Foro organizado por

agers | Asociación Española de Gerencia de Riesgos y Seguros

Instituto de Auditores Internos de España

Hacia la unión del gobierno corporativo y la ciberseguridad

Madrid, 29 de noviembre de 2017

Índice

OBJETIVOS DE LA JORNADA

Expertos europeos en gestión de riesgos instan a las organizaciones a crear grupos de tratamiento interno de los Ciberriesgos para abordar los riesgos digitales en toda la empresa a medida que evolucionan las amenazas.

La recomendación para un modelo de gobernanza del riesgo cibernético aparece en el informe publicado 29 de junio por la Federación Europea de Asociaciones de Gerencia de Riesgos (FERMA) y la Confederación Europea de Institutos de Auditoría Interna (ECIIA).

FERMA y ECIIA presentaron su informe en un destacado acto en la sede del Parlamento Europeo, en Bruselas, con representantes de las instituciones de la UE, el Foro Económico Mundial, profesionales de riesgos y auditoría de empresas y otros interesados europeos.

Este foro está organizado por las dos asociaciones españolas que han participado en la creación del informe, el Instituto de Auditores Internos de España IAI y la Asociación Española de Gerencia de Riesgos y Seguros, AGERS. quienes presentarán las conclusiones del mencionado informe, que traducimos y sintetizamos en las siguientes páginas.

PROGRAMA DEL ACTO

09:00 - 09:30h. Acreditaciones

09:30 - 11.00h. Intervenciones

D. Alfredo Zorzo, Director de Riesgos y Seguros (Risk & Insurance Director) de One eSecurty representante de AGERS

D. Raúl Mateos, Gerente de Auditoría Interna del BBVA, representante de Auditores Internos.

D. Santiago Sánchez, Representante de riesgos cibernéticos de Insurance Europe, en representación de UNESPA, Head of Sales & Distribution, Spain & Portugal Chubb

Moderará y presentará la jornada: D. Juan Gayá, Director de Organización y actualmente es Gerente de Riesgos y Seguros del Grupo El Corte Inglés.

D. Alfredo Zorzo

Director de Riesgos y Seguros (Risk & Insurance Director) de One eSecurty representante de AGERS

Master en Dirección Económico Financiera (CEF), Mediador de Seguros Titulado grupo "A" (Udima), Experto en Gerencia de Riesgos y Seguros (Mapfre), con formación en distintos ámbitos de la gerencia de riesgos y seguros y con una experiencia profesional de más de 20 años, Alfredo Zorzo ocupa actualmente la Dirección de Desarrollo de Negocio y de Riesgos y Seguros de One eSecurity, encargándose de la estrategia de la entidad en el mercado de los ciberseguros, asumiendo también la responsabilidad de la gerencia de riesgos y seguros. Anteriormente y durante 11 años desempeñó el cargo de Responsable de Seguros de Orange España.

Desde 2011 es miembro de la Junta Directiva de AGERS (Asociación Española de Gerencia de Riesgos y Seguros), en la que ha ostentado los cargos de Vicepresidente II y I, participando en diferentes Comisiones y Grupos de Trabajo, habiendo sido Director del Curso sobre Ciberriesgos y de Gestión de Riesgos Tecnológicos que la Asociación viene impartiendo desde 2012 y el responsable del Grupo de Trabajo sobre Ciberriesgos. En la actualidad participa en el Grupo de Trabajo de FERMA (Federation of European Risk Management Associations) y ECIIA (European Confederation of Institutes of Internal Auditing) sobre "Cyber Risk Management Governance".

D. Raúl Mateos

Gerente de Auditoría Interna del BBVA, representante de Auditores Internos.

Licenciado en Físicas por la Universidad de Salamanca, donde inició su carrera profesional. Posee las certificaciones CISA y CRISC de ISACA, y CISSP de ISC2. Ha sido responsable del Departamento Técnico del Grupo ADD en Madrid y Responsable de Aplicaciones en Producción de AOL Spain. Lleva 15 años como auditor de sistemas del Grupo BBVA, donde realiza funciones de Gerente de Auditoría

D. Santiago Sánchez

Representante de riesgos cibernéticos de Insurance Europe, en representación de UNESPA, Head of Sales & Distribution, Spain & Portugal Chubb

Ingeniero Industrial por la Universidad Politécnica de Madrid y ha desempeñado distintos puestos de responsabilidad durante los últimos 15 años en la industria aseguradora en compañías como Musaat, AIG y ahora en Chubb. Además, es el representante de UNESPA en el grupo de trabajo de Cyber que Insurance Europe está desarrollando a nivel europeo.

D. Juan Gayá

Director Gerencia de Riesgos de EL CORTE INGLÉS y Vocal de la Junta Directiva de AGERS.

Ingeniero Superior - Industrial por la Universidad Politécnica de Madrid, Máster MBA – IEDE.

Consultor de Sistemas de Información en Arthur Andersen 1988-1990 y Jefe de Proyecto (Dirección de Informática) en Peugeot, 1990 – 1992.

Desde entonces y hasta la actualidad trabaja en el Grupo de Seguros de El Corte Inglés. Pasó por los cargos de Jefe de Proyecto (TI), Director de Organización y actualmente es Gerente de Riesgos y Seguros del Grupo El Corte Inglés.

PRÓLOGO

El informe Corporate governance & cybersecurity que ha sido publicado por ECIIA y FERMA nos presenta una propuesta de modelo de gestión del riesgo corporativo procedente de las amenazas cibernéticas. De esta forma, trata de integrar en la estructura corporativa los principios de la normativa europea que resultará aplicable durante el próximo año (en materia de seguridad de sistemas tecnológicos y protección de datos).

La Directiva 2016/1148 de 6 de julio ha reconocido el deber que tienen las instituciones de fomentar "una cultura de gestión de riesgos" derivados de los sistemas tecnológicos. Así, las compañías deberán elaborar políticas y estrategias que permitan llevar a cabo una gestión racional, evaluable y sistemática de los riesgos cibernéticos. Y, junto con ello, el continuo desarrollo de la dependencia del ámbito socioeconómico a las IT pone de manifiesto la creación de un nuevo régimen de responsabilidad que podrá afectar a cualquier órgano de la estructura corporativa.

En definitiva, los ciber riesgos podrán afectar a toda la estructura y actividades de una entidad, por lo que deberán implementar un modelo de gestión adecuada de los mismos para garantizar la integridad y estabilidad financiera de toda la compañía. De tal forma, estos modelos de gestión deberán ir más allá del cumplimiento de la legislación en materia de protección de datos, y procurar garantizar la resilencia y responsabilidad de la entidad y de sus órganos de administración.

Jesús Jimeno Muñoz,

Autor de la síntesis del informe Corporate governance & cybersecurity

MODELO DE GOBIERNO CORPORATIVO DE CIBER RIESGOS: RESUMEN

1. INTRODUCCIÓN

La European Confederation of Institutes of Internal Auditing (ECIIA) y la Federation of European Risk Management Associations (FERMA) han creado un grupo de trabajo formado por gerentes de riesgos y auditores internos, con el objetivo desarrollar principios orientativos que permitan atender los riesgos cibernéticos como un riesgo corporativo. El resultado del trabajo desempeñado por este grupo ha dado lugar a la creación de un documento de trabajo con recomendaciones para la implementación de un modelo de gobernanza de ciber riesgos. Tales recomendaciones fueron publicadas el pasado 29 de junio, bajo el título *"corporate governance At the junction of & cybersecurity".*

El mencionado documento tiene por objeto facilitar la implementación de modelos que permitan la gestión corporativa -de instituciones públicas y privadas- de los riesgos cibernéticos. De esta forma, se pone de manifiesto que las normas de la UE en materia de seguridad de sistemas y protección de datos (la Directiva de seguridad de la red y la información –NIS- y el Reglamento General de Protección de Datos –GDPR-), cuya aplicación será efectiva durante el próximo año abogan por la creación de sistemas de gobierno y estructuras de gestión efectiva de ciber riesgos. Y por ello, el estudio advierte de que las instituciones *"deben ir más allá de la implementación de medidas IT, con el objeto de proteger efectivamente sus activos y garantizar su resilencia y continuidad"*.

El modelo de gestión propuesto se basa en la creación de un Grupo de Gobierno Corporativo de Ciber Riesgos ("Cyber Risk Governance Group" –CRGG-), cuya misión es determinar la exposición al riesgo cibernético en términos financieros, y designar los posibles planes para la contención y mitigación de estos efectos. El grupo tiene carácter multidisciplinar, está presidido por el Gerente de Riesgos, y reporta al Comité de Riesgos. Además, desarrolla funciones operativas que permiten clasificar el grado de exposición y establecer respuestas adecuadas, entre las que se diferencian: las funciones operativas de la primera línea de defensa (que incluyen la aplicación de soluciones técnicas en el ámbito de las IT); y, las

funciones de la segunda línea de defensa (en las que participan el Chief Information Oficer -CISO- y el Data Protection Officer -DPO-).

La categoría del CRGG dentro de la estructura corporativa debe permitir implementar planes de contención y mitigación de los riesgos cibernéticos. Además, este grupo tendrá que tener capacidad suficiente para decidir sobre las inversiones en ciber seguridad, y adoptar soluciones de transferencia de riesgos (como la suscripción de ciber seguros). A su vez, sus funciones operativas deben de llevarse a cabo de manera coordinada con el departamento de auditoría interna, de tal forma que permitan la revisión de los procesos de gestión implementados.

En definitiva, el modelo de gobierno corporativo propuesto constituye una herramienta que permitirá al órgano de administración analizar la exposición a los riesgos cibernéticos, adoptar decisiones estratégicas adecuadas a los mismos, y demostrar que se lleva a cabo una gestión racional, evaluable y sistemática de las ciber amenazas a las que se encuentra expuesta la institución.

Actualmente, la continua evolución de las IT y la implementación de proyectos de Big Data, se deben analizar a la luz del continuo desarrollo legislativo en materia de protección de datos personales. Así, resulta necesario combinar los sistemas estratégicos de innovación con planes de cumplimiento normativo, lo que permitirá mejorar la gestión de los riesgos cibernéticos de la compañía.

La Directiva 2016/1148 de 6 de julio ha recogido que *"debe fomentarse una cultura de gestión de riesgos que implique una evaluación del riesgo y la aplicación de medidas de seguridad adecuadas"*. En tal sentido, se podría considerar que la gestión de los riesgos cibernéticos queda recogida dentro del deber de diligencia propio de los administradores. Y por ello, el consejo de administración deberá demostrar que se han implementado políticas tendentes al análisis y control de estas amenazas.

2. FUNDAMENTOS DE LA GESTIÓN DE LOS CIBER RIESGOS

Los ciber riesgos pueden afectar en menor o mayor medida a cualquier nivel de la estructura de gestión y operativa de una organización. Por ello, resulta necesario que los planes de gestión de estos riesgos tengan en cuenta todos los niveles de la compañía, e involucren a todos los miembros de la misma. Así, el documento presentado por ECIIA y FERMA desarrolla un modelo completo de gestión sobre la base de los principios recogidos por el OECD *"Recommendation Digital Security Risk Management for Economic and Social Prosperity"*, y el informe *"The Three Lines of Defence model promoted in the joint document Audit and Risk Committees".*

2.1 The OECD Principles for Digital Security Risk Management

La OCDE publicó en 2015 una guía con 8 principios dirigidos a proteger a la información, el negocio, las operaciones, la reputación, los miembros y accionistas de organizaciones públicas y privadas de las amenazas relacionadas con el ámbito tecnológico. Tales principios han sido recogidos por el documento que venimos analizando como las bases para la creación de un modelo de gerencia de riesgos cibernéticos, y se clasifican conforme a los siguientes apartados:

- **Refuerzo de la conciencia y habilidades** para la creación de una cultura corporativa capaz de atender los ciber riesgos en cualquier punto de la estructura.
- **Responsabilidad**, individualización y determinación del rol y grado de responsabilidad de cada miembro de la organización.
- **Valores fundamentales y protección de los derechos humanos**, cuya salvaguarda debe ser atendida por medio de un sistema de *compliance* adecuado. Tal sistema estará enfocado a analizar las políticas y procesos corporativos conforme a la legislación aplicable en cada caso.
- **Cooperación**, que permita trabajar de forma conjunta a las distintas áreas de negocio dentro de una misma organización, y a ésta con otras compañías y entidades; y así, identificar sinergias y aprovechar fortalezas conjuntas para gestionar de manera más eficiente la ciber seguridad.
- **Evaluación de riesgos**, diseñada para identificar eventos potenciales que puedan afectar a la compañía, y proveer el nivel de seguridad

adecuado a los mismos[1]. Este principio trata de establecer herramientas que permitan identificar los riesgos estratégicos derivados de las IT; introducir medidas operativas para su gestión (en el ámbito tecnológico dirigidas por el CIO y en materia de *compliance* por el DPO); y, en última instancia cuantificar la exposición a escenarios catastróficos.

- **Medidas de seguridad apropiada y suficiente**, para reducir las vulnerabilidades, monitorizar los sistemas, detectar intrusiones y poder actuar en caso de que el sistema haya sido comprometido.
- **Innovación técnica y operativa** que permita la implementación de sistemas de control y gestión de los ciber riesgos.
- **Preparación y desarrollo de la resilencia** de los sistemas y procesos corporativos, para poder simultanear de forma efectiva la **continuidad** del negocio y la gestión de las crisis.

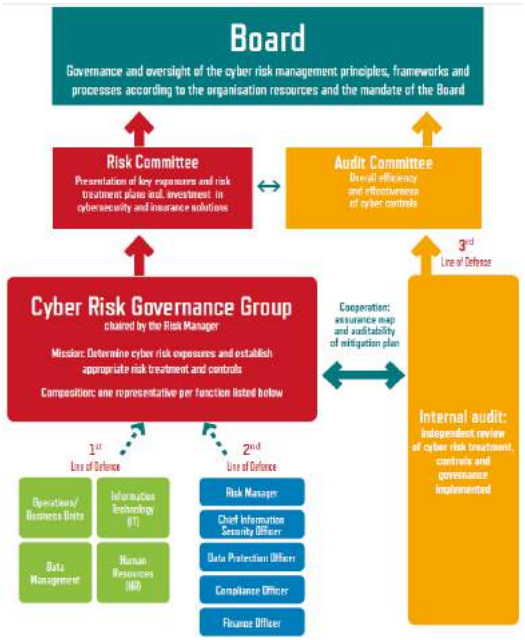
2.2 The three lines of defence

El Intitute of Internal Auditors (IIA) ha desarrollado el modelo *"the three lines of defence"* como una herramienta práctica para la gestión del riesgo corporativo. Así, el documento que venimos estudiando utiliza éste modelo para adecuar los mencionados principios a cada nivel de la estructura de una organización. Y, de esta forma desarrolla un completo modelo de gestión corporativa de los riesgos cibernéticos, basado en las tres líneas de actuación que propone el IIA:

- La **primera línea de defensa** es responsable de la implementación de las políticas de seguridad, monitorizar los sistemas y gestionar su control. Además, esta línea operativa debe ser capaz de identificar las tareas de control correspondientes a cada área de negocio.
- La **segunda línea de defensa** (dirigida por el CISO) se encarga de las actividades propias de la gestión de la ciber seguridad; elaborar el análisis de la exposición a los ciber riesgos con los datos que proporciona la primera línea; y, diseñar, desarrollar, e implementar las políticas de ciber seguridad.
- La **tercera línea de defensa** está formada por el área de auditoría interna que analiza las actividades llevadas a cabo por las otras líneas, y su adecuación a las políticas generales de ciber defensa.

1 Committee of Sponsoring Organizations of the Treadway Commission (COSO), (2004). Enterprise Risk Management — Integrated Framework Executive Summary (p. 2). http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf

En conclusión, el informe mantiene que las tres líneas de defensa deben colaborar y trabajar de forma conjunta, para garantizar que el órgano de administración tenga el nivel suficiente de conocimiento de la exposición de la compañía a los ciber riesgos. Tal conocimiento debe facilitar la adopción estrategias que permitan su adecuada gestión de los riesgos cibernéticos, y garantizar la responsabilidad de los miembros del mismo.



Modelo de Gobernanza del Ciberriesgo FERMA-ECIIA

Basado en el Modelo de las Tres Líneas de Defensa

3. MODELO DE GOBIERNO CORPORATIVO EN UN CONTEXTO DIGITAL

La responsabilidad del órgano de administración de una entidad se circunscribe al ámbito de sus deberes y obligaciones, y estas se centran en la adopción de políticas y en la toma de decisiones organizativas y estrategias. No obstante, podrá derivarse la responsabilidad de tales órganos en la medida en la que los problemas operativos relacionados con las IT, afecten o tengan relación con situaciones propias de aquel ámbito.

Así, la implementación de un modelo de gobierno corporativo de gestión de los riesgos cibernéticos, adecuado a la estructura de la entidad, podrá evitar que se derive esta responsabilidad.

La oportuna introducción de este modelo permite definir cada una de las funciones estratégicas y operativas, y distribuirlas dentro de los distintos grupos de interés que forman parte de la estructura de la entidad. De esta forma, el modelo propuesto por el informe de referencia distingue:

3.1 Consejo de Administración

El desarrollo de los riesgos tecnológicos hace que los órganos de administración deban tener la capacidad de adaptar la estrategia de la compañía a los nuevos desafíos, y procurar que esta disponga de los recursos adecuados. Por ello, será necesario que estos órganos dispongan de la formación e información adecuada, sobre las circunstancias propias de los ciber riesgos y el grado de exposición a los mismos. De esta forma, resultará conveniente que tales órganos de administración trabajen de forma coordinada con el comité de riesgos y el comité de auditoría interna.

3.2 Comité de riesgos y Grupo de Gobierno Corporativo de Ciber Riesgos.

El carácter estratégico de los ciber riesgos, y su posible relación con materias propias de la competencia de los órganos de administración, hacen que resulte apropiado que el Grupo de Gobierno de Ciber Riegos –CRGG- se constituya como un órgano separado. De esta forma, deberá ostentar competencias y funciones propias, atinentes a las áreas de la entidad con mayor explosión a los ciber riesgos. El CRGG estará dirigido por el gerente de riesgos, y formado por representantes de aquellos grupos internos de interés entre los que destacan los departamentos de IT y HR, el DPO y el CISO.

Tal composición permite al CRGG ejecutar sus principales funciones entre las que se encuentra: el análisis de la exposición a los riesgos cibernéticos; el desarrollo de planes para mitigarlos; y, en su caso, la trasmisión de esta información al comité de riesgos y a los órganos de administración. Además, el CRGG deberá trabajar de forma coordinada con el comité de auditoría para desarrollar planes de actuación susceptibles de ser

auditables, y facilitar la detección de la exposición a los ciber riesgos en las distintas áreas de la entidad.

3.3 La aplicación del modelo "The three lines of defense" en el contexto digital.

- **First line of defense**, permite gestionar de forma operativa los ciber riesgos y aplicar los programas de mitigación por medio de los siguientes grupos de interés:

    a. El **departamento de IT** se encarga de la implantación de protocolos y herramientas de seguridad, y comprobar la integridad y seguridad de los sistemas.
    b. El **Chief Data Officer (CDO**), cuyas funciones pueden ser asumidas por el CISO, se encarga de controlar las políticas de protección de datos y privacidad, y desarrollar procesos que permitan su control y seguridad.
    c. El departamento de **recursos humanos**, debe asegurar que el tratamiento de los datos y de la información corporativa por parte de los empleados es correcto. Y, en su caso, procurar evitar el ejercicio de malas prácticas en esta materia, sancionar, y derivar responsabilidades.

- **Second line of defense,** permite monitorizar los efectos de los ciber riesgos y gestionarlos mediante las funciones operativas correspondientes de la primera línea de defensa. Esta segunda línea de defensa se encuentra formada por los siguientes grupos de interés:

    a. El **Gerente de Riesgos** tiene por objetivo principal establecer planes para mitigar los efectos de un ciber evento, y procurar que la entidad continúe funcionando de manera adecuada en tales casos. Para ello, dirige el comité de riesgos y el CR.GG, y coordina con los distintos grupos de interés –HR, IT, DPO y CISO- las decisiones adoptadas por los órganos de administración en materia de ciber riesgos.

    Los Gerentes de Riesgos deben ser capaces de determinar el grado de exposición al riesgo cibernético, el coste de los

sistemas de ciber seguridad, y equilibrar tal seguridad con los requisitos operativos. Además, es responsable de procurar la correcta transmisión de los ciber riesgos a la industria aseguradora, por medio de la suscripción de pólizas adecuadas al riesgo concreto.

b. El **Data Protection Officer** es una figura introducida por el Reglamento (UE) 2016/679, cuyas funciones se desarrollan en torno a la protección de datos. Particularmente, se encarga de prestar la información y asesoramiento en la materia; monitorizar los procesos y asegurar que se llevan a cabo conforme a la regulación aplicable (compliance); facilita el enlace entre la entidad y las autoridades públicas encargadas de la protección de datos; y, se encarga de informar a los órganos de administración de las circunstancias relevantes en esta materia[2].

c. El **Chief Information Security Officer (CISO)** se encarga de gestionar la seguridad de los sistemas de información (IT) de la organización, de manera que permitan alcanzar un equilibrio entre seguridad innovación y productividad.

d. La **Dirección financiera** analiza y controla las inversiones y presupuestos en materia de ciber seguridad y gestión del riesgo cibernético (entre los que se encuentra el coste de los seguros); y, permite cuantifica la exposición de la entidad a los ciber riesgos.

e. **Compliance Officer**, los cometidos relacionados con el asesoramiento legal de las entidades son mayores en la medida en la que se desarrolla la exposición a los ciber riesgos, y aumentan las posibles responsabilidades –contractuales y extracontractuales- derivadas de los mismos. Por ello, las funciones de este grupo de interés exceden del mero asesoramiento en materia de cumplimiento normativo.

2 Data Protection Officers (DPOs), ARTICLE 29 DATA PROTECTION WORKING PARTY, (13 diciembre 2016) http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

- **Third line of defence: auditoría interna.** La misión de la comisión de auditoría es *"mejorar y proteger el valor de la organización mediante el suministro de información objetiva basada en el riesgo, el asesoramiento y la comprensión"*[3] de los procedimientos de la entidad. De esta forma, el principal cometido de la auditoría interna en materia de ciber riesgos es proveer información independiente al órgano de administración sobre los procesos de ciber seguridad. Y además, revisar las actividades llevadas a cabo por la primera y segunda línea de defensa para gestionar y mitigar los ciber riesgos.

3.4 Grupos externos de interés

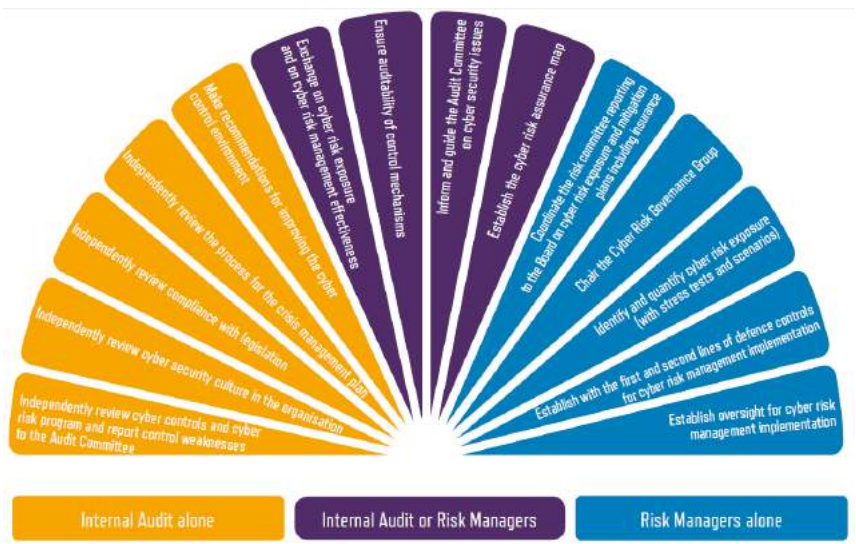
- Aseguradoras, la transmisión de los ciber riesgos a la industria aseguradora exige que el gerente de riesgos tenga un conocimiento adecuado de la exposición de la entidad a los mismos, y de las características propias de estos riesgos. De esta forma, resulta necesario que se alcance un grado de comunicación óptimo entre la aseguradora, el asegurado y los sujetos que intervengan durante la suscripción y vigencia del contrato.
- Instituciones públicas y organismos reguladores, la ciber seguridad es una cuestión social y política, ya que puede llegar a afecta a las infraestructuras críticas y a los derechos de los ciudadanos. Por ello, la colaboración entra las instituciones públicas y privadas permite mejorar la resilencia y resulta imprescindible en ciertos casos (como los ciber eventos catastróficos).
- Proveedores, el CRGG debe ser capaz de identificar a los proveedores que puedan estar expuestos a riesgos cibernéticos, y determinar el grado de exposición que producen esos riesgos para la compañía. En este sentido, se deben fomentar políticas de contratación de proveedores que adopten medidas de ciber seguridad adecuadas a su actividad. Y definir las posibles responsabilidades derivadas de la exposición a los ciber riesgos en los acuerdos que alcance la entidad.

3 IIA, 'International Professional Practices Framework', https://global.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx

4. CONCLUSIONES

La nueva regulación de la UE en materia de seguridad de sistemas y protección de datos, y la tendencia general a implementar políticas de transparencia en esta materia hacen que las compañías tengan que reforzar sus sistemas de ciber seguridad. En este sentido, la ciber seguridad se ha convertido en una materia estratégica que forma parte del gobierno corporativo de todas las compañías.

La adecuada gestión de los riesgos cibernéticos permite a las compañías garantizar la exposición de todas las áreas de su negocio, y adoptar planes operativos que mitiguen estos riesgos. Por ello, el informe propone la creación del *"Cyber Risk Governance Group"* –CRGG- liderado por el gerente de riesgos, y supervisado por el comité de auditoría interna. De esta forma, las compañías tendrán una herramienta de gestión eficiente de los ciber riesgos que faciliten su identificación, cuantificación, análisis de la exposición y la transmisión de la información sobre los mismos a los órganos de administración y grupos de interés. Y, con ello, se podrá lograr garantizar la resilencia y preservar la responsabilidad de los miembros de la entidad.



Áreas clave de actividad complementaria y colaboración entre la gestión de riesgos y las profesiones de auditoría interna.

agers
Asociación Española
de Gerencia de
Riesgos y Seguros
www.agers.es

Instituto de
AuditoresInternos
de España
www.auditoresinternos.es