

“El futuro de la ciberdefensa y la confianza digital”

18 de noviembre de 2026 – Espacio Dobble (Serrano Anguita, 14. Madrid)

Café y recepción: 9.00h - Desarrollo de la mesa: 9.30 a 11:30h

El contexto actual, marcado por un aumento de los ciberataques dirigidos a infraestructuras críticas, el uso geopolítico del ciberespacio y la expansión de tecnologías disruptivas como la inteligencia artificial o la computación cuántica redefine los límites de la seguridad. Las fronteras físicas se diluyen y los conflictos híbridos se libran también en entornos digitales, donde la desinformación, el espionaje y el sabotaje tecnológico son armas estratégicas.

Asimismo, ante la disolución del perímetro tradicional de ciberseguridad y la disrupción que ha supuesto la llegada de la inteligencia artificial, el foco de la ciberseguridad se ha ido desplazando poco a poco de la protección lógica como tal a la capacidad de resiliencia. El espectro de la ciberseguridad y la ciberdefensa es cada vez más amplio, abarcando desde la detección temprana automatizada hasta la capacidad de recuperación tras un incidente.

Las normativas europeas continúan evolucionando en paralelo al sector de la ciberseguridad, ofreciendo palancas que impulsan la capacidad de protección colectiva.

En este contexto de constante cambio en el panorama de la ciberseguridad, de evolución de las tecnologías que impulsan este sector y de nuevos planteamientos normativos, toca rearmarse. Este observatorio IT Digital Security, "El futuro de la ciberdefensa y la confianza digital", tomará el pulso al sector. Un sector, además, expuesto tanto a importantes iniciativas gubernamentales como al impacto de la compleja situación geopolítica internacional.

OBSERVATORIOS ITDS

Estos observatorios consisten en mesas redondas en las que 6-8 responsables de IT y seguridad, junto con proveedores de soluciones de ciberseguridad, analizarán las prácticas llevadas a cabo por las organizaciones en su tarea de proteger los activos

digitales de la empresa. El objetivo es el fomento del networking y el conocimiento del mercado.

Los observatorios tendrán una duración de dos horas. Las conclusiones se recogerán en un documento específico que se publicará en IT Digital Security y habrá un extenso reportaje en el número de diciembre de nuestra revista IT Digital Magazine.

Además de contenido escrito, se hará un vídeo resumen, con imágenes de la celebración, pero sin declaraciones de los participantes durante el transcurso de la mesa, para dejar total libertad de expresión. **Sí se solicitará a los participantes la respuesta posterior a cámara de una pregunta, que se fijará anteriormente, sobre lo tratado en la mesa.** También realizaremos alguna entrevista a los ponentes a lo largo de la jornada; necesitaríamos saber si está interesado en la posibilidad de entrevista.

El futuro de la ciberdefensa y la confianza digital (9.30-11.30)

Ante la evidencia de un volumen siempre creciente de ciberamenazas, cada vez es mayor la necesidad de hacer un frente común frente a los ciberataques, además de potenciar la capacidad de recuperación tras un incidente. Se parte de la premisa de Zero Trust como política de protección, pero también nos encaminamos hacia ecosistemas de confianza.

- Frente a los ataques de deepfake que apuntan a la dirección empresarial o a transacciones sensibles, ¿qué controles tecnológicos y de proceso se están implementando para verificar la autenticidad de las comunicaciones?
- Más allá de la prevención, ¿cómo de preparada están realmente las organizaciones para recuperar operaciones tras un ataque de ransomware?
- ¿En qué punto se encuentra la transición desde el acceso remoto basado en VPN hacia modelos Zero Trust Network Access? ¿Cuáles han sido los mayores obstáculos —técnicos, presupuestarios o de cultura interna— para acelerar esa migración?
- Con la entrada en vigor de NIS2 y la creciente presión regulatoria europea, ¿cómo se está abordando la protección de entornos OT/infraestructura crítica?
- ¿Está la soberanía digital —dónde y con qué proveedores se procesan y protegen los datos— entrando ya en los criterios de decisión tecnológica?
- Si hubiera que priorizar una sola inversión en los próximos 12 meses entre resiliencia de datos, control de accesos/Zero Trust o protección de infraestructura crítica, ¿cuál sería y por qué? ¿Dónde está hoy el eslabón más débil de la confianza digital en las organizaciones?

PROGRAMA AUDIOVISUAL IT TELEVISIÓN

Como parte de esta actividad destinada a fomentar el conocimiento del mercado e iniciativas de ciberseguridad, se grabará un programa audiovisual que se emitirá el día 2 de diciembre de 2026, con entrevistas y ponencias. Por ello se ofrece a los participantes de los Observatorios la **posibilidad de realizarles una entrevista individual** para dicho programa audiovisual. Estas intervenciones se grabarán posteriormente en una sala paralela el mismo día del Observatorio (18 de noviembre). Si está interesado en ser entrevistado, háganoslo saber para cerrar contenido y tiempo de grabación.

Esperamos que le resulte interesante participar en nuestro Observatorio IT Digital Security y podamos contar con su participación como experto en tecnología y ciberseguridad. Por favor, indíquenos si podemos gestionar directamente la intervención con usted o si es con su departamento de comunicación.

Muchas gracias por su interés.

Atentamente,

[Arancha Asenjo](#)

Directora eventos #ComunidadIT
IT Digital Media Group

[Rafa M. Claudín](#)

Redactor jefe IT Digital Security
IT Digital Media Group

Notas:

- La participación en este encuentro implica la compartición de sus datos (nombre, cargo, empresa, teléfono y dirección de email) con los patrocinadores de su mesa (SonicWall, Stormshield, Veeam).

[IT Digital Security](#) es una publicación de la editorial IT Digital Media Group orientada a CIO, CISO y responsables de seguridad de las empresas, que proporciona información relacionada con el estado de la ciberseguridad, mejores prácticas para la protección de las empresas y soluciones tecnológicas. Mantiene la filosofía del grupo de presentar una propuesta cien por cien digital, en la que los contenidos audiovisuales tienen un papel preponderante.