REGIONE DEL VENETO

Allegato A4: Criteri di valutazione

PROCEDURA APERTA TELEMATICA, AI SENSI DELL'ART. 71 DEL D.LGS. N. 36/2023 E SS.MM.II, PER L'ACQUISTO DI SERVIZI DI SICUREZZA PER IL CSIRT REGIONALE DELLA DURATA DI 48 MESI, IN DUE LOTTI.

CODICE GARA APPTEL: **G03944**

Lotto 1 CUI: **S80007580279202600043**
Lotto 2 CUI: **S80007580279202600044** - **S80007580279202400040** - **S80007580279202400043** - **S80007580279202500049**

CRITERI DI VALUTAZIONE

LOTTI 1 E 2

CRITERI DI VALUTAZIONE

Di seguito gli **elementi di valutazione tecnica per ciascun servizio dei due Lotti**, con punteggio massimo pari a **80 punti per lotto**. Per ogni servizio sono stati individuati una serie di elementi essenziali, calibrando i punteggi sulla criticità delle attività descritte nel capitolato.

LOTTO 1 – Governance, controllo e supporto normativo

Sintesi dei criteri di valutazione (**Massimo 80 punt**i)

Tabella dei criteri discrezionali (D), quantitativo (Q) e tabellari (T) di valutazione dell'offerta tecnica

ID	CRITERIO	max punti	SUB - CRITERIO		CRITERIO DI VALUTAZIONE	max punti D	max punti Q	max punti T
A	**Servizio Governance, controllo, supporto normativo e presidio operativo**	**68**	**A1**	**Strategia e Governance**	La commissione valuta la conformità dell'offerta sulla base di: ● l'approccio strategico alla gestione della Constituency, inclusa la capacità di coordinamento multi-ente; ● la scalabilità del modello di Governance; ● l'efficacia delle procedure di presidio operativo e di crisis management.	**10**		
			A2	**Presidio e controllo**	La commissione valuta la conformità dell'offerta relativa alla capacità operativa: ● nel modello organizzativo descritto; ● nella gestione dei reportistica periodica; ● nella proposta di indicatori di performance (KPI/SLA) evolutivi; ● nella validazione dei tool;	**10**		

			A3	**Supporto evolutivo e innovazione**	La commissione valuta la conformità dell'offerta relativamente alla qualità del supporto: • nella descrizione di soluzioni propositive innovative per l'evoluzione efficace del CSIRT; • nell'assistenza per bandi/finanziamenti; • nella migrazione al PSR; • nel potenziamento dei SOC territoriali. • nell'adozione di AI per processi cyber predittivi;	**10**		
			A4	**Supporto normativo** **Richiesta:** erogazione di un supporto normativo e regolamentare, con pareri a validità legale in favore di tutti Enti che compongono la Constituency	La commissione valuta la conformità dell'offerta sulla base dei seguenti sub criteri: • conformità alle best practice e alle normative di settore (D.Lgs. 138/2024, Legge 90/2024, AI Act & Cloud, GDPR. Cyber Resilient ACT) • redazione di pareri legali sulla normativa sopra citata • redazione e l'aggiornamento annuale di linee guida per l'aggiornamento del portale ACN, l'individuazione dei fornitori	**10**		

					rilevanti e l'effettuazione dei relativi risk assessment. • redazione di linee guida per la categorizzazione annuale dei servizi secondo la NIS 2 e le relative analisi • formazione specifica correlata per ciascuna attività			
			A5	**Supporto specialistico per la Cyber Resilienza** **Richiesta:** erogazione di un supporto mirato nel rivedere, strutturare e implementare i processi operativi e di gestione degli incidenti informatici, creazione di flussi mancanti (es. nuovi vettori di minaccia) e ottimizzazione delle procedure di difesa già esistenti presso gli Enti e allineamento alle più recenti normative cyber e standard di sicurezza.	La commissione valuta la conformità dell'offerta sulla base dei seguenti sub criteri: • Standardizzazione della gestione delle crisi cyber: integrazione di playbook standardizzati per la gestione efficace delle crisi di sicurezza informatica. • Conformità e tempestività nelle notifiche: adeguamento dei processi per garantire la notifica degli incidenti gravi entro i termini di legge. • Rafforzamento della resilienza: potenziamento della resilienza operativa digitale. • Integrazione immediata dei flussi: assicurare l'integrazione immediata tra la procedura di gestione degli incidenti del CSIRT	**10**		

					e il processo di notifica delle violazioni dei dati personali al Garante per la Protezione dei Dati Personali e le autorità competenti (es. Polizia Postale)			
			A6	**Elaborazione di Newsletter e Bollettini di sicurezza** **Richiesta:** elaborazione, redazione e successiva diffusione di strumenti informativi periodici, ovvero newsletter e bollettini di sicurezza.	La commissione valuta la conformità dell'offerta sulla base dei seguenti sub criteri: ● cadenza e periodicità ● processo di elaborazione, redazione, validazione e diffusione ● gestione dei bollettini di sicurezza	**8**		
			A7	**Valutazione e monitoraggio continuo dei Servizi** **Richiesta:** stabilire e mantenere un ciclo continuo di valutazione, implementazione e verifica delle misure di sicurezza	La commissione valuta la conformità dell'offerta sulla base dei seguenti sub criteri: ● analisi dei divari (Gap Analisys) ● audit di conformità ● verifica e validazione degli interventi eseguiti; ● nella descrizione della modalità e	**10**		

				relativamente a tutti i servizi forniti dal CSIRT.	degli strumenti di monitoraggio dei servizi.			
B	**Servizio di Reperibilità in caso di Crisi**	**10**		Reperibilità H24x7x365 e gestione crisi a livello all'interno della Constituency. La commissione valuta la conformità dell'offerta sulla base dei seguenti sub criteri: • modello di reperibilità • tempi di attivazione • modalità di coordinamento di incidenti multi-Ente • qualità dei playbook di crisi e integrazione con il SOC		**10**		
C	**Misure in materia di sostenibilita' ambientale del proponente**	**1**	**-**	È richiesto al proponente di indicare le proprie misure di sostenibilità ambientale Descrizione delle soluzioni adottate dal proponente per la riduzione dell'impatto ambientale. Il concorrente dovrà descrivere gli interventi realizzati per ridurre il fabbisogno energetico e le emissioni delle proprie operazioni, con particolare riferimento a: - dispositivi elettronici (es. acquisto notebook e altri dispositivi elettronici dotati di un'etichetta ambientale di tipo I, conforme alla UNI EN ISO 14024, come ad esempio TCO Certified, EPEAT 2018, Blue Angel, TÜV Green Product Mark, di etichetta equivalente o di etichetta legata all'efficienza energetica dei dispositivi come Etichetta EPA Energy Star); - spostamenti per lavoro (es. politiche aziendali e incentivi finalizzati a favorire l'utilizzo di servizi trasporto collettivo per gli spostamenti di lavoro). La valutazione terrà conto dell'efficacia e concretezza delle azioni descritte		**1**		

				in termini di riduzione dell'impatto ambientale.			
D	**Certificazione sulla parita' di genere**	**1**	**-**	È richiesto al proponente di indicare il possesso o meno della certificazione in materia di parità di genere ex art. 46-bis del codice delle pari opportunità tra uomo e donna, di cui al D.Lgs. n. 198/2006. Possesso di una certificazione in materia di parità di genere ex art. 46-bis del codice delle pari opportunità tra uomo e donna, di cui al D.Lgs. n. 198/2006, rilasciata da un organismo di valutazione della conformità accreditato ai sensi del regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, che opera sulla base della prassi UNI/PdR 125:2022 (art. 108 comma 7 del D.lgs n. 36/2023). In caso di partecipazione in forma associata il punteggio sarà attribuito: - per i soggetti di cui all'articolo 65, comma 2, lettere e), f), g) e h) del Codice se tutti i soggetti che costituiscono il raggruppamento, consorzio ordinario, GEIE, imprese retiste che partecipano alla gara siano in possesso della certificazione; - per i consorzi di cui all'articolo 65, comma 2, lettere b), c) e d) del Codice se il consorzio e le consorziate esecutrici siano in possesso della certificazione. il punteggio verrà attribuito al concorrente come di seguito riportato: • possesso della certificazione: 1 punto, • mancato possesso della certificazione: 0 punti.			**1**

LOTTO 2 – Servizi Integrati di Cyber Security

Sintesi dei criteri di valutazione – Lotto 2 (Massimo 80 punti)
Tabella dei criteri discrezionali (D), quantitativo (Q) e tabellari (T) di valutazione dell'offerta tecnica

ID	CRITERIO	max punti	SUB - CRITERIO		CRITERIO DI VALUTAZIONE	max punti D	max punti Q	max punti T
A	**SOC, Incident Management e Cyber Threat Intelligence**	**24**	**A1**	**Architettura, anti-lock-in e onboarding degli Enti** Richiesta: descrivere l'architettura tecnica proposta per la Security Data Platform, con indicazione della modalità di erogazione (Cloud, Ibrida, On-Premise), delle modalità di onboarding degli Enti a basso impatto e delle garanzie di portabilità e uscita dal contratto.	La commissione valuta la conformità dell'offerta, complessivamente intesa, sulla base dei seguenti elementi: • solidità e qualità della soluzione SDP proposta in relazione alla modalità di erogazione proposta. • modalità di onboarding degli Enti alla Security Data Platform, con particolare riferimento alla continuità del monitoraggio e al minimo impatto sull'operatività di ciascun Ente durante la migrazione • adozione di standard aperti e misure anti-lock-in (conversione delle regole di correlazione, normalizzazione degli eventi, esportabilità dello storage) • completezza dell'exit plan al termine del contratto;	**3**	**-**	**-**

			A2	**Sistemi di rilevamento, AI Augmented SOC e correlazione laterale** Richiesta: descrivere le tecnologie di detection avanzata e l'impiego reale dell'intelligenza artificiale per il triage, la riduzione dei falsi positivi e la correlazione laterale tra Enti, con particolare riferimento alla riduzione del carico operativo sugli Enti.	La commissione valuta la conformità dell'offerta, complessivamente intesa, sulla base dei seguenti elementi: • maturità operativa della soluzione di AI Augmented SOC per il triage e la riduzione dei falsi positivi, con evidenza della spiegabilità dei modelli e dell'operatività al giorno zero rispetto a una roadmap; • capacità di correlazione laterale tra Enti e di propagazione automatica delle regole di detection e degli alert preventivi, così che un attacco rilevato su un Ente protegga automaticamente gli altri; • ampiezza e profondità delle sorgenti di telemetria che la soluzione è in grado di raccogliere, normalizzare e correlare, con particolare riferimento alla capacità di integrare — oltre alle sorgenti on-premise — anche la telemetria proveniente dai servizi cloud degli Enti mediante integrazioni native con le principali piattaforme cloud; • valore aggiunto complessivo delle tecnologie di rilevamento nel contesto della Constituency, in termini di	**4**	**-**	**-**

					capacità di analisi e reazione agli attacchi.			

			A3		Copertura del framework MITRE ATT&CK Enterprise da parte delle regole di detection attive alla data del collaudo di avvio, verificata mediante ATT&CK Navigator in sede di valutazione: • 4 punti se copertura ≥ 60%; • 3 punti se compresa tra 50% e 59%; • 2 punti se compresa tra 40% e 49%; • 0 punti se inferiore al 40%.	**-**	**2**	**-**

			A4	**Orchestrazione SOAR, playbook operativi e gestione delle crisi** Richiesta: descrivere i meccanismi di automazione della risposta agli incidenti, la struttura del processo di Incident Response e il modello di gestione delle crisi, incluso il ruolo del Service Manager quale riferimento contrattuale unico.	La commissione valuta la conformità dell'offerta, complessivamente intesa, sulla base dei seguenti elementi: • livello di automazione SOAR nel rispetto dei limiti autorizzativi definiti per ciascun Ente e portabilità dei workflow in formato aperto; • qualità e specificità dei playbook per gli scenari tipici della Pubblica Amministrazione (phishing, ransomware, accessi anomali) e struttura del processo di Incident Response nelle sue fasi; • solidità del modello di gestione delle crisi (War Room, Decision Log, procedure di comunicazione) e presidio del Service Manager per gli incidenti di Severità 1.	**4**	**-**	**-**

			A5	**Cyber Threat Intelligence contestualizzata su asset inventory e SBOM** Richiesta: descrivere le modalità di raccolta, contestualizzazione e distribuzione della threat intelligence, con particolare riferimento alla correlazione delle minacce con l'inventario degli asset (CMDB) e gli SBOM degli Enti.	La commissione valuta la conformità dell'offerta, complessivamente intesa, sulla base dei seguenti elementi: • qualità della contestualizzazione della threat intelligence sul reale parco tecnologico di ciascun Ente, mediante correlazione automatica degli indicatori di compromissione e delle vulnerabilità note con gli asset del CMDB e con gli SBOM, così da distribuire a ogni Ente le sole segnalazioni pertinenti; • capacità di monitoraggio del Deep Web e Dark Web per la rilevazione di data leakage, credential leakage e domain squatting riferiti agli Enti; numerosità, profondità e qualità delle fonti informative complessivamente proposte.	**4**	**-**	**-**

			A6	**Integrazione MISP Regionale** Integrazione nativa della MISP Regionale con i protocolli STIX 2.1 / TAXII 2.1 e presenza dei feed obbligatori attivi (CERT-AGID, MISP ACN, NVD e almeno una fonte di indicatori aggregati), con dimostrazione pratica dello scambio di IoC:	• 2 punti se l'integrazione nativa è dimostrata e tutti i feed obbligatori risultano attivi; • 1 punto se l'integrazione avviene tramite adattatore documentato o i feed sono parzialmente attivi; 0 punti se assente.	**-**	**2**	**-**

			A7	**Team SOC: competenze, seniority e trasferimento di know-how** Richiesta: descrivere il team dedicato al contratto, le certificazioni e la seniority degli analisti e il piano di trasferimento delle competenze al personale del CERT regionale.	La commissione valuta la conformità dell'offerta, complessivamente intesa, sulla base dei seguenti elementi: • qualità del piano di threat hunting proattivo (metodologia, frequenza delle sessioni, struttura dei report) e del piano di trasferimento di know-how al personale interno, anche in relazione alle giornate offerte oltre il minimo contrattuale.	**2**	**-**	**-**

			A8	**Medical SOC ed elementi premiali** Richiesta: descrivere le competenze specifiche in ambito sanitario per il monitoraggio dei dispositivi IoMT, applicabili in caso di estensione del servizio all'Azienda Sanitaria pilota, e le eventuali migliorie offerte rispetto ai requisiti minimi.	La commissione valuta la conformità dell'offerta, complessivamente intesa, sulla base dei seguenti elementi: • qualità del piano di inventario passivo dei dispositivi IoMT e dei guardrail per gli asset clinici safety-critical, con garanzia di non interferenza con i dispositivi clinici, ed esperienza documentata in ambienti sanitari; • elementi migliorativi offerti senza oneri aggiuntivi.	**3**	**-**	**-**

Tabella dei criteri discrezionali (D), quantitativo (Q) e tabellari (T) di valutazione dell'offerta tecnica

ID	CRITERIO	max punti	SUB - CRITERIO		CRITERIO DI VALUTAZIONE	max punti D	max punti Q	max punti T
B	**Servizio Vulnerability Management**	**20**	**B1**	**Esposizione e Governance delle vulnerabilità** **Richiesta:** Descrivere il modello organizzativo proposto per l'esposizione e la gestione delle vulnerabilità in contesti distribuiti.	La commissione valuta la conformità dell'offerta sulla base dei seguenti sub criteri. • Robustezza del modello di Exposure Management. • Efficacia nel coordinamento dei processi di rimedio.	**6**		

			B2	**Assessment su larga scala (13.000 IP)** **Richiesta:** Illustrare la metodologia per l'esecuzione di scansioni massive e la gestione degli asset.	La commissione valuta la conformità dell'offerta sulla base dei seguenti sub criteri. • Metodologia per scansioni su 13.000 IP. • Accuratezza nel censimento degli asset. • Capacità di gestione dei volumi di rilevamento annuali.	**6**		
			B3	**Penetration Test e Purple Teaming** **Richiesta:** Descrivere la qualità e la profondità dei test di intrusione e delle simulazioni di attacco proattivo.	La commissione valuta la conformità dell'offerta sulla base dei seguenti sub criteri. • Qualità dei penetration test e completezza tipologia di applicazioni verificabili. • Profondità delle simulazioni Purple Teaming.	**4**		

					• Collaborazione con i team di difesa.			
			B4	**DevSecOps e sicurezza della supply chain** **Richiesta:** Descrivere l'integrazione della sicurezza nel ciclo di sviluppo e il monitoraggio delle terze parti.	La commissione valuta la conformità dell'offerta sulla base dei seguenti sub criteri. • Integrazione dei controlli DevSecOps. • Monitoraggio della postura di sicurezza della supply chain.	**2**		

			B5	**Prioritizzazione e Reportistica dinamica** **Richiesta:** Illustrare i criteri di classificazione delle vulnerabilità e la qualità dell'output documentale.	La commissione valuta la conformità dell'offerta sulla base dei seguenti sub criteri: • Classificazione basata sul contesto operativo. • Qualità della reportistica dinamica.	**2**		

ID	CRITERIO	max punti	SUB - CRITERIO		CRITERIO DI VALUTAZIONE	max punti D	max punti Q	max punti T
C	**Servizio Gestione del Rischio, TPRM e Business Continuity**	**19**	C1	**Gestione del rischio** **Richiesta:** supportare gli Enti della Constituency nell'identificazione, analisi, valutazione, trattamento e monitoraggio continuo dei rischi di cybersicurezza, secondo un approccio progressivo e proporzionato alla dimensione, alla tipologia, al livello di maturità e alla criticità dei servizi erogati da ciascun Ente.	La commissione valuta la conformità dell'offerta sulla base dei seguenti sub criteri: ● definizione delle linee guida e del framework metodologico ● esecuzione del maturity assessment e della gap analysis ● esecuzione del risk assessment ● analisi e valutazione del rischio ● creazione e mantenimento del Risk Register ● definizione e aggiornamento del Piano dei Trattamenti ● monitoraggio dell'attuazione delle misure di trattamento ● gestione delle eccezioni e delle accettazioni del rischio ● produzione della reportistica e deliverables	**6**		

			C2	**Modello evoluto per gli Enti del perimetro NIS2** **Richiesta:** erogazione di un modello evoluto, quale rafforzamento del modello base per i soggetti rientranti nel perimetro NIS.	La commissione valuta la conformità dell'offerta sulla base dei seguenti sub criteri: ● analisi del rischio più approfondita e dettagliata ● analisi del rischio continuativa e basata su segnali operativi in tempo reale ● presidio rafforzato dei rischi di supply chain ● reportistica direzionale dedicata	**4**		
			C3	**Third Party Risk Management (TPRM)** **Richiesta:** implementare un processo di Third Party Risk Management (TPRM) che copra l'intero ciclo di vita del rapporto con le terze parti, dall'onboarding fino alla cessazione del rapporto contrattuale	La commissione valuta la conformità dell'offerta sulla base dei seguenti sub criteri: ● censimento e classificazione delle terze parti ● valutazione del rischio inerente, ● due diligence proporzionata al livello di rischio ● utilizzo del cyber scoring come indicatore di rischio ● supporto nella gestione delle anomalie e delle criticità riscontrate ● supporto alla definizione di clausole contrattuali di sicurezza ● monitoraggio continuativo delle terze parti critiche ● gestione degli accessi remoti delle terze parti	**4**		

					• supporto alla definizione delle exit strategy • numerosità soggetti terzi sottoposti a valutazione			
			C4	**Business Continuity & Disaster Recovery (BC/DR):** **Richiesta:** garantire la continuità dei servizi critici e la capacità di ripristino a fronte di eventi avversi, inclusi incidenti cyber ad elevato impatto	La commissione valuta la conformità dell'offerta sulla base dei seguenti sub criteri: • esecuzione della Business Impact Analysis (BIA) • supporto nella definizione dei parametri di ripristino (RTO, RPO e MTPD) • redazione, aggiornamento e manutenzione dei piani di Business Continuity e Disaster Recovery • predisposizione dei runbook operativi di ripristino • supporto nella definizione delle procedure di crisi • supporto nell'esecuzione di test ed esercitazioni periodiche • verifica dei processi di backup e restore • produzione di report post-test e	**5**		

					lessons learned • monitoraggio e supporto alla chiusura delle azioni correttive			

Tabella dei criteri discrezionali (D), quantitativo (Q) e tabellari (T) di valutazione dell'offerta tecnica

ID	CRITERIO	max punti	SUB - CRITERIO		CRITERIO DI VALUTAZIONE	max punti D	max punti Q	max punti T
D	**Servizio Formazione e Security Awareness**	15	**D1**	**LMS e Simulazioni** **Richiesta:** Descrivere l'usabilità della piattaforma LMS e l'aderenza alle	La commissione valuta la conformità dell'offerta sulla base dei seguenti sub criteri: • Usabilità della piattaforma LMS. • Predisposizione percorsi formativi onboarding intensivo. • Aderenza delle simulazioni ai requisiti ACN.	**3**		

				linee guida ACN.				
			D2	**Formazione profilata per Ruoli** **Richiesta:** Illustrare la segmentazione dei contenuti formativi e il piano di sensibilizzazione continua.	La commissione valuta la conformità dell'offerta sulla base dei seguenti sub criteri: • Capacità di segmentazione per mansioni. • Qualità del piano di sensibilizzazione continua.	**3**		

			D3	**Campagne di Phishing etico** **Richiesta:** Definire la varietà e la frequenza dei test multicanale.	La commissione valuta la conformità dell'offerta sulla base dei seguenti sub criteri: • Varietà e frequenza delle campagne multicanale. • Misurazione della prontezza del personale.	**2**		
			D4	**Indicatori e Cultura della Sicurezza** **Richiesta:** Descrivere le modalità di promozione della cultura della sicurezza e i KPI utilizzati.	La commissione valuta la conformità dell'offerta sulla base dei seguenti sub criteri: • Efficacia nella promozione delle segnalazioni. • Qualità dei KPI per l'evoluzione del fattore umano.	**2**		

			D5	**Innovazione didattica e Valore Aggiunto** **Richiesta:** Presentare le tecniche didattiche moderne e le proposte di ingaggio utenza.	La commissione valuta la conformità dell'offerta sulla base dei seguenti sub criteri: • Adozione di tecniche di erogazione moderne • Proposte migliorative per l'ingaggio dell'utenza.	**2**		
			D6	**Sinergia con SOC e Reportistica** **Richiesta:** Illustrare l'integrazione tra formazione e monitoraggio SOC.	La commissione valuta la conformità dell'offerta sulla base dei seguenti sub criteri: • Integrazione dati formativi con monitoraggio operativo. • Qualità della rendicontazione per il management.	**2**		

			D7	**Zainetto formativo** **Richiesta:** Descrivere la gestione del trasferimento di personale garantendo la conservazione dello stato formativo.	La commissione valuta la conformità dell'offerta sulla base dei seguenti sub criteri: • Gestione trasferimento personale tra Enti. • Garanzia di conservazione dello stato formativo.	**1**		

Tabella dei criteri discrezionali (D), quantitativo (Q) e tabellari (T) di valutazione dell'offerta tecnica

ID	CRITERIO	CRITERIO DI VALUTAZIONE	max punti D	max punti Q	max punti T
E	**Misure in materia di sostenibilita' ambientale del proponente**	È richiesto al proponente di indicare le proprie misure di sostenibilità ambientale Descrizione delle soluzioni adottate dal proponente per la riduzione dell'impatto ambientale. Il concorrente dovrà descrivere gli interventi realizzati per ridurre il fabbisogno energetico e le emissioni delle proprie operazioni, con particolare riferimento a: - dispositivi elettronici (es. acquisto notebook e altri dispositivi elettronici dotati di un'etichetta ambientale di tipo I, conforme alla UNI EN ISO 14024, come ad esempio TCO Certified, EPEAT 2018, Blue Angel, TÜV Green Product Mark, di etichetta equivalente o di etichetta legata all'efficienza energetica dei dispositivi come Etichetta EPA Energy Star); - spostamenti per lavoro (es. politiche aziendali e incentivi finalizzati a favorire l'utilizzo di servizi trasporto collettivo per gli spostamenti di lavoro). La valutazione terrà conto dell'efficacia e concretezza delle azioni descritte in termini di riduzione dell'impatto ambientale.	**1**		
F	**Certificazione sulla parita' di genere**	È richiesto al proponente di indicare il possesso o meno della certificazione in materia di parità di genere ex art. 46-bis del codice delle pari opportunità tra uomo e donna, di cui al D.Lgs. n. 198/2006. Possesso di una certificazione in materia di parità di genere ex art. 46-bis del codice delle pari opportunità tra uomo e donna, di cui al D.Lgs. n. 198/2006, rilasciata da un organismo di valutazione della conformità accreditato ai sensi del regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, che opera sulla base della prassi UNI/PdR 125:2022 (art. 108 comma 7 del D.lgs n. 36/2023). In caso di partecipazione in forma associata il punteggio sarà attribuito: - per i soggetti di cui all'articolo 65, comma 2, lettere e), f), g) e h) del Codice se tutti i soggetti che costituiscono il raggruppamento, consorzio ordinario, GEIE, imprese retiste che partecipano alla gara siano in possesso della certificazione; - per i consorzi di cui all'articolo 65, comma 2, lettere b), c) e d) del Codice se il consorzio e le consorziate esecutrici siano in possesso della certificazione. il punteggio verrà attribuito al concorrente come di seguito riportato:			**1**

		• possesso della certificazione: 1 punto, • mancato possesso della certificazione: 0 punti.			