PRIMER ESTUDIO SOBRE EL BUEN GOBIERNO DE LA CIBERSEGURIDAD EN ESPAÑA

ISMS CYBER-REPORTING INITIATIVE
PRELIMINARY REPORT

isms forum

UNIVERSIDAD COMPLUTENSE MADRID

PRIMER ESTUDIO SOBRE EL BUEN GOBIERNO DE LA CIBERSEGURIDAD EN ESPAÑA – ISMS CYBER-REPORTING INITIATIVE PRELIMINARY REPORT

Pedro López Sáez

Director de la Cátedra UCM-ISMS Forum sobre ciberseguridad y protección de datos

plopezsa@ucm.es

Profesor titular de Organización de Empresas en la Universidad Complutense de Madrid (UCM). Doctor en Dirección de Empresas por la UCM (2005), con Premio Extraordinario, cuenta con una experiencia docente de más de veinte años, de los cuales, los diez últimos han estado dedicados a asignaturas relacionadas con el emprendimiento y la creación de empresas. Entre 2015 y 2019 ha sido coordinador del Máster Universitario en Comercio Electrónico de la UCM, y entre 2018 y 2023, director de la Preincubadora de Empresas de la Facultad de Comercio y Turismo de la UCM. Actualmente, es asesor de Estrategias de Emprendimiento del Vicerrectorado de Formación Permanente, Empleabilidad y Emprendimiento de la UCM, director de la Cátedra Extraordinaria UCM-ISMS Forum sobre Ciberseguridad y Protección de Datos (desde 2024), así como director del Máster de Formación Permanente en Protección de Datos y Seguridad de la Información (desde 2021).

RESUMEN EJECUTIVO

Los incidentes de ciberseguridad representan una amenaza creciente y de carácter estratégico para las organizaciones modernas, pues sus impactos potenciales no sólo son significativos, sino que trascienden el ámbito técnico, pudiendo afectar a la estabilidad financiera, la reputación y la confianza de los grupos de interés. Esta problemática tiene especial relevancia para las sociedades cotizadas. En respuesta a este panorama y al creciente escrutinio regulatorio a nivel global (ej. SEC en EE.UU., Directiva NIS2 en la UE), que exige una mayor supervisión y rendición de cuentas por parte de los órganos de administración de las sociedades cotizadas, el Foro Nacional de Ciberseguridad y la CNMV publicaron el Código de Buen Gobierno de la Ciberseguridad. Este Código sirve como una guía esencial para las sociedades cotizadas españolas, promoviendo un marco de Gobernanza, Riesgo y Cumplimiento (GRC) en ciberseguridad.

Sin embargo, hasta la fecha existía una notable falta de conocimiento sobre el grado de adopción y seguimiento de estas recomendaciones por parte del tejido empresarial español. Para abordar esta carencia, la Cátedra Extraordinaria UCM-ISMS Forum sobre ciberseguridad y protección de datos ha llevado a cabo el primer estudio nacional en la materia, basado en entrevistas en profundidad con responsables de ciberseguridad (CISOs) de 20 de las empresas que conforman el IBEX-35 (representando el 57,14% del índice). Este informe presenta los primeros resultados del análisis de las entrevistas realizadas, ofreciendo una evaluación de referencia sobre el estado actual del buen gobierno de la ciberseguridad en este tipo de empresas.

Algunos de los hallazgos clave del análisis realizado revelan que:

- Existe un **alto nivel de conocimiento y compromiso** con el Código de Buen Gobierno de la Ciberseguridad entre los CISOs del IBEX-35. Un 95% de los entrevistados conoce el Código, y muchos participan activamente en su implementación o han realizado auditorías internas de adecuación al mismo en sus organizaciones.
- Las empresas del IBEX-35 muestran un **progreso significativo en el reporte regular** de temas de ciberseguridad a la alta dirección y los órganos de administración. Si bien la frecuencia varía (predominantemente trimestral para comisiones, anual para el Consejo), la mayoría tiene mecanismos definidos para esta comunicación. Un 80% de las empresas tienen definida una periodicidad para este reporte.

- La ciberseguridad se está incorporando **de manera habitual en las agendas** de las reuniones del órgano de administración o de sus comisiones delegadas especializadas (principalmente Auditoría, Control y Riesgos), con un 95% de los entrevistados afirmando que esto ocurre. Un 60% la incluye la supervisión de la ciberseguridad regularmente en alguna comisión. Esto subraya la creciente conciencia en el más alto nivel.
- La **presencia de consejeros con experiencia específica en ciberseguridad** no está aún generalizada, habiendo un margen de mejora para alinearse con las recomendaciones nacionales e internacionales más exigentes en la materia. Algo más de la mitad de las empresas dice tener consejeros con conocimientos de ciberseguridad o de tecnología, siendo este un matiz importante, pues no cabe considerarlos como equivalentes.
- Los **comités de ciberseguridad con la participación de la alta dirección y las áreas más importantes** de la empresa ya son una práctica generalizada en las sociedades cotizadas (el 85% de los entrevistados cuenta con uno), planteando algunas incluso varios niveles jerárquicos para los mismos, con una configuración en cascada de acuerdo con los diferentes estratos de la dirección estratégica.
- A pesar de que los CISOs cuentan con las capacidades técnicas adecuadas, hay bastantes casos en los que se percibe una **insuficiencia de recursos humanos especializados** y una configuración de estructura organizativa que deriva en un **posicionamiento jerárquico del CISO que puede limitar su influencia estratégica** dentro de la empresa y su independencia en el desarrollo de sus funciones.
- La **realización de simulacros y pruebas** de las medidas de protección, respuesta y recuperación es una práctica extendida, con todos los entrevistados confirmando su realización. Sin embargo, la frecuencia y el alcance de pruebas y simulacros varía, y existe una limitación notable en la **inclusión de toda la organización (55% no lo hace) y, de forma más acuciante, de la cadena de suministro (90% no la incluye completamente)** debido a la complejidad y limitaciones de recursos que supondría hacerlo.
- Un **desafío crítico e identificado por los propios CISOs es la gestión de incidentes significativos en la cadena de suministro o de actividades dependientes de terceros**. Solo la mitad de los entrevistados informa sobre estos incidentes de manera regular, y casi la mitad (45%) reconoce dificultades

importantes para manejarlos y reportarlos eficazmente. Las entrevistas destacan que actualmente los riesgos de terceros son percibidos como los de mayor crecimiento e impacto potencial.

En conjunto, si bien los resultados preliminares indican un conocimiento y una creciente incorporación de la ciberseguridad en la dinámica de reporte y agenda de los órganos de administración, aún existen áreas significativas de mejora. El desafío de la cadena de suministro y la necesidad de ampliar el alcance de los simulacros destacan como puntos críticos que requieren atención y recursos, pero que sin duda resultan considerablemente complejos de abordar. Del mismo modo lo es la escasez de recursos para las unidades de ciberseguridad, especialmente los de carácter humano.

El mensaje clave de este informe es claro: para afrontar eficazmente el panorama de ciberamenazas y cumplir con las crecientes expectativas regulatorias y de los stakeholders, es fundamental **reforzar la implicación estratégica y la supervisión activa de los órganos de administración en la dirección y ejecución de las actividades de ciberseguridad**. Actualmente, la ciberseguridad debe ser considerada como un pilar esencial del Buen Gobierno Corporativo y un factor crítico para la resiliencia y el éxito empresarial a largo plazo, lo que requiere una supervisión activa y estratégica.

Este informe busca ser una evaluación de referencia que impulse a los CISOs a escalar la conversación sobre ciberseguridad a los más altos niveles de sus organizaciones y a los miembros de los órganos de administración a asumir un rol más proactivo y estratégico en esta materia.

1. INTRODUCCIÓN

La ciberseguridad ha dejado de ser una preocupación meramente técnica para convertirse en uno de los riesgos estratégicos más urgentes a los que se enfrentan las organizaciones en la actualidad. Los ciberincidentes pueden acarrear pérdidas financieras significativas, interrupciones de las operaciones, daños irreparables para la reputación corporativa y una erosión crítica de la confianza de inversores, clientes y otros grupos de interés (Valkenburg y Bongiovanni, 2024). Este escenario, exacerbado por un panorama de amenazas en constante evolución, exige un enfoque integral que trascienda la implementación de controles técnicos para abarcar también dimensiones organizativas, humanas y, fundamentalmente, de buen gobierno corporativo de la ciberseguridad (Gale, Bongiovanni, y Slapnicar, 2022).

En paralelo a la creciente sofisticación de las ciberamenazas, en los últimos años el entorno regulatorio global ha evolucionado drásticamente para imponer una mayor responsabilidad a los órganos de administración en materia de ciberseguridad. Iniciativas como las nuevas normativas de la Securities and Exchange Commission (SEC) en Estados Unidos o la Directiva (UE) 2022/2557 (conocida como NIS2) en Europa, subrayan la expectativa de que la alta dirección no solo supervise activamente los riesgos cibernéticos, sino que también asegure la existencia de procesos robustos para su identificación, gestión y comunicación. La NIS2, en particular, demanda un elevado nivel común de ciberseguridad y establece un claro mandato para que los consejos de administración evalúen amenazas, respondan a incidentes y promuevan la resiliencia organizativa, introduciendo además un régimen sancionador significativo para impulsar su cumplimiento.

Este contexto global de creciente riesgo y exigencia regulatoria ha puesto de manifiesto la necesidad de contar con marcos de referencia sólidos para el buen gobierno de la ciberseguridad. En España, el Foro Nacional de Ciberseguridad, en colaboración con la Comisión Nacional del Mercado de Valores (CNMV), publicó en julio de 2023 el Código de Buen Gobierno de la Ciberseguridad (CNMV - Foro Nacional de Ciberseguridad, 2023). Este Código, estructurado en principios y recomendaciones alineados con el Código de Buen Gobierno de las Sociedades Cotizadas, tiene como objetivo servir de guía para que las organizaciones, especialmente las cotizadas, fortalezcan sus mecanismos de supervisión y rendición de cuentas en materia de ciberseguridad y mejoren la toma de decisiones en esta área crítica.

A pesar de la existencia de este marco normativo y la creciente conciencia sobre la importancia de la ciberseguridad a nivel ejecutivo (Pearlson y Hetner, 2022; Rothrock, Kaplan y Van Der Oord, 2018), la investigación académica previa y la práctica sugieren que la ciberseguridad a menudo no recibe la atención estratégica adecuada por parte de los órganos de administración (Gale, Bongiovanni, y Slapnicar, 2022). Esto puede deberse a la percepción persistente de la ciberseguridad como un problema técnico complejo, o a la delegación excesiva de su supervisión en comités sin asegurar una comprensión global por parte de todo el consejo de administración (Savaș y Karataș, 2022; Hartmann y Carmenate, 2021). Asimismo, existe una carencia de estudios que evalúen empíricamente el grado de adopción de las recomendaciones de buen gobierno de la ciberseguridad por parte de las empresas españolas.

Para abordar esta falta de conocimiento y contribuir a la mejora de las prácticas de gobernanza de la ciberseguridad en España, la Cátedra Extraordinaria UCM-ISMS Forum sobre ciberseguridad y protección de datos ha llevado a cabo el primer estudio nacional enfocado específicamente en el buen gobierno de la ciberseguridad en el contexto del IBEX-35. Las empresas que conforman este índice no solo representan un pilar fundamental de la economía española, sino que también actúan como referentes en materia de transparencia y buen gobierno, enfrentándose a su vez a las ciberamenazas de mayor impacto y a las mayores exigencias regulatorias. Comprender su nivel de madurez en la adopción de un marco GRC para la ciberseguridad y los desafíos que encuentran al hacerlo es esencial para promover las mejores prácticas en el sector.

Este informe presenta los resultados preliminares de este estudio, basado en entrevistas en profundidad con responsables de ciberseguridad de una parte significativa de las empresas del IBEX-35. A través del análisis de respuestas a preguntas clave desarrolladas a partir de las recomendaciones del Código de Buen Gobierno de la Ciberseguridad, buscamos ofrecer una evaluación de referencia sobre el estado actual de la gobernanza de la ciberseguridad en estas organizaciones. Nuestro objetivo es proporcionar información valiosa para los CISOs, ayudándoles a presentar la ciberseguridad como un factor estratégico a sus órganos de administración, y para los propios consejeros, facilitando la comprensión de su papel y responsabilidades en la supervisión de este riesgo crítico. En último término, aspiramos a que este estudio contribuya a la integración de la ciberseguridad como un elemento esencial de la información clave y la estrategia de negocio de las empresas cotizadas españolas.

La estructura de este informe es la siguiente: Tras esta introducción, el lector encontrará un detalle del marco de situación y la motivación que impulsaron este estudio. Posteriormente, se presentará la metodología empleada. Las secciones centrales detallarán los hallazgos clave obtenidos de las entrevistas, seguidas de un análisis más de desafíos específicos como la gestión del riesgo en la cadena de suministro y la realización de simulacros. Finalmente, se ofrecerán algunas conclusiones y un conjunto de recomendaciones prácticas derivadas de los hallazgos realizados por el estudio.

2. MARCO DE SITUACIÓN

Los ciberincidentes no solo provocan pérdidas financieras para las organizaciones que los sufren, sino que también afectan a la confianza que tienen en ellas sus grupos de interés.

Por ello, aunque tradicionalmente la ciberseguridad se ha abordado de manera predominante a través de controles técnicos, es necesario comprender que su naturaleza y repercusiones resultan multifacéticas (Valkenburg y Bongiovanni, 2024).

El 26 de julio de 2023, la Stock Exchange Comission (SEC en lo sucesivo), la equivalente norteamericana de la Comisión Nacional del Mercado de Valores (CNMV) española, adoptó nuevas normas para mejorar y estandarizar la comunicación relativa a la gestión, estrategia, gobierno e incidentes relacionados con la ciberseguridad por parte de empresas cotizadas. Estas nuevas normas tienen dos componentes principales:

a) Comunicación de incidentes de ciberseguridad que se hayan materializado.

b) Comunicación anual sobre la gestión, estrategia y gobierno de la ciberseguridad.

Respecto al primer punto, las empresas cotizadas deben informar sobre cualquier incidente de ciberseguridad experimentado y que se considere materializado, describiendo su naturaleza, alcance y tiempo, y también su impacto concreto o razonablemente probable.

En cuanto a las comunicaciones anuales, las sociedades cotizadas deben describir sus procesos (en caso de haberlos) para la evaluación, identificación y gestión de los riesgos derivados de las ciberamenazas, y describir si alguno de estos riesgos ha afectado (o es razonablemente probable que afecte) materialmente a su estrategia empresarial, resultados operativos o situación financiera. Esto incluye, de manera específica:

- Describir la supervisión del consejo sobre los riesgos derivados de las amenazas de ciberseguridad.
- Describir el papel de la dirección en la evaluación y gestión de riesgos materiales derivados de amenazas de ciberseguridad.

Como puede verse, la SEC atribuye a los consejos de administración la responsabilidad de supervisar la gestión del riesgo cibernético en las organizaciones y lo que se ha denominado gobernanza de la ciberseguridad.

La Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas, conocida popularmente como NIS2, comparte las preocupaciones planteadas por la SEC y adelanta que la trasposición de la citada directiva en el territorio de la Unión Europea apuntará en una dirección similar a la que sigue Estados Unidos.

En concreto, la NIS2 requiere que las entidades con más de 250 empleados y

una facturación anual de más de 50 millones de euros y/o un balance anual superior a 43 millones de euros desarrollen medidas de ciberseguridad específicas, entre las que se incluyen el análisis de riesgos y las políticas de seguridad del sistema de información, la respuesta a incidentes, la continuidad del negocio y la gestión de crisis, la seguridad de la cadena de suministro, la evaluación de la eficacia de las medidas de gestión de riesgos y la divulgación de vulnerabilidades y encriptación.

La mayor exigencia impuesta por la Directiva NIS2 tiene como objetivo garantizar un elevado nivel común de ciberseguridad en toda la Unión y avanza hacia un marco de buen gobierno de la ciberseguridad, gestión del riesgo cibernético y cumplimiento normativo, conocido internacionalmente mediante el acrónimo de GRC (*Governance, Risk, and Compliance*). Para lograr este objetivo, destaca la importancia de que los consejos de administración estén involucrados en la ciberseguridad y que se establezcan marcos nacionales de seguridad de los sistemas de redes e información, definiendo estrategias nacionales de seguridad, estableciendo capacidades nacionales y aplicando medidas reguladoras.

La NIS2 también señala la necesidad de que los consejos de administración evalúen los riesgos y amenazas cibernéticas, y tomen medidas en respuesta a incidentes de ciberseguridad. Se plantea así, la necesidad de supervisión y rendición de cuentas en materia de ciberseguridad por parte de los consejos de administración, exigiendo que implementen y cumplan con las medidas de seguridad reforzadas propias de las entidades importantes y esenciales.

Como sucediera con el RGPD, posiblemente el argumento de la NIS2 con mayor peso para llamar la atención de las organizaciones obligadas sea el marco de sanciones que la acompañará, con multas por incumplimiento que pueden alcanzar hasta los 10 millones de euros o el 2% de la facturación anual (la que suponga mayor cuantía). Como señalan Gale, Bongiovanni, y Slapnicar (2022), las presiones coercitivas impuestas por las regulaciones son el principal impulso para la reacción de los consejos de administración de cara a tomar medidas y promover un marco de GRC de ciberseguridad en sus organizaciones. Sin embargo, como indican estos mismos autores, la alta dirección no siempre es completamente consciente de sus deberes y responsabilidad en lo que respecta a la supervisión de la ciberseguridad.

Las potenciales multas de hasta 10 millones de euros o del 2% de la facturación anual suponen cifras muy considerables para la mayoría de las empresas, y especialmente para las grandes cotizadas. Con este régimen sancionador significativo, la NIS2

otorga a las autoridades nacionales de supervisión de potentes herramientas coercitivas con las que asegurar el cumplimiento de las medidas de ciberseguridad y gobernanza planteadas. No obstante, más allá de la amenaza de la sanción, es necesario contar con una adecuada conciencia situacional sobre la problemática de base.

Como sugieren Pearlson y Hetner (2022), para lograr una adecuada supervisión y cumplir con un entorno normativo cada vez más exigente, los consejeros necesitan mejorar sus conocimientos sobre ciberseguridad. La formación es esencial para entender la problemática específica de la ciberseguridad en cada organización y poder tomar decisiones informadas. En primer lugar, los miembros del consejo de administración deben aceptar que es imposible lograr una protección absoluta contra cualquier amenaza, por lo que toda organización tiene un riesgo determinado de ser atacada y verse comprometida. Así, el enfoque más racional es asegurarse de que la organización esté preparada para recuperarse de un ciberataque con el menor daño posible para sus operaciones, resultados financieros y reputación corporativa.

Rothrock, Kaplan y Van Der Oord (2018) apuntan que, para mejorar la situación actual, la alta dirección debe contar con una formación básica en ciberseguridad, que muestre su naturaleza estratégica y el alcance e implicaciones de los riesgos cibernéticos. Sin esta base, no se podrán diseñar e implementar estrategias que permitan mantener el negocio durante un ciberataque, recuperarse rápidamente después del mismo y adoptar mejoras en la infraestructura digital de la organización con posterioridad, a partir de las lecciones aprendidas.

3. MOTIVACIÓN Y OBJETIVOS DEL ESTUDIO

Con el fin de contribuir a una mejor la toma de decisiones en materia de ciberseguridad por parte de los órganos de administración y de la alta dirección, haciéndoles más conscientes de los riesgos cibernéticos y de su papel y responsabilidades de gestión en este ámbito, el 14 de julio de 2023, el Foro Nacional de Ciberseguridad publicó el Código de Buen Gobierno de la Ciberseguridad. Dada la especial relevancia que este código puede tener para las sociedades cotizadas, en su elaboración y difusión participó la CNMV, reconociendo que la creciente frecuencia e intensidad de las ciberamenazas está incrementando su importancia para la supervisión de la gestión y control de los riesgos corporativos.

El código aspira a ser utilizado por las organizaciones como guía para el cumplimiento de sus obligaciones de información ante los distintos organismos de supervisión. Para ello, sigue un esquema similar al Código de Buen Gobierno de las Sociedades Cotizadas, basado en principios y recomendaciones. De este modo, el Código de Buen Gobierno de la Ciberseguridad propone 13 principios y 25 recomendaciones, organizados en torno a tres grandes bloques: estrategia y organización, gestión y supervisión.

En las últimas décadas, los consejos de administración han incorporado a su estrategia valores de concienciación ambiental, social y buen gobierno (*Environmental, Social, and Governance* o el acrónimo inglés ESG). La Ley de Sociedades de Capital establece el deber de difundir información sobre el grado de seguimiento de las recomendaciones del Código de Buen Gobierno de las Sociedades Cotizadas o bien la explicación de la falta de seguimiento de dichas recomendaciones. En los aspectos sociales y medioambientales, las memorias anuales de las sociedades cotizadas suelen incorporar uno o varios estados de información no financiera, de acuerdo con estándares internacionales como los de la GRI (Global Reporting Initiative). Sin embargo, la ciberseguridad aún no está presente ni como obligación legal de información ni adecuadamente desglosada y definida en estándares reconocidos sobre la elaboración de informes periódicos. El Código de Buen Gobierno de la Ciberseguridad sería un primer paso en esta dirección.

Como demuestran tanto la práctica como varios trabajos académicos, la ciberseguridad no es únicamente un desafío técnico, sino que también abarca dimensiones organizativas, humanas y de buen gobierno (Valkenburg y Bongiovanni, 2024). Por ello, con negocios cada día más digitalizados, es lógico que la SEC o la CNMV consideren que incorporar a las memorias anuales una serie elementos básicos sobre ciberseguridad sea crítico para que las sociedades cotizadas puedan:

- Generar confianza y demostrar transparencia ante accionistas e inversores.
- Mejorar el control interno y la responsabilidad corporativa, para mejorar la competitividad y responder de manera satisfactoria ante los intereses legítimos de los distintos grupos de interés.
- Contar con una diferenciación de funciones, deberes y responsabilidades, que ofrezca el máximo rigor y profesionalidad en la definición, ejercicio y supervisión de la ciberseguridad.

Se espera que los consejos de administración asuman un papel estratégico en la gestión del riesgo

cibernético, participando en el desarrollo de un plan estratégico de ciberseguridad y una hoja de ruta para su implantación. De este modo, el buen gobierno de la ciberseguridad es fundamental para poder alinear los esfuerzos de ciberseguridad con los objetivos organizativos, garantizar una asignación adecuada de recursos y fomentar una cultura de seguridad a nivel corporativo (Valkenburg y Bongiovanni, 2024).

Lamentablemente, investigaciones recientes (Gale, Bongiovanni, y Slapnicar, 2022) señalan que, en general, en la actualidad la ciberseguridad no recibe suficiente atención por parte de los consejos de administración por varios motivos:

- La ciberseguridad todavía se percibe como un problema principalmente técnico, que requiere conocimientos previos para ser discutido adecuadamente. Así, se produce un doble problema sobre los informes sobre ciberseguridad empleados para la toma de decisiones y la rendición de cuentas. Por una parte, los informes excesivamente técnicos pueden provocar una falta de compromiso de la dirección en caso de que no tenga experiencia o conocimientos específicos sobre este ámbito. Por otra, emplear informes poco formalizados puede llevar a tomar decisiones de ciberseguridad subóptimas.
- Delegar la supervisión de la ciberseguridad en comités de riesgo y auditoría, puede reducir la carga de trabajo para el conjunto del consejo y reducir en parte algunos de los problemas anteriores. No obstante, esta delegación puede generar informes de menor calidad que cuando la cuestión debe de decidirse por el conjunto del consejo.

Hasta la fecha, se desconoce el grado de madurez que existe en España en cuanto a buen gobierno de la ciberseguridad o las dificultades que tienen los consejeros españoles para desarrollar un marco adecuado para el Gobierno, Riesgo y Cumplimiento (GRC) en sus organizaciones. Por ello, desde la Cátedra Extraordinaria UCM-ISMS Forum sobre ciberseguridad y protección de datos ha decidido desarrollar el primer estudio nacional en materia de buen gobierno de la ciberseguridad. La Cátedra, nacida del compromiso de la Universidad en las áreas de formación, investigación y desarrollo, y difusión y transferencia del conocimiento en el ámbito de la ciberseguridad, entiende que esta se ha convertido únicamente en un aspecto crítico para el desarrollo económico de organizaciones y países, así como de la calidad de vida de los ciudadanos en la sociedad de la información.

Dado que para poder desarrollar su ciberresiliencia, las organizaciones necesitan contar con el compromiso de

sus líderes, unas políticas internas adecuadas y una cultura de seguridad (Valkenburg y Bongiovanni, 2024), es necesario investigar quiénes y cómo lo han logrado, de cara a promover las mejores prácticas en este ámbito. Comprender mejor el grado de madurez de las empresas españolas en cuanto a buen gobierno de la ciberseguridad y los aspectos más problemáticos para mejorar en estas actividades es un paso esencial para incorporar la ciberseguridad como una parte esencial de la información clave de cualquier empresa cotizada.

4. METODOLOGÍA

La elaboración del presente informe se fundamenta en un diseño de investigación cuidadosamente estructurado, buscando proporcionar una comprensión profunda del grado de madurez en materia de Gobernanza, Riesgo y Cumplimiento (GRC) de ciberseguridad en las principales empresas cotizadas españolas. Este enfoque metodológico combina la profundidad cualitativa con un análisis inicial que permite cuantificar ciertas tendencias, sentando las bases para futuras investigaciones más amplias.

Desde una perspectiva académica, este estudio constituye una investigación de carácter exploratorio, utilizando un enfoque cualitativo o de métodos mixtos, siguiendo la línea marcada por trabajos recientes como los de Gale, Bongiovanni, y Slapnicar (2022) y Valkenburg y Bongiovanni (2024). El objetivo primordial es analizar el estado actual y el grado de madurez en GRC de ciberseguridad dentro de la población de estudio, identificando las prácticas existentes, los desafíos y las áreas de mejora. Este diseño es particularmente pertinente dada la limitada investigación previa en este campo en el contexto español. A pesar de su evidente importancia, el campo del buen gobierno de la ciberseguridad está muy poco desarrollado por parte de la investigación académica, según indican, por ejemplo, Savaș y Karataș (2022) y Hartmann y Carmenate (2021).

Esta metodología se ha diseñado para generar *insights* accionables y fiables, basándose en la experiencia directa de los líderes de ciberseguridad de algunas de las organizaciones más relevantes del panorama económico español. La selección del enfoque cualitativo mediante entrevistas en profundidad permite capturar la complejidad y los matices de la gestión de la ciberseguridad a nivel estratégico, información crucial para comprender las dinámicas del sector y asesorar eficazmente.

La población objetivo del estudio estaba constituida por las empresas que integran el índice IBEX-35. Este índice representa a las 35 sociedades cotizadas de mayor liquidez y capitalización en la Bolsa de Madrid, lo que las convierte en un referente

fundamental para el tejido empresarial español y además las somete a un mayor escrutinio público y exigencia en términos de transparencia y buen gobierno.

Se intentó contactar con la totalidad de CISOs de las empresas que conforman el IBEX-35. Finalmente, la muestra final del estudio está compuesta por 20 de estas 35 empresas, lo que representa una tasa de participación del 57,14% del índice. La selección de los participantes que actuaron como representantes de cada organización se centró en los responsables de ciberseguridad (CISOs), puesto que son ellos quienes poseen el conocimiento y la experiencia directa en la implementación y supervisión de las prácticas de ciberseguridad a nivel ejecutivo.

La principal técnica de recogida de datos empleada fue la entrevista en profundidad, puesto que permite explorar en detalle las percepciones, experiencias y opiniones de los entrevistados. Las entrevistas en profundidad son una técnica de investigación cualitativa que permite recopilar información detallada y profunda, lo cual resulta de especial relevancia en estudios de carácter exploratorio como el que se plantea. El *Institute of Internal Auditors* (IAA) plantea el modelo de las 3 líneas de defensa, que autores como Slapnicar, Axelsen, Bongiovanni y Stockdale (2023) han aumentado a 5 líneas para el caso de las responsabilidades en el gobierno de la ciberseguridad. Estos autores también emplean entrevistas en profundidad para entender el riesgo cibernético y el gobierno de la ciberseguridad, así como los roles implicados en este campo.

En el contexto de este estudio, las entrevistas con los CISOs del IBEX-35 facilitaron la obtención de información rica y matizada no sólo sobre el cumplimiento o no de las recomendaciones del Código de Buen Gobierno de la Ciberseguridad, sino sobre los desafíos y las buenas prácticas asociadas a cada una de las recomendaciones. Como se ha indicado, la utilización de entrevistas en profundidad con perfiles clave es una técnica validada en estudios similares sobre gobernanza y riesgo cibernético (véase Slapnicar, Axelsen, Bongiovanni y Stockdale, 2023). En general, las entrevistas tuvieron una duración aproximada de una hora, requiriendo algunas de ellas más tiempo y cerrándose otras en menos. Las entrevistas se llevaron a cabo por Pedro López Sáez, Director de la Cátedra Extraordinaria UCM-ISMS Forum sobre Ciberseguridad y Protección de Datos y/o Beatriz García González, Deputy Director – Head of Projects Unit de ISMS Forum.

El instrumento utilizado para guiar las entrevistas fue un cuestionario estructurado, diseñado específicamente para evaluar el grado de alineación de las empresas con las

25 recomendaciones del Código de Buen Gobierno de la Ciberseguridad. El cuestionario completo consta de 56 preguntas, ya que algunas recomendaciones fueron evaluadas a través de múltiples preguntas para asegurar una comprensión exhaustiva de las prácticas de cada organización. El cuestionario completo empleado como guía de las entrevistas en profundidad se incluye como anexo de este informe. El cuestionario fue diseñado para permitir tanto respuestas dicotómicas (sí/no) como la recopilación de información cualitativa detallada sobre los motivos y obstáculos para el cumplimiento.

Completadas las entrevistas en profundidad y ante la imposibilidad de incrementar la tasa de respuesta con más CISOs de empresas del IBEX-35 por su negativa a participar o falta de respuesta a la solicitud para hacerlo, se procedió al análisis de la información recogida en ellas. La primera fase del análisis de datos, cuyos resultados preliminares se presentan en este informe, consistió en la transcripción y análisis de las respuestas literales obtenidas en las entrevistas. Se realizó una evaluación cualitativa inicial enfocada en un subconjunto específico de preguntas consideradas como de mayor interés (17 de las 56 preguntas totales, representando el 30%). A partir de este análisis cualitativo, se intentaron generar porcentajes de cumplimiento para las preguntas analizadas siempre que fuese posible, así como una extracción de la información más relevante para incluir en este informe, presentándola de manera anonimizada y que impidiera identificar a la persona entrevistada o su organización.

Es importante destacar que, en todo momento del estudio, se ha garantizado la estricta confidencialidad de las respuestas proporcionadas por parte de los entrevistados, con el compromiso de que las grabaciones realizadas durante las entrevistas serían borradas una vez transcritas las mismas y que la información recopilada será manejada de manera agregada, asegurando la no identificación de personas u organizaciones específicas en la presentación de los resultados en informes como este o cualquier otro tipo de comunicación derivada del estudio. La confidencialidad no sólo se ha establecido para asegurar el respeto a los principios éticos de la investigación, sino también para fomentar un ambiente de confianza durante las entrevistas que permitiera a los participantes ofrecer respuestas lo más sinceras y detalladas posible, evitando posibles sesgos en la información facilitada.

5. HALLAZGOS CLAVE

Esta sección presenta una parte representativa de los hallazgos del estudio, en este caso derivados del

análisis de 17 de las 56 preguntas incluidas en las entrevistas con los responsables de ciberseguridad de las 20 empresas del IBEX-35 participantes. Si bien este subconjunto representa una visión parcial (12,5% del total de preguntas realizadas en las entrevistas), proporciona *insights* valiosos sobre aspectos fundamentales del buen gobierno de la ciberseguridad en el contexto español.

Los hallazgos que se muestran a continuación destacan áreas donde las empresas del IBEX-35 demuestran un compromiso sólido con el buen gobierno de la ciberseguridad, así como desafíos persistentes que requieren atención estratégica para fortalecer la resiliencia organizacional y cumplir con las expectativas regulatorias y de los *stakeholders*. Estos resultados proporcionan la primera evidencia empírica sobre el grado de seguimiento de aspectos clave del Código de Buen Gobierno de la Ciberseguridad por parte de las principales sociedades cotizadas españolas, contribuyendo a llenar el vacío de investigación identificado en estudios previos (Savaş y Karataş, 2022; Hartmann y Carmenate, 2021).

5.1. Conocimiento del Código de Buen Gobierno de la Ciberseguridad

Como elemento preliminar de análisis abordaremos el nivel de conocimiento y percepción sobre el Código de Buen Gobierno de la Ciberseguridad, para el que incluimos una pregunta en la parte preliminar de la entrevista.

Las empresas del IBEX-35 muestran un alto nivel de conocimiento y compromiso con el Código de Buen Gobierno de la Ciberseguridad, con esfuerzos activos para implementar sus principios y mejorar sus prácticas de ciberseguridad. En concreto, el 95% de los encuestados conoce el Código.

Algunos CISOs mencionaron haber participado en la redacción o elaboración del código, lo que sugiere un compromiso activo con sus principios. Algunas sociedades mencionaron estar adheridas al código, lo que implica incluso un compromiso formal con sus directrices.

Varias organizaciones han realizado un análisis o auditoría sobre la adecuación al Código que tienen sus organizaciones o incluso están desarrollando un plan de mejora al respecto, lo que indica un esfuerzo proactivo para alinearse con sus recomendaciones.

Este alto grado de conocimiento y adopción inicial del Código por parte de las empresas líderes del mercado es una señal positiva. Demuestra que el Código está sirviendo como una guía efectiva para la gestión de la ciberseguridad y la toma de decisiones en este ámbito. Esto facilita el diálogo interno sobre GRC de ciberseguridad y sienta las bases para una gobernanza más madura en este campo.

Además, de cara a nuestra investigación, el alto grado de conocimiento y utilidad atribuido al Código valida su elección como marco de referencia para la elaboración del guion a seguir en las entrevistas en profundidad, habiendo logrado utilizar un lenguaje común con los CISOs entrevistados y una estructura de temáticas sobre gobierno de la ciberseguridad que encaja con la práctica de las empresas cotizadas. De hecho, los resultados sugieren que las presiones regulatorias y de mercado están impulsando a las organizaciones a formalizar su enfoque hacia el buen gobierno de la ciberseguridad.

A continuación, se detallan los hallazgos por área temática, vinculándolos con las recomendaciones correspondientes del Código de Buen Gobierno de la Ciberseguridad.

5.2. Información sobre el CISO, su papel e influencia

Recomendación 7: El máximo responsable de esta unidad será el director de ciberseguridad, director de seguridad de la información o Chief Information Security Officer (en adelante CISO). Esta figura será una persona con el conocimiento, experiencia y competencias adecuadas para desarrollar la función y contará con la suficiente capacidad de decisión e influencia en la organización.

El 75% de los entrevistados se identifican a sí mismos (ocupando el rol de CISO o similar) y máximos responsables de la unidad de ciberseguridad en sus respectivas organizaciones.

Las denominaciones de los cargos relacionados con la ciberseguridad en la alta dirección varían, incluyendo CISO Global, Director de Seguridad de la Información, Director Corporativo de Seguridad, entre otros. Algunos de los entrevistados tiene roles más amplios que incluyen la ciberseguridad, como CIO o Director de Control de Riesgos no Financieros, o reportan directamente al CISO. En definitiva, se ha logrado un contacto directo con los máximos responsables de la ciberseguridad en estas organizaciones, lo que valida el perfil de los entrevistados de cara a ofrecer información cualificada sobre este ámbito. Precisamente, se ha evaluado su nivel de responsabilidad determinando su distancia jerárquica al CEO o Presidente de la compañía, la cual muestra una distribución variada entre los entrevistados, que indica también que no todas las organizaciones conceden el mismo nivel de autoridad o responsabilidad a estos perfiles:

- Un 25% tiene sólo un nivel intermedio hasta el CEO, y un 5% indica incluso dependencia directa del mismo sin niveles intermedios. La mayoría de entrevistados indica tener dos niveles intermedios (40%) entre su cargo y el CEO/Presidente. El 25% tiene tres o más niveles intermedios.

- La dispersión en el número de niveles jerárquicos sugiere que, si bien la función de ciberseguridad está presente en la alta dirección, su posicionamiento exacto y, potencialmente, su acceso directo a la toma de decisiones estratégicas varía significativamente entre las grandes empresas cotizadas. Además, aunque la tendencia es que el CISO sea el máximo responsable (75% de los casos), la existencia de otras figuras en la cúpula de la unidad de ciberseguridad o la división de responsabilidades indica que la estructura y liderazgo de la función pueden variar bastante. Cabe destacar tres casos muy particulares observados. Uno en el que hay dos responsables (el CISO y otra persona para la parte más técnica ligada a sistemas), otro en el que se ha contratado un servicio de "CISO as a Service" y oficina de ciberseguridad, y otro que se define como "pre-CISO", siendo el CISO el máximo responsable.
- Existe un consenso absoluto entre los entrevistados (100%) sobre la adecuación de los conocimientos, experiencia y competencias de la figura responsable de la ciberseguridad para desempeñar su función.
- La mayoría de los entrevistados (65%) afirma de manera clara que la figura responsable tiene suficiente capacidad de decisión e influencia. Aunque el 35% restante también dice tener influencia, matiza su respuesta explicando los mecanismos a través de los cuales la ejerce o mencionando ciertas limitaciones, como cuestiones políticas y jerárquicas.
- Respecto a la influencia del CISO, los encuestados han destacado la importancia que tiene el conocimiento del negocio y no sólo técnico, los mecanismos de escalado y el acceso directo o frecuente a la alta dirección o el consejo, la participación en comités clave y la capacidad de aprobar normas o incluso bloquear iniciativas que no cumplan los requisitos de seguridad. En cualquier caso, se subraya que la influencia se incremente cuando existe una alta dirección proactiva y consciente del impacto de la ciberseguridad en el negocio.

Aunque la percepción general es que el CISO o responsable de ciberseguridad posee la cualificación necesaria en las empresas del IBEX-35, su capacidad de influir y tomar decisiones no siempre es absoluta y puede depender en gran medida de factores organizativos, el nivel de reporte y los canales de comunicación y escalado establecidos. Esto sugiere que, si bien la competencia técnica está cubierta, la efectividad del rol puede verse modulada por su empoderamiento formal e informal dentro de la estructura corporativa.

5.3. Ciberseguridad en el órgano de gobierno

Recomendación 5: La organización aspirará a que, dentro del órgano de administración, haya, al menos, un miembro con experiencia en gestión de ciberseguridad que apoye y valide los objetivos con anterioridad a su aprobación por el equipo directivo.

La mayoría de los entrevistados (58%) afirma que existe al menos un miembro en el órgano de administración o en comités relacionados (como el de auditoría o dirección) con experiencia o conocimientos en ciberseguridad o tecnología relevante. Aproximadamente un tercio de las empresas carece de un miembro con experiencia específica en ciberseguridad en el órgano de administración. Y merece la pena destacar que un 10% matiza sus respuestas, pues menciona "experiencia en tecnología" pero no específicamente en ciberseguridad a nivel de consejo, aunque sí en el comité de dirección, o indicando que, si bien no hay expertos directos, se cuenta con un comité asesor de ciberseguridad para el consejo.

- Los perfiles de estas personas varían: se mencionan miembros del consejo oficialmente formados, personas con buena experiencia en ciberseguridad (en algunos casos con perfiles públicos), miembros con experiencia técnica, con conocimientos específicos de ciberseguridad en el comité de auditoría, consejeros ejecutivos y externos con experiencia en tecnología, una persona experta que ha trabajado en ciberseguridad, un consejero externo cuya experiencia es específicamente en digitalización y ciberseguridad, y un consejero que ha sido CEO y director con responsabilidad sobre la función de CISO.
- Aunque se reconoce la relevancia de esta recomendación del Código, sorprende que varias respuestas indiquen que la experiencia está más relacionada con la tecnología en general que con la ciberseguridad de forma específica. De hecho, algunas empresas conocen los requisitos de la SEC al respecto y cuentan con una persona experta apropiada, pero afirman que "su rol no está definido oficialmente como pide la SEC, sino que es un consejero más".
- En un caso, se señala que el rol de la persona con experiencia no está definido oficialmente como un experto en ciberseguridad según recomendaciones externas (SEC).

Si bien más de la mitad de las empresas representadas cuentan con algún miembro en sus órganos de gobierno (consejo o comités) con experiencia en ciberseguridad o tecnología relacionada, existe una proporción

significativa que aún no la tiene de forma específica en el órgano de administración principal. La experiencia relevante se encuentra en diversas posiciones y con distintos grados de especialización (desde experiencia general en tecnología hasta haber ocupado roles de CISO). La presencia de esta experiencia se percibe como valiosa, aunque su formalización o reconocimiento explícito como experto en ciberseguridad en el órgano de administración principal no es universal ni parece demasiado extendida. En general, la conclusión de este apartado puede describirse con las palabras de uno de los entrevistados cuando afirma que "hay gente que tiene experiencia de IT, etcétera, pero no propiamente en ciberseguridad, y la verdad es que tener la visión de un consejero con experiencia en esto nos vendría genial".

Aunque en un primer momento se barajó la posibilidad de realizar entrevistas también a los consejeros del IBEX con experiencia en ciberseguridad, la dificultad para identificarlos, la escasa definición de su rol de manera forma y su número reducido hace desaconsejable en estos momentos intentar continuar la investigación en esa línea.

5.4. La unidad de ciberseguridad

Recomendación 6: La organización dispondrá de una unidad que asuma la función de definición, impulso y control de la ciberseguridad y que participe en la toma de decisiones y estrategias en este ámbito. Del mismo modo deberá asegurar el reporte adecuado, y a los niveles oportunos, de los riesgos relacionados con la ciberseguridad, así como de los mecanismos de mitigación y control de los mismos que sean necesarios. Esta unidad contará con suficientes capacidades y recursos, materiales y humanos, para la consecución de sus objetivos, y dependerá funcionalmente del órgano de administración, de alguna de sus comisiones especializadas o de cualquier otro órgano o miembro de la alta dirección de la organización, siempre que se mantenga la debida independencia respecto de los responsables de sistemas de redes y de información.

Una abrumadora mayoría de los entrevistados (95%) confirma la existencia de una unidad o área formalmente dedicada a la ciberseguridad dentro de sus organizaciones (el 5% restante menciona la existencia de varias unidades con responsabilidades distribuidas). Esto indica que la función de ciberseguridad cuenta con estructuras dedicadas en la gran mayoría de las grandes empresas españolas. Además, las respuestas sugieren que la unidad de ciberseguridad no es meramente ejecutora, sino que tiene un rol activo en la conceptualización y dirección de las

políticas y medidas de seguridad, aunque el grado de integración en la estrategia general del negocio puede variar.

- El 90% considera que participación de esta unidad en la toma de decisiones y en la definición estratégica. El 10% restante indica participación, pero con matices, por no participar lo suficiente en decisiones de áreas de negocio o planes de futuro, no participando. en todas las decisiones estratégicas de la compañía.
- También el 90% afirma que su unidad asegura el reporte adecuado de los riesgos y mecanismos de control a los niveles oportunos, si bien hay algunas empresas que declaran hacerlo "casi siempre".
- Los niveles de reporte incluyen el comité de dirección, el consejo de administración, la dirección de riesgos, unidades corporativas encargadas del reporte y unidades descentralizadas de gestión de riesgos en cada negocio, o de la mano de auditoría interna.
- El reporte al consejo de administración se ha incrementado en frecuencia por la influencia de las recomendaciones del código de buen gobierno, y algún entrevistado indica que el reporte es una "batalla mensual", lo que indica un esfuerzo constante en esta área.
- Sólo el 25% responde afirmativamente y sin ambigüedad a la cuestión sobre si su unidad cuenta con las capacidades y recursos suficientes para alcanzar sus objetivos de manera eficaz. Aunque otro 40% afirma tener recursos expresan salvedades como que siempre se necesitan más y que les gustaría tener más (expresiones como "siempre te faltan recursos", "siempre se necesita más", o "siempre te gustaría tener más" fueron recurrentes durante las entrevistas.
- Un 20% de los entrevistados ofrece respuestas con matices significativos en cuanto a la disponibilidad de recursos, considerando que se quedan "un poco cortos", especialmente en personal, que es "casi siempre" insuficiente. A pesar de que llegan "de mejor manera" que a otras áreas de la empresa, los recursos humanos parecen ser especialmente escasos. Varios entrevistados resaltan que tienen mayor facilidad para conseguir tecnología que personal, y es común señalar la falta de talento, tanto interno como externo como un problema estructural, no necesariamente resoluble con el apoyo de la alta dirección ("En tecnologías vamos avanzando (…) y ahí nuestra madurez es adecuada, pero si vamos a la capacidad

humana, nos cuesta muchísimo, tanto externamente como internamente, conseguir esos recursos", "estamos formando internamente para que ciertas personas puedan dar el salto, pero eso no nos va a solventar el problema que tenemos"), si bien algunos indican que aunque tienen que "pelear y justificarlo muy bien" para obtener los recursos necesarios, hasta ahora no han tenido problemas mayores.

- Un 15% de las empresas dice sin ambages que su unidad de ciberseguridad no cuenta con las capacidades y recursos suficientes para alcanzar sus objetivos de manera eficaz.
- Un 70% indica dependencia o reporte a un órgano de alta dirección (órgano de administración, comités especializados, o miembro de alta dirección). Los órganos mencionados incluyen el Consejo, Comisión de Auditoría y Control, Comité de Dirección, Director General de Tecnología, Director de Auditoría Interna (quien reporta a Comisión de Auditoría), Comité de Seguridad y Resiliencia, y la Dirección de Riesgos. Un 5% menciona ser parte de un comité paralelo al de riesgo, lo que sugiere una estructura matricial o transversal. El 25% restante indica que no hay una dependencia funcional directa o reportan a otra área no explícitamente de alta dirección en este contexto.
- La independencia de las áreas de Sistemas, Redes o Información (IT) es un factor clave para evitar conflictos de interés y garantizar la objetividad de la función de ciberseguridad. En este aspecto, el 55% afirma tener esta independencia claramente o haberla conseguido recientemente (haber pasado de depender del CIO a estar en paralelo), un indica la falta de esta independencia, señalando que, en la práctica, prima la funcionalidad sobre la seguridad al depender del área de tecnología u otras. Y el 35% restante, aunque dice tener independencia, esta tiene matices (a pesar de reportar al CTO, "mucha independencia, pero con necesidad de entender a otros", independencia práctica a pesar de dependencia formal del CIO, o la independencia derivada de reportar a un nivel superior que integra Operaciones y Tecnología). La frase "todo lo independiente que puede ser" resume la percepción de una independencia deseada, pero a menudo con condicionantes estructurales y operativos.

Las preocupaciones sobre la insuficiencia de recursos para el área de ciberseguridad se centran, en muchos casos, en el factor humano (personal interno y externo especializado), más que en la tecnología. Se menciona la

dificultad para encontrar esas capacidades fuera de la organización. Aunque los presupuestos pueden estar creciendo, la sensación es que no resuelven el problema de fondo ante el crecimiento exponencial de las necesidades impulsado por la transformación digital. Se destaca la necesidad de justificar y mostrar *benchmarks* ante la alta dirección para demostrar las necesidades reales y también la importancia de contar con de un plan de recursos a largo plazo. Esto sugiere que, a pesar de los esfuerzos y el crecimiento de la inversión, la brecha entre las necesidades de ciberseguridad y los recursos disponibles sigue siendo un desafío importante.

Los hallazgos realizados sugieren que la función de ciberseguridad tiende a estar vinculada jerárquica o funcionalmente a la alta dirección o sus comités especializados, lo que le otorga visibilidad, relevancia y cierta independencia. No obstante, la independencia respecto a las áreas operativas de IT, aunque afirmada por la mayoría, presenta matices en una proporción significativa de los casos, indicando que la relación con las áreas de sistemas es un equilibrio complejo que requiere mecanismos de gobernanza y comunicación efectivos para asegurar que la seguridad no se vea comprometida por prioridades operacionales o de negocio. La falta de independencia sigue siendo un problema en algunas organizaciones.

5.5. El comité de ciberseguridad

Recomendación 8: Existirá un comité de ciberseguridad, constituido formalmente, en el que estarán representado, además del CISO, un número adecuado de áreas de la organización para adoptar cualquier resolución, con relevancia en materia de seguridad de la información, que pueda afectar sustancialmente a la actividad de la organización.

La creación de un comité o estructura formal para el gobierno de la ciberseguridad es una práctica consolidada en las grandes empresas cotizadas españolas analizadas en este estudio. Estos comités se caracterizan por una composición multidisciplinar que busca incluir a representantes de alta dirección y de áreas clave afectadas por la ciberseguridad, lo que facilita la discusión y la toma de decisiones transversales. La percepción general es que esta representación es adecuada para abordar asuntos de calado estratégico.

- El 80% de los entrevistados confirma la existencia de un comité de ciberseguridad formal y un 5% adicional indica que ya lo tienen diseñado, pero aún no ha empezado a funcionar.
- Un 5% utiliza un comité de dirección existente (Operaciones y Tecnología) para tratar temas de ciberseguridad en lugar de tener un comité separado, aunque afirma

que, en las reuniones del mismo, el orden del día acaba tratando temas de ciberseguridad en su mayoría.

- Otro 10% indica que no tiene un comité formal dedicado como tal, pues el responsable de ciberseguridad participa en otras reuniones relevantes, o directamente se ha suprimido el comité, habiendo evolucionado hacia un enfoque más informal, donde priman las "reuniones 1on1" y la interacción diaria ("ya no necesito reunirme formalmente. Puedo acceder a todos, tanto al negocio como a las unidades transversales de la compañía como recursos humanos, finanzas, legal, etc.").
- El 85% considera que hay un número adecuado de áreas de la organización que participan en el comité para poder adoptar cualquier resolución que pueda afectar sustancialmente a la actividad de la empresa. El 15% restante, o carece de comité o considera su composición inadecuada por la falta de presencia de ciertos directivos clave.
- La composición de los comités de ciberseguridad es variada, reflejando la naturaleza transversal de la ciberseguridad. Es común la participación en ellos de altos directivos (miembros del comité de dirección, directores generales, e incluso el CEO o COO), actuando la figura del CISO o responsable de seguridad de la información como secretario o líder del comité generalmente. Hay una representación significativa de áreas clave como Gestión de Riesgos, Auditoría Interna, y áreas de Tecnología/Digitalización. También se incluyen representantes de las unidades de negocio, Legal/Compliance/DPO, Operaciones, Recursos Humanos, Comunicación o Finanzas, e incluso Seguridad Física. Algunos comités incluyen representación de las tres líneas de defensa o la participación de proveedores externos como CISO as a Service o consultores de GRC. Además, se suele invitar a las áreas que no forman parte en muchas ocasiones ("se formó para eso, para que las distintas áreas estén representadas en un comité estable. Lógicamente, si hay algún tema que involucra otra área, invitamos").

Los datos recogidos sugieren que la formalización de un espacio dedicado al gobierno de la ciberseguridad a nivel de comité es una práctica extendida en las grandes empresas cotizadas españolas. Así mismo, en la gran mayoría de los casos, la diversidad de miembros presentes en el comité dedicado a la ciberseguridad se considera adecuada para lograr la colaboración y el compromiso de múltiples áreas de la organización en aras de lograr una

ciberseguridad efectiva y abordar resoluciones con impacto sustancial en el negocio. No obstante, a pesar de la percepción general de adecuada representación, algunas empresas indican la **ausencia de directivos clave** que limita la efectividad del comité de ciberseguridad ("echo en falta que esté el director general, pero lo ha delegado y no está asistiendo").

En algunos casos, las estructuras de comités pueden ser locales y globales o replicarse en distintos niveles organizativos como el corporativo y el de negocio, implicando a diferentes responsables para lograr una mayor capilaridad en la toma de decisiones, lo que cabría ser considerado como una buena práctica detectada en la investigación cualitativa y originalmente no contemplada en el Código. Del mismo modo, parece que alguna empresa está logrando la colaboración necesaria a través de interacciones directas con las diferentes unidades de una manera flexible, rápida e informal, considerando este sistema incluso más eficiente que un comité formal de ciberseguridad. Estos casos requieren una cultura organizativa muy particular que soporte este tipo de mecanismos de contacto y apunta que existe cierta diversidad en cuanto a los modelos de gobernanza adoptados para supervisar la ciberseguridad en la alta dirección.

5.6. Información a la dirección y al órgano de administración sobre ciberamenazas y gestión de ciberseguridad

Recomendación 19: El comité de ciberseguridad informará a la dirección y al órgano de administración de las ciberamenazas que podrían afectar a los objetivos de la organización. Para ello, se tendrán en cuenta, al menos, los principales actores y las principales y más recientes ciberamenazas, considerando su potencial impacto sobre las operaciones de la organización.

Recomendación 20: El órgano de administración realizará un seguimiento regular de la ciberseguridad, incluyendo este tema en el orden del día de sus reuniones o en las de sus comisiones especializadas correspondientes donde aplique (auditoría, riesgos, sostenibilidad u otras comisiones específicas para el tratamiento del riesgo de ciberseguridad), para lo que requerirá informes periódicos de la gestión de ciberseguridad al responsable ejecutivo (director de seguridad de la información o CISO). Este reporte deberá realizarse periódicamente. Se considera una buena práctica su realización al menos dos veces al año.

Existe un reconocimiento generalizado sobre la necesidad de informar a la alta dirección y al órgano de administración,

aunque la formalización y frecuencia varían.

- El 80% de los entrevistados afirma tener una periodicidad definida para informar a la dirección/órgano de administración sobre ciberamenazas.
- La frecuencia más común de reporte formal es trimestral (43,75% de quienes tienen periodicidad definida). Otras frecuencias observadas incluyen la semestral y mensual.
- Un 10% informa sin una periodicidad definida, a demanda o según lo requiera la situación.
- Un pequeño porcentaje (5%) indica que no es habitual o formal el reporte a la dirección.
- Algunos CISOs gestionan distintos niveles y frecuencias de informe para comisiones especializadas (como Riesgos o Auditoría y Control) y el Consejo de Administración, siendo los informes a comisiones más frecuentes.

A partir de la información obtenida, cabe concluir que, en el caso de las empresas cotizadas españolas, la ciberseguridad ya forma parte del orden del día de los órganos de gobierno.

- El 95% de los entrevistados afirma que la ciberseguridad se incluye regularmente en el orden del día de las reuniones del órgano de administración o sus comisiones especializadas.
- La inclusión más frecuente se da en comisiones especializadas, particularmente la de Auditoría, Control y Riesgos (60% de las empresas).
- En algunos casos, también se incluye en las reuniones del Consejo de Administración o se informa a este mediante resúmenes.
- Las periodicidades varían, desde "cuando es necesario y como mínimo de manera anual" (15%), "mínimo dos veces al año" (5% - alineado con la recomendación del Código), hasta semestral, trimestral o mensual según circunstancias (5%).

Todos los CISOs entrevistados afirman presentar informes periódicos de gestión de ciberseguridad al menos dos veces al año, cumpliéndose por tanto esta recomendación del Código en todos los casos. No obstante, aunque el resultado generalizado sea el de cumplimiento, hay diferencias notables entre empresas.

- Un 10% indica que este informe se limita a la comparecencia en comisiones, sin un documento formal.
- Otro 10% lo hace al menos dos veces al año, aunque sin tener una periodicidad formalmente establecida.

- La periodicidad habitual para comisiones delegadas suele ser trimestral, mientras que para el consejo de administración suele ser anual.
- Un 15% supera la periodicidad mínima recomendada con informes mensuales o bimestrales.
- Además de los informes ordinarios o formales, una amplia mayoría informa de manera extraordinaria ante incidentes o situaciones especiales.

Nuestros hallazgos indican un compromiso general en la cima organizacional con la supervisión de la ciberseguridad, impulsado en gran parte por el enfoque de las comisiones de Auditoría en cuanto a los riesgos ESG. Sin embargo, la variabilidad en la frecuencia y formalidad del reporte sugiere que aún hay margen para estandarizar y asegurar que la información clave llegue de manera consistente y comprensible a los niveles adecuados. La tendencia a delegar la supervisión en la Comisión de Auditoría es una práctica común para gestionar diversos riesgos, pero hay que subrayar la necesidad de que esta comisión cuente con la experiencia y enfoque adecuados para cumplir sus responsabilidades en ciberseguridad.

Los datos obtenidos muestran que, si bien la inclusión de la ciberseguridad en la agenda del gobierno corporativo es una realidad para la mayoría. La adherencia estricta a la recomendación de informes periódicos al menos dos veces al año es un hecho (el 100% afirma hacerlo, aunque con matices en la formalidad), y la frecuencia trimestral emerge como una práctica común para el reporte a comisiones delegadas del consejo. Esto demuestra que las recomendaciones del Código relativas al informe periódico han sido adoptadas, formalmente o de facto, por las sociedades cotizadas del IBEX-35.

5.7. Información sobre incidentes significativos y estado de la seguridad en la cadena de suministro

Recomendación 21: El informe periódico debe contener al menos el estado de la ciberseguridad, la evolución del grado de madurez y del ciberriesgo, la evolución de las amenazas, la asignación de los recursos destinados a la seguridad de las redes y los sistemas de información, los incidentes significativos gestionados si los hubiera, el estado de la seguridad de las operaciones de la cadena de suministro que dependan de terceros, así como cualquier resolución con relevancia en materia de ciberseguridad adoptada por el equipo directivo que pueda afectar sustancialmente a la actividad de la organización. El director de seguridad de la información o CISO también deberá reportar, en su caso, cualquier obstáculo o impedimento que

pudiera restringir el adecuado desempeño de su actividad.

Existe una notable dificultad y preocupación en torno a la gestión y reporte de la seguridad de terceros. Sólo la mitad de los entrevistados informa sobre incidentes significativos *y* del estado de la seguridad en la cadena de suministro o de terceros.

- Un 5% declara directamente no informar sobre incidentes de terceros [Source 49]. Un significativo 45% expresa que tiene importantes dificultades en este ámbito, mencionando la falta de atención específica ("no existe una atención especial sobre el riesgo de terceros, o al menos no en todos"), la ausencia explícita en los informes ("no hay una sección específica para la cadena de suministro"), o el gran volumen de compromisos de terceros ("no, a no ser que sea algo persistente o que tenga muchísimo impacto, porque hay un montón de compromisos de terceros") que limita el reporte solo a casos severos o muy impactantes ("sólo si se trata de un caso severo", "lo que entra en el rango de incidencia crítica, importante o urgente", "se informa de los incidentes o situaciones más significativas, porque la palabra incidente tiene implicaciones legales de reporte a las autoridades").
- Este es un área de alta preocupación para los CISOs entrevistados debido a la creciente frecuencia de incidentes originados en terceros ("terceros que tienen incidentes cada vez hay más", "los incidentes externos o de terceros superan claramente a los internos"), la percepción de los riesgos de terceros como el mayor riesgo ("los riesgos de terceros son el mayor riesgo que nos encontramos actualmente"), y la complejidad para medir la situación de seguridad de los proveedores ("cada vez tenemos más incidentes provocados por los proveedores y ninguno tiene una solución buena", "Es difícil medir la situación de seguridad que da el suministrador. No sería capaz. Sí que soy capaz de decir que controles tenemos en esa cadena para que sea lo más fiable posible y que minimicen el número y el impacto de los incidentes asociados a la cadena", "hacemos una auditoría de proveedores todos los años con unos cuantos proveedores, no todos, y eso se escala, pero solo el resultado (.,,) Hacemos varias decenas de auditorías a proveedores", o "prestamos especial atención a los incidentes de cadena de suministro. También a las acciones que hacemos sobre proveedores, como auditorías, revisiones de contrato, etc.").

Estos hallazgos demuestran lo acertado de haber optado por las entrevistas en profundidad como técnica de investigación. Mientras que otros instrumentos de recogida de información, como los cuestionarios, permitirían medir el grado o porcentaje de adherencia a una recomendación particular del código, las entrevistas han permitido detectar que la cadena de suministro es considerada una vulnerabilidad crítica por las grandes organizaciones.

La dificultad que se indica en cuanto a su gestión y visibilidad revela un riesgo estratégico significativo y la falta de reporte formal o estructurado sobre este tema a la alta dirección limita su capacidad para supervisar y gestionar este riesgo adecuadamente. Este hallazgo muestra una debilidad importante en las prácticas de GRC de ciberseguridad. Mientras que realizar reuniones de seguimiento puede ser una recomendación relativamente sencilla de seguir, la complejidad de gestionar la seguridad en entornos interconectados y dependientes de terceros hace extremadamente difícil cumplir con las recomendaciones relativas a la cadena de suministro. Este problema, tanto por su relevancia como por su complejidad de resolución, es especialmente evidente en el caso de empresas altamente diversificadas, internacionalizadas o con redes especialmente extensas de agentes conectados al sistema de valor del negocio.

La disparidad entre la conciencia del riesgo (alta preocupación de los CISOs) y la práctica de reporte formal (solo el 50%) sugiere la presencia de barreras operativas importantes que afectan a la gobernanza y limitan la transparencia y la rendición de cuentas en este ámbito.

5.8. Ejecución de simulacros y pruebas de ciberresiliencia

Recomendación 23: El órgano de administración requerirá el desarrollo de pruebas periódicas completas que pongan a prueba los mecanismos de resiliencia de la organización como parte de los planes de ciberseguridad.

En este contexto:

- Deben realizarse pruebas del plan de continuidad de negocio, así como simulaciones y ejercicios de preparación de los comités de gestión de crisis.
- En general, las compañías deben ejecutar de forma sistemática simulacros y pruebas efectivas de las distintas medidas de protección, respuesta y recuperación.
- Estos ejercicios han de implicar a toda la organización, con especial atención a los procesos críticos de la compañía, y deben involucrar también a la cadena de suministro.

Todas las empresas entrevistadas realizan simulacros y pruebas de medidas de protección, respuesta y recuperación. A priori, este resultado revelaría un cumplimiento absoluto con la recomendación del Código. Sin embargo, gracias a haber planteado preguntas abiertas en nuestras entrevistas en profundidad, se han podido detectar realidades complejas en la gestión de estas actividades por parte de las empresas del IBEX-35.

- Todas los CISOs entrevistados indican que realizan simulacros y pruebas de las medidas de protección, respuesta y recuperación, si bien algunas consideran que "pocas" o que "sistemáticamente no, pero al menos tres veces al año y vamos cambiando".
- La frecuencia y el alcance con el que se llevan a cabo estas actividades varían significativamente. La mayoría de las organizaciones realizan estos ejercicios al menos una vez al año, y algunas hasta tres veces.
- El 55% de las empresas no incluye a toda la organización en los simulacros.
- Generalmente, se involucra a áreas críticas, directivos, y personal clave, pero no a toda la sociedad, por las lógicas limitaciones en términos de tiempo y recursos, que impiden la participación de toda la organización en cada ejercicio ("es imposible involucrar a toda la compañía", "los órganos de gobierno y determinadas áreas, como legal, están, pero meter a todos los mercados siempre sería una locura", "tenemos un sistema de prioridades, dado que el conjunto de servicios, aplicaciones y cargas de trabajo que tenemos globalmente es muy amplio").
- Si bien las organizaciones son conscientes de la importancia de realizar estos ejercicios, afrontan importantes desafíos en términos de recursos y operativa para involucrar a toda la compañía ("no tenemos tiempo ni recursos para probar todo. Pero a nivel de organización, intentamos que estén involucradas todas las áreas o la mayoría").
- Como solución a estas limitaciones, las empresas suelen centrarse en áreas específicas cada año, rotando el enfoque para cubrir diferentes aspectos de la organización ("cada año nos centramos en un determinado ámbito de la organización y rota. En el ámbito que corresponda, involucra todo a todos los responsables asociados al proceso"). La rotación de áreas de enfoque asegura que, con el tiempo, diferentes partes de la organización sean evaluadas y preparadas.

- Otra solución a las restricciones para la participación de toda la organización que se ha observado en las entrevistas es la participación selectiva en los simulacros, priorizando áreas críticas y personal clave, lo cual es una estrategia eficiente dadas las limitaciones de recursos ("en esos ejercicios se involucra a todas las personas que soportan los procesos críticos, pero no a toda la organización", "principalmente participan las áreas de IT y algún área de negocio en particular, pero no todas siempre", "con personas designadas como críticas porque desarrollan actividades asociadas a procesos críticos. Ellas prueban y confirman que ese proceso está funcionando").

- Existen algunas empresas (un 10%) que muestran una clara excelencia, por su amplitud o profundidad de enfoque ("para todos los negocios. Tanto para gestión de crisis, como para planes de continuidad, y también ejercicios del plan de gestión de incidentes" o "depende de lo que queramos probar. A veces lo hemos hecho a nivel del Comité Ejecutivo. Otras veces, si simulamos una disrupción total de la compañía, pues toda la compañía ha estado involucrada").

Es positivo que todas las empresas realicen simulacros, lo que indica una conciencia sobre la importancia de probar la resiliencia. Sin embargo, la limitada inclusión de toda la organización y, de manera muy acusada, de la cadena de suministro, que se comentará a continuación, representa un riesgo operativo significativo. La resiliencia de una organización es tan fuerte como su eslabón más débil, que a menudo se encuentra en la cadena de valor extendida. Abordar esta brecha es crucial para una preparación efectiva ante incidentes a gran escala.

- En general, la inclusión de toda la organización y la cadena de suministro es bastante limitada, y existe un amplio margen de mejora a la hora de incluir estos elementos en los ejercicios de simulación.

- El 90% no incluye a la cadena de suministro en su totalidad en los ejercicios de simulacro.

- La mayoría de las organizaciones no involucran a toda la cadena de suministro, optando por establecer prioridades estratégicas ("hay alguno que sí, porque cuando lo analizas, la amenaza venía por parte de un tercero", "si el escenario contempla que el proveedor es relevante para para el ejercicio, entonces sí", o "la cadena de suministro no se incluye salvo que sean proveedores críticos o empresas con las que se trabaja en exclusiva").

- Aunque la inclusión de la cadena de suministro es limitada, algunas

organizaciones incluyen a proveedores críticos, especialmente aquellos relacionados con IT o ciberseguridad, pero no a toda la cadena ("alguna vez algún proveedor concreto, además de los de TIC", "si dependemos en algo que queramos probar, sí, pero depende", "sólo los proveedores más relacionados con IT o con ciberseguridad", "depende de qué tercera parte tengas y de lo crítica que sea", "tenemos mucha subcontratación. Incluso el propio CISO ya está subcontratado y la propia oficina de ciberseguridad", "incluimos a los operadores mantenedores de centros críticos. Dependiendo del tipo de ejercicio se incluyen todos los equipos tecnológicos, de comunicaciones, cíber, etc.", "varios proveedores del ámbito de tecnología o de procesos de negocio tienen sus propios ejercicios y pruebas").

- La inclusión selectiva de proveedores críticos sugiere un enfoque estratégico para asegurar la continuidad de operaciones esenciales. La mayoría de las organizaciones se centran en su propia resiliencia antes de considerar la cadena de suministro ("primero consolidaremos internamente y luego ya…", "nos centramos más en nuestra propia resiliencia, que en la de la cadena de suministros").
- Existe una limitación evidente en cuanto a recursos y operativa, que en muchos casos impide incluir a toda la cadena de suministro ("a la totalidad de la cadena de suministro, es imposible", "sí en cuanto a la parte de ventas, pero en otros casos es más complejo"), y algunas organizaciones no contemplan un seguimiento exhaustivo de la misma mientras no extiendan estos ejercicios de manera satisfactoria en su ámbito interno o cubran las áreas que consideran críticas ("en el caso de los clientes. No, en el caso de toda la cadena de suministros").

Los resultados empíricos de nuestro estudio confirman una brecha importante entre la realización de simulacros (práctica extendida) y su alcance (limitado en términos de inclusión de toda la organización y de la cadena de suministro). Esto sugiere que, si bien se cumplen los requisitos básicos de realizar pruebas, la profundidad y amplitud necesarias para una verdadera ciberresiliencia en ecosistemas complejos son un desafío en organizaciones complejas como las sociedades cotizadas de gran tamaño. La concentración en procesos y proveedores críticos en la cadena de suministro es una estrategia lógica dada la complejidad, pero subraya la necesidad de metodologías y recursos que permitan una evaluación y prueba más amplia de la seguridad de terceros.

6. CONCLUSIONES Y LIMITACIONES

Este informe ha presentado un panorama detallado de la importancia y el enfoque integral que exige la ciberseguridad, resaltando la necesidad de supervisión y rendición de cuentas en esta materia por parte de los consejos de administración. Los marcos regulatorios de EE.UU. y la UE han establecido lo que podría denominarse un nuevo paradigma en cuanto a la comunicación de incidentes y la gestión de la ciberseguridad en empresas cotizadas y entidades consideradas importantes y esenciales.

No obstante, a pesar de la presión de las regulaciones, los estudios recientes indican que la ciberseguridad no recibe la atención adecuada por parte de los consejos de administración. El estudio realizado desde la Cátedra Extraordinaria UCM-ISMS Forum sobre Ciberseguridad y Protección de datos tiene un carácter pionero al evaluar el grado de adopción del Código de Buen Gobierno de la Ciberseguridad en las empresas del IBEX-35.

6.1. Conclusiones

Una inmensa mayoría de los responsables de ciberseguridad entrevistados demuestra familiaridad con el Código y afirma estar realizando esfuerzos proactivos para alinear a su organización con sus principios. El Código se revela como una base sólida para facilitar el diálogo interno sobre la Gobernanza, el Riesgo y el Cumplimiento (GRC) en ciberseguridad, sentando las bases para una gobernanza más madura en las sociedades cotizadas españolas.

Si bien los responsables de ciberseguridad (CISOs) en las empresas del IBEX-35 poseen los conocimientos y la experiencia adecuados para desempeñar sus funciones, se observa bastante diversidad en su posicionamiento jerárquico dentro de las organizaciones, lo que puede modular su capacidad de decisión e influencia estratégica. Aunque la mayoría considera que ya tiene la influencia necesaria, una parte significativa percibe limitaciones a la misma, derivadas de factores organizativos y jerárquicos.

Se observa una incorporación efectiva de la ciberseguridad en la agenda de los órganos de administración y sus comisiones especializadas, principalmente Auditoría, Control y Riesgos. La presentación de informes periódicos por parte del CISO es una práctica extendida, evidenciando que las recomendaciones del Código relativas al reporte periódico están siendo adoptadas, ya sea formalmente o de facto. No obstante, se observan variaciones en la frecuencia y formalidad de dicho reporte, lo que sugiere la necesidad de estandarizar y asegurar que la información clave llegue de manera consistente y oportuna a

todos los niveles relevantes. Así, aunque el reporte periódico de gestión de ciberseguridad al CISO se cumple en todos los casos analizados con una frecuencia de al menos dos veces al año, la frecuencia trimestral es la más común para las comisiones delegadas. No obstante, aún persisten variaciones en la formalidad y frecuencia específica del reporte a los distintos niveles de la alta dirección, lo que indica margen para una mayor estandarización y consistencia en la comunicación de riesgos.

Aunque más de la mitad de las empresas cuenta en sus órganos de gobierno con algún miembro con experiencia en ciberseguridad (o tecnología), persiste una carencia significativa de perfiles con experiencia específica en ciberseguridad en el órgano de administración principal, lo que sugiere un área de mejora para fortalecer la supervisión cualificada en esta materia.

La creación de un comité o estructura formal para el gobierno de la ciberseguridad es una práctica consolidada, con una representación multidisciplinar considerada como adecuada en la mayoría de los casos. Esto indica un alto grado de seguimiento de las recomendaciones del Código al respecto. Sin embargo, la diversidad de modelos observados, incluyendo enfoques más informales con reuniones directas y rápidas con individuos clave de la organización, y la percepción en algunos casos de una composición inadecuada, sugieren que la efectividad de este tipo de comités varía y depende no sólo de su formalización y composición, sino también de su alineación con la cultura organizativa.

La existencia de una unidad o área dedicada a la ciberseguridad es una realidad en la práctica totalidad de las empresas, un desafío persistente identificado es la percepción generalizada de insuficiencia de recursos, especialmente en cuanto a talento humano especializado. De hecho, sólo una cuarta parte de los entrevistados considera que su unidad cuenta con capacidades y recursos suficientes sin reservas, lo que sugiere que, a pesar de los avances realizados en este campo y reconocidos por los entrevistados, la dotación adecuada puede seguir siendo un factor crítico y limitante para el adecuado desempeño de la unidad de ciberseguridad. Como afirmaba una de las personas entrevistadas, quien haya respondido que tiene recursos suficientes “o miente o tiene mucha suerte”.

Otro de los posibles obstáculos para que la unidad de ciberseguridad cuente con la influencia y relevancia adecuadas es su independencia. A nivel jerárquico, en las empresas analizadas, tiende a depender o reportar directamente a la alta dirección o alguno de sus comités, lo que estaría en consonancia con las recomendaciones del Código. No

obstante, la independencia respecto a las áreas operativas de Tecnologías de la Información (IT), si bien afirmada por algo más de la mitad de los entrevistados, presenta matices importantes o directamente no existe en un porcentaje considerable de casos. Esto demuestra que garantizar la objetividad y evitar conflictos de interés en la gestión de la seguridad es aún un reto en una parte importante de las empresas cotizadas, al menos en su aspecto formal o estructural.

A pesar de estos avances, el estudio también identifica algunos desafíos críticos que requieren atención estratégica para fortalecer la ciberresiliencia en un perímetro y entorno de amenazas cada vez más complejo. La gestión y el reporte de incidentes significativos y del estado de la seguridad en la cadena de suministro o de terceros emergen como una debilidad importante.

Sólo la mitad de los entrevistados informa sobre estos aspectos, y una proporción significativa reconoce importantes dificultades en su manejo y reporte eficaz. Los CISOs muestran una alta preocupación por la creciente frecuencia de incidentes originados en terceros y empiezan a ver los riesgos de terceros como uno de los mayores problemas actuales. Esta disparidad entre la conciencia del riesgo y la práctica de reporte formal limita la capacidad de la alta dirección para supervisar y gestionar este riesgo estratégico de manera adecuada.

En cuanto a la ejecución de simulacros y pruebas de ciberresiliencia, si bien todas las empresas afirman realizarlos, la profundidad y amplitud de estos ejercicios presentan limitaciones notables. La inclusión de toda la organización es limitada (el 55% no lo hace), y de forma aún más acusada y consistente con lo señalado anteriormente, la cadena de suministro prácticamente no se incluye en su totalidad en las actividades de ensayo y simulación (90%). Aunque algunas organizaciones incluyen proveedores críticos, la complejidad que supone la cadena de valor extendida, las limitaciones de recursos y la priorización de la resiliencia interna dificultan la extensión completa de estos ejercicios. Esta brecha entre la realización de pruebas y su alcance puede representar un riesgo operativo significativo.

En resumen, las empresas del IBEX-35 muestran un compromiso inicial prometedor con el buen gobierno de la ciberseguridad y han integrado el reporte a la alta dirección en sus rutinas. Sin embargo, cuestiones como la gestión eficaz del riesgo en la cadena de suministro y la ampliación del alcance de los simulacros de ciberresiliencia representan desafíos complejos, pero fundamentales para alcanzar un nivel de madurez que responda a un panorama de ciberamenazas en

constante evolución y a las crecientes exigencias regulatorias.

6.2. Limitaciones

No podemos terminar este informe sin señalar las principales limitaciones del estudio realizado. En primer lugar, los resultados comentados se basan en el análisis de un subconjunto de preguntas limitado del total de las incluidas en las entrevistas en profundidad (17 de 56), lo que implica que no representan una evaluación completa del cumplimiento del Código. Así mismo, hasta la fecha sólo se ha utilizado este método para la recogida de información, por lo que existe la limitación potencial del uso de datos autodeclarados.

Si bien la garantía de confidencialidad proporcionada a los participantes busca fomentar la sinceridad y minimizar el sesgo, este no deja de ser una limitación inherente a la metodología empleada en el estudio y no puede asegurarse que no hayan existido sesgos de deseabilidad social (responder lo que se cree que el entrevistador quiere oír) o de ofrecer una percepción inflada de las propias prácticas organizativas.

Con el fin de superar estas a limitaciones, el plan a futuro contempla el análisis completo de la totalidad de las 56 preguntas del cuestionario, lo que proporcionará una visión mucho más detallada del grado de madurez de las empresas del IBEX-35 en relación con las 25 recomendaciones del Código. También en una fase posterior, se planea complementar los hallazgos de las entrevistas con el análisis de toda la información públicamente disponible sobre ciberseguridad de las empresas participantes, lo que permitirá validar y enriquecer los resultados obtenidos.

Aún reconociendo estas limitaciones iniciales, la información obtenida de las entrevistas con líderes de ciberseguridad de empresas de la talla del IBEX-35 posee un valor significativo. Los resultados, aunque preliminares en su alcance cuantitativo, ofrecen *insights* cualitativos profundos sobre las realidades y desafíos a los que se enfrentan estas organizaciones, proporcionando una base sólida para entender las áreas prioritarias de atención en el ámbito del GRC de ciberseguridad.

7. RECOMENDACIONES

A partir de los hallazgos de este estudio y con el objetivo de impulsar la mejora continua en el buen gobierno de la ciberseguridad en las empresas del IBEX-35, se proponen las siguientes recomendaciones, dirigidas tanto a los responsables de ciberseguridad (CISOs) como a los miembros de los órganos de administración:

Para los órganos de gobierno corporativo:

- **Fortalecer la supervisión estratégica:** Para garantizar que la ciberseguridad sea un elemento central en la estrategia de negocio y no solo un asunto técnico es necesario asumir un rol proactivo en su supervisión, trascendiendo la delegación en comisiones y asegurando una comprensión global de los riesgos cibernéticos a nivel de todo el consejo de administración.
- **Evaluar y fortalecer el posicionamiento del CISO:** Es recomendable revisar y considerar la posición jerárquica del máximo responsable de ciberseguridad, así como su línea de reporte para poder asegurar su acceso directo y capacidad de influir en las decisiones estratégicas de la organización.
- **Garantizar la independencia de la función de ciberseguridad:** La estructura organizativa y de reporte para la unidad de ciberseguridad debe asegurar su independencia funcional respecto a las áreas responsables de la operación de los sistemas y redes de información (IT), facilitando la toma de decisiones objetiva en materia de seguridad y mitigación de riesgos, tal y como ya recomendaba el Código.
- **Promover la formación continua en ciberseguridad de los consejeros:** Invertir en la formación especializada en ciberseguridad para los miembros del consejo, permitiéndoles comprender la naturaleza estratégica de los riesgos cibernéticos, las implicaciones de las amenazas y las buenas prácticas de gestión.
- **Incorporar al consejo miembros expertos en ciberseguridad:** Además de la formación general, es altamente recomendable evaluar la composición del órgano de administración para asegurar la presencia de miembros con *experiencia probada y específica* en gestión de riesgos de ciberseguridad y no en tecnología en general, en línea con las mejores prácticas internacionales y los requisitos regulatorios emergentes.
- **Exigir reportes o informes estandarizados y orientados al negocio:** Se deben establecer requisitos claros para los informes periódicos de ciberseguridad, asegurando que sean comprensibles, relevantes para el negocio y aborden no solo el estado técnico, sino también la evolución del ciberriesgo, la asignación de recursos y, fundamentalmente, la gestión de incidentes significativos y el riesgo en la cadena de suministro. La frecuencia de reporte debería ser revisada para asegurar que se alinea con la dinámica del riesgo de la compañía en todo momento.

- **Asegurar una dotación suficiente de recursos para la ciberseguridad:** A pesar de las limitaciones presupuestarias y de recursos que toda organización experimenta, el buen gobierno de la ciberseguridad exige garantizar que la unidad encargada, así como otras áreas con responsabilidades conexas, dispongan de los recursos materiales y, muy especialmente, humanos especializados necesarios para cumplir eficazmente con sus funciones y alcanzar los objetivos estratégicos de ciberseguridad. Es importante reconocer el talento como un factor crítico de éxito, pues actualmente es escaso y se prevé que lo sea aún más en el futuro.
- **Incentivar la transparencia en la cadena de suministro:** Es necesario impulsar iniciativas para mejorar la visibilidad y la gestión del riesgo en la cadena de suministro. Esto puede incluir la revisión de cláusulas contractuales, la realización de auditorías conjuntas con proveedores críticos y el fomento de ecosistemas de ciberseguridad colaborativos.
- **Asegurar los recursos para simulacros completos:** Se debe garantizar que las unidades de ciberseguridad y otras áreas clave dispongan de los recursos (materiales, humanos y de tiempo) necesarios para llevar a cabo simulacros y pruebas de resiliencia que involucren a toda la organización y, de manera progresiva, a los proveedores críticos de la cadena de suministro.
- **Entender el cumplimiento y la adaptación a los estándares más rigurosos como una oportunidad estratégica:** Las exigencias de la SEC o la NIS2 no deben contemplarse como meros requisitos de cumplimiento, sino como una posibilidad real de mejorar las capacidades organizativas de ciberresiliencia, además de demostrar transparencia y poder mejorar la confianza de los stakeholders.

Para responsables de ciberseguridad:

- **Elevar la conversación a nivel estratégico:** Comunicar la ciberseguridad en términos de riesgo de negocio, impacto financiero y reputacional, y la alineación con los objetivos estratégicos de la organización es imprescindible para recibir el respaldo de la alta dirección y los órganos de gobierno. Para ello resulta imprescindible evitar el lenguaje excesivamente técnico en las relaciones con la cúpula organizativa y empezar a "hablar su idioma".
- **Desarrollar métricas clave de desempeño (KPIs) estandarizadas y relevantes para la dirección:** El altamente recomendable definir y presentar indicadores que muestren la evolución del grado de madurez,

la efectividad de las medidas de control, el impacto potencial de las amenazas y la gestión de riesgos, incluyendo métricas específicas para la cadena de suministro.

- **Cuantificar y justificar las necesidades de recursos:** Desarrollar métricas e informes que permitan cuantificar de manera clara las necesidades de recursos, especialmente de personal especializado, y justificar su solicitud ante la alta dirección y el órgano de gobierno, relacionando la inversión en recursos con la reducción del riesgo y el logro de los objetivos de negocio (ver las dos recomendaciones anteriores).
- **Estandarizar los informes para la alta dirección:** Definir cuidadosamente la estructura y contenido de los informes periódicos es importante para garantizar su consistencia, claridad y relevancia para la toma de decisiones por parte del consejo y sus comisiones delegadas.
- **Priorizar la gestión del riesgo de terceros:** Reconociendo que los riesgos de terceros son percibidos como los de mayor crecimiento e impacto potencial por los responsables de ciberseguridad, es necesario implantar y fortalecer procesos que permitan la evaluación y supervisión continuada de la seguridad en la cadena de suministro. Por ello, resulta especialmente crítico desarrollar mecanismos que permitan la detección y reporte ágil de incidentes originados en terceros.
- **Diseñar un plan gradual de ampliación del alcance de simulacros de ciberseguridad:** Se debe desarrollar una hoja de ruta para aumentar progresivamente el alcance de los simulacros de ciberresiliencia, involucrando a más áreas de la organización y planificando ejercicios específicos que incluyan a proveedores críticos, aunque suponga vencer resistencias y exigir recursos adicionales. Se debe sacar el máximo partido de los simulacros documentando las lecciones aprendidas de cada uno para impulsar la mejora continua de los planes de respuesta y recuperación.

Consideramos que el seguimiento de estas recomendaciones contribuirá a fortalecer el marco de GRC en materia de ciberseguridad en las principales sociedades cotizadas españolas, mejorando su capacidad para gestionar los riesgos cibernéticos de manera eficaz y generando una mayor confianza entre los inversores y otros grupos de interés.

BIBLIOGRAFÍA

- Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing cybersecurity from the boardroom: challenges, drivers, and ways ahead. *Computers & Security*, 121, 102840.
- CNMV — Foro Nacional de Ciberseguridad (2023), *Código de buen gobierno de la ciberseguridad*, Administración General del Estado. NIPO (edición online):098-23-01309
- Hartmann, C. C., & Carmenate, J. (2021). Academic research on the role of corporate governance and IT expertise in addressing cybersecurity breaches: Implications for practice, policy, and research. *Current Issues in Auditing*, 15(2), A9-A23.
- Pearlson, K., & Hetner, C. (2022). Is Your Board Prepared for New Cybersecurity Regulations? *Harvard Business Review*, November 11, 2022.
- Rothrock, R. A., Kaplan, J., & Van Der Oord, F. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review*, 59(2), 12-15.
- Savaș, S., & Karataș, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International Cybersecurity Law Review*, 3(1), 7-34.
- Slapničar, S., Axelsen, M., Bongiovanni, I., & Stockdale, D. (2023). A pathway model to five lines of accountability in cybersecurity governance. *International Journal of Accounting Information Systems*, 51, 100642.
- Valkenburg, B., & Bongiovanni, I. (2024). Unravelling the three lines model in cybersecurity: a systematic literature review. *Computers & Security*, 139, 103708.

ANEXO: PREGUNTAS-GUÍA EMPLEADAS DURANTE LAS ENTREVISTAS

BLOQUE 0: PRESENTACIÓN Y PERFIL

0.1. ¿Podría indicarnos su nombre y apellidos, y la empresa para la que trabaja?
0.2. ¿Qué cargo ocupa en la empresa? ¿Cuántos niveles hay entre su cargo y el CEO/presidencia de la empresa?
0.3. ¿Conoce el Código de Buen Gobierno de la Ciberseguridad?

El Código de Buen Gobierno de la Ciberseguridad propone 13 principios y 25 recomendaciones, organizados en torno a tres grandes bloques: estrategia y organización, gestión y supervisión.

Las siguientes preguntas de la entrevista pretenden determinar en qué medida su empresa cumple con las 25 recomendaciones del Código. Algunas recomendaciones se evalúan con una sola pregunta, mientras que otras necesitan varias preguntas.

Puede responder con un simple sí o no, pero agradecemos que nos ofrezca detalles sobre su respuesta, con el fin de tener información cualitativa sobre los obstáculos que tienen las empresas cotizadas para cumplir con el Código.

BLOQUE 1: ESTRATEGIA Y ORGANIZACIÓN

Recomendación 1 (las recomendaciones no es necesario leerlas durante la entrevista, salvo que fuera necesario comentarlas a lo largo de la interacción con la persona entrevistada): El órgano de administración reconocerá formalmente, en un documento visible públicamente, los principios y compromisos de la ciberseguridad como elemento fundamental para proteger los activos del negocio, con el fin de lograr sus objetivos y cumplir con su misión.

1.1. ¿El órgano de administración ha reconocido formalmente los principios y compromisos de la ciberseguridad en un documento público?
1.2. ¿Este documento es accesible y visible públicamente? ¿Cómo podríamos acceder al documento?

Recomendación 2: Uno de los ámbitos explícitos de la política de control y gestión de riesgos de la organización será la ciberseguridad.

1.3. ¿Está usted en contacto con el órgano o comité responsable de la política de control y gestión de riesgos? ¿La política de control y gestión de riesgos de la organización incluye explícitamente la ciberseguridad?

Recomendación 3: La organización, teniendo en cuenta las necesidades operativas del negocio y los riesgos que puedan afectar a la consecución de sus objetivos, definirá planes a corto, medio y largo plazo que aseguren la visión de futuro y mejora continua de la ciberseguridad, permitiendo reducir su exposición al riesgo dentro de los niveles de tolerancia definidos.

1.4. ¿Su empresa ha definido planes a corto, medio y largo plazo para la ciberseguridad? ¿En la elaboración de estos planes se han tenido en cuenta las necesidades operativas del negocio y los riesgos que puedan afectar a la consecución de los objetivos de la empresa?
1.5. ¿Estos planes permiten la mejora continua de la ciberseguridad? ¿Reducen la exposición al riesgo dentro de los niveles de tolerancia definidos?

Recomendación 4: Se tomarán decisiones en materia de ciberseguridad en función del riesgo real de la materialización de las amenazas sobre la organización. Se implantará, de igual manera, un sistema de monitorización de la eficiencia y el cumplimiento de los objetivos de seguridad definidos.

1.6. ¿Las decisiones en ciberseguridad se basan en el riesgo real de las amenazas?
1.7. ¿Existe un sistema de monitorización de la eficiencia y cumplimiento de los objetivos de seguridad definidos?

Recomendación 5: La organización aspirará a que, dentro del órgano de administración, haya, al menos, un miembro con experiencia en gestión de ciberseguridad que apoye y valide los objetivos con anterioridad a su aprobación por el equipo directivo.

1.8. ¿Existe al menos un miembro en el órgano de administración con experiencia en gestión de ciberseguridad? ¿Quién es esta persona? ¿Podríamos entrevistarla?
1.9. ¿Este miembro apoya y valida los objetivos de ciberseguridad antes de su aprobación por el equipo directivo?

Recomendación 6: La organización dispondrá de una unidad que asuma la función de definición, impulso y control de la ciberseguridad y que participe en la toma de decisiones y estrategias en este ámbito. Del mismo modo deberá asegurar el reporte adecuado, y a los niveles oportunos, de los riesgos relacionados con la ciberseguridad, así como de los mecanismos de mitigación y control de los mismos que sean necesarios. Esta unidad contará con suficientes capacidades y recursos, materiales y humanos, para la consecución de sus objetivos, y dependerá funcionalmente del órgano de administración, de alguna de sus comisiones especializadas o de cualquier otro órgano o miembro de la alta dirección de la organización, siempre que se

mantenga la debida independencia respecto de los responsables de sistemas de redes y de información.

1.10. ¿La organización tiene una unidad dedicada a la definición, impulso y control de la ciberseguridad? ¿Participa en la toma de decisiones y estrategias en este ámbito?
1.11. ¿La unidad de ciberseguridad de su empresa, asegura el reporte adecuado, y a los niveles oportunos, de los riesgos relacionados con la ciberseguridad, y de los mecanismos de mitigación y control de riesgos necesarios?
1.12. ¿Esta unidad cuenta con las capacidades y recursos suficientes para alcanzar sus objetivos de manera eficaz?
1.13. ¿Esta unidad depende funcionalmente del órgano de administración, de alguna de sus comisiones especializadas o de cualquier otro órgano o miembro de la alta dirección de la organización? ¿Esta unidad tiene la debida independencia respecto de los responsables de sistemas de redes y de información?

Recomendación 7: El máximo responsable de esta unidad será el director de ciberseguridad, director de seguridad de la información o Chief Information Security Officer (en adelante CISO). Esta figura será una persona con el conocimiento, experiencia y competencias adecuadas para desarrollar la función y contará con la suficiente capacidad de decisión e influencia en la organización.

1.14. ¿Quién es el máximo responsable de la unidad de ciberseguridad? ¿Es el CISO?
1.15. ¿Esta figura cuenta con los conocimientos, experiencia y competencias adecuadas para desarrollar la función que tiene encomendada? ¿Tiene suficiente capacidad de decisión e influencia dentro de la organización?

Recomendación 8: Existirá un comité de ciberseguridad, constituido formalmente, en el que estarán representado, además del CISO, un número adecuado de áreas de la organización para adoptar cualquier resolución, con relevancia en materia de seguridad de la información, que pueda afectar sustancialmente a la actividad de la organización.

1.16. ¿Existe un comité de ciberseguridad constituido formalmente? ¿Quiénes forman parte de él?
1.17. ¿Cuenta con representación de un número adecuado de áreas de la organización para adoptar cualquier resolución que pueda afectar sustancialmente a la actividad de la empresa?

Recomendación 9: Las organizaciones, en función de su complejidad y exposición al riesgo cibernético, deberán tener en cuenta la ciberseguridad al menos en uno de sus comités de crisis.

1.18. ¿Su empresa tiene en cuenta la ciberseguridad al menos en uno de sus comités de crisis? ¿Debería tenerse en cuenta en un mayor número de comités?

Recomendación 10: El órgano de administración asignará la supervisión ejecutiva de la gestión de la ciberseguridad a alguna de sus comisiones especializadas (por ejemplo, la comisión de riesgos, la comisión de auditoría…).

1.19. ¿El órgano de administración de su empresa ha asignado la supervisión ejecutiva de la gestión de la ciberseguridad a alguna de sus comisiones especializadas? ¿A cuál (comisión de riesgos, comisión de auditoría…)?

Recomendación 11: El órgano de administración comprenderá las implicaciones de las buenas prácticas, entre otras, en la gestión de los riesgos en materia de ciberseguridad, tanto en su organización, como en cada uno de los mercados en los que opera y en su relación con los distintos grupos de interés.

1.20. ¿El órgano de administración de su empresa comprende las implicaciones de las buenas prácticas en gestión de riesgos en materia de ciberseguridad? ¿Lo hace para el total de la organización? ¿Lo hace para cada uno de los mercados en los que opera? ¿Lo hace en su relación con los distintos grupos de interés de la empresa?

BLOQUE 2: GESTIÓN

Recomendación 12: La organización se apoyará en reconocidos estándares, nacionales, europeos o internacionales, adecuados a sus necesidades, para un mejor seguimiento de la evolución de su madurez.

2.1. ¿La organización utiliza estándares reconocidos (nacionales, europeos o internacionales) para guiar sus prácticas de ciberseguridad? ¿Cuáles son estos estándares?
2.2. ¿Estos estándares se adaptan a las necesidades específicas de la organización?
2.3. ¿Se realiza un seguimiento de la evolución de la madurez en ciberseguridad utilizando estos estándares?

Recomendación 13: El órgano de administración se asegurará de que la unidad responsable de la gestión de la ciberseguridad, así como otras unidades con responsabilidad en la consecución de los objetivos establecidos, disponen de suficientes capacidades materiales y humanas para poder llevar a cabo las funciones asignadas de forma efectiva y eficiente.

2.4. ¿El órgano de administración ha evaluado y asegurado que la unidad de ciberseguridad cuenta con suficientes recursos materiales y humanos para llevar a cabo sus funciones de forma efectiva y eficiente?
2.5. ¿Otras unidades responsables de los objetivos de ciberseguridad también disponen de los recursos necesarios?

Recomendación 14: Se definirá cuándo un incidente tiene la consideración de significativo en función del impacto, del tipo de organización, su sector y las regulaciones a las que pudiera estar sometida en los mercados en los que opere.

2.6. ¿Tiene su empresa una definición clara de cuándo un incidente se considera significativo? ¿Esta definición toma en cuenta el impacto, tipo de organización, sector y regulaciones aplicables?

Recomendación 15: Se identificarán los grupos operativos encargados de su gestión (tanto a nivel técnico y táctico, como estratégico) para minimizar el impacto en el negocio y para asegurar el cumplimiento regulatorio y la adecuada comunicación interna o externa.

2.7. ¿Se han identificado los grupos operativos encargados de la gestión de incidentes a nivel técnico, táctico y estratégico?
2.8. ¿Estos grupos están preparados para minimizar el impacto en el negocio?
2.9. ¿Estos grupos aseguran el cumplimiento regulatorio en la gestión de incidentes?
2.10. ¿Estos grupos permiten una adecuada comunicación interna y externa durante la gestión de incidentes?

Recomendación 16: Se dispondrá de capacidades que permitan a la organización ser resiliente para asegurar la continuidad de las operaciones y la recuperación completa de los servicios en un plazo adecuado de tiempo que se determinará en el plan de continuidad de negocio.

2.11. ¿Su empresa tiene un plan de continuidad de negocio? ¿Determina este plan un plazo adecuado para la recuperación completa de los servicios tras un ciberincidente?
2.12. ¿Cuenta su organización con capacidades suficientes para su resiliencia cibernética y la continuidad de las operaciones?

Recomendación 17: La dirección y el órgano de administración fomentarán la formación, concienciación y cultura de ciberseguridad en toda la organización con el objetivo de capacitar a su personal acerca de los hábitos y prácticas recomendables para prevenir y mitigar riesgos en el ámbito de la ciberseguridad.

2.13. ¿La dirección y el órgano de administración promueven activamente la formación y concienciación y cultura de ciberseguridad en toda la organización?

2.14. ¿Se realizan programas de capacitación para todo el personal sobre hábitos y prácticas recomendables para prevenir y mitigar los riesgos de ciberseguridad?

Recomendación 18: La gestión de la ciberseguridad estará en constante mejora y evolución para garantizar una defensa adecuada ante las amenazas.

2.15. ¿Se revisan y actualizan regularmente las medidas de ciberseguridad para garantizar una defensa adecuada ante nuevas amenazas? ¿Podría decirse que en su empresa la gestión de la ciberseguridad se encuentra en constante mejora y evolución?

BLOQUE 3: SUPERVISIÓN

Recomendación 19: El comité de ciberseguridad informará a la dirección y al órgano de administración de las ciberamenazas que podrían afectar a los objetivos de la organización. Para ello, se tendrán en cuenta, al menos, los principales actores y las principales y más recientes ciberamenazas, considerando su potencial impacto sobre las operaciones de la organización.

3.1. ¿El comité de ciberseguridad informa regularmente a la dirección y al órgano de administración de las ciberamenazas que podrían afectar a los objetivos de la organización? ¿Con qué frecuencia?

3.2. ¿Estos informes incluyen los principales actores, las ciberamenazas principales y más recientes, y su impacto potencial sobre las operaciones de la empresa?

Recomendación 20: El órgano de administración realizará un seguimiento regular de la ciberseguridad, incluyendo este tema en el orden del día de sus reuniones o en las de sus comisiones especializadas correspondientes donde aplique (auditoría, riesgos, sostenibilidad u otras comisiones específicas para el tratamiento del riesgo de ciberseguridad), para lo que requerirá informes periódicos de la gestión de ciberseguridad al responsable ejecutivo (director de seguridad de la información o CISO). Este reporte deberá realizarse periódicamente. Se considera una buena práctica su realización al menos dos veces al año.

3.3. ¿El órgano de administración incluye regularmente la ciberseguridad en el orden del día de sus reuniones o comisiones especializadas?

3.4. ¿Se requieren informes periódicos de la gestión de ciberseguridad al director de seguridad de la información (CISO)?
3.5. ¿Estos informes se presentan al menos dos veces al año?

Recomendación 21: El informe periódico debe contener al menos el estado de la ciberseguridad, la evolución del grado de madurez y del ciberriesgo, la evolución de las amenazas, la asignación de los recursos destinados a la seguridad de las redes y los sistemas de información, los incidentes significativos gestionados si los hubiera, el estado de la seguridad de las operaciones de la cadena de suministro que dependan de terceros, así como cualquier resolución con relevancia en materia de ciberseguridad adoptada por el equipo directivo que pueda afectar sustancialmente a la actividad de la organización. El director de seguridad de la información o CISO también deberá reportar, en su caso, cualquier obstáculo o impedimento que pudiera restringir el adecuado desempeño de su actividad.

3.6. ¿El informe periódico contiene el estado actual de la ciberseguridad y la evolución del grado de madurez y del ciberriesgo?
3.7. ¿Se incluye la evolución de las amenazas y la asignación de recursos para la seguridad de redes y sistemas de información?
3.8. ¿Se informa sobre los incidentes significativos gestionados y el estado de la seguridad en la cadena de suministro o de las actividades dependientes de terceros?
3.9. ¿El CISO reporta cualquier obstáculo o impedimento que pueda restringir su desempeño?

Recomendación 22: Cuando en el orden del día de las reuniones del órgano de administración figure algún tema que pueda afectar a la ciberseguridad, se tendrán que tratar las repercusiones que tenga la ciberseguridad en el referido tema como, por ejemplo: grandes iniciativas de transformación digital, implementación de nuevas tecnologías y grandes inversiones en activos tecnológicos, fusiones y adquisiciones, expansión de instalaciones o grandes actualizaciones.

3.10. ¿Se consideran las repercusiones de ciberseguridad en otros temas del orden del día (como iniciativas de transformación digital, implementación de nuevas tecnologías y grandes inversiones en activos tecnológicos, fusiones y adquisiciones, expansión de instalaciones o grandes actualizaciones)?

Recomendación 23: El órgano de administración requerirá el desarrollo de pruebas periódicas completas que pongan a prueba los mecanismos de resiliencia de la organización como parte de los planes de ciberseguridad.

En este contexto:

▪ Deben realizarse pruebas del plan de continuidad de negocio, así como simulaciones y ejercicios de preparación de los comités de gestión de crisis.

▪ En general, las compañías deben ejecutar de forma sistemática simulacros y pruebas efectivas de las distintas medidas de protección, respuesta y recuperación.

▪ Estos ejercicios han de implicar a toda la organización, con especial atención a los procesos críticos de la compañía, y deben involucrar también a la cadena de suministro.

3.11. ¿Se realizan pruebas del plan de continuidad de negocio, simulaciones y ejercicios de preparación de los comités de gestión de crisis?
3.12. ¿Se ejecutan sistemáticamente simulacros y pruebas de medidas de protección, respuesta y recuperación?
3.13. ¿Estos ejercicios involucran a toda la organización y prestan especial atención a los procesos críticos? ¿Se incluyen en los ejercicios a la cadena de suministro?

Recomendación 24: El órgano de administración se asegurará de que la dirección apoye la creación, implementación, prueba y mejora continua de los mecanismos de ciberresiliencia.

3.14. ¿El órgano de administración asegura el apoyo de la dirección para la creación, implementación, prueba y mejora de los mecanismos de ciberresiliencia?
3.15. ¿La dirección fomenta la mejora continua de estos mecanismos?

Recomendación 25: Se deberán realizar evaluaciones independientes respecto a la unidad de ciberseguridad, al menos una vez al año, que permitan al órgano de administración obtener un punto de vista adicional y complementario del correcto estado del programa de gestión de los riesgos de ciberseguridad de los procesos críticos de la organización, incluyendo a la cadena de suministro.

3.16. ¿Se realizan evaluaciones independientes de la unidad de ciberseguridad al menos una vez al año?
3.17. ¿Estas evaluaciones permiten al órgano de administración tener un punto de vista adicional y complementario sobre el estado del programa de gestión de riesgos de ciberseguridad?
3.18. ¿Se incluyen en estas evaluaciones a la cadena de suministro y los procesos críticos de la organización?

PRIMER ESTUDIO SOBRE EL BUEN GOBIERNO DE LA CIBERSEGURIDAD EN ESPAÑA

ISMS CYBER-REPORTING INITIATIVE PRELYMINARY REPORT

www.ismsforum.es
info@ismsforum.es
(+34) 915 63 50 62

Cátedra Extraordinaria Ciberseguridad y Protección de Datos

isms forum

UNIVERSIDAD COMPLUTENSE