Resumen ejecutivo de la jornada

Siniestros cyber: análisis, gestión y respuesta en el entorno actual

Barcelona | 20 de mayo de 2026

AGERS, en colaboración con Marsh y SOMPO, celebró en Barcelona una sesión especializada para analizar la evolución de los siniestros cyber, los criterios de gestión y respuesta ante incidentes, y el papel del seguro como herramienta de transferencia y mitigación del riesgo. La jornada reunió a profesionales del sector asegurador y de la gerencia de riesgos en un formato orientado al intercambio de conocimiento experto y lecciones prácticas.

Ficha de la jornada

Fecha	20 de mayo de 2026
Lugar	Centre de Formació CaixaBank, Gran Via Carles III, 85 BIS, Barcelona
Formato	Presencial, con bloque de contenidos y networking
Organización	AGERS, en colaboración con Marsh y SOMPO
Eje temático	Siniestros cyber: coberturas, gestión, respuesta, tendencias y controles críticos

1. Resumen ejecutivo

La jornada puso de manifiesto que los siniestros cyber han dejado de ser eventos puramente tecnológicos para convertirse en crisis empresariales integrales. Su impacto combina costes de respuesta, recuperación de activos digitales, interrupción de negocio, eventuales reclamaciones de terceros, obligaciones regulatorias, exposición reputacional y, en determinados supuestos, pérdidas derivadas de extorsión o fraude.

Uno de los mensajes centrales fue la necesidad de conectar tres planos que con frecuencia se gestionan de forma separada: la prevención técnica, la preparación organizativa y la arquitectura aseguradora. La eficacia ante un incidente depende tanto de los controles implementados antes del siniestro como de la claridad del condicionado, la activación temprana de proveedores especializados y la capacidad de coordinar decisiones legales, técnicas, operativas y de comunicación.

La sesión también evidenció una estabilización relativa en el número de notificaciones de siniestros cyber en Europa tras ejercicios de elevada actividad, aunque con una advertencia relevante: los resultados medios pueden ocultar una cola de pérdidas severas cada vez más significativa. En ese contexto, el ransomware sigue siendo un vector de pérdida especialmente complejo por la combinación de cifrado, restauración tecnológica, interrupción del negocio y exposición de datos.

Desde una perspectiva de gerencia de riesgos, la principal conclusión es clara: el seguro cyber aporta valor cuando se integra en un marco robusto de gobernanza, controles básicos reforzados, planificación de respuesta y revisión continua de brechas de cobertura. La póliza no sustituye a la resiliencia, pero puede ser decisiva para movilizar capacidades y financiación en las primeras horas de una crisis.

2. Principales conclusiones

Conclusión	Implicación ejecutiva
El riesgo cyber es transversal	El incidente afecta simultáneamente a tecnología, operaciones, legal, compliance, finanzas, comunicación, clientes y cadena de suministro.
La preparación previa condiciona el resultado	MFA, backups protegidos, EDR, filtrado de correo, parcheo, PAM, SOC y formación aparecen como controles críticos para reducir frecuencia y severidad.
La póliza debe entenderse antes del siniestro	Activadores, definiciones, exclusiones, sublímites, franquicias y condiciones de seguridad pueden determinar la existencia o alcance de cobertura.
La rapidez de respuesta es determinante	Las primeras 72 horas son críticas para contener, preservar evidencias, activar proveedores, evaluar notificaciones y minimizar interrupción de negocio.
La cadena de suministro digital amplifica el riesgo	Los incidentes vinculados a terceros, proveedores tecnológicos y ecosistemas digitales seguirán ganando peso.
Las nuevas tecnologías generan nuevos escenarios	La inteligencia artificial, los navegadores agénticos y la computación cuántica introducen vectores emergentes que exigen revisión continua de controles y modelos de aseguramiento.

3. Desarrollo de la jornada

Apertura institucional - AGERS

La apertura, a cargo de Alicia Soler, Directora de AGERS, enmarcó la jornada como un espacio especializado para abordar un riesgo de creciente relevancia en el entorno empresarial. La colaboración con Marsh y SOMPO permitió articular una visión completa del siniestro cyber: desde el diseño de coberturas hasta la gestión técnica y operativa del incidente.

El enfoque de la sesión fue eminentemente práctico: compartir experiencias, criterios de actuación y lecciones aprendidas que ayuden a las organizaciones a anticipar, responder y transferir adecuadamente el riesgo.

Coberturas de la póliza cyber - SOMPO

La intervención de Olivier Marcen Prieto, Head of Financial Lines Iberia de SOMPO, se centró en los elementos que deben revisarse en una póliza cyber para evitar sorpresas en el momento de la reclamación. La sesión subrayó la importancia de contar con condicionados amplios, comprensibles y adaptables a la realidad de cada organización.

Entre los activadores relevantes se destacaron los sucesos de privacidad, los incidentes de seguridad y los fallos de sistema. En cuanto a prestaciones, se abordaron costes de respuesta a incidentes, recuperación de activos digitales, interrupción del servicio del asegurado y de proveedores, extorsión, recompensa, daño reputacional, cyber crime y fraude en telecomunicaciones.

La presentación incidió en que la póliza debe estar alineada con un plan de respuesta y emergencia, disponer de proveedores adecuados y contemplar la operativa real de la organización. Las condiciones de seguridad -por ejemplo, MFA en accesos remotos o privilegiados- no son meros requisitos formales: pueden convertirse en elementos decisivos en la cobertura del siniestro.

Casos reales y siniestralidad - Marsh

La intervención de Sofía García-Ollauri Antolín, Head of FINPRO & CYBER Claims Advocacy Turnaround & Restructuring Practice Leader en Marsh, aportó una lectura práctica de la siniestralidad y del comportamiento de los incidentes antes, durante y después de su materialización.

Los datos compartidos de Marsh Europe mostraron que el 73% de los incidentes reportados incorporan componente de brecha de privacidad, el 15% están relacionados con extorsión cyber, incluido ransomware, el 14% se vinculan a

terceros y el 18% generan impacto de interrupción de negocio. Este reparto confirma que la gestión del siniestro exige integrar respuesta técnica, cumplimiento normativo, gestión de proveedores y continuidad de negocio.

La ponencia reforzó la idea de que la mediana de resultados puede enmascarar un incremento de las pérdidas severas. En particular, el ransomware sigue actuando como principal driver de pérdida por su capacidad de combinar cifrado, restauración, interrupción de actividad y posible afectación a datos personales o corporativos.

Tendencias, controles y metodología de caso - Marsh

Nelia Argaz Durango, Director, Head of Cyber, Digital and Resilience Risks, Europe en Marsh, abordó las tendencias de amenaza, los controles esenciales y la metodología aplicable a un caso real. La ponencia situó el riesgo cyber en un contexto de ataques más sofisticados, dirigidos, frecuentes y persistentes.

Las tendencias expuestas incluyen la inteligencia artificial, la geopolítica, la democratización del cibercrimen, la exposición de la cadena de suministro, la soberanía digital, el incremento de la superficie de ataque y riesgos emergentes como el enfoque "harvest now, decrypt later" asociado a la computación cuántica.

La respuesta propuesta se resumió en una vuelta a los fundamentos, pero reforzada: planificación y pruebas de respuesta a incidentes, concienciación y simulaciones de phishing, monitorización, protección de red, mitigación de RDP, sustitución o protección de sistemas end-of-life, gestión de proveedores, MFA, parcheo, filtrado de correo y web, PAM, backups cifrados y probados, y EDR.

4. Lecciones prácticas

Momento	Acciones prioritarias
Antes del incidente	Realizar un diagnóstico de exposición cyber, mapear activos críticos, identificar dependencias de proveedores, revisar el encaje de la póliza con la realidad operativa y comprobar que los controles declarados se aplican de forma efectiva.
Durante el incidente	Activar un comité de crisis, preservar evidencias, contactar con aseguradora/corredor, coordinar proveedores forenses y legales, evaluar impacto en negocio y datos, y mantener una comunicación controlada con partes interesadas.
Después del incidente	Documentar decisiones, costes y evidencias; revisar causas raíz; actualizar controles; ajustar procedimientos de respuesta; renegociar gaps de cobertura y reforzar formación interna.

5. Riesgos emergentes destacados

Navegadores agénticos e instrucciones ocultas

La sesión presentó un escenario en el que agentes o navegadores con capacidad de actuar por el empleado pueden ejecutar instrucciones ocultas incluidas en páginas aparentemente legítimas. La amenaza es especialmente sensible porque opera con sesiones autenticadas y credenciales legítimas, lo que dificulta la detección por controles tradicionales.

Cadena de suministro digital

La invisibilidad de dependencias tecnológicas y proveedores externos incrementa la superficie de ataque. Los incidentes en MSP, plataformas, servicios cloud o proveedores críticos pueden trasladarse rápidamente al asegurado y multiplicar el impacto operativo.

Riesgo cuántico y exposición futura

El enfoque "harvest now, decrypt later" recuerda que la confidencialidad de la información sensible debe evaluarse también en horizontes temporales largos. Las organizaciones con datos de alto valor deben empezar a considerar estrategias de criptoagilidad y clasificación reforzada de información.

6. Recomendaciones ejecutivas

- Revisar el condicionado cyber con una matriz que conecte escenarios de pérdida, activadores, exclusiones, límites, sublímites, franquicias, tiempos de espera y proveedores preaprobados.
- Validar que los controles exigidos o declarados en suscripción están realmente implantados y son auditables, especialmente MFA, PAM, backups, EDR, parcheo y protección de accesos remotos.
- Ensayar el plan de respuesta con simulacros que incluyan a dirección, legal, comunicación, tecnología, finanzas, corredor, aseguradora y proveedores forenses.
- Reforzar la gestión de terceros mediante inventario, criticidad, requisitos contractuales, evidencias de seguridad y planes de continuidad compartidos.
- Incorporar escenarios emergentes vinculados a inteligencia artificial, agentes autónomos y exposición de credenciales legítimas en los programas de formación y pruebas de control.
- Mantener una trazabilidad exhaustiva de costes, decisiones y evidencias desde el primer momento del incidente para facilitar la reclamación y la defensa de cobertura.

7. Valor aportado por la jornada

La sesión permitió trasladar al mercado una visión integrada del siniestro cyber, combinando el enfoque asegurador, la experiencia en reclamaciones y la perspectiva de resiliencia digital. Su principal aportación fue convertir conceptos técnicos y contractuales en decisiones concretas de gestión.

Para AGERS, la jornada refuerza su papel como punto de encuentro entre empresas, gerentes de riesgos, aseguradoras, corredores y especialistas, facilitando un debate necesario sobre cómo anticipar, transferir y gestionar uno de los riesgos con mayor capacidad de disrupción para las organizaciones.

Anexo. Agenda y ponentes

Horario	Ponente	Contenido
16:00 - 16:05	Alicia Soler, Directora de AGERS	Apertura del evento
16:05 - 16:35	Olivier Marcen Prieto, VP. Head of Financial Lines Iberia de SOMPO	Coberturas póliza cyber
16:35 - 17:00	Sofía García-Ollauri Antolín, Marsh	Casos reales: análisis antes, durante y después de un incidente
17:00 - 17:45	Nelia Argaz Durango, Marsh	Tendencias, controles y metodología de un caso
17:45 - 18:00	Ponentes y asistentes	Preguntas del público y cierre
18:00 - 19:00	Asistentes	Networking

-