

Decreto del Presidente del Consiglio dei Ministri 11 aprile 2002 ⁽¹⁾.

Schema nazionale per la valutazione e la certificazione della sicurezza delle tecnologie dell'informazione, ai fini della tutela delle informazioni classificate, concernenti la sicurezza interna ed esterna dello Stato ⁽²⁾.

(1) Pubblicato nella Gazz. Uff. 6 giugno 2002, n. 131.

(2) Vedi, anche, il *D.P.C.M. 3 febbraio 2006*.

**IL PRESIDENTE
DEL CONSIGLIO DEI MINISTRI**

Visti gli articoli 1 e 12 della *legge 24 ottobre 1977, n. 801*, recante «Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato»;

Visto il regio decreto-legge 11 luglio 1941, n. 1161 recante «Norme relative al segreto militare»;

Vista la pubblicazione del Presidente del Consiglio dei Ministri P.C.M.-A.N.S. 1/R - Norme unificate per la tutela del segreto di Stato - Volume I - Sistema di sicurezza - Edizione 1987;

Vista la pubblicazione del Presidente del Consiglio dei Ministri P.C.M.-A.N.S. 1/R - Norme unificate per la tutela del segreto di Stato - Volume III - Sicurezza industriale - Edizione 1993;

Vista la pubblicazione del Presidente del Consiglio dei Ministri P.C.M.-A.N.S. 1/R/A - Norme unificate per la tutela del segreto di Stato - Direttiva per la protezione delle informazioni coperte dal segreto di Stato trattate nei sistemi di elaborazione automatica e/o elettronica di dati (E.A.D.) - Edizione 1993;

Vista la pubblicazione del Presidente del Consiglio dei Ministri P.C.M.-A.N.S. 1/R - Norme unificate per la tutela del segreto di Stato - Volume II - Sicurezza delle comunicazioni ed organizzazioni e procedure del servizio cifra - Edizione 1994;

Vista la pubblicazione del Presidente del Consiglio dei Ministri P.C.M.-A.N.S. COMSEC 256 (B) - Norme relative all'installazione di apparati elettrici ed elettronici che elaborano informazioni classificate - Edizione 1998;

Visto l'atto della Commissione europea datato giugno 1991 con il quale sono stati stabiliti i criteri di valutazione della sicurezza dei sistemi informatici denominati «ITSEC» (Information Technology Security Evaluation Criteria);

Vista la Raccomandazione del Consiglio dell'Unione europea (95/144/CE) in data 7 aprile 1995 concernente l'applicazione di omogenei criteri per la valutazione della sicurezza delle tecnologie dell'informazione (ITSEC) nell'ambito delle procedure di valutazione e certificazione;

Visto l'atto del Comitato di gestione dell'ISO che recepisce quale International Standard ISO/IEC IS n. 15408, la versione 2.1 dei «Common Criteria», documento recante la definizione dei criteri tecnici di valutazione delle tecnologie dell'informazione;

Visto l'accordo sul Mutuo riconoscimento dei certificati emessi secondo i predetti Criteri comuni nel campo della sicurezza della tecnologia dell'informazione, sottoscritto il 23 maggio 2000 al fine di assicurare la cooperazione e il mutuo riconoscimento, a livello comunitario e internazionale, dei certificati di valutazione della sicurezza delle tecnologie dell'informazione;

Visto l'art. 5 del citato accordo che dispone che le valutazioni siano condotte secondo uno schema da adottare a cura di ciascun Paese aderente, che garantisca la competenza tecnica dei centri adibiti alla valutazione e l'imparzialità del procedimento;

Vista la Risoluzione del Consiglio dell'Unione europea del 28 gennaio 2002 relativa a un approccio comune e ad azioni specifiche nel settore della sicurezza delle reti e dell'informazione;

Ravvisata pertanto la necessità di definire uno schema nazionale per la valutazione e certificazione della sicurezza delle tecnologie dell'informazione, dei sistemi e dei prodotti destinati alla trattazione delle informazioni classificate, che individui procedure, competenze e responsabilità dei soggetti coinvolti nei processi di valutazione e certificazione;

Acquisito il parere dell'Autorità per l'informatica nella pubblica amministrazione, espresso nell'adunanza del 28 febbraio 2002;

Decreta:

1. *Oggetto e ambito di applicazione dello schema nazionale.*

Il presente schema nazionale per la valutazione e la certificazione della sicurezza nel settore delle tecnologie dell'informazione per la tutela delle informazioni classificate disciplina le linee essenziali per la definizione dei criteri e delle procedure da osservare per il funzionamento degli organismi di certificazione e per la valutazione dei prodotti e dei sistemi che gestiscono informazioni classificate.

Lo schema si applica ogniqualvolta una persona fisica o giuridica, le amministrazioni pubbliche e qualsiasi altro ente, associazione od organismo chiede la fornitura o lo sviluppo di un prodotto o di un sistema per la trattazione di tali informazioni.

2. Definizioni.

Ai fini del presente decreto si intende per:

1. «Autorità Nazionale per la Sicurezza», in seguito A.N.S., il Presidente del Consiglio dei Ministri ovvero l'Organo dallo stesso delegato per l'esercizio delle funzioni in materia di tutela delle informazioni, documenti e materiali classificati;

2. «Ufficio Centrale per la Sicurezza», l'articolazione della Segreteria Generale del Comitato esecutivo per i servizi di informazione e sicurezza (CESIS), di cui l'A.N.S. si avvale per l'attività amministrativa concernente la tutela delle informazioni, documenti e materiali classificati;

3. «informazione classificata», ogni informazione, documento o materiale cui sia stata attribuita, da un'autorità competente, una classifica di segretezza;

4. «criteri di valutazione della sicurezza delle tecnologie dell'informazione» ITSEC, i criteri uniformi di base, a livello europeo, per la valutazione e la certificazione della sicurezza della tecnologia della informazione idonei a consentire il mutuo riconoscimento di un prodotto o di un sistema a livello internazionale;

5. «manuale di valutazione della sicurezza delle tecnologie dell'informazione» ITSEM, il manuale recante i criteri base necessari per la valutazione della sicurezza delle tecnologie dell'informazione;

6. «criteri comuni» (o Common Criteria) i criteri base per la valutazione della sicurezza delle tecnologie dell'informazione, definiti in un documento tecnico costituente, nella versione 2.1, lo standard internazionale ISO denominato «International standard 15408»;

7. «schema nazionale», l'insieme delle procedure e delle regole nazionali necessarie per la valutazione e certificazione, in conformità ai criteri europei

ITSEC e ITSEM o agli standard internazionali ISO/IEC IS-15408, emanati dall'Organizzazione Internazionale per la Standardizzazione - ISO;

8. «tecnologie dell'informazione», l'insieme delle tecniche hardware e software applicate alla gestione automatica delle informazioni;

9. «sistema», l'insieme di prodotti, funzionalmente o fisicamente interconnessi, destinato al trattamento automatico delle informazioni per un utilizzo specifico in un ambiente definito;

10. «sistema classificato», un sistema impiegato per l'elaborazione, la trattazione, la conservazione e la trasmissione di informazioni classificate;

11. «prodotto», un elemento software o hardware, idoneo a fornire una determinata funzionalità, progettato per essere utilizzato o incorporato in uno o più sistemi;

12. «manuale di valutazione comune» o CEM, il documento tecnico recante i metodi e le procedure di valutazione della sicurezza della tecnologia dell'informazione, secondo i criteri comuni, idonei a consentire il mutuo riconoscimento di un prodotto o di un sistema a livello di omologhi organismi internazionali;

13. «linee guida», gli elementi di base esplicativi delle modalità di applicazione dello schema nazionale di valutazione e certificazione;

14. «committente», il soggetto pubblico o privato che richiede al fornitore lo sviluppo o la fornitura di un prodotto o di un sistema;

15. «fornitore», il soggetto pubblico o privato fornitore del prodotto o del sistema;

16. «ente di certificazione», l'organismo pubblico responsabile della certificazione dei prodotti e dei sistemi informatici, dell'accreditamento dei centri di valutazione nonché della definizione, dell'applicazione e dell'aggiornamento dello schema nazionale;

17. «certificazione», l'attestazione della corretta applicazione dei criteri di valutazione adottati per la realizzazione di un prodotto o sistema;

18. «centro di valutazione» o «CE.VA.», un organismo accreditato dall'A.N.S. in conformità agli standard internazionali, competente per le valutazioni di sicurezza di un prodotto o di un sistema;

19. «valutazione», l'analisi e la verifica da parte di un centro di valutazione della conformità di un prodotto o di un sistema ai requisiti di sicurezza;

20. «accreditamento», il riconoscimento formale dell'imparzialità e competenza di un centro di valutazione ad effettuare le valutazioni;

21. «target di sicurezza», l'insieme degli obiettivi di sicurezza predefiniti per un prodotto o un sistema da utilizzare quale parametro di riferimento per la valutazione e per la condotta cui attenersi nel corso delle valutazioni;

22. «oggetto della valutazione» il prodotto o il sistema sottoposto a valutazione;

23. «piano di valutazione», il documento prodotto da un centro di valutazione sottoposto all'approvazione dell'ente di certificazione recante la descrizione dell'organizzazione e delle attività necessarie per una specifica valutazione;

24. «profili di protezione», l'insieme dei requisiti ed obiettivi di sicurezza richiesti ad una categoria di prodotti o di sistemi;

25. «integrità», l'idoneità di un prodotto o di un sistema ad impedire che le informazioni classificate trattate possano essere modificate senza autorizzazione;

26. «disponibilità delle informazioni», la possibilità riconosciuta agli utenti autorizzati, di accedere alle informazioni o ai prodotti dell'attività di elaborazione;

27. «assistenza», il complesso dell'attività di supporto connessa alla formazione dei criteri, all'interpretazione delle disposizioni e alla redazione della documentazione richiesta dallo «schema»;

28. «rapporto finale di valutazione», il rapporto, emesso da un centro di valutazione e sottoposto all'approvazione dell'ente di certificazione, recante in dettaglio le operazioni e le conclusioni di una valutazione di un prodotto o di un sistema;

29. «rapporto di certificazione», il rapporto redatto dall'ente di certificazione nel quale viene attestata l'idoneità del prodotto o del sistema a garantire la sicurezza predefinita nel «target di sicurezza».

3. *Organismi responsabili.*

L'ente di certificazione è l'A.N.S. che a tal fine si avvale dell'Ufficio Centrale per la Sicurezza della Segreteria Generale del Comitato di cui all'art. 3 della *legge 24 ottobre 1977, n. 801*. L'ente di certificazione assicura l'applicazione dello schema nazionale per la valutazione e certificazione della sicurezza delle tecnologie dell'informazione per la tutela delle informazioni, documenti ed elementi classificati dalle stesse trattati.

Il Centro di valutazione è l'organo responsabile delle valutazioni di verifica della conformità di un prodotto o di un sistema ai requisiti di sicurezza predefiniti.

4. *Compiti dell'ente di certificazione.*

L'ente di certificazione:

a) definisce le regole procedurali per la certificazione dei prodotti o dei sistemi sulla base delle norme e direttive di riferimento nazionali ed internazionali;

b) cura l'accreditamento dei Ce.Va. secondo le procedure individuate dall'art. 7; determina la sospensione o la revoca dell'accreditamento in caso di accertate inadempienze agli obblighi nascenti dalle presenti disposizioni;

c) approva i piani di valutazione ed emana i rapporti di certificazione dei prodotti e dei sistemi sulla base dei rapporti finali di valutazione redatti dal CE.VA., ai sensi dell'art. 8;

d) rilascia le certificazioni sulla base delle valutazioni effettuate;

e) esamina, secondo le procedure individuate dall'art. 10, le eventuali controversie tra le parti coinvolte nel presente schema allo scopo di pervenire, ove possibile, ad una definizione consensuale delle stesse;

f) approva le disposizioni per la valutazione dei prodotti e dei sistemi;

g) esprime pareri sulle procedure concernenti l'attuazione dello schema nazionale di valutazione e certificazione;

h) coordina le attività dei CE.VA.;

i) cura le relazioni con gli enti di certificazione degli altri Paesi;

l) sottoscrive accordi di mutuo riconoscimento con le omologhe strutture degli altri Paesi e sovrintendere alla loro applicazione nell'ambito nazionale;

m) cura la tenuta dell'elenco dei CE.VA. accreditati, con l'indicazione dei settori di attività e del livello massimo di classifica delle informazioni classificate cui i medesimi sono abilitati ad avere accesso;

n) vigila sull'attività dei CE.VA. nel corso delle attività di valutazione;

o) redige ed aggiorna periodicamente la lista nazionale dei prodotti valutati;

p) provvede alla formazione tecnico professionale dei soggetti adibiti alla certificazione e valutazione, curando altresì il rilascio delle abilitazioni di sicurezza richieste agli stessi;

q) istruisce in materia di tutela amministrativa delle informazioni classificate il personale a diverso titolo impiegato nelle attività di valutazione.

5. *Compiti dei Centri di Valutazione.*

I CE.VA. valutano i prodotti o i sistemi secondo criteri di indipendenza e imparzialità, nel rispetto degli obblighi di segretezza e di riservatezza. A tal fine:

a) assistono il committente ed il fornitore di un prodotto o di un sistema nella redazione dei documenti di sicurezza;

b) forniscono all'ente di certificazione gli elementi utili per l'individuazione delle metodologie più idonee da adottare, informandolo sulle attività compiute ai fini della valutazione;

c) assicurano la salvaguardia di tutte le informazioni classificate relative al prodotto o al sistema sottoposto alla loro valutazione, anche quelle concernenti le informazioni tecniche acquisite nel corso dell'attività di valutazione;

d) il valutatore di un CE.VA. che abbia prestato assistenza al fornitore per un «oggetto della valutazione» o per parte di esso, non può partecipare alla valutazione dello stesso.

6. *Compiti del committente e del fornitore.*

1. Il committente provvede alla definizione dei requisiti di sicurezza del prodotto o del sistema richiesti, ai quali perviene attraverso un'adeguata analisi del rischio del prodotto o del sistema di cui si chiede la certificazione.

2. Il fornitore presenta al CE.VA. la documentazione di propria competenza necessaria per la condotta della valutazione. Egli, inoltre, fornisce al CE.VA. l'oggetto della valutazione, il target di sicurezza e tutta la documentazione e il materiale di supporto relativi agli aspetti di efficacia, correttezza e funzionalità, previsti dai criteri di valutazione applicati. A tale scopo egli può chiedere la collaborazione del committente e del CE.VA.

3. Il fornitore può chiedere al CE.VA. una stima del costo della valutazione, al fine di definire l'offerta da presentare al committente. A tale scopo fornisce:

a) la documentazione concernente i requisiti di sicurezza redatti dal committente;

b) il disegno architettonico della soluzione;

c) le proposte identificative dei prodotti e dei sottosistemi previsti dalla soluzione proposta;

d) eventuali profili di protezione di riferimento.

4. Il fornitore può chiedere in qualsiasi momento l'interruzione di una valutazione in corso, dandone comunicazione all'ente di certificazione.

7. Procedure per l'accreditamento del CE.VA.

L'ente pubblico o privato, che intende ottenere l'accreditamento del proprio laboratorio quale centro di valutazione di prodotti o di sistemi in conformità al presente schema, deve farne domanda all'ente di certificazione. L'accreditamento è subordinato all'accertamento del possesso da parte del laboratorio dei seguenti requisiti:

a) lo svolgimento dell'attività in locali adeguati e con mezzi idonei ad effettuare le valutazioni dei prodotti o dei sistemi;

b) l'esistenza di un'organizzazione interna in grado di assicurare il controllo ed il rispetto delle misure di sicurezza prescritte e di operare in piena autonomia di giudizio, indipendenza e imparzialità;

c) il possesso delle abilitazioni di sicurezza industriali prescritte;

d) la presenza di personale in possesso delle capacità professionali necessarie per la valutazione di prodotti o di sistemi di sicurezza, in conformità ai criteri in vigore;

e) il possesso da parte del personale impiegato delle abilitazioni di sicurezza richieste dall'ente di certificazione;

f) la conformità ai parametri definiti dalla «european norm (EN) 45001».

L'ente di certificazione, ricevuta la domanda di accreditamento, istruisce la pratica e avvia le necessarie procedure finalizzate ad esaminare le effettive capacità valutative del laboratorio richiedente. L'ente di certificazione richiede altresì al laboratorio di effettuare una valutazione di prova, al termine della quale il laboratorio produce il rapporto di valutazione.

L'ente di certificazione, a conclusione della prova di valutazione e di eventuali accertamenti suppletivi e sulla base della documentazione relativa alle caratteristiche del laboratorio e del personale impiegato, redige entro 90 giorni dalla ricezione della domanda di accreditamento un verbale recante la descrizione delle procedure osservate nonché l'assenso o il diniego al rilascio del certificato di accreditamento.

L'accreditamento ha validità triennale.

8. Procedure per la valutazione e certificazione di un prodotto o di un sistema.

1. Il committente interessato alla realizzazione e acquisizione di un prodotto o di un sistema definisce le specifiche di sicurezza richieste che costituiscono il riferimento base per lo sviluppo e la valutazione dell'oggetto della valutazione.

2. La valutazione di un prodotto o di un sistema è effettuata su richiesta del fornitore che fornisce all'ente di certificazione e al CE.VA. gli elementi necessari per il giudizio. A tal fine il fornitore produce l'oggetto della valutazione e ogni documentazione o materiale necessari per la valutazione del prodotto o del sistema.

3. Il fornitore individua tra i CE.VA. accreditati quello al quale affidare la valutazione di sicurezza, dandone comunicazione all'ente di certificazione.

4. Il CE.VA. produce all'ente di certificazione il piano di valutazione recante la descrizione delle attività necessarie al processo di valutazione. Il piano viene valutato dall'ente di certificazione che si esprime per l'approvazione entro 60 giorni dalla sua ricezione.

5. Il CE.VA. redige il rapporto finale di valutazione inoltrandolo all'ente di certificazione. Il rapporto è un documento recante informazioni classificate e non può essere rilasciato a terzi senza il consenso delle parti coinvolte nel procedimento.

6. L'ente di certificazione, sulla base dell'analisi della documentazione prodotta dal committente, dal fornitore e dal CE.VA., redige il rapporto di certificazione entro 90 giorni dalla ricezione del rapporto finale di valutazione approvato, rilasciandone copia al committente, al fornitore e al CE.VA.

7. In ordine al piano di valutazione ed al rapporto finale di valutazione prodotti dai CE.VA., possono essere formulate da parte dell'ente di certificazione osservazioni e richieste di chiarimenti.

8. In relazione alla valutazione di sistemi, i termini di cui ai numeri 4 e 6 del presente articolo possono essere differiti, d'intesa tra le parti, in ragione della complessità del sistema stesso. Ai fini del decorso dei predetti termini non è computato il tempo richiesto per il riscontro ad eventuali osservazioni e chiarimenti.

9. Nel caso in cui un fornitore realizza autonomamente un «prodotto» e questo si rivela d'interesse di un ente pubblico o privato, il fornitore può chiederne direttamente all'ente di certificazione l'attestazione di sicurezza.

9. Rapporto di certificazione.

Il rapporto di certificazione redatto dall'ente di certificazione attesta l'idoneità del prodotto o del sistema a garantire i livelli di sicurezza predefiniti. A tal fine il rapporto dichiara la conformità della valutazione alle procedure individuate nel presente decreto e la rispondenza del prodotto o del sistema ai criteri tecnici predefiniti per garantire la sicurezza delle informazioni trattate.

Quando il rapporto di certificazione si conclude con una decisione negativa, l'ente di certificazione inoltra motivato rapporto al CE.VA. e al fornitore, informandone nel contempo il committente.

Sulla base del rapporto, l'ente di certificazione rilascia il certificato attestante la conformità del prodotto o del sistema ai requisiti previsti dai criteri di riferimento.

10. Clausole di risoluzione consensuale delle controversie.

In caso di controversia relativa all'applicazione o all'interpretazione delle disposizioni contenute nel presente schema nazionale, il rappresentante del CE.VA. e il fornitore richiedono il preventivo intervento dell'ente di certificazione per la definizione della stessa anche quando la richiesta attenga il riesame del diniego relativo all'accreditamento del laboratorio, la sua sospensione o revoca ovvero il rifiuto di certificazione del prodotto o del sistema.

A tal fine, le parti interessate formulano specifica richiesta all'ente di certificazione da comunicarsi anche alle altre parti coinvolte nella procedura.

La richiesta reca una sintetica esposizione e descrizione dei fatti e degli elementi attinenti alle questioni, anche quelle di natura interpretativa, sulle quali è fondata la controversia.

L'ente di certificazione convoca le parti che si riuniscono entro 30 giorni dalla ricezione della richiesta per definire consensualmente la questione.

11. Abrogazioni e disposizioni finali.

Sono abrogate, in particolare, le direttive tecniche P.C.M.-A.N.S./TI-006 e P.C.M.-A.N.S./TI-007, recanti disposizioni per l'omologazione dei centri di valutazione della sicurezza informatica e per la certificazione dei prodotti e dei sistemi informatici destinati a gestire dati coperti dal segreto di Stato o di vietata divulgazione, approvate in data 30 agosto 1995 dall'Autorità nazionale per la sicurezza.

Con separati atti da emanarsi entro centoventi giorni dalla data di pubblicazione del presente decreto nella Gazzetta Ufficiale della Repubblica italiana, l'Autorità nazionale per la sicurezza delibera le linee guida per la realizzazione dei piani di valutazione cui dovranno attenersi il personale dei CE.VA., il committente e il fornitore al fine di assicurare la piena attuazione del presente schema nazionale.

Le disposizioni di cui al presente decreto entrano in vigore dal giorno successivo a quello della sua pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana.