REGOLAMENTO DI ESECUZIONE (UE) 2024/482 DELLA COMMISSIONE

del 31 gennaio 2024

recante modalità di applicazione del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio per quanto riguarda l'adozione del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC)

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza») ([1]), in particolare l'articolo 49, paragrafo 7,

considerando quanto segue:

(1) Il presente regolamento specifica i ruoli, le norme e gli obblighi, nonché la struttura del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (*European Common Criteria-based cybersecurity certification* – EUCC) in conformità del quadro europeo di certificazione della cibersicurezza di cui al regolamento (UE) 2019/881. L'EUCC si fonda sull'accordo sul reciproco riconoscimento (ARR) dei certificati di valutazione della sicurezza delle tecnologie dell'informazione del gruppo di alti funzionari competente in materia di sicurezza dei sistemi d'informazione ([2]) (*Senior Officials Group – Information Systems Security*, SOG-IS) e si basa sui criteri comuni, comprese le procedure e i documenti del gruppo.

(2) Il sistema dovrebbe basarsi su norme internazionali consolidate. I criteri comuni (*Common Criteria*) sono una norma internazionale per la valutazione della sicurezza delle informazioni pubblicata, ad esempio, come ISO/IEC 15408 *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security*. Essa si basa sulla valutazione da parte di terzi e prevede sette livelli di garanzia della valutazione (*Evaluation Assurance Level* – EAL). I criteri comuni sono accompagnati dalla metodologia comune di valutazione (*Common Evaluation Methodology*), pubblicata, ad esempio come ISO/IEC 18045 - *Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Methodology for IT security evaluation*. Le specifiche e i documenti che applicano le disposizioni del presente regolamento possono riferirsi a una norma disponibile al pubblico che rispecchia la norma utilizzata per la certificazione nel quadro del presente regolamento, ad esempio i criteri comuni per la valutazione della sicurezza delle tecnologie dell'informazione (*Common Criteria for Information Technology Security Evaluation*) e la metodologia comune per la valutazione della sicurezza delle tecnologie dell'informazione (*Common Methodology for Information Technology Security Evaluation*).

(3) L'EUCC utilizza la famiglia di valutazione delle vulnerabilità dei criteri comuni (AVA_VAN), componenti da 1 a 5. I cinque componenti forniscono tutti i determinanti e tutte le dipendenze principali per l'analisi delle vulnerabilità dei prodotti TIC. Dal momento che corrispondono ai livelli di affidabilità del presente regolamento, i componenti consentono di compiere una scelta consapevole in merito all'affidabilità sulla base delle valutazioni dei requisiti di sicurezza e del rischio associato all'uso previsto del prodotto TIC che sono state effettuate. Il richiedente di un certificato EUCC dovrebbe fornire la documentazione relativa all'uso previsto del prodotto TIC e l'analisi dei livelli di rischio associati a tale uso per consentire all'organismo di valutazione della conformità di valutare l'idoneità del livello di affidabilità selezionato. Se le attività di valutazione e certificazione sono svolte dallo stesso organismo di valutazione della conformità, il richiedente dovrebbe presentare le informazioni richieste un'unica volta.

(4) Un settore tecnico costituisce un quadro di riferimento in cui rientra un gruppo di prodotti TIC con funzionalità di sicurezza specifiche e simili in grado di attenuare gli attacchi e nell'ambito del quale le caratteristiche sono comuni a un determinato livello di affidabilità. Esso indica nei documenti sullo stato dell'arte i requisiti di sicurezza specifici, nonché i metodi, le tecniche e gli strumenti di valutazione supplementari applicabili alla certificazione dei prodotti TIC che rientrano in tale settore tecnico. Pertanto promuove anche l'armonizzazione della valutazione dei prodotti

([1]) GU L 151 del 7.6.2019, pag. 15.

([2]) Accordo sul reciproco riconoscimento dei certificati di valutazione della sicurezza delle tecnologie dell'informazione, versione 3.0 del gennaio 2010, disponibile su sogis.eu, approvato dal gruppo di alti funzionari competente in materia di sicurezza dei sistemi d'informazione della Commissione europea in risposta al punto 3 della raccomandazione 95/144/CE del Consiglio, del 7 aprile 1995, su criteri comuni per la valutazione della sicurezza delle tecnologie d'informazione (GU L 93 del 26.4.1995, pag. 27).