APOYANDO LA CIBERSEGURIDAD

CIBER

El pasado 29 de junio, FERMA y ECIIA realizaron una llamada ante el Parlamento Europeo para aumentar la resiliencia de las organizaciones ante el desarrollo de las nuevas ciberamenzas.

AGERS se ha preocupado y ocupado en desarrollar entre sus asociados la cultura en seguridad, porque según dicen muchos expertos **El usuario es el eslabón más IMPORTANTE de la cadena de la seguridad.**

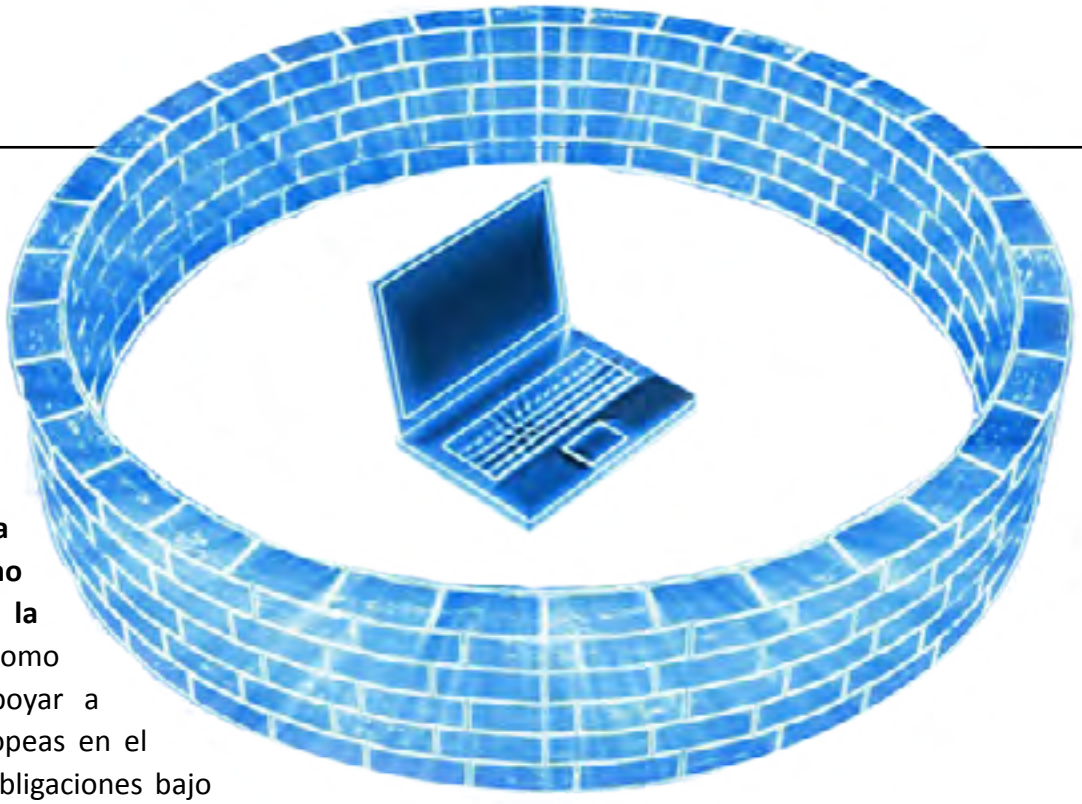
Nuestra Asociación dispone de la Comisión de Cyber desde el año 2012 compuestas por Directores de Riesgos y Seguros de grandes corporaciones, desde donde se promueve junto con organizaciones especializadas, fomentar los conocimientos de los profesionales de la gestión de riesgos y seguros en España, mediante la organización de eventos y foros, así como la elaboración de materiales didácticos centrados en los fundamentos y en los últimos avances relativos a la gestión de cyber riesgos.

Este año la Comisión de Cyber de AGERS presentó en el XXVIII Congreso Nacional de la Asociación, celebrado el 1 de junio en el Colegio Oficial de Arquitectos de Madrid, su Guía de terminología de ciberseguridad, realizada junto a ISMS FORUM, donde se recogen de manera sencilla y ágil una selección de términos con los que cualquier persona no experta debe conocer en su día a día, especialmente los profesionales de riesgos y seguros.

Descarga exclusivo para asociados

En la actualidad la Comisión de Cyber, se plantea nuevos proyectos sobre ciberseguridad que esperemos vean la luz muy pronto.

Como extensión de este objetivo, D. Alfredo Zorzo, Business Development Director / Risk & Insurance Director en One eSecurity y Vocal de la Junta Directiva de AGERS en representación de AGERS ha formado parte del Grupo de trabajo de cyber de **FERMA (Federación Europea de Asociaciones de Gerencia de Riesgos) y junto con ECIIA se ha elaborado el "Cyber Risk Governance Report"**, informe que las dos organizaciones presentaron en el Parlamento Europeo de Bruselas al que acudieron representantes de las instituciones de la Unión



Europea, del Foro Económico Mundial, profesionales de riesgos y auditorías así como otros interesados en la materia.

El informe **"Hacia la unión del gobierno corporativo y la ciberseguridad"** tiene como objetivo primordial apoyar a las organizaciones europeas en el cumplimiento de sus obligaciones bajo el Reglamento General de Protección de Datos de la UE (GDPR) y la Directiva de Seguridad de la Información en las Redes (NIS).

Los recientes ataques cibernéticos, sin embargo, aumentaron la preocupación de los expertos, en lo que ven como una mayor falta de enfoque de la gerencia del riesgo respecto a la ciberseguridad.

El presidente de FERMA Jo Willaert afirma: "Como demuestran los recientes ataques, el riesgo cibernético es una cuestión empresarial que afecta a los aspectos estratégicos de los directivos incluyendo la valoración, la reputación y la confianza. La gestión del ciberriesgo se ha convertido, por lo tanto, en una cuestión corporativa que debe reflejarse en el gobierno de la empresa".

Añade, "Nuestras dos profesiones están uniendo sus fuerzas en la gestión del riesgo cibernético mediante el intercambio de información sobre el sistema ERM y los controles cibernéticos propios, asegurando que los planes de mitigación sean auditables desde su concepción. Esto es crucial para evaluar su impacto y revisar correctamente la estrategia".

El informe pide la creación de grupos que gobiernen los ciberriesgos, presididos por el Gerente de riesgos, para operar en todas las funciones dentro de la empresa.

El papel de los grupos es determinar el coste potencial de los riesgos cibernéticos en toda la organización, incluyendo escenarios de riesgo catastrófico y proponiendo medidas de mitigación al Comité de Riesgos y a los órganos de Alta Dirección.

Además de los Gerentes de riesgos, el grupo se compondrá de representantes de todas las funciones clave a nivel empresarial involucrados en el riesgo digital, en particular las tecnologías de la información (IT), recursos humanos, comunicaciones, finanzas, responsable de protección de datos (DPO), responsable de la seguridad de la información (CISO).

La Auditoría Interna proporcionará la seguridad necesaria a la Junta Directiva de que los controles de riesgo cibernético están operando de manera efectiva.

Agrega Jo Willaert, "Esta propuesta de modelo de gobernanza de ciberriesgos constituye una innovadora manera para que las organizaciones aborden la ciberseguridad. Permitirá demostrar a la Junta Directiva que los ciberriesgos se gestionan mediante un análisis racional y documentado de los riesgos a lo largo de toda la organización ".

El modelo de gobernanza del riesgo cibernético FERMA-ECIIA se basa en dos sólidos principios: los ocho principios establecidos en la Gestión de Riesgos de Seguridad Digital de la OCDE (2015) y el modelo de las Tres Líneas de Defensa, reconocido como el estándar de la Gerencia de Riesgos Empresarial (ERM).

Acceso al informe completo

D. Alfredo Zorzo, Business Development Director / Risk & Insurance Director en One eSecurity, Vocal de la Junta Directiva de AGERS y participante en el grupo de Trabajo de Ciberriesgos de la Federación Europea afirma:

"El trabajo realizado durante estos 6 meses entre Risk Managers y Auditores Internos europeos ha sido un ejemplo de la capacidad que FERMA y ECIIA, así como todas las asociaciones nacionales, como es el caso de AGERS, ofrecen a la sociedad en general cuando debemos enfrentarnos a cualquier tipo de riesgo y, en concreto, a los que actualmente figuran en la lista de los más preocupantes, como son los Ciberriesgos.

Las conclusiones y propuestas recogidas en este informe son una guía para todas las organizaciones, tanto públicas como privadas, que hoy están sujetas al impacto de estos riesgos.

La definición de un **modelo de gobernanza en ciberriesgos** no es sencilla y, probablemente, cada organización adecuará el suyo conforme a sus características, pero **este informe servirá para sentar las bases de cómo abordarlo y qué y quién tener en cuenta en cada momento.** La tecnología permite la evolución de las organizaciones pero exige que éstas se adapten a los riesgos inherentes a ella, esto es una muestra de ello."