



AMCS
Alianza México Ciberseguro



Anáhuac
México

3^{ER} FORO NACIONAL DE CIBERSEGURIDAD

#AMCS2026

**Colaboración multisectorial para un
entorno digital seguro, resiliente y con derechos**

**Convocatoria, bases generales
y calendario de referencia**



Convocatoria

La Alianza México CiberSeguro convoca a personas, instituciones públicas, empresas, academia, organizaciones de la sociedad civil, comunidades técnicas, medios de comunicación, unidades especializadas e iniciativas nacionales e internacionales a participar en los **Premios AMCS 2026**.

Estos premios buscan visibilizar contribuciones relevantes para fortalecer la ciberseguridad, la confianza digital, la prevención de riesgos, la formación de talento, la innovación tecnológica, la cooperación multisectorial y el uso responsable de tecnologías emergentes.

Se reconocen prácticas, trayectorias, proyectos e iniciativas con impacto verificable en México, América Latina o en el ecosistema digital internacional, desde una perspectiva de seguridad, resiliencia, ética, derechos, inclusión, colaboración y mejora continua.

Categorías 2026

#	Categoría	Dirigido a	Se evaluará
1	Trayectoria profesional en ciberseguridad	Personas con una contribución sostenida al desarrollo, la protección y el impulso de la ciberseguridad.	Trayectoria, liderazgo, ética, contribución al ecosistema, formación de talento e impacto nacional, regional o sectorial.
2	Comunicación, periodismo y divulgación en ciberseguridad	Periodistas, comunicadores, medios o iniciativas de divulgación que informen, eduquen y promuevan una cultura de seguridad digital.	Rigor, claridad, alcance, responsabilidad informativa, impacto social y contribución a la prevención.
3	Buenas prácticas organizacionales en ciberseguridad	Organizaciones públicas, privadas, académicas o sociales con prácticas implementadas, verificables y replicables.	Pertinencia frente al riesgo, impacto, gobernanza, mejora continua, protección de derechos y sostenibilidad.
4	Policías cibernéticas y unidades de prevención del ciberdelito	Unidades o instituciones que destaquen en prevención, orientación, atención ciudadana, investigación y coordinación institucional.	Impacto en la prevención, la profesionalización, los protocolos, la colaboración interinstitucional, la protección de las víctimas y los resultados verificables.
5	Formación de talento y profesionalización	Instituciones, programas, academias, comunidades o iniciativas que impulsen la capacitación, el desarrollo de competencias, la mentoría, la certificación, la inclusión y el desarrollo del talento.	Calidad del programa, impacto, inclusión, vinculación con el ecosistema, sostenibilidad y evaluación de resultados.
6	Políticas públicas, gobernanza y cooperación multisectorial	Instituciones o iniciativas que impulsen estrategias, marcos de gobernanza, políticas, consultas, estándares, así como la cooperación o la coordinación entre sectores.	Relevancia pública, calidad técnica o institucional, participación multisectorial, impacto, transparencia y sostenibilidad.



#	Categoría	Dirigido a	Se evaluará
7	Cooperación internacional para un ciberespacio seguro	Personas, organizaciones, redes, organismos internacionales o iniciativas regionales con impacto en México, en América Latina o en comunidades hispanohablantes.	Cooperación, transferencia de conocimiento, generación de capacidades, resiliencia, colaboración transfronteriza e impacto verificable.
8	Investigación, innovación tecnológica e inteligencia artificial aplicada a la ciberseguridad	Investigadores, equipos, laboratorios, empresas, startups, comunidades o proyectos que desarrollen, implementen o transfieran soluciones innovadoras para fortalecer la ciberseguridad, incluidas herramientas, metodologías, prototipos, tecnologías emergentes o aplicaciones de inteligencia artificial responsables.	Originalidad, innovación técnica, rigor metodológico, pertinencia del problema abordado, validación, impacto medible, seguridad, privacidad, gobernanza, escalabilidad, potencial de adopción y evidencia de resultados.

Periodo de postulaciones

Las postulaciones estarán abiertas durante el periodo de registro establecido en la convocatoria.

Calendario de referencia 2026

Fase	Periodo de referencia
Publicación de convocatoria	20 de julio de 2026
Registro de postulaciones	Del 20 de julio al 21 de agosto de 2026
Cierre de registro	7 de septiembre de 2026
Validación documental	24 de agosto al 8 de septiembre de 2026
Evaluación	9 al 21 de septiembre de 2026
Deliberación y notificación de resultados	21-24 de septiembre de 2026
Ceremonia de premiación	9 de octubre de 2026
Publicación de la memoria	Noviembre de 2026

Proceso de postulación



Criterios generales de evaluación

El proceso considerará criterios de verificabilidad, pertinencia, impacto, ética e integridad, inclusión, replicabilidad y sostenibilidad. La valoración se realizará con base en la información presentada y en la evidencia documental disponible.

Criterio	Descripción operativa
Verificabilidad	La evidencia permite confirmar la existencia, el alcance, los resultados y la autoría de la contribución.
Pertinencia	La contribución aborda un problema o una necesidad relevante del ecosistema de ciberseguridad.
Impacto	Existen resultados, beneficios, productos, cambios o efectos observables.
Ética e integridad	La contribución respeta los derechos, evita conflictos de interés y promueve prácticas responsables.
Inclusión	La iniciativa considera la diversidad, la accesibilidad, la reducción de brechas o el beneficio social.
Replicabilidad	El modelo, la práctica o la experiencia pueden adoptarse, adaptarse o transferirse.
Sostenibilidad	Cuenta con continuidad, gobernanza, recursos, aprendizaje y mejora continua.



Alcance del reconocimiento

El reconocimiento no constituye certificación, acreditación, auditoría, validación técnica exhaustiva, aval comercial ni declaración de cumplimiento normativo. Su propósito es reconocer los méritos, el impacto y la contribución al ecosistema de ciberseguridad.

Premiación

Las candidaturas reconocidas recibirán reconocimiento público por parte de la Alianza México CiberSeguro, difusión en canales oficiales, uso del distintivo de Premios de Ciberseguridad AMCS 2026 conforme a los lineamientos y posible participación en la memoria o en el repositorio de buenas prácticas.

Cierre

Participa y ayuda a visibilizar las contribuciones que fortalecen la ciberseguridad en México y en la región. Un México más ciberseguro lo construimos entre todos.

Contacto

Para cualquier duda o aclaración relacionada con la convocatoria, las categorías, el proceso de postulación o los requisitos de participación, puedes escribirnos a: premios26@mexicociberseguro.org.mx