INFORME

II RANKING DE TRANSPARENCIA DE INFORMACIÓN EN CIBER SEGURIDAD

Informe de transparencia y buen gobierno de información en Ciber Seguridad en las empresas del IBEX 35

Por Javier Silva y 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 son puntuales y completamente gratuitas.

Watch & Act Protection Services. Correduría de seguros especialista en seguros de ciber riesgo, 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

Presentación

Presentamos por segundo año consecutivo un informe de transparencia y buen gobierno de la información en Ciber Seguridad que las empresas del IBEX 35 publican en sus cuentas anuales referidos a los Estados de Información no Financieras.

La crisis del Covid-19 que ha provocado nuevas formas de trabajar y comunicarse ha continuado haciendo estragos en las empresas incrementando de forma significativa frente a años anteriores el número de ataques informáticos o ciberataques y consecuentemente el importe económico de los mismos. En el año 2021, el INCIBE gestionó más de 109.126 casos de ciberataques sin contar aquellos que no fueron detectados por las empresas o denunciados como tal. Este elevado número de vulneraciones de la ciberseguridad no sólo afecta a grandes o medianas empresas, sino también a los pequeños empresarios. **Según el reciente informe de Hiscox, "Informe de Ciberpreparación 2022" un 48% de las PYMES españolas sufrieron al menos un ciberataque el año pasado. Los ataques se han intensificado en el 2022 frente al 43% del año anterior.**

De igual manera el informe de Hiscox indica que el coste medio de un ciberataque en una pyme de 0 a 49 empleados es de 16.300 euros y de 22.950 euros para empresas de 50 a 249 empleados.

La percepción y consecuentemente la inversión en medidas de protección en ciberseguridad de las pymes españolas es muy baja según afirma el informe de Google "La Ciberseguridad en 2022 y el efecto postpandemia en las pymes españolas". Las pymes en general no son conscientes de que un ataque cibernético es un riesgo real que puede llevar a la ruina a la empresa y es algo que parecen no haber interiorizado, especialmente, las de menor tamaño. De hecho, según indica el mencionado informe de Google, al decrecer la percepción de riesgo, también lo ha hecho ligeramente la implicación activa de las empresas en materia de ciberseguridad, reduciéndose del 36% al 31%.

Sin embargo, en el presente ranking de transparencia en Ciberseguridad, una de las conclusiones que hemos podido constatar es, que las grandes empresas son cada vez más conscientes de estos peligros provocando una implicación directa de los comités de dirección en el establecimiento de unas políticas, medidas y estrategias adecuadas en materia de ciberseguridad además de incrementar la inversión y buscar alternativas para la transferencia de estos riesgos como son los seguros de ciber riesgo.

El aumento del gasto medio en ciberseguridad de todos los encuestados para la elaboración del informe de Hiscox indica un incremento de un 60% frente al año anterior.

Por ello, un año más hemos vuelto a coger de referencia a las empresas del IBEX 35 para ver como han evolucionado en sus políticas y acciones en materia de ciberseguridad, analizar cómo lo comunican y señalar la importancia que le dan desde el punto de vista estratégico del negocio y por ende en sus cuentas de resultados.

Esperemos nuevamente que esta segunda edición del estudio con sus recomendaciones y conclusiones sirva de guía para una mejora tanto en las medidas de ciber seguridad como para la transparencia y comunicación del buen gobierno corporativo de todas las empresas empezando por estas del IBEX 35

Introducción

La concienciación en la seguridad de la información y protección de los datos (ciberseguridad) es la premisa básica que deberían tener todas las empresas conforme indica el informe de Google. "La Ciberseguridad en 2022 y el efecto postpandemia en las pymes española".

En líneas generales y conforme detallamos en las conclusiones del presente ranking, la gran empresa ha tomado buena nota y es plenamente consciente de esta problemática por las importantes consecuencias económicas que ello pudiera suponer en sus cuentas de resultados.

Por ello, en Watch & Act Protection Services hemos querido analizar un año más cómo se comportan las empresas del Ibex 35 en lo que respecta a, la información que publican sobre sus propias medidas de seguridad de la información y protección de los datos haciendo una comparativa frente al año anterior y destacando las diferencias encontradas.

Queremos dejar bien claro, que en el presente informe/ ranking no hemos analizado o valorado las medidas técnicas de ciberseguridad implementadas en estas empresas ni cuestionado su efectividad, sino que nos hemos centrado en valorar como y de qué manera comunican las acciones que están llevando a cabo para proteger los intereses de los clientes, accionistas, empleados, usuarios, inversores, proveedores, etc. y la relevancia que le otorgan a estas medidas.

Para ello, hemos identificado y puntuado una serie de aspectos que consideramos relevantes y que deben ser adecuadamente explicados en los informes de cuentas anuales en los estados de información no financiera de las empresas

Aspectos referidos a la involucración y liderazgo del comité de dirección de la empresa en la gestión de los riesgos de ciberseguridad, las políticas, estrategias, planes de continuidad, centros de respuesta y control, la formación a empleados, la responsabilidad de la seguridad de la información (CISO) y la protección de datos, entre otras, es información esencial y que entendemos debe ser claramente publicadas.

Con todo ello, y con la información disponible publicada en los citados informes hemos realizado por segundo año consecutivo el ranking de transparencia de la información en medidas de ciberseguridad que estas empresas publican y su comparativa frente al año anterior.

Adicionalmente, este año hemos incluido tres aspectos clave que entendemos deben informar todas las empresas en materia de ciberseguridad, si bien no los hemos puntuado en esta ocasión pero que si nos ha servido para otorgar una mejor posición a aquellas empresas que considerábamos tenían una igualdad de cumplimiento. Estas son:

- Información referente a la existencia de un seguro de ciber riesgo.
- Indicación de ataques o incidentes en materia de ciberseguridad acaecidos a lo largo del año y su repercusión económica y reputacional.
- Medidas adoptadas en materia de ciberseguridad y requeridas a los proveedores que forman parte de la cadena de suministro de la empresa.

Metodología: Ranking Ibex 35

A partir de los informes anuales que publican las empresas del Ibex en sus correspondientes páginas WEB accesibles en la sección dedicada a Accionistas e Inversores y de forma muy rigurosa, hemos revisado la información relacionada con la Ciberseguridad, la hemos evaluado y hemos construido el II Ranking entre las empresas del IBEX 35.

El II Ranking de Transparencia y Relevancia en Ciberseguridad de las empresas del IBEX 35 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.

Para realizar la evaluación de la información publicada por las empresas, hemos utilizado la norma ISO 27001 de requisitos de sistemas de gestión de la seguridad de la información. Los requisitos que establece esta norma internacional nos permiten identificar y valorar si una empresa ha establecido los elementos clave de un sistema de gestión de la seguridad de la información para gestionar los riesgos de ciberseguridad. Para ello, hemos definido 10 criterios cuya puntuación puede alcanzar los 100 puntos. Evaluamos cada criterio en una escala de puntuación de 0 a 10 con cinco valores posibles a obtener que se otorgan de la siguiente forma:

- 0 puntos si la empresa no ha publicado alguna información relacionada con el criterio.

- 2,5 puntos si ha publicado información que menciona el criterio evaluado pero que no aporta evidencia sobre su establecimiento e implementación.

- 5 puntos si la información publicada aporta evidencia sobre la que se infiere o se puede deducir que se cumple el criterio.

- 7,5 puntos si la información publicada aporta evidencias sobre el cumplimiento de una parte del criterio.

- 10 puntos si la información publicada aporta evidencias sobre el cumplimiento del criterio.

Los 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 tercera parte.

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

Adicionalmente a los 10 criterios evaluados se ha enriquecido el análisis con **tres criterios adicionales** que conforme indicamos anteriormente no han sido puntuados en esta edición. pero que serán incorporados en las próximas ya que los consideramos de especial relevancia.

Los criterios de **contratación de una póliza de seguros, la indicación de ataques o incidentes en materia de ciberseguridad y las medidas de seguridad exigidas a los proveedores** se pueden inferir de la Norma ISO 27001 y por ello en esta ocasión los hemos considerado como información adicional de interés determinante de una mejor valoración en aquellas empresas que lo informan.

Resultados Ranking Ibex 35

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. Además, conforme reflejan en las memorias, en la mayoría de los casos, las inversiones en el capítulo de ciberseguridad son crecientes año a año dando especial relevancia a los distintos comités de seguimiento.

II RANKING DE TRANSPARENCIA EN CIBERSEGURIDAD

POSICIÓN	EMPRESA	VARIACIÓN	POSICIÓN	EMPRESA	VARIACIÓN	POSICIÓN	EMPRESA	VARIACIÓN
1	Banco Santander	↑	11	Amadeus	↓	25	Grifols	↓
2	Ferrovial	↑	12	Caixabank	↓	26	ACS	↓
3	Enagas	↑	13	Repsol	↑	27	Merlin Properties	↓
4	Mapfre	↑	14	BBVA	↓	28	Solaria	↑
5	Naturgy	↑	15	Red Eléctrica	↑	29	Pharmamar	↓
6	Sacyr	NV	16	Inditex	↓	30	Cellnex	↓
7	Telefónica	↓	17	Bankinter	↑	31	Siemens Gamesa	↑
8	AENA	↓	18	Endesa	↓	32	Colonial	↓
9	Fluidra	↑	19	Indra	↓	33	Rovi	NV
10	Iberdrola	↑	20	Acciona	↑	34	Acerinox	↓
			21	Acciona Energía	NV	35	ArcelorMittal	↓
			22	Banco Sabadell	↓			
			23	IAG	↓			
			24	Meliá	↓			

Este año el ranking lo lidera nuevamente una entidad bancaria, Banco de Santander y lo cierra ArcelorMittal ofreciendo el resto de las empresas una gran mejoría frente al año pasado.

Con carácter general señalar, aunque posteriormente haremos una mención por sectores, que determinadas empresas del sector de energía, banca y construcción proporcionan una información, amplia, clara y trasparente dado que han tomado conciencia del creciente y enorme riesgo que suponen los ataques cibernéticos en sus empresas y de las importantes consecuencias económicas y reputacionales que ello puede provocar en clientes, accionistas inversores, etc.

En la tabla media del ranking, es decir aquellas situadas en los puestos del 11 al 24 incluidos merece la pena señalar que han mejorado sustancialmente su nivel de transparencia debido a la toma de conciencia de los peligros existentes en esta materia, si

bien no dejan suficientemente claro o no explican entre otras, la estrategia, medidas, certificaciones y auditorias que se han llevado a cabo a lo largo del año.

Por último, en las posiciones del 25 al 35 repiten en su gran mayoría las mismas empresas que el año pasado. Esto no quiere decir que estas empresas no estén tomando las medidas necesarias para evitar un ataque cibernético dado que los sectores a las cual pertenecen son de infraestructuras críticas o de consumo principalmente. No obstante, y por esto mismo, entendemos que el deber de informar y poner de manifiesto que hay interés en uno de los principales riesgos de las empresas en el momento actual y a futuro, es absolutamente necesario.

Resultados por criterios

Es importante señalar que los valores aplicados a los criterios seleccionados no son ponderados, es decir, les hemos otorgado la misma importancia a todos ellos y por lo tanto los resultados obtenidos corresponde a la suma de las puntuaciones atribuidas a cada uno de ellos.

Los criterios que han obtenido una mayor valoración agregada por las 35 empresas del IBEX al haber sido los que en mayor número las empresas han publicado información sobre ellos, han sido por orden de mayor a menor transparencia son:

Criterio nº 2: **Liderazgo de la alta dirección** con respecto al sistema de gestión de seguridad de la información.

Criterio nº 8**: Concienciación y formación a los empleados** en ciberseguridad.

Criterio nº 4: **Gestión de los riesgos de ciberseguridad** por la comisión de riesgos que reporta a la alta dirección.

Criterio nº 9. **Cumplimiento obligaciones legales** relativas a la seguridad de la información.

Criterio nº 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.

Es relevante señalar como la alta dirección de las empresas han tomado conciencia de estos riesgos y la gran mayoría de los miembros del consejo de administración de estas, forman parte de distintos comités para abordar y liderar una estrategia eficaz para evitarlos. De igual forma, han trasladado la innegable necesidad de proporcionar formación en materia de ciberseguridad a todo el personal de la empresa empezando por ellos mismos.

El cumplimiento de las obligaciones legales a raíz del Reglamento General de Protección de Datos (RGPD) y las consecuentes políticas y medidas de seguridad a aplicar son

también aspectos muy considerados a nivel informativo en las memorias de sostenibilidad y no financieras de las empresas.

En el otro extremo, los criterios que han obtenido una peor valoración mostrando que las empresas del Ibex 35 han publicado en un menor número información sobre ellos siguen siendo por orden de más transparencia a menor son:

> Criterio nº 10: **Plan de continuidad de negocio** ante eventos disruptivos relacionados con la seguridad de la información.
>
> Criterio nº 7: **Existencia de un SOC (Centro de Operaciones de Seguridad**) o entidad similar para detectar, analizar, informar y corregir incidentes de seguridad.
>
> Criterio nº 6: **Certificación por normas internacionales / Auditoría** por terceras partes.

Estos tres criterios de los que menor información comparten en sus informes las empresas coinciden que son los que requieren un mayor grado de madurez y por tanto, su implementación requiere un plazo de tiempo mayor. A pesar de ello, en líneas generales aquellas que los han informado, han sido muy concretas, detalladas y específicas.

Los criterios 5 y 1 entendemos que requieren una mayor definición y concreción. Son los referidos a los objetivos, planificación y de identificación clara y concreta del responsable de ciberseguridad dejando constancia clara en el caso de este último, de sus competencias y su dependencia directa del consejo de administración.

Finalmente, hay que indicar nuevamente que los tres criterios adicionales no puntuables para esta edición han sido tenidos en cuenta a la hora de determinar una mejor posición en el ranking en los casos de igualdad de posiciones.

Resultados por sectores

A continuación, mostramos los resultados por sectores y su comparativa frente al año anterior:

RESULTADO POR SECTORES 2021

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

RESULTADO POR SECTORES 2020

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

Los sectores cuyas empresas tienen un mayor grado de transparencia en la información en Ciberseguridad son los de Servicios Financieros y Seguros, seguidos por los de Servicios de Consumo.

Las empresas de banca y seguros lideran y han mostrado un gran interés y preocupación por los riesgos cibernéticos demostrando a sus accionistas en inversores que es una prioridad y así lo manifiestan claramente.

El sector de Servicios de Consumo se mantiene en el ranking, pero mejoran la puntuación por la preocupación y concienciación que han tomado de estos riesgos y las repercusiones que pueden tener en sus clientes.

El sector de las Telecomunicaciones sin embargo baja en el ranking, aunque las puntuaciones son muy altas con la salvedad de Cellnex. Existe interés y preocupación en informar, pero hay margen de mejora en algunas de ellas.

Construcción mejora sensiblemente, pero determinadas empresas no consideran un aspecto crítico el informar de estos riesgos a pesar de ser conscientes de lo que ello implica para sus clientes, proveedores y accionistas.

Inmobiliario continua a la cola no informando acerca de estos riesgos ni las medidas o políticas a desarrollar.

Conclusiones

Nuevamente **el objetivo de este II Ranking de Transparencia en Ciberseguridad es poner de manifiesto la importancia y relevancia que otorgan las empresas del Ibex 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.

Mediante este análisis, hemos detectado aspectos relevantes y diferenciadores en cuanto a la importancia que otorgan las distintas empresas a los problemas de ciberseguridad, pero hemos constatado en esta segunda edición que, en comparación con el año pasado, **las empresas del Ibex muestran una mayor sensibilidad y preocupación por los riesgos cibernéticos y así lo han reflejado en las memorias no financieras del 2021**. De igual forma, hemos podido observar como muchas de estas empresas han hecho especial **mención al incremento en las partidas de gasto en medidas de protección en ciberseguridad incluyendo la contratación de seguros específicos para ellos como son los de Ciber riesgo.**

El Instituto Nacional de Ciberseguridad (INCIBE), dependiente del Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, gestionó desde su Centro de Respuesta a Incidentes de Seguridad (INCIBE-CERT), 109.126 incidentes de ciberseguridad durante el año 2021.

Del total de esta cifra, 90.168 afectaron a ciudadanos y empresas, 680 a operadores estratégicos y 18.278 a la Red Académica y de Investigación Española (RedIRIS). En cuanto a su tipología, el 29,88% correspondió malware o software malicioso, seguido de las distintas variantes de fraude con un 28,60%. En tercer lugar, destacan los ataques a sistemas vulnerables, con un 18,89%. Estas cifras consolidan las tendencias de incidentes de ciberseguridad de los últimos años.

Estos son los resultados oficiales de los ciberataques reportados en el 2021 que sin lugar a duda serán inferiores a los que se reportarán en el 2022**. Para ser más concretos, ya en este 2022 se ha producido un incremento sin precedentes de ataques informáticos como consecuencia de la guerra en Ucrania**. (Leer artículo "España, en el punto de mira de los piratas informáticos" publicado el pasado mes de junio por Watch & Act Protection Services).

La repercusión final de estos ataques es el impacto económico que estas brechas de seguridad han provocado en las cuentas de resultados de las empresas y su consecuente daño reputacional. En el sexto informe de Ciberpreparación 2022 elaborado por la aseguradora Hiscox indican que se ha duplicado para las empresas españolas el coste económico de los ataques informáticos pasando de 54.388 euros en el 2020 hasta los 105.655 euros en 2021.

La gran empresa española en contraposición de la Pyme no solo ha tomado conciencia, sino que está poniendo medidas técnicas y aumentando la inversión tecnológica y la prevención.

Otro de los aspectos del presente ranking es, además de **informar, ayudar a poner en común las distintas medidas que las empresas publican y complementar con ideas y mejores prácticas a implementar para la mejora no solo de la información y transparencia sino también de la concienciación en ciberseguridad.**

Por ello, los aspectos ya sobradamente mencionados de, compromiso, apoyo y liderazgo de los miembros del comité de dirección y directivos en la organización junto con una formación integral continua y específica para toda la plantilla son requisitos para establecer las bases de una correcta ciber protección.

Finalmente queremos volver a incidir en **los tres aspectos relevantes** que no hemos puntuado en el presente ranking pero que si se puntuarán para estudios sucesivos. Estos son:

- **Que la empresa disponga de un seguro de ciber riesgo adecuado** que cubra, además de los gastos económicos ocasionados por un ataque cibernético, el que proporcione la ayuda tecnológica de emergencia para minimizar su impacto en la empresa.
- **Indicación de ataques o incidentes en materia de ciberseguridad acaecidos a lo largo del año y su repercusión económica y reputacional**. En aras de una transparencia de estas empresas, consideramos que las menciones y consecuencias de hechos relevantes en esta materia se han de especificar.
- **Medidas adoptadas en materia de ciberseguridad requeridas a los proveedores que forman parte de la cadena de suministro de la empresa.** Se está convirtiendo en los últimos tiempos en una de las principales vías de ataques y brechas de seguridad en las mismas. Los controles y auditorías en medidas de seguridad cibernética implementadas a estos proveedores han de ser consideradas con más detalle y rigor en lo referente a medidas de ciberseguridad aplicadas.

En conclusión, este año, **hemos podido constatar como en el capítulo de Gestión de Riesgos de las empresas del IBEX, la Ciberseguridad ha pasado a ser uno de los objetivo prioritarios.**

El grupo Watch & Act, a través de su correduría de **seguros Watch & Act Protection Services especializada en seguros de ciber riesgo** y de su consultora de transformación digital en el área de personas, proporciona las soluciones más idóneas para el seguro y el análisis de la huella digital de las empresas.

El grupo Watch & Act International Consulting, especializado en procesos de transformación empresarial con foco en las personas, dispone de un área específica de ciberseguridad que ofrece servicios como el análisis de la huella digital de empleados y directivos, implementación de políticas y procedimientos de continuidad de negocio y, a través de su correduría de seguros **Watch & Act Protection Services**, la contratación de pólizas de ciber riesgo con las principales aseguradoras del mercado nacional además de otros seguros de responsabilidad civil, administradores y directivos, riesgos especiales vida, accidentes y salud.

Recomendaciones

Entre las posibles mejores prácticas y recomendaciones que se pueden considerar en materia de ciberseguridad destacamos las siguientes:

- Participación de la alta dirección en Comisiones dependientes del Consejo que gestionen asuntos de ciberseguridad
- Designación de un CISO global y participación de este en Comités de Dirección.
- Programas de formación en ciberseguridad a toda la plantilla de forma continua y reiterada.
- Programa de recompensas a empleados por descubrimiento de vulnerabilidades
- Realización de auditorías de ciber seguridad propias y de proveedores externos de servicios con especial atención a la cadena de suministro de la empresa.
- Revisión y adecuación de protocolos de seguridad de la información para adaptarlos a la situación post Covid – 19.
- Políticas de seguridad de la información y recursos de gestión y de respuesta ante incidentes coordinados globalmente. Definición del Plan de gestión de crisis (Crisis Management Plan – CMP)
- Protocolos y recursos de respuesta ante incidentes de ciberseguridad para restaurar la normalidad en el menor tiempo y con el menor impacto posible. Descripción de los planes de Continuidad de Negocio (PCN), de Continuidad TIC y plan de Recuperación ante Desastres (Disaster Recovery Plan - DRP)
- Utilización como referencia de sus actuaciones de estándares internacionales con gran reconocimiento entre los que hay que mencionar: National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) e ISO 27001.
- Certificación CERT y cooperación activa nacional e internacional con otros CERT.
- Planes de Continuidad de Negocio con planes de acción que permitan a la organización prestar servicios esenciales en el caso que los sistemas de información sufran un deterioro por un ataque de ciberseguridad.
- Aprobación de planes e inversiones estratégicas en Ciberseguridad.
- La contratación de un seguro de ciber riesgo con un capital de cobertura y franquicia adecuados.

Anexo I

II RANKING DE TRANSPARENCIA EN CIBERSEGURIDAD	
POSICIÓN	EMPRESA
1	Banco Santander
2	Ferrovial
3	Enagas
4	Mapfre
5	Naturgy
6	Sacyr
7	Telefónica
8	AENA
9	Fluidra
10	Iberdrola
11	Amadeus
12	Caixabank
13	Repsol
14	BBVA
15	Red Eléctrica
16	Inditex
17	Bankinter
18	Endesa
19	Indra
20	Acciona
21	Acciona Energía
22	Banco Sabadell
23	IAG
24	Meliá
25	Grifols
26	ACS
27	Merlin Properties
28	Solaria
29	Pharmamar
30	Cellnex
31	Siemens Gamesa
32	Colonial
33	Rovi
34	Acerinox
35	ArcelorMittal

Anexo II

RESULTADO POR SECTORES 2021

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

RESULTADO POR SECTORES 2020

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