TITOLO III DEL REGOLAMENTO (UE) 2019/881, "REGOLAMENTO SULLA CIBERSICUREZZA"

ATTUAZIONE NAZIONALE DEL QUADRO EUROPEO DI CERTIFICAZIONE DELLA CIBERSICUREZZA

QUESTIONARIO

INDICAZIONI OPERATIVE:

- *Rispondere al questionario facendo riferimento alla SCHEDA INFORMATIVA sul "Titolo III del Regolamento (UE) 2019/881, "Regolamento sulla cibersicurezza", Attuazione nazionale del quadro europeo di certificazione della cibersicurezza".*
- *I campi marcati con l'asterisco (*) sono da compilare obbligatoriamente.*
- *Saranno considerati solo i questionari pertinenti, compilati in tutte le parti obbligatorie (contrassegnate con asterisco) e debitamente sottoscritti con firma digitale o firma olografa, allegando in questo secondo caso al questionario anche copia di un documento d'identità.*
- *I questionari compilati in tutte le parti obbligatorie e sottoscritti sono da inviarsi all'indirizzo email consultazione.CSA@mise.gov.it.*
- *Questa consultazione non prevede la raccolta di dati personali e non necessita di fornire dati aziendali riservati. Pertanto nella compilazione del questionario si invita a non fornire dati personali o dati aziendali riservati.*

SEZIONE 0. – TIPOLOGIA DI INVIO DEL QUESTIONARIO

Scegliere una delle due seguenti tipologie di invio*:

☑	Questionario inviato per conto di un'organizzazione.
○	Questionario inviato a titolo personale.

SEZIONE 1. – DATI IDENTIFICATIVI DELL'EVENTUALE ORGANIZZAZIONE RAPPRESENTATA

NOTA: Compilare i seguenti dati, solo se il questionario è inviato a nome della propria organizzazione e non a titolo personale.

ORGANIZZAZIONE E COMPILATORE DEL QUESTIONARIO	Nome dell'Organizzazione*	ACCREDIA
	Sede Legale dell'Organizzazione*	VIA SALICETO 7/9 00161 ROMA
CATEGORIE DI APPARTENENZA DELL'ORGANIZZAZIONE	Selezionare una o più categorie*	
	☐	Autorità o agenzie nazionali attive nel campo della cibersicurezza, protezione dei dati personali, vigilanza/sorveglianza sul mercato

	☑	Organismi di normazione, di accreditamento, di valutazione della conformità, laboratori accreditati dell'OCSI
	☐	Associazioni di Piccole e Medie Imprese
	☐	Associazioni dei Consumatori
	☐	Imprese fornitrici ed utilizzatrici di prodotti, servizi e processi TIC
	☐	Centri di ricerca ed università
	☐	Altri soggetti destinatari del Regolamento (UE) 2019/881
	In caso si sia selezionata l'ultima categoria, specificare — nel riquadro sottostante — in che modo l'attuazione nazionale del regolamento (UE) 2019/881 può incidere sulle attività della propria organizzazione.*	

SEZIONE 2. – ESAME DELLE OPZIONI DI RIFEREIMENTO PER LA PROPOSTA NORMATIVA

Con riferimento alla sezione 4 della SCHEDA INFORMATIVA (Le opzioni di intervento), valutare l'opzione di riferimento per ogni area

2.1. Nella sezione 4.1 della SCHEDA INFORMATIVA è indicata la seguente opzione di riferimento:

***Opzione di riferimento**: Non ravvisandosi motivi particolari per prevedere più di uno schema di decreto legislativo, si propone per semplicità di attuare con un singolo decreto legislativo la delega complessiva di cui all'articolo 18 della Legge di delegazione europea 2019-2020 per rendere completamente operativo a livello nazionale il regolamento (UE) 2019/881, fatti salvi atti di esecuzione della Commissione Europea che dovessero essere adottati successivamente ai sensi del regolamento (UE) 2019/881.*

Si condivide la posizione del Ministero dello sviluppo economico in merito all'opzione di riferimento proposta?*

Rispondere alla domanda utilizzando il riquadro sottostante:

Si condivide l'opzione proposta

Si ritiene utile rappresentare ulteriori osservazioni in merito?

In tal caso riportare le proprie osservazioni nel riquadro di seguito:

2.2. Nella sezione 4.2 della SCHEDA INFORMATIVA è indicata la seguente opzione di riferimento:

***Opzione di riferimento**: Dal momento che le scelte riguardo all'emissione dei certificati potranno essere fatte per ogni sistema europeo di certificazione che sarà adottato dalla Commissione Europea, in seno alla proposta di decreto legislativo si ritiene di lasciare aperta ogni possibilità per l'emissione dei certificati prevedendo possibili collaborazioni pubblico-privato che potranno coinvolgere l'NCCA, i laboratori di prova e gli altri organismi di valutazione della conformità pubblici e privati accreditati dall'organismo nazionale di accreditamento. Saranno eventualmente operate scelte specifiche sulla base delle esigenze del singolo sistema di certificazione che sarà adottato, ove necessario.*

Si condivide la posizione del Ministero dello sviluppo economico in merito all'opzione di riferimento proposta?*

Rispondere alla domanda utilizzando il riquadro sottostante:

Si condivide l'opzione proposta

Si ritiene utile rappresentare ulteriori osservazioni in merito?

In tal caso riportare le proprie osservazioni nel riquadro di seguito:

ACCREDIA è disponibile a collaborare alla definizione di schemi di accreditamento per specifiche valutazioni di conformità, in base alle necessità determinate dall'attivazione dei sistemi europei di certificazione adottati dalla Commissione europea.

2.3. Nella sezione 4.3 della SCHEDA INFORMATIVA è indicata la seguente opzione di riferimento:

***Opzione di riferimento**: La proposta normativa traccerà alcuni principi generali di cooperazione della NCCA con le altre autorità competenti e l'organismo nazionale di accreditamento. Le effettive modalità di collaborazione potranno essere oggetto di accordi successivi tra le autorità/organismo di accreditamento nazionale.*

Si condivide la posizione del Ministero dello sviluppo economico in merito all'opzione di riferimento proposta?*

Rispondere alla domanda utilizzando il riquadro sottostante:

Si condivide l'opzione di riferimento, con informazioni aggiuntive riportate nel riquadro seguente.

Si ritiene utile rappresentare ulteriori osservazioni in merito?

In tal caso riportare le proprie osservazioni nel riquadro di seguito:

• Verifica esterna della qualità a supporto dell'accreditamento dei Laboratori di prova
La norma ISO/IEC 17025 (§7.7.2) prevede quale strumento di assicurazione e verifica della validità dei risultati di prova i confronti interlaboratorio.
Tali confronti sono organizzati e gestiti anche dalla Pubblica Amministrazione (p. es. Agenzia delle Dogane e Monopoli, Istituto Superiore di Sanità, Istituti Zooprofilattici, ISPRA, ARPA).
Tali confronti sono tanto più necessari nei settori in cui, come quello in oggetto, la maggior parte delle prove non è eseguita utilizzando metodi metrologicamente riferibili, e quindi non si può avvalere della garanzia di validità che deriva dall'utilizzo di strumentazione tarata con riferimento ai campioni di misura mantenuti dall'Istituto Nazionale di Ricerca Metrologica di Torino.
In questo caso quindi è altamente auspicabile che il MISE possa mettere a disposizione della comunità dei laboratori di sicurezza informatica un circuito interlaboratorio, caratterizzato dal massimo rigore tecnico e dalla erogazione periodica (p. es. su base annuale).
• Modalità di accreditamento dell'organismo di certificazione (OCSI), operativo nella DG TCSI-ISCTI
L'accreditamento ISO/IEC 17065 di OCSI, qualora richiesto ad ACCREDIA, avverrà con le modalità standardizzate ed applicate ad ogni organismo di certificazione, descritte nel Regolamento Generale RG-01.
ACCREDIA, ove necessario per specifici settori tecnici emette, ad integrazione dei Regolamenti Generali, ulteriori Regolamenti Tecnici o Circolari applicative, nelle quali sono meglio specificati i requisiti che gli organismi di certificazione devono soddisfare e/o le relative modalità di accreditamento. Sarà valutata la necessità di emettere tali documenti nel caso di accreditamento dell'OCSI e di altri organismi di certificazione operanti nell'ambito della cybersecurity, anche alla luce delle linee guida pubblicate da ENISA.
• Modalità di autorizzazione/accreditamento dei CAB
L'acccreditamento dei CAB in quanto Organismi di certificazione privati avverrà come sopra indicato.
I CAB Laboratori di prova saranno accreditati con le modalità descritte nel Regolamento Generale RG-02 e nel Regolamento Tecnico RT-08, con le medesime considerazioni sopra riportate circa la eventuale necessità di documenti integrativi.
• Modalità di cooperazione DG-TCSI-ISCTI con ACCREDIA per monitoraggio dei CAB
ACCREDIA chiederà a DG-TCSI-ISCTI di nominare un Esperto Tecnico da inserire nel competente Comitato settoriale di Accreditamento, il quale avrà accesso alle risultanze degli audit di accreditamento e di sorveglianza, e verrà chiamato a concorrere alle decisioni del Comitato relative a concessione, mantenimento, estensione, riduzione, sospensione o revoca dell'accreditamento.
L'Esperto Tecnico nominato dal DG-TCSI-ISCTI sarà consultato nel caso in cui pervengano dal mercato segnalazioni o reclami a carico del CAB.
• Vigilanza su accreditamento dei CAB da parte di ACCREDIA
ACCREDIA esercita sui CAB la sorveglianza prevista dalla norma ISO/IEC 17011 e dai propri regolamenti, che consiste nell'effettuazione di audit a cadenza non superiore ai 18 mesi. La convenzione di accreditamento stipulata con i CAB ha la durata di 4 anni, e prima della scadenza viene effettuato un audit di rinnovo dell'accreditamento, sostituendo, ove possibile, il team ispettivo.
• Sanzioni accessorie per i CAB
ACCREDIA comunicherà alla NCCA le sanzioni comminate ai CAB secondo le previsioni dei Regolamenti applicabili RG-02, RG-01, RG-09. Tali sanzioni consistono nella sospensione temporanea, parziale o totale, dell'accreditamento, o nella sua revoca.
• Reclami ricevuti dai CAB e ricorsi giurisdizionali contro i CAB
I reclami e i ricorsi ricevuti dai CAB contro l'operato di ACCREDIA vengono gestiti secondo quanto previsto dai Regolamenti Generali per l'accreditamento dei CAB RG-02 e RG-01, dal Regolamento di funzionamento della Commissione d'Appello RG-06.
Inoltre, relativamente a reclami e segnalazioni da parte dei CAB, indicazioni specifiche sono descritte sul sito web di ACCREDIA, al link https://www.accredia.it/segnalazioni-2/ .
Infine le modalità di gestione delle richieste di accesso agli atti ricevute da ACCREDIA sono disciplinate dal Regolamento per l'accesso agli atti RG-23.
I ricorsi giurisdizionali contro i CAB possono essere avviati da ACCREDIA nel caso di gravi inadempienze contrattuali rispetto agli impegni previsti dalla Convenzione di Accreditamento e nel caso di comportamenti lesivi del nome e dell'immagine di ACCREDIA e della reputazione dell'accreditamento.
• Notifica dei CAB accreditati al MISE
ACCREDIA notificherà al MISE l'avvenuto accreditamento dei CAB, così come gli eventuali provvedimenti di sospensione (parziale o totale) e di revoca dell'accreditamento

2.4. Nella sezione 4.4 della SCHEDA INFORMATIVA è indicata la seguente opzione di riferimento:

***Opzione di riferimento**: La NCCA costituirà due elenchi distinti nei quali saranno inseriti rispettivamente i laboratori privati da essa abilitati per le attività di certificazione e per le attività di vigilanza nazionale della NCCA. Per quanto riguarda il secondo elenco sarà necessario prevedere per i soggetti iscritti l'astensione da qualsiasi attività di emissione dei certificati o di valutazione di sicurezza informatica nell'ambito vigilato.*

Si condivide la posizione del Ministero dello sviluppo economico in merito all'opzione di riferimento proposta?*

Rispondere alla domanda utilizzando il riquadro sottostante:

Non si condivide l'opzione di riferimento, con informazioni aggiuntive riportate nel riquadro seguente

Si ritiene utile rappresentare ulteriori osservazioni in merito?

In tal caso riportare le proprie osservazioni nel riquadro di seguito:

Non si condivide la necessità di costituire due elenchi distinti e mutuamente esclusivi di Laboratori. Se l'attività di vigilanza non fosse di volume adeguato a sostenere economicamente l'attività di un Laboratorio privato, la maggioranza, o tutti, potrebbero scegliere di iscriversi nell'elenco dei laboratori abilitati alle attività preliminari alla certificazione lasciando sguarnita la vigilanza.

Si potrebbe consentire ad ogni Laboratorio di iscriversi in entrambi gli elenchi, considerando che già la norma ISO/IEC 17025 (§ 4.1) impone ai Laboratori requisiti di imparzialità nello svolgimento delle proprie attività, e l'analisi continuativa dei rischi di compromissione dell'imparzialità.

Si può rafforzare la garanzia di imparzialità con le seguenti modalità (o altre da individuare):

1) Richiedendo al Laboratorio che desidera iscriversi nell'elenco della vigilanza la sottoscrizione di un impegno più dettagliato e circostanziato relativamente alla tipologia di rischi per l'imparzialità che il Laboratorio deve considerare quando effettua attività ai fini della vigilanza, e delle modalità operative con cui deve effettuare il relativo riesame preliminare della richiesta di prove.

2) Gestendo opportunamente degli incarichi di prova, includendo nel riesame preliminare della NCC una indagine circa l'indipendenza del laboratorio candidato all'affidamento rispetto a quello che ha effettuato le prove di certificazione del prodotto.

3) Una volta individuato un laboratorio candidato all'affidamento, e prima dell'incarico:
- comunicare al produttore il nominativo del laboratorio candidato invitandolo ad accettarlo oppure a presentare ricusazione sostanzialmente motivata
- comunicare al Laboratorio candidato il nominativo del produttore ed del laboratorio che ha effettuato le prove di certificazione, chiedendo la sottoscrizione di un documento nel quale il laboratorio candidato si dichiara indipendente e privo di conflitti di interesse nei confronti del produttore e dell'altro laboratorio

4) Qualora un produttore fosse in grado di presentare ricusazioni sostanzialmente motivate per tutti i laboratori proposti, consentire al produttore o ad un suo rappresentante, anche facente parte del laboratorio di certificazione, di presenziare alle prove, con la presenza di personale della NCCA a garanzia della trasparenza e correttezza dell'iter di prova.

2.5. Nella sezione 4.5 della SCHEDA INFORMATIVA è indicata la seguente opzione di riferimento:

***Opzione di riferimento**: Per quanto riguarda i certificati di livello elevato, ove fossero confermate delle non conformità l'NCCA effettuerà la revoca del certificato. Invece per l'ambito dei certificati di livello di base e sostanziale la revoca del certificato sarà effettuata dalla NCCA qualora a fronte dell'accertamento da parte della stessa di certificati non conformi, l'organismo di conformità emittente, non provveda alla riconduzione a conformità del certificato. Il certificato sarà revocato in eventuali altre situazioni particolarmente critiche, ad esempio nel caso in cui il certificato non conforme sia relativo ad un prodotto TIC, servizio TIC o processo TIC che ha comportato un concreto e dimostrato pregiudizio*

- *ad un servizio essenziale ai sensi della Direttiva (UE) 2016/1148,*
- *o servizio di comunicazione elettronica ai sensi della Direttiva (UE) 2018/1972,*
- *o alla salute o all'incolumità personale.*

Sarà inoltre effettuata la revoca di un certificato di livello di base o sostanziale se previsto espressamente dallo specifico sistema europeo di certificazione.

Si condivide la posizione del Ministero dello sviluppo economico in merito all'opzione di riferimento proposta?*

Rispondere alla domanda utilizzando il riquadro sottostante:

Si, con le precisazioni riportate nel riquadro seguente

Si ritiene utile rappresentare ulteriori osservazioni in merito?

In tal caso riportare le proprie osservazioni nel riquadro di seguito:

A meno di diverse disposizioni nell'ambito cogente, la sospensione o revoca dei certificati viene effettuata dall'organismo di certificazione che ha sottoscritto ed emesso il certificato, come indicato nella norma ISO/IEC 17065 (§ 7.11).

Tali sospensioni o revoche possono avvenire nel caso in cui siano riscontrate da parte dell'organismo, delle non conformità sui prodotti da esso certificati, oppure nel caso che ACCREDIA riscontri non conformità o irregolarità nel processo di certificazione.

E' opportuno che ACCREDIA possa emettere ulteriori prescrizioni per il settore delle certificazioni in ambito EUCC, sotto forma di Circolari o Regolamenti Tecnici

2.6. Nella sezione 4.6 della SCHEDA INFORMATIVA è indicata la seguente opzione di riferimento:

***Opzione di riferimento**: La scelta di operare un cambio di regime di un sistema di certificazione da volontario ad obbligatorio sarà effettuata direttamente dall'autorità nazionale. Tale scelta potrebbe essere motivata dalla tutela di particolari interessi pubblici e sarà preceduta da una consultazione con i portatori di interesse. Infatti, se da una parte l'attività di certificazione dei prodotti TIC, servizi TIC e processi TIC conferisce un livello maggiore di affidabilità ai prodotti commercializzati e servizi erogati, dall'altro potrebbe comportare maggiori costi a carico dei fabbricanti/fornitori ed utilizzatori di prodotti TIC e servizi TIC, che siano cittadini, imprese o pubbliche amministrazioni. Inoltre, una certificazione obbligatoria in un determinato settore impegnerebbe maggiormente il sistema di vigilanza nazionale che dovrebbe monitorare un numero considerevolmente maggiore di emissioni di certificati rispetto ai numeri di un sistema volontario.*

Si condivide la posizione del Ministero dello sviluppo economico in merito all'opzione di riferimento proposta?*

Rispondere alla domanda utilizzando il riquadro sottostante:

Si condivide l'opzione proposta

Si ritiene utile rappresentare ulteriori osservazioni in merito?

In tal caso riportare le proprie osservazioni nel riquadro di seguito: