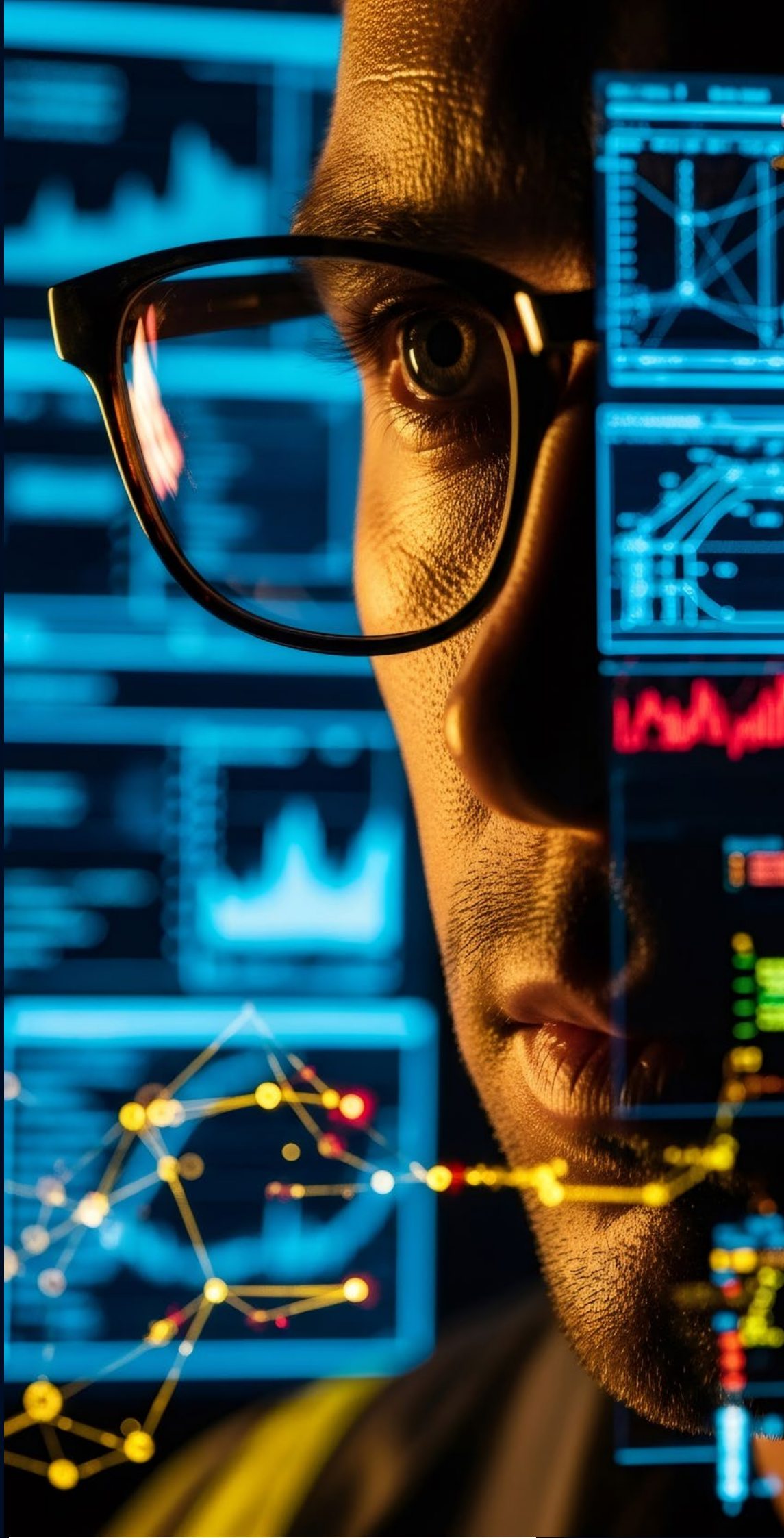
isms forum

CSC
CYBER SECURITY CENTRE

XIV Edición

CYBER MS 26



Edición

Beatriz García

Maquetación y diseño

Susana Marín

Agradecimientos

Queremos expresar nuestro más sincero agradecimiento a todas las organizaciones que han participado en la edición 2026 de los Ciberejercicios Multisectoriales (CyberMS26). Su compromiso, disponibilidad y vocación de mejora continua constituyen la base sobre la que se construye este proyecto, permitiendo avanzar de forma tangible en la madurez y resiliencia del ecosistema de ciberseguridad.

Agradecemos especialmente a INCIBE, por su papel como anfitrión en la presentación de la iniciativa, así como por su apoyo constante al impulso de ejercicios que permiten poner a prueba, de forma controlada y rigurosa, las capacidades reales de las organizaciones frente a ciberamenazas. Su implicación refuerza el valor público y estratégico de este tipo de ejercicios como instrumento de mejora colectiva.

Nuestro reconocimiento se extiende igualmente a las entidades que han participado como atacantes y evaluadores, cuyo nivel técnico, profesionalidad y dedicación han sido clave para garantizar el rigor metodológico y la calidad de los resultados obtenidos. En particular, queremos destacar la contribución de: Accenture, Deloitte, Infoblox, Picus Security y Mastercard.

Su aportación, basada en conocimiento especializado, herramientas avanzadas y experiencia práctica, permite trasladar al ejercicio escenarios realistas y métricas objetivas, alineadas con los principales estándares y marcos regulatorios internacionales.

Contenido

Resumen Ejecutivo

El presente documento recoge la justificación, el alcance y los principales resultados del programa anual de la **XIV Edición de Ciberejercicios Multisectoriales**, organizado por ISMS Forum en colaboración con entidades públicas y privadas de referencia.

La iniciativa se articula mediante la ejecución de **pruebas técnicas especializadas** sobre distintos vectores de ataque, permitiendo estructurar la evaluación de la postura de ciberseguridad de las organizaciones participantes. A través de este enfoque, se analizan capacidades clave como la gestión de identidades, la resiliencia frente a amenazas DNS, la eficacia de los controles de seguridad y la exposición al riesgo en la cadena de suministro.

Los resultados, agregados y anonimizados, ofrecen una **visión comparativa del nivel de madurez**, identificando fortalezas y áreas de mejora. La continuidad del ejercicio permite, además, seguir la evolución del ecosistema y consolidar buenas prácticas.

Los principales resultados de esta edición han sido presentados en el marco del **XV Foro de la Ciberseguridad de ISMS Forum**[1], consolidando este evento como punto de encuentro para la puesta en común de aprendizajes y tendencias del sector.

Desde el punto de vista regulatorio, CyberMS contribuye a evidenciar la diligencia debida en materia de ciberseguridad, alineándose con marcos como **NIS2, DORA y estándares internacionales**, que requieren la validación periódica de capacidades de detección y respuesta.

En un entorno caracterizado por la creciente sofisticación de las amenazas, este ejercicio se consolida como una herramienta clave para **evaluar, comparar y mejorar de forma continua la resiliencia técnica de las organizaciones.**

[1] https://www.ismsforum.es/evento/798/xv-foro-de-la-ciberseguridad/

Contexto y justificación

El entorno digital actual está marcado por una creciente complejidad tecnológica y por un incremento sostenido en la sofisticación de las amenazas cibernéticas. Los vectores de ataque han evolucionado hacia modelos más avanzados que combinan técnicas como la explotación de identidades, la exfiltración de datos mediante DNS, el uso de malware sofisticado y los ataques dirigidos a la cadena de suministro.

En este contexto, las organizaciones requieren ir más allá de modelos teóricos o auditorías estáticas, incorporando mecanismos que permitan **validar de forma práctica la eficacia real de sus controles de seguridad.** La evidencia demuestra que muchas de las brechas críticas solo se identifican cuando los sistemas son sometidos a escenarios reales de ataque.

Los ciberejercicios multisectoriales surgen como respuesta a esta necesidad, proporcionando un entorno controlado en el que es posible reproducir comportamientos de adversarios reales y evaluar la capacidad de las organizaciones para detectar, contener y responder ante incidentes.

Asimismo, el contexto regulatorio europeo, con la entrada en vigor de normativas como **NIS2 y DORA**, refuerza la necesidad de realizar pruebas periódicas que permitan evidenciar la eficacia de los mecanismos de seguridad implantados. En este sentido, iniciativas como CyberMS no solo aportan valor operativo, sino que se configuran como instrumentos de apoyo al cumplimiento.

La presentación de los resultados en el **XV Foro de la Ciberseguridad** refuerza, además, la dimensión colaborativa del proyecto, permitiendo compartir aprendizajes de forma agregada y contribuir a la mejora del conjunto del ecosistema.

En definitiva, la iniciativa responde a una doble necesidad de **reforzar la resiliencia técnica real de las organizaciones y generar conocimiento compartido** que eleve el nivel de madurez sectorial.

Alcance, objetivos, metodología y modelo de gobierno

1 Alcance

El programa CyberMS 2026 se orienta a la evaluación técnica de las capacidades de ciberseguridad de las organizaciones participantes, cubriendo los principales dominios del ciclo de seguridad:

- Gestión de identidades
- Protección en red y endpoint
- Resiliencia frente a amenazas DNS
- Análisis de superficie de ataque externa
- Evaluación del riesgo en la cadena de suministro

Las pruebas están diseñadas para ser aplicables a múltiples sectores, garantizando la comparabilidad de resultados y la consistencia metodológica.

2 Objetivos

El ejercicio persigue los siguientes objetivos:

- Evaluar la eficacia real de los controles de seguridad
- Medir capacidades de detección, análisis y respuesta
- Identificar vulnerabilidades técnicas específicas
- Proporcionar una visión comparativa sectorial
- Impulsar la capacidad operativa de ciberseguridad mediante recomendaciones prácticas

La metodología del CyberMS 2026 se basa en un enfoque estructurado que permite evaluar de forma objetiva y comparable la postura de ciberseguridad de las organizaciones participantes, desde la ejecución de pruebas hasta la obtención de resultados agregados y su posterior análisis.

Este proceso se articula en una secuencia de fases claramente definidas:

Pruebas llevadas a cabo por los atacantes

- Prueba 1: Gestión de Identidades
- Prueba 2: Security Resilience - DNS Security
- Prueba 3: BAS. Simula ataques reales sobre la infraestructura de red y endpoint.
- Prueba 4: RiskRecon + CyberQuant

Recopilación y análisis de resultados por atacante

Cada atacante recopilará los resultados de las pruebas realizadas,.

Evaluación de resultados

Evaluación de resultados aplicando criterios de valoración basados en NIST CSF 2.0.

Nivel de Madurez en ciberseguridad

Este nivel de madurez hará referencia únicamente a aquellas funciones NIST CSF 2.0 y sistemas/activos que tengan relación con los ejercicios planteados y no pretende mostrar, en ningún caso, un nivel de madurez general de la organización.

Resultados y comparativa

Se realizará inicialmente una presentación de resultados globales, para continuar luego de la realización de ajustes de resultados con la entrega de resultados individualizados.

Como se muestra en la figura, el modelo parte de la ejecución de pruebas técnicas especializadas, continúa con la recopilación y análisis de resultados por parte de los distintos atacantes, y culmina en una evaluación estructurada que permite determinar el nivel de madurez de las organizaciones y generar una comparativa anonimizada.

Este enfoque garantiza que los resultados no se limiten a una visión puntual, sino que se integren en un modelo de evaluación homogéneo, repetible y orientado a la mejora continua.

3 Metodología

Marco de referencia (NIST CSF 2.0)

La evaluación de los resultados se realiza conforme a los principios del NIST Cybersecurity Framework (CSF) 2.0, que permite estructurar el análisis en torno a las principales funciones de ciberseguridad:

La adopción del NIST CSF 2.0 como marco de referencia permite asegurar una evaluación integral, alineada con estándares internacionales y con los principales requisitos regulatorios. Este enfoque facilita, además, la comparabilidad de resultados entre organizaciones y la identificación de áreas de mejora desde una perspectiva estructurada.

3 Metodología

Modelo de evaluación

Cada una de las pruebas ejecutadas aporta una valoración independiente sobre distintos vectores de ataque. Estas valoraciones se normalizan en una escala común (0–10), lo que permite:

- obtener una nota global agregada
- realizar una comparativa sectorial homogénea
- identificar brechas por dominios NIST **(Govern, Identify, Protect, Detect, Respond y Recover)**

Asimismo, el modelo incorpora una fase específica orientada a la determinación del nivel de madurez, centrada exclusivamente en aquellas capacidades evaluadas durante el ejercicio, evitando extrapolaciones no fundamentadas sobre el conjunto de la organización.

Valor diferencial del enfoque

La combinación de un flujo metodológico estructurado con un marco de referencia internacional permite que CyberMS se posicione como un modelo:

- objetivo y basado en evidencia técnica
- comparable entre organizaciones y sectores
- alineado con NIS2, DORA y estándares internacionales
- orientado a la postura de seguridad y a la toma de decisiones

3 Metodología

4 Modelo de Gobierno

El modelo de gobierno del ejercicio se estructura en los siguientes roles:

- ISMS Forum (organizador): dirección, coordinación y supervisión del proyecto
- Entidades colaboradoras: aportación de capacidades técnicas y ejecución de pruebas
- Evaluador: análisis objetivo de resultados
- Entidades participantes: ejecución y validación de sus capacidades

El proceso se rige por una estricta política de confidencialidad que garantiza que:

- los resultados individuales son confidenciales
- las comparativas se presentan de forma anonimizada
- la información sensible se gestiona de forma controlada

La posterior presentación de resultados en el Foro de la Ciberseguridad permite trasladar conclusiones agregadas al conjunto del sector, reforzando el valor del ejercicio como herramienta de mejora colectiva.

Resultados 2026

El programa CyberMS 2026 ha permitido obtener una visión consolidada del nivel de madurez técnica de las organizaciones participantes, a partir de la evaluación práctica de sus capacidades frente a distintos vectores de ataque.

A diferencia de otros ejercicios centrados en la gestión organizativa de crisis, CyberMS se articula en torno a la ejecución de pruebas técnicas especializadas, diseñadas para simular comportamientos reales de adversarios y evaluar la eficacia de los controles implantados en entornos productivos.

El ejercicio ha permitido analizar, de forma homogénea y comparable, capacidades clave como:

- la gestión de identidades y accesos
- la resiliencia frente a amenazas DNS
- la eficacia de los controles de prevención y detección en infraestructuras
- la exposición externa y el riesgo asociado a la cadena de suministro

Los resultados obtenidos reflejan un nivel de madurez general sólido, con diferencias significativas entre organizaciones en determinados vectores, especialmente en capacidades de detección y visibilidad, así como en la gestión de amenazas emergentes.

El carácter agregado y anonimizado de los resultados ha permitido generar una visión comparativa, identificando tendencias comunes, fortalezas consolidadas y áreas prioritarias de mejora.

Pruebas

El ejercicio se ha articulado en torno a cuatro pruebas principales, cada una enfocada a un vector de ataque específico:

Prueba 1:
Gestión de Identidades Digitales

Esta prueba evalúa la capacidad de las organizaciones para gestionar el ciclo de vida de las identidades y detectar comportamientos anómalos en entornos complejos.

Permite analizar:

- gobernanza de accesos
- detección de anomalías en cuentas
- capacidad de respuesta ante incidentes de identidad

Prueba 2:
Resiliencia DNS y amenazas asociadas

Se centra en la evaluación de los controles de seguridad DNS frente a amenazas avanzadas.

Incluye:

- detección de dominios maliciosos
- exfiltración e infiltración de datos vía DNS
- monitorización de dominios fraudulentos
- análisis de superficie de ataque externa

Esta prueba es especialmente relevante por el creciente uso del DNS como vector de ataque.

Prueba 3:
Simulación de ataques (BAS – Breach & Attack Simulation)

Evalúa la eficacia real de los controles de seguridad mediante la simulación de ataques sobre red y endpoint.

Permite medir:

- capacidad de prevención (bloqueo de amenazas)
- capacidad de detección (alertas y visibilidad)
- cobertura frente a técnicas MITRE ATT&CK

Aporta una visión objetiva de la seguridad efectiva, más allá de configuraciones declarativas.

Prueba 4:
Superficie de ataque y riesgo cuantificado

Analiza la exposición externa de la organización y cuantifica el riesgo cibernético en términos de impacto.

Incluye:

- análisis OSINT de la superficie de ataque
- evaluación de configuraciones de seguridad
- valoración del riesgo financiero
- análisis de la seguridad de proveedores críticos

Esta prueba incorpora una dimensión diferencial:
la evaluación de la cadena de suministro.

Resultados: modelo de reporting y outputs entregados

El programa CyberMS 2026 no se limita a la ejecución de pruebas técnicas, sino que proporciona a las organizaciones participantes un modelo estructurado de resultados, diseñado para transformar la evaluación técnica en información accionable y comparable.

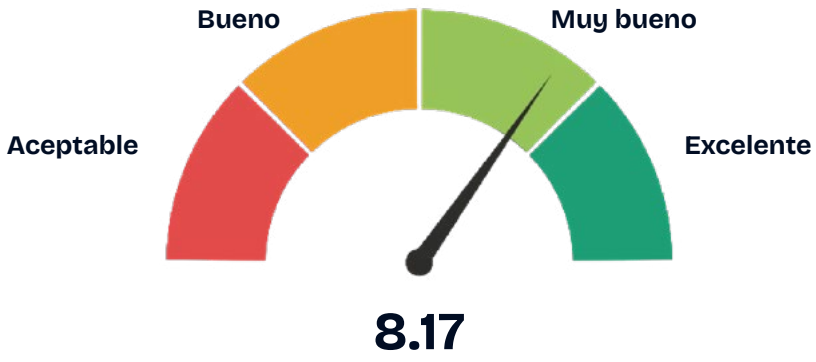
Cada entidad participante recibe un informe individual confidencial, complementado con una visión comparativa frente al conjunto del grupo, permitiendo situar su nivel de madurez en el contexto sectorial.

Estructura de resultados

Los resultados se presentan a las organizaciones en tres niveles principales:

1. Evaluación global de la madurez

Cada organización obtiene una puntuación global normalizada (0–10), que sintetiza el resultado agregado de las pruebas realizadas.

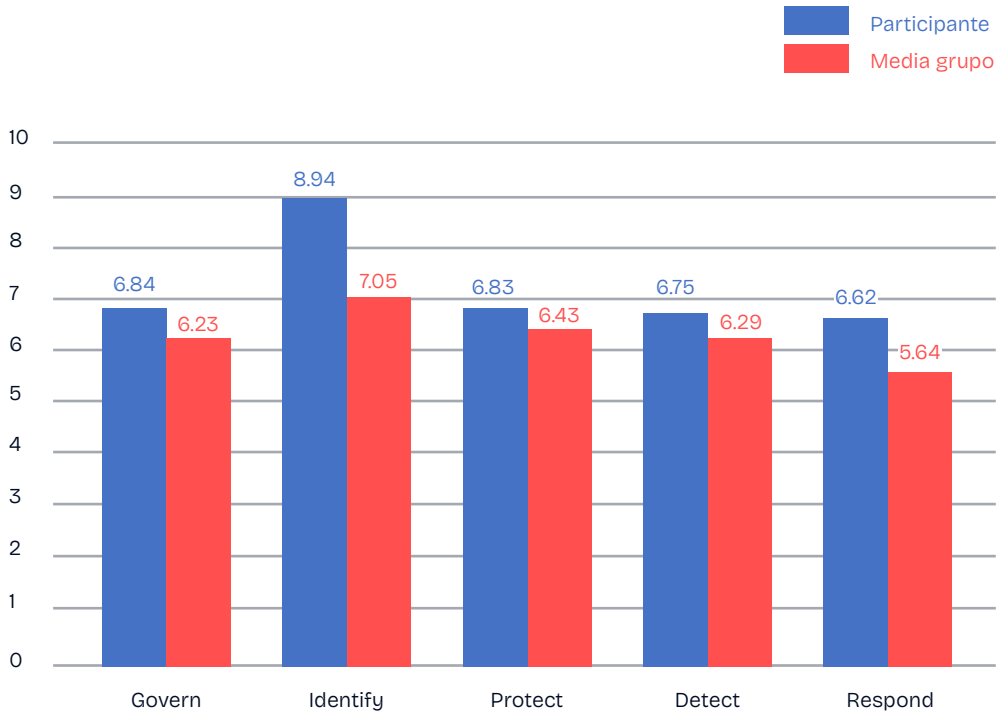


Este indicador permite:

- obtener una visión rápida del nivel global de ciberseguridad
- posicionarse dentro de una categoría (Aceptable, Bueno, Muy Bueno, Excelente)
- facilitar la comunicación con dirección y comités de gobierno

2. Evaluación por dominios NIST (NIST CSF 2.0)

Los resultados se descomponen en las principales funciones del modelo NIST:



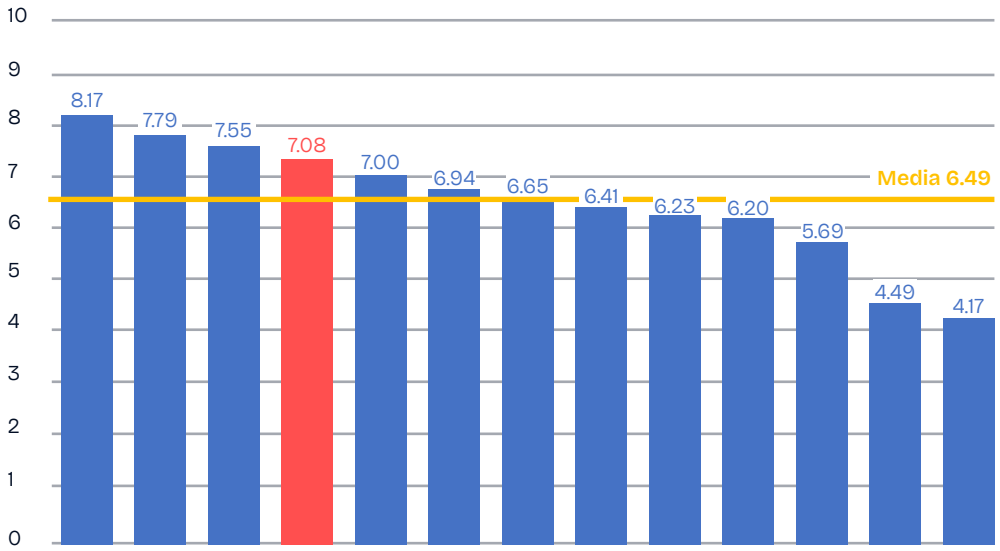
Esta representación permite:

- comparar el desempeño de la organización frente a la media del grupo
- identificar fortalezas relativas
- detectar brechas específicas por dominio

3. Detalle de resultados por prueba y dominio

El informe incluye una descomposición completa de los resultados por prueba, vinculándolos directamente con las funciones NIST evaluadas.

	Govern	Identify	Protect	Detect	Respond	Recover
Prueba 1	6.17	9.17	7.33	7.10	8.25	N/A
Prueba 2	7.75	8.25	3.09	4.98	5.00	N/A
Prueba 3	N/A	N/A	8.90	5.50	N/A	N/A
Prueba 4	6.60	9.40	8.00	9.40	N/A	N/A
Organización	**6.84**	**8.94**	**6.83**	**6.75**	**6.62**	**N/A**
Media participantes	**6.23**	**7.05**	**6.43**	**6.29**	**5.64**	**N/A**



Comparativa de los resultados globales obtenidos por las empresas participantes en el ejercicio

Esto permite:

- entender el origen de cada puntuación
- identificar qué pruebas impactan en cada dominio
- analizar con precisión las capacidades técnicas evaluadas

Principales aprendizajes y recomendaciones

A partir del análisis de los resultados obtenidos en el CyberMS 2026, se identifican una serie de aprendizajes clave que permiten orientar la evolución de las capacidades de ciberseguridad en las organizaciones participantes.

Principales aprendizajes

- **La prevención ya no es suficiente como indicador de madurez**. Aunque la mayoría de organizaciones presentan buenos niveles de protección, el ejercicio evidencia que la capacidad de detección y visibilidad sigue siendo el principal reto, especialmente en entornos de red.
- **Persisten brechas en la detección de amenazas avanzadas.** Técnicas asociadas a exfiltración DNS, ejecución de malware o actividad lateral no siempre generan la visibilidad necesaria, lo que limita la capacidad de respuesta temprana.
- **La identidad digital se consolida como vector crítico de riesgo.** La gestión de identidades muestra niveles elevados de madurez en general, pero continúa siendo un punto clave de exposición si no se monitoriza de forma continua.
- **El DNS emerge como un área prioritaria de mejora.** La creciente utilización de este canal como vector de ataque exige reforzar las capacidades de inspección, análisis y control, especialmente en entornos cifrados (DoH/DoT).
- **La cadena de suministro sigue siendo un factor de incertidumbre.** La variabilidad en la postura de seguridad de proveedores confirma la necesidad de integrar su evaluación dentro del modelo de gestión del riesgo.

Recomendaciones prioritarias

A partir de los resultados del ejercicio, se proponen las siguientes líneas de actuación:

- **Reforzar las capacidades de detección y monitorización.** Implantar soluciones que permitan obtener visibilidad en tiempo real (NDR, SIEM avanzado, correlación de eventos).
- **Evolucionar hacia modelos de seguridad basados en comportamiento.** Incorporar capacidades de detección de anomalías y técnicas asociadas a MITRE ATT&CK.
- **Fortalecer la seguridad en entornos DNS.** Integrar inteligencia de amenazas, mecanismos de inspección y protección frente a exfiltración de datos.
- **Consolidar la gobernanza de identidades.** Complementar los modelos existentes con capacidades de monitorización continua y validación periódica.
- **Integrar la gestión de terceros en el modelo de ciberseguridad.** Establecer mecanismos de evaluación continua de proveedores críticos y definir criterios de aceptación de riesgo.
- **Adoptar un enfoque continuo de validación de controles.** Incorporar ejercicios periódicos que permitan verificar la eficacia real de los sistemas de seguridad implantados.

La ciberseguridad no debe medirse únicamente por la existencia de controles, sino por la capacidad de detectar, analizar y responder de forma efectiva a las amenazas.

Próximos pasos

El programa CyberMS se consolida como una herramienta estratégica dentro del ecosistema de ISMS Forum, con un enfoque orientado a la mejora continua y a la generación de valor tanto para las organizaciones participantes como para el conjunto del sector.

¿Quieres formar parte de la próxima edición?

Invitamos a todas las entidades, públicas y privadas, que deseen evaluar y fortalecer sus capacidades técnicas de ciberseguridad y contribuir al desarrollo de la resiliencia sectorial, a sumarse a la próxima edición de los Ciberejercicios Multisectoriales 2027.

Participar en CyberMS es una oportunidad única para:

- Validar la eficacia real de los controles de seguridad frente a escenarios de ataque basados en técnicas reales.
- Medir el nivel de madurez técnica de la organización mediante un modelo objetivo y comparable.
- Compararse de forma anonimizada con otras organizaciones, obteniendo una referencia clara de posicionamiento sectorial.
- Identificar vulnerabilidades y brechas específicas, con impacto directo en la mejora de la postura de seguridad.
- Acceder a recomendaciones personalizadas y planes de mejora, basados en evidencias técnicas.
- Contribuir activamente al desarrollo de buenas prácticas en ciberseguridad a nivel multisectorial.

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 proyectos@ismsforum.es o visitar nuestra web oficial.

Te esperamos en la próxima edición de 2027 para seguir evaluando, mejorando y construyendo juntos un ecosistema digital más seguro y resiliente.

isms forum

CSC
CYBER SECURITY CENTRE

XIV Edición

CYBER MS 26