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

Organismo di Certificazione

Il Piano di Valutazione: indicazioni generali

Linee Guida Provvisorie - parte 5

LGP5

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 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.

Lo scopo della Linea Guida Provvisoria 5 (LGP5) è quello di fornire ai Valutatori di un Laboratorio di Valutazione della Sicurezza (LVS) gli elementi fondamentali per definire, in base ai Criteri di Valutazione ITSEC e Common Criteria e le relative metodologie, un Piano Di Valutazione (PDV) della Sicurezza di un Sistema/Prodotto o di un Profilo di Protezione (PP). Nel presentare le indicazioni sul PDV si affrontano anche i passaggi più rilevanti che caratterizzano un processo di valutazione, passaggi che sono stati affrontati in dettaglio nella LGP3.

Il PDV contiene la descrizione di tutte le attività che i Valutatori debbono eseguire per la valutazione di un Sistema/Prodotto/PP e le modalità con le quali esse sono organizzate, pianificate, correlate e suddivise nell'ambito del piano.

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 LVS 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, attività che verranno eseguite durante le fasi di valutazione e i cui risultati saranno riportati nella documentazione che gli LVS sono tenuti a redigere durante il processo di valutazione.

Le parti coinvolte nella definizione di un PDV sono:

- l'LVS, che è responsabile della redazione;
- il Fornitore, che deve fornire tutto il materiale necessario alla sua stesura;
- il Committente, che deve fornire tutto il supporto necessario, principalmente nel caso di valutazione di sistemi, per la corretta definizione delle varie fasi della valutazione.

Il PDV viene presentato all'Organismo di Certificazione che, esaminatolo nella forma e nei contenuti, e consideratolo adeguato ai fini della valutazione, lo approva.

Nel par.2, dopo aver richiamato le tre fasi che costituiscono un processo di valutazione, vengono svolte delle considerazioni su come si definisce un PDV specifico, sui materiali che interessano una valutazione e sugli aspetti generali che interessano le caratteristiche di una valutazione.

Nel par.3 vengono proposti i contenuti e la struttura di un PDV standard, quale base comune per ogni realizzazione specifica di PDV.

2 Definizione di un PDV e richiami sugli elementi essenziali di una valutazione

2.1 Premessa alla definizione di un Piano di Valutazione

Di seguito si identificano le attività che un LVS deve svolgere per definire un PDV, tenendo in considerazione tutte le dipendenze ed i fattori che influenzano il processo di valutazione dell'Oggetto della Valutazione (ODV).

Si precisa che nel presente documento non vengono prese in considerazione la complessità e l'ampiezza del processo di valutazione, ma vengono semplicemente fornite le linee guida per la definizione di un Piano di Valutazione. Quindi nella trattazione che segue non si specifica il dettaglio del peso delle attività, limitandosi a definire l'esistenza, la sequenza logica e le relative interazioni nella totalità del processo. Oltre alle attività di valutazione previste nei criteri, l'LVS potrà identificare ulteriori attività necessarie alla conduzione del processo di valutazione dell'ODV, aggiungendo eventuali attività a seconda degli obiettivi di sicurezza fissati e della complessità del Sistema/Prodotto/PP sotto valutazione.

Quando l'LVS riceve dal Committente l'incarico di effettuare una valutazione di un Sistema/Prodotto/PP deve ricevere anche la documentazione necessaria per poter definire il PDV.

Tale documentazione è costituita sostanzialmente dal Traguardo di Sicurezza che descrive i requisiti di sicurezza relativi ai criteri di valutazione adottati.

A seguito dell'analisi della documentazione ricevuta e dopo aver effettuato riunioni di studio con il Committente, atte a chiarire i problemi emersi nel corso della stessa analisi, l'LVS deve redigere il PDV, che sarà poi sottoposto a verifica ed approvazione da parte dell'OC.

2.2 Suddivisione della valutazione in Fasi

Il processo di valutazione, indipendentemente dalla complessità del Sistema/Prodotto/PP in esame, si suddivide in tre fasi:

- Fase 1 - Preparazione della valutazione;
- Fase 2 - Conduzione della valutazione;
- Fase 3 - Conclusione della valutazione.

Il PDV deve considerare e pianificare tutte le attività identificate nella Fase 2 di Conduzione della valutazione e nella Fase 3 di Conclusione della valutazione, mentre le attività della Fase 1 di Preparazione della valutazione sono escluse dal piano.

2.2.1 Fase 1 - Preparazione della valutazione

Durante la Fase 1 l'LVS deve:

- analizzare i documenti ricevuti dal Committente, nell'ottica di comprendere la complessità del lavoro di valutazione che si accinge ad eseguire e di verificare la completezza e congruità della documentazione stessa ai fini della produzione del PDV;
- identificare i documenti di cui l'LVS necessita durante la valutazione, indicando nel piano il momento in cui tali documenti sono attesi;
- partecipare a riunioni con il Committente per chiarire, prima dell'inizio della valutazione, tutti i problemi emersi e per valutare tutti quei fattori ed interazioni che possono influenzare la definizione del PDV;
- produrre il PDV specificando dettagliatamente le attività da eseguire, il tempo e le persone allocate nel processo di valutazione;
- definire il contratto con il Committente per la valutazione in oggetto;
- sottoporre il PDV all'approvazione dell'Organismo di Certificazione.

Il contenuto di un PDV deve essere approvato dall'OC per confermare che:

1) sono stati correttamente applicati i requisiti dei criteri di valutazione e dello Schema e/o ogni previsto scostamento da questi è stato accettato;
2) la pianificazione delle attività è commisurata ai requisiti della valutazione;
3) l'attività di valutazione che deve essere effettuata è in accordo al livello di garanzia richiesto;
4) il lavoro, se completato con successo, è adeguato per la certificazione dell'ODV o del PP al livello di garanzia richiesto;
5) gli strumenti da utilizzare sono giudicati dall'OC idonei per la valutazione.

La complessità e l'entità del processo di valutazione dipende da molti fattori che debbono essere considerati in questa fase; tra i più importanti si indicano i seguenti:

- stabilire se la valutazione si riferisce ad un Prodotto o Sistema o PP;
- accertare se la valutazione si esegue in modo consecutivo (sistema/prodotto già realizzato di cui si chiede la valutazione) o concomitante (sistema/prodotto in fase di realizzazione e di cui si chiede la valutazione);
- accertare se è una valutazione o ri-valutazione di un ODV già valutato;
- accertare se l'ODV usa prodotti già valutati come componenti;
- indicare se la complessità dell'ODV è notevole;
- stabilire i tempi di sviluppo dell'ODV nel caso di valutazione concomitante;

- indicare la necessità di addestramento dei Valutatori sull'ODV sotto esame o sugli strumenti o le metodologie usate per la sua realizzazione;
- evidenziare i requisiti di sicurezza dell'ambiente di sviluppo;
- indicare il livello di garanzia richiesto;
- indicare l'entità e la complessità dei rapporti da redarre, la quantità ed il tipo delle riunioni tecniche da effettuarsi durante la valutazione, etc.

2.2.2 Fase 2 - Conduzione della valutazione

Dopo l'approvazione del PDV da parte dell' OC, l'LVS inizia la fase di conduzione della valutazione che prevede:

- riunione di avvio dei lavori;
- avvio della valutazione;
- esecuzione dell'attività di valutazione;
- redazione dei rapporti per:
  - completamento di specifiche attività indicate nel PDV;
  - riunioni con il Committente/Fornitore;
  - errori e/o anomalie emerse durante il processo di valutazione.

2.2.3 Fase 3 - Conclusione della valutazione

In questa fase l'LVS redige il Rapporto Finale di Valutazione (RFV) che integra in un unico documento tutte le analisi, i Rapporti e le prove eseguite durante il processo di valutazione.

A partire dall'RFV l'OC emette un Rapporto di Certificazione (RC) e un Certificato.

2.3 Attività di valutazione

Nel caso di una valutazione di un Profilo di Protezione secondo i Common Criteria, l'unica attività prevista sarà quella di valutazione del PP stesso in base ai requisiti della classe APE descritta in [CCI3]. Nel seguito vengono descritte le attività previste in un PDV standard relativo alla valutazione di un ODV, organizzate in modo distinto a seconda dei criteri di valutazione adottati.

2.3.1 PDV standard nel caso di applicazione di ITSEC

Le attività previste in un PDV standard nel caso di applicazione dei criteri ITSEC sono:

- inizio della valutazione;
- verifica dei requisiti di sicurezza del Sistema/Prodotto sotto valutazione;
- verifica del progetto architetturale;
- verifica del progetto di dettaglio;
- verifica dell'implementazione;
- verifica dell'ambiente di sviluppo;

- verifica della documentazione operativa (documentazione utente e amministratore);
- verifica dell'ambiente operativo (configurazione della documentazione e suo inoltro);
- verifica dell'analisi dell'idoneità;
- verifica dell'analisi dell'integrazione;
- esame della robustezza dei meccanismi di sicurezza;
- valutazione delle vulnerabilità di costruzione;
- valutazione delle vulnerabilità di esercizio;
- valutazione della facilità d'uso;
- prove di intrusione;
- produzione dei rapporti di valutazione;
- gestione del processo di valutazione (verifica della realizzazione dei piani, relazioni con Committente, Fornitore ed Organismo di Certificazione);
- chiusura del processo di valutazione.

Ognuna delle attività indicate utilizzerà un modello di documentazione che prevede:

- obiettivi dell'attività;
- documenti in ingresso;
- identificazione e descrizione delle azioni svolte dai Valutatori per raggiungere gli obiettivi;
- tecniche e strumenti utilizzati;
- documenti in uscita.

Nel periodo di validità della Linee Guida Provvisorie, ad integrazione delle indicazioni fornite in questa LGP, si potrà richiedere all'Organismo di Certificazione ulteriore documentazione per la stesura di un PDV.

2.3.2 PDV standard nel caso di applicazione dei Common Criteria (CC)

Le attività (e le corrispondenti classi di garanzia) previste in un PDV standard nel caso di applicazione dei criteri CC sono:

- inizio della valutazione;
- valutazione del Traguardo di Sicurezza (Security Target Evaluation, ASE);
- valutazione della gestione della configurazione (Configuration Management, ACM);
- valutazione della consegna e della messa in opera dell'ODV (Delivery and Operation, ADO);
- valutazione del processo di sviluppo dell'ODV (Development, ADV);
- valutazione della documentazione destinata agli utenti e agli amministratori dell'ODV (Guidance Documents, AGD);

- valutazione delle misure di sicurezza connesse al ciclo di vita dell'ODV (Life Cycle Support, ALC);
- test (Tests, ATE);
- stima di vulnerabilità (Vulnerability Assessment, ASE);
- produzione dei Rapporti di Valutazione;
- gestione del processo di valutazione (verifica della realizzazione dei piani, relazioni con Committente, Fornitore ed Organismo di Certificazione);
- chiusura della valutazione.

Ognuna delle attività indicate utilizzerà un modello di documentazione che prevede:

- obiettivi dell'attività;
- documenti in ingresso;
- identificazione e descrizione delle azioni svolte dai Valutatori per raggiungere gli obiettivi;
- tecniche e strumenti utilizzati;
- documenti in uscita.

Nel periodo di validità della Linee Guida Provvisorie si suggerisce di prendere a riferimento la LGP4 per la definizione delle attività, sottoattività, azioni e unità di lavoro per le valutazioni con livello di garanzia EAL1, EAL2, EAL3 e EAL4. In particolare:

- la pianificazione temporale (descritta mediante un diagramma di Gantt) deve essere sviluppata riportando le attività (corrispondenti alle classi di garanzia descritte in [CCI3]);
- l'allocazione delle risorse deve essere effettuata sulle azioni di valutazione (corrispondenti agli elementi di garanzia descritti in [CCI3]) sebbene debbano essere dettagliate nei contenuti anche le unità di lavoro (vedi LGP4).

2.3.3 Considerazioni nel definire un PDV specifico

L'attività di valutazione di un ODV può essere un processo complesso sia per le dimensioni e l'architettura dell'oggetto sotto valutazione, sia per le molteplici attività che la valutazione richiede. Inoltre, ogni processo di valutazione è un processo specifico sull'Oggetto della Valutazione, nel senso che sebbene ci possano essere delle analogie e similitudini tra diverse valutazioni, ognuna di esse presenta delle caratteristiche proprie dettate dal livello di garanzia, dal tipo e dalle modalità operative dell'ODV, dalle informazioni che deve gestire, etc.

Quando un ODV presenta nella sua architettura uno o più componenti già valutati è possibile usare, nel processo di valutazione, i risultati delle valutazioni di tali componenti come input per la presente valutazione con vantaggio in alcune attività di analisi.

La definizione di un PDV specifico dovrà considerare, analizzare e documentare aspetti specifici della valutazione in atto, quali:

- le tecniche e gli strumenti adatti alla specifica valutazione;

- i diversi documenti da controllare durante la valutazione;
- le dimensioni e la complessità dell'ODV;
- i tempi di realizzazione dell'ODV e della valutazione;
- i diversi tipi di rapporti da tenere con il Committente durante la valutazione;
- la necessità o meno di addestrare i Valutatori su specifiche parti o tecniche impiegate nello sviluppo dell'ODV;
- la necessità di suddividere il processo di valutazione in sotto processi relativi a parti definite dell'ODV.

2.3.4 Errori trovati durante la valutazione e tempo necessario per la correzione

Durante il processo di valutazione possono essere scoperti errori nella documentazione e/o nell'ODV. Essi verranno riportati nei rapporti tecnici ed il Committente dovrà apportare le correzioni necessarie per poter completare la valutazione. Le parti corrette saranno nuovamente verificate dai Valutatori, per accertare che tutti i problemi siano stati risolti con le correzioni apportate. Il Rapporto Finale di Valutazione non potrà essere emesso finché tutti i problemi/errori non siano stati risolti. E' consigliabile prevedere nel PDV che alcune attività debbano essere parzialmente ripetute a causa di errori e/o documentazione non completa, anche se risulta difficile prevedere correttamente quanti casi di errori possono verificarsi in una valutazione. L'LVS può inserire specifiche clausole nel contratto e nel PDV per prevedere eventuali estensioni del Piano di Valutazione conseguenti ad esempio:

- al ritardo provocato dal Committente per le correzioni che l'LVS dovrà apportare;
- al lavoro addizionale che dovrà affrontare dovendo ripetere alcune parti della valutazione, a causa della non adeguata qualità della documentazione o degli eccessivi aggiornamenti della documentazione e/o dell'ODV.

2.3.5 Aggiornamenti

Nel corso di una valutazione, potrebbe essere necessario emendare alcuni aspetti di un PDV per poter valutare l'ODV al livello di garanzia richiesto. Per assicurarsi che qualsiasi modifica al PDV non abbia un impatto sulla sua accettabilità per quello specifico livello di garanzia, tutte le variazioni apportate a un PDV devono essere approvate dall'OC. Un aggiornamento del PDV può essere necessario come risultato, ad esempio, di:

- modifiche nell'ODV durante la valutazione (per rendere possibile una maggiore diffusione di un prodotto o perché alcuni problemi sono stati eliminati);
- non rispetto, da parte del Committente, dei tempi di consegna dei materiali per la valutazione nel formato e nel modo concordati, o non rispetto dei tempi di esecuzione stabiliti.

Per una valutazione di breve durata (tipicamente meno di otto settimane), è improbabile che il relativo PDV abbia bisogno di essere aggiornato, come potrà non esserci una Riunione di Controllo della Valutazione in tale breve valutazione. Comunque il PDV dovrà ancora essere discusso nella Riunione di Avvio Lavori.

Durante una valutazione, i Valutatori potrebbero voler effettuare attività che non fanno parte della valutazione "standard". Ad esempio:

- i Valutatori possono ritenere necessario scostarsi da una rigida interpretazione dei requisiti dello Schema o dei criteri di valutazione;
- i Valutatori possono voler effettuare attività opzionali per facilitare future ri-valutazioni dell'ODV.

È importante che qualsiasi attività aggiuntiva, come quelle sopra indicate, sia chiaramente identificata come tale e approvata in anticipo dall'OC. Per individuare accettabili scostamenti da una rigida interpretazione dello Schema o dei criteri di valutazione si possono utilizzare Rapporti di Osservazione dello Schema (ROS).

Si osservi che modifiche del PDV possono, in alcuni casi, richiedere emendamenti al contratto tra il Committente e l'LVS.

Durante l'intera valutazione, l'OC sorveglierà il lavoro dei Valutatori. È quindi importante che i Valutatori forniscano all'OC informazioni sulla pianificazione che siano adeguate e mantenute aggiornate. Tali informazioni devono essere fornite e conservate come allegati del PDV.

2.4 Dipendenze nella pianificazione

Alcune attività non possono iniziare se non sono state completate altre attività precedenti. Ciò introduce una rigidità nel piano di lavoro e un possibile propagarsi dei ritardi se queste attività, che debbono essere completate prima di altre, vengono terminate più tardi del previsto.

Per sopperire parzialmente a tale rigidità della pianificazione, le attività che dipendono dal completamento di altre possono essere iniziate usando i risultati provvisori delle prime, ma si dovranno comunque attendere i dati definitivi di valutazione per poter completare i relativi processi valutativi.

Nell'Appendice F si riportano le attività che prevedono di generare/utilizzare i dati parziali che verranno utilizzati/generati dalle attività successive/precedenti.

2.5 Complessità e caratteristiche dell'ODV

La complessità e le caratteristiche dell'ODV sotto valutazione ed il livello di garanzia prescelto influenzano in modo significativo la durata del processo di valutazione e di conseguenza la complessità e la lunghezza del PDV. Infatti, la valutazione di un sistema di ridotta complessità ad un basso livello di garanzia permette di combinare diverse fasi di analisi abbreviando i tempi di valutazione, mentre la valutazione di un sistema complesso che richieda un alto livello di garanzia obbliga i Valutatori ad affrontare un articolato processo di verifica con una notevole mole di lavoro in termini:

- quantitativi (dimensioni del sistema, numero dei componenti presenti, etc);
- qualitativi (strumenti di verifica, linguaggi di sviluppo, documentazione da verificare, prove d'Intrusione, complessità dei rapporti da produrre, linguaggi formali da utilizzare, etc);
- organizzativi (gruppi di lavoro più numerosi, maggior numero d'incontri tecnici con le parti, necessità di addestramento dei Valutatori su metodologie - strumenti - linguaggi usati dal Fornitore, maggiore possibilità di ritardi etc).

Nel gestire una valutazione complessa risulta utile suddividere un ODV in sotto sistemi o parti omogenee (macroattività) per le quali il processo di valutazione può essere condotto separatamente per poi consolidarne i risultati. Tale organizzazione agevola l'LVS perché consente di affrontare la valutazione con gruppi di lavoro più piccoli, indirizzati su moduli di attività di durata minore rispetto a tutto il processo di valutazione, consentendo una maggiore flessibilità di organizzazione delle risorse, un migliore controllo del lavoro ed una riduzione dei ritardi nella risoluzione dei problemi emersi durante la valutazione. Tale organizzazione agevola, altresì, l'Organismo di Certificazione nel momento di verifica delle attività dell'LVS, perché consente una verifica in moduli di tutto il processo.

2.6 Valutazione di soluzioni hardware e firmware

Quando l'ODV comprende componenti hardware da valutare, gli LVS dovranno essere dotati di laboratori opportunamente attrezzati (protocol analyzer, network equiment, Automated Test Equipment, multimeters, oscilloscopi, etc) e anche i Valutatori dovranno avere una opportuna conoscenza della materia ed una esperienza tecnica appropriata. Potrà risultare necessario che i Valutatori seguano corsi di specializzazione per migliorare le loro conoscenze sugli specifici apparati sotto valutazione e/o l'LVS potrà richiedere l'aiuto di specialisti del settore. In quest'ultimo caso gli specialisti lavoreranno sotto il controllo di un Valutatore esperto dell'LVS. L'Organismo di Certificazione dovrà essere informato del tipo di soluzione adottata e il PDV ed l'RFV dovranno riportare, nella descrizione delle attività, l'impiego di esperti esterni e/o i corsi di addestramento seguiti dai Valutatori.

Quando l'ODV comprende componenti firmware, la valutazione interessa sia aspetti legati al software, sia aspetti legati all'hardware. Infatti, potrà essere necessario esaminare il codice del firmware, le interfacce hardware, il software dei protocolli adottati, l'eventuale interfaccia utente, etc. Anche in questo caso potrà essere necessario l'approfondimento da parte dei Valutatori di aspetti specifici, o l'intervento di specialisti del settore.

3 Contenuto di un Piano di Valutazione standard per un ODV

3.1 Premessa alla stesura di un Piano di Valutazione

In questo capitolo viene riportata la descrizione della struttura di un PDV standard riferita al caso di un sistema/prodotto (ODV). Nel caso la valutazione si riferisca ad un Profilo di Protezione, il PDV andrà ricavato effettuando le opportune semplificazioni o modifiche.

Nel seguito è descritto il contenuto dei diversi capitoli che compongono il PDV, gli argomenti che debbono essere trattati nei singoli capitoli, il dettaglio che tali contenuti debbono precisare, la documentazione minima che deve essere allegata al documento.

Il PDV standard fornisce la base per la costruzione di un PDV specifico per l'ODV, in dipendenza del livello di garanzia e dei criteri adottati.

Il PDV dovrà contenere i seguenti capitoli:

- Pagine iniziali informative di presentazione del documento
- Capitolo I - Introduzione
- Capitolo II - Descrizione dell'ODV
- Capitolo III - Macroattività del Processo di valutazione
- Capitolo IV - Attività di valutazione
- Capitolo V - Vincoli e Limiti della valutazione
- Appendice A - Specifiche delle Attività di valutazione;
- Appendice B - Piano delle Attività
- Appendice C - Risorse e Timescale
- Appendice D - Documenti per il Processo di valutazione
- Appendice E - Strategia di Campionamento
- Appendice F - Risultati Intermedi di valutazione

3.2 Pagine iniziali

Le pagine iniziali del PDV dovranno riportare almeno le seguenti informazioni:

- nome dell'LVS che ha redatto il PDV;
- sigla identificativa della valutazione, concordata tra l'LVS e l'OC;
- numero di versione del PDV e data di emissione di tale versione;
- numero delle pagine modificate, motivo e data della modifica;
- nome del redattore del PDV e del revisore.
- indice del PDV;

- lista dei documenti referenziati nel PDV;
- glossario dei termini usati.

3.3 Capitolo I - Introduzione

Questo capitolo deve identificare sinteticamente, ma in modo chiaro:

- l'ODV sotto valutazione;
- la piattaforma hardware, software, firmware, il livello di garanzia richiesto e i meccanismi di sicurezza adottati per raggiungerlo;
- i Criteri secondo cui dovrà essere effettuata la valutazione;
- l'LVS prescelto;
- il Committente della valutazione.

Nel caso di ODV complessi può risultare utile suddividere l'ODV stesso in sottosistemi o parti per i quali il processo di valutazione può essere condotto separatamente, per poi consolidarne i risultati; in questo caso si genereranno più PDV, uno per ogni parte in cui l'ODV sarà suddiviso, e il capitolo I del documento dovrà indicare chiaramente a quale sottosistema o parte di valutazione questo PDV si riferisce.

E' possibile condurre una valutazione parziale del sistema. Ciò avviene nei casi di sistemi complessi in cui la sicurezza è applicata solo in una piccola e definita parte del sistema stesso.

In questo capitolo l'LVS deve indicare la struttura del PDV adottata e se vi è motivo di organizzare il documento in modo diverso rispetto allo standard. Ciò accade normalmente quando la valutazione richiede la generazione di informazioni aggiuntive oppure quando può essere necessario gestire in modo riservato alcune informazioni.

3.4 Capitolo II - Descrizione dell'ODV

Le caratteristiche dell'ODV sono normalmente contenute nel Traguardo di Sicurezza. Se le informazioni ivi riportate sono sufficientemente chiare e adeguate non occorre riportare nel PDV questa descrizione, ma si può far riferimento a tale documento; qualora ciò non si verificasse, occorre fornire in questo capitolo del PDV tutte le informazioni di seguito indicate.

3.4.1 Descrizione Generale dell'ODV

Questa sezione deve fornire una descrizione generale dell'ODV e specificare, in particolare, quali informazioni l'ODV gestisce, il numero degli utenti del sistema, la loro qualifica, il loro livello di sicurezza.

3.4.2 Sviluppo dell'ODV

In questa parte occorre precisare come è stato sviluppato dal Committente/Fornitore l'ODV sotto valutazione, riportando quando è stato sviluppato la prima volta, le metodologie e la tecnologia applicata al suo sviluppo, le fasi principali del piano di

realizzazione e se eventualmente è stato sottoposto a precedenti valutazioni e con quale esito.

3.4.3 Architettura dell'ODV

Questa sezione del documento deve riportare i dettagli architetturali dell'hardware, software e firmware con le funzionalità di sicurezza fornite da ognuno di questi moduli. Per i sistemi che sono costituiti da un certo numero di prodotti deve essere fornita la descrizione di ognuno di essi evidenziando per ciascun prodotto il contributo alla sicurezza del sistema e specificando i metodi d'integrazione di tali moduli per raggiungere un sistema globale con un determinato livello di sicurezza.

3.4.4 Documentazione dell'ODV

In questa sezione vengono referenziati i documenti che il Committente deve fornire specificando il livello di dettaglio delle informazioni richiesto e il tempo di consegna concordato.

Qualora tali documenti debbano essere forniti da altre organizzazioni si deve indicarne il nome, il responsabile e la data concordata per la consegna.

3.5 Capitolo III - Macroattività del processo di valutazione

E' già stato precisato che nel caso di ODV complesso può risultare utile suddividere l'ODV stesso in sottosistemi o parti omogenee (macroattività) per le quali il processo di valutazione può essere condotto separatamente, per poi consolidarne i risultati. Quindi, per tale ODV si genererà un insieme di PDV, che conterranno in modo distinto i vari PDV relativi alle sottoparti in cui l'ODV è stato suddiviso.

In questa sezione del documento occorre identificare il numero delle parti in cui l'ODV viene suddiviso e fornire, per ogni parte, la descrizione delle attività ad essa correlate.

Supponendo ad esempio che l'ODV complesso sia suddiviso in tre parti, si avrà un processo di valutazione così articolato:

- processo di valutazione della prima parte, con evidenziata l'integrazione delle tre parti per raggiungere il livello globale di sicurezza del sistema;
- processo di valutazione della seconda parte;
- processo di valutazione della terza parte.

Di conseguenza, per ogni parte di valutazione saranno indicati:

- obiettivi della parte di valutazione;
- scopo della parte di valutazione;
- attività correlate alla parte di valutazione;

Le attività di valutazione saranno riportate nell'Appendice A in modo distinto per ogni parte. L'Appendice B, che descrive il piano delle Attività, dovrà riportare in modo specifico le varie parti in cui è stato suddiviso il processo di valutazione.

3.6 Capitolo IV - Attività di valutazione

Il capitolo IV dovrà contenere la descrizione generale delle attività che verranno svolte dai Valutatori, durante il processo di valutazione. La descrizione specifica di tali attività sarà riportata nell'Appendice A del PDV. Qualora l'LVS decida di eseguire delle attività di valutazione che differiscono da quelle previste dal PDV standard, dovrà dettagliare i motivi di tale decisione ed elencare e descrivere le attività prescelte e correlarle con le attività indicate nel PDV standard.

In particolare, in questo capitolo potranno essere svolte osservazioni anche su:

- *Tecniche e strumenti di valutazione*, al fine di fornire motivazioni relative al loro utilizzo e indicazioni relative al loro funzionamento;
- *Classi di Funzionalità e Protection Profile* a cui si fa riferimento nel Traguardo di Sicurezza;
- *Campionamento dei test*, al fine di motivare la scelta della strategia di campionamento adottata;
- *Ri-Valutazioni e Ri-uso di Valutazioni*, al fine di segnalare l'eventuale adesione allo Schema di Gestione dei Certificati, di esprimere la volontà di sottoporre l'ODV a successive ri-valutazioni, o di indicare se e come la valutazione utilizzi i risultati di una precedente valutazione;
- *Requisiti di Tracciabilità*, per confermare che ogni livello di descrizione dell'ODV sia un raffinamento adeguato rispetto a ciò che è riportato nel livello più alto, senza alterazione dei requisiti.

3.7 Capitolo V - Vincoli e limiti della valutazione

In questo capitolo del PDV si devono riportare tutti gli elementi critici che si prevede di incontrare durante il processo di valutazione e che possono avere un impatto con la durata, con i metodi e con i risultati della valutazione stessa.

Si possono prevedere vincoli sui seguenti aspetti a carico dell'LVS:

- l'LVS può non avere disponibili, in alcuni periodi previsti per la valutazione, un numero sufficiente di Valutatori;
- l'LVS deve interfacciare più organizzazioni durante la valutazione (riunioni, documenti d'analizzare, report da generare);
- l'LVS si può trovare nelle condizioni di dover utilizzare specifici metodi o strumenti per la valutazione, per cui necessita di tempo e risorse per apprenderli.

Si possono prevedere limiti sugli aspetti della gestione della valutazione a carico del Committente, quali ad esempio:

- la ritardata disponibilità dei documenti;

- la ritardata risoluzione ai problemi emersi durante la valutazione che può costringere i Valutatori a limitare e/o ripianificare attività o riunioni con il Committente stesso e con l'OC.

3.8 Appendice A - Specifiche delle attività di valutazione

Questa Appendice contiene la descrizione di tutte le attività che l'LVS pianifica di eseguire sull'ODV per raggiungere il Livello di garanzia richiesto dal Committente.

Nel caso di una valutazione condotta secondo i criteri ITSEC, si potrà richiedere all'Organismo di Certificazione ulteriore documentazione per la stesura di questa Appendice.

Nel caso di una valutazione condotta secondo i Common Criteria, in questa Appendice devono essere riportate le unità di lavoro, descritte nella LGP4 per le valutazioni ai livelli di garanzia fino ad EAL4.

3.9 Appendice B - Piano delle Attività

Questa Appendice contiene la pianificazione (descritta mediante un diagramma di Gantt) di tutte le attività che l'LVS esegue sull'ODV per raggiungere il Livello di garanzia richiesto dal Committente. Si faccia riferimento al par. 2.3 per l'individuazione delle attività previste per le valutazioni svolte secondo i criteri ITSEC e CC.

3.10 Appendice C - Risorse e Timescale

Questa Appendice contiene la stima di impegno (giorni/uomo) di tutte le attività e per ogni azione che i Valutatori eseguono sull'ODV per raggiungere il Livello di garanzia richiesto dal Committente. Per il caso dei CC, si faccia riferimento alle azioni di valutazione descritte nella LGP4 per le valutazioni ai livelli di garanzia fino ad EAL4

3.11 Appendice D - Documenti per il processo di valutazione

Questa Appendice contiene l'elenco di tutti i documenti relativi alle attività di valutazione. Per ogni documento deve essere indicata la data di consegna e delle eventuali revisioni.

3.12 Appendice E - Strategia di campionamento

Questa Appendice contiene la descrizione delle metodologie di campionamento dei test adottate dall'LVS durante il processo di valutazione dell'ODV.

3.13 Appendice F - Risultati intermedi di valutazione

Questa Appendice riporta quelle attività e sottoattività (vedi LGP4) che prevedono di generare dati parziali (intermedi), durante il processo di valutazione, che sono utilizzati come dati di ingresso da attività successive. Nel caso di una valutazione condotta secondo i criteri ITSEC, si potrà richiedere all'Organismo di Certificazione ulteriore documentazione per la stesura di questa Appendice, mentre nel caso dei

Common Criteria valgono in generale le dipendenze tra le componenti riportate nell'annesso A di [CCI3].

4 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.

5 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