Organismo di Certificazione
della Sicurezza Informatica

Nota Informativa dello Schema N. 2/07

Modifiche alla LGP2

Marzo 2007
Versione 1.0

REGISTRAZIONE DELLE AGGIUNTE E VARIANTI

L'elenco delle aggiunte e varianti al documento verrà mantenuto aggiornato in modo tale da riportare tutti gli emendamenti effettuati sul presente documento.

Paragrafi della LGP2 modificati	**Data**
2.2, 2.3.2, 2.4, 2.6, 3.1, 3.2.1, 3.2.2, 3.3, 4.2, 4.3, 4.4, 4.6, 4.7, 5, 5.1 e 5.3	Marzo 2007

INDICE

Scopo del documento

La Nota Informativa dello Schema N. 2/07, nel seguito brevemente indicata NIS 2/07, viene emessa dall'OCSI in base a quanto previsto dalle vigenti pubblicazioni dello Schema, ed in particolare dalla Linea Guida Provvisoria LGP3.

Il presente documento ha lo scopo di modificare e integrare le procedure descritte nella Linea Guida Provvisoria LGP2 avente per titolo "Accreditamento degli LVS e abilitazione degli Assistenti".

In particolare, sono stati modificati i seguenti paragrafi della LGP2: 2.2, 2.3.2, 2.4, 2.6, 3.1, 3.2.1, 3.2.2, 3.3, 4.2, 4.3, 4.4, 4.6, 4.7, 5, 5.1 e 5.3, che sostituiscono integralmente gli analoghi paragrafi attualmente contenuti nella LGP2 stessa.

Per facilità di lettura, nel seguito viene riportata l'intera Linea Guida Provvisoria LGP2, così come appare per effetto delle modifiche intervenute.

Le disposizioni contenute nella NIS 2/07 sono immediatamente operative e quindi sostituiscono a tutti gli effetti le parti corrispondenti contenute nella LGP2; tali disposizioni verranno successivamente integrate nelle Linee Guida Definitive.

1 Introduzione

L'istituzione dell'Organismo di Certificazione italiano per la sicurezza dei sistemi e dei prodotti nel settore della tecnologia dell'informazione, avvenuta attraverso un decreto del Ministro per l'Innovazione e le Tecnologie di concerto con i Ministri delle Comunicazioni, delle Attività Produttive e dell'Economia e delle Finanze, si pone come naturale termine di un percorso che è stato individuato e seguito in questi ultimi anni anche da numerosi altri stati nazionali, sia in Europa sia nel resto del mondo.

Il decreto riconosce che l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCTI) del Ministero delle Comunicazioni possiede i requisiti di indipendenza, affidabilità e competenza tecnica richiesti dalla decisione della Commissione europea del 6 novembre 2000 (2000/709/CE) e stabilisce che:

"l'ISCTI è l'Organismo di Certificazione della sicurezza nel settore della tecnologia dell'informazione, anche ai sensi dell'articolo 10 del decreto legislativo 23 gennaio 2002, n. 10 e dell'articolo 3, paragrafo 4 della direttiva 1999/93/CE".

Per consentire l'applicazione dello Schema nazionale previsto dal decreto l'Organismo di Certificazione ha predisposto le "Linee Guida Provvisorie" (LGP). Tali LGP sono organizzate in documenti distinti: una breve sintesi del contenuto di tutte le LGP è presentata nella LGP1.

La Linea Guida Provvisoria 2 (LGP2) definisce le procedure per ottenere e mantenere nel corso del tempo l'accreditamento di un Laboratorio per la Valutazione della Sicurezza informatica (LVS) secondo lo Schema nazionale per la valutazione e certificazione della sicurezza nel settore della tecnologia dell'informazione. Inoltre, vengono specificati gli ambiti di attività di un LVS e descritti i requisiti generali gestionali e di competenza tecnica per i laboratori. Infine, vengono descritti i requisiti e le procedure per ottenere l'abilitazione al ruolo di Assistente

Per la comprensione di questa linea guida si presuppone una buona familiarità con la norma internazionale [UNI1] che definisce i "Requisiti generali per la competenza dei laboratori di prova e di taratura".

2 Quadro di riferimento

Lo Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione prevede che le attività di valutazione siano necessariamente condotte da laboratori, denominati Laboratori per la Valutazione della Sicurezza (LVS), che abbiano ricevuto preventivamente un accreditamento da parte dell'Organismo di Certificazione (OC).

Ai fini dell'accreditamento, l'LVS deve possedere i seguenti requisiti:

1. la capacità di garantire l'imparzialità, l'indipendenza, la riservatezza e l'obiettività, che sono alla base del processo di valutazione;
2. la disponibilità di locali e mezzi adeguati ad effettuare valutazioni ai fini della sicurezza nel settore della tecnologia dell'informazione;
3. una organizzazione in grado di controllare il rispetto delle misure di sicurezza e della qualità previste per il processo di valutazione;
4. la disponibilità di personale sufficiente dotato delle necessarie competenze tecniche e iscritto nell'elenco dei Valutatori dell'OC;
5. la capacità di mantenere nel tempo i requisiti in virtù dei quali è stato accreditato.

Le procedure e i requisiti necessari per ottenere e mantenere l'accreditamento sono riportati nel seguito di questo documento.

Si precisa che l'accreditamento del laboratorio non implica una garanzia sulla qualità della valutazione di uno specifico prodotto o sistema, bensì rappresenta una dichiarazione riguardo alle competenze tecniche generiche possedute da un LVS.

2.1 Tipologie di accreditamento

Lo Schema prevede la possibilità di valutare e certificare prodotti e sistemi IT in conformità ai criteri europei ITSEC [ITS1] e allo standard internazionale Common Criteria [CC1,2,3] e alle relative metodologie.

Sia ITSEC, sia i Common Criteria, prevedono vari livelli di valutazione che richiedono, da parte dell'LVS che effettua la valutazione, una diversa e crescente competenza tecnica.

Per tali motivi, lo Schema prevede diverse tipologie di accreditamento, in dipendenza della competenza dell'LVS. Le tipologie standard di accreditamento previste sono riportate, per i criteri ITSEC e per i Common Criteria, nelle tabelle seguenti, congiuntamente alla portata dell'accreditamento, intesa come l'insieme delle prove che l'LVS è autorizzato a svolgere. L'Organismo di Certificazione si riserva la facoltà di consentire l'accreditamento di un LVS sulla base di tipologie di accreditamento *ad hoc* nei casi in cui ne riconosca la necessità. Ad esempio, un laboratorio potrebbe richiedere l'accreditamento *ad hoc* per azioni specifiche dei Valutatori o per specifiche tecnologie.

Il suddetto accreditamento verrà rilasciato dall'OC, a fronte di una richiesta formale da parte del laboratorio, con modalità che verranno individuate volta per volta, a seconda della specifica richiesta.

125 Tabella 1: Tipologie standard di accreditamento per i criteri ITSEC

Tipologie	Portata dell'accreditamento
E1	Azioni del Valutatore previste nella parte "Assurance-Effectiveness" relativa al livello E1 dei criteri ITSEC
E1-E2	Azioni del Valutatore previste nella parte "Assurance-Effectiveness" fino al livello E2 dei criteri ITSEC
E1-E2-E3	Azioni del Valutatore previste nella parte "Assurance-Effectiveness" fino al livello E3 dei criteri ITSEC
E1-E2-E3-E4	Azioni del Valutatore previste nella parte "Assurance-Effectiveness" fino al livello E4 dei criteri ITSEC
E1-E2-E3-E4-E5	Azioni del Valutatore previste nella parte "Assurance-Effectiveness" fino al livello E5 dei criteri ITSEC
E1-E2-E3-E4-E5-E6	Azioni del Valutatore previste nella parte "Assurance-Effectiveness" fino al livello E6 dei criteri ITSEC

Tabella 2: Tipologie standard di accreditamento per i Common Criteria

Tipologie	Portata dell'accreditamento
EAL1	Azioni associate alla valutazione delle componenti di garanzia al livello EAL1 (*)
EAL1-EAL2	Azioni associate alla valutazione delle componenti di garanzia al livello EAL2 (*)
EAL1-EAL2-EAL3	Azioni associate alla valutazione delle componenti di garanzia al livello EAL3 (*)
EAL1-EAL2-EAL3-EAL4	Azioni associate alla valutazione delle componenti di garanzia al livello EAL4 (*)
EAL1-EAL2-EAL3-EAL4-EAL5	Azioni associate alla valutazione delle componenti di garanzia al livello EAL5
EAL1-EAL2-EAL3-EAL4-EAL5-EAL6	Azioni associate alla valutazione delle componenti di garanzia al livello EAL6
EAL1-EAL2-EAL3-EAL4-EAL5-EAL6-EAL7	Azioni associate alla valutazione delle componenti di garanzia al livello EAL7

(*) Le azioni del Valutatore per questo livello di valutazione sono descritte in [CEM].

2.2 Validità e durata dell'accreditamento

130 Agli LVS che otterranno l'accreditamento ad operare nell'ambito dello Schema verrà rilasciato un Certificato di Accreditamento in cui viene riportata la tipologia e la portata dell'accreditamento stesso.

L'accreditamento ha una validità di tre anni. Durante tale periodo, l'Organismo di Certificazione effettuerà delle visite ispettive, tipicamente con frequenza annuale,

finalizzate a verificare il perdurare delle condizioni necessarie ad operare nell'ambito dello Schema.

Al termine dei tre anni, la validità dell'accreditamento dovrà essere confermata dall'Organismo di Certificazione, attraverso visita ispettiva o altri controlli che l'OC dovesse ritenere opportuni. Le modalità specifiche verranno comunicate all'LVS con congruo anticipo.

La variazione della tipologia dell'accreditamento potrà essere richiesta in qualsiasi momento da un LVS. Le procedure di variazione sono simili a quelle previste per l'accreditamento iniziale e vengono attivate mediante una richiesta formale alla Sezione Accreditamento dei Laboratori dell'OC. L'Organismo di Certificazione si riserva la facoltà di estendere temporaneamente la portata dell'accreditamento di un LVS, su richiesta esplicita di quest'ultimo, per lo svolgimento di una specifica valutazione che richieda un livello di valutazione 'con aggiunta' (*augmented* nella terminologia dei Common Criteria).

2.3 Entità coinvolte nel processo di accreditamento

La struttura generale del processo di accreditamento coinvolge le seguenti entità:

- il laboratorio richiedente l'accreditamento;
- la Sezione Accreditamento dei Laboratori dell'Organismo di Certificazione;
- gli Ispettori;
- la Commissione Tecnico-consultiva;
- l'Organismo di Certificazione.

2.3.1 Laboratorio richiedente l'accreditamento

Il laboratorio richiedente l'accreditamento può essere un organismo pubblico o una impresa regolarmente registrata secondo le norme vigenti.

Il laboratorio, all'inizio della procedura, deve indicare un responsabile per i rapporti con la Sezione Accreditamento: tale responsabile sarà l'unica persona autorizzata a intrattenere rapporti formali durante la procedura di accreditamento.

2.3.2 Sezione Accreditamento dei Laboratori dell'Organismo di Certificazione

La Sezione Accreditamento dei Laboratori è la struttura dell'Organismo di Certificazione che gestisce e coordina l'intero processo di accreditamento.

Il Responsabile della Sezione Accreditamento svolge i seguenti ruoli:

- è la persona responsabile per l'OC dei rapporti formali con il Responsabile del laboratorio, sia durante la procedura di accreditamento sia durante le procedure legate al mantenimento dell'accreditamento nel tempo;
- nomina gli Ispettori incaricati ad effettuare le verifiche previste;
- coordina e supervisiona l'attività degli Ispettori;

- redige per ogni richiesta di accreditamento ricevuta, sulla base del Rapporto Finale di Visita Ispettiva redatto dagli Ispettori[1], il Rapporto Finale di Accreditamento da sottoporre alla Commissione Tecnico-consultiva;
- convoca la Commissione Tecnico-consultiva;
- gestisce l'elenco degli Ispettori autorizzati;
- gestisce l'elenco dei laboratori accreditati;
- gestisce l'elenco dei Valutatori abilitati ad operare negli LVS.

2.3.3 Ispettori

L'Organismo di Certificazione si avvale di Ispettori da lui riconosciuti per effettuare le verifiche previste da questa Linea Guida per l'accreditamento dei laboratori. Gli Ispettori vengono incaricati dal Responsabile della Sezione Accreditamento.

L'attività svolta dagli Ispettori si suddivide essenzialmente in tre fasi:

1. verifica della documentazione di qualità fornita dal laboratorio;
2. verifica della competenza tecnica del laboratorio nel suo insieme e dei singoli componenti lo staff tecnico;
3. esecuzione di visite ispettive presso la sede del laboratorio.

Gli Ispettori durante la loro attività possono interagire con il Responsabile del laboratorio al fine di richiedere modifiche e integrazioni alla documentazione e alle procedure.

Gli Ispettori devono fornire al Responsabile della Sezione Accreditamento il Rapporto Finale di Visita Ispettiva, riguardante l'esito della visita ispettiva e di tutte le attività di verifica di competenza effettuate.

L'attività degli Ispettori è regolamentata da disposizioni specificate dalla Sezione Accreditamento dell'OC. Essi devono rispondere al Responsabile della Sezione Accreditamento dell'OC della corretta attuazione delle suddette disposizioni.

2.3.4 Commissione Tecnico-consultiva

La Commissione Tecnico-consultiva svolge il ruolo di garante della corretta applicazione delle procedure di accreditamento dei laboratori.

La Commissione è nominata con decreto del Ministro delle Comunicazioni ed è composta:

- da un rappresentante del Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri che ricopre il ruolo di Presidente della Commissione Tecnico-consultiva;
- dal Responsabile della Sezione Accreditamento dell'OC;

1 Nel caso in cui la procedura di accreditamento si interrompa prima che vengano coinvolti gli Ispettori, ovviamente non sarà disponibile il Rapporto finale di Visita Ispettiva. In questo caso, il Responsabile della Sezione accreditamento è comunque tenuto a redigere il Rapporto Finale di Accreditamento e sottoporlo alla Commissione tecnico-consultiva

– da un rappresentante del Ministero dello Sviluppo Economico.

Alla Commissione Tecnico-consultiva viene fornita dal Responsabile della Sezione Accreditamento tutta la documentazione relativa ad una pratica di accreditamento, indipendentemente dall'esito delle verifiche ispettive effettuate.

La Commissione Tecnico-consultiva deve esprimere, con voto unanime, il parere finale sull'accreditamento del laboratorio.

La Commissione redige, per ogni pratica analizzata, il Rapporto di Certificazione dell'Accreditamento.

2.3.5 Organismo di Certificazione

L'OC emette il Certificato di Accreditamento sulla base del Rapporto di Certificazione dell'Accreditamento;

2.4 Durata del processo di accreditamento

La durata del processo di accreditamento fino all'emissione del Rapporto Finale di Visita Ispettiva, conteggiata a partire dalla ricezione della attestazione di pagamento dell'importo specificato nel preventivo emesso dall'OC per le attività di accreditamento, è stimata in circa 60 giorni lavorativi. Tale stima è stata effettuata sotto le seguenti ipotesi:

– il Manuale di Qualità fornito è essenzialmente corretto;
– le procedure di attuazione del Manuale di Qualità sono corrette;
– il laboratorio possiede all'atto della richiesta di accreditamento tutti i requisiti formali necessari;
– adeguata competenza tecnica del personale operante nel laboratorio;
– gli impegni economici sono stati rispettati.

L'LVS può richiedere all'OC, motivandola, una o più sospensioni delle attività di accreditamento. In ogni caso, se il processo di accreditamento a causa della/delle sospensioni non si conclude entro 180 giorni dalla presentazione della richiesta di accreditamento, l'OC si riserva di concludere con esito negativo il processo. L'LVS in questo caso è comunque tenuto a versare all'OC il saldo per le attività di accreditamento effettuate nel periodo dei 180 giorni.

2.5 Gestione dei conflitti tra LVS e la Sezione Accreditamento dell'OC

Ogni controversia inerente le attività di accreditamento dei laboratori deve essere riferita alla Commissione Tecnico-consultiva che ha il compito di dirimere le controversie.

2.6 Sospensione e revoca dell'accreditamento

La Sezione Accreditamento dell'OC può sospendere o revocare la validità dell'accreditamento di un LVS, motivando dettagliatamente le ragioni della sospensione o della revoca. Tali azioni possono essere determinate dal venir meno, nel corso del tempo, delle condizioni sotto le quali è stato ottenuto l'accreditamento.

3 La procedura di accreditamento

L' accreditamento di un LVS si svolge in tre fasi:

1. richiesta di accreditamento;
2. istruttoria della richiesta;
3. rilascio dell'accreditamento.

Nella Figura 1 viene fornito uno schema riassuntivo di tutte le azioni che caratterizzano la procedura di accreditamento di un LVS.

3.1 Richiesta di accreditamento

La richiesta di accreditamento deve essere indirizzata a:

Ministero delle Comunicazioni
ISCOM
Uff. VI, OCSI - Sezione Accreditamento dei Laboratori
Viale America, 201
00144 ROMA

La richiesta di accreditamento puo' essere presentata da un organismo pubblico o da una impresa regolarmente registrata secondo le norme vigenti.
La richiesta deve contenere le seguenti indicazioni:

1. nome e ragione sociale del laboratorio candidato;
2. indirizzo della sede del laboratorio candidato;
3. tipologia e livello dell'accreditamento richiesto;
4. nominativo del Responsabile dei rapporti con l'OC;
5. nominativo delle persone coinvolte operativamente nell'attività di laboratorio e, per i Valutatori, il profilo di orientamento di ciascuno (Documentale o Operativo)
6. dichiarazione di impegno a sostenere le spese relative all'accreditamento del laboratorio;
7. firma del Legale Rappresentante per il laboratorio.

Sulla base delle informazioni presenti nella richiesta di accreditamento, L'OC emette, entro 15 giorni lavorativi dal ricevimento della richiesta, un preventivo di spesa per l'accreditamento dell'LVS.

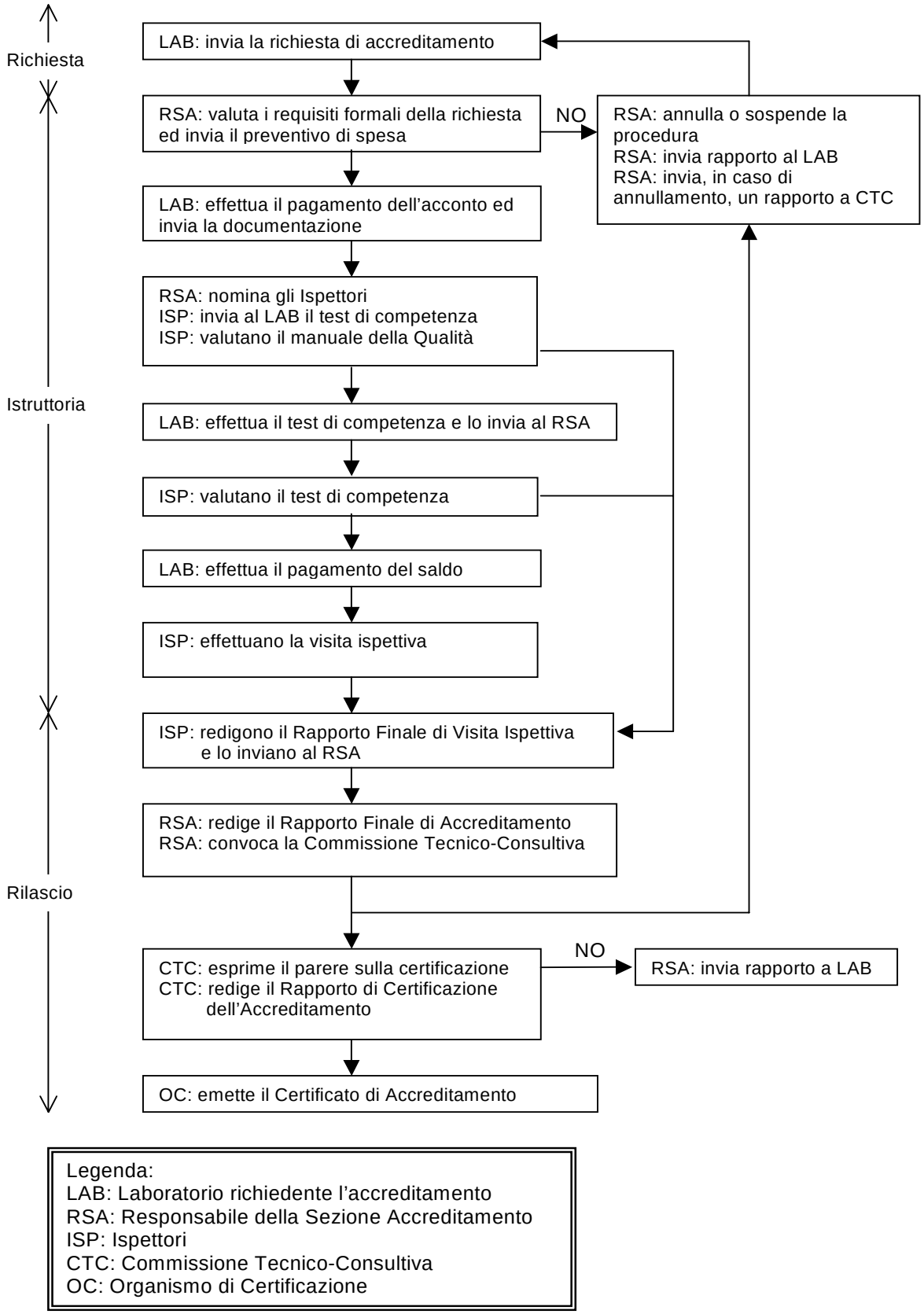
Il richiedente, ricevuto il preventivo, per avviare la fase delle verifiche di competenza e dell'organizzazione del Laboratorio deve presentare la seguente documentazione:

1. Attestazione di pagamento dell'acconto specificato nel preventivo;

2. Manuale della qualità del laboratorio redatto secondo le norme [UNI1] e tenendo in conto le competenze tecniche richieste descritte nell'Appendice A;
3. Curriculum Vitae dei valutatori;
4. Certificato di iscrizione alla Camera di commercio, industria, artigianato e agricoltura qualora si configuri come impresa nazionale o documentazione equivalente per imprese non nazionali;
5. Attestazione comprovante l'appartenenza, solo quando di pertinenza, ad una Amministrazione dello Stato o Ente Pubblico.

Si osservi che il laboratorio richiedente l'accreditamento, superata la fase delle verifiche di competenza e dell'organizzazione del Laboratorio, e comunque 10 giorni solari prima della data dell'effettuazione della verifica ispettiva finale, deve presentare all'OC l'attestazione di pagamento del saldo specificato nel preventivo.

Figura 1 – Schema riassuntivo della procedura di accreditamento



Legenda:
LAB: Laboratorio richiedente l'accreditamento
RSA: Responsabile della Sezione Accreditamento
ISP: Ispettori
CTC: Commissione Tecnico-Consultiva
OC: Organismo di Certificazione

3.2 Fase di istruttoria della richiesta

La fase di istruttoria della richiesta prevede due attività fondamentali: la verifica dei requisiti imposti dalla norma [UNI1] e la verifica di requisiti riguardanti la competenza tecnica sia del laboratorio nel suo insieme sia dei singoli componenti il laboratorio stesso.

3.2.1 Verifica dei requisiti

Dopo aver ricevuto la richiesta di accreditamento (precedentemente registrata in un apposito repertorio in ordine cronologico di ricezione presso la segreteria dell'OC), il Responsabile della Sezione Accreditamento dell'OC provvede all'esame della documentazione presentata verificando l'esistenza dei requisiti generali prescritti.

In caso di esito positivo, il Responsabile della Sezione Accreditamento in cooperazione con la segreteria dell'OC, comunica al laboratorio richiedente il preventivo di spesa per le attività di accreditamento.

L'eventuale esito negativo dell'esame della richiesta è comunicato al richiedente con le relative motivazioni.

All'atto della presentazione della documentazione, comprensiva della ricevuta di pagamento dell'acconto specificato nel preventivo, il Responsabile della Sezione Accreditamento nomina uno o più Ispettori scelti tra quelli inseriti in un apposito elenco tenuto presso la Sezione Accreditamento, conferendo ad uno degli Ispettori il ruolo di Team Leader. Il Team Leader è il referente per le comunicazioni con l'LVS relative alle fasi di ispezione. Gli Ispettori nominati hanno l'incarico di esaminare in dettaglio la documentazione fornita dall'LVS e di effettuare le verifiche tecniche necessarie al fine di confermare l'adeguata competenza dell'LVS e la corretta applicazione delle procedure previste, in conformità alla norma [UNI1] e con la presente Linea Guida.

In caso di non conformità riscontrate dagli Ispettori, il Responsabile della Sezione Accreditamento può:

- annullare la procedura di accreditamento;
- sospendere la procedura di accreditamento;
- fissare modalità e termini per l'adeguamento del Manuale della Qualità o per l'integrazione della competenze.

Al termine dell'analisi del Manuale della Qualità, con esito positivo, e in presenza di risultato positivo anche per i test di verifica delle competenze tecniche (vedi paragrafo successivo), gli Ispettori provvedono ad organizzare le visite ispettive (verifica ispettiva finale) presso la sede del laboratorio richiedente l'accreditamento. Durante l'attività ispettiva in loco verranno verificate le procedure di attuazione di quanto descritto nel Manuale della Qualità e verranno svolti degli ulteriori colloqui tecnici per

verificare la competenza individuale dei singoli Valutatori. Gli Ispettori potranno richiedere, se necessario, variazioni o integrazioni della documentazione fornita.

Gli Ispettori, sulla base delle risultanze emerse dalla loro attività ispettiva complessiva, provvedono ad inoltrare al Responsabile della Sezione Accreditamento un Rapporto Finale di Verifica Ispettiva.

La ricezione del Rapporto Finale di Verifica Ispettiva da parte del Responsabile della Sezione Accreditamento conclude la fase di istruttoria della richiesta.

3.2.2 Verifica dei requisiti riguardanti la competenza tecnica

La valutazione della competenza tecnica del laboratorio è finalizzata a verificare la capacità del laboratorio ad eseguire valutazioni e prove come descritto in Appendice A.

Nel caso di esito positivo dell'esame dei requisiti generali, il Responsabile della Sezione Accreditamento, o l'Ispettore da lui nominato, invia al laboratorio richiedente il test finalizzato a verificare la competenza tecnica del laboratorio richiedente.

Il laboratorio, utilizzando esclusivamente le competenze del proprio personale, dovrà completare il test proposto e inviarlo al Responsabile della Sezione Accreditamento che provvederà ad inoltrarlo agli Ispettori incaricati.

Il test di competenza potrà riguardare uno o più dei seguenti argomenti:

1. le procedure previste dallo Schema;
2. i criteri ITSEC e/o Common Criteria e le relative metodologie;
3. effettuazione della valutazione, completa o parziale, di un prodotto o di un sistema IT in accordo con quanto previsto dallo Schema e dai criteri ITSEC o Common Criteria e dalle relative metodologie;
4. produzione di documentazione atta a costituire materiale di documentazione per la valutazione di un prodotto o sistema IT;
5. elementi generali di sicurezza IT.

Durante la visita ispettiva saranno effettuate ulteriori verifiche di competenza tecnica rivolte sia al laboratorio nel suo insieme sia ai singoli componenti dello staff tecnico, tenendo in conto anche le specifiche competenze dichiarate nel Manuale della Qualità. Gli elementi generali di sicurezza IT oggetto di verifica di competenza tecnica sono quelli indicati nell'Appendice A.

Nel caso in cui il test di competenza abbia esito negativo, gli Ispettori non effettuano la visita ispettiva e inoltrano al Responsabile della Sezione Accreditamento un rapporto. Il Responsabile della Sezione Accreditamento, sulla base di quanto evidenziato dagli Ispettori, può:

1. annullare la procedura di accreditamento;
2. sospendere la procedura di accreditamento.

L'esito delle verifiche di competenza tecnica verrà incluso dagli Ispettori nel Rapporto Finale di Visita Ispettiva.

3.3 Fase di rilascio dell'accreditamento

Il Responsabile della Sezione Accreditamento, ricevuto il Rapporto Finale di Visita Ispettiva, predispone un Rapporto Finale di Accreditamento e convoca la Commissione Tecnico-consultiva che deve esprimere un parere (positivo o negativo) sull'accreditamento del laboratorio. La Commissione, prima di esprimere il suo parere in forma definitiva, ha facoltà di richiedere al Responsabile della Sezione Accreditamento di predisporre indagini supplementari.

In caso di parere positivo della Commissione, l'Organismo di Certificazione predispone ed emette il Certificato di accreditamento del laboratorio.

In caso di parere negativo della Commissione, il Responsabile della Sezione Accreditamento comunica al laboratorio richiedente l'esito e le motivazioni per le quali la domanda di accreditamento non può essere accolta.

4 Norme operative

4.1 Attività dell'LVS

Un LVS può svolgere, oltre alla attività di valutazione, anche le seguenti attività:

a) Assistenza al Committente per:
   1) la stesura della documentazione di sicurezza durante la preparazione della valutazione;
   2) la determinazione della valutabilità del TDS, ODV o Profilo di Protezione;
   3) le attività connesse con la gestione e il mantenimento dei Certificati.

b) Formazione sulle tematiche della sicurezza nel settore della tecnologia dell'informazione in generale e, in particolare, sulle tecniche di valutazione.

L'LVS, ogni volta che effettua una delle suddette attività, è tenuto a darne comunicazione preventiva all'OC.

4.2 Cooperazione tra l'LVS e l'Organismo di Certificazione

Un LVS deve fornire all'OC e ai suoi rappresentanti tutta la cooperazione necessaria al fine di verificare che le prescrizioni previste dallo Schema siano correttamente realizzate. Questa cooperazione comprende, ad esempio, la possibilità da parte dell'OC di presenziare, in determinate fasi, le attività di valutazione.

Un LVS deve comunicare tempestivamente all'OC ogni variazione della sua identità giuridica, nonché ogni variazione riguardante l'organico o la strumentazione rispetto alla situazione verificata dall'OC nella fase di accreditamento o nell'ultima visita ispettiva di controllo effettuata.

Un LVS deve partecipare, su richiesta dell'OC, a scambi di informazioni tecniche con altri LVS riguardanti le modalità di applicazione dei criteri e delle procedure dello Schema, al fine di migliorare la qualità e l'efficacia dello Schema stesso.

4.3 I Valutatori

Al personale tecnico la cui competenza sia stata verificata durante la procedura di accreditamento o durante una visita ispettiva periodica viene riconosciuta la qualifica di "Valutatore".

La qualifica di Valutatore può essere riconosciuta secondo due profili distinti:

- Valutatore Documentale, svolge l'attività di analisi e scrittura della documentazione di valutazione;
- Valutatore Operativo, svolge il ruolo di verifica e predisposizione dei test funzionali, delle prove di intrusione e di analisi delle vulnerabilità dell'ODV.

Un Valutatore può ottenere l'accreditamento per entrambi i profili. La qualifica di Valutatore è valida solo ed esclusivamente all'interno di un LVS.

In un LVS è richiesto un numero minimo tre persone operanti nel laboratorio, con almeno due valutatori (uno per ogni profilo) in aggiunta al Responsabile dell'LVS.

I Valutatori. in base all'esperienza, potranno assumere il ruolo di Valutatore senior nel profilo di competenza accertato all'atto dell'inserimento, dopo aver svolto attività ufficiali in almeno tre processi completi di valutazione o almeno tre anni di esperienza lavorativa.

4.4 Il Responsabile del Laboratorio

Il Responsabile del Laboratorio è chiamato a rispondere delle attività svolte complessivamente dall'LVS, a mantenere i rapporti con l'OC, a nominare i Valutatori del gruppo di valutazione e il Responsabile per l'LVS in ogni singola valutazione.

Inoltre, il Responsabile del Laboratorio deve dare comunicazione immediata in modo formale all'OC su qualsiasi variazione del personale impegnato nel laboratorio o di qualsiasi modifica significativa rispetto alle informazioni fornite in fase di accreditamento.

Qualora il Responsabile del Laboratorio non fosse disponibile (ad esempio perché non ancora designato o perché non più in carica) i rapporti con l'OC verranno mantenuti da un responsabile designato dalla direzione dell'impresa a cui fa capo il laboratorio, in base a quanto indicato nel relativo manuale di qualità.

4.5 Gruppo di valutazione

Il personale tecnico che svolge una valutazione (Gruppo di Valutazione) deve avere una competenza tecnica adeguata ed essere in numero sufficiente per completare i compiti richiesti dal Piano di Valutazione. La stima dell'adeguatezza del Gruppo di Valutazione e, in particolare, del Responsabile della valutazione, è di pertinenza esclusiva dell'Organismo di Certificazione.

4.6 Competenza tecnica

Tutto il personale tecnico di un LVS deve possedere una adeguata preparazione nel campo della sicurezza IT, deve conoscere lo Schema e i criteri ITSEC e/o Common Criteria e le relative metodologie. Inoltre, dovrà essere in grado di svolgere attività di redazione ed analisi della documentazione di valutazione nonché di verificare la corretta operatività di un ODV.

In fase di accreditamento e durante le visite ispettive periodiche viene normalmente verificata la competenza di ogni componente dell'LVS, secondo quanto previsto nella presente Linea Guida.

L'OC si riserva la possibilità di verificare la competenza tecnica del personale di un LVS anche in tempi diversi dalle visite ispettive periodiche, ad esempio quando si verifichi una qualsiasi variazione nella composizione dell'organico dell'LVS rispetto a quanto dichiarato nel Manuale di Qualità: immissione di nuovo personale, variazione di compiti e responsabilità anche di personale già in forze all'LVS stesso, ecc.

4.7 Impiego di esperti esterni all'LVS

Nello svolgimento delle sue attività di valutazione o di assistenza, l'LVS potrebbe avere la necessità di avvalersi, anche per un periodo di tempo limitato, delle prestazioni di esperti su particolari tematiche si sicurezza. In tal caso dovrà darne tempestiva comunicazione all'OC, indicando il nome degli esperti esterni coinvolti e le modalità del loro contributo. La stima dell'adeguatezza degli esperti proposti per la partecipazione ad una attività di valutazione è di pertinenza esclusiva dell'Organismo di Certificazione.

5 Gli Assistenti

Lo Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione prevede il ruolo di Assistente.

L'Assistente è una persona abilitata a fornire assistenza al Committente, al Fornitore o a un LVS nella fase di stesura della documentazione per la valutazione di un ODV. Inoltre, l'Assistente può curare la gestione del Certificato come descritto nella LGP1.

Per uno stesso ODV, il ruolo di Assistente è incompatibile con il ruolo di Valutatore.

L'abilitazione ad Assistente può essere rilasciata secondo due profili distinti:

- Assistente Documentale, svolge l'attività di analisi e scrittura della documentazione di valutazione;
- Assistente Operativo, svolge il ruolo di progettazione e produzione di test funzionali, delle prove di intrusione e delle analisi di vulnerabilità dell'ODV.

L'Assistente deve garantire:

1. l'imparzialità, l'indipendenza, la riservatezza e l'obiettività nello svolgimento del proprio ruolo;
2. la capacità di mantenere nel tempo i requisiti in virtù dei quali è stato abilitato.

5.1 Competenza tecnica

Il candidato al ruolo di Assistente deve possedere una adeguata preparazione nel campo della sicurezza IT, deve conoscere lo Schema e i criteri ITSEC e/o Common Criteria e le relative metodologie.

Inoltre, dovrà essere in grado di svolgere attività di redazione ed analisi della documentazione di valutazione nonché di verificare la corretta operatività di un ODV.

5.2 Richiesta di abilitazione

La persona interessata all'abilitazione al ruolo di Assistente deve presentare formale richiesta all'OC, corredata dal Curriculum Vitae, specificando, in particolare, la propria esperienza nel campo della sicurezza IT.

5.3 Rilascio dell'abilitazione

Il rilascio dell'abilitazione è subordinato al superamento di un test di valutazione, propostogli dall'OC, sulla competenza tecnica del richiedente. Il suddetto test è volto ad accertare da un lato la competenza tecnica in materia di sicurezza IT e la conoscenza dei criteri di valutazione di sicurezza, dall'altro della padronanza nell'uso delle metodologie per la redazione e l'analisi della documentazione di valutazione e per la verifica della corretta operatività di un ODV.

5.4 Durata dell'abilitazione

L'abilitazione ha una durata di tre anni.

L'OC si riserva la facoltà di verificare, nel periodo di validità dell'abilitazione, il mantenimento dei requisiti per lo svolgimento del ruolo di Assistente.

5.5 Elenco degli Assistenti

L'OC mantiene l'elenco degli Assistenti abilitati a operare nell'ambito dello Schema.

5.6 Gestione dei conflitti tra l'Assistente e l'OC

Ogni controversia inerente le attività di abilitazione di un Assistente deve essere riferita alla Commissione Tecnico-consultiva.

5.7 Sospensione e revoca dell'abilitazione

L'OC può sospendere o revocare l'abilitazione di un Assistente, motivando dettagliatamente le ragioni della sospensione o della revoca. Tali azioni possono essere determinate dal venir meno, nel corso del tempo, delle condizioni sotto le quali è stato ottenuta l'abilitazione.

6 Appendice A - Competenze tecniche dell'LVS

Gli LVS dovranno essere in grado di effettuare valutazioni e prove che riguardano le realizzazioni dei seguenti servizi di sicurezza:

- Riservatezza
- Integrità
- Disponibilità
- Autenticazione
- Non ripudio

Alcune aree in cui saranno effettuate le prove sono (la lista non è esaustiva):

- Sicurezza nei malfunzionamenti
- Aggiramento delle funzionalità di sicurezza
- Separazione logica dei dati
- Controllo d'accesso
- Accountability
- Tolleranza ai malfunzionamenti
- Robustezza
- Selftest
- Protezione fisica (prevenzione e rilevamento del tampering)
- Protezione ambientale
- Accesso al servizio
- Archiviazione di informazioni critiche per la sicurezza
- Interfacce
- Allarmistica
- Audit di sicurezza

Alcune delle tecniche che saranno utilizzate sono (la lista non è esaustiva)

- Test a risposta nota
- Tracciamento dei requisiti di sicurezza
- Analisi e revisione formale
- Prove funzionali
- Test di intrusione
- Analisi di vulnerabilità
- Revisione del codice sorgente
- Prove sul codice eseguibile
- Revisione della documentazione

7 Riferimenti bibliografici

[CC1] CCMB-2005-08-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, version 2.3, agosto 2005

[CC2] CCMB-2005-08-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional requirements”, version 2.3, agosto 2005

[CC3] CCMB-2005-08-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance requirements”, version 2.3, agosto 2005

[CEM] CCMB-2005-08-004, “Common Evaluation Methodology for Information Technology Security Evaluation – Evaluation Methodology”, version 2.3, agosto 2005

[ISO1] ISO/IEC 2382-8 “Information technology – Vocabulary” – Part 8: Security, 1998

[ISO2] ISO/IEC TR 15446 “Information technology – Security techniques – Guide for the production of Protection Profiles and Security Targets”, dicembre 2003

[ITS1] Information Technology Security Evaluation Criteria, version 1.2, giugno 1991

[ITS2] Information Technology Security Evaluation Manual, version 1.0, settembre 1993

[SGC] OCSI, Procedure dello Schema di Gestione dei Certificati

[UNI1] UNI/CEI EN ISO/IEC 17025 Requisiti generali per la competenza dei laboratori di prova e di taratura, 2000.

8 Lista degli acronimi

EAL	=	(Evaluation Assurance Level) Livello di garanzia della valutazione
IT	=	Information Technology
LVS	=	Laboratorio di Valutazione della Sicurezza
NAV	=	Nota per Anomalia nella Valutazione
NEV	=	Nota per Errore nella Valutazione
NIL	=	Notifica di Inizio Lavori
NIS	=	Nota Informativa dello Schema
NOC	=	Nota dell'Organismo di Certificazione
NT	=	Nota Tecnica
OC	=	Organismo di Certificazione
ODV	=	Oggetto Della Valutazione (TOE - Target of Evaluation)
OSP	=	(Organisational Security Policy) Politica di Sicurezza di un'Organizzazione
PGC	=	Piano per la Gestione del Certificato
PDV	=	Piano Di Valutazione
PP	=	Profilo di Protezione
RA	=	Rapporto di Attività
RAL	=	Riunione di Avvio dei Lavori
RC	=	Rapporto di Certificazione
RCC	=	Rapporto di Classificazione delle Componenti dell'ODV
RFV	=	Rapporto Finale di Valutazione
RGC	=	Responsabile per la Gestione del Certificato
RM	=	Rapporto delle Metodologie
RO	=	Rapporto di Osservazione
ROA	=	Rapporto di Osservazione: Anomalia
ROE	=	Rapporto di Osservazione: Errore
ROS	=	Rapporto di Osservazione sullo Schema
SAR	=	(Security Assurance Requirement) Requisito di Garanzia
SGC	=	Schema di Gestione dei Certificati
SFP	=	(Security Function Policy) Politica della Funzione di Sicurezza
SFR	=	(Security Functional Requirement) Requisito Funzionale di Sicurezza
SOF	=	(Strength of Function) Robustezza di una Funzione di Sicurezza
TDS	=	Traguardo di Sicurezza (ST - Security Target)
TSF	=	(TOE Security Function) Funzione di Sicurezza dell'ODV
TSP	=	(TOE Security Policy) Politica di Sicurezza dell'ODV
UL	=	Unità di Lavoro