Agenzia per la Cybersicurezza Nazionale

Attuazione nazionale del

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)

Decreto Direttoriale recante "Organizzazione e procedure per lo svolgimento dei compiti dell'agenzia quale autorità nazionale di certificazione della cybersicurezza ex art. 7, comma 1, lettera e), del decreto – legge 14 giugno 2021, e 4, comma 2, del d. lgs. 3 agosto 2022, n. 123" (*integrazione ex articolo 15 del decreto legislativo 3 agosto 2022, n. 123*)

Organismo di Certificazione della Sicurezza Informatica

Linea Guida OCSI N. 3

Attività di valutazione ed emissione dei certificati per il sistema EUCC (art. 6 d.lgs. 123/2022)

Versione 1.0

3 febbraio 2025

REGISTRO DELLE VERSIONI

L'elenco delle versioni sarà mantenuto aggiornato in modo da riportare le modifiche apportate al presente documento.

Versione	Autore	Modifiche	Data
1.0	OCSI	Prima emissione	3 febbraio 2025

1. Indice

2. Acronimi

CC	Common Criteria
CCRA	CC Recognition Arrangement
CEI	Comitato Elettrotecnico Italiano
CEM	Common Evaluation Methodology
EAL	(Evaluation Assurance Level) Livello di garanzia della valutazione
EN	European Norm
EUCC	European Common Criteria Certification scheme
FW	Firmware
HW	Hardware
IEC	International Electrotechnical Commission
IPSec	Internet Protocol Security
ISO	International Organization for Standardization
IT	Information Technology
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
NOC	Nota dell'Organismo di Certificazione
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto Della Valutazione (TOE - Target of Evaluation)
PDV	Piano Di Valutazione
PP	Profilo di Protezione (Protection Profile)
RA	Rapporto di Attività
RAI	Rapporto di Analisi di Impatto
RAL	Riunione di Avvio dei Lavori
RAM	Random Access Memory
RC	Rapporto di Certificazione
RFV	Rapporto Finale di Valutazione
RO	Rapporto di Osservazione
ROA	Rapporto di Osservazione per Anomalia
ROE	Rapporto di Osservazione per Errore
ROS	Rapporto di Osservazione sullo Schema

	UNI	Ente Nazionale Italiano di Unificazione
	SOGIS	Senior Officials Group – Information Security
	SW	Software
	TCP	Transmission Control Protocol
	TDS	Traguardo di Sicurezza (ST - Security Target)
	TIC	Tecnologie dell'Informazione e della Comunicazione (ICT – Information and Communication Technology)
	UNI	Ente Nazionale Italiano di Unificazione
	VPN	Virtual Private Network

3. Scopo del documento

Il presente documento ha come scopo la definizione delle modalità operative dell'organismo di certificazione dell'autorità nazionale di certificazione della cybersicurezza designata per l'Italia ai sensi dell'articolo 58, paragrafo 1, del regolamento europeo sulla cybersicurezza ([CSA]) nell'ambito del sistema europeo di certificazione della cybersicurezza basato sui Common Criteria ([EUCC]).

L'autorità di certificazione della cybersicurezza in Italia è l'Agenzia per la cybersicurezza nazionale[1] ([ACN]), nel seguito indicata con il termine «Agenzia». L'organismo di certificazione dell'Agenzia è individuato nell'Organismo di certificazione della Sicurezza Informatica (OCSI)[2], stabilito inizialmente presso il Ministero delle comunicazioni ([OCSI])[3] e trasferito presso l'Agenzia per la cybersicurezza nazionale dal primo luglio 2022 ([TRNSF])[4].

L'OCSI è l'organismo di certificazione originariamente istituito per sovrintendere alle attività operative di valutazione e certificazione nell'ambito dello schema nazionale di certificazione della cybersicurezza basato sui Common Criteria ([OCSI]). Con l'entrata in vigore dell'EUCC, lo schema nazionale cessa di produrre i propri effetti[5], come altri schemi nazionali stabiliti in EU basati sui Common Criteria, venendo superato dalle nuove regole armonizzate stabilite dall'EUCC ([EUCC]).

La presente linea guida tratta in particolare delle **modalità operative per le attività di valutazione condotte dagli LVS e l'emissione di certificati dell'OCSI, nonché le attività successive di monitoraggio e gestione dei certificati e l'esecuzione di test da remoto** nell'ambito delle nuove regole europee armonizzate del sistema europeo di certificazione della cybersicurezza EUCC attuato in Italia.

Si evidenzia che per gli eventuali aspetti non trattati dalla presente linea guida che dovessero rientrare nell'ambito della stessa, si applicano le disposizioni contenute nel regolamento di esecuzione [EUCC].

[1] I compiti dell'autorità nazionale di certificazione della cybersicurezza in Italia sono assegnati all'Agenzia nazionale per la cybersicurezza (ACN) dall'articolo 7, comma 1, lettera e) del decreto-legge del 14 giugno 2021, n. 82 ([ACN]), la designazione dell'ACN quale autorità di certificazione della cybersicurezza è anche confermata dall'articolo 4, comma 1 del decreto legislativo 3 agosto 2022, numero 123 ([DLGS]).

[2] L'organismo di certificazione dell'autorità è individuato nell'OCSI dall'articolo 6, comma 1 del decreto legislativo 3 agosto 2022, numero 123 ([DLGS]).

[3] L'articolo 4 del Decreto del Presidente del consiglio dei ministri del 30 ottobre 2003 ([OCSI]) istituisce l'OCSI presso l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione del Ministero delle comunicazioni.

[4] Il Decreto del Presidente del consiglio dei ministri del 15 giugno 2022 ([TRNSF]), trasferisce l'OCSI presso l'Agenzia per la cybersicurezza nazionale dal primo luglio 2022, in attuazione dell'articolo 7, lettera e) del decreto-legge 14 giugno 2021, n. 82 ([ACN]).

[5] Le modalità di transizione degli schemi nazionali operativi in EU verso le regole armonizzate dell'EUCC sono stabilite nell'art. 49 di [EUCC].

4. Introduzione

L'OCSI, quale organismo di certificazione dell'Agenzia, nelle attività di rilascio dei certificati di cybersicurezza per l'EUCC si avvale di laboratori di prova denominati Laboratori per la Valutazione della Sicurezza (LVS) che interagiscono con l'OCSI, con il Committente della valutazione e con lo Sviluppatore del prodotto TIC[6] sottoposto a valutazione[7] nell'ambito del processo di certificazione.

La Linea Guida OCSI N. 3 ([LG3-OC]) definisce in primo luogo le modalità operative che devono essere seguite nel corso di un processo di valutazione supervisionato dall'OCSI, da parte dell'LVS abilitato[8], dal Committente e dallo Sviluppatore nell'ambito del sistema europeo di certificazione della cybersicurezza EUCC. Sono descritte, in particolare, le modalità secondo cui effettuare:

- le comunicazioni tra l'LVS, il Committente, lo Sviluppatore e l'OCSI nel corso del processo di valutazione;
- l'organizzazione e la pianificazione delle attività di una valutazione;
- il monitoraggio di una valutazione;
- la pubblicazione dei risultati di una valutazione;
- la segnalazione di anomalie.

Le modalità operative per la valutazione definite in questo documento sono applicabili alla valutazione della sicurezza di:

- un prodotto o un insieme di prodotti software, firmware e/o hardware per l'elaborazione elettronica delle informazioni, cioè l'Oggetto della Valutazione (ODV), così come definito nei Common Criteria [CC1], [CC2], [CC3], [CC4] e [CC5];
- un Profilo di Protezione (PP), cioè il documento che descrive per una certa categoria di ODV ed in modo indipendente dalla realizzazione, gli obiettivi di sicurezza, le minacce, l'ambiente ed i requisiti funzionali e di garanzia, definito nei Common Criteria [CC1], [CC2], [CC3], [CC4] e [CC5].

[6] Non sempre lo Sviluppatore del prodotto TIC coincide con il Committente della valutazione che richiede l'avvio del processo di valutazione all'OCSI. Nel caso in cui i due soggetti non coincidano in alcune attività del processo di valutazione è necessario il coinvolgimento anche dello Sviluppatore.

[7] Nell'ambito di un processo di certificazione il Committente di una valutazione è il soggetto che presenta la domanda di certificazione all'organismo di certificazione ingaggiando un LVS abilitato dall'OCSI, che normalmente sostiene i costi della certificazione e si impegna a cooperare con l'LVS nell'attività di valutazione. Il Committente, in alcuni casi, è un soggetto diverso dallo Sviluppatore che ha realizzato il prodotto da valutare. In tal caso l'LVS potrà dover interagire anche con lo Sviluppatore per l'esecuzione di alcune azioni di valutazione come ad esempio la visita ispettiva presso il sito o i siti di sviluppo del prodotto.

[8] Per l'abilitazione dell'LVS si rimanda alla [LG2-OC].

Le procedure di valutazione sono altresì applicabili a:

- una valutazione concomitante (cioè effettuata durante lo sviluppo di un ODV);
- una valutazione consecutiva (cioè effettuata dopo lo sviluppo di un ODV);
- una rivalutazione di un ODV o di un PP;
- il riuso dei risultati di una precedente valutazione di un ODV o di un PP.

La Linea Guida OCSI N. 3 ([LG3-OC]) descrive altresì le modalità per:

- il monitoraggio dei certificati successivamente alla loro emissione da parte dell'OCSI e del Titolare del certificato[9];
- la gestione delle non conformità di un certificato da parte dell'OCSI e del Titolare del certificato[10];
- il riesame del certificato per l'aggiornamento dell'analisi di vulnerabilità per un certificato dopo la sua emissione[11];
- il riesame di un certificato per stabilire se tale certificato e il relativo livello di garanzia possa estendersi a un ODV modificato o allo stesso ODV in ambiente di sviluppo modificato[12];
- l'applicazione di una *procedura di patch* ad un prodotto certificato in caso di vulnerabilità critica.[13]

La Linea Guida OCSI N. 3 ([LG3-OC]) fornisce infine le indicazioni da seguire nel caso in cui l'LVS richieda all'OCSI, attraverso giustificata richiesta, di poter effettuare le attività operative di valutazione (test di corretta implementazione e test di intrusione) da una postazione remota rispetto all'ODV e all'ambiente di test, connessa a questi ultimi attraverso la rete con modalità operative sicure e in grado di assicurare il pieno controllo dell'ambiente di test remoto e l'assenza di interferenze esterne sullo stesso.

[9] Articoli 25, 26 e 27 dell'[EUCC].
[10] Articoli 28, 29, 30, 31 dell'[EUCC].
[11] Articolo 13 e allegato IV.2 dell'EUCC].
[12] Articolo 13 e allegato IV.3 dell'[EUCC].
[13] Allegato IV.4 dell'[EUCC].

5. Ruolo e responsabilità dell'LVS nel processo di certificazione

5.1. Attività di valutazione ed altre mansioni

In questo capitolo sono descritti in dettaglio il ruolo e le responsabilità dell'LVS nel processo di valutazione e certificazione. Per quanto riguarda le altre parti coinvolte, si rimanda a quanto esposto nella [LG1-OC].

Il ruolo dei Valutatori, durante il corso di una valutazione, è quello di svolgere le azioni definite nei criteri di valutazione e di riportare all'OCSI i risultati dell'attività svolta, come descritto dettagliatamente nel seguito.

Oltre ad essere impegnato in una valutazione per l'OCSI, un LVS può svolgere altre mansioni. Esempi di tali attività non di valutazione svolte dall'LVS includono:

1. supporto all'OCSI (ad esempio relativamente alla definizione delle metodologie di valutazione);
2. addestramento;
3. produzione di Traguardi di Sicurezza e/o Profili di Protezione,
4. assistenza per la valutazione al Committente.

Tra queste, particolare importanza assume quella di assistenza per la valutazione al Committente.

5.2. Assistenza per la valutazione

A causa dell'elevata complessità del processo di valutazione, il Committente di una valutazione o lo Sviluppatore dell'ODV avrà a volte la necessità di richiedere l'assistenza di esperti, che potranno appartenere o meno a un LVS. L'assistenza da parte di un LVS può essere fornita prima che una valutazione inizi o in parallelo alla valutazione stessa.

L'assistenza può coprire ogni aspetto della valutazione: tipicamente consiste in assistenza al Committente per la stesura o la revisione di un TDS o di un PP e/o di ogni altra documentazione necessaria per la valutazione, oppure per stimare la probabilità di riuscita del processo di certificazione prima che lo stesso sia avviato.

L'ambito dell'assistenza durante la valutazione viene direttamente negoziato tra il Committente e l'LVS a cui è richiesta assistenza. L'OCSI lascia i dettagli contrattuali alle due parti in gioco, senza alcun coinvolgimento. Tuttavia, quando un LVS fornisce sia l'assistenza sia il servizio di valutazione per un particolare ODV o PP, è obbligato a comunicarlo all'OCSI definendo chiaramente l'ambito dell'assistenza e a dimostrare all'OCSI, mediante una analisi dei rischi ed eventuali misure di mitigazione adeguate, che l'assistenza fornita non influenzi l'indipendenza dei Valutatori e l'imparzialità della valutazione, assicurando che sia sempre rispettata la separazione e la distinzione tra le strutture e le persone che forniscono l'assistenza e quelle che effettuano la valutazione.

L'LVS deve informare l'OCSI di tutte le assistenze fornite prima dell'avvio della valutazione e che intende fornire durante la valutazione attraverso il piano di valutazione da approvare a cura dell'OCSI.

Nella sezione 6.4 della Linea Guida OCSI N. 2 ([LG2-OC]) sono dettagliate le possibili modalità di assistenza.

5.3. Trasmissione della documentazione

La trasmissione di documenti ufficiali tra l'OCSI, l'LVS e il Committente avviene con modalità protette al fine di garantire la riservatezza dei documenti e delle informazioni condivisi durante la valutazione. In particolare, le modalità di trasmissione[14] della documentazione e dei materiali attinenti ad una valutazione vengono concordate durante la Riunione di Avvio dei Lavori.

[14] Generalmente mediante l'utilizzo di crittografia asimmetrica.

6. Generalità sul processo di valutazione

6.1. Fasi del processo di valutazione

Un processo di valutazione corrisponde alle attività di valutazione svolte da un LVS su un singolo ODV o PP e comprende le seguenti fasi:

1. Preparazione;
2. Conduzione;
3. Conclusione.

La fase di preparazione vede coinvolti il Committente e l'LVS, che esamina il TDS o il PP del Committente e produce un Piano di Valutazione (PDV), dettagliando come sarà effettuata la valutazione.

L'LVS produce anche un elenco di materiali per la valutazione, individuando la documentazione necessaria e l'eventuale supporto richiesto allo Sviluppatore dell'ODV.

Prima di definire un rapporto contrattuale, il Committente e l'LVS possono contattare l'OCSI per discutere la possibilità di condurre la valutazione nell'ambito del sistema di certificazione EUCC ([EUCC]).

Una volta definito l'accordo tra LVS e Committente, quest'ultimo deve sottoporre all'OCSI la richiesta di iscrizione formale della valutazione nel sistema EUCC, allegando il TDS o il PP e il Piano di Valutazione (PDV) predisposto dall'LVS designato.

La fase di conduzione inizia quando l'OCSI, esaminata la domanda di iscrizione della valutazione ricevuta, approva il PDV e Traguardo di Sicurezza e accetta formalmente la valutazione nel sistema EUCC.

Nella fase di conclusione, l'LVS produce un Rapporto Finale di Valutazione (RFV) che riassume tutti i risultati ottenuti durante la valutazione. Esaminato l'RFV l'OCSI potrebbe richiedere chiarimenti, modifiche, integrazioni all'RFV e ad ulteriori documenti di valutazione necessari per l'approvazione dell'RFV.

Con l'approvazione dell'RFV, l'OCSI dichiara conclusa la valutazione da parte dell'LVS. L'RFV approvato viene utilizzato dall'OCSI come base per la stesura del Rapporto di Certificazione.

Maggiori dettagli sulle singole fasi vengono forniti nei paragrafi successivi.

6.2. Riservatezza del processo di valutazione

I Valutatori di un LVS sottoscrivono delle clausole di riservatezza con lo stesso LVS nel contratto di assunzione e, ove necessario, in accordi separati stabiliti per specifiche attività di valutazione.

Nell'ambito degli impegni contrattuali assunti dall'LVS relativamente alla riservatezza, l'LVS, avendo accesso a informazioni proprietarie relative a un ODV, è tenuto a sua volta a stabilire un accordo di riservatezza con il Committente e/o lo Sviluppatore. Tale accordo

copre tutte le attività svolte dai valutatori dell'LVS, sia presso la sede dell'LVS, sia quando in trasferta presso la sede del Committente o dello Sviluppatore. L'obiettivo di tale accordo è assicurare che i Valutatori dell'LVS impegnati nella valutazione non comunichino documenti o informazioni concernenti la loro attività ad alcuna terza parte non autorizzata a ricevere tali informazioni, all'interno o all'esterno dell'LVS.

Nel firmare un accordo di riservatezza, un LVS si impegna, in solido con i propri valutatori, a:

- usare le informazioni ottenute nel corso della valutazione soltanto ai fini della valutazione stessa;
- non divulgare tali informazioni ad alcuna terza parte se non espressamente autorizzato dal Committente o dallo Sviluppatore.

Oltre all'accordo di riservatezza tra l'LVS e il Committente/Sviluppatore, le informazioni su ciascun processo di valutazione devono essere controllate all'interno di uno stesso LVS sulla base della "necessità di conoscere".

Si noti che alcuni ambiti della valutazione potrebbero implicare la presenza di informazioni proprietarie dello Sviluppatore che questi non desidera siano comunicate al Committente o a qualsiasi altra parte tranne che all'LVS e all'OCSI. In questi casi è raccomandata la discussione della disciplina di tali informazioni nella Riunione di Avvio dei Lavori. Eventuali modifiche a queste decisioni possono essere apportate durante le Riunioni di Controllo della Valutazione.

I materiali per la valutazione sono gestiti, come materiale sensibile, in accordo al manuale di qualità dell'LVS verificato in fase di accreditamento.

L'OCSI, inoltre, protegge i documenti e le informazioni scambiate per e-mail o via PEC con Committente ed LVS durante una valutazione utilizzando cifratura asimmetrica, salvo diverso accordo con Committente ed LVS.

L'OCSI gestisce e tratta tutte le informazioni ottenute nel corso delle attività di certificazione in modo tale da garantirne la protezione della riservatezza.

6.3. Diritti di proprietà

Prima dell'inizio di una valutazione, l'LVS, il Committente e lo Sviluppatore determinano se il Committente o lo Sviluppatore potrà riservarsi eventuali diritti d'uso dei documenti prodotti durante la valutazione dall'LVS. Entrambe le parti devono inoltre considerare che l'OCSI può richiedere il riuso della documentazione prodotta dall'LVS nel corso di una valutazione allo scopo di rivalutare un ODV o un PP, o di riutilizzarla nella valutazione di un diverso ODV o PP.

È importante ricordare che sarà responsabilità del Committente della nuova valutazione fare in modo che i relativi rapporti, di cui fare riuso, siano forniti all'LVS che conduce la valutazione. Questo richiederà il rilascio di autorizzazioni da parte del detentore del diritto di proprietà, e di ogni altra parte con interessi commerciali.

A tal proposito, è bene evidenziare che con riferimento alle valutazioni composite:

- nel caso di un prodotto TIC sottoposto a una valutazione di prodotto composito conformemente ai pertinenti documenti sullo stato dell'arte dell'EUCC, l'LVS che ha effettuato la valutazione del prodotto TIC utilizzato nella composizione condivide le informazioni pertinenti con l'LVS che effettua la valutazione del prodotto TIC composito[15];
- inoltre, nel caso di un prodotto TIC sottoposto a una certificazione di prodotto composito, l'organismo di certificazione che ha effettuato la certificazione del prodotto TIC utilizzato nella composizione condivide le informazioni pertinenti con l'organismo di certificazione che effettua la certificazione del prodotto TIC composito[16];
- inoltre, se una vulnerabilità potenziale di un prodotto certificato interessa un prodotto composito, il titolare del certificato EUCC ne informa il titolare dei certificati EUCC da esso dipendenti.

Nelle attività di abilitazione e mantenimento degli LVS, l'OCSI assicura, per quanto di pertinenza, che i Laboratori per la Valutazione della Sicurezza applichino analoghi criteri di riservatezza e protezione alle informazioni da loro acquisite durante le attività di valutazione[17].

6.4. Lingua utilizzata

Per la produzione dei Verbali delle Riunioni, delle Note Informative dello Schema, dei Rapporti di Attività, del Rapporto Finale di Valutazione e delle comunicazioni tra OCSI, LVS, Committente e Sviluppatore, oltreché per tutti gli altri documenti prodotti nel corso del processo di certificazione è consentito anche l'uso della lingua inglese, in alternativa alla lingua italiana.

Viceversa, l'uso della lingua inglese è obbligatorio per le parti riportate integralmente dai criteri internazionali, quali ad esempio la formulazione dei requisiti funzionali e di garanzia definiti secondo i Common Criteria.

6.5. Gestione del contenzioso

Ogni controversia inerente alle attività di valutazione e certificazione deve essere riferita all'OCSI come indicato al capitolo 11 della LG1 ([LG1-OC]).

[15] Articolo 7, paragrafo 5 dell'[EUCC].
[16] Articolo 9, paragrafo 3 dell'[EUCC].
[17] Come riportato nell'LG2 nella sezione 5.6, l'eventuale comunicazione di documenti o informazioni riservate a terzi senza autorizzazione è causa di revoca dell'abilitazione rilasciata dall'OCSI.

7. Preparazione della valutazione

Gli obiettivi di questa fase sono:

- assicurare che tutte le parti coinvolte nella valutazione abbiano un'interpretazione comune dello scopo e dell'ambito della valutazione, e siano consapevoli delle loro responsabilità;
- determinare l'adeguatezza dei presupposti per la valutazione del TDS o del PP;
- determinare l'adeguatezza per la valutazione dei materiali disponibili;
- produrre un PDV e un elenco dei materiali per la valutazione.

Il primo passo in questa fase è compiuto dal Committente, che individua un LVS per lo svolgimento delle attività di valutazione, al quale consegna un TDS o un PP. Il Committente può richiedere all'LVS anche attività di assistenza, ad esempio per la stesura di un TDS o di un PP o di altra documentazione necessaria per la valutazione. In tal caso valgono le considerazioni fatte nella sezione 5.2.

L'ambito di questa fase è oggetto di accordo tra il Committente e l'LVS[18]. Tuttavia, se necessario, prima di definire un rapporto contrattuale, il Committente e l'LVS possono contattare, sia pure in modo informale, l'OCSI per accertare la possibilità di condurre la valutazione nel sistema EUCC.

7.1. Relazioni tra Committente e Sviluppatore

È responsabilità del Committente assicurarsi che lo Sviluppatore sia in grado di fornire i materiali per la valutazione richiesti.

L'LVS deve controllare che il Committente e lo Sviluppatore siano pienamente a conoscenza:

- del processo di valutazione;
- delle esigenze di sicurezza delle informazioni del Committente e di quelle dello Sviluppatore;
- del ruolo dell'LVS;
- dell'esigenza di garantire, laddove previsto, l'accesso ai siti di sviluppo al personale valutatore dell'LVS e, ove richiesto, dello stesso OCSI;
- delle loro responsabilità durante tutta la valutazione.

L'LVS deve assicurarsi che il Committente e lo Sviluppatore abbiano concordato contrattualmente la fornitura dei materiali per la valutazione e che siano state considerate

[18] L'accordo potrebbe includere anche lo Sviluppatore, se distinto dal Committente, ad es. per individuare particolari clausole di riservatezza in merito ai materiali e informazioni acquisite e relativa condivisione con il Committente o per regolare le modalità di accesso ai siti di sviluppo dell'ODV.

le conseguenze sull'andamento della valutazione di eventuali condizioni particolari che potrebbero causare ritardi nello svolgimento delle attività previste.

7.2. Richiesta di iscrizione della valutazione nel sistema

Affinché una valutazione sia formalmente accettata nel sistema EUCC, il Committente deve sottoporre una richiesta all'OCSI, utilizzando il modulo predisposto disponibile sul sito web dell'ACN.

Al modulo, compilato nella sua interezza, devono essere obbligatoriamente allegati il TDS o il PP e il PDV predisposto dall'LVS designato dal Committente.

Una volta ricevuta la richiesta, l'OCSI esamina la documentazione allegata per verificare l'assenza di elementi che possano pregiudicare il buon esito della valutazione.

In particolare, l'OCSI verifica che il PDV contenga la descrizione di tutte le attività che i Valutatori eseguiranno durante la valutazione e le modalità secondo le quali queste attività risultano organizzate, pianificate nel tempo, correlate e suddivise nell'ambito del periodo di valutazione.

L'OCSI inoltre verifica la congruità delle risorse e delle tempistiche previste dall'LVS per la conduzione della valutazione con il livello di garanzia richiesto e con la natura e la complessità del prodotto da valutare, descritto nel relativo TDS, o del PP.

Se non sussistono motivi ostativi per l'accoglimento della richiesta, entro trenta giorni dalla ricezione della richiesta l'OCSI approva il PDV e iscrive la valutazione nel sistema EUCC, designando il responsabile del procedimento, che fungerà da referente della certificazione verso il Committente e l'LVS. L'OCSI comunica tale decisione simultaneamente al Committente e all'LVS, che può quindi avviare le attività di valutazione.

Nel caso in cui l'OCSI rilevi la presenza di potenziali problemi nella documentazione esaminata, richiede al Committente e/o all'LVS le necessarie integrazioni e correzioni. Tale richiesta sospende, fino alla ricezione della documentazione aggiornata, il decorso del suddetto termine fino a trenta giorni.

7.3. Piano di Valutazione (PDV)

Il PDV deve descrivere le attività previste per il processo di valutazione, fornendo sufficienti dettagli per poter monitorare lo stato di avanzamento del processo di valutazione per ciascuna attività prevista.

Il PDV deve essere redatto tenendo conto di tutte le informazioni presenti nel TDS o nel PP, seppur alcune informazioni relative ad aspetti della valutazione risulteranno disponibili solo durante la fase di conduzione.

Il PDV deve includere l'elenco del personale valutatore abilitato coinvolto nella valutazione, con il relativo ruolo e profilo (livello sostanziale o livello elevato) ed eventuali esperti esterni coinvolti nella valutazione per uno specifico dominio tecnologico o prodotto TIC. Il PDV deve obbligatoriamente includere una descrizione delle eventuali

attività di assistenza in aggiunta alle attività di valutazione, prestate al Committente prima dell'avvio della valutazione e che intende eventualmente condurre durante la valutazione, specificando il personale impegnato e le modalità, con un'analisi dei rischi per l'imparzialità (rif. sezione 6.4 della [LG2-OC]).

Nel corso di una valutazione, potrebbe essere necessario emendare alcune parti di un PDV, ad esempio, nei seguenti casi:

- l'ODV viene modificato durante la valutazione (per il rilascio di una nuova versione di un prodotto o perché alcuni problemi sono stati eliminati);
- il Committente non fornisce i materiali per la valutazione nel formato e nel modo concordati, o non rispetta i tempi di esecuzione stabiliti.

Tutte le variazioni apportate a un PDV devono essere trasmesse in modo formale all'OCSI, che provvede a ricalcolare ove necessario gli oneri dovuti in tutti quei casi in cui gli oneri dovuti all'OCSI sono calcolati in dipendenza dell'impegno giornaliero (giorni persona) stimati dal laboratorio. Le variazioni al PDV saranno inserite nelle registrazioni della specifica certificazione.

Mentre il primo PDV allegato alla domanda di registrazione di una nuova valutazione è soggetto ad esplicita approvazione da parte dell'OCSI, le versioni del PDV successive all'avvio della valutazione e comunicate all'OCSI sono approvate dall'OCSI per silenzio assenso entro 30 giorni dall'invio del PDV aggiornato. Entro lo stesso termine l'OCSI, ove ritenga opportuno rettificare il PDV, comunicherà all'LVS eventuali rilievi sul PDV comunicato e ne richiederà ove necessario un aggiornamento.

Durante una valutazione, l'LVS, di comune accordo con il Committente, potrebbe effettuare attività non incluse nel piano di valutazione. Ad esempio, i Valutatori possono effettuare attività opzionali, quali ispezioni al sito di sviluppo dell'ODV, da riutilizzare in future rivalutazioni dell'ODV con livelli di garanzia superiori.

LVS potrebbe inoltre voler omettere l'esecuzione di alcune attività di valutazione, come ad esempio la visita ispettiva presso un sito di sviluppo già visitato di recente.

È importante che qualsiasi attività aggiuntiva o da omettere, come quelle sopra indicate, sia chiaramente identificata come tale e approvata in anticipo dall'OCSI a fronte di una richiesta dell'LVS.

7.4. Elenco dei materiali per la valutazione

Affinché i Valutatori possano effettuare le singole azioni specificate nel PDV, devono avere a disposizione i materiali per la valutazione richiesti. I criteri di valutazione forniscono un elenco dei materiali per la valutazione per ciascun livello di garanzia. Questo elenco deve essere dettagliato dai Valutatori per ogni specifica valutazione, e di norma fa parte integrante del PDV.

I materiali per la valutazione possono comprendere:

- gli elementi *hardware*, *firmware* o *software* che costituiscono l'ODV;
- la documentazione per l'utente dell'ODV;

- la documentazione tecnica di supporto, generata durante lo sviluppo dell'ODV o per sostenere il processo di valutazione.

Sono considerati materiali per la valutazione anche:

- il supporto tecnico dello Sviluppatore;
- l'accesso al sito in cui è in esercizio l'ODV;;
- l'accesso al sito di sviluppo dell'ODV.

Si evidenzia che l'accesso al sito di sviluppo da assicurare per l'esecuzione di una visita *in loco* può richiedere un accordo preventivo tra Sviluppatore, Committente ed LVS. L'accesso al sito di sviluppo da parte dell'LVS e dell'OCSI deve essere sempre garantito se richiesto dalle attività di valutazione previste per il pacchetto di garanzia selezionato.[19]

[19] In caso di componenti di garanzia ALC_DVS.1 o ALC_DVS.2 è necessario permettere una visita ispettiva al sito di sviluppo dell'ODV.

8. Conduzione della valutazione

Gli obiettivi di questa fase sono avviare la valutazione, assicurare che siano effettuati gli appropriati controlli e svolgere l'attività di valutazione tecnica, registrando il lavoro eseguito, le osservazioni fatte ed i risultati ottenuti in modo tale che:

- sia dimostrato che l'attività è stata effettuata nel rispetto dello standard Common Criteria, delle Linee Guida dell'OCSI e del PDV;
- sia dimostrato che l'attività è stata effettuata in modo obiettivo e imparziale;
- i risultati siano ripetibili e riproducibili;
- sia fornita sufficiente evidenza per giustificare le conclusioni dei Valutatori.

8.1. Avvio del processo di valutazione

8.1.1. Riunione di Avvio dei Lavori

Dopo l'approvazione formale del PDV, l'OCSI convoca una Riunione di Avvio dei Lavori (RAL), durante la quale vengono affrontati diversi argomenti, quali ad esempio:

- identificazione dei responsabili della valutazione per conto del Committente e dell'LVS, e se del caso, dello Sviluppatore;
- identificazione dei componenti del gruppo di certificazione designati dall'OCSI;
- accordo di certificazione (sez. 10 di [LG1-OC]);
- precisazioni sui contenuti del TDS o del PP;
- precisazioni sui contenuti del PDV;
- gestione di documenti garantendone la riservatezza;
- organizzazione dei materiali per la valutazione;
- aspetti riguardanti il personale designato dall'LVS per la valutazione;
- vincoli sulla valutazione (ad esempio limitazioni sull'accesso a determinate aree o sui contatti con lo Sviluppatore e/o il Committente);
- comunicazione da parte dell'LVS della data di inizio effettivo della valutazione;
- riutilizzazione di risultati di precedenti valutazioni;
- frequenza delle Riunioni di Controllo della Valutazione;
- modalità di trasmissione della documentazione e dei materiali prodotti durante la valutazione.

L'organizzazione della Riunione di Avvio dei Lavori è responsabilità dell'OCSI, che è anche responsabile per la produzione e la distribuzione dell'ordine del giorno e del successivo verbale.

Alla Riunione di Avvio dei Lavori partecipano, oltre all'OCSI stesso, l'LVS e il Committente (di solito i rispettivi responsabili designati per la valutazione). Vista l'importanza di tale riunione, potrebbe rendersi opportuno o necessario invitare anche lo Sviluppatore, se distinto dal Committente.

8.1.2. Inserimento nell'elenco dei prodotti e PP in valutazione

Un ODV o un PP in valutazione può essere incluso nell'elenco dei prodotti, sistemi e PP in valutazione, pubblicato sul sito web dell'ACN, previo consenso del Committente. Se un ODV o un PP in valutazione è inserito nell'elenco, ma la valutazione viene sospesa o annullata, l'OCSI rimuove l'ODV o PP dall'elenco.

8.2. Materiali per la valutazione

Per poter effettuare le Attività di valutazione, i Valutatori devono avere a disposizione i materiali per la valutazione richiesti.

Per una valutazione consecutiva, tutti i materiali sono normalmente disponibili all'inizio della valutazione.

Per una valutazione concomitante, la tempistica delle attività di valutazione dipende dai tempi di sviluppo dell'ODV. Lo slittamento delle tappe fondamentali di tale sviluppo ha inevitabilmente un impatto sui tempi di esecuzione della valutazione. Affinché il Valutatore possa modificare di conseguenza la pianificazione delle attività di valutazione, è necessario uno stretto raccordo con lo Sviluppatore.

Un ritardo nella data di rilascio di un materiale per la valutazione può avere diverse conseguenze sui tempi di esecuzione della valutazione stessa. L'LVS può, ad esempio:

- sospendere soltanto la singola attività interessata dal ritardo (se attuabile) e procedere con un'altra attività,
- sospendere la valutazione finché il materiale richiesto non sia disponibile.

I cambiamenti nei tempi di esecuzione della valutazione sono materia contrattuale tra l'LVS e il Committente. Tuttavia, poiché tali cambiamenti potrebbero avere un impatto sulle risorse di certificazione disponibili, l'LVS deve avvisare l'OCSI sui ritardi e sulle modifiche proposte nelle tappe fondamentali del processo di valutazione. La non disponibilità o i ritardi nel rilascio dei materiali per la valutazione può condurre alla produzione di un Rapporto di Osservazione.

8.3. Rapporti di Osservazione (RO)

Durante una valutazione, i Valutatori possono rilevare vari problemi relativi all'ODV o al PP. Alcuni di questi problemi possono consistere specificamente in vulnerabilità sfruttabili, mentre altri possono riferirsi ad anomalie più generali (riguardanti, ad esempio, l'ambiente di sviluppo o la documentazione operativa). Qualunque sia il problema, è essenziale che riceva un'appropriata e pronta attenzione dalle parti interessate.

Tutti i problemi riscontrati nel corso del processo di valutazione, devono essere riportati dai Valutatori sotto forma di Rapporti di Osservazione.

Per facilitare la supervisione da parte dell'OCSI dell'attività di valutazione, sono usati due tipi di Rapporti di Osservazione:

- Rapporto di Osservazione per Errore (ROE);
- Rapporto di Osservazione per Anomalia (ROA).

8.3.1. Rapporti di Osservazione per Errore (ROE)

Un ROE viene prodotto quando si identifica, in qualsiasi momento della valutazione, una vulnerabilità, anche se solo potenziale. Tale rapporto è da considerarsi estremamente importante, poiché in caso di vulnerabilità sfruttabile non risultano più soddisfatti gli obiettivi di sicurezza previsti nel TDS.

I ROE non devono essere usati per riportare altri problemi relativi alla sicurezza dell'ODV diversi dalle vulnerabilità.

L'emissione di un ROE comporta una successiva attività di analisi di vulnerabilità volta ad accertare se esistano vulnerabilità realmente sfruttabili. In particolare, una vulnerabilità sfruttabile è confermata dall'OCSI sulla base dell'analisi condotta dall'LVS e comporta un'interruzione della valutazione con esito negativo. Va tuttavia osservato che la stessa potrà essere riavviata a seguito di modifiche del TDS, con un diverso ambito dell'ODV e problema di sicurezza, concordate con il Committente. Pertanto, si raccomanda all'LVS a seguito dell'emissione di un ROE di eseguire le sole attività di valutazione riguardanti la classe AVA e sospendere le altre attività in attesa degli esiti dell'analisi di vulnerabilità per la chiusura del ROE.

L'invio del ROE al Committente deve essere preventivamente autorizzato dall'OCSI.

8.3.2. Rapporti di Osservazione per Anomalia (ROA)

Il ROA deve essere usato per riportare tutti i problemi relativi all'ODV o al PP diversi dalle vulnerabilità. Questo copre un'ampia tipologia di problemi, quali ad esempio:

- problemi riguardanti lo sviluppo o la gestione dell'ODV;
- problemi riguardanti il contenuto, la presentazione e l'evidenza di materiali per la valutazione;
- problemi che possono avere un impatto sulla sicurezza.

Ci sono casi in cui i Valutatori necessitano di chiedere chiarimenti di minore entità su documenti del Committente. In tali casi, può non essere appropriato usare i ROA, ma utilizzare invece comunicazioni per e-mail con il Committente e/o con lo Sviluppatore, a seconda dei casi, evidenziando la necessità di una risposta tempestiva. Di tali comunicazioni dovrà in ogni caso essere tenuta traccia conservandone l'occorrenza e il contenuto, dandone evidenza, ove richiesto, all'OCSI.

In caso di dubbio sull'opportunità di emettere un ROA, dovrebbe essere consultato l'OCSI.

8.3.3. Procedure di emissione

I Valutatori possono produrre un Rapporto di Osservazione in ogni momento durante la valutazione. Un Rapporto di Osservazione può essere usato per descrivere un singolo problema o più problemi tra loro collegati.

I Rapporti di Osservazione devono essere firmati dal Valutatore che ha riscontrato il problema e dal responsabile per la valutazione dell'LVS.

I ROA devono essere distribuiti al Committente e all'OCSI simultaneamente, mentre i ROE devono essere inviati per la revisione all'OCSI prima di essere consegnati al Committente e se necessario allo Sviluppatore. Solo se l'OCSI ne autorizza la condivisione, i ROE saranno consegnati anche al Committente.

8.3.4. Azioni susseguenti ad un ROA

Nel caso in cui venga emesso un ROA, il Committente intraprende le azioni necessarie a risolvere tempestivamente il problema sollevato.

Una volta individuate le azioni e le contromisure proposte per la risoluzione del problema sollevato, il Committente dovrà emettere la risposta al ROA, che verrà inviata contemporaneamente all'LVS e all'OCSI assieme ai materiali di valutazione opportunamente corretti.

8.3.5. Azioni susseguenti ad un ROE

Il ROE richiede in generale un diverso trattamento rispetto ai ROA. Inizialmente il ROE è trasmesso solo all'OCSI e classifica le vulnerabilità riscontrate come potenziali o direttamente come sfruttabili. Per le vulnerabilità potenziali, l'LVS porta avanti un'analisi di vulnerabilità che ha lo scopo di determinare se le vulnerabilità identificate siano sfruttabili o non sfruttabili.

Per la conferma di una vulnerabilità sfruttabile è richiesta in generale l'esecuzione di un test di intrusione. Tuttavia, non è necessario dimostrare che le vulnerabilità siano sfruttabili tramite una prova di intrusione nel caso di vulnerabilità già note che interessino effettivamente funzioni di sicurezza dell'ODV. Per stabilire se una vulnerabilità nota non si applichi all'ODV sarà richiesta in generale un'analisi della documentazione di sviluppo e, se necessario, eventuale richiesta di chiarimento o integrazione della stessa al Committente[20].

[20] Ad esempio, si può dimostrare che una vulnerabilità nota non si applica all'ODV, nel caso in cui l'ODV utilizza una libreria di terze parti che ha delle vulnerabilità note e però si può dimostrare, mediante ispezione del codice sorgente o attraverso altre verifiche, che l'ODV non richiama la specifica funzione vulnerabile.

Più in generale, laddove per determinare se una vulnerabilità potenziale sia realmente sfruttabile, l'LVS ritenga necessario acquisire chiarimenti o evidenze aggiuntive dal Committente, l'LVS propone all'OCSI la condivisione del ROE con il Committente. Il ROE è inviato al Committente solo se l'OCSI ne autorizza l'invio.

Nel caso in cui una vulnerabilità potenziale sia confermata come sfruttabile, o viceversa come non sfruttabile, a seguito, dell'analisi della documentazione, di ulteriori elementi forniti dal Committente o a seguito di una prova di intrusione, il ROE prodotto dovrà essere aggiornato, modificando lo stato della vulnerabilità da potenziale a sfruttabile o non sfruttabile.

Inoltre, nel caso di vulnerabilità sfruttabile, l'LVS condurrà un'analisi del potenziale di attacco necessario per sfruttare la vulnerabilità, in modo da stabilire se la vulnerabilità sfruttabile richieda un potenziale di attacco superiore rispetto al livello di resistenza ad attacchi per il quale è richiesta la certificazione dell'ODV. Le vulnerabilità identificate inizialmente come sfruttabili ma con potenziale di attacco al di sopra di tale livello saranno riclassificate come residue.

Pertanto, l'analisi delle vulnerabilità potrebbe portare in generale a concludere che:

- una o più vulnerabilità identificate nel ROE sono effettivamente sfruttabili e non può essere emesso il certificato sulla base del TDS in valutazione, pertanto, la valutazione termina con esito negativo oppure si procede ad una modifica del TDS, ad esempio aggiornando le assunzioni dell'ambiente operativo, oppure eleminando o aggiornando alcuni componenti funzionali o di garanzia;
- sebbene sfruttabili, le vulnerabilità identificate sono da ritenersi residue, ovvero sfruttabili ma solo con un potenziale d'attacco superiore rispetto a quello corrispondente al livello di resistenza agli attacchi richiesto per la certificazione dell'ODV; in tal caso l'ODV sarà certificabile rispetto al TDS valutato ma nel rapporto di certificazione sarà data tuttavia menzione di vulnerabilità residue individuate durante la valutazione;
- le vulnerabilità identificate sono da ritenersi non sfruttabili perché non interessano le funzioni di sicurezza dell'ODV.

8.4. Rapporti di Attività (RA)

L'LVS predispone un Rapporto di Attività (RA) che riassume i risultati delle analisi condotte per quella specifica attività, indicando anche se sono stati impiegati metodi di valutazione e/o di sviluppo che presentano carattere innovativo. Tali Rapporti vengono di norma inviati all'OCSI al termine di ciascuna attività o nel momento in cui occorre sospendere un'attività per acquisire chiarimenti o azioni correttive sui materiali di valutazione da parte del Committente o più in generale ogniqualvolta sia necessario emettere un ROE o un ROA. In tal caso, LVS emetterà un RA nel quale evidenzierà le unità di lavoro della [CEM] non passate o non concluse, anche per assenza di materiali da parte del Committente, in relazione alle note riportate nel ROE o ROA.

Le modalità di emissione degli RA possono essere concordate nella Riunione di Avvio dei Lavori. Tuttavia, come regola generale, in una valutazione di un prodotto ICT, è bene

dedicare in una prima parte della valutazione alla verifica del TDS ed alle altre attività di verifica documentale, riservando alle attività di test una fase successiva della valutazione in cui trarre pieno profitto di quanto consolidato nella fase di analisi documentale.

È richiesto, inoltre, che l'analisi di vulnerabilità e relativi test di intrusione siano eseguiti entro un mese dalla consegna dell'RFV.

8.5.Note dell'Organismo di Certificazione (NOC)

Qualora lo ritenga necessario, l'OCSI può emettere autonomamente, in qualsiasi fase della valutazione, una Nota dell'Organismo di Certificazione (NOC), rivolta all'LVS e/o al Committente. Una NOC contiene indicazioni dell'OCSI relativamente alle attività svolte nel corso di quella specifica valutazione, quali ad esempio i problemi esposti in un ROA/ROE, il corretto svolgimento di un'attività, la corretta interpretazione delle norme, ecc.

8.6. Rapporti di Osservazione sul Sistema (ROS)

Tutti gli LVS possono fare osservazioni sull'attuazione del sistema [EUCC], anche se non coinvolti in processi di valutazione. Ad esempio, possono essere segnalati:

- difficoltà di applicazione delle regole dell'EUCC;
- problemi di interpretazione dei criteri di valutazione o dell'EUCC;
- problemi circa l'applicabilità di un particolare metodo di valutazione;
- tecniche di valutazione, strumenti o procedure interessanti o innovative.

Le segnalazioni sono inviate all'OCSI sotto forma di Rapporto di Osservazione sul Sistema (ROS). In tale rapporto dovrebbe anche essere proposta una soluzione per il problema rilevato.

L'OCSI, esaminato il ROS, adotterà una soluzione che sarà oggetto di una Nota dell'Organismo di Certificazione (NOC), rivolta all'LVS che ha prodotto il ROS.

Nei casi in cui il problema sia di interesse generale, la soluzione adottata dall'OCSI potrà essere oggetto di aggiornamento della Linea Guida.

8.7. Riunioni di Controllo della Valutazione

Le Riunioni di Controllo della Valutazione sono un'occasione per l'LVS e l'OCSI (ed eventualmente il Committente e/o lo Sviluppatore) per discutere l'attività tecnica dettagliata relativa ad una particolare valutazione, revisionare lo stato di avanzamento ed i tempi di esecuzione del processo di valutazione, individuare e discutere i problemi e attivare le azioni appropriate. Tali riunioni possono essere tenute periodicamente durante il corso della valutazione o possono essere convocate 'ad hoc' per discutere un particolare problema (individuato, ad esempio, in un ROA).

La pianificazione delle Riunioni di Controllo della Valutazione dovrebbe essere concordata all'inizio della valutazione nella Riunione di Avvio dei Lavori. Tuttavia, tale programmazione può essere modificata nel corso della valutazione.

Le Riunioni di Controllo della Valutazione possono essere convocate dall'OCSI, autonomamente o su richiesta dell'LVS o del Committente.

8.7.1. Partecipanti

Alla Riunione di Controllo della Valutazione partecipano uno o più rappresentanti dell'OCSI e dell'LVS (almeno i rispettivi responsabili designati per la valutazione). Altri partecipanti, quali il Committente e/o lo Sviluppatore, possono essere invitati se necessario. Il Committente può infatti desiderare che anche lo Sviluppatore sia invitato a partecipare ad alcune o a tutte le riunioni.

L'organizzazione della Riunione di Controllo della Valutazione è responsabilità dell'OCSI, che è anche responsabile per la produzione e la distribuzione dell'ordine del giorno e del successivo verbale.

9. Conclusione della valutazione

Nella fase di conclusione l'LVS produce il Rapporto Finale di Valutazione (RFV), in cui vengono riportati i verdetti e le considerazioni svolte dai Valutatori.

In via preferenziale, l'RFV dovrebbe consistere in un documento che riporta in forma sintetica i risultati riportati per esteso negli RA, referenziando gli stessi per eventuali approfondimenti.

In linea di massima, i contenuti minimi di un RFV dovrebbero essere i seguenti:

- un "Executive Summary" che, in massimo una pagina, riporta la sintesi dell'intero documento;
- una chiara indicazione della specifica configurazione dell'ODV valutata;
- le modalità di consegna, installazione e configurazione dell'ODV verificate dal laboratorio per la gestione e l'utilizzo sicuro dell'ODV a beneficio dell'utente finale;
- i principali punti di attenzione concernenti l'ODV e/o la valutazione, gli eventuali motivi di ritardo, i problemi più rilevanti riscontrati e le relative azioni di mitigazione intraprese;
- le informazioni di base sui risultati della valutazione, a beneficio dell'OCSI;
- le procedure di valutazione adottate, con riferimento al PDV, motivandone gli eventuali scostamenti;
- un riassunto dei risultati della valutazione in termini di Attività di valutazione, così come riportate nei corrispondenti capitoli del PDV;
- i siti di sviluppo ispezionati dall'LVS;
- una sintesi dei test funzionali dello Sviluppatore e dei test funzionali indipendenti dell'LVS;
- una sintesi dei test d'intrusione dell'LVS e delle eventuali vulnerabilità residue riscontrate;
- una tabella riassuntiva con i verdetti sui componenti di garanzia verificati;
- una lista dei ROA/ROE emessi nel corso della valutazione.

L'RFV viene emesso dall'LVS al termine della valutazione e inviato esclusivamente all'OCSI, che lo revisiona per accertare che fornisca un adeguato riassunto dei risultati della valutazione.

L'RFV viene usato dall'OCSI come base per la produzione del Rapporto di Certificazione.

10. Preparazione ed emissione del certificato

La fase di certificazione prevede, nella sua parte iniziale, la revisione dell'RFV da parte dell'OCSI. Terminata questa parte con esito favorevole, l'OCSI è nella condizione di produrre il Rapporto di Certificazione e il Certificato. Nel seguito vengono descritti gli adempimenti e le attività che l'OCSI, interagendo con l'LVS e il Committente, svolgerà in questa fase.

10.1. Ruolo dell'LVS nella fase di certificazione

Il ruolo dell'LVS durante la fase di certificazione è quello di fornire supporto tecnico all'OCSI nella revisione dell'RFV e nella produzione del Rapporto di Certificazione. Ad esempio, questo supporto potrebbe coinvolgere i Valutatori nel:

- fornire accesso a specifiche dimostrazioni tecniche (ad esempio materiali per la valutazione, risultati ottenuti grazie all'utilizzo di specifici strumenti) per supportare le conclusioni dei Valutatori;
- fornire eventuali chiarimenti sui contenuti degli RA e dell'RFV;
- revisionare la bozza del Rapporto di Certificazione per assicurare che sia tecnicamente accurato, contenga solo informazioni liberamente pubblicabili e sia un adeguata rappresentazione dell'ODV o del PP e dell'RFV.

10.2. Esame del Rapporto Finale di Valutazione

Quando l'OCSI riceve l'RFV dall'LVS, lo revisiona per determinare se soddisfi i requisiti del sistema EUCC e dei criteri di valutazione. Se tale revisione dà esito positivo, l'RFV viene approvato entro trenta giorni dalla sua ricezione.

Qualora nell'RFV vengano individuate delle anomalie risolvibili, l'OCSI ne richiede all'LVS la correzione tramite l'emissione di una NOC. In tal caso, l'LVS è tenuto a reinviare un nuovo rapporto entro i successivi trenta giorni.

Sul nuovo RFV l'OCSI si pronuncerà entro trenta giorni.

10.3. Rapporto di Certificazione

Entro trenta giorni dall'approvazione dell'RFV, l'OCSI redige una bozza di Rapporto di Certificazione (RC) che invia all'LVS e al Committente per avere conferma dell'assenza di errori materiali, nonché dell'assenza di elementi che contengano informazioni ritenute confidenziali e quindi non liberamente pubblicabili. L'LVS e il Committente si pronunciano sulla richiesta entro i successivi cinque giorni lavorativi.

Acquisita la conferma da parte dell'LVS e del Committente, o decorso inutilmente il termine per la loro pronuncia, l'OCSI emette entro i successivi trenta giorni il Rapporto di Certificazione. Tale rapporto riassume i risultati della valutazione e contiene commenti e raccomandazioni da parte dell'OCSI. L'RC deve contenere esclusivamente informazioni liberamente pubblicabili, e può essere reso pubblico solo integralmente.

I contenuti minimi del Rapporto di Certificazione devono includere le informazioni riportate nell'Allegato V dell'EUCC ([EUCC]).

Inoltre, nel rapporto l'OCSI deve:

- dichiarare che la valutazione è stata condotta secondo i criteri e la metodologia prevista del sistema EUCC;
- dichiarare che il Profilo di Protezione o il Traguardo di Sicurezza è completo, congruente e tecnicamente corretto;
- dichiarare che l'Oggetto della Valutazione soddisfa il Traguardo di Sicurezza al livello di garanzia richiesto;
- menzionare la presenza di eventuali vulnerabilità residue ed eventualmente raccomandare delle misure per il successivo monitoraggio o rimozione.

Nei casi di valutazioni di ODV particolarmente complessi, i termini di cui sopra possono essere differiti, d'intesa con le parti. Ai fini della decorrenza dei termini non è computato il tempo richiesto per il riscontro ad eventuali osservazioni e chiarimenti.

10.4. Emissione del Certificato

In caso di valutazione conclusa positivamente, l'OCSI allega all'RC il relativo Certificato, cioè l'attestazione che l'ODV o il PP è stato valutato da un LVS in conformità con i criteri di valutazione e con le procedure del sistema EUCC. Il Certificato si applica soltanto alla specifica versione dell'ODV o del PP nella configurazione valutata ed attesta che il livello di garanzia richiesto è stato raggiunto. Per i dettagli si fa esplicito riferimento al TDS o al PP e all'RC.

I contenuti minimi da garantire nel certificato sono riportati nell'Allegato VII dell'EUCC ([EUCC]).

Nel certificato è referenziato l'identificatore del Rapporto di Certificazione, che individua l'ambito e le condizioni di validità del certificato.

I certificati emessi dall'OCSI hanno validità massima di 5 anni dalla data di emissione, fatte salve eventuali proroghe concesse dall'Agenzia.[21]

10.5. Lingua utilizzata

Per permettere la pubblicazione delle informazioni sul processo di certificazione in lingua inglese sul sito web di ENISA[22]:

[21] Articolo 12 dell'[EUCC].
[22] L'articolo 42, paragrafo 1 dell'[EUCC] stabilisce che sul sito web di ENISA dovranno essere pubblicata almeno in lingua inglese documentazione e informazioni per ciascun processo di certificazione, fra cui il certificato ed il rapporto di certificazione.

- il certificato emesso a valle del processo di certificazione dall'OCSI sarà bilingue italiano e inglese;
- il rapporto di certificazione con validità legale, che specifica l'ambito e le condizioni di applicabilità del certificato, sarà emesso in lingua italiana;
- sarà inoltre emesso un rapporto di certificazione in lingua inglese come traduzione di cortesia del rapporto di certificazione in lingua italiana con validità legale.

11. Chiusura di un processo di certificazione

Il processo di valutazione ha termine con l'approvazione dell'RFV emesso dall'LVS.

La chiusura formale del processo di certificazione avviene con l'emissione del Rapporto di Certificazione e del Certificato e con la relativa pubblicazione.

L'OCSI può convocare una riunione di chiusura della certificazione, eventualmente su richiesta dell'LVS o del Committente.

11.1. Riunione di Chiusura della Certificazione

Gli obiettivi di una Riunione di Chiusura della Certificazione possono essere:

- consentire alle organizzazioni coinvolte nella valutazione di esprimere una opinione sulla conduzione complessiva della valutazione;
- fornire all'LVS commenti sulla sua esecuzione della valutazione;
- rappresentare ogni esperienza maturata nella valutazione;
- accordarsi sull'assegnazione dei materiali del processo di valutazione;
- estendere il periodo di tempo oltre i 5 anni[23] in cui i materiali archiviati dovranno essere conservati.

Per l'individuazione dei partecipanti alla riunione si adottano i seguenti criteri:

- partecipano di norma i responsabili per la valutazione designati da ciascuna organizzazione coinvolta nella valutazione;
- a discrezione dell'OCSI e in consultazione con l'LVS, possono essere invitati altri partecipanti, quali ad esempio il Committente ed altri Valutatori dell'LVS.

L'OCSI sarà responsabile della produzione e della distribuzione dell'agenda della riunione e del successivo verbale.

11.2. Pubblicazione nell'elenco dei prodotti, sistemi e PP certificati

A seguito dell'emissione del Rapporto di Certificazione e del Certificato, l'OCSI inserisce nell'elenco dei prodotti e i PP certificati, pubblicato sul sito web dell'ACN, e sul sito web di ENISA, una voce specifica per quel prodotto o PP, allegando la versione elettronica del TDS e dell'RC.

[23] Articolo 40, paragrafo 1 dell'[EUCC].

12. La gestione nel tempo delle garanzie dei prodotti certificati

Questa sezione descrive le modalità di valutazione per:

- il monitoraggio dei certificati, successivamente alla loro emissione, da parte dell'OCSI e del Titolare del certificato[24];
- la gestione delle non conformità di un certificato da parte dell'OCSI e del Titolare del certificato[25];
- il riesame del certificato per l'aggiornamento dell'analisi di vulnerabilità per un certificato dopo la sua emissione[26];
- il riesame di un certificato per stabilire se tale certificato e il relativo livello di garanzia possa estendersi a un ODV modificato o allo stesso ODV in ambiente di sviluppo modificato[27];
- l'applicazione di una *procedura di patch* ad un prodotto certificato in caso di vulnerabilità critica[28].

12.1. Monitoraggio dei certificati emessi dall'OCSI

Nel monitoraggio dei certificati emessi sul territorio nazionale, l'Agenzia controlla il rispetto degli obblighi in capo ai Soggetti coinvolti nei processi di certificazione che hanno portato ad un certificato EUCC, il rispetto dei requisiti stabiliti dall'EUCC per i prodotti TIC e PP certificati e il livello di garanzia dei certificati rispetto all'evoluzione delle minacce nel tempo.

Per le verifiche l'Agenzia seleziona un campione dei certificati emessi sul territorio nazionale dall'OCSI chiedendo eventualmente assistenza all'OCSI e agli LVS. In particolare, l'Agenzia può richiedere all'OCSI e all'LVS coinvolto un riesame di certificati emessi[29] attraverso l'aggiornamento dell'analisi di vulnerabilità rispetto al nuovo scenario di minacce per l'ODV con le modalità specificate nella sezione 12.3.

L'OCSI, indipendentemente dalle eventuali richieste di riesame dall'Agenzia, effettua una attività di monitoraggio[30] dei certificati da esso emessi. In particolare, monitora:

- il rispetto, da parte dei Titolari di un certificato, degli obblighi a essi incombenti a norma del regolamento [EUCC] e del regolamento [CSA] per quanto riguarda i certificati EUCC rilasciati dall'OCSI;

[24] Articoli 25, 26 e 27 dell'[EUCC].
[25] Articoli 28, 29, 30, 31 dell'[EUCC].
[26] Articolo 13 e allegato IV.2 dell'[EUCC].
[27] Articolo 13 e allegato IV.3 dell'[EUCC].
[28] Allegato IV.4 dell'[EUCC].
[29] Articolo 13 e allegato IV.2 dell'[EUCC].
[30] Articolo 26 dell'[EUCC].

- il rispetto, da parte dei prodotti TIC che ha certificato, dei rispettivi requisiti di sicurezza;
- il livello di affidabilità espresso nei profili di protezione certificati.

L'OCSI svolge le proprie attività di monitoraggio sulla base:

- delle informazioni fornite in base agli impegni assunti dal Committente;
- delle informazioni derivanti dalle attività di altre autorità di vigilanza del mercato competenti;
- dei reclami ricevuti;
- delle informazioni sulle vulnerabilità che potrebbero avere un impatto sui prodotti TIC che ha certificato.

12.2. Monitoraggio da parte del Titolare del certificato

Il Titolare di un certificato deve effettuare un monitoraggio del certificato. In particolare, il Titolare del certificato monitora:

- le vulnerabilità note che possano interessare il certificato;
- le ulteriori vulnerabilità che dovessero emergere durante lo sviluppo dell'ODV orientato alla correzione degli errori, l'arricchimento di funzioni e l'emissione di nuove versioni;
- le vulnerabilità potenziali e residue emerse durante la valutazione iniziale[31];
- le vulnerabilità segnalate da altre fonti (ad esempio utenti dell'ODV o ricercatori).

È bene evidenziare che nel caso in cui il Titolare del certificato sia un soggetto diverso dallo Sviluppatore, il Titolare del certificato dovrà stabilire idonei accordi per il monitoraggio del certificato a valle del processo di certificazione.

Il Titolare di un certificato EUCC istituisce e mantiene in essere tutte le procedure di gestione delle vulnerabilità in conformità agli articoli 33-36 dell'[EUCC] e alla norma EN ISO/IEC 30111.

Il Titolare del certificato mantiene in essere e pubblica metodi appropriati per ricevere informazioni sulle vulnerabilità relative ai propri prodotti trasmesse da fonti esterne, compresi gli utenti, gli organismi di certificazione e i ricercatori nel settore della sicurezza.[32]

[31] Poiché i metodi di attacco possono evolvere nel tempo, il potenziale richiesto per condurre alcuni specifici attacchi può diminuire rispetto alla valutazione iniziale e può risultare necessario rieseguire nuovamente un'analisi delle vulnerabilità per valutare se vulnerabilità inizialmente classificate come residue siano diventate sfruttabili.
[32] Articolo 33, paragrafo 2 dell'[EUCC].

Il Titolare del certificato, riscontrando una vulnerabilità potenziale produce un'analisi di impatto delle vulnerabilità[33]. L'analisi dell'impatto delle vulnerabilità è effettuata in un intervallo di tempo adeguato in relazione alla sfruttabilità e alla criticità della potenziale vulnerabilità del prodotto TIC certificato. L'analisi riporta un calcolo del potenziale di attacco al fine di determinare la sfruttabilità delle vulnerabilità individuate rispetto al livello di affidabilità certificato. Le informazioni relative alle possibili modalità di sfruttamento della vulnerabilità sono trattate conformemente a misure di sicurezza adeguate per proteggerne la riservatezza e garantirne, se necessario, una diffusione limitata.

Se la vulnerabilità potenziale interessa prodotti compositi, il Titolare del certificato informa i Titolari dei certificati da esso dipendenti senza indugio.

In risposta a una richiesta dell'OCSI, il Titolare di un certificato trasmette tutte le informazioni pertinenti sulle potenziali vulnerabilità riscontrate[34]. Il titolare del certificato trasmette senza indebito ritardo una relazione sull'analisi dell'impatto delle vulnerabilità all'OCSI.

Se dalla relazione sull'analisi dell'impatto delle vulnerabilità emerge che la vulnerabilità non è residua, ovvero il livello di affidabilità attestato nel certificato non può essere più garantito, si distinguono due casi:

- se la vulnerabilità può essere risolta[35] con un aggiornamento del TDS e/o dell'ODV, il Titolare del certificato propone all'OCSI le misure correttive, avviando contestualmente un riesame del certificato come previsto nella sezione 12.6; tale riesame, riguardando una modifica *major*, richiederà la rivalutazione del prodotto, la revoca del certificato attuale e l'emissione di un nuovo certificato in caso di esito positivo;
- se invece dalla relazione sull'analisi dell'impatto delle vulnerabilità emerge che la vulnerabilità non può essere risolta[36], il certificato EUCC è semplicemente revocato dall'OCSI.

In caso di revoca di un certificato, il Titolare del certificato divulga e registra[37] qualsiasi vulnerabilità del prodotto TIC pubblicamente nota e risolta nella banca dati europea delle vulnerabilità[38], o in altri archivi online[39].

Il Titolare del certificato monitora le eventuali vulnerabilità residue per garantire che non possano essere sfruttate in caso di modifiche dell'ambiente operativo.

[33] Articolo 34 dell'[EUCC].
[34] Articolo 33, paragrafo 5 dell'[EUCC].
[35] Articolo 35, paragrafo 5 dell'[EUCC].
[36] Articolo 35, paragrafo 6 dell'[EUCC].
[37] Articolo 39 dell'[EUCC].
[38] La banca dati europea è istituita in conformità dell'articolo 12 della direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio.
[39] L'articolo 55, paragrafo 1, lettera d), del regolamento (UE) 2019/881 prevede la pubblicazione online di informazioni sui certificati regolarmente aggiornate.

12.2.1. Relazione sull'analisi d'impatto delle vulnerabilità

La relazione sull'analisi dell'impatto delle vulnerabilità[40] contiene una valutazione degli elementi seguenti:

905 1. l'impatto della vulnerabilità sul prodotto TIC certificato;
2. i possibili rischi associati alla disponibilità, attuale o in un prossimo futuro, di un attacco;
3. la possibilità di risolvere la vulnerabilità;
4. laddove la vulnerabilità possa essere risolta, le possibili modalità di risoluzione.

910 La relazione sull'analisi dell'impatto delle vulnerabilità contiene, se del caso, dettagli sulle possibili modalità di sfruttamento della vulnerabilità.

12.3. Aggiornamento dell'analisi di vulnerabilità

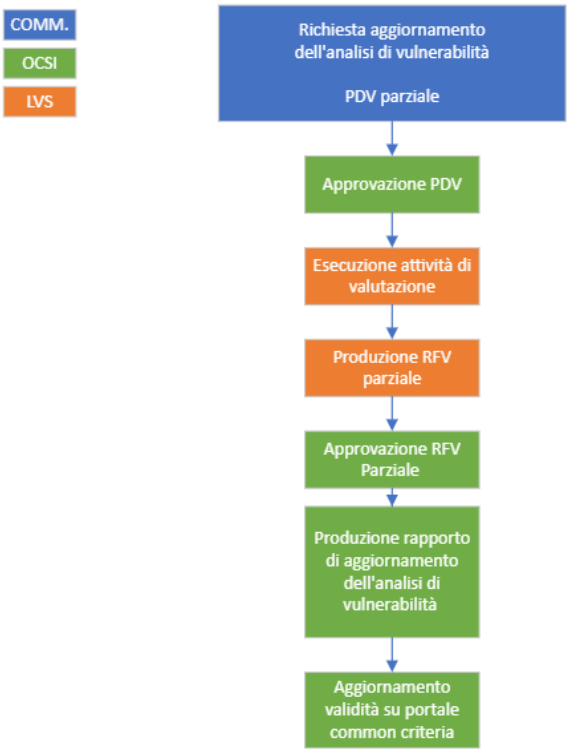

Figura 1 - Diagramma di flusso per l'aggiornamento dell'analisi di vulnerabilità

L'attività di aggiornamento dell'analisi di vulnerabilità potrebbe essere portata avanti dal
915 Titolare del certificato per:

[40] Articolo 35, paragrafi 2 e 3 dell'[EUCC].

- confermare successivamente all'emissione del certificato che la baseline di garanzia non è variata rispetto al nuovo scenario di minacce attuale, essendo emerse delle vulnerabilità potenziali da verificare;
- estendere la validità di un certificato già emesso oltre la data di scadenza prevista per lo stesso, anche in assenza di vulnerabilità potenziali da verificare.

Nel caso in cui il Titolare del certificato intenda verificare la resistenza dell'ODV certificato nel panorama del nuovo scenario di attacchi, invia una richiesta di **aggiornamento dell'analisi di vulnerabilità** all'OCSI. In alternativa, l'aggiornamento dell'analisi di vulnerabilità può essere avviato su richiesta dello stesso OCSI, o dell'Agenzia.

Il processo di aggiornamento delle vulnerabilità comporterà una ri-esecuzione parziale delle sole attività di valutazione relative alle classi AVA ed eventualmente ALC. Le stesse dovranno essere svolte dall'LVS che ha eseguito le attività di valutazione per la certificazione originaria. Il diagramma di flusso da seguire è mostrato in Figura 1**Errore. L'origine riferimento non è stata trovata.**.

Il Titolare del certificato invia all'OCSI la richiesta di avvio della procedura di aggiornamento dell'analisi di vulnerabilità corredata dal PDV parziale redatto dallo stesso LVS che ha eseguito la certificazione originaria.

Nel richiedere l'aggiornamento dell'analisi di vulnerabilità, il Titolare del certificato include:

- l'eventuale analisi preliminare d'impatto[41] con le vulnerabilità riscontrate attraverso le modalità in sezione 12.2 o, in alternativa, la dichiarazione di non aver riscontrato vulnerabilità potenziali attraverso alcun mezzo o fonte dall'emissione del certificato o dall'ultimo aggiornamento di analisi di vulnerabilità; l'eventuale analisi di impatto ha le caratteristiche dettagliate nella sezione 12.6.1[42]; è bene precisare che l'aggiornamento dell'analisi di vulnerabilità ha come scopo confermare la baseline di garanzia dell'ODV attraverso una rivalutazione parziale del TDS e può essere richiesta solo per un TDS immutato e in assenza di vulnerabilità sfruttabili conosciute. Pertanto, l'eventuale analisi preliminare d'impatto condotta dal Titolare del certificato e allegata alla richiesta di aggiornamento dell'analisi di vulnerabilità potrà contenere al massimo vulnerabilità residue, ma non sfruttabili o sfruttabili con un potenziale di attacco superiore rispetto al livello di resistenza attestato dal certificato; inoltre, non potrà contenere misure correttive del TDS per risolvere vulnerabilità segnalate;
- relativamente alla possibile rivalutazione dell'ambiente di sviluppo, qualora applicabile, eventuali evidenze integrative necessarie a dimostrare che risultino ancora valide le garanzie relative alle attività di verifica dell'ambiente di sviluppo.

[41] Articolo 33, par. 3.
[42] Articolo 35 dell'[EUCC].

L'OCSI, valutata l'idoneità del PDV, eventualmente revisionato dall'LVS a seguito di chiarimenti e integrazioni richiesti dall'OCSI, approva il PDV autorizzando l'LVS ad avviare le attività previste per l'aggiornamento dell'analisi di vulnerabilità. Nella comunicazione rivolta al Titolare del certificato, sarà compreso anche il preventivo dei costi dovuti all'OCSI per le attività di certificazione.

L'LVS esegue le attività di garanzia che risultano avere un impatto per l'evoluzione del panorama di attacchi per il prodotto (nello specifico le attività previste dalla famiglia AVA_VAN) e, quando ritenuto rilevante, riesegue anche l'attività di garanzia della classe ALC nel momento in cui le evidenze non sono più sufficienti a confermare che tale garanzia ALC sia ancora soddisfatta.

In caso di vulnerabilità potenziali segnalate dal Titolare del certificato o di rilevamento di nuove vulnerabilità, errori o anomalie, l'LVS produce i relativi Rapporti di Osservazione, gestiti da Titolare del certificato e OCSI come previsto nella sezione 8.3.

L'LVS produce rapporti di attività per la classe AVA e ove applicabile per la classe ALC.

Al termine dell'attività l'LVS produce quindi un RFV parziale che invia all'OCSI.

Quando l'OCSI riceve l'RFV dall'LVS, lo revisiona per determinare se soddisfi i requisiti del sistema EUCC e dei criteri di valutazione. Se tale revisione dà esito positivo l'RFV viene approvato entro trenta giorni dalla sua ricezione.

Qualora nell'RFV vengano individuate delle anomalie risolvibili, l'OCSI ne richiede all'LVS la correzione. In tal caso, l'LVS è tenuto a modificare il rapporto entro i successivi quindici giorni. Tale richiesta sospende, fino al relativo esito, il decorso del suddetto termine di trenta giorni.

In caso di esito positivo, l'OCSI emette un *rapporto di aggiornamento dell'analisi di vulnerabilità* che può essere pubblicato su eventuale richiesta del Committente.

Inoltre, a seguito di un aggiornamento dell'analisi di vulnerabilità che si conclude con esito positivo, è prevista l'emissione di un nuovo certificato, con validità estesa rispetto al certificato originario. La validità del nuovo certificato sarà al massimo 5 anni, dalla data di emissione del nuovo certificato, come per tutti i certificati EUCC, salvo deroghe concesse dall'Agenzia[43]. Tuttavia, essendo svolta una rivalutazione parziale (solo la classe AVA ed eventualmente ALC), la data di scadenza del nuovo certificato non potrà superare i 10 anni dalla data di emissione del certificato iniziale. **Viceversa, in caso di esito negativo, il certificato iniziale non è più valido e l'OCSI revoca il certificato, eventualmente riemettendo un certificato con livello di garanzia ridotto[44].**

Il Committente può richiedere di avviare una rivalutazione beneficiando dei risultati conseguiti durante la procedura di aggiornamento dell'analisi di vulnerabilità**.**

[43] Articolo 12, paragrafo 3 dell'[EUCC].
[44] Articolo 13 dell'[EUCC].

12.4. Gestione delle non conformità di un certificato

La gestione delle non conformità di un certificato[45] diverse dalle vulnerabilità rilevate, richiede collaborazione da parte del Titolare del certificato con l'OCSI.

Se un prodotto TIC o un PP certificato dovesse risultare non conforme al [CSA] o all'[EUCC], l'OCSI ne informerà il Titolare del certificato e chiederà un'azione correttiva e ove necessario informerà anche l'Agenzia. Il Titolare del certificato entro il termine stabilito dall'OCSI proporrà un'azione correttiva all'OCSI, che ne effettuerà un riesame.

In caso di inerzia o in situazioni di emergenza l'OCSI potrà, alternativamente:

- sospendere il certificato in attesa che la non conformità sia risolta per un massimo di 42 giorni, salvo proroghe da parte dell'Agenzia fino a un massimo di un anno;
- revocare il certificato.

[45] Capo VI – Sezione II dell'[EUCC].

12.5. Applicazione di patch ad un prodotto TIC certificato

È possibile apportare *patch* (correzioni)[46] ad un prodotto TIC certificato in caso di rilevazione di vulnerabilità critiche con il coinvolgimento dell'OCSI nei seguenti casi:

(a) le funzionalità interessate dalla *patch* non rientrano nell'ODV del prodotto TIC certificato;

(b) la *patch* riguarda una modifica di piccola entità predeterminata del prodotto TIC certificato;

(c) la *patch* riguarda una vulnerabilità confermata con effetti critici sulla sicurezza del prodotto TIC certificato.

Se la modifica non è di piccola entità occorrerà procedere ad una rivalutazione del prodotto TIC.

L'applicazione della correzione avverrà sulla base di una procedura esaminata durante la certificazione del prodotto TIC, valutata dall'LVS e inclusa nel rapporto di certificazione del prodotto TIC certificato.

Il Titolare del certificato può applicare la procedura di *patch* certificata

- nel caso (a) senza l'emissione di un nuovo certificato,
- nel caso (b), a fronte di una nuova valutazione condotta dall'LVS ingaggiato nella valutazione precedente, con l'aggiornamento del certificato e del rapporto di certificazione,
- nel caso (c), a fronte di una nuova valutazione condotta dall'LVS ingaggiato nella valutazione precedente, con l'aggiornamento del certificato e del rapporto di certificazione, potendo applicare e distribuire la *patch* durante la valutazione.

12.6. Il mantenimento e la rivalutazione

Nella gestione di un prodotto TIC certificato, il Titolare del certificato potrebbe aver bisogno di estendere le garanzie offerte dalle funzionalità di sicurezza del prodotto TIC certificato a fronte di alcune modifiche intervenute sull'ODV o sul suo ambiente di sviluppo successivamente all'emissione del certificato. Si procede quindi a valutare tali modifiche sulla base di una analisi di impatto dei cambiamenti intercorsi e si decide di ripetere la valutazione dell'ODV in alternativa:

- su una parte di attività già eseguite (*mantenimento del certificato*),
- o su tutte le attività (*rivalutazione del prodotto TIC*).

[46] Allegato IV.4 dell'[EUCC].

In particolare, a seguito di una o più modifiche *considerate nel complesso minor* si potrà effettuare una rivalutazione parziale, invece, nel caso in cui intervenga almeno una modifica di tipo *major* sarà necessario ripetere integralmente la valutazione.

Un ODV nella versione modificata potrebbe avere una delle seguenti forme:

- una nuova versione dell'ODV o del prodotto di cui l'ODV costituisce un sottoinsieme di funzionalità;
- l'ODV certificato su cui sono installati degli aggiornamenti a correzione di errori di codifica e/o vulnerabilità;
- l'ODV in versione certificata ma per il quale viene aggiornato l'ambiente operativo (ad esempio una piattaforma *hardware*, *firmware* o *software* parzialmente differente da quella indicata nella versione valutata e certificata) come rappresentato nel Traguardo di Sicurezza (TDS).

Inoltre, ulteriori modifiche potrebbero riguardare l'ambiente di sviluppo senza alcuna modifica all'ODV o al prodotto TIC che lo contiene.

Una modifica *minor* consiste in una modifica il cui impatto sull'ODV non ha effetti sulle garanzie offerte dalle funzioni di sicurezza dell'ODV certificato (da intendersi con il significato che i risultati delle attività svolte dal valutatore per la certificazione iniziale dell'ODV risultano ancora validi dopo le modifiche[47]), oppure in una modifica all'ambiente di sviluppo che tuttavia non ha effetti sulle garanzie offerte dalle funzioni di sicurezza dell'ODV certificato. Inoltre, modifiche alla baseline di garanzia per l'aggiunta del componente ALC_FLR sono considerate *minor*. In particolare, l'aggiunta di ALC_FLR.x a un certificato esistente o la selezione di un componente superiore di ALC_FLR, esaminato come parte delle attività di valutazione con RFV parziale, viene considerata una modifica minor a condizione che le procedure nuove o modificate non influiscano sull'ODV o sulle informazioni di progettazione stesse.

Una modifica *major* consiste invece in una modifica il cui impatto ha effetti sulle garanzie offerte dalle funzioni di sicurezza dell'ODV certificato e conseguentemente richiede di eseguire nuovamente tutte le attività di verifica da parte di un LVS. Per questo motivo, le modifiche di tipo *minor* sono gestite nell'ambito del processo detto "mantenimento", mentre le modifiche di tipo *major* sono gestite ripetendo integralmente le attività di valutazione a seguito di una richiesta di "rivalutazione"[48].

In Figura 2 si riporta il diagramma di flusso ad alto livello per la gestione nel tempo delle garanzie dei prodotti certificati, nei casi di modifiche all'ODV.

La procedura prevede i seguenti passi:

1. a seguito dell'emissione del certificato, durante il ciclo di vita dell'ODV certificato, può essere necessario effettuare delle modifiche all'ODV;

[47] Sebbene il Committente eseguirà comunque attività di test di non regressione.
[48] Si rimanda al documento prodotto dal CCRA [AC] per esempi di modifiche di tipo *minor* e *major*.

2. il Titolare del certificato (o Sviluppatore, di seguito solo Titolare del certificato) aggiorna le evidenze, analizza le modifiche all'ODV certificato attraverso una analisi di impatto, e riassume i risultati in un rapporto di analisi di impatto (RAI),
    - il Titolare del certificato, nel RAI, classifica le modifiche in ***minor o major***,
    - il Committente invia quindi il RAI all'OCSI, insieme alle evidenze di valutazione che hanno subito un aggiornamento. Per la struttura ed i contenuti del RAI si rimanda alla sezione12.6.1..
3. **In caso di modifica valutata di tipo *minor***, l'OCSI autorizza l'avvio del processo di mantenimento ed invia al Committente il preventivo dei costi dovuti all'OCSI per le attività. Nel caso di modifiche *major* si avvia la procedura di rivalutazione come specificato nelle sezioni da 7 a 11 allegando alla documentazione richiesta anche la RAI.

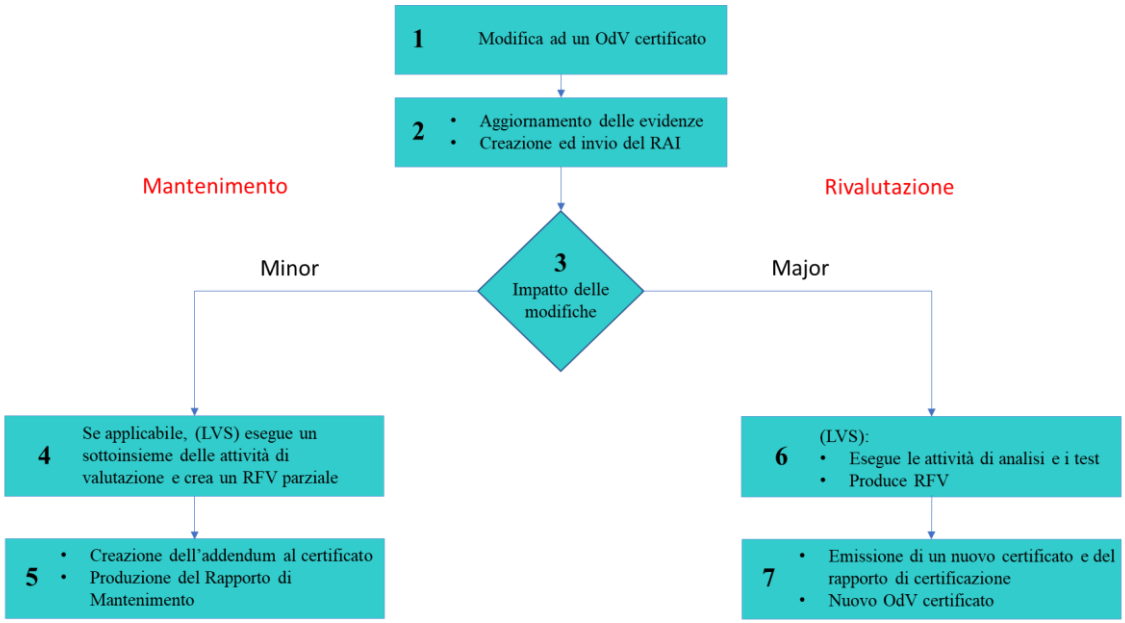

Figura 2 - Diagramma di flusso delle procedure di rivalutazione e mantenimento

4. Qualora, in caso di modifica *minor*, sia necessario eseguire parte delle attività di valutazione sull'ambiente di sviluppo, la RAI deve essere corredata dall'indicazione dell'LVS incaricato di eseguire tali attività e dal piano di valutazione (PDV) parziale redatto dallo stesso LVS. l'LVS, al termine di suddette attività, produce un RFV parziale,
5. al termine delle attività l'OCSI, revisiona, se presente, l'RFV per determinare se soddisfa i requisiti del sistema EUCC. Se tale revisione dà esito positivo l'RFV viene approvato entro trenta giorni dalla sua ricezione. Qualora nell'RFV vengano individuate delle anomalie risolvibili, l'OCSI ne richiede all'LVS la correzione. In tal

caso, l'LVS è tenuto a modificare il rapporto entro i successivi quindici giorni. Tale richiesta sospende, fino alla ricezione dell'RFV aggiornato, il decorso del suddetto termine di trenta giorni. Una volta che l'OCSI concorda sul fatto che la baseline di garanzia non è stata influenzata negativamente, viene creato un addendum all'elenco di certificazione e viene prodotto un rapporto di mantenimento derivato dallo IAR come addendum al rapporto di certificazione originale che viene reso pubblico.

Le informazioni contenute nel rapporto di mantenimento sono essenzialmente un sottoinsieme del contenuto del documento RAI. Le seguenti sezioni del documento RAI dovrebbero essere incluse nel rapporto di manutenzione:

1. introduzione,
2. descrizione delle modifiche,
3. evidenze di valutazione su cui la modifica ha un impatto.

La sezione 12.6.1 contiene ulteriori informazioni sulla struttura del documento RAI.

Il certificato originario viene confermato ancora valido senza alcuna estensione temporale.

6. Nel caso in cui sia stata avviata la procedura di rivalutazione per effetto di modifiche major, occorrerà ripetere le fasi di cui alle sezioni da 7 a 11, trasmettendo una nuova domanda di valutazione ed allegando alla documentazione richiesta anche la RAI.

7. Al termine del processo di rivalutazione, con esito positivo, l'OCSI **emette un nuovo certificato e un nuovo rapporto di certificazione**. Il nuovo certificato dell'ODV rappresenta il livello di garanzia di riferimento rispetto al quale saranno valutate le future modifiche.

12.6.1. La struttura del rapporto di analisi di impatto

Il RAI deve essere strutturato come segue:

- Introduzione;
- Descrizione delle modifiche;
- Evidenze di valutazione su cui la modifica ha un impatto (ed attività di valutazione sull'ambiente di sviluppo che eventualmente un LVS deve eseguire);
- Statement in cui viene riportato che le interfacce di sicurezza sono rimaste invariate;
- Descrizione delle modifiche alle evidenze di valutazione;
- Conclusione;
- Allegato: evidenze di valutazione aggiornate.

Per il dettaglio del contenuto si rimanda al documento Assurance Continuity prodotto dal CCRA [AC].

12.7. Lingua utilizzata

Per permettere la pubblicazione delle informazioni sul processo di certificazione in lingua inglese sul sito web di ENISA[49], a valle di un processo di aggiornamento delle vulnerabilità concluso positivamente:

- il nuovo certificato emesso dall'OCSI sarà bilingue italiano e inglese;
- il rapporto di aggiornamento delle vulnerabilità con validità legale, che specifica l'ambito e le condizioni di applicabilità del certificato, sarà emesso in lingua italiana;
- sarà inoltre emesso un rapporto di aggiornamento delle vulnerabilità in lingua inglese come traduzione di cortesia del rapporto di certificazione in lingua italiana con validità legale.

Il Rapporto di Aggiornamento delle Vulnerabilità include i riferimenti all'identificatore del Certificato e del Rapporto di Certificazione.

Nel caso in cui sia concluso positivamente un processo di mantenimento per un certificato esistente sarà emesso:

- un rapporto di mantenimento in lingua italiana, quale addendum del rapporto di certificazione con validità legale;
- un rapporto di mantenimento in lingua inglese, quale addendum del rapporto di certificazione in lingua inglese.

Il Rapporto di Mantenimento include i riferimenti all'identificatore del Certificato e del Rapporto di Certificazione.

[49] L'articolo 42, paragrafo 1 dell'[EUCC] stabilisce che sul sito web di ENISA dovranno essere pubblicata almeno in lingua inglese documentazione e informazioni per ciascun processo di certificazione, fra cui il certificato ed il rapporto di certificazione.

13. Condizioni per lo svolgimento di test da remoto in valutazioni Common Criteria

Questa sezione fornisce le indicazioni da seguire nel caso in cui il Valutatore richieda all'OCSI, attraverso motivata e giustificata richiesta, di poter effettuare le attività operative della valutazione come esecuzione di test di corretta implementazione e analisi di vulnerabilità da remoto.

L'OCSI valuta la richiesta e decide sulla base delle motivazioni e della descrizione delle modalità di test fornite se approvare o meno l'esecuzione da remoto delle attività operative.

Se la richiesta viene approvata dall'OCSI, l'LVS deve agire in accordo alla seguente linea guida per poter effettuare le attività mantenendo un livello adeguato di sicurezza.

L'OCSI, nella comunicazione di approvazione per l'esecuzione di test da remoto, può fornire ulteriori prescrizioni che vanno a complementare la seguente sezione.

13.1. Scenario di riferimento

Ai fini del presente documento, si considera unicamente la situazione in cui l'ODV (o il test bed predisposto dallo Sviluppatore) è ospitato in una sede differente rispetto alla sede in cui opera il Valutatore e accede all'ODV solo tramite una rete pubblica (Internet) mediante un canale adeguatamente protetto.

Si presuppone altresì che il Valutatore operi fisicamente nella sede dell'LVS[50] e che siano garantite le misure di sicurezza IT e fisiche atte a preservare la confidenzialità e l'integrità delle informazioni accolte e utilizzate durante le attività di valutazione, nel rispetto delle procedure esaminate dagli ispettori OCSI in fase di visita ispettiva di abilitazione.

Il Valutatore esegue i test utilizzando una postazione situata presso l'LVS, sotto il completo controllo del Valutatore, collegata direttamente all'ODV. In alternativa, la postazione del valutatore può essere connessa a una macchina remota collegata alle interfacce dell'ODV e dedicata all'esecuzione dei test.

Ciascuna deroga alle modalità "standard" di esecuzione delle attività oggetto di questo documento, individuate in modo esplicito nei Criteri di Valutazione e nella relativa metodologia, rende comunque necessaria l'individuazione di specifiche soluzioni e modalità operative ad hoc da sottoporre caso per caso all'approvazione del Certificatore.

[50] Qualora, sempre per motivi eccezionali, il Valutatore si trovasse ad operare in un sito diverso dall'LVS (ad es. in regime di lavoro a distanza), dovrà essere sottoposto a misure di sicurezza fisiche, procedurali e tecniche adeguate a garantire la protezione delle informazioni allo stesso livello del sito dell'LVS. Tali misure dovranno essere comunicate all'Organismo di Certificazione per approvazione.

13.2. Misure di sicurezza minime

Per poter effettuare le attività operative da remoto nello scenario di riferimento, il Valutatore deve mettere in atto alcune misure di sicurezza per:

- proteggere il canale di comunicazione fra la postazione del laboratorio e l'ambiente remoto di test da:
  a. compromissioni dell'integrità dei messaggi che transitano in esso;
  b. compromissioni della riservatezza delle informazioni in transito ove tale compromissione possa recare danni al Committente dell'ODV;
  c. minacce alla disponibilità dell'oggetto delle verifiche operate tramite la rete pubblica;
- assicurarsi che durante le attività di verifica non siano stabilite altre comunicazioni da e verso il sistema che ospita l'ODV (o la macchina remota di test) eccetto eventuali comunicazioni ben identificate, giustificate per l'operatività del test bed e monitorabili dal Valutatore, in modo tale da non creare interferenze con le verifiche in corso, invalidandone i risultati;
- assicurarsi che prima, durante e dopo le attività di verifica sia l'ODV e sia l'ambiente di test si trovino nello stato che il Valutatore si aspetta sulla base della documentazione di valutazione, in particolare sulla base della guida all'installazione e configurazione sicura.

Il canale di comunicazione tra la postazione del Valutatore e l'ODV (o eventualmente la macchina remota) deve avvenire mediante una rete VPN che adotta algoritmi di cifratura robusti e utilizza la mutua autenticazione tra i nodi basata su certificato digitale.

13.3. Preparazione e conduzione dei test da remoto

L'attività di verifica della corretta implementazione eseguita da remoto consiste nell'esecuzione di specifici test funzionali (sulla base, ad esempio, di quanto richiesto dai componenti di garanzia della famiglia ATE_IND) utilizzando le interfacce dell'ODV stimolate dalla postazione del Valutatore (o eventualmente dalla macchina remota) senza la possibilità di accedere fisicamente all'ODV e di osservarne lo stato se non attraverso la connessione sicura instaurata.

Allo stesso modo, l'attività di prove di intrusione da remoto consiste nell'esecuzione della sequenza di operazioni previste per lo sfruttamento delle vulnerabilità in esame dalla postazione remota del Valutatore accedendo all'ODV attraverso la connessione instaurata.

Per lo svolgimento delle verifiche da remoto, le attività del Valutatore si possono dividere nelle seguenti quattro fasi:

- attività di verifica dell'ambiente operativo;
- attività di preparazione sicura dell'ODV;

- attività di connessione preliminare al sistema remoto;
- attività di monitoraggio del sistema durante le verifiche da remoto.

13.3.1. Verifica dell'ambiente operativo

Il Valutatore deve accertarsi che l'ambiente di test dell'ODV sia una corretta istanza dell'ambiente operativo ipotizzato per l'ODV e che quindi realizzi gli obiettivi di sicurezza ad esso associati.

Rispetto al caso ideale il Valutatore deve collezionare una serie di parametri che caratterizzano l'ambiente al fine di poter stabilire lo stato del sistema e quindi poter verificare lo stato noto dell'ODV in fase di attività di verifica da remoto.

Esempi di parametri che il Valutatore dovrebbe collezionare, per ciascun componente presente nell'ambiente operativo, sono i seguenti:

- informazioni di configurazione dell'HW a supporto dell'ODV, tra cui parametri in grado di identificare univocamente il sistema impiegato per il test;
- informazioni di configurazione del Sistema Operativo e del SW/FW a supporto dell'ODV (ad esempio le informazioni estratte dal policy manager di Windows, le informazioni di configurazione del Web Server, le informazioni di configurazione della scheda di rete).

13.3.2. Preparazione sicura dell'ODV

Il Valutatore deve accertarsi che l'ODV sia installato nell'ambiente di test e sia configurato in accordo alla documentazione di valutazione (TDS e guide).

Ove il Valutatore non sia in grado di testimoniare direttamente l'installazione e la configurazione dell'ODV, questi deve collezionare parametri aggiuntivi al fine di poter verificare lo stato noto dell'ODV in fase di attività di verifica da remoto.

Oltre ai parametri elencati per l'ambiente operativo, esempi di parametri relativi all'ODV che il Valutatore dovrebbe collezionare sono i seguenti:

- informazioni di configurazione dell'ODV (incluso un hash dei file binari dell'ODV);
- copia dei file di log al termine dell'istallazione per eseguire verifiche successive.

Prima di iniziare la vera e propria attività di verifica il Valutatore deve essere in grado di accedere da remoto (tramite canale protetto e possibilmente separato, logicamente o fisicamente, da quello che verrà usato per le attività di verifica) al test bed sul quale è installato l'ODV con privilegi necessari per le operazioni da svolgere.

Il Valutatore dovrebbe ad esempio predisporre assieme al Committente una connessione VPN fra la macchina del proprio laboratorio e il sistema operativo remoto dell'ODV o della macchina predisposta per i test.

Le operazioni sopra descritte non devono essere incluse nelle guide dell'ODV, ma sono solo propedeutiche per i test effettuati dal Valutatore e devono essere documentate esclusivamente nei rapporti di attività corrispondenti.

13.3.3. Monitoraggio del sistema durante le verifiche da remoto

Prima, durante e dopo ciascuna verifica svolta da remoto sull'ODV, il Valutatore deve monitorare i parametri individuati sull'ODV e del suo eventuale ambiente, in fase di preparazione sicura, al fine di determinarne lo stato noto.

Il Valutatore, mediante ad esempio, una istanza di desktop remoto o un terminale, deve verificare:

- i parametri del sistema raccolti in fase di verifica dell'ambiente operativo e preparazione sicura dell'ODV;
- gli utenti connessi all'ODV e alla postazione remota del valutatore;
- le porte aperte e le connessioni tramite interfaccia di rete all'ODV e ad altri servizi del sistema operativo eventuale dell'ODV così come del sistema operativo della postazione del valutatore;
- la presenza di interazioni con altri nodi della rete;
- la qualità del canale di connessione verso la postazione locale del valutatore, verificando per esempio il tempo di percorrenza dei pacchetti TCP.

Il Valutatore deve anche verificare che la connessione al sistema remoto, dedicata alle attività di verifica dell'ambiente di test durante l'esecuzione delle verifiche, non interferisca in modo da invalidare l'esito delle verifiche eseguite.

In caso di altre connessioni attive all'ODV il Valutatore deve valutare se queste connessioni possano inficiare il risultato delle verifiche condotte. In caso positivo, il Valutatore deve gestire la presenza di tali connessioni eventualmente prendendo contromisure per limitarle/bloccarle (ad esempio servendosi di strumenti di filtraggio del traffico).

13.3.4. Considerazioni conclusive nel caso di esecuzione test da remoto

Fatto salvo l'impegno degli LVS ad ottemperare alle linee guida illustrate nella presente sezione 13, ove applicabile, l'OCSI si riserva la facoltà di attuare le opportune verifiche sui Rapporti di Attività e sulla documentazione relativa ai test prodotta dagli LVS e di specificare ulteriori requisiti e condizioni ove ciò si riveli necessario.

Allo scopo di consentire una verifica preliminare, le informazioni sulle modalità di esecuzione dei test in modalità remota e di attuazione delle misure di protezione aggiuntive richieste, unitamente al piano di test, dovranno essere inviate all'OCSI con congruo anticipo rispetto alla data prevista per lo svolgimento delle attività connesse.

In caso di eventuali inosservanze delle condizioni e dei principi espressi in questo documento, nello standard Common Criteria e nelle Linee Guida dell'OCSI, i responsabili degli LVS e i Committenti/Sviluppatori accettano implicitamente le

conseguenze, che possano comportare, a seconda dei casi, l'invalidazione delle attività svolte, la richiesta di ripetizione in parte o in tutto delle attività, fino alla conclusione con esito negativo della valutazione e alla mancata emissione del Certificato.

14. Riferimenti

[AC] Assurance Continuity: CCRA requirements, v.3.1, 2024-02-29

[ACN] Decreto-legge 14 giugno 2021, n. 82, "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale." convertito con modificazioni dalla L. 4 agosto 2021, n. 109.

[CC1] "Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model", November 2022, CC:2022, Revision 1, CCMB-2022-11-001.

[CC2] "Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional requirements", November 2022, CC:2022, Revision 1, CCMB-2022-11-002.

[CC3] "Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance requirements", November 2022, CC:2022, Revision 1, CCMB-2022-11-003.

[CC4] "Common Criteria for Information Technology Security Evaluation, Part 4 – Framework for the specification of evaluation methods and activities", November 2022, CC:2022, Revision 1, CCMB-2022-11-004.

[CC5] "Common Criteria for Information Technology Security Evaluation, Part 5 – Pre-defined packages of security requirements", November 2022, CC:2022, Revision 1, CCMB-2022-11-005.

[CEM] "Common Methodology for Information Technology Security Evaluation – Evaluation methodology", November 2022, CC:2022, Revision 1, CCMB-2022-11-006.

[CSA] 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»).

[DLGS] Decreto Legislativo 3 agosto 2022, n. 123, "Norme di adeguamento della normativa nazionale alle disposizioni del Titolo III «Quadro di certificazione della cibersicurezza» del 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»).

[EUCC] 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).

[LG1-CA] Linea Guida NCCA N. 1– Attività di vigilanza nazionale e autorizzazione per il sistema EUCC (art. 5, art. 8 cc. 3-4 d.lgs. 123/2022).

[LG1-OC] Linea Guida OCSI N. 1 – Sistema EUCC: le caratteristiche generali e gli attori del processo di certificazione dell'OCSI (art. 4 c. 2, art. 11 cc. 3-4 d.lgs. 123/2022).

[LG2-OC] Linea Guida OCSI N. 2 – Abilitazione dei laboratori per la valutazione della sicurezza per il sistema EUCC (art. 8 c. 4 d.lgs. 123/2022).

[LG3-OC] Linea Guida OCSI N. 3 – Attività di valutazione ed emissione dei certificati per il sistema EUCC (art. 6 d.lgs. 123/2022).

[OCSI] Decreto del Presidente del Consiglio dei ministri del 30 ottobre 2003, "Approvazione dello schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione, ai sensi dell'art. 10, comma 1, del decreto legislativo 23 febbraio 2002, n. 10".

[TRNSF] Decreto del Presidente del Consiglio dei ministri 15 giugno 2022 - "Definizione dei termini e delle modalità del trasferimento di funzioni, beni strumentali e documentazione dal Ministero dello sviluppo economico all'Agenzia per la cybersicurezza nazionale.