Organismo di Certificazione
della Sicurezza Informatica

Nota Informativa dello Schema N. 1/13

Modifiche alla LGP1

Novembre 2013
Versione 1.0

REGISTRAZIONE DELLE AGGIUNTE E VARIANTI

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

Paragrafi della LGP1 modificati	**Data**
2.4.1, 3.1, 4.5, 5.3, 5.4, 5.5, 7	Marzo 2007
Tutti	Novembre 2013

INDICE

Scopo del documento

Il presente documento ha lo scopo di modificare e integrare le procedure descritte nella Linea Guida Provvisoria LGP1 avente per titolo “Descrizione Generale dello Schema Nazionale”.

Tali modifiche includono e ampliano anche le disposizioni contenute nella NIS 1/07 (marzo 2007), che pertanto si intende superata.

Per facilità di lettura, nel seguito viene riportata l’intera Linea Guida Provvisoria LGP1, così come appare per effetto delle modifiche intervenute.

Le disposizioni contenute nella NIS 1/13 sono immediatamente operative e quindi sostituiscono a tutti gli effetti le parti corrispondenti contenute nella LGP1.

1 Lo Schema nazionale

L'istituzione dello Schema nazionale italiano per la valutazione e la certificazione della sicurezza dei sistemi e dei prodotti nel settore della tecnologia dell'informazione, avvenuta attraverso un Decreto del Presidente del Consiglio dei Ministri, "Approvazione dello Schema nazionale per la valutazione e certificazione della sicurezza nel settore della tecnologia dell'informazione, ai sensi dell'art.10, comma 1, del decreto legislativo 23 febbraio 2002, n. 10", DPCM del 30 ottobre 2003, GU n. 98 del 27 aprile 2004 [DPCM], 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" o "Schema", recante l'insieme delle procedure e delle regole nazionali necessarie per la valutazione e certificazione, in conformità allo standard ISO/IEC15408[1] (Common Criteria) [CC1,2,3] e alla corrispondente metodologia [CEM];
- la definizione, nell'ambito dello Schema nazionale, della "sicurezza nel settore della tecnologia dell'informazione" come 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;
- la necessità di favorire, anche 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.

Si riportano di seguito i riferimenti normativi e politici adottati nell'istituzione dell'Organismo di Certificazione:

- 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

[1] Lo standard ISO/IEC 15408 corrisponde alla versione 2.3 dei CC, non più in uso dal marzo 2008; pertanto, le nuove valutazioni dovranno essere condotte utilizzando la versione 3.1 o successiva.

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 [UNI1] concernenti i requisiti generali per la competenza dei laboratori di prova e di taratura e UNI CEI EN 45011[2] concernenti i requisiti generali relativi agli organismi che gestiscono sistemi di certificazione di prodotti;
- l'atto del Comitato di gestione dell'ISO (International Organization for Standardization) che definisce come International Standard ISO/IEC 15408 i "Common Criteria for Information Technology Security Evaluation".

In questo contesto, il decreto [DPCM] riconosce che l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCTI) del Ministero delle Comunicazioni (oggi "Ministero dello Sviluppo Economico - Dipartimento per le 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'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (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".

Le procedure relative allo Schema nazionale devono essere osservate 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 agli standard internazionali.

L'utilità primaria della certificazione della sicurezza di un prodotto/sistema/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 Common Criteria [CC1,2,3] e la corrispondente metodologia [CEM].

Lo Schema aderisce agli accordi internazionali di mutuo riconoscimento delle certificazioni, che si occupano anche dell'applicazione, dell'armonizzazione e dell'evoluzione dello standard Common Criteria, in ambito mondiale [CCRA] ed europeo [SOGIS].

Lo Schema non si applica ai prodotti e sistemi che trattano informazioni classificate.

[2] Nel 2012, la norma è stata sostituita dalla UNI CEI EN ISO/IEC 17065 [UNI2].

2 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 (OC);
b) il Laboratorio per la Valutazione della Sicurezza (LVS);
c) il Committente;
d) il Fornitore;
e) l'Assistente.

2.1 L'Organismo di Certificazione

Lo Schema abilita un solo Organismo di Certificazione (OC); in base al decreto istitutivo [DPCM]: "l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCTI) del Ministero delle Comunicazioni (oggi "Ministero dello Sviluppo Economico - Dipartimento per le Comunicazioni") è l'Organismo di Certificazione della sicurezza nel settore della tecnologia dell'informazione".
L'OC 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) la predisposizione, l'aggiornamento e la pubblicazione dell'elenco degli LVS accreditati;
h) l'approvazione dei Piani di Valutazione;
i) l'iscrizione delle valutazioni nello Schema;
j) l'approvazione dei Rapporti Finali di Valutazione;
k) l'emissione dei Rapporti di Certificazione;
l) l'emissione e la revoca dei Certificati;
m) la definizione, l'aggiornamento e la pubblicazione della lista di prodotti, sistemi e profili di protezione certificati e in corso di certificazione;
n) la promozione delle attività per la diffusione della cultura della sicurezza nel settore della tecnologia dell'informazione;
o) la formazione e l'addestramento dei Certificatori, personale dipendente dell'OC;

p) la formazione e l'abilitazione dei Valutatori, dipendenti degli LVS, e degli Assistenti, ai fini dello svolgimento delle attività di valutazione;
q) la definizione, l'aggiornamento e la pubblicazione dell'elenco degli Assistenti.

2.2 Il Laboratorio per la Valutazione della Sicurezza

Nell'attività di valutazione l'OC si avvale di Laboratori per la Valutazione della Sicurezza (LVS), che svolgono le attività connesse alla valutazione e che devono essere accreditati dall'OC stesso.
Ai fini dell'accreditamento, l'LVS deve possedere i seguenti requisiti:

a) la capacità di garantire l'imparzialità, l'indipendenza, la riservatezza e l'obiettività, che sono alla base del processo di valutazione;
b) la disponibilità di locali e mezzi adeguati ad effettuare valutazioni della sicurezza nel settore della tecnologia dell'informazione;
c) un'organizzazione in grado di controllare il rispetto delle misure di sicurezza e di gestione della qualità previste per il processo di valutazione;
d) la disponibilità di personale sufficiente dotato delle necessarie competenze tecniche;
e) conformità ai requisiti specificati nelle norme UNI CEI EN ISO/IEC 17025 [UNI1] e UNI CEI EN 17065 [UNI2], per quanto applicabili;
f) la capacità di mantenere nel tempo i requisiti in virtù dei quali è stato accreditato.

Oltre alle attività di valutazione, un LVS può svolgere anche le attività sotto elencate:

a) Assistenza al Committente per:
   1) la stesura della documentazione di sicurezza durante le fasi di preparazione e/o di conduzione della valutazione;
   2) la determinazione della valutabilità del TDS, ODV o Profilo di Protezione;
   3) le attività connesse con la gestione e il mantenimento dei Certificati.
b) Formazione sulle tematiche della sicurezza nel settore della tecnologia dell'informazione in generale e, in particolare, sulle tecniche di valutazione.

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

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.

2.3 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 richiede all'Organismo di Certificazione l'iscrizione della valutazione nello Schema nazionale.

2.4 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.

2.5 L'Assistente

L'Assistente è una persona formata, addestrata e abilitata dall'OC per fornire supporto tecnico al Committente o al Fornitore o a un LVS che ne faccia richiesta, ad esempio per:

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

3 Pubblicazioni dello Schema nazionale

Per consentire l'applicazione dello Schema nazionale l'OC ha predisposto le "Linee Guida Provvisorie" (LGP), organizzate in documenti distinti, brevemente descritti di seguito.

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

La LGP1 introduce il concetto di Schema nazionale, definendo i ruoli dei soggetti coinvolti nel processo di valutazione e certificazione: l'Organismo di Certificazione, il Laboratorio per la Valutazione della Sicurezza, il Committente, il Fornitore e l'Assistente.

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 LVS secondo lo Schema nazionale. Inoltre, vengono specificati gli ambiti di attività di un LVS e descritti i requisiti generali gestionali e di competenza tecnica per i laboratori. Infine, vengono descritti i requisiti e le procedure per ottenere l'abilitazione al ruolo di Assistente.

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 prodotto o un sistema (insieme di prodotti) software, firmware e/o hardware per l'elaborazione elettronica delle informazioni, cioè l'Oggetto Della Valutazione (ODV), così come definito nei Common Criteria, 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.

Oltre alle Linee Guida, l'Organismo di Certificazione può emettere anche le Note Informative dello Schema (NIS), che costituiscono uno strumento agile per interpretare ed integrare le pubblicazioni dello Schema e/o dei criteri di valutazione in modo più immediato rispetto all'aggiornamento periodico delle Linee Guida. Una NIS potrà contenere disposizioni dell'OC riguardo diversi argomenti, quali ad esempio:

- aggiornamento delle Linee Guida provvisorie (LGP);
- 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.

L'OC gestisce un elenco aggiornato delle NIS, che costituiscono norme e/o procedure obbligatorie dello Schema e, come tali, sono immediatamente operative, distribuite a tutti gli LVS e pubblicate sul proprio sito web [OCSI]. Pertanto, si deve obbligatoriamente fare riferimento all'ultima versione disponibile.

Infine, l'OC può emanare altri documenti di supporto, a carattere non cogente, contenenti 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. Anche tali documenti sono pubblicati sul sito web dell'OC e quindi, anche per essi, si deve fare riferimento all'ultima versione disponibile.

Con la pubblicazione del presente documento, le Linee Guida LGP4, LGP5, LGP6 e LGP7 sono abrogate.

4 Gestione di reclami e contenziosi

Per ogni segnalazione riguardante possibili problemi riscontrati durante l'applicazione dello Schema, quali ad esempio i processi di certificazione, di accreditamento o altro, si applicherà la specifica procedura dell'OC per la gestione di reclami e contenziosi. Al riguardo, le eventuali istanze dovranno essere presentate direttamente all'OC.

Nella richiesta dovrà essere chiaramente specificato l'oggetto cui si riferisce l'istanza presentata, allegando tutta la documentazione ritenuta necessaria.

L'OC esaminerà la richiesta e comunicherà la sua proposta di risoluzione del problema segnalato entro trenta giorni lavorativi dal ricevimento. Qualora tale risoluzione non fosse accettata dal richiedente, si proseguiranno tempestivamente gli atti al Segretario Generale del Ministero dello Sviluppo Economico, che nominerà un apposito comitato di esperti, prescelti anche sulla base del merito della specifica istanza, per giungere a definitiva soluzione.

Riferimenti bibliografici

[CC1] CCMB-2012-09-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 4, September 2012

[CC2] CCMB-2012-09-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 4, September 2012

[CC3] CCMB-2012-09-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 4, September 2012

[CEM] CCMB-2012-09-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 4, September 2012

[CCRA] "Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security", Version 1.0, May 2000

[DPCM] "Approvazione dello Schema nazionale per la valutazione e certificazione della sicurezza nel settore della tecnologia dell’informazione, ai sensi dell'art.10, comma 1, del decreto legislativo 23 febbraio 2002, n. 10", DPCM del 30 ottobre 2003, GU n. 98 del 27 aprile 2004

[OCSI] Sito web dell'OCSI: <www.ocsi.isticom.it>

[SOGIS] Senior Officials Group Information Systems Security (SOG-IS) of the European Commission, "Mutual Recognition Agreement of Information Technology Security Evaluation Certificates", Version 3.0, January 2010

[UNI1] UNI/CEI EN ISO/IEC 17025. “Requisiti generali per la competenza dei laboratori di prova e di taratura”, 2005

[UNI2] UNI/CEI EN ISO/IEC 17065, “Valutazione della conformità: requisiti per organismi che certificano prodotti, processi e servizi”, 2012

Lista degli acronimi

CC	=	Common Criteria
CE	=	Commissione Europea
CEI	=	Comitato Elettrotecnico Italiano
DPCM	=	Decreto del Presidente del Consiglio dei Ministri
EAL	=	(Evaluation Assurance Level) Livello di garanzia della valutazione
EN	=	European Norm
GU	=	Gazzetta Ufficiale
IEC	=	International Electrotechnical Commission
ISCTI	=	Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione
ISO	=	International Organization for Standardization
IT	=	Information Technology
LGP	=	Linea Guida Provvisoria
LVS	=	Laboratorio di Valutazione della Sicurezza
NIS	=	Nota Informativa dello Schema
OC	=	Organismo di Certificazione
ODV	=	Oggetto Della Valutazione (TOE - Target of Evaluation)
PP	=	Profilo di Protezione (Protection Profile)
TDS	=	Traguardo di Sicurezza (ST – Security Target)
UNI	=	Ente Nazionale Italiano di Unificazione