INFORME DE TRANSPARENCIA EN LA INFORMACIÓN SOBRE CIBERSEGURIDAD EN LAS EMPRESAS DEL IBEX 35

Por Javier Silva y Javier Huergo

INDEPENDENCIA DE NUESTROS INFORMES El presente informe no ha sido financiado por ninguna de las instituciones analizadas en el mismo. El grupo Watch&Act no ha recibido ningún tipo de contraprestación por la elaboración del mismo. 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 Service*s es una correduría de seguros especializada en seguros de ciber riesgo, de responsabilidad civil, administradores y directivos, riesgos especiales vida, accidentes y salud. (www.waprotection.com). Participada por

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

"Informe de transparencia en la información sobre ciberseguridad en las empresas del IBEX 35. 2021"

La presentación de es este primer informe de transparencia en la información en Ciber Seguridad en las empresas del IBEX 35 2021, viene motivada por las consecuencias provocadas por la crisis del Covid-19. El teletrabajo impuesto de manera precipitada y acelerada en la mayoría de las empresas ha supuesto una fragilidad en las medidas de ciberseguridad que los piratas informáticos han aprovechado para obtener grandes y pingues beneficios con gran impunidad y sin temor a ser descubiertos.

Las grandes mafias de delincuencia han visto una oportunidad única e imparable para extorsionar y chantajear a empresas y organizaciones y en algunas ocasiones sin siquiera un interés económico como tal.

La capacidad de manipulación y chantaje de los ciberdelincuentes ha logrado desestabilizar gobiernos, amañar elecciones, falsear opiniones y, en definitiva, hacernos tomar conciencia de que estamos totalmente expuestos en lo que respecta a nuestra información personal y profesional, pudiendo afectar claramente a nuestra vida privada.

Nos hemos vueltos vulnerables y estamos expuestos a cualquier ataque cibernético desde el momento en que aceptamos y cedemos nuestros datos para su tratamiento para cualquier servicio, empezando por el más básico que es una conexión a internet.

Por ello y en la medida en que una gran parte de la población y la economía se halla directa o indirectamente relacionada con las grandes empresas, hemos seleccionado, las empresas del IBEX 35 como la muestra más representativa, y es el foco de este análisis de transparencia que estas empresas han de cumplir, a la vista de la transcendencia y las implicaciones que ello conlleva.

Esperemos que este primer 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

2 Introducción

En los tiempos que corren, la seguridad de la información y la privacidad de los datos personales son aspectos cada vez más críticos e importantes. Los usuarios somos vulnerables, y dependemos de las medidas de seguridad que las empresas adopten para proteger la información relevante y de carácter confidencial que manejan, así como los datos personales que voluntaria o necesariamente hemos tenido que poner a su disposición.

Durante la pandemia, se han disparado el número de ataques. Según los datos publicados en el informe del Consejo General de los Colegios de Mediadores de Seguros, en España, como en el resto del mundo, la situación no es precisamente buena pues se produjeron más de 40.000 ciber ataques diarios. Las PYMES, que constituyen el 97% de nuestro tejido empresarial, son las que más sufren, INCIBE asegura que , reciben el 70% de los ciberataques que se producen en nuestro país. Estos ataques además, les generan un coste medio, conforme a los estudios de INCIBE, de 35.000 euros, cantidad que no podría ser asumible para muchas de ellas y podría suponer el cierre de sus actividades.
La ciberseguridad se ha convertido en la prioridad tecnológica para la mayoría de las empresas. Según el informe de Ciberpreparación de la aseguradora Hiscox, de 2021, señalan que los presupuestos de TI de las empresas se reorientan a la ciberseguridad. La empresa media dedica más de la quinta parte, un 21% de su presupuesto TI a la ciberseguridad, lo que supone un aumento del 63%, el impacto económico en la cuenta de resultados como consecuencia de un incidente informático es considerable.

La gran empresa tampoco está exenta del riesgo de sufrir estos ataques en donde las consecuencias son mayores en términos económicos y de responsabilidad social. Podemos citar ejemplos recientes de grandes compañías que han sufrido ciberataques, en España tales como: Telefónica, BBVA, Prosegur, Cadena Ser, Everis, Mapfre o el Hospital Universitario de Torrejón de Ardoz., etc. y a nivel mundial, empresas de reconocido prestigio como Tesla, Zoom, Twitter, Yahoo, Sony y hasta el mismo Pentágono de los Estados Unidos han sido víctimas de ciberataques, a pesar de estar tomando medidas para prevenirlos.
Por ello, en Watch & Act Protection Services hemos querido analizar 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.

"Informe de transparencia en la información sobre ciberseguridad en las empresas del IBEX 35. 2021"

Los aspectos más relevantes para gestionar adecuadamente sus riesgos de ciberseguridad, como la formación a empleados en ciberseguridad, el liderazgo y responsabilidad de la seguridad de la información (CISO) o la existencia de políticas y procedimientos de seguridad de la información y de protección de datos, entre otras, deben ser publicados en sus cuentas anuales de información no financiera, pues es importante que tanto sus inversores y accionistas como sus usuarios, clientes, empleados y consumidores conozcan las principales medidas adoptadas para cumplir la normativa y prevenir ataques que puedan afectar a la reputación de la propia empresa y, por ende, provocar un menoscabo económico para los accionistas.
Por todo ello, y con la información disponible publicada en los citados informes anuales de información no financiera correspondientes a 2020, hemos evaluado y puntuado a cada empresa del Ibex 35 y realizado un ranking de transparencia de la información en medidas de ciberseguridad que estas empresas publican.

Adicionalmente, hemos incluido dos aspectos clave que entendemos deben cumplir todas las empresas en materia de ciberseguridad:

- Las medidas de detección y recuperación organizadas en un plan de continuidad.

- La transferencia del riesgo a través de un buen seguro de ciber riesgo.

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 soluciones de continuidad de negocio soportadas en tecnología en la nube 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.

3 Metodología: Ranking Ibex 35

A partir de los informes anuales correspondientes a 2020 publicados por las empresas del Ibex en sus respectivas páginas WEB, accesibles en la sección dedicada a Accionistas e Inversores, de forma muy rigurosa hemos analizado la información relacionada con la Ciberseguridad y hemos construido el primer Ranking de Transparencia en información sobre Ciber Seguridad de las empresas del IBEX 35.

Se trata del único ranking que evalúa y puntúa a las empresas a partir de la información no financiera publicada que da evidencia de actuaciones que llevan a cabo en relación a la gestión de los riesgos de ciberseguridad, a las medidas de 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 agregada 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 ninguna 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 indirectamente evidencias sobre el cumplimiento de una parte del criterio.
- 10 puntos si la información publicada aporta evidencias sobre el cumplimiento del criterio.

"Informe de transparencia en la información sobre ciberseguridad en las empresas del IBEX 35. 2021"

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. (Miembro del comité de dirección o del consejo de administración).

2. Liderazgo de la alta dirección con respecto al sistema de gestión de seguridad de la información. Que se haya demostrado por la existencia de una comisión que gestione riesgos en ciberseguridad habiendo sido constituida por el comité de dirección y/o consejo aprobando inversiones/plan de seguridad.

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/ auditoría 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 a los empleados en seguridad.

9. Cumplimiento obligaciones legales relativas a la seguridad de la información que se concreta en el cumplimiento del Reglamente General de Protección de Datos (RGPD).

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 un último criterio no puntuable pero de gran interés: La contratación de una póliza de seguros que cubra los riesgos de ciberseguridad, una medida muy necesaria para las empresas del IBEX 35 ante el aumento de la incidencia en el número de ciberataques y porque entendemos que interesa sobremanera a los accionistas, inversores, proxis y otras terceras partes interesadas.

4 Resultados: Ranking Ibex 35

Es importante aclarar que los resultados obtenidos a través del análisis realizado valoran exclusivamente la información publicada, es decir, el grado de transparencia de una empresa en la gestión relacionada con la Ciberseguridad. En ningún caso se pretende hacer una valoración de las medidas de Ciberseguridad de que disponen la empresa siendo normalmente servicios que tendrían que hacerse por encargo de una empresa. tener acceso a los sistemas e infraestructuras de tecnologías de la información que es la única forma de conocer y evaluar el alcance y grado de protección de las medidas adoptadas.

El análisis divide a las compañías en cuatro grupos:

- Del 1 al 9: empresas muy transparentes debido a que perciben como muy relevante para sus accionistas e inversores la información sobre ciberseguridad.

- Del 10 al 17: nivel medio-alto, aunque tienen la oportunidad de mejorar significativamente su transparencia en ciberseguridad.

- Del 18 al 26: tienen un nivel medio-bajo de transparencia en ciberseguridad presentando un alto potencial de mejora.

- Del 27 al 35: estas empresas presentan un nivel muy bajo o incluso nulo de transparencia y, por tanto, son las que tienen un mayor recorrido para hacer pública su información relevante sobre ciberseguridad.

Ranking Ibex 35 año 2020 Transparencia en Ciberseguridad

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

Las empresas situadas en el top 5 podrían ser clasificadas como referentes en la información que publican sobre ciberseguridad, pues han obtenido puntuaciones muy elevadas. Llama la atención que dichas 5 empresas son de sectores diferentes, lo que indica que el interés en conocer actuaciones llevadas a cabo en la gestión de riesgos relacionados con la ciberseguridad es transversal e interesa a la mayoría de los accionistas e inversores de las empresas con independencia del sector en el que desarrollen su actividad.

Resultados por criterios

Los criterios que han obtenido una mayor valoración agregada por las 35 empresas del IBEX han sido, en orden de mayor a menor transparencia , los siguientes:

Criterio 4: Gestión de los riesgos de ciberseguridad por la comisión de riesgos que reporta a la alta dirección.
Criterio 9. Cumplimiento obligaciones legales relativas a la seguridad de la información.
Criterio 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.

Estos tres criterios, objeto de un mayor grado de transparencia hacia sus accionistas e inversores, son los aspectos más básicos por los que normalmente comienzan las empresas sus actuaciones respecto a la gestión de la seguridad de la información. Es coherente que, junto a la designación de un responsable (Criterio 2), y el liderazgo de la alta dirección (Criterio 1), sean objeto de una mayor transparencia.

El Criterio 4, cuya evidencia es que el riesgo de ataques de ciberseguridad sea incluido en la gestión de riesgos por la alta dirección, es la evidencia de que el riesgo ha sido identificado y requiere unas actuaciones para controlarlo y minimizar su posible impacto en la empresa.

Respecto al Criterio 9, el nivel de transparencia del cumplimiento de obligaciones legales relacionados con la información en general y con los datos sensibles de los clientes y empleados en particular, se ha visto impulsado con las medidas adoptadas para cumplir el Reglamento General de Protección de Datos (RGPD).

El Criterio 3, la publicación de una política de seguridad de la información es una de las primeras medidas que la alta dirección de una empresa lleva a cabo para evidenciar su importancia, compromiso e implicación en la gestión de la seguridad de la información.
En el otro extremo, los criterios que han obtenido una peor valoración, mostrando que las empresas del Ibex 35 han publicado menos información sobre ellos han sido, en orden de mayor a menor transparencia:

Criterio 10: Plan de continuidad de negocio ante eventos disruptivos relacionados con la seguridad de la información
Criterio 7: Existencia de un SOC (Centro de Operaciones de Seguridad) o entidad similar para detectar, analizar, informar y corregir incidentes de seguridad.
Criterio 6: Certificación por normas internacionales / Auditoría por tercera parte.

Estos tres criterios requieren un mayor grado de madurez y, por tanto, su implementación necesita un plazo de tiempo mayor.

Lamentablemente, el Criterio 10, suele adquirir relevancia a consecuencia de un ataque o una caída por una actuación no planificada de los servicios que proporcionan los sistemas de información. Es entonces cuando la alta dirección es consciente del terrible impacto ocasionado por este tipo de acciones, y cuando las empresas reaccionan para estar preparadas ante situaciones similares en el futuro.

Respecto al Criterio 7, se ha constatado que hay muy bajo nivel de información respecto a la existencia de un SOC propio o contratado, lo que puede deberse bien a que, teniendo dichos servicios SOC, la empresa ha considerado que informar a los accionistas e inversores sobre su existencia no es relevante, o bien porque, al destinar muy pocos recursos a dichos servicios, no considera que sea suficientemente significativo como para informar sobre dicha actuación. En cualquier caso, el cumplimiento de este criterio indica alto un grado de madurez en gestión de riesgos de ciberseguridad.

"Informe de transparencia en la información sobre ciberseguridad en las empresas del IBEX 35. 2021"

Con respecto al resto de criterios que quedan en posiciones intermedias, los resultados en orden de mayor a menor grado de transparencia han sido:

Criterio 8: Concienciación y capacitación a los empleados en seguridad.
Criterio 5: Objetivos y planificación de las actuaciones en seguridad de la información.
Criterio 2: Liderazgo de la alta dirección con respecto al sistema de gestión de seguridad de la información.
Criterio 1: Responsable de ciberseguridad en la organización con reporte directo a la Alta Dirección.

El Criterio 8 ha sido el cuarto criterio sobre el que mayor cantidad de información se ha publicado. El hecho de que los empleados sean la principal puerta de entrada de virus informáticos es la razón principal para que las empresas lleven a cabo actuaciones de concienciación en ciberseguridad.

El Criterio 5 indica que hay numerosas empresas del IBEX que tienen un plan de ciberseguridad con el que fijan objetivos, priorizan actuaciones y recursos y contemplan otros aspectos relevantes de la gestión de la ciberseguridad.

Los Criterios 2 y 3 van muy de la mano. Es una condición esencial tener un responsable de seguridad de la información (CISO) y que este se sienta apoyado formalmente por la alta dirección. La información publicada no indica en muchos casos la designación de dicho responsable y que esté reportando a la alta dirección de la organización.

Finalmente, aunque como se ha explicado la mención a la contratación de una póliza de seguros de ciberseguridad no se ha incluido como criterio de valoración en el ejercicio realizado, cabe destacar que tan sólo 5 empresas mencionan en sus informes anuales que cuentan con una póliza de seguros para cubrir los riesgos de ciberseguridad. Dichas empresas son: Telefónica; Ferrovial, Endesa, Mapfre y Griffols.

Resultados por sectores

A continuación, se incluye una agrupación en sectores de las empresas del IBEX 35:

Sector	Compañías
Servicios Financieros y seguros	Banco Sabadell, Banco Santander, BBVA, Bankinter, CaixaBank y Mapfre
Energía	Enagás, Endesa, Naturgy, Iberdrola, Red Eléctrica, Repsol, Siemens Gamesa y Solaria
Construcción e Industria	Acciona, Acerinox, Arcelormittal, ACS, Cie automotive, Fluidra y Ferrovial
Servicios de Consumo	Meliá Hoteles, AENA e IAG
Bienes de Consumo	Inditex, Grifols, Viscofan, Almirall y Pharmamar
Tecnología y Telecomunicaciones	Amadeus, Cellnex, Telefónica e Indra
Inmobiliario	Colonial y Merlin Properties

"Informe de transparencia en la información sobre ciberseguridad en las empresas del IBEX 35. 2021"

Los sectores cuyas empresas presentan un mayor grado de transparencia en ciberseguridad son los de tecnología y telecomunicaciones, seguidos de servicios financieros y seguros, y en un tercer lugar se sitúan las empresas de servicios de consumo. Entre las empresas de servicios financieros llama la atención la baja puntuación de Bankinter en comparación con el resto.

Las empresas del sector de la energía presentan una dicotomía. Por una parte, Naturgy, Endesa, Enagás y Red Eléctrica tienen un nivel de transparencia medio alto, mientras que Repsol, Iberdrola, Solaria y Siemens Gamesa se encuentran entre las de menor nivel de transparencia, con niveles de medio-bajo a muy bajo o nulo.

Las empresas de los sectores inmobiliario y de construcción e industria son las que han mostrado el peor nivel de transparencia.

5 Conclusiones

Mediante este análisis, hemos detectado aspectos relevantes y diferenciadores en cuanto a la importancia que otorgan las empresas del IBEX 35 a las actuaciones en Ciberseguridad que llevan a cabo a tenor de la información publicada en sus informes anuales de información no financiera.
Las cifras de ataques informáticos a las empresas son alarmantes y crecientes, y se han agravado aún más en el escenario de pandemia provocada por el Covid 19.
Por ello, hemos creído conveniente poner de manifiesto, en aras de la transparencia que deben mostrar estas grandes empresas, el grado de importancia que dan a informar en sus memorias anuales no financieras sobre las acciones y medidas llevadas a cabo, para proporcionar la mayor tranquilidad posible a inversores, clientes, proveedores y otras instituciones, además de demostrar que cumplen las medidas mínimas exigidas por el regulador.
No hemos entrado a valorar en las empresas analizadas si los criterios utilizados para elaborar el ranking son eficaces técnicamente o no, pues entendemos que todas estas empresas tienen personal suficientemente cualificado para poner remedios técnicos válidos, pero si hemos puesto de manifiesto las carencias de aquellos aspectos básicos que entendemos son de obligado cumplimiento, y que deberían formar parte de dicha información, en línea con la transparencia y el buen gobierno corporativo esperado .
Tampoco hemos ponderado en función de la relevancia de los criterios valorados, pues entendemos que todos en sí mismo conllevan consecuencias en caso de su no aplicación.
Además del ranking y su resultado, queremos hacer una mención especial a la importancia y relevancia que se da al responsable de ciber seguridad en estas empresas. Su función y participación son indispensables en los comités de dirección, por cuanto que, además de manejar presupuestos cada vez más elevados el impacto económico en la cuenta de resultados como consecuencia de un incidente informático es considerable

El análisis realizado nos lleva a las siguientes conclusiones:

☐ Hay una gran dispersión en los resultados obtenidos, que denotan enormes diferencias entre las empresas situadas en el Top 5, en una posición de excelencia en la transparencia en ciberseguridad, y las que se encuentran a la cola del ranking, que no muestran apenas interés por informar a sus accionistas e inversores en este sentido.

☐ Al ordenar las empresas y sus resultados por sectores se observa una mejor puntuación en transparencia en aquellos sectores en los que las empresas hacen un uso más intensivo de la tecnología por ser inherente a su actividad (Ej. tecnología y telecomunicaciones) y en aquellos en los que tienen un mayor protagonismo los canales digitales utilizados en la relación con los clientes (Ej. servicios financieros y seguros, servicios de consumo).

☐ En lo relativo a los 10 criterios objeto de evaluación se pone de manifiesto que las empresas han informado en su gran mayoría sobre los aspectos más básicos de la gestión en ciberseguridad, pero de forma insuficiente para alcanzar los niveles deseables de transparencia, demostrar el buen gobierno en la gestión y, sobre todo, dar respuesta al interés que suscita la ciberseguridad entre las partes interesadas. La identificación de los ataques en ciberseguridad como un riesgo relevante, el cumplimiento de las obligaciones legales y el establecimiento de una política de seguridad de la información son elementos necesarios, pero también es necesario informar sobre la existencia de un CISO y sobre el apoyo que recibe de la alta dirección. La involucración de la alta dirección podría mostrarse aportando información sobre otros dos criterios: la concienciación y capacitación a los empleados en Ciberseguridad y la estrategia de las actuaciones en seguridad de la información.

"Informe de transparencia en la información sobre ciberseguridad en las empresas del IBEX 35. 2021"

☐ Las empresas del IBEX 35, salvo excepciones, aportan poca o ninguna información sobre aspectos que pondrían de manifiesto una madurez y compromiso claro de la alta dirección con la gestión de los riesgos ante ataques de ciberseguridad, como la existencia de un órgano interno o externo para detectar vulnerabilidades y gestionar incidentes adoptando las medidas adecuadas; la certificación de cumplimiento en ciberseguridad de estándares internacionales, que conlleva una auditoría realizada por una tercera parte independiente; o la existencia de un plan que asegure la continuidad de los servicios esenciales de sus clientes hasta la total recuperación de sus sistemas informáticos.

Por último, queremos resaltar dos aspectos relevantes no valorados, pero si es conveniente tener en cuenta:
- La disponibilidad de un seguro de ciber riesgo como última barrera de protección frente a los ciberataques, que esté adecuadamente dimensionado (no todas las empresas con independencia del tamaño. tienen la misma exposición al riesgo) y garantice la correcta cobertura de sus necesidades.
- El análisis y medición de la huella digital de todos sus empleados, lo que afecta, no sólo a las políticas de contratación, sino más importante aún, al comportamiento y manejo que estos hacen en sus entornos digitales públicos y privados, y que afectan claramente a la empresa.

6. Recomendaciones

Las empresas que se sitúan en el Top 5 del ranking de transparencia en ciberseguridad, esto es, CaixaBank, Telefónica, Ferrovial, Aena y Amadeus, pueden ser consideradas ejemplo a imitar por otras empresas. Por ello, incluimos a continuación una relación de las mejores prácticas en transparencia de información observadas en ellas, así como otras que consideramos son de aplicación e interés para todo el conjunto de empresas.

☐ Realización de auditorías de ciber seguridad.
☐ Utilización como referencia de sus actuaciones de reconocidos estándares internacionales como National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) e ISO 27001.
☐ Certificación CERT y cooperación activa nacional e internacional con otros CERT.
☐ Revisión y adecuación de protocolos de seguridad de la información para adaptarlos a la situación COVID 19.
☐ Consideración de la gestión de la seguridad de la información como un proceso de mejora continua.
☐ 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), que incluyan un Plan de Recuperación ante Desastres (Disaster Recovery Plan DRP) y un Plan de Servicio sin TIC.
☐ Políticas de seguridad de la información y recursos de gestión y de respuesta ante incidentes coordinados globalmente.
☐ Programa de recompensas a empleados por descubrimiento de vulnerabilidades.
☐ Lecciones aprendidas a partir de los incidentes, que constituyen una parte fundamental de la realimentación hacia los proyectos de mejora de la seguridad.
☐ Implantación de Indicadores de actuaciones en Ciberseguridad, como el número de asistentes a cursos de formación en Protección de Datos y Ciberseguridad, el número de auditorías internas o de incidentes de ciberseguridad.
☐ Participación de la alta dirección en comisiones dependientes del Consejo que gestionen asuntos de ciberseguridad.
☐ Aprobación de planes e inversiones estratégicas en ciberseguridad.
☐ Designación de un CISO global y su participación en los Comités de Dirección.

I. Anexo

RANKING DE TRANSPARENCIA EN CIBERSEGURIDAD EMPRESAS IBEX 35

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

RESULTADOS POR SECTORES

SECTOR	POSICIÓN
Tecnología y Telco.	1
Serv. Financieros y Seguros	2
Servicios de Consumo	3
Bienes de Consumo	4
Energía	5
Construcción e Industria	6
Inmobiliario	7