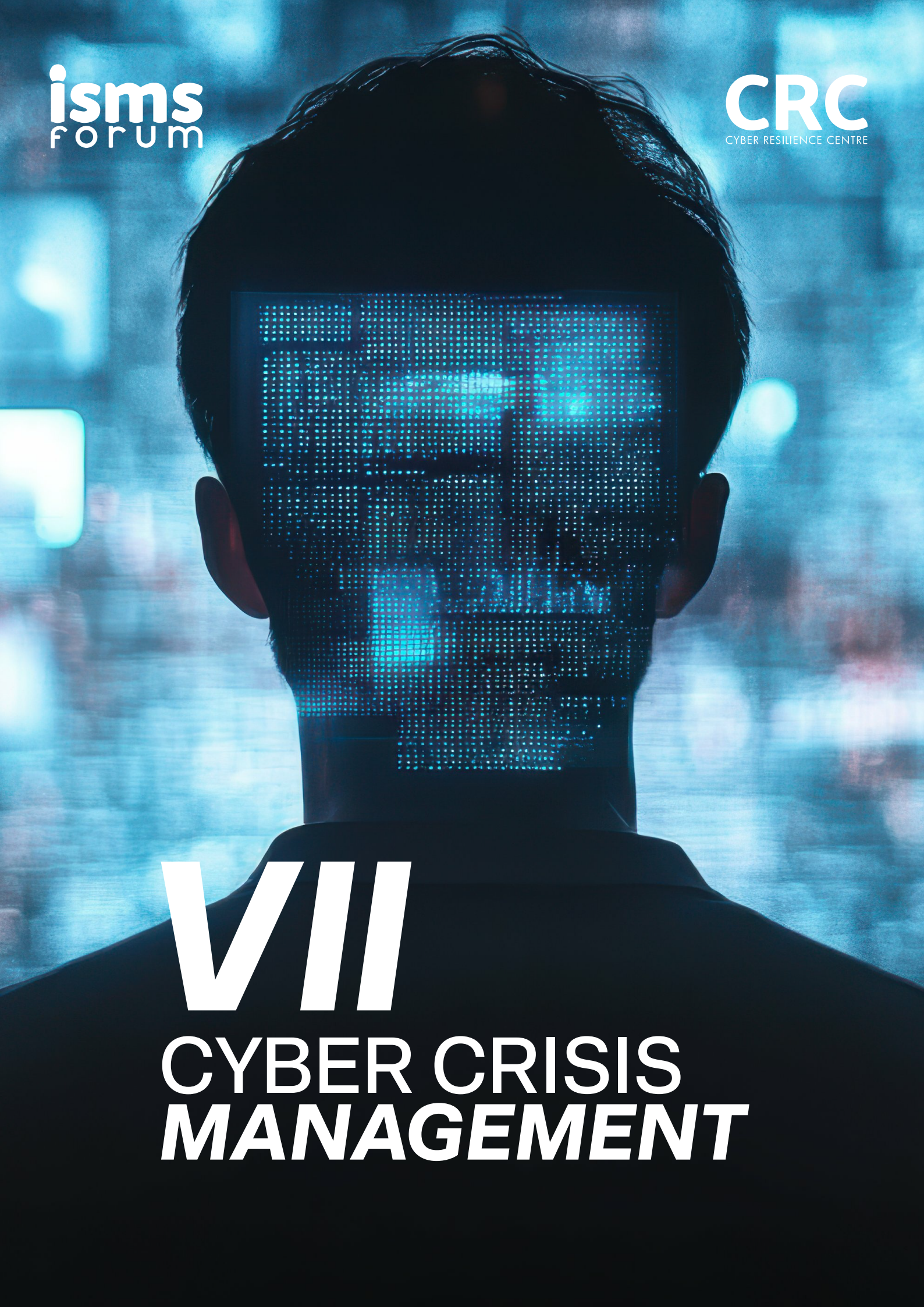
isms forum

CRC
CYBER RESILIENCE CENTRE



VII

CYBER CRISIS *MANAGEMENT*

Edición
Beatriz García

Maquetación y diseño
Susana Marín

Agradecimientos
Queremos expresar nuestro más sincero agradecimiento a todas las empresas que, año tras año, participan activamente en el ejercicio de gestión de crisis cibernéticas, contribuyendo con su experiencia y compromiso a la mejora continua de la ciberresiliencia sectorial.

Agradecemos especialmente a **Inmersive Labs**, que este año ha cedido la plataforma tecnológica para la realización del simulacro, y al **Institut Cerdà**, entidad evaluadora de la presente edición.

Reconocemos la labor de **José Manuel Rivera**, responsable de la elaboración del guion de la simulación, así como la implicación de todos los profesionales que han hecho posible el desarrollo y la evaluación del ejercicio.

Contenido

Resumen Ejecutivo

Este documento consolida la justificación, el alcance y la aportación de valor del programa anual de **Ciber Crisis Management**, que en 2025 celebra su **VI edición consecutiva** bajo la organización de **ISMS Forum** y la colaboración de entidades públicas y privadas de referencia. Esta continuidad evidencia el compromiso sostenido del sector con la mejora de la ciberresiliencia y la profesionalización de la gestión de crisis cibernéticas en España.

La iniciativa, pionera en el ámbito nacional, se ejecuta mediante un **simulacro virtual gamificado** que expone a los equipos a **dilemas de decisión, coordinación interdepartamental y comunicación** (interna y externa), midiendo tiempos y eficacia de respuesta. Los **resultados agregados y anonimizados** se presentan este año en la **XXVII Jornada Internacional de Seguridad de la Información**[1], consolidando una comparativa sectorial y un repositorio de lecciones aprendidas. La reiteración anual del ejercicio permite observar la evolución de la madurez sectorial y la consolidación de buenas prácticas.

Desde el prisma regulatorio, la participación en estos ejercicios evidencia la diligencia debida frente a **NIS2**[2] (gestión de riesgos, respuesta a incidentes, continuidad, y pruebas periódicas) y alinea el programa con **ISO 22301**[3] (BCMS), que exige mantener un programa de ejercicios y pruebas con informes post-ejercicio y acciones de mejora.

La presión del entorno de amenaza en la Unión Europea —con DDoS y ransomware como vectores predominantes y un impacto especialmente alto en administraciones públicas, transporte y finanzas— refuerza la necesidad de institucionalizar estos ejercicios como palanca de prosiliencia (anticipación, preparación, aprendizaje y mejora continua).

[1] https://www.ismsforum.es/evento/786/xxvii-jornada-internacional-de-seguridad-de-la-informaci-n/

[2] Parlamento Europeo y Consejo de la Unión Europea. (2022). Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2). Diario Oficial de la Unión Europea, L 333, 80-152. https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963

[3] Organización Internacional de Normalización. (2019). ISO 22301:2019 Seguridad y resiliencia — Sistemas de gestión de continuidad del negocio. https://www.iso.org/standard/75106.html

Contexto y justificación

El entorno digital en el que operan hoy las organizaciones está marcado por una aceleración tecnológica y una presión creciente derivada de la sofisticación de las amenazas cibernéticas. La experiencia de los últimos años demuestra que los incidentes son más frecuentes y su impacto puede comprometer **la continuidad de negocio, la confianza de los clientes y la reputación institucional** en cuestión de horas.

En este escenario, la resiliencia deja de ser opcional para convertirse en una exigencia estratégica. La anticipación, la respuesta efectiva y la recuperación ágil de una crisis cibernética depende tanto de la tecnología como de la **preparación de las personas y la solidez de los procesos.** La gestión de crisis cibernéticas requiere una visión transversal, donde convergen áreas técnicas, jurídicas, de comunicación y negocio para minimizar daños y acelerar la recuperación.

ISMS Forum ha evolucionado su estructura interna para abordar la ciberresiliencia de forma integral. Junto con las áreas históricas como Ciberseguridad, Privacidad del Dato, Cloud e Inteligencia Artificial, se ha incorporado el **área de Resiliencia (CRC)**, dando respuesta a la creciente demanda de un enfoque experto en resiliencia, continuidad de negocio y gestión de crisis. En el seno de CRC se ha constituido un Comité Técnico Operativo que, con un enfoque multidisciplinar, contribuye al diseño de escenarios, la definición de buenas prácticas y la emisión de recomendaciones operativas, orientadas a anticipar, gestionar y superar situaciones de crisis con mayores garantías.

La evolución normativa —con la transposición de NIS2— exige políticas y procedimientos robustos, incluyendo la realización periódica de ejercicios y pruebas que verifiquen la eficacia de los mecanismos de resiliencia. En paralelo, ISO 22301 establece, en el artículo 8.5, mantener un programa estructurado de simulacros con objetivos claros, escenarios realistas, evaluación objetiva y ciclo de mejora continua.

En definitiva, el ejercicio anual de Ciber Crisis Management trasciende el mero cumplimiento normativo y se consolida como práctica de referencia para fortalecer la gobernanza, la coordinación público-privada y la confianza de los órganos de gobierno y la Alta Dirección. Su reiteración permite identificar tendencias, compartir lecciones aprendidas y elevar la madurez del ecosistema digital, posicionando a las entidades participantes en la vanguardia de la ciberresiliencia en Europa.

Alcance, objetivos, metodología y modelo de gobierno

El Ejercicio de Crisis Cibernéticas de ISMS Forum se ha consolidado como un **referente en la evaluación y fortalecimiento de las capacidades organizativas** frente a incidentes de seguridad de alto impacto. Su diseño responde a la necesidad de poner a prueba, en un entorno controlado pero realista, la capacidad de las entidades para detectar, contener, erradicar y recuperar la normalidad ante una crisis cibernética, así como para gestionar la comunicación y la coordinación interna y externa en situaciones de máxima presión.

El alcance del ejercicio va mucho más allá de la mera simulación técnica. Se trata de una **experiencia integral** que exige la activación de procedimientos reales de crisis, la implicación de equipos multidisciplinares y la toma de decisiones bajo incertidumbre. El objetivo es doble: por un lado, **medir la madurez** y la eficacia de los mecanismos existentes; por otro, **identificar oportunidades de mejora** y fomentar la adopción de buenas prácticas que permitan evolucionar hacia modelos de resiliencia más robustos y adaptativos.

La **metodología** del ejercicio de Crisis Cibernéticas se basa en la construcción de un escenario diseñado para ser aplicable a organizaciones de distintos sectores y evitar casuísticas excesivamente específicas. La plataforma de gamificación empleada plantea dilemas y retos que requieren la toma de decisiones en tiempo real, midiendo tanto la calidad de las respuestas como los tiempos de reacción y la eficacia de las medidas adoptadas, siempre bajo criterios de resiliencia. Este enfoque fomenta la **coordinación interdepartamental**, involucrando a áreas como Seguridad, IT, Legal, Comunicación y Negocio, y permite establecer criterios de puntuación objetivos que facilitan la comparación entre participantes y la elaboración de planes de mejora personalizados.

El **modelo de gobierno** del ejercicio se apoya en una estricta política de confidencialidad. Toda la información de contexto, técnica, sensible y los resultados generados durante el simulacro se consideran confidenciales y se gestionan bajo protocolos de almacenamiento cifrado y acceso restringido al personal autorizado. Las comunicaciones externas que se derivan del ejercicio, especialmente tras su finalización, se presentan siempre de forma agregada y anonimizada, con una intencionalidad positiva. Las comunicaciones internas, por su parte, pueden ser colectivas —sin datos que permitan identificar vulnerabilidades concretas— o individuales, en cuyo caso se mantienen estrictamente confidenciales.

En cuanto a la **evaluación y los entregables**, cada entidad participante recibe un informe individual y confidencial, que incluye la puntuación obtenida en cada control evaluado y una justificación detallada, así como una comparativa frente a la media anónima del conjunto de participantes. Además, se elabora un informe global anonimizado que recoge tendencias, insights, brechas y buenas prácticas identificadas, sirviendo de base para la presentación pública en la Jornada Internacional de Seguridad de la Información. Finalmente, se proporciona un plan de mejora que recoge tanto **quick wins** como **recomendaciones** para el desarrollo de capacidades estructurales en personas, procesos, tecnología y modelos de sourcing.

La estructura de roles del ejercicio refleja la apuesta por la colaboración y la excelencia técnica. ISMS Forum actúa como organizador y promotor, liderando la dirección y coordinación global del ejercicio. Las entidades colaboradoras aportan recursos, conocimiento y visión sectorial, enriqueciendo el diseño y la ejecución del simulacro. El papel del evaluador, desempeñado por expertos independientes, garantiza la objetividad y el rigor en el análisis de los resultados. Finalmente, las entidades participantes asumen el reto de someter sus capacidades a evaluación, facilitando la interlocución y los medios necesarios para el desarrollo del ejercicio.

Esta dinámica colaborativa, basada en la confianza, la transparencia y el aprendizaje compartido, es la que permite que el Ejercicio de Crisis Cibernéticas trascienda el ámbito de la simulación para convertirse en una auténtica palanca de transformación y madurez para el ecosistema digital español.

Resultados 2025

El VI Ejercicio de Crisis Cibernéticas ha proporcionado una fotografía comparativa del grado de madurez y capacidad de respuesta de las organizaciones.

Articulándose en torno a un incidente reputacional con extorsión y fuga de información, inicialmente sin impacto tecnológico directo, pero con consecuencias económicas, legales y de imagen. Entre sus ingredientes: fake news, gestión de proveedores, presión mediática y social, extorsión a empleados, investigación/forense, robo de información sensible y procesos de notificación de violación de datos.

Fases del ejercicio

Fase 1
Preparación y diseño

Incluye sesión informativa y planificación (entrega de acuerdos firmados).

Fase 2
Ejecución

Ejecución del ejercicio de simulación.

Fase 3
Evaluación

Examen cualitativo (justificaciones, metodología) y cuantitativo (resultados gráficos).

Fase 4
Resultados

Presentación de resultados agregados y comparativa entre entidades en la Jornada Internacional.

Fase 5
Informes individuales

Presentación de informes individuales, con énfasis en las opciones de mejora.

Figura 1. Time line del proceso de ejecución del Ejercicio de Crisis Cibernéticas de 2025.

2

Modelo de gestión resiliente

Antes de analizar los resultados cuantitativos, es fundamental enmarcar el Ejercicio de Crisis Cibernéticas dentro de un marco conceptual sólido y adaptado a la realidad de las organizaciones españolas. El modelo de gestión resiliente que inspira la metodología de ISMS Forum parte de la necesidad de abordar la ciberresiliencia como un proceso integral, que va mucho más allá de la mera respuesta técnica ante incidentes. Este modelo ha sido desarrollado a partir de estándares internacionales y mejores prácticas, pero se ha enriquecido con la experiencia acumulada en el sector nacional, integrando dimensiones clave como la misión, la visión y los valores corporativos, el liderazgo, la cultura organizativa, la gestión del conocimiento y la mejora continua.

La adaptación de este modelo al contexto español responde a la diversidad sectorial, la madurez regulatoria y la importancia de la gestión del cambio en entornos complejos. Así, la pirámide que se presenta a continuación no solo sirve como referencia teórica, sino que constituye la base sobre la que se evalúan las capacidades de las organizaciones participantes y se diseñan los escenarios del simulacro, garantizando una aproximación holística y alineada con las necesidades reales del tejido empresarial y administrativo de nuestro país.

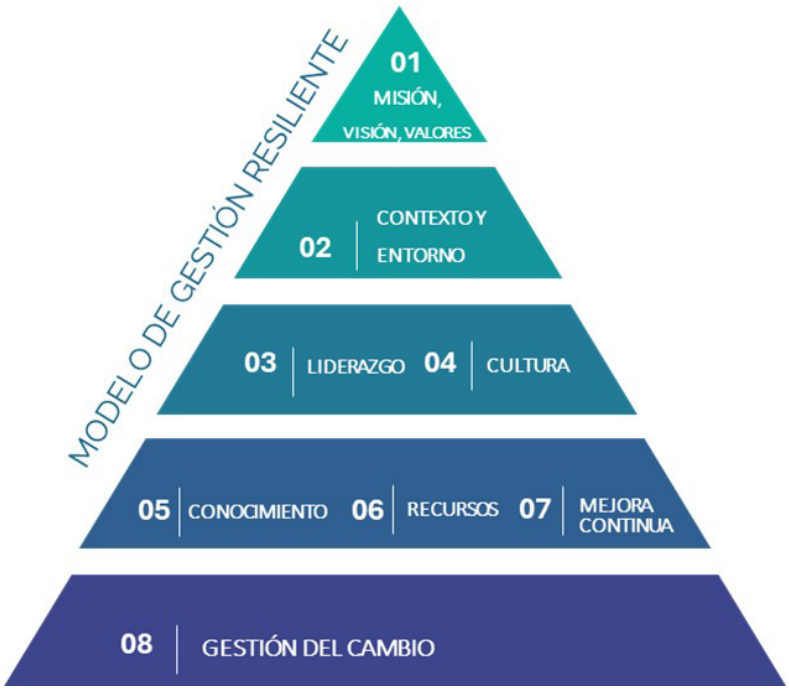


Figura 2. Modelo de gestión resiliente aplicado al Ejercicio de Crisis Cibernéticas.

3

Escenario detallado y puntos de decisión

La narrativa del caso avanza desde **señales inquietantes** (archivos que desaparecen/cifran en Finanzas) y **rumores** que se propagan por canales no oficiales (WhatsApp no corporativo), hasta la **confirmación de ransomware** y demandas de pago en **BTC**; se simula **presión mediática, colapso de canales (CAU) y tensión ejecutiva** con solicitud urgente de informe de situación al CISO. Se intercalan **preguntas de decisión** (p. ej., verificación de amenaza, activación de comités, grado de crisis, protocolo de evidencias, notificación a autoridades) y **ramas condicionales** (pago/no pago del rescate). El caso culmina con recuperación progresiva, **comunicación transparente y mejora continua.**

El ejercicio se ha parametrizado por **misiones y ámbitos** (comunicación y *stakeholders*, gestión de riesgos, planificación de trabajos operativos, organización y comité de crisis) con criterios **reglados por la calidad de las justificaciones y expresión gráfica** de resultados; se valora coherencia metodológica, referencia a procesos y grado de madurez en gestión de riesgos, respuesta a incidentes y uso del plan de comunicación

4

Síntesis de resultados y análisis comparativo

La evaluación de las respuestas se ha estructurado en cinco bloques fundamentales: actuación según los planes existentes, funcionamiento de los comités de gestión de crisis, respuesta operativa, comunicación con partes interesadas y gestión de herramientas y recursos.

La valoración de los resultados muestra una madurez homogénea, con puntuaciones medias que oscilan entre el 6,88 y el 7,26 sobre 10.

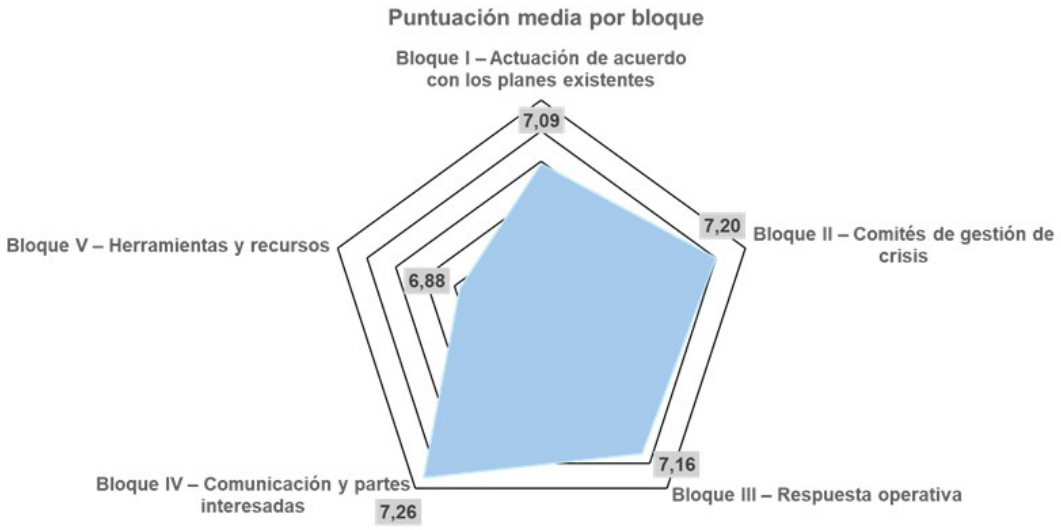


Figura 3. Visualización comparativa de la puntuación media obtenida por bloque de madurez en el Ejercicio de Crisis Cibernéticas

Este gráfico permite visualizar de forma clara las fortalezas y áreas de mejora del conjunto de participantes:

- **Comunicación y partes interesadas** destaca como el bloque mejor valorado, reflejando la importancia creciente de la transparencia y la proactividad en la gestión de crisis.
- **Comités de gestión de crisis y respuesta operativa** presentan también puntuaciones sólidas, evidenciando la consolidación de procedimientos y la capacidad de adaptación ante escenarios cambiantes.
- **Herramientas y recursos** es el bloque con mayor margen de mejora, especialmente en lo relativo a la integración de la gestión contractual y la priorización de recursos críticos.

5

Distribución de resultados por participante

La siguiente gráfica muestra la dispersión de resultados individuales, permitiendo identificar tanto la consistencia general del sector como la existencia de casos de éxito y áreas donde persisten retos relevantes.

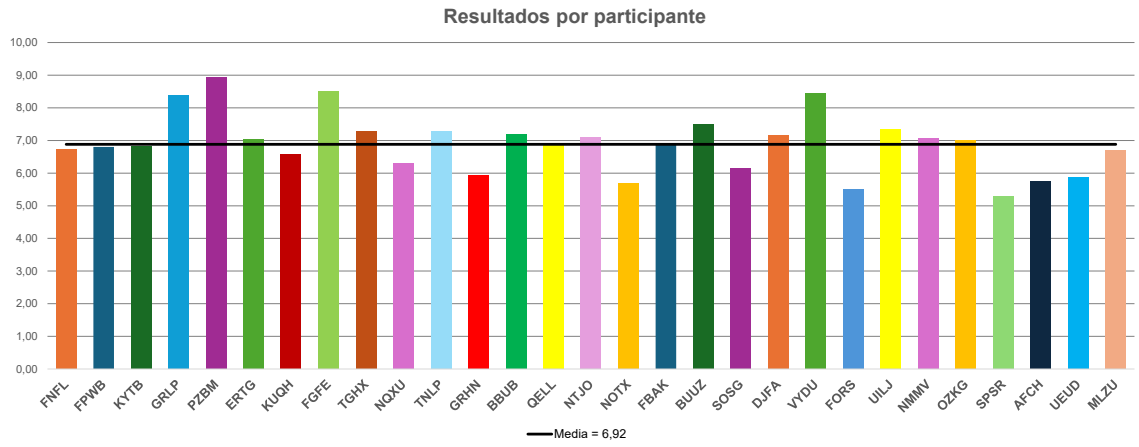


Figura 4. Distribución de puntuaciones individuales (anonimizadas) por participante.

La mayoría de las organizaciones se sitúan en torno a la media global, lo que evidencia una madurez sectorial creciente y una asimilación progresiva de las mejores prácticas. No obstante, la dispersión observada invita a seguir trabajando en la personalización de los planes de mejora y en el refuerzo de las capacidades menos desarrolladas.

6

Principales aprendizajes y recomendaciones

A partir del análisis de los resultados, se identifican los siguientes aprendizajes clave:

- La **existencia de planes y playbooks específicos** para ciberincidentes es ya una realidad en la mayoría de las entidades, aunque se recomienda contemplar escenarios donde los RTO no puedan cumplirse.
- Los comités de gestión de crisis funcionan de manera eficaz, pero es necesario justificar la presencia de **perfiles no permanentes y reforzar la gobernanza post-crisis.**
- La respuesta operativa destaca por su capacidad de adaptación y la integración de herramientas como el **análisis forense** y los **ciberseguros**.
- La comunicación con autoridades y partes interesadas es proactiva, aunque debe mejorarse la **justificación de la frecuencia y la política de transparencia**.
- La gestión de herramientas y recursos requiere una **mayor claridad en los criterios de fiabilidad y una mejor integración de la capa contractual** en los planes de crisis.

Recomendaciones prioritarias:

1. Actualizar playbooks con escenarios de estrés en los RTO.
2. Revisar la composición y criterios de activación de los comités de crisis.
3. Completar el catálogo de herramientas con fichas de propósito y fiabilidad.
4. Integrar cláusulas contractuales y OLAs de terceros críticos en los planes de crisis.
5. Establecer métricas de cierre de lecciones aprendidas y auditoría interna post-ejercicio.

Reflexión Final

El ejercicio confirma que la resiliencia no es un estado, sino un proceso dinámico de adaptación y mejora continua. La consolidación de una comunidad que practica el intercambio de experiencias y la sistematización de la evaluación permiten avanzar hacia un ecosistema digital más robusto, preparado para afrontar los desafíos presentes y futuros.

Próximos pasos

El Ejercicio de Crisis Cibernéticas de ISMS Forum ha demostrado, edición tras edición, su valor como herramienta de aprendizaje, benchmarking y mejora continua para las organizaciones comprometidas con la ciberresiliencia.

¿Quieres formar parte de la próxima edición?

Invitamos a todas las entidades, públicas y privadas, que deseen fortalecer sus capacidades de gestión de crisis cibernéticas y contribuir al desarrollo de la resiliencia sectorial, a sumarse a la siguiente convocatoria. Participar en el Ejercicio de Crisis Cibernéticas es una oportunidad única para:

- Validar y mejorar los procedimientos internos ante incidentes reales.
- Compararse de forma anónima con otras organizaciones del sector.
- Acceder a recomendaciones personalizadas y planes de mejora.
- Contribuir activamente a la construcción de un estándar de referencia en ciberresiliencia.
- Para más información sobre el proceso de inscripción, requisitos de participación o cualquier consulta adicional, puedes contactar con el equipo de ISMS Forum a través de ***cibercrisis@ismsforum.es*** o visitar nuestra web oficial.

¡Te esperamos en la próxima edición de 2026 para seguir construyendo juntos un entorno digital más seguro y resiliente!

isms forum

VII
CYBER CRISIS *MANAGEMENT*

REVISIÓN
Beatriz García

DISEÑO Y MAQUETACIÓN
Susana Marín

CRC
CYBER RESILIENCE CENTRE