Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione

Organismo di Certificazione

Descrizione Generale dello Schema Nazionale

Linee Guida Provvisorie - parte 1

LGP1

Dicembre 2004

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.

Paragrafo e/o linea	Pagine modificate	Modifica effettuata da: nominativo e firma	Data

INDICE

1 Introduzione

L'istituzione dell'Organismo di Certificazione (OC) italiano per la sicurezza dei sistemi e dei prodotti nel settore della tecnologia dell'informazione, avvenuta attraverso un decreto ("Approvazione dello schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione", GU n. 98 del 27-4-2004) 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.

In questo contesto il decreto identifica:

- la necessità di individuare un Organismo di Certificazione e di definire uno Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione, di seguito denominato "Schema nazionale", recante l'insieme delle procedure e delle regole nazionali necessarie per la valutazione e certificazione, in conformità ai criteri europei ITSEC (Information Technology Security Evaluation Criteria) [ITS1] o agli standard internazionali CC (Common Criteria) [CCI1,2,3], emanati dall'ISO;
- la definizione, nell'ambito dello Schema nazionale, della 'sicurezza nel settore della tecnologia dell'informazione' come la protezione della riservatezza, integrità, disponibilità delle informazioni mediante il contrasto delle minacce originate dall'uomo o dall'ambiente, al fine di impedire, a coloro che non siano stati autorizzati, l'accesso, l'utilizzo, la divulgazione, la modifica delle informazioni stesse e di garantirne l'accesso e l'utilizzo a coloro che siano stati autorizzati.

Le motivazioni di tali necessità e definizioni derivano dalle seguenti considerazioni:

- l'informazione, nell'attuale società, costituisce un bene essenziale e si rende necessario garantirne l'integrità, la disponibilità e la riservatezza con misure di sicurezza che costituiscano parte integrante di un sistema informatico;
- da tempo i produttori offrono sistemi e prodotti dotati di funzionalità di sicurezza, per le quali dichiarano caratteristiche e prestazioni al fine di orientare gli utenti nella scelta delle soluzioni più idonee a soddisfare le proprie esigenze;
- in molte applicazioni caratterizzate da un elevato grado di criticità, le predette dichiarazioni potrebbero risultare non sufficienti, rendendo necessaria una loro valutazione e certificazione della sicurezza, condotte da soggetti indipendenti e qualificati, sulla base di standard riconosciuti a livello nazionale ed internazionale;

- le garanzie concernenti l'adeguatezza, la qualità e l'efficacia dei dispositivi di sicurezza di un sistema informatico possono essere fornite solo da certificatori e valutatori indipendenti ed imparziali;
- la necessità di favorire, a livello comunitario e internazionale, la cooperazione tra gli Organismi di Certificazione e il mutuo riconoscimento dei certificati di valutazione della sicurezza nel settore della tecnologia dell'informazione.

In aggiunta a queste considerazioni, a corollario normativo e politico della scelta di istituire un Organismo di Certificazione possono essere schematicamente elencati i seguenti punti fondamentali:

- la risoluzione del Consiglio dell'Unione Europea del 28 gennaio 2002 (2002/C 43/02) relativa ad un approccio comune e ad azioni specifiche nel settore della sicurezza delle reti e dell'informazione;
- la decisione della Commissione Europea del 6 novembre 2000 (2000/709/CE) relativa ai criteri minimi di cui devono tener conto gli Stati membri all'atto di designare gli organismi di cui all'articolo 3, paragrafo 4, della direttiva 1999/93/CE del Parlamento Europeo e del Consiglio, relativa ad un quadro comunitario per le firme elettroniche;
- il varo delle norme UNI CEI EN ISO/IEC 17025 concernenti i requisiti generali per la competenza dei laboratori di prova e di taratura e UNI CEI EN 45011 concernenti i requisiti generali relativi agli organismi che gestiscono sistemi di certificazione di prodotti;
- l'esistenza dei criteri ITSEC, dal giugno 1991, e ITSEM (Information Technology Security Evaluation Manual) [ITS2], dal settembre 1993;
- la raccomandazione del Consiglio dell'Unione Europea (95/144/CE) in data 7 aprile 1995, concernente l'applicazione dei criteri ITSEC per la valutazione della sicurezza della tecnologia dell'informazione;
- l'atto del Comitato di gestione dell'ISO (International Standard Organization) che definisce come International Standard ISO/IEC 15408 i "Common Criteria for Information Technology Security Evaluation".

In questo contesto, 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 l'Organismo di Certificazione ha predisposto le "Linee Guida Provvisorie" (LGP). Sarà compito dell'Organismo di

Certificazione predisporre entro 12 mesi dalla pubblicazione del decreto, le "Linee Guida Definitive", recanti indicazioni dettagliate relative allo svolgimento delle attività di valutazione e certificazione.

Le Linee Guida Provvisorie sono organizzate in documenti distinti, brevemente descritti di seguito.

LGP1 - *Descrizione generale dello Schema nazionale di valutazione e certificazione della sicurezza*

La LGP1, dopo aver introdotto il concetto di Schema nazionale, di sicurezza IT e di accreditamento dei laboratori, affronta una descrizione sintetica del processo di valutazione, identificando le finalità e i requisiti generali per svolgere una valutazione e certificazione di un sistema/prodotto o Profilo di Protezione. Quindi, vengono definiti e descritti i ruoli dei soggetti coinvolti nel processo di valutazione e certificazione, con particolare enfasi per l'Organismo di Certificazione, il Laboratorio per la Valutazione della Sicurezza, il Committente, il Fornitore e l'Assistente. Inoltre, vengono delineate le tre fasi che caratterizzano il processo di valutazione: la preparazione, la conduzione e la conclusione. Infine, viene delineata la fase di certificazione e si forniscono delle informazioni per quanto concerne la gestione dei Certificati e il loro mantenimento.

LGP2 - *Accreditamento degli LVS e abilitazione degli Assistenti*

La LGP2 definisce le procedure per ottenere e mantenere nel corso del tempo l'accreditamento di un Laboratorio per la Valutazione della Sicurezza informatica 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 Laboratorio per la Valutazione della Sicurezza 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.

LGP3 - *Procedure di valutazione*

La LGP3 definisce le procedure che devono essere seguite nel corso di un processo di valutazione condotto all'interno dello Schema. Tale processo è suddiviso in tre fasi distinte: preparazione, conduzione e conclusione. Le procedure descritte in questa linea guida sono applicabili alla valutazione della sicurezza di un sistema/prodotto o di un Profilo di Protezione, così come definiti in ITSEC o nei Common Criteria, e descrivono le modalità secondo cui effettuare:

- le comunicazioni tra un Laboratorio per la Valutazione della Sicurezza, un Committente, un Fornitore e l'Organismo di Certificazione;
- l'organizzazione e la pianificazione delle attività di una valutazione;
- la finalità e il contenuto delle diverse tipologie di rapporti prodotti nel corso della valutazione;
- il controllo di una valutazione;

- la pubblicazione dei risultati di una valutazione;
- la chiusura della valutazione e il processo di certificazione con il rilascio da parte dell'Organismo di Certificazione del Certificato.

LGP4 – *Attività di valutazione secondo i Common Criteria*

La LGP4 si prefigge l'obiettivo di definire la terminologia di riferimento in lingua italiana per descrivere, discutere e analizzare l'insieme minimo di unità di lavoro in cui possono essere decomposte le azioni di valutazione richieste per svolgere la valutazione di un Profilo di Protezione e la valutazione di un sistema/prodotto ai livelli di garanzia EAL1, EAL2, EAL3 e EAL4 secondo i Common Criteria. Tutti i punti relativi alla valutazione di un ODV o di un Profilo di Protezione contenuti nella LGP4 sono stati sviluppati tenendo conto dello stato della normativa al gennaio 2004.

La LGP4 contiene informazioni utili agli utenti finali di prodotti/sistemi IT che sono stati sottoposti al processo di valutazione, al personale direttamente responsabile della valutazione di un sistema/prodotto o di un Profilo di Protezione, al personale che fornisce assistenza al Committente di una valutazione, al personale responsabile della stesura di un Traguardo di Sicurezza o di un Profilo di Protezione, e agli sviluppatori di prodotti/sistemi IT che sono interessati a richiedere la valutazione e la certificazione dei loro prodotti/sistemi.

LGP5 - *Il Piano di Valutazione: indicazioni generali*

La LGP5 fornisce ai Valutatori gli elementi fondamentali per definire, in base ai Criteri di valutazione ITSEC e Common Criteria, un Piano Di Valutazione (PDV) della Sicurezza di un sistema/prodotto o di un Profilo di Protezione. Il PDV è il documento che contiene la descrizione di tutte le attività che i Valutatori debbono eseguire durante la valutazione e le modalità secondo le quali queste attività risultano organizzate, pianificate, correlate e suddivise nell'ambito del periodo di valutazione.

La necessità di fornire delle istruzioni per la definizione di un PDV nasce dall'esigenza di soddisfare più requisiti, quali:

- armonizzare tutta la documentazione e le procedure di valutazione alla normativa internazionale e nazionale in vigore;
- rendere omogenei e confrontabili i PDV prodotti da Laboratori per la Valutazione della Sicurezza diversi;
- garantire, mediante il rispetto delle Linee Guida, l'obiettività, l'imparzialità, la ripetitività e la riproducibilità delle attività di valutazione indicate in un PDV.

LGP6 – *Guida alla scrittura dei Profili di Protezione e dei Traguardi di Sicurezza*

Nella LGP6 sono fornite indicazioni per la scrittura dei Profili di Protezione (PP) e dei Traguardi di Sicurezza (TDS) secondo le norme fissate dai Common Criteria.

Questa LGP è indirizzata principalmente a coloro che sono coinvolti nello sviluppo dei PP/TDS. Tuttavia, può anche essere utile ai Valutatori e ai responsabili della

definizione e del controllo della metodologia per la valutazione dei PP/TDS. Gli utenti finali possono altresì trovare utile questo documento per comprendere i PP/TDS o per individuare le parti di loro interesse.

Viene dapprima fornita una panoramica sui PP/TDS, che comprende un indice di riferimento; vengono quindi descritte in dettaglio le sezioni del PP/TDS.

Infine, sono riportate alcune appendici che approfondiscono aspetti di particolare rilievo, tra cui la descrizione di esempi di minacce, politiche di sicurezza, assunzioni e obiettivi di sicurezza, e l'identificazione di adeguati componenti funzionali per specificare i requisiti funzionali di sicurezza.

LGP7 – *Glossario e terminologia di riferimento*

Nella LGP7 sono raccolte tutte le definizioni in uso nello Schema nazionale. Inoltre, è fornito un elenco di termini di uso comune che assumono un significato specifico nei Common Criteria.

2 Lo Schema nazionale

In questo capitolo viene presentata la descrizione generale dello Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione, di seguito denominato "Schema nazionale". Tale Schema nazionale raccoglie l'insieme delle procedure e delle regole necessarie per la valutazione e certificazione, in conformità ai criteri europei ITSEC o ai Common Criteria.

Le procedure relative allo Schema nazionale devono essere osservate dall'Organismo di Certificazione (OC), dai Laboratori per la Valutazione della Sicurezza (LVS), nonché da tutti coloro (persone fisiche, giuridiche e qualsiasi altro organismo o associazione) cui competono le decisioni in ordine alla richiesta, acquisizione, progettazione, realizzazione, installazione ed impiego di sistemi e prodotti nel settore della tecnologia dell'informazione, e che necessitano di una certificazione di sicurezza conforme ai criteri europei e agli standard internazionali esplicitati precedentemente.

Lo Schema nazionale non si applica per i sistemi e prodotti che trattino informazioni classificate.

2.1 La sicurezza IT

Nell'ambito dello Schema nazionale, la sicurezza nel settore della tecnologia dell'informazione consiste nella protezione della riservatezza, integrità, disponibilità delle informazioni mediante il contrasto delle minacce originate dall'uomo o dall'ambiente, al fine di impedire, a coloro che non siano stati autorizzati, l'accesso, l'utilizzo, la divulgazione, la modifica delle informazioni stesse, e di garantirne l'accesso e l'utilizzo a coloro che siano stati autorizzati.

2.2 L'Organismo di Certificazione e i Laboratori per la Valutazione della Sicurezza

Lo Schema abilita un solo Organismo di Certificazione. Nell'attività di valutazione l'Organismo di Certificazione si avvale di Laboratori per la Valutazione della Sicurezza che svolgono le attività connesse alla valutazione e che devono essere accreditati dall'Organismo di Certificazione stesso.

2.3 Accreditamento dei laboratori

L'Organismo di Certificazione determina la linea di condotta per l'accreditamento dei Laboratori per la Valutazione della Sicurezza.

L'accreditamento degli LVS è l'atto con cui l'Organismo di Certificazione riconosce formalmente l'indipendenza, l'affidabilità e la competenza tecnica di un Laboratorio per la Valutazione della Sicurezza.

2.4 Il processo di certificazione

Il processo di certificazione comprende tutte le attività che vengono svolte durante la valutazione e certificazione di un sistema/prodotto IT o di un Profilo di Protezione. In particolare, si individuano il processo di valutazione, articolato in tre fasi distinte, e la fase di certificazione. Nel par. 2.4.1, dopo aver introdotto delle definizioni generali, vengono descritti gli elementi fondamentali delle varie fasi del processo di valutazione. Nel par.2.4.2 si descrive la fase di certificazione che conduce all'emissione del Rapporto di Certificazione e del Certificato.

2.4.1 Il processo di valutazione

Definizioni

L'Oggetto della Valutazione (ODV) costituisce il sistema o prodotto sottoposto alla valutazione.

Il Traguardo di Sicurezza (TDS) è il documento che specifica le funzioni di sicurezza che l'Oggetto della Valutazione dovrebbe svolgere, l'ambiente operativo in cui l'ODV è destinato ad operare e il livello di garanzia al quale l'ODV viene valutato.

Il Profilo di Protezione (PP) è 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, definiti secondo i Common Criteria.

Il Piano di Valutazione (PDV) è il documento che descrive le attività che saranno svolte dal Laboratorio per la Valutazione della Sicurezza durante il processo di valutazione, i tempi di esecuzione e le risorse necessarie.

Finalità e requisiti

Il processo di valutazione è finalizzato all'emissione di un rapporto in cui viene dichiarato se:

a) il Profilo di Protezione è completo, congruente e tecnicamente corretto;
b) il Traguardo di Sicurezza è completo, congruente, tecnicamente corretto ed adatto ad essere usato come base per la valutazione del corrispondente ODV,
c) l'Oggetto della Valutazione soddisfa il Traguardo di Sicurezza al livello di garanzia richiesto.

Il processo di valutazione deve seguire i seguenti quattro principi generali:

a) *imparzialità*: la valutazione deve essere condotta senza pregiudizi e, in particolare, deve essere possibile dimostrare che l'LVS e i Valutatori coinvolti non abbiano interessi commerciali o finanziari dipendenti dall'esito della valutazione stessa;

b) *obiettività*: le conclusioni del processo di valutazione devono essere motivate da evidenze sperimentali ogni qual volta sia possibile, in modo da limitare il più possibile opinioni e valutazioni soggettive;
c) *ripetibilità*: la valutazione dello stesso sistema/prodotto/PP effettuata con gli stessi requisiti di sicurezza e dallo stesso LVS deve portare agli stessi risultati;
d) *riproducibilità*: la valutazione dello stesso sistema/prodotto effettuata con gli stessi requisiti di sicurezza da un diverso LVS deve portare agli stessi risultati.

Gli LVS devono garantire, mediante l'adozione di specifiche misure, elevati livelli di confidenzialità al fine di garantire la riservatezza di informazioni tecnicamente e commercialmente rilevanti riguardanti l'ODV e che, se diffuse, potrebbero creare un danno al proprietario dell'ODV stesso.
La certificazione stabilisce che la valutazione è stata condotta conformemente ai criteri necessari a verificare il soddisfacimento del livello di garanzia, della robustezza dei meccanismi o delle funzioni di sicurezza dichiarati e conseguentemente garantisce i risultati della valutazione stessa.
La certificazione effettuata dall'Organismo di Certificazione avviene a titolo oneroso. Le relative tariffe e modalità di versamento sono stabilite dal Ministro delle Comunicazioni di concerto con il Ministro dell'Economia e delle Finanze.
L'Organismo di Certificazione, l'LVS e il Committente devono rispettivamente designare un responsabile per ogni valutazione.

Le fasi della valutazione: aspetti fondamentali
Il processo di valutazione è articolato in tre fasi distinte:

1. la preparazione;
2. la conduzione;
3. la conclusione.

- Preparazione della valutazione

Le attività di preparazione della valutazione sono svolte dall'LVS e dal Committente al fine di predisporre il Traguardo di Sicurezza o Profilo di Protezione in modo tale che costituisca una solida base per la conduzione del processo di valutazione.
L'LVS, in ragione delle informazioni di cui dispone, verifica l'assenza di elementi che possano pregiudicare il buon esito della valutazione e predispone il Piano di Valutazione; tale PDV viene presentato all'Organismo di Certificazione che lo esamina e, una volta riconosciuta la sua adeguatezza, lo approva.

- Conduzione della valutazione

Le attività di conduzione della valutazione sono svolte dall'Organismo di Certificazione, dall'LVS e dal Committente.

Il Laboratorio di Valutazione della Sicurezza conduce la valutazione dell'Oggetto della Valutazione o del Profilo di Protezione svolgendo le attività previste nel Piano di Valutazione.

Il Laboratorio di Valutazione della Sicurezza può produrre, per il Committente e l'OC, Rapporti di Osservazione finalizzati alla richiesta di chiarimenti o modifiche all'Oggetto della Valutazione, al Profilo di Protezione, al Traguardo di Sicurezza o al Materiale per la Valutazione.

L'LVS produce, per l'Organismo di Certificazione, Rapporti di Attività (RA) per l'aggiornamento sullo stato e sui risultati della valutazione.

L'Organismo di Certificazione sovrintende la valutazione mediante l'analisi dei Rapporti di Attività, dei Rapporti di Osservazione, e attraverso le eventuali riunioni di aggiornamento.

- Conclusione della valutazione

Il Laboratorio di Valutazione della Sicurezza produce il Rapporto Finale di Valutazione (RFV) in cui, sulla base dei risultati dei Rapporti di Attività, documenta i verdetti intermedi e finali emessi con le relative giustificazioni.

2.4.2 La fase di certificazione

Nella fase di certificazione, l'Organismo di Certificazione esamina il Rapporto Finale di Valutazione (RFV) e lo utilizza come base per la produzione del Rapporto di Certificazione e dell'eventuale Certificato, concludendo con questo atto il processo di certificazione.

2.5 Standard di riferimento

L'utilità primaria della valutazione/certificazione della Sicurezza di un sistema/prodotto/PP secondo le regole dello Schema è quella di fornire una stima del livello di sicurezza secondo standard condivisi da tutti i soggetti coinvolti e di garantire che tale stima venga eseguita da una terza parte indipendente rispetto ai soggetti stessi.

Lo Schema nazionale utilizza i criteri contenuti nello standard ISO/IEC15408 (Common Criteria) e la corrispondente metodologia. Quando richiesto, sarà anche possibile l'utilizzazione dei criteri di valutazione ITSEC e della corrispondente metodologia ITSEM.

Lo Schema riconosce gli accordi internazionali sull'interpretazione delle norme dei suddetti standard.

3 Organizzazione e ruoli

I soggetti coinvolti nel processo di valutazione e certificazione della sicurezza all'interno dello Schema nazionale sono:

a) l'Organismo di Certificazione
b) la Commissione di Garanzia
c) il Laboratorio per la Valutazione della Sicurezza;
d) il Committente;
e) il Fornitore;
f) l'Assistente.

3.1 L'Organismo di Certificazione

L'ISCTI del Ministero delle comunicazioni è l'Organismo di Certificazione della sicurezza nel settore della tecnologia dell'informazione.

L'Organismo di Certificazione sovrintende alle attività operative di valutazione e certificazione nell'ambito dello Schema nazionale attraverso:

a) la predisposizione di regole tecniche in materia di certificazione sulla base delle norme e direttive nazionali, comunitarie ed internazionali di riferimento;
b) il coordinamento delle attività nell'ambito dello Schema nazionale in armonia con i criteri ed i metodi di valutazione;
c) la predisposizione delle Linee Guida per la valutazione di prodotti, traguardi di sicurezza, profili di protezione e sistemi, ai fini del funzionamento dello Schema;
d) la divulgazione dei princìpi e delle procedure relative allo Schema nazionale;
e) l'accreditamento, la sospensione e la revoca dell'accreditamento degli LVS;
f) la verifica del mantenimento dell'indipendenza, imparzialità, affidabilità, competenze tecniche e capacità operative da parte degli LVS accreditati;
g) l'approvazione dei Piani di Valutazione;
h) l'ammissione e l'iscrizione delle valutazioni;
i) l'approvazione dei Rapporti Finali di Valutazione;
j) l'emissione dei Rapporti di Certificazione sulla base delle valutazioni eseguite dagli LVS;
k) l'emissione e la revoca dei Certificati;
l) la definizione, l'aggiornamento e la diffusione, almeno su base semestrale, di una lista di prodotti, sistemi e profili di protezione certificati e in corso di certificazione;
m) la predisposizione, la tenuta e l'aggiornamento dell'elenco degli LVS accreditati;
n) la promozione delle attività per la diffusione della cultura della sicurezza nel settore della tecnologia dell'informazione;

o) la formazione, abilitazione e addestramento dei Certificatori, personale dipendente dell'Organismo di Certificazione, nonché dei Valutatori, dipendenti degli LVS e Assistenti, ai fini dello svolgimento delle attività di valutazione;

p) la predisposizione, tenuta e aggiornamento dell'elenco dei Certificatori, Valutatori e Assistenti.

L'Organismo di Certificazione riferisce semestralmente sull'attività al Dipartimento per l'Innovazione e le Tecnologie (DIT) della Presidenza del Consiglio dei Ministri. Il resoconto semestrale verterà, al minimo, sui seguenti elementi:

- elenco degli LVS accreditati, dei Certificatori, dei Valutatori e degli Assistenti abilitati;
- Rapporti di Certificazione emessi dall'OC e relativa documentazione pubblica;
- attività di formazione effettuata;
- andamento dello Schema di Gestione dei Certificati;
- variazioni tariffarie;
- informazioni statistiche sulla durata dei processi di valutazione e certificazione.

Sulla base degli indirizzi stabiliti dal Presidente del Consiglio dei Ministri o, per sua delega, dal Ministro per l'Innovazione e le Tecnologie e dal Ministro delle Comunicazioni, l'Organismo di Certificazione cura i rapporti con Organismi di Certificazione esteri congiuntamente con l'Autorità Nazionale di Sicurezza, nonché partecipa alle altre attività in ambito internazionale e comunitario riguardanti il mutuo riconoscimento dei Certificati.

Inoltre, l'Organismo di Certificazione comunica agli LVS qualsiasi cambiamento significativo introdotto nello Schema nazionale che possa influenzare i termini, le condizioni e la durata dell'attività di valutazione.

All'interno dell'Organismo di Certificazione opera il Certificatore che è addestrato e abilitato dall'Organismo stesso per condurre le attività di certificazione.

Ogni controversia inerente alle attività svolte all'interno dello Schema nazionale deve essere riferita, da qualsiasi soggetto coinvolto nello Schema nazionale, all'Organismo di Certificazione. Nel caso in cui nella controversia sia coinvolto anche l'Organismo di Certificazione, o quest'ultimo non sia riuscito a dirimerla, la controversia deve essere riferita alla Commissione di Garanzia.

3.2 La Commissione di Garanzia

La Commissione di Garanzia ha il compito di dirimere ogni tipo di controversia inerente alle attività svolte all'interno dello Schema nazionale quando nella controversia sia coinvolto anche l'Organismo di Certificazione o quando quest'ultimo, pur non essendo coinvolto, non sia riuscito a dirimerla. La Commissione di Garanzia è presieduta da un membro prescelto dal Dipartimento per l'Innovazione e le

Tecnologie della Presidenza del Consiglio dei Ministri e vede rappresentati al suo interno:

- il Ministro per l'Innovazione e le Tecnologie;
- il Ministero delle Comunicazioni;
- il Ministero delle Attività Produttive;
- il Ministero dell'Economia e delle Finanze;
- altri Ministeri che risultino interessati al funzionamento dello Schema nazionale;
- l'ISCTI;
- gli LVS;
- i Fornitori;
- le Associazioni dei Consumatori.

La Commissione di Garanzia può interagire con l'OC presentando dei Rapporti di Osservazione sullo Schema (ROS) su proposta dei componenti della Commissione stessa.

Ad esempio, possono essere segnalati:

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

La Commissione di Garanzia, a seguito di una controversia, può produrre un ROS specificando:

- l'oggetto dell'osservazione sullo Schema attinente alla controversia;
- le implicazioni;
- eventuali soluzioni proposte.

In questo caso, al fine di evitare future controversie analoghe, l'OC può redigere una NIS in conseguenza del ROS legato alla controversia: tale NIS sarà sottoposta all'approvazione della Commissione di Garanzia prima della sua diffusione.

L'organizzazione interna e la gestione della Commissione ricade sotto il controllo del DIT.

3.3 Il Laboratorio per la Valutazione della Sicurezza

I Laboratori per la Valutazione della Sicurezza sono accreditati dall'Organismo di Certificazione ed effettuano le valutazioni di ODV o di PP secondo lo Schema nazionale e sotto il controllo dell'Organismo di Certificazione medesimo.

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

a) capacità di garantire l'imparzialità, l'indipendenza, la riservatezza e l'obiettività, che sono alla base del processo di valutazione;

b) disponibilità di locali e mezzi adeguati ad effettuare valutazioni ai fini della sicurezza nel settore della tecnologia dell'informazione;
c) organizzazione in grado di controllare il rispetto delle misure di sicurezza e della qualità previste per il processo di valutazione;
d) disponibilità di personale sufficiente dotato delle necessarie competenze tecniche e iscritto nell'elenco dell'organismo di certificazione;
e) conformità ai requisiti specificati nelle norme UNI CEI EN ISO/IEC 17025 e UNI CEI EN 45011 per quanto applicabili;
f) capacità di mantenere nel tempo i requisiti in virtù dei quali è stato accreditato.

L'LVS deve garantire la massima riservatezza su tutte le informazioni acquisite relative all'Oggetto della Valutazione. A tal fine il Committente può chiedere la sottoscrizione di un documento nel quale l'LVS si impegna a mantenere la riservatezza su informazioni tecniche acquisite durante le attività di valutazione.
Oltre a quanto descritto precedentemente, l'LVS può svolgere le attività sotto elencate.

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.

I Valutatori devono essere indipendenti nello svolgimento delle loro attività. Il Valutatore è formato, addestrato ed abilitato dall'Organismo di Certificazione a condurre le attività di valutazione. Qualora uno o più Valutatori di un LVS diano assistenza ad un Fornitore o Committente per un ODV o parte di esso, gli stessi non potranno partecipare alla valutazione dello stesso ODV.

3.4 Il Committente

Il Committente è la persona fisica, giuridica o qualsiasi altro organismo che commissiona la valutazione.
Il Committente può anche rivestire il ruolo di Fornitore.
Il Committente sceglie il Laboratorio di Valutazione della Sicurezza e stipula con lo stesso il contratto per la valutazione. Successivamente alla stipula del contratto, l'LVS richiede all'Organismo di Certificazione l'iscrizione della valutazione nello Schema nazionale.
Il Committente è responsabile della fornitura all'LVS del Traguardo di Sicurezza, dell'Oggetto della Valutazione e di tutto il Materiale per la Valutazione richiesto nel Piano di Valutazione prodotto dall'LVS ed approvato dall'Organismo di Certificazione.

Il Committente deve garantire all'LVS e all'Organismo di Certificazione il libero accesso ad ogni tipo di informazione, inerente il sistema, Profilo di Protezione, prodotto o Traguardo di Sicurezza, che risulti necessaria per lo svolgimento delle attività di valutazione e certificazione. L'Organismo di Certificazione e l'LVS devono garantire che le informazioni a cui hanno accesso non siano divulgate a soggetti non autorizzati.

3.5 Il Fornitore

Il Fornitore è la persona fisica, giuridica o qualsiasi altro organismo che fornisce l'ODV o parti componenti dell'ODV. Il Fornitore può anche rivestire il ruolo di Committente della valutazione.

Nel caso in cui il Committente non sia anche il Fornitore, sarà necessario che quest'ultimo si renda disponibile a cooperare con il Committente nel processo di valutazione e certificazione, fornendo le informazioni tecniche e la documentazione in suo possesso richieste per la valutazione.

3.6 L'Assistente

L'Assistente è una persona formata, addestrata e abilitata dall'Organismo di Certificazione per fornire supporto tecnico al Committente o al Fornitore che ne faccia richiesta. All'Assistente può essere richiesta, tra l'altro, un'analisi del Traguardo di Sicurezza o del Profilo di Protezione al fine di accertare, sulla base anche di eventuale ulteriore documentazione richiesta al Committente, che lo stesso costituisca una solida base per la conduzione del processo di valutazione. A tal fine, l'Assistente, in ragione delle informazioni di cui dispone, verifica l'assenza di elementi che possano pregiudicare il buon esito della valutazione. Inoltre, l'Assistente può curare il processo di gestione del Certificato come descritto nel Cap.7.

4 Fase di preparazione

4.1 Introduzione

Questo capitolo fornisce una veduta d'insieme della prima fase del processo di valutazione. Uno schema riassuntivo della fase di preparazione delle attività di valutazione della sicurezza è fornito nella fig.1.

La guida più particolareggiata sulle procedure di valutazione è descritta nella LGP3.

4.2 Considerazioni generali

Le attività di preparazione della valutazione sono svolte dall'LVS e dal Committente.

Il Committente chiede l'intervento dell'LVS, specificando il Traguardo di Sicurezza o il Profilo di Protezione richiesto.

Il Committente potrà ottenere dall'LVS l'indicazione del costo delle attività di valutazione.

Analoga indicazione potrà essere ottenuta dall'Organismo di Certificazione per quanto riguarda l'attività di certificazione.

Si consiglia il Committente affinché:

a) tenga conto della necessità di ottenere collaborazione dal Fornitore per quanto riguarda le informazioni tecniche e la documentazione richieste per la valutazione;
b) qualora l'ODV contenga componenti già certificati, si predisponga per reperire i documenti più rilevanti del processo di certificazione, in particolare, il Traguardo di Sicurezza e il Rapporto di Certificazione;
c) tenga nella dovuta considerazione i costi per il mantenimento del Certificato, quando previsto;
d) ottenga la disponibilità dei risultati della valutazione, in modo da poterli riutilizzare in eventuali future attività di valutazione, certificazione e mantenimento.

4.3 Obiettivo

L'obiettivo della fase della preparazione è quello di stimare l'adeguatezza dell'ODV o del PP per la valutazione, prima dell'inizio della fase di conduzione.

Questo processo è basato sui seguenti elementi:

a) individuazione del TDS;
b) determinazione della documentazione necessaria per sostenere la valutazione;
c) accordo su un PDV;
d) determinazione dello scopo della valutazione e analisi delle responsabilità per assicurare che tutte le parti in causa siano consapevoli dei loro compiti;
e) accettazione formale dei requisiti previsti dallo Schema per la valutazione.

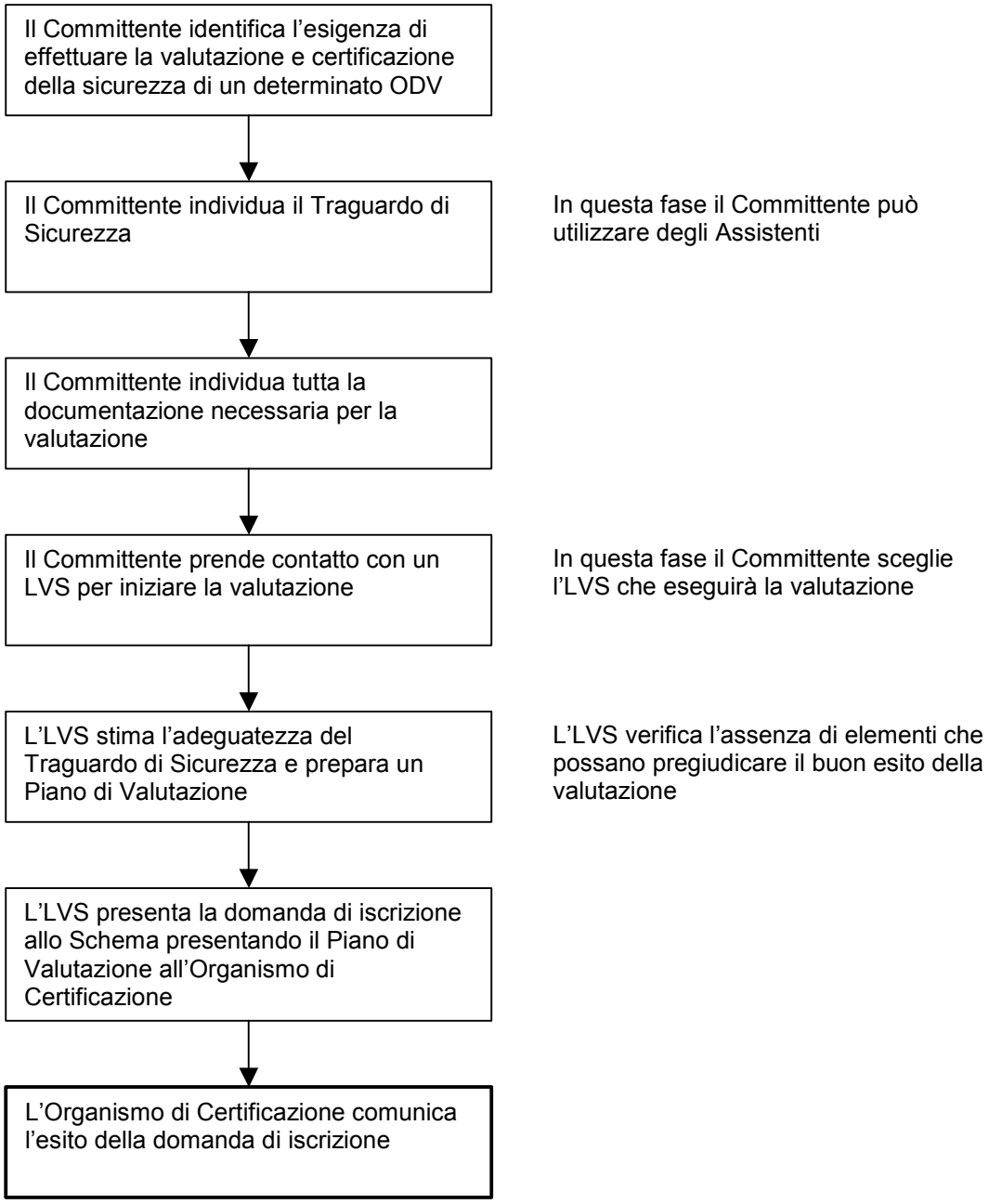

Fig.1 - Passi fondamentali della fase di preparazione della valutazione di un ODV.

4.4 Traguardo di Sicurezza e ulteriori documenti

Al Committente è richiesto di fornire il Traguardo di Sicurezza e gli ulteriori documenti che è necessario sviluppare ai fini della valutazione/certificazione. L'LVS esamina il Traguardo di Sicurezza o il Profilo di Protezione al fine di accertare, sulla base anche di eventuale ulteriore documentazione richiesta al Committente, che IL TDS o PP costituisca una solida base per la conduzione del processo di valutazione; ove necessario richiede modifiche.

4.5 Materiale per la valutazione

Il Materiale per la Valutazione necessario al Valutatore per condurre la valutazione può comprendere:

- gli elementi hardware, firmware o software che costituiscono l'ODV stesso;
- la documentazione per l'utente dell'ODV;
- la documentazione tecnica di supporto, generata o durante lo sviluppo dell'ODV o per sostenere il processo di valutazione;
- il supporto tecnico del Fornitore.

Si considerano materiali per la valutazione anche

- l'accesso al sito operativo (nel caso di un sistema);
- l'accesso al sito dello sviluppo dell'ODV.

Per la produzione di tutti i tipi di documentazione relativi alla valutazione e certificazione è obbligatorio l'uso della lingua italiana, con deroghe unicamente concesse a:

- eventuali terminologie in lingua inglese, non tradotte nel glossario di riferimento dello Schema, che siano utilizzate nei documenti originali che descrivono i criteri e le metodologie
- documenti di valutazione e certificazione già esistenti in lingua inglese.

Il processo di valutazione può essere semplificato se l'ODV è progettato tenendo in conto sin dall'inizio dello sviluppo i requisiti della valutazione. Questa considerazione è particolarmente importante nel caso di valutazioni ai più alti livelli di garanzia.
I Committenti devono assicurare la loro capacità di fornire la documentazione necessaria per la valutazione nei tempi stabiliti. Il Committente deve essere consapevole che questo può richiedere la cooperazione di altre entità coinvolte nel processo della valutazione. In particolare molta documentazione potrebbe essere di proprietà del Fornitore dell'ODV e, quindi, potrebbe non essere automaticamente disponibile al Committente.
Il Fornitore potrebbe desiderare di limitare l'accesso del Committente a informazioni di proprietà riservata. L'LVS e l'Organismo di Certificazione dovranno comunque poter accedere in modo adeguato alle informazioni di proprietà riservata al fine di realizzare la valutazione e la certificazione dell'ODV.
L'intera documentazione richiesta deve essere concordata tra il Committente, l'LVS e qualsiasi altra entità coinvolta, con l'obiettivo di fornire tutta la documentazione necessaria per poter condurre la valutazione in modo ottimale.

4.6 Il Piano di Valutazione

Il Piano di Valutazione, che è preparato dall'LVS, specifica il lavoro che deve essere condotto dall'LVS stesso durante la valutazione.

L’LVS, in ragione delle informazioni di cui dispone, verifica l’assenza di elementi che possano pregiudicare il buon esito della valutazione e predispone un Piano di Valutazione.

Tale piano indirizza tutti gli aspetti che riguardano l'applicazione dei criteri e delle metodologie per la valutazione dell'ODV, fornendo inoltre tutte le scadenze temporali connesse con l'attività di valutazione proposta.

L’LVS chiede formalmente all'Organismo di Certificazione l'iscrizione della valutazione nello Schema, fornendo il Piano di Valutazione predisposto. Contestualmente, il Committente, in modo diretto o attraverso l’LVS, documenta l’avvenuto pagamento dell’onere finanziario legato alle prestazioni dell'Organismo di Certificazione per l’analisi del PDV.

4.7 Accettazione formale della valutazione e Notifica di Inizio Lavori

La valutazione sarà accettata formalmente se sussistono tutte le seguenti condizioni:

a) l'Organismo di Certificazione avrà ritenuto adeguato che l'ODV o il PP venga valutato e certificato nell'ambito dello Schema;
b) l'Organismo di Certificazione avrà ritenuto adeguati il Traguardo di Sicurezza e il PDV presentati;
c) il Committente avrà accettato di sostenere l'onere finanziario legato alle prestazioni dell'Organismo di Certificazione per le attività di certificazione.

L'Organismo di Certificazione comunica formalmente all’LVS l'esito della richiesta di iscrizione allo Schema, motivando adeguatamente l'eventuale esito negativo e conferma gli oneri dovuti all’OC per le fasi successive della certificazione. Tale comunicazione conclude la fase di preparazione della valutazione.

Successivamente alla comunicazione dell'esito della richiesta di iscrizione allo Schema l'LVS coinvolto notifica formalmente all'Organismo di Certificazione l'effettivo inizio della valutazione, attraverso una Notifica di Inizio Lavori (NIL), dando così inizio alla fase di conduzione della valutazione.

Il Committente, per sue esigenze specifiche (per esempio per stringenti requisiti temporali), può richiedere all'LVS di presentare la Notifica di Inizio Lavori contestualmente alla presentazione del PDV. In questo caso il Committente deve essere consapevole che, se la richiesta di iscrizione allo Schema dovesse avere esito negativo, resterebbero comunque a suo carico tutti gli oneri e i rischi relativi alla mancata attesa dell'esito della richiesta di iscrizione.

In caso di esito positivo, si terrà normalmente una Riunione di Avvio dei Lavori (RAL) in cui saranno coinvolti l'Organismo di Certificazione, il Committente, l’LVS e qualsiasi altra entità interessata, al fine di discutere qualsiasi aspetto che sia attinente alla valutazione, alla certificazione e alle specifiche dell'ODV. Tale riunione sarà convocata dall’OC di sua iniziativa o su richiesta dell’LVS o del Committente, prima dell'inizio della effettiva fase di conduzione della valutazione.

4.8 Assistenza

L’assistenza costituisce l’attività di supporto tecnico, inerente la sicurezza nel settore della tecnologia dell’informazione, fornita al Committente durante la fase di preparazione della valutazione di un ODV o di un Profilo di Protezione.

L’attività dell’Assistente nella fase di preparazione potrà prevedere, ad esempio, le seguenti azioni:

- produrre la documentazione necessaria per la valutazione;
- attuare un'analisi iniziale del Traguardo di Sicurezza;
- stimare la probabilità di riuscita del processo di certificazione.

L’attività di assistenza potrà essere svolta da un LVS o da professionisti abilitati al ruolo di Assistente dall’Organismo di Certificazione.

L'ambito di sviluppo dell'azione di assistenza durante la fase di preparazione della valutazione viene direttamente negoziato tra il Committente e l'LVS, o qualsiasi altro Assistente. Comunque, quando un LVS fornisce sia l'assistenza sia il servizio di valutazione per un particolare ODV, è obbligato sia a definire chiaramente l'ambito dell'assistenza, sia a dimostrare all'Organismo di Certificazione che l'assistenza fornita non influenza l'indipendenza del Valutatore o l'imparzialità nella valutazione.

Durante la fase di preparazione, se il Committente lo desidera, potrà consultare l'Organismo di Certificazione per richiedere chiarimenti generali sugli aspetti coinvolti in una valutazione/certificazione.

5 Fasi di conduzione e conclusione

5.1 Introduzione

660 Questo capitolo fornisce una panoramica delle fasi di conduzione e conclusione del processo di valutazione. Da un punto di vista formale la fase di conduzione della valutazione inizia alla risposta con esito positivo alla domanda d'iscrizione nello Schema. Uno schema grafico delle attività di valutazione e certificazione è fornito in fig.2.

665 La guida più particolareggiata delle procedure per la valutazione è descritta nella LGP3.

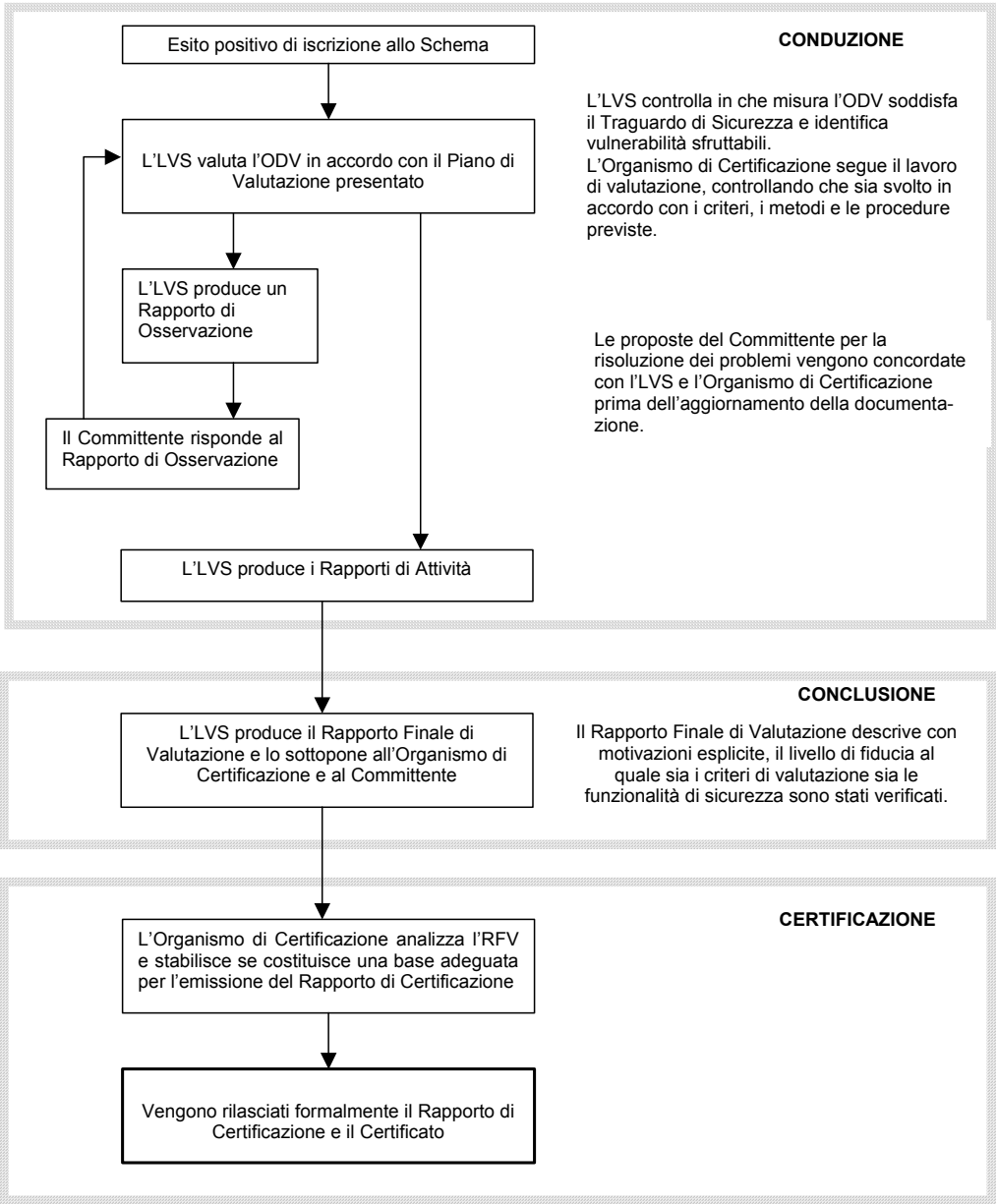

Fig.2 - Passi fondamentali delle fasi di conduzione-conclusione di una valutazione e della fase di certificazione.

670

5.2 Obiettivo

L'obiettivo delle fasi di conduzione e conclusione della valutazione è determinare se l'ODV soddisfa il Traguardo di Sicurezza e se è esente da vulnerabilità sfruttabili. Per raggiungere questo obiettivo occorre svolgere le seguenti attività:

a) valutazione dell'ODV;
b) interazione fra i vari soggetti coinvolti, al fine di assicurare l'efficacia del processo di valutazione;
c) produzione da parte dell'LVS di eventuali Rapporti di Osservazione per anomalie o per errori.

5.3 Conduzione della valutazione

I Valutatori effettuano l'attività di conduzione della valutazione tecnica seguendo le modalità dettagliate nel Piano di Valutazione. Questa attività implica la valutazione imparziale e dettagliata dell'ODV in accordo con i criteri di valutazione, al fine di determinare in che misura l'ODV realizzi il Traguardo di Sicurezza e di identificare eventuali vulnerabilità sfruttabili.

Se nel corso del lavoro di valutazione vengono rilevati errori, incongruenze o vulnerabilità, devono essere prodotti dei Rapporti di Osservazione che li descrivano in dettaglio. Al termine di ogni attività, l'LVS predispone dei Rapporti di Attività che riassumono i risultati delle analisi condotte per la specifica attività.

I risultati del lavoro di valutazione devono essere documentati in modo continuativo al procedere della valutazione stessa.

L'LVS organizzerà regolarmente degli incontri sull'avanzamento della valutazione con il Committente e con tutte le altre parti interessate, al fine di instaurare una efficiente interazione durante tutta l'attività di valutazione.

Durante la valutazione l'LVS potrebbe avere la necessità di interagire direttamente con il Fornitore: in questo caso deve, però, ottenere l'autorizzazione del Committente.

L'Organismo di Certificazione controlla ogni valutazione, al fine di confermare che esse siano effettuate in accordo con i criteri, i metodi e le procedure previste dallo Schema. Durante la fase di conduzione l'Organismo di Certificazione è coinvolto nelle seguenti attività:

a) se necessario, partecipa agli incontri sull'avanzamento della valutazione;
b) se necessario, concorda con l'LVS il modo in cui devono essere applicati i criteri per la valutazione di uno specifico ODV o PP;
c) controlla i rapporti tecnici prodotti dai Valutatori durante il corso delle valutazioni;
d) controlla i documenti di valutazione.

LVS e Committente richiedono l'intervento dell'Organismo di Certificazione al verificarsi di problemi per i quali è non è stato possibile individuare una soluzione o laddove sia necessaria una interpretazione dei criteri o delle metodologie. Se non è

possibile risolvere il problema e l'LVS decide che questa circostanza influisce negativamente sulla valutazione, l'LVS notifica formalmente il fatto al Committente. Il Committente può, in accordo con il contratto stipulato con l'LVS:

a) abbandonare la valutazione;
b) continuare la valutazione, accettando il problema e le sue implicazioni sul processo di certificazione;
c) riprogrammare temporalmente la valutazione e, in accordo con l'Organismo di Certificazione, istruire il Fornitore per modificare l'ODV nel modo concordato.

Durante una valutazione l'LVS può trovarsi nella condizione di fornire delle interpretazioni, su aspetti specifici della valutazione, che non risultano presenti nella normativa relativa ai criteri applicati nello Schema. In tali circostanze i compiti dell'Organismo di Certificazione sono quelli di:

a) verificare che le interpretazioni proposte siano in accordo con le finalità e gli obiettivi generali dello Schema;
b) gestire e aggiornare la metodologia di valutazione al fine di ridurre gli elementi soggettivi nelle future valutazioni;
c) promuovere accordi per il mutuo riconoscimento internazionale di eventuali interpretazioni e nuove metodologie adottate.

5.4 Conclusione della valutazione: il Rapporto Finale di Valutazione

I Valutatori documentano la loro attività all'Organismo di Certificazione attraverso il Rapporto Finale di Valutazione, che rappresenta il documento finale della valutazione che raccoglie tutti i Rapporti di Attività e le considerazioni sulla valutazione svolta. Le conclusioni documentate nel Rapporto Finale di Valutazione dimostrano e descrivono il grado con cui i criteri di valutazione sono stati soddisfatti.

L'LVS rilascia il Rapporto Finale di Valutazione al Committente dopo aver verificato che non contenga informazioni proprietarie.

L'RFV è un documento confidenziale e il Committente può farlo visionare solo a un limitato numero di persone appartenenti al suo staff e non può distribuirlo alle altre parti senza il consenso dell'Organismo di Certificazione.

6 Fase di certificazione

La fase di certificazione ha come obiettivo l'emissione da parte dell'OC del Rapporto di Certificazione (RC) e dell'eventuale Certificato (fig.2). A tal fine, l'Organismo di Certificazione esamina il Rapporto Finale di Valutazione (RFV) e, qualora riscontri la coerenza con i criteri, la metodologia ed i requisiti dello Schema, lo approva. Nel caso in cui vengano individuate delle anomalie risolvibili, l'Organismo di Certificazione richiede l'intervento del Laboratorio di Valutazione della Sicurezza per l'eventuale perfezionamento del Rapporto Finale di Valutazione.

Il Rapporto di Certificazione deve:

a) dichiarare se la valutazione è stata condotta secondo i criteri e la metodologia prevista dallo Schema nazionale;
b) dichiarare se il Profilo di Protezione è completo, congruente e tecnicamente corretto;
c) dichiarare se il Traguardo di Sicurezza è completo, congruente e tecnicamente corretto;
d) dichiarare se l'Oggetto della Valutazione soddisfa il Traguardo di Sicurezza al livello di garanzia richiesto;
e) identificare le eventuali vulnerabilità sfruttabili ed eventualmente raccomandare delle contromisure;
f) motivare l'eventuale emissione di verdetti in contrasto con quelli dell'LVS.

Nel caso in cui nell'RFV si evidenzino delle vulnerabilità sfruttabili, il processo di certificazione non potrà essere completato con l'emissione del Certificato.

La bozza dell'RC viene consegnata al Committente e all'LVS per confermare che:

- il rapporto ben descrive il Traguardo di Sicurezza;
- il rapporto descrive adeguatamente la conduzione e i risultati della valutazione;
- le conclusioni del rapporto sono accurate;
- il Committente e l'LVS non sono a conoscenza di fatti che potrebbero invalidare le conclusioni del rapporto stesso.

La versione definitiva del Rapporto di Certificazione e il Certificato vengono emessi dall'Organismo di Certificazione.

La certificazione si riferisce solo agli aspetti di sicurezza sottoposti a valutazione: questo implica il permanere di una probabilità non nulla che in un ODV certificato esistano alcune vulnerabilità sfruttabili non individuate perché al di fuori degli aspetti di sicurezza sottoposti a valutazione e certificazione.

I risultati del processo di valutazione e certificazione sono riferibili a una specifica e determinata configurazione dell'Oggetto della Valutazione: pertanto la

commercializzazione di un sistema/prodotto certificato è vincolata a tale configurazione. Successivamente ad una avvenuta certificazione, si potrebbero palesare delle nuove vulnerabilità, non considerate nel processo di valutazione e certificazione dell'ODV, tali da impedire il raggiungimento degli obiettivi di sicurezza dichiarati nel TDS: in questo caso l'OC si riserva la facoltà di revocare il Certificato. Al fine di espletare in modo adeguato la funzione di controllo della validità dei Certificati nel tempo, l'OC svolge una costante attività di monitoraggio al fine di aggiornare la lista delle vulnerabilità sfruttabili.

Il Committente che desideri mantenere nel corso del tempo la validità del Certificato associato ad un ODV può aderire allo Schema di Gestione dei Certificati, così come descritto nel cap.7.

7 Schema di Gestione dei Certificati

Un Certificato rilasciato nell'ambito dello Schema nazionale di valutazione e certificazione della sicurezza è valido solo per la versione dell'ODV valutata nella configurazione dichiarata. Comunque, la maggior parte degli ODV sono soggetti a revisioni, come, per esempio, quando vengono realizzate delle correzioni o delle migliorie che hanno un qualche impatto sulla sicurezza.

Lo Schema di Gestione dei Certificati (SGC) è uno strumento mediante il quale è possibile, in caso di modifiche apportate ad un ODV già certificato, evitare la ripetizione completa di tutte le attività di valutazione svolte nel corso della certificazione originale, al fine di mantenere il livello di garanzia dell'ODV

Lo Schema di Gestione dei Certificati costituisce parte integrante dello Schema nazionale di valutazione e certificazione della sicurezza. Una descrizione completa dell'SGC verrà fornita nelle Linee Guida Definitive.
Fino alla pubblicazione di tali Linee Guida Definitive l'SGC risulterà, nelle sue linee generali, conforme alle indicazioni fornite nel documento [CCR1].

Nel seguito si forniscono gli elementi essenziali per consentire, sin dalle prime fasi di operatività dell'Organismo di Certificazione, l'attivazione dello Schema di Gestione dei Certificati.
Nel caso in cui vengano apportate modifiche ad un ODV certificato, o vengano individuate vulnerabilità sfruttabili che compromettano uno o più obiettivi di sicurezza di un ODV certificato, la Certificazione perde la sua validità.
Se il Committente/Fornitore non si avvale dell'SGC questa circostanza comporta la revoca del Certificato.

Qualora invece il Committente/Fornitore abbia aderito all'SGC, egli può estendere la validità della certificazione all'ODV modificato dimostrando, mediante lo svolgimento di un sottoinsieme minimo di azioni di valutazione, l'idoneità delle modifiche apportate ai fini del raggiungimento degli obiettivi di sicurezza. In particolare, nel caso in cui siano state individuate vulnerabilità sfruttabili che compromettono gli obiettivi di sicurezza dell'ODV, l'OC concede al Committente/Fornitore un periodo temporale per predisporre efficaci contromisure e valutarne l'idoneità in relazione al livello di garanzia dell'ODV. Durante questo periodo il Certificato viene posto in uno stato di osservazione pur mantenendo la sua validità.

Dallo stato di osservazione sono possibili due transizioni:

- se durante il periodo temporale previsto dall'OC per la risoluzione della vulnerabilità riscontrata, è stata approntata una contromisura efficace e valutata idonea, il Certificato riacquisisce la sua validità;
- una volta trascorso completamente il periodo temporale previsto dall'OC per la risoluzione della vulnerabilità riscontrata, se non è stata approntata una contromisura efficace e valutata idonea, il Certificato viene revocato. Esso potrà comunque riacquisire pienamente la sua validità al momento in cui sia resa disponibile una contromisura efficace e valutata idonea.

Lo Schema di Gestione dei Certificati prevede due distinti processi:

- mantenimento della certificazione
- ri-certificazione.

Entrambi i processi mettono a frutto i risultati di valutazione ottenuti per l'ODV nelle precedenti fasi di valutazione-certificazione e di gestione del certificato.

Lo Schema di Gestione dei Certificati adottato dall'OC si basa sulle seguenti ipotesi:

- adesione volontaria allo Schema di Gestione da parte del Committente/Fornitore, che può avvenire o in fase di valutazione o successivamente alla emissione del Certificato, a patto che al momento dell'adesione l'ODV non risulti affetto da vulnerabilità sfruttabili;
- possibilità di emissione da parte dell'OC di 'Addendum' alla Certificazione effettuata sull'ODV nell'ambito del processo di mantenimento

L'adesione del Committente all'SGC avviene attraverso una sottoscrizione di contratto con l'OC a titolo oneroso e di durata minima annuale. Il contratto vincola il Committente a indicare un Responsabile per la Gestione del Certificato (RGC) (o facente parte dell'organizzazione del Committente/Fornitore, o un Assistente appartenente o meno ad un LVS) che si impegna a predisporre l'attuazione delle procedure di Gestione del Certificato.

8 Riferimenti bibliografici

[CCI1] CCIMB-2004-01-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, version 2.2, gennaio 2004

[CCI2] CCIMB-2004-01-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional requirements”, version 2.2, gennaio 2004

[CCI3] CCIMB-2004-01-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance requirements”, version 2.2, gennaio 2004

[CCR1] CCIMB-2004-02-09 “Assurance Continuity: CCRA Requirements”; febbraio 2004

[CEM1] CEM-97/017, “Common Evaluation Methodology for Information Technology Security Evaluation, Part 1 – Introduction and general model”; version 0.6, gennaio 1997

[CEM2] CCIMB-2004-01-004, “Common Evaluation Methodology for Information Technology Security Evaluation, Part 2 – Evaluation Methodology”, version 2.2, gennaio 2004

[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

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

9 Lista degli acronimi

EAL = (Evaluation Assurance Level) Livello di garanzia della valutazione
IT = Information Technology
LVS = Laboratorio di Valutazione della Sicurezza
NIL = Notifica di Inizio Lavori
NIS = Nota Informativa dello Schema
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