ISSN 1127-8579

Pubblicato dal 28/01/2010

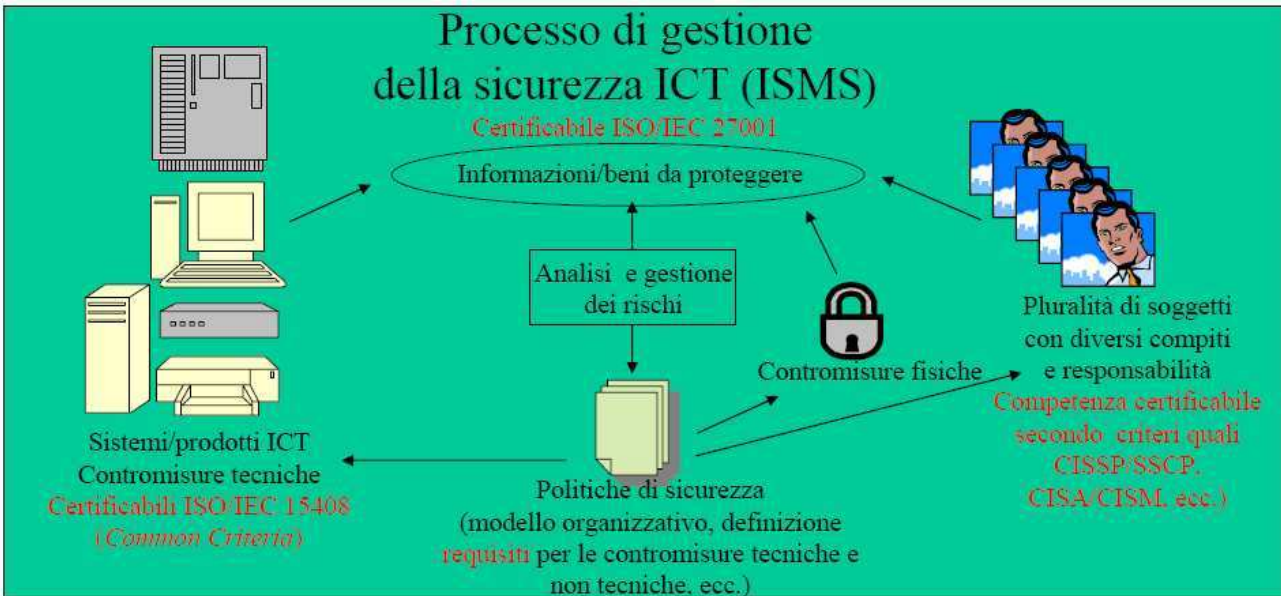
All'indirizzo http://www.diritto.it/docs/28862-l-esame-dei-tipi-di-certificazione-della-sicurezza-che-utilizzano-come-norma-di-riferimento-uno-standard-iso-iec-e-le-differenze-dei-rispettivi-schemi-di-certificazione

Autore: Guzzo Antonio

L’esame dei tipi di certificazione della sicurezza che utilizzano come norma di riferimento uno standard ISO/IEC e le differenze dei rispettivi schemi di certificazione

L’esame dei tipi di certificazione della sicurezza che utilizzano come norma di riferimento uno standard ISO/IEC e le differenze dei rispettivi schemi di certificazione. (a cura del Dottor Antonio Guzzo – Responsabile CED – Sistemi Informativi del Comune di Praia a Mare)

I principali tipi di certificazione della sicurezza ICT che utilizzano come norma di riferimento uno standard ISO/IEC sono la ISO/IEC IS 27001 (BS7799) e ISO/IEC IS 15408 (Common Criteria). In particolare si farà riferimento a due principali tipi di schemi di certificazione che sono ISO/IEC IS 27001 (BS7799) e ISO/IEC IS 15408 (Common Criteria). Per poter esaminare gli schemi di certificazione della sicurezza ict è necessario applicarli al processo intorno al quale ruota la sicurezza ict che è quello dell’analisi dei rischi. Deve essere eseguito all’interno di un organizzazione (azienda, pa, etc) ma viene fuori il problema di come delegare lo svolgimento di questo processo nella struttura aziendale (individuazione di compiti, responsabilità, etc). Tutto l’insieme di queste previsioni, definizioni costituisce quello che nello standard ISO IEC 27001 (BS7799) prende il nome di ISMS (International Standard Management Security cioè il sistema di gestione della sicurezza informatica all’interno di un organizzazione). Questo sistema (ISMS) coinvolge un po’ tutto, le informazioni ed i beni da proteggere, il processo di analisi e gestione dei rischi, i soggetti che devono interagire con le informazioni ed i beni da proteggere, i documenti cartacei che definiscono politiche di sicurezza, modelli organizzativi all’interno dell’organizzazione e coinvolge infine i sistemi dei prodotti ict. Li coinvolge però in modo non dettagliato, in quanto non è scopo di questo standard verificare quanto questi oggetti siano robusti dal punto di vista della sicurezza ma tutto al più dare delle indicazioni sulle modalità di utilizzo, etc. Per cui quando parliamo di standard ISO IEC 27001 (BS7799) ci riferiamo al rettangolo verde della successiva figura però ad un livello di generalità abbastanza alto proprio per poter abbracciare tutto.



Invece quando ci riferiamo ad altri tipi di certificazioni ICT che sono i criteri a sinistra (certificabili ISO/IEC 15408 Common Criteria) e a destra (CISP/SSCP, CISA/CISM) qui cambia l’oggetto della certificazione non è più tutto il sistema di gestione della sicurezza come nel caso delle ISO/IEC 27001 vista in precedenza ma in un caso (ISO/IEC 15408 Common Criteria) l’oggetto della certificazione cambia e si basa specificamente sui sistemi ed i prodotti ICT e cioè la sicurezza che possono offrire questi oggetti ICT, nell’altro caso (CISSP/SSCP, CISA/CISM) l’oggetto della

certificazione è rappresentato dalla competenza dei soggetti che operano nel settore della sicurezza ICT (personale). Purtroppo in quest'ultimo caso non esiste un vero e proprio standard però ci sono dei criteri che godono di un buon riconoscimento internazionale (CISSP/SSCP, CISA/CISM). ***Quindi le differenze fra gli schemi di certificazione appena esaminati sono meglio riassunti nella seguente tabella:***

Oggetto certificato	Norme di riferimento
Processo di gestione della sicurezza ICT (ISMS)	ISO/IEC 27001
Sistema/prodotto ICT	ISO/IEC 15408 (*Common Criteria*) ITSEC
Competenza del personale	CISSP/SSCP, CISA/CISM, ecc.

Passiamo ora ad esaminare i cosiddetti schemi di certificazione cioè le strutture che vengono messe in piedi per fornire questo sistema di certificazione. Esistono infatti delle differenze sensibili dei due tipi di certificazione (ISO/IEC 27001 e ISO/IEC 15408) negli schemi di certificazione che essi adottano. La differenza sensibile che esiste tra i due schemi sta nel fatto che a seconda dei due casi si considera, vengono inglobate due funzioni associate ad un unico soggetto. In generale, potremmo distinguere dal punto di vista delle funzioni svolte tre soggetti che principalmente fanno parte strettamente dello schema di certificazione mentre esistono altri soggetti esterni (quelli che interagiscono con lo schema di certificazione) che sono il fornitore/titolare dell'oggetto da certificare ed il fruitore dei servizi forniti dall'oggetto certificato (l'utente finale). I tre soggetti sono costituti dalla figura del valutatore, del certificatore e dell'accreditatore. Per accreditatore si intende il soggetto che in qualche modo approva, abilita all'interno dello schema di certificazione gli altri due soggetti (il valutatore ed il certificatore). Per valutatore si intende quel soggetto che direttamente va ad utilizzare la norma di riferimento (ISO/IEC 27001 e/o ISO/IEC 15408) la applica all'oggetto da certificare e verifica se questo oggetto soddisfa i requisiti previsti dalla norma, successivamente il risultato di queste verifiche le trasmette ad un altro soggetto, il certificatore il quale potrà eventualmente interagire con il valutatore, nei casi in cui ciò è previsto, ed una volta che anche il certificatore abbia trovato che tutti i requisiti sono soddisfatti procederà all'emissione del certificato. In questo esame appena effettuato abbiamo considerato questi soggetti come se fossero tutti e tre distinti, in realtà non è cosi e per quanto concerne lo schema di certificazione ISO/IEC 27001 i due ruoli uniti sono quelli relativi al rettangolo orizzontale della figura (valutatore e certificatore) mentre per quanto concerne lo schema di certificazione ISO/IEC 15408 i due ruoli sono quelli relativi al rettangolo verticale (accreditatore e certificatore). Questo indica che quando parliamo di certificazioni ISO 27001 c'è un unico soggetto accreditatore che in questo caso è il SINCERT che accredita un soggetto che svolge contemporaneamente le funzioni di valutatore e certificatore e dal momento che svolge anche la funzione di certificatore può emettere in autonomia i certificati. Viceversa nel caso dell'altro schema ISO/IEC 15408 vi è un unico soggetto che svolge congiuntamente le funzioni di accreditatore e certificatore (in questo caso l'accreditamento la svolge solo in riferimento a quest'altro soggetto) e vi sono una pluralità di valutatori. Il certificatore è sempre unico e deve essere approvato dall'OCSI (Organismo di Certificazione/Accreditamento). Questa caratteristica non è casuale ed è fondamentale per aver distinto questi due standard sono proprio alcuni questi elementi ad aver portato schemi di

certificazioni di questo tipo. Nel caso dei common criteria vi è stata l'intenzione di cercare di privilegiare la sua applicabilità a prodotti e sistemi ict di tipo anche molto diverso. Questa intenzione di applicabilità ha fatto si che lo standard stesso sia stato reso meno dettagliato proprio per non pregiudicare l'applicabilità ad altri tipi di prodotti e sistemi ict. Questo ha avuto come contropartita il fatto che mancando questo dettaglio spinto sulle modalità di applicazione dello standard occorre supplire con una funzione centralizzata di coordinamento svolta dal certificatore unico che deve garantire che lo standard venga applicata in modo uniforme da tutti i laboratori di valutazione. Cosi facendo si prevede che per ogni singola certificazione ci sia una revisione tecnica del certificatore unico che approvi o meno il lavoro svolto dal laboratorio di valutazione. Nel caso della certificazione ISO/IEC 27001 non c'era questa esigenza di mantenere un pò a livello elevato dal punto di vista delle generalità le indicazioni fornite dallo standard per aumentare l'applicabilità dello standard all'interno del contesto. Si è potuto dare delle indicazioni molto precise nello standard ed una volta eseguita l'accreditamento iniziale di questa figura unica che svolge le funzioni sia di valutatore che di certificatore, non è necessario su ogni processo di certificazione che si vada a controllare come ha operato questo soggetto accreditato. Si veda in dettaglio la seguente figura.