



INTERVENTO SUL TEMA



**Sicurezza delle Tecnologie
dell'Informazione nella tutela
del Segreto di Stato**



ATTUAZIONE DELLA SICUREZZA INFORMATICA

In questi ultimi anni, le “Tecnologie dell’informazione” hanno assunto un ruolo rilevante e spesso vitale in quasi tutte le branche delle società industrializzate. L’introduzione delle cennate Tecnologie ha interessato ogni attività, ogni area, ogni settore con obiettivi sia tradizionali, quali l’efficienza e la efficacia dei sistemi informativi, sia avanzati, quali l’innovazione, la produttività e la competitività.

Un aspetto essenziale di tali problematiche, in continuo sviluppo ed evoluzione, è quello della protezione dei sistemi informativi, soprattutto nell’ambito della trattazione delle informazioni sensibili ai fini della sicurezza dello Stato (informazioni classificate).

Si parla di sicurezza nel campo informatico in modo massiccio da non molti anni. Ciò significa - e la cosa è nota a tutti - che il nuovo mezzo ha subito preso la mano e ne sono state intuite immediatamente le enormi possibilità, ma solo pochi, inizialmente, si sono posti interrogativi relativi alla sicurezza.

Ci si è, quindi, trovati di fronte a diversissime realtà, da efficientissimi centri d’elaborazione a Personal Computer (PC) che trattano informazioni di ogni tipo, classificate e non classificate, senza alcuna predisposizione di sicurezza. E’ da sottolineare che la prima, ed unica, norma sulla sicurezza informatica è costituita dalla direttiva PCM-A.N.S. 1/R/A edita nel 1985 a firma del Presidente del Consiglio dei Ministri e successivamente completamente revisionata nel 1993. Con questa direttiva si è cercato di dare ordine alla materia. La cennata direttiva non è perfetta, ma certamente fornisce delle linee guida, utili per l’adattamento di quei sistemi EAD già esistenti e per la corretta impostazione di quelli che stanno sorgendo in questi ultimi anni.. Come per i Centri Cifra anche per i Sistemi EAD, l’A.N.S., tramite l’UCSi, provvede a verificarne l’idoneità alla trattazione di informazioni coperte dal Segreto di Stato o di vietata divulgazione, mediante la loro “Certificazione ed Omologazione”:

- la **Certificazione** consiste nella valutazione tecnica, in base alla documentazione prodotta, delle misure previste per il sistema EAD ai fini di soddisfare i requisiti di sicurezza prescritti per il sistema stesso, tenuto conto della sua ubicazione fisica, del livello di classifica delle informazioni da elaborare, della modalità operativa del sistema, del profilo utenti e dell’installazione.
- la **Omologazione** consiste nella autorizzazione all’impiego operativo del sistema EAD, sulla base dei risultati della certificazione e delle condizioni operative ambientali (requisiti operativi e valutazione della minaccia e del rischio).

SCHEMA ITALIANO PER LA VALUTAZIONE E LA CERTIFICAZIONE DELLA SICUREZZA DELLA TECNOLOGIE DELL'INFORMAZIONE

Il riferimento per la valutazione di sicurezza dei prodotti e sistemi informatici è costituito attualmente in Europa dai criteri ITSEC e dal relativo manuale ITSEM, come risulta dalla recente pubblicazione sulla Gazzetta Ufficiale della Comunità Europea, del 26 aprile 1995, della raccomandazione 95/144/CE, con la quale il Consiglio dell'Unione Europea ha invitato tutti gli stati membri all'applicazione degli ITSEC.

Nell'agosto del 1995, per aderire a quanto richiesto dalla Raccomandazione della Comunità Europea del 7 aprile 1995 per l'adozione dei criteri ITSEC (Information Technology Security Evaluation Criteria) per la valutazione e certificazione dei sistemi e prodotti informatici l'ANS ha emanato le seguenti direttive che costituiscono lo "*schema nazionale*" per sistemi e reti in ambito difesa:

PCM-ANS TI-001

Procedura nazionale per l'omologazione di sistemi/reti EAD militari.

- La direttiva tecnica costituisce una guida per la definizione, in sede di formulazione delle specifiche, da parte del committente di sistemi EAD, dei requisiti di sicurezza del sistema da sviluppare, quale base per la successiva omologazione.
- Vengono pertanto individuati i vari tipi di requisiti di sicurezza, il ruolo che questi svolgono ai fini dello studio di fattibilità dei sistemi/reti dell'approvazione di sicurezza, dell'omologazione, della determinazione del ciclo di vita operativo dei sistemi EAD.

PCM-ANS TI-002

Standard di sicurezza per sistemi/reti EAD militari.

- La direttiva delinea le procedure per l'accertamento del rischio e della vulnerabilità residua dei sistemi informatici, espressa in forma numerica, mediante l'applicazione di formule matematiche. Viene così determinato il valore di garanzia del sistema da valutare in relazione al tipo di classifica delle informazioni trattate (SS, S, RR, R), del grado di rischio e della modalità operativa del sistema ("dedicato", "al più alto livello di classifica", "multilivello").
- In questa direttiva vengono pertanto individuate le risorse da proteggere, le minacce, la capacità offensiva dei potenziali aggressori, il grado di esposizione dei sistemi, la sensibilità e l'appetibilità dei dati, per la individuazione delle vulnerabilità e la scelta delle misure di sicurezza da adottare.

PCM-ANS TI-006

Disposizioni per l'omologazione di un centro di valutazione della sicurezza informatica di sistemi o prodotti destinati a gestire dati coperti dal segreto di Stato o di vietata divulgazione.

Nella direttiva vengono dettagliate le disposizioni relative a metodi e procedure per la omologazione di un centro di valutazione della sicurezza dei sistemi o prodotti informatici destinati alla trattazione di informazioni classificate.

PCM-ANS TI-007

Disposizioni per la valutazione, certificazione ed approvazione, ai fini della sicurezza informatica, di sistemi o prodotti destinati a gestire dati coperti dal segreto di Stato o di vietata divulgazione.

Vengono descritte le metodologie di valutazione, certificazione ed approvazione di un sistema o prodotto informatico destinato a gestire dati classificati.

La emanazione di queste direttive hanno consentito all'Italia di non essere esclusa da contratti internazionali, con perdita sia di "know how" sia economica, realizzando così le basi per ottenere la reciproca fiducia.

Attualmente lo schema è diretto a soddisfare le necessità del settore governativo e di quello industriale impegnato in progetti nazionali od internazionali che richiedano la tutela del segreto di Stato.

Per agevolare l'interpretazione delle direttive e le relative procedure di valutazione sono state redatte le seguenti guide:

- **Linee guida per l'applicazione dello schema nazionale per la valutazione della sicurezza delle tecnologie dell'informazione (approvata il 24 marzo 1998)** - definiscono, nel dettaglio, le interazioni tra i soggetti di valutazione/certificazione, alla luce delle esperienze sviluppate e delle esigenze palesate dagli utenti e forniscano un quadro di raccordo tra la documentazione richiesta secondo la filosofia ITSEC/ITSEM e quella relativa alla normativa nazionale, tenendo conto anche delle esigenze relative ai sistemi misti nazionale/NATO, che fanno riferimento anche a norme NATO;
- **Procedura per la condotta di valutazioni ai fini della sicurezza informatica di prodotti/sistemi EAD (approvata il 24 marzo 1998)** - definisce:
 - le responsabilità dell'EC, del CEVA, dell'Organismo richiedente, del Fornitore;
 - la descrizione dell'organizzazione delle attività pianificate dal CEVA;
 - le attività di monitoraggio e di controllo svolte dall'EC;
- **Manuale di valutazione di sicurezza informatica - Tecniche e Strumenti di Valutazione (TSV)** - contiene le linee guida di carattere tecnico su come espletare le azioni del valutatore specificate da ITSEC. Tale documento è

consistente con ITSEM ed approfondisce quegli aspetti che, sebbene già trattati in ITSEC/ITSEM, necessitano di ulteriori chiarimenti. E' da sottolineare che questo documento è diretto ai valutatori, ma risulta utile anche alle altre parti coinvolte nel processo di valutazione;

- **Piano di valutazione della sicurezza di un sistema informatico** - contiene la descrizione di tutte le attività che i valutatori di un CEVA devono eseguire per la valutazione di un prodotto/sistema e come esse sono organizzate, pianificate, correlate e suddivise nell'ambito del PDV. Attualmente sono state redatte sino al livello E3 :
 - SEZIONE 0 - PIANO DI VALUTAZIONE STANDARD E0;
 - SEZIONE 1 - PIANO DI VALUTAZIONE LIVELLO E1;
 - SEZIONE 2 - PIANO DI VALUTAZIONE LIVELLO E2;
 - SEZIONE 3 - PIANO DI VALUTAZIONE LIVELLO E3.

Queste ultime due guide non sono state soli CE.VA..

Inoltre, va sottolineato che i Requisiti di Sicurezza, così come descritti nello schema nazionale, consentono la redazione di documentazione ottemperante anche a quanto richiesto dalla normativa NATO.

Si sottolinea anche, che in ambito NATO è stata riconosciuta la validità dello Schema Nazionale italiano ed i Centri di Valutazione Italiani sono stati abilitati ad effettuare valutazioni su sistemi NATO.

L'11 aprile 2002 è stato firmato dal Presedente del Consiglio un nuovo schema italiano per la valutazione e certificazione della sicurezza delle tecnologie dell'informazione, che tiene conto anche dei nuovi criteri di valutazione internazionali ISO/IEC 15408, denominati anche Common Criteria. E sarà pubblicato come DPCM sulla Gazzetta Ufficiale. Tale schema è diretto a soddisfare le necessità del settore della Pubblica Amministrazione e di quello industriale coinvolti in progetti e lavorazioni che richiedono la trattazione di informazioni classificate.

ACCORDI DI MUTUO RICONOSCIMENTO DELLE VALUTAZIONI E CERTIFICAZIONI A LIVELLO EUROPEO E MONDIALE

In ambito Unione Europea l'ANS-UCSi, in qualità di Ente di Certificazione, è membro del *“Gruppo di Accordo per il Mutuo Riconoscimento”* delle valutazioni e certificazioni effettuate secondo i criteri europei ITSEC (Information Technology Evaluation Criteria), istituito dal SOGIS (Senior Officials Group Information Systems Security).

In tale ambito è stato sottoscritto un documento “ad hoc” che si prefigge lo scopo di determinare delle regole per le quali i sistemi od i prodotti provvisti di certificato di valutazione della sicurezza delle T.I. (Tecnologie dell'Informazione) emesso da un Paese membro, sia utilizzabile dagli altri Paesi senza il bisogno che questi vengano rivalutati e certificati, con piena fiducia sull'attendibilità del certificato emesso.

Il 23 maggio 2000 a Baltimora, nell'ambito della “1^a International Common Criteria Conference”, è stato sottoscritto da 16 paesi l' **“ARRANGEMENT on the Recognition of Common Criteria Certificates in the field of Information Technology Security”**. L'Italia, in tale occasione è stata rappresentata dall'ANS-UCSi in qualità di Ente di Certificazione nell'ambito della sicurezza delle informazioni classificate.