Efecto redistributivo: La incorporación de estos criterios ha beneficiado especialmente a empresas con estrategias digitales avanzadas y ha penalizado relativamente a aquellas con enfoques más tradicionales, contribuyendo a la reconfiguración del ranking.

Proyecciones y tendencias emergentes

El análisis evolutivo permite identificar tendencias que configurarán futuras ediciones del ranking:

Aceleración regulatoria: La próxima aplicación plena de NIS2, DORA y la Ley de Ciberresiliencia generará presión adicional hacia mayor transparencia, especialmente en sectores hasta ahora menos regulados.

Competencia por talento: La creciente escasez de profesionales especializados en ciberseguridad convertirá la transparencia sobre recursos humanos en un elemento diferenciador para atraer y retener talento.

Integración ESG: La ciberseguridad se integrará progresivamente en los marcos ESG corporativos, elevando las expectativas de transparencia por parte de inversores especializados.

La IA y las amenazas futuras: Se espera un incremento de personal técnico especializado en ciberseguridad con conocimientos en IA.

Fuente: Informe de ciberperparación Hiscox 2025. En encuesta a 5.750 empresas de EU y USA

8.- Conclusiones y recomendaciones estratégicas

El V Ranking de Transparencia en Ciberseguridad del IBEX 35 evidencia un panorama de maduración progresiva en la comunicación corporativa sobre ciberseguridad, caracterizado por la coexistencia de empresas que han alcanzado niveles de excelencia con otras que mantienen oportunidades significativas de desarrollo. Los resultados obtenidos reflejan tanto los avances logrados como los desafíos que persisten en la construcción de un ecosistema empresarial verdaderamente transparente en materia de ciberseguridad.

Las conclusiones derivadas del análisis trascienden la mera clasificación empresarial para proporcionar información estratégica relevante para la toma de decisiones de todos aquellos posibles afectados en el funcionamiento de la empresa como son: los consejos de administración, los inversores, clientes, proveedores, acreedores y accionistas.

De igual forma **este estudio puede proporcionar información valiosa a los reguladores para evaluar la efectividad de las políticas públicas en ciberseguridad**.

Conclusiones principales

1. **Maduración heterogénea del ecosistema**: El mercado español presenta una maduración heterogénea en transparencia de ciberseguridad, con sectores altamente regulados (financiero, telecomunicaciones) liderando la adopción de mejores prácticas, mientras que sectores tradicionales mantienen enfoques más conservadores en la divulgación de información.

2. **Impacto transformador de la regulación**: Las nuevas regulaciones europeas (NIS2, DORA, Ley de Ciberresiliencia) están generando un efecto catalizador en la mejora de la transparencia, especialmente visible en empresas que anticipan su aplicación. Sin embargo, persiste una brecha entre la concienciación regulatoria y la implementación efectiva de medidas de transparencia.

3. **Emergencia de la inteligencia artificial**: La incorporación de criterios específicos sobre IA revela una adopción aún incipiente pero creciente de estas tecnologías en ciberseguridad. Las empresas pioneras en esta área obtienen ventajas competitivas significativas en transparencia, sugiriendo una tendencia de diferenciación tecnológica

4. **Déficit en transparencia sobre recursos humanos en ciberseguridad**: La reticencia generalizada a divulgar información sobre dotación de personal especializado en ciberseguridad constituye una de las principales oportunidades de mejora identificadas.

5. **Volatilidad competitiva creciente**: La alta volatilidad posicional observada (equilibrio perfecto entre empresas que mejoran y empeoran) evidencia un mercado dinámico donde las inversiones en transparencia generan ventajas competitivas tangibles, incentivando la mejora continua.

Recomendaciones para empresas

Recomendaciones estratégicas de alto nivel:

1. Desarrollo de estrategias integrales de transparencia: Las empresas deben desarrollar estrategias comprehensivas que integren la transparencia en ciberseguridad como componente de su propuesta de valor hacia los accionistas, inversores, clientes y proveedores. Esto implica superar el enfoque reactivo de cumplimiento normativo para adoptar una perspectiva proactiva de diferenciación competitiva.

2. Preparación anticipada ante cambios regulatorios: Se recomienda la implementación de programas de preparación regulatoria que permitan anticipar las exigencias de NIS2, DORA y la Ley de Ciberresiliencia. Las empresas que comuniquen proactivamente sus medidas de adaptación obtendrán ventajas en reputación y confianza.

3. Inversión en capacidades de comunicación técnica: El desarrollo de capacidades internas para comunicar aspectos técnicos de ciberseguridad de manera comprensible para audiencias no especializadas constituye una inversión estratégica de alto retorno en términos de transparencia y confianza.

Recomendaciones operativas específicas:

1. Implementación de métricas estandarizadas: Adoptar marcos estandarizados de métricas de ciberseguridad (KPIs, KRIs) que faciliten la comparabilidad sectorial y la evaluación temporal de la evolución de la postura de seguridad organizacional.

2. Establecimiento de calendarios de divulgación: Desarrollar calendarios sistemáticos de divulgación que incluyan actualizaciones regulares sobre incidentes, mejoras implementadas, inversiones realizadas y cambios en la estrategia de ciberseguridad.

6. Aprovechamiento de tecnologías emergentes: Comunicar de manera específica las inversiones y aplicaciones de IA en ciberseguridad, posicionando a la organización como innovadora y tecnológicamente avanzada en este ámbito crítico.

Recomendaciones para grupos de interés en las empresas

1. Creación de sello de transparencia en ciberseguridad.
Es un reconocimiento a la calidad de la información que proporcionan en materia de ciberseguridad aumentando el prestigio de la empresa en el entorno empresarial a la vista de inversores, clientes, proveedores y empleados. Ofrece una ventaja diferencial frente a la competencia y consolida la confianza de los inversores y accionistas. Obliga a una mejora continua en la materia que se califica promoviendo la calidad de la información y la trasparencia de esta.

2. Integración en marcos ESG: Los inversores deben integrar sistemáticamente la transparencia en ciberseguridad como componente de sus marcos de evaluación ESG, reconociendo su impacto material en la sostenibilidad y resiliencia empresarial de largo plazo.

3. Utilización del ranking como herramienta de detección: Emplear el ranking como herramienta de detección inicial para identificar empresas con potenciales riesgos ocultos en ciberseguridad o, alternativamente, oportunidades de inversión en organizaciones con ventajas competitivas en transparencia.

4. **Interlocución activa con empresas**: Utilizar los resultados del ranking para estructurar diálogos constructivos con las empresas sobre mejoras específicas en transparencia, contribuyendo al desarrollo del ecosistema empresarial.

Recomendaciones para los reguladores.

Desarrollo de marcos normativos:

1. Armonización de estándares de transparencia: Desarrollar marcos normativos armonizados que establezcan estándares mínimos de transparencia en ciberseguridad, facilitando la comparabilidad y reduciendo la carga administrativa para las empresas.

2. Incentivos para transparencia proactiva: Establecer sistemas de incentivos que recompensen la transparencia proactiva por encima del cumplimiento mínimo normativo, fomentando una cultura de mejora continua en el ecosistema empresarial.

3. Facilitación de intercambio de mejores prácticas: plataformas y mecanismos que faciliten el intercambio sectorial de mejores prácticas en transparencia, aprovechando las fortalezas específicas de cada industria.

Monitorización y Evaluación:

1. Establecimiento de métricas de efectividad: Desarrollar métricas específicas para evaluar la efectividad de las políticas públicas en la mejora de la transparencia empresarial en ciberseguridad.

2. Coordinación internacional: Promover la coordinación con iniciativas similares a nivel europeo e internacional, asegurando la coherencia con mejores prácticas globales y evitando fragmentación regulatoria.

Perspectivas futuras y áreas de desarrollo

Evolución Metodológica del Ranking:

El V Ranking representa un punto de inflexión en la maduración de la metodología de evaluación. Las futuras ediciones incorporaremos refinamientos adicionales que reflejen:

- La evolución del marco regulatorio europeo y su transposición nacional.
- El desarrollo de estándares internacionales específicos para transparencia en ciberseguridad.
- La integración de métricas cuantitativas que complementen el análisis cualitativo actual
- La incorporación de tecnologías emergentes y su impacto en las estrategias de ciberseguridad
- Impacto en el ecosistema empresarial.

Se anticipa que la consolidación del ranking como herramienta de referencia generará efectos catalíticos en el ecosistema empresarial español como son:

- Mayor competencia entre empresas por mejorar su posicionamiento en transparencia
- Desarrollo de capacidades internas especializadas en comunicación de ciberseguridad
- Incremento en las inversiones destinadas a mejoras en transparencia corporativa.
- Nuevos servicios profesionales especializados en optimización de transparencia.

Contribución al objetivo nacional de ciberseguridad:

Este ranking contribuye a los objetivos de la Estrategia Nacional de Ciberseguridad mediante:

- El fortalecimiento de la cultura de transparencia en el sector privado.
- La identificación de mejores prácticas transferibles al conjunto del tejido empresarial
- La generación de incentivos reputacionales para la mejora continua en ciberseguridad. Sello de transparencia en ciberseguridad.

En conclusión:

La ciberseguridad es una cuestión esencial de seguridad nacional con impacto directo en la protección de las instituciones, las infraestructuras críticas, la actividad económica y el bienestar de la ciudadanía.

El V Ranking de Transparencia en Ciberseguridad del IBEX 35 no solo constituye una herramienta de evaluación y clasificación, sino un instrumento de transformación del ecosistema empresarial español hacia mayores niveles de responsabilidad en la transparencia y excelencia en ciberseguridad.

Agradecimientos y referencias

El V informe- ranking de transparencia en ciberseguridad del IBEX 35 ha sido posible gracias a la colaboración y el compromiso de múltiples actores del ecosistema de ciberseguridad español.

Agradecemos especialmente a todas las empresas del IBEX 35 por su compromiso con la transparencia corporativa y la publicación de información relevante sobre sus estrategias de ciberseguridad.

Referencias metodológicas:

- ISO/IEC 27001:2022 - Sistemas de gestión de la seguridad de la información
- NIST Cybersecurity Framework 2.0
- Directiva NIS2 (UE 2022/2555)
- Reglamento DORA (UE 2022/2554)
- Estrategia Nacional de Ciberseguridad 2024
- Ley de Ciberresiliencia de la UE (en desarrollo)

Para más información sobre la metodología y resultados:

info@watchandact.eu

(1) **Informe Control Risk para QBE** https://qbeespana.com/biblioteca-de-documentos/resiliencia-del-sector/negocios-conectados-la-dependencia-digital-alimenta-el-riesgo/?token=273889

(2) https://segurosnews.com/news/el-53-de-las-empresas-espanolas-con-entre-100-y-2-000-empleados-sufrio-un-ciberataque-el-ultimo-ano

(3) **Health-ISAC** https://www.tripwire.com/state-of-security/health-isac-report-ransomware-still-reigns-threat-healthcare#:~:text=Health%2DISAC's%202025%20report%20reveals%20ransomware%20as%20the,healthcare%2C%20highlighting%20patient%20extortion%20and%20large%2Dscale%20attacks.