

Quaderni Clusit

500

**Implementazione e
certificazione dei
sistemi di gestione
per la sicurezza
delle informazioni**

Fabrizio Cirilli

Implementazione e certificazione dei sistemi di gestione per la sicurezza delle informazioni

Fabrizio Cirilli

Comitato Tecnico Scientifico



Quaderni CLUSIT – Febbraio 2007

CLUSIT

Il CLUSIT - Associazione Italiana per la Sicurezza Informatica, è una associazione "no profit" con sede presso l'Università degli studi di Milano, Dipartimento di Informatica e Comunicazione, fondata nel luglio 2000.

Le principali attività del CLUSIT sono:

- la diffusione di una cultura della sicurezza informatica rivolta alle Aziende, alla Pubblica Amministrazione ed ai cittadini;
- l'elaborazione sia a livello comunitario che italiano di leggi, norme e regolamenti che coinvolgono la sicurezza informatica;
- la definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza ICT;
- la promozione dell'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

I soci del CLUSIT sono rappresentativi dell'intero "sistema Paese", in particolare della ricerca, dell'industria, del commercio, del settore bancario ed assicurativo, della Pubblica Amministrazione, della Sanità, dei servizi, delle telecomunicazioni e di Internet.

Copyright e Disclaimer

Copyright © 2007 Fabrizio Cirilli

Copyright © 2005-2007 CLUSIT

Tutti i diritti sull'Opera sono riservati all'Autore e al Clusit.

Sono tuttavia attribuiti i seguenti diritti:

1. I Soci Clusit fruitori dell'Opera hanno il diritto di utilizzare l'Opera nell'ambito della propria attività professionale purchè: a) riconoscano la paternità dell'Opera in capo all'Autore e al Clusit; b) non la utilizzino per scopi commerciali; c) non creino opere derivate e/o alterino l'Opera e/o la trasformino e/o la sviluppino.
2. I diritti attribuiti ai Soci Clusit sopra riportati sono estesi a tutti i fruitori dell'Opera dopo che la stessa sarà rilasciata in forma elettronica sul sito www.clusit.it in area pubblica.

Gli Autori e il Clusit non garantiscono che l'Opera sia esente da errori. Qualora vengano segnalati errori, nel limite del possibile si provvederà a correggerli nelle eventuali edizioni successive.

Gli Autori e il Clusit non assumono alcuna responsabilità in relazione al contenuto dell'Opera e/o ai risultati attesi e/o ai risultati conseguenti all'uso della stessa e, pertanto, non risponderanno di eventuali e qualsivoglia danni diretti e/o indiretti che dovessero derivarne.

In particolare non viene garantito che il contenuto dell'Opera sia esauriente, completo, preciso o aggiornato.

Il contenuto dell'Opera non costituisce un parere di tipo professionale o legale.

Eventuali denominazioni di prodotti e/o aziende e/o i loghi e/o i marchi e/o i segni distintivi eventualmente citati nell'Opera sono di esclusiva proprietà dei rispettivi titolari.

Presentazione

In questi ultimi dieci anni il settore della sicurezza delle informazioni e dei sistemi è stato caratterizzato da un flusso continuo di evoluzioni e miglioramenti, che hanno contraddistinto tutte le diverse componenti della disciplina, quella tecnologica e quella organizzativa e di processo.

Dal punto di vista tecnologico sistemi di prevenzione e rilevamento sempre più precisi e sofisticati, accompagnati da un costante miglioramento della qualità del codice hanno contribuito ad accrescere sensibilmente la robustezza dei sistemi alle intrusioni. Certo la strada da percorrere è ancora lunga, ma credo che nessuno possa negare che oggi un sistema informatico aggiornato con le ultime patch ed opportunamente protetto da firewall e IDS, è di gran lunga molto più difficile da attaccare di quanto non lo fosse una decina di anni fa.

Un ruolo importante in questo processo evolutivo è stato svolto anche dai progressi fatti nel settore della governance della Sicurezza. Poco meno di dieci anni fa la documentazione a disposizione di una qualunque organizzazione che volesse affrontare sistematicamente questo problema, la cui complessità è spesso sottostimata, non aveva altra fonte disponibile che il famoso BS7799:1, uno standard britannico costituito da una raccolta di buone pratiche su come amministrare la sicurezza in azienda. Con l'andare del tempo e con l'affermarsi della Società dell'Informazione quelli che oramai sono diventati i Sistemi di Gestione per la Sicurezza delle Informazioni (o SGSI) hanno assunto un rilievo sempre maggiore, e oggi disponiamo di due corposi standard ISO (ISO/IEC 17799:05 e ISO 27001:05) legati alla realizzazione e certificazione di SGSI. Altri standard "di processo" sono all'orizzonte.

Ad onor del vero il processo che ha portato dallo standard britannico BS7799 agli standard ISO è stato un po' caotico, inizialmente solo la componente BS7799:1 dello standard è stata adottata come ISO 17799:2000, successivamente la stessa è stata rivista (ISO 17799:2005) e affiancata dallo standard ISO 27001:05 che costituisce a sua volta una revisione della versione più aggiornata di BS7799:2. Ovviamente non è facile districarsi in tutti questi standard e soprattutto riuscire a cogliere gli aspetti salienti che li differenziano, per contro è estremamente importate per chiunque voglia seriamente occuparsi di sicurezza ICT in ambito aziendale cogliere appieno questi aspetti.

Per far fronte a questa esigenza il CLUSIT ha deciso di affidare a Fabrizio Cirilli, presidente del capitolo italiano del Information Security Management System International User Group, un autore sicuramente tra i più rappresentativi in tema di SGSI nel nostro paese, il compito di predisporre un documento che consentisse di avere un panorama sui diversi processi di standardizzazione in corso presso l'ISO in materia di sicurezza informatica, e di avere una breve panoramica sulle diverse tematiche trattate dagli standard già approvati, sottolineandone aspetti unificanti e non.

Il risultato ottenuto è questa guida dedicata agli addetti ai lavori, estremamente chiara nell'esposizione e di facile lettura. Direi che il pregio principale di questo lavoro, oltre a cogliere appieno gli obiettivi prefissati, è quello di fornire al lettore gli elementi necessari per leggere in modo critico il contenuto degli standard ed apprezzare il significato intrinseco del processo di certificazione proposto. A questo proposito mi sembra importante richiamare due paragrafi del manoscritto che possono fornire al lettore, in estrema sintesi, il tipo di contenuto

che potrà trovare all'interno dello stesso. Ad esempio, in relazione ai contenuti da ricercarsi all'interno degli standard analizzati l'autore ribadisce con estrema chiarezza:

“... lo standard costituisce un modello organizzativo piuttosto che uno standard tecnico. Non vi troveremo quindi il come fare ma solo il cosa fare in materia di gestione della sicurezza delle informazioni. Ogni organizzazione trova nello standard un riferimento per organizzare la propria sicurezza delle informazioni e non le soluzioni migliori o più innovative. Questa è nel contempo la forza ed il limite di ciascun standard ISO.”

Ancora più preciso è l'inquadramento che si fornisce del processo di certificazione e del suo valore:

“L'audit di certificazione consente al team di audit dell'OdC di valutare la conformità (e l'efficacia) del SGSI dell'organizzazione. E' importante ricordare che gli audit degli OdC si svolgono “a campione”, cioè le valutazioni si riferiscono solamente alle parti di SGSI verificate direttamente e che, pertanto, la valutazione non è da considerarsi esaustiva o affidabilistica¹. Come si dice “l'audit dà confidenza che il SGSI sia conforme ed efficace nel campione esaminato” e non vi è presunzione di affidabilità nella valutazione eseguita². Forse è questo il tallone d'Achille del sistema di certificazione ma dobbiamo anche ricordare che si tratta pur sempre e comunque di un processo volontario a fronte di uno standard “gestionale” e non tecnologico. L'esaustività della valutazione non solo comporterebbe costi rilevanti ma soprattutto condurrebbe alla “clonazione” dei SGSI con ovvio irrigidimento organizzativo e tecnico delle soluzioni ed interpretazioni della norma stessa.”

In conclusione, ci troviamo di fronte ad un testo sintetico e alla portata di chiunque abbia un decoroso bagaglio di nozioni in materia. Un testo che non si limita a elencare e descrivere i contenuti dei diversi standard legati alla realizzazione di un SGSI, come il titolo potrebbe suggerire, ma entra nel merito degli stessi fornendone una chiave di lettura ed interpretazione. Un testo che va nella direzione di dare il giusto peso agli sforzi compiuti in sede di standardizzazione evitando toni trionfalistici, e la diffusione di miscredenze o cattive interpretazioni, spesso alimentate da improvvisatori dell'ultima ora, che a lungo andare non possono che nuocere all'intero comparto della Sicurezza ICT.

*Prof. Danilo Bruschi
Presidente del
Comitato Tecnico-Scientifico Clusit*

¹ Il concetto di campionamento si riferisce a documenti, registrazione e/o interviste rilevate durante l'audit.

² Le attività di audit per i SGSI si svolgono secondo quanto indicato da: UNI EN ISO 19011:03, ISO 27006 (dal 2007), EA 7/03 e dai documenti tecnici SINCERT.

Abstract

Breve excursus nel mondo della certificazione dei Sistemi di Gestione per la sicurezza delle informazioni e delle norme della famiglia ISO 27000.

Il primo capitolo introduce l'argomento della sicurezza delle informazioni con una rapida analisi del mercato seguita da una breve storia sulla normazione relativa e dal richiamo ai principi ispiratori, delineando così lo scenario di base per una corretta comprensione dei capitoli successivi.

Il secondo capitolo analizza in dettaglio la struttura ed i contenuti della norma. Ciascun argomento è trattato in modo pragmatico individuando le richieste della norma ed i relativi documenti da produrre.

Il terzo capitolo descrive il contenuto ed il significato della ISO/IEC 17799:05 analizzando il collegamento alla ISO/IEC 27001:05.

Il capitolo quattro schematizza il corollario delle norme della famiglia ISO 27000 in fase di pubblicazione.

Il capitolo cinque permette una rapida comprensione delle differenze esistenti tra BS7799-2:02 e ISO/IEC 27001:05 , questo capitolo è di particolare interesse per tutte le organizzazioni che si trovano a dover convertire la propria certificazione entro il 31/3/2007.

I capitoli sei e sette introducono il lettore nel mondo della certificazione dei sistemi ed in particolare dei Sistemi per la Gestione per la Sicurezza delle Informazioni, ponendo l'enfasi sugli aspetti operativi e cercando, nel contempo, di sfatare "miti e leggende" della certificazione.

Il capitolo otto affronta invece il complesso aspetto dell'accreditamento fornendo al lettore gli strumenti per orientarsi nel vasto mondo delle certificazioni dei SGSI e dell'accreditamento degli Organismi di Certificazione.

I capitoli nove e dieci sono di particolare utilità per le organizzazioni che devono affrontare o completare il percorso conversione della propria certificazione verso la ISO/IEC 27001:05 . In particolare il capitolo dieci suggerisce un pratico approccio per guidare il lettore verso l'obiettivo finale.

Infine il capitolo 11 presenta il capitolo italiano del gruppo utenti internazionali della ISO/IEC 27001:05 ed i legami esistenti tra l'associazione e lo sviluppo della norma a livello internazionale e nazionale.

L'autore

Fabrizio Cirilli

Consulente e auditor dei sistemi di gestione per la sicurezza delle informazioni, docente presso il Master di II livello dell'Università La Sapienza di Roma Dipartimento di Informatica (Direttore Prof. L.V.Mancini) , progettista e docente di corsi nazionali ed internazionali per la qualifica degli auditor ISO 27001, lead auditor certificato IRCA e RICEC, membro del comitato ISO JTC1/SC27/WG1 per le norme della famiglia ISO 27000 e membro della task force ISO/IAF per la ISO 27006. Attualmente collabora con organismi di certificazione ed aziende in ambito nazionale ed internazionale sui temi della sicurezza delle informazioni, della qualità dei servizi e dei processi dell'ICT. Socio CLUSIT, AIEA-ISACA e IEEE. Chairman del capitolo italiano degli utilizzatori della ISO 27001 ISMS IUG ITALY

SOMMARIO

1. INTRODUZIONE	9
1.1. IL MERCATO DI RIFERIMENTO	9
1.2. BREVI CENNI SUL CONTENUTO DELLO STANDARD	9
1.3. LA STORIA DELLA ISO/IEC 27001:05	10
1.4. PRINCIPI ISPIRATORI DELLO STANDARD	11
1.5. IL CICLO PLAN-DO-CHECK-ACT	13
2. LA ISO/IEC 27001:05	14
2.1. OBIETTIVI DELLO STANDARD	14
2.2. SPECIFICITÀ DELLO STANDARD	14
2.3. STRUTTURA	14
2.4. INTRODUZIONE AI REQUISITI DELLO STANDARD	15
2.5. ANALISI DEI REQUISITI – PDCA	15
2.6. ANALISI DEI REQUISITI – DOCUMENTAZIONE	16
2.7. DOCUMENTAZIONE OBBLIGATORIA	17
2.8. ASPETTI SPECIFICI DEI REQUISITI 4.2 E 4.3	17
2.9. ANALISI DEI REQUISITI – 5 RESPONSABILITÀ DELLA DIREZIONE	17
2.10. ANALISI DEI REQUISITI – 6 AUDIT INTERNI	18
2.11. ANALISI DEI REQUISITI – 7 RIESAME DELLA DIREZIONE	18
2.12. ANALISI DEI REQUISITI – 8 MIGLIORAMENTO DEL SGSI	19
2.13. L'ALLEGATO A – I CONTROLLI	19
2.14. L'ALLEGATO B – L'INTEGRAZIONE PRINCIPI-PDCA-REQUISITI	20
3. COSA È ED A COSA SERVE LA ISO/IEC 17799:05	21
3.1. OBIETTIVO	21
3.2. STRUTTURA	22
3.3. ALTERNATIVE	23
4. LE ALTRE NORME DELLA FAMIGLIA ISO 27000	24
4.1. PROSSIME SCADENZE	24
5. COSA CAMBIA RISPETTO ALLA BS7799-2:02	25
5.1. LE INNOVAZIONI	25
5.2. LE DIFFERENZE	25
5.3. LA MISURABILITÀ	25
6. LA CERTIFICAZIONE DEI SGSI	27
6.1. OBIETTIVO	27
6.2. SIGNIFICATO	27
6.3. VALENZA	28
6.4. EFFICACIA VS CONFORMITÀ	28
7. COME CERTIFICARSI ISO/IEC 27001:05	29
7.1. I PASSI DA FARE PER IMPLEMENTARE IL SGSI	29
7.1.1. <i>Campo di applicazione</i>	29
7.1.2. <i>Ampiezza</i>	30
7.1.3. <i>Politica</i>	30
7.1.4. <i>Analisi e valutazione dei rischi</i>	30
7.1.5. <i>Dichiarazione di applicabilità</i>	30
7.1.6. <i>La scelta dei controlli</i>	31
7.2. I PASSI PER IDENTIFICARE E SCEGLIERE L'ORGANISMO DI CERTIFICAZIONE (ODC)	31

7.3.	AUDIT PRELIMINARE	31
7.4.	IL PROCESSO DI CERTIFICAZIONE.....	32
7.4.1.	<i>Quanto può durare un audit</i>	32
7.4.2.	<i>Fase 1 (o audit documentale)</i>	34
7.4.3.	<i>Fase 2 (o audit di certificazione)</i>	34
7.5.	SORVEGLIANZA E RINNOVO.....	35
7.6.	VALENZA DEGLI AUDIT.....	36
8.	LA CERTIFICAZIONE ACCREDITATA	37
8.1.	PERCHÉ ACCREDITATA.....	37
8.2.	CHI ACCREDITA.....	38
8.2.1.	<i>SINCERT</i>	38
8.2.2.	<i>EA</i>	39
8.2.3.	<i>IAF</i>	40
8.3.	COME ACCREDITA.....	40
8.4.	IL MULTI LATERAL AGREEMENT EUROPEO.....	41
8.5.	IL MULTI RECOGNITION ARRANGMENT MONDIALE	41
9.	IL PERIODO DI TRANSIZIONE.....	42
9.1.	QUANDO SCADE LA BS7799-2:02	42
10.	COME CONVERTIRE I CERTIFICATI DA BS7799-2:02 A ISO/IEC 27001:05.....	43
10.1.	CONVERTIRE IL SGSI ALLA NUOVA NORMA.....	43
10.2.	CONVERTIRE IL CERTIFICATO	44
11.	IL GRUPPO UTENTI INTERNAZIONALI (ISMS IUG).....	45
11.1.	RUOLO DEL ISMS IUG ITALY NEL COMITATO ISO JTC1/SC 27/WG 1	45

CLUSIT

Associazione Italiana per la Sicurezza Informatica

Sede legale presso:

Dipartimento di Informatica e Comunicazione

Università degli Studi di Milano

Via Comelico 39 - 20135 MILANO

www.clusit.it – info@clusit.it

tel. 347 23 19 285