Guía práctica del CCN-CERT para hacer frente a la IA ofensiva

SECONDARY

Publisher	Laboratorio de Innovación AEPD
Published	2026-06-25
Retrieved	2026-09-18
Cite key	laboratorio2026gua
URL	https://laboratorio.aepd.es/novedades/guia-practica-del-ccn-cert-para-hacer-frente-la-ia-ofensiva

Claims drawn from this source. CLAIM-2026-09-18-09

CCN-CERT BP/36, Guía de buenas prácticas frente al modelo de IA ofensiva, Centro Criptológico Nacional, June 2026 — summarised by the AEPD's own innovation lab (laboratorio.aepd.es), page dated 25 June 2026.

Scope: how AI lets attackers "automatizar, acelerar y ampliar a gran escala ataques ya conocidos". Threat areas analysed include advanced phishing and deepfakes, automated malicious code generation, accelerated vulnerability exploitation, mass reconnaissance, attacks on language-model systems, and agentic AI systems with autonomous execution.

Recommendations centre on vulnerability management, identity protection, secure development lifecycle, supplier oversight and operational environment security, promoting "supervisión continua, la resiliencia y la seguridad desde el diseño".

Note: the CCN-CERT's own page (ccn-cert.cni.es) returned HTTP 403 to this run; the content above is taken from the AEPD laboratory's summary, which is an aepd.es property. Treated as secondary.