Ministero delle Comunicazioni

iscom

CERTIFICAZIONE DELLA SICUREZZA ICT

Linee Guida iscom

La certificazione della sicurezza ICT

Il presente documento è stato realizzato da (in ordine alfabetico):

Giovanni ABBADESSA	(IBM)
Paolo AGNOLI	(ELECOM scrl)
Stefano AMICI	(ENAV)
Silvano BARI	(ALITALIA, AIEA)
Giannicola BELCASTRO	(GRTN)
Michele BIANCO	(Bull, AIEA)
Riccardo BIANCONI	(SINCERT)
Isabella BRIZI	(SECURTEAM - ELSAG)
Fabio BRUSCHI	(APC)
Stefania CAPORALINI-AJELLO	(DATAMAT)
Bruno CARBONE	(ENAV)
Giuseppe CONCORDIA	(Min. econ. e finanze - Dip.per le politiche fiscali)
Marcella DI DOMENICO	(Siemens Informatica)
Luisa FRANCHINA	(ISCOM Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione)
Massimo GALBIATI	(APC)
Francesco GENTILE	(OIS)
Franco GOLA	(CSI Piemonte)
Alessandro LORENZINI	(Systimax by Commscope)
Mariano LUPO	(Min. econ. e finanze - Dip. per le politiche fiscali)
Paolino MADOTTO	(Progesoftware)
Gianluca MORSANIGA	(CSI)
Omar OCCHIPINTI	(Agenzia Entrate)
Ombretta PALMA	(Siemens Informatica)
Daniele PERUCCHINI	(Fondazione Ugo Bordoni)
Armando PERUGINI	(Seprotec)
Enrico POZZA	(Progesoftware)
Federico SANDRUCCI	(Seprotec)
Roberto SETOLA	(Presidenza Cons. Min. - Dip. per l'Innovazione e le Tecnologie & Università Campus Bio-Medico-Roma)
Mauro SARTI	(Anixter)
Franco SORESINA	(Vanguard)
Emiliano TAGLIAVINI	(Securteam - ELSAG)
Alfredo VALENZA	(Oracle)
Raffaele VISCIANO	(Min. econ. e finanze - Dip. per le politiche fiscali)
Francesco PICCOLO	(ELECOM SCSI)

Per le parti specificatamente relative alla certificazione Common Criteria e all'OCSI, hanno contribuito:

Marco CARBONELLI	(ISCOM)
Giacinto DAMMICCO	(ISCOM)
Giovanni DESIRÒ	(ISCOM)
Laura GRATTA	(ISCOM)
Franco GUIDA	(Fondazione Ugo Bordoni)

Copertina e Progetto Grafico
Roberto Piraino (Graphics Lab - Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione)

Le opinioni e le considerazioni espresse in questo volume, nonchè le proposte avanzate, sono da considerarsi come personali dei singoli partecipanti e non riflettono necessariamente la posizione dei rispettivi Enti e Società d'appartenenza.
Il contenuto del presente volume è da considerarsi unicamente come studio tecnico/scientifico orientativo delle problematiche inerenti la sicurezza delle reti e la tutela delle comunicazioni.
Pertanto nessuna responsabilità potrà essere attribuita agli autori o all'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, che cura questa pubblicazione, per ogni eventuale conseguenza derivante da qualsivoglia utilizzo dei contenuti del presente testo.

Le citazioni di specifici marchi o nomi di prodotti presenti nel documento sono riportati a mero scopo esemplificativo, non esauriscono il novero di prodotti esistenti sul mercato e in nessun caso costituiscono elemento di valutazione o di raccomandazione per l'utilizzo dei prodotti stessi.

Indice

CERTIFICAZIONE DELLA SICUREZZA ICT

Introduzione

La presente pubblicazione si inquadra in una serie di attività svolte da un gruppo di esperti volontari appartenenti al settore pubblico e privato nel 2005 e relative alla realizzazione di linee guida su:

Gestione delle emergenze locali

Risk analysis approfondimenti

Qualità del servizio su UMTS

Qualità dei servizi per le PMI su reti fisse a larga banda

Outsourcing e sicurezza

Certificazione della sicurezza ICT

Si coglie volentieri l'occasione per ringraziare quanti hanno, con entusiasmo e professionalità, collaborato alla redazione del presente documento:

Giovanni ABBADESSA (IBM), Paolo AGNOLI (ELECOM scrl), Stefano AMICI (ENAV), Silvano BARI (ALITALIA, AIEA), Giannicola BELCASTRO (GRTN), Michele BIANCO (Bull, AIEA), Riccardo BIANCONI (SINCERT), Isabella BRIZI (SECURTEAM - ELSAG), Fabio BRUSCHI (APC), Stefania CAPORALINI-AJELLO (DATAMAT), Bruno CARBONE (ENAV), Giuseppe CONCORDIA (Min. econ. e finanze - Dip.per le politiche fisc.), Marcella DI DOMENICO (Siemens Informatica) Massimo GALBIATI (APC), Francesco GENTILE (OIS), Franco GOLA (CSI Piemonte), Alessandro LORENZINI (Systimax by Commscope), Mariano LUPO (Min. econ. e finanze - Dip. per le politiche fiscali), Paolino MADOTTO (Progesoftware), Gianluca MORSANIGA (CSI), Ombretta PALMA (Siemens Informatica), Omar OCCHIPINTI (Agenzia Entrate), Daniele PERUCCHINI (Fondazione Ugo Bordoni), Armando PERUGINI (Seprotec), Enrico POZZA (Progesoftware), Federico SANDRUCCI (Seprotec), Roberto SETOLA (Presidenza Cons. Min. - Dip per l'innovazione e le Tecnologie & Università Campus Bio -Medico- Roma), Mauro SARTI (Anixter), Franco SORESINA (Vanguard), Emiliano TAGLIAVINI (Securteam-ELSAG), Alfredo VALENZA (Oracle), Raffaele VISCIANO (Min. econ. e finanze - Dip. per le politiche fiscali), Francesco PICCOLO (ELECOM SCSI)

Per le parti specificatamente relative alla certificazione Common Criteria e all'OCSI, hanno contribuito:
Marco CARBONELLI (ISCOM), Giacinto DAMMICCO (ISCOM), Giovanni DESIRÒ (ISCOM), Laura GRATTA (ISCOM), Franco GUIDA (Fondazione Ugo Bordoni).

Roma, luglio 2006

Il Direttore
dell'Istituto Superiore delle Comunicazioni
e delle Tecnologie dell'Informazione

Ing. Luisa Franchina

Guida alla lettura

Questo documento rappresenta la sintesi del lavoro svolto dal gruppo "Infrastrutture Critiche" cui hanno partecipato esponenti delle diverse istituzioni pubbliche insieme con rappresentanti dei principali operatori di infrastrutture critiche operanti in Italia e di società impegnate nel settore della sicurezza delle reti di telecomunicazioni.

Il gruppo di lavoro nasceva dalla necessità di analizzare le implicazioni sulla continuità di esercizio e sulla sicurezza delle infrastrutture critiche rispetto al mutato contesto socio-economico e tecnologico che ha visto crescere l'importanza e la crucialità delle infrastrutture di telecomunicazione nei confronti di tutte le infrastrutture critiche nazionali. Questo si riflette in un crescente livello di interdipendenza fra le diverse infrastrutture, in gran parte dovuto alla diffusione delle tecnologie ICT. Inoltre occorre rilevare un aumento delle minacce che affliggono le infrastrutture sia legate a fenomeni naturali che ad azioni delittuose, ed in special modo terroristiche.

Queste motivazioni, come illustrato nel primo capitolo, hanno portato alla nascita di specifiche iniziative, sia a livello Nazionale che Europeo, tese ad innalzare il livello globale di sicurezza delle infrastrutture critiche e che genericamente sono indicate come strategie di Protezione delle Infrastrutture Critiche.

Il successivo capitolo delinea il nuovo scenario architetturale che caratterizza le infrastrutturale nazionali evidenziando gli elementi di interdipendenza e le minacce che affliggono gli elementi da considerare per una corretta gestione degli aspetti di sicurezza e continuità di servizio di tali infrastrutture.

Il capitolo terzo analizza in maggior dettaglio, in un ottica di Best Practice o Buone Regole, gli aspetti connessi con la necessità di proteggere le reti di comunicazione, non solo per la loro importanza intrinseca, ma perché il loro corretto funzionamento è indispensabile per garantire che le altre infrastrutture critiche eroghino i propri servizi.

In quest'ottica vengono analizzati gli aspetti peculiari che caratterizzano le reti di comunicazione che sono utilizzate per il supporto delle infrastrutture critiche nazionali evidenziando l'importanza delle diverse componenti che costituiscono queste infrastrutture di comunicazione. Un paragrafo specifico è dedicato agli aspetti di certificazione della sicurezza e alla sua importanza per aumentare la fiducia degli utenti sui livelli di sicurezza garantibili.

La sicurezza d queste infrastrutture non può ricondursi, ovviamente a meri aspetti tecnologici (che pure rivestono un ruolo non trascurabile), ma occorre prevedere un'opportuna organizzazione in grado di gestire efficacemente ed efficientemente le situazioni di crisi ed un'adeguata formazione di tutto il personale coinvolto a vario titolo nella gestione ed utilizzo di queste infrastrutture.

Esistono, inoltre, diverse attività di R&S tese ad individuare soluzioni tecnologiche che possono meglio adattarsi al mutato contesto infrastrutturale.

Il capitolo quattro riporta le principali conclusioni del lavoro svolto.

Completano il volume alcune appendici di cui una dedicata ai diversi standard di riferimento ed ai riferimenti normativi, una seconda nella quale sono descritte in dettaglio le linee guida che hanno portato alla stesura di un business continuity plan di un importante operatore di infrastrutture critiche ed, infine, un questionario di auto valutazione che può essere di ausilio ai responsabili delle diverse infrastrutture per effettuare una prima analisi del proprio livello di sicurezza rispetto a vulnerabilità connesse con l'utilizzo di infrastrutture di telecomunicazione.

CERTIFICAZIONE DELLA SICUREZZA ICT

1 - La certificazione di sicurezza

Il termine "certificazione di sicurezza" è attualmente utilizzato in molti contesti diversi e con significati che, a volte, sono addirittura incompatibili tra loro. Per questo motivo è importante definire correttamente il significato del termine "certificazione di terza parte" (nel seguito semplicemente "certificazione"), così come verrà utilizzato nel resto del documento.

Innanzitutto, la certificazione di sicurezza è, in generale, un processo composito in cui agiscono, normalmente, vari soggetti e in cui sono definite alcune regole. I ruoli più importanti eventualmente coinvolti in un processo di certificazione sono:

- La Norma di riferimento;
- Lo Schema di certificazione, che descrive le regole che governano il processo di applicazione della norma di riferimento;
- il Gestore dello schema, che garantisce tutti gli altri soggetti rispetto alla corretta applicazione delle regole stabilite dallo Schema stesso e negozia eventuali accordi di mutuo riconoscimento con i gestori di schemi analoghi in altri Paesi;
- Il Garante dello Schema che dirime eventuali controversie che coinvolgono il Gestore dello Schema;
- il Certificatore, che rilascia i certificati di sicurezza sulla base dei risultati delle verifiche tecniche condotte da Valutatori accreditati (laboratori di verifica o ispettori) e vigila sulla corretta gestione dei certificati;
- il Valutatore (Laboratorio di verifica o Ispettori), che ese-

gue la valutazione di sicurezza e costituisce il braccio operativo del Certificatore;
- l'ente Accreditatore, che si occupa dell'accreditamento iniziale dei Certificatori e/o dei Valutatori (laboratori di verifica / ispettori), così come del controllo periodico del mantenimento dei requisiti da parte di tali soggetti.

Occorre comunque considerare che negli schemi di certificazione realmente attivi non tutti i ruoli sopra citati sono presenti e che alcuni ruoli possono essere svolti da uno stesso soggetto. Inoltre, anche per ragioni storiche, nei vari schemi di certificazione i diversi ruoli possono essere più noti con nomi diversi rispetto a quelli qui presentati. Queste circostanze, come meglio vedremo in seguito, non inficiano, di per sé, la validità dei vari schemi di certificazione, a patto che rimangano sostanzialmente garantite le caratteristiche principali descritte nel seguito.

La legittimazione dello Schema di Certificazione (e, conseguentemente, di tutti i soggetti coinvolti nello schema) ad operare in un determinato ambito può essere fornita secondo varie modalità, che spaziano dall'intervento normativo emesso da organi istituzionali di uno Stato, al riconoscimento della bontà dello Schema effettuato da un organismo sovranazionale, fino al riconoscimento "oggettivo" di competenza ottenuto dalla comunità di operatori e utenti che si avvale dello Schema stesso.

Sempre in linea generale, un processo di certificazione deve garantire almeno quattro caratteristiche principali:

1. l'imparzialità: la valutazione deve essere condotta senza pregiudizi e, in particolare, deve essere possibile dimostrare che i valutatori coinvolti non abbiano interessi commerciali o finanziari dipendenti dall'esito della valutazione stessa;
2. l'oggettività: le conclusioni del processo di valutazione devono essere motivate da evidenze sperimentali ogni qual volta sia realizzabile, in modo da limitare il più possibile opinioni e valutazioni soggettive;
3. la ripetibilità: la valutazione dello stesso oggetto effettuata con gli stessi requisiti di sicurezza e dallo stesso Valutatore deve portare agli stessi risultati;

4. la riproducibilità: la valutazione dello stesso oggetto effettuata con gli stessi requisiti di sicurezza da un diverso Valutatore deve portare agli stessi risultati.

In questo contesto, si definisce "di terza parte" uno schema di valutazione e certificazione nel quale il Valutatore, qualora sia presente, il Certificatore e l'Accreditatore siano terza parte indipendente rispetto al Titolare dell'oggetto da certificare e al Fruitore della certificazione.

Le caratteristiche descritte in precedenza, a loro volta, non hanno un significato assoluto ma dovrebbero essere ulteriormente precisate, stabilendo, per esempio, la portata delle verifiche che devono essere svolte sull'oggetto che deve essere certificato, quali garanzie debbano essere fornite per garantire la terzietà dei vari soggetti, come verificare la competenza di chi applica le norme di riferimento.

Tenendo in considerazione le caratteristiche sopra enunciate e verificando con quali modalità esse sono realizzate in un particolare schema di certificazione, è possibile comprendere, sia pure in forma qualitativa, quale sia la vera "garanzia" offerta dal processo di certificazione considerato e, in particolare, su chi o su che cosa, in definitiva, occorre effettivamente riporre la propria fiducia. E' quasi ovvio sottolineare che è praticamente irrealizzabile uno schema di certificazione "perfetto", cioè che soddisfi pienamente tutte le caratteristiche sopra enunciate nella loro accezione più ampia. Per alcune caratteristiche, come la "oggettività", l'irrealizzabilità è dovuta al fatto che in alcuni schemi, come ad esempio quelli relativi alla verifica di competenza del personale, la valutazione di sicurezza (l'esame finale) si basa o sul giudizio soggettivo del valutatore (esaminatore) o sull' inevitabile parzialità delle prove effettuate rispetto alla portata della certificazione. In altri casi, come spesso accade nel settore della sicurezza fisica, il processo di certificazione non può essere fondato su una norma di riferimento perché essa, molto semplicemente, non esiste.

Nel campo della certificazione di sicurezza è quindi necessario accettare dei compromessi: l'importante è che questi compromessi siano conosciuti e accettati da tutti i soggetti che si avvalgono, in varie forme, di una particolare certificazione di sicurezza.

Anche per questi motivi, in questa linea guida non si esprimeranno giudizi o comparazioni tra i vari schemi di certificazione che mirino a stabilire la superiorità di uno schema rispetto ad un altro. Piuttosto, per ogni schema si cercherà di evidenziare quali dei ruoli sopra citati sono realizzati, con quali modalità e le garanzie poste in essere per cercare di realizzare le desiderate caratteristiche di imparzialità, oggettività, ripetibilità e riproducibilità.

Nel seguito di questo documento ci si occuperà in dettaglio delle certificazioni di sicurezza che fanno riferimento allo standard ISO27001, allo standard ISO15408 (Common Criteria) e alle certificazioni di competenza del personale. Verranno fornite anche indicazioni rispetto alla certificazione di sicurezza fisica con lo scopo, in questo caso, di evidenziare la complessità e la vastità del problema, cercando, al contempo, di fornire alcuni suggerimenti in un caso specifico (il cablaggio strutturato) che potranno essere presi a riferimento nei casi differenti da quello proposto.

A conclusione di questo paragrafo, è utile definire anche altri termini che spesso sono confusi con la certificazione di terza parte e che, al contempo, sono molto diffusi:

1. omologazione: per "omologazione" si intende una attestazione che un "tipo" di prodotto è conforme ad una specifica norma. L'omologazione, in generale, viene rilasciata verificando solamente un campione del prodotto e, quindi, fornisce una garanzia solo parziale rispetto, per esempio, alla qualità di un intero lotto di fornitura. L'omologazione viene normalmente rilasciata da un Ente od Istituto indipendente ed accreditato: limitatamente a questo aspetto, quindi, può essere considerata come una verifica di "terza parte";
2. Certificazione di conformità: indica la dichiarazione di un produttore, sotto la sua responsabilità, sulla conformità dei suoi prodotti a un insieme di requisiti, senza l'intervento di un Ente terzo indipendente. Il costruttore redige la dichiarazione sulla base di un fascicolo tecnico contenente una documentazione completa ed adeguata per dimostrare la conformità dei prodotti ai suddetti requisiti.

Il costruttore può scegliere di effettuare le prove, relative alle normative tecniche applicabili al prodotto, nel suo laboratorio o presso Laboratori esterni di sua fiducia. In alcuni casi le Direttive prevedono l'intervento di un Organismo di terza parte indipendente.

1.1 Quadro normativo attuale

In Italia, l'attuale quadro normativo relativo al problema generale della sicurezza delle informazioni appare caratterizzato da una elevata frammentarietà e da una scarsa coerenza sistematica. Per una ricostruzione dettagliata di tale situazione si rimanda al cap. 1.6 del documento "Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione" redatto dal Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni, e pubblicato nel marzo 2004[4].

In questo contesto, non è sorprendente che il tema specifico della obbligatorietà della certificazione di terza parte non sia oggetto di specifica regolamentazione, escludendo, comunque, il caso non secondario dei sistemi che trattino informazioni classificate[5] , per i quali è previsto un obbligo di certificazione secondo gli standard ITSEC o Common Criteria.

In ambito europeo, occorre segnalare, nel contesto delle certificazioni di sicurezza, un approccio più esplicito - rispetto a quanto accade in Italia - che tende a diffondere l'uso delle certificazioni di sicurezza su base volontaria. A tale proposito, vorremmo citare, a titolo di esempio significativo, la risoluzione del Consiglio del 28 gennaio

4 Il documento citato è disponibile all'indirizzo web: http://www.cnipa.gov.it/site/it IT/Attività/Sicurezza_informatica/, che descrive anche tutte le ulteriori iniziative del Comitato Tecnico.

5 D.P.C.M. 11 aprile 2002 – 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.

2002 "*On a common approach and specific actions in the area of network and information security*". In questa risoluzione il Consiglio chiede agli Stati Membri "*to promote the use of the common criteria standard (ISO15408) and to facilitate mutual recognition of related certificates*" ed esprime il suo parere favorevole rispetto alla intenzione della Commissione europea di proporre misure adeguate "*to promote the ISO15408 (Common Criteria) standard, to facilitate mutual recognition of certificates, and to improve the process by which products are evaluated, i.e. by developing adequate protection profiles*".

Nello stesso contesto, il Consiglio riconosce anche che lo standard ISO17799 è un approccio riconosciuto come valido per la gestione della sicurezza sia in ambito privato, sia per le pubbliche amministrazioni.

Pur in assenza di obblighi di legge, la certificazione di sicurezza di terza parte effettuata su base volontaria, e in particolare quella effettuata secondo gli standard ISO 27001 (ex BS7799-2) e/o i Common Criteria, può, in alcuni casi, essere utilizzata per dimostrare a terzi di aver ottemperato ad obblighi di legge in materia di sicurezza delle informazioni. A questo proposito, si cita l'esempio notevole del Codice sulla Privacy (D.Lgs. n. 196/2003 - Codice in materia di protezione dei dati personali). In particolare, considerando che:

- l'art.31 recita che "i dati personali, oggetto di trattamento, sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al **progresso tecnico**, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di **idonee** e **preventive** misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta";
- l'art. 15, che recita "Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile", impone al Titolare dei trattamenti "l'onere di inversione della prova" di aver adottato misure idonee e preventive; è evidente che l'utilizzo delle opportune certificazioni di sicurezza volontarie di terza parte possa costituire una adegua-

ta dimostrazione a terzi (per es., in Tribunale) dell'adempimento di quanto previsto all'art.31 sopracitato.

1.2 Il valore aggiunto della certificazione di sicurezza

In assenza di obblighi di legge, il processo di certificazione volontaria della sicurezza ICT può essere iniziato da diversi soggetti, ognuno dei quali potrebbe avere interessi particolari nell'affrontare il processo di certificazione stesso. Nel seguito, a titolo di esempio, vengono fornite alcune motivazioni che potrebbero essere alla base, per vari soggetti, della decisione di avviare un processo di certificazione volontaria:

1. Il soggetto fornitore dell'oggetto/processo da certificare può ritenere utile ottenere una certificazione di terza parte in quanto ritiene che tale certificazione possa essere utilizzata come leva di marketing per incrementare le vendite o per uniformarsi allo standard di mercato imposto dai concorrenti. Queste motivazioni sono state sicuramente ed evidentemente particolarmente importanti almeno in alcuni settori specifici, quale, ad esempio, quello del mercato dei firewall, in cui tutti i leader di mercato hanno ottenuto per i loro prodotti una certificazione secondo i Common Criteria, generalmente di livello medio alto (EAL4);
2. Il soggetto titolare (o fruitore) dell'oggetto/processo certificato (ad esempio, l'ISMS di una banca o un sistema/prodotto di e-banking) vuole dimostrare anche verso terzi, siano essi i "clienti" o una autorità statale (ad esempio, la magistratura, o il Garante per la tutela dei dati personali) di aver curato adeguatamente la gestione della sicurezza. In questo contesto, la certificazione di sicurezza assume nel primo caso la valenza di leva di marketing, nel secondo caso rappresenta un modo per dimostrare a terzi, a fronte di eventuali "incidenti" ICT, la pro-pria diligenza nell'attuare in via preventiva tutte le contromisure ritenute necessarie per limitare la probabilità di accadimento dell'incidente stesso. In questi casi, in particolare, il soggetto titolare (o fruitore) dell'oggetto certificato dimostra di non

essersi fidato delle sole dichiarazioni sulla sicurezza ICT eventualmente rilasciate dal fornitore dell'oggetto;

3. Il soggetto titolare (o fruitore) dell'oggetto/processo certificato vuole acquisire la consapevolezza della "propria" sicurezza, affidando a terzi il compito della verifica. Questa decisione non implica, ovviamente, una mancanza di fiducia nella competenza del proprio personale incaricato di verificare la sicurezza, ma piuttosto deve essere considerata come l'acquisizione di servizi professionali altamente qualificati che, come tali, assicurano all'organizzazione che si avvale della certificazione di sicurezza volontaria un valore aggiunto finalizzato all'incremento di efficienza dell'organizzazione stessa.

Inoltre, occorre evidenziare che sempre più spesso i "clienti" finali di un' organizzazione, sia essa pubblica amministrazione o azienda privata, richiedono la certificazione di terza parte come elemento determinante per potersi avvalere dei servizi di quella particolare organizzazione. In questo caso rientrano, ad esempio, le certificazioni di qualità del tipo ISO9000 (che non vengono trattate in questa linea guida in quanto non sono specifiche per la sicurezza ICT) che la Pubblica Amministrazione impone, in molti casi, ai propri fornitori. E' prevedibile che anche in materia di sicurezza informatica, verranno adottate dalla PA prescrizioni analoghe, anche in considerazione delle indicazioni strategiche individuate dal Comitato tecnico nazionale per la sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni, riportate nel paragrafo seguente.

1.3 Ambiti di applicazione della certificazione di sicurezza

Considerando che, in generale, i processi di certificazione della sicurezza sono onerosi, sia in termini economici, sia in termini di utilizzo delle risorse umane, è opportuno delineare una strategia di ricorso alle certificazioni di sicurezza che, perlomeno, individui i contesti più critici e prioritari, in modo tale da ottimizzare l'utilizzo delle suddette risorse.

Nel presente paragrafo vengono riportate, per comodità del lettore, le indicazioni fornite dal Comitato tecnico nazionale per la sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni riportate nel n.23 del marzo 2006 de "i Quaderni" edito dal CNIPA, in cui sono riportati, tra l'altro, i contesti nei quali utilizzare la certificazione nella PA .

Le considerazioni del Comitato sono applicabili, a nostro avviso e con le dovute e naturali differenziazioni, anche agli Enti privati.

Il Comitato, nel proporre le suddette indicazioni, ha perseguito l'obiettivo di stimolare l'uso dei servizi di certificazione soprattutto nei contesti a più elevata criticità individuabili all'interno della PA[6]. Successivamente, compatibilmente con i vincoli di carattere economico, il Comitato fornirà ulteriori indicazioni ai fini di estendere l'utilizzo di tali servizi, graduando opportunamente il livello delle certificazioni, a contesti cui sia associabile un rischio meno elevato.

Al fine di individuare con esattezza le indicazioni fornite dal Comitato, nel seguito esse sono riportate in carattere corsivo.

Contesti a massima priorità (certificazione altamente raccomandata)

Per ciò che concerne la criticità dei contesti appare prioritario citare quelli attinenti alla tutela dell'incolumità fisica e della salute dei cittadini. Si tratta infatti di contesti per i quali, in settori diversi da quello relativo alle tecnologie ICT, lo Stato ha ritenuto non sufficienti le autocertificazioni o le certificazioni volontarie ed ha quindi introdotto l'obbligo di verifiche di terza parte. Per ciò che concerne in particolare l'incolumità dei cittadini è evidente la notevole importanza dei contesti che afferiscono al mantenimento dell'ordine pubblico, alla tutela della sicurezza dei cittadini, alla protezione civile, alle infrastrutture critiche (servizi di trasporto, di comunicazione, di erogazione dell'energia elettrica, di distribuzione del gas e dell'acqua, ecc.). Per molti dei contesti citati, specifici settori della PA hanno competenze

6 CNIPA, "i Quaderni", n. 23 marzo 2006, "Linee Guida per la sicurezza ICT nelle Pubbliche Amministrazioni. Piano Nazionale della sicurezza delle ICT per la PA. Modello organizzativo nazionale di sicurezza ICT per la PA", disponibile in formato elettronico all'indirizzo web www.cnipa.gov.it/site/_files/Quaderno%20n%2023.pdf., pagg 52 e 53.

esclusive ed una piena autonomia nelle scelte organizzative ed operative. In questi casi quindi, ancor più che in generale, le indicazioni fornite costituiscono suggerimenti miranti a consentire la fruizione dei benefici della certificazione negli ambiti che appaiono più appropriati. Non vengono invece presi in considerazione i contesti relativi alla tutela delle informazioni coperte dal segreto di stato, per i quali è vigente già dal 1995 l'obbligo di certificazione della sicurezza ICT. L'importanza di eseguire certificazioni di sicurezza ICT nei contesti relativi alla tutela dell'incolumità fisica e della salute dei cittadini risulta evidente una volta che si consideri il ruolo sempre più centrale che i sistemi ICT stanno assumendo in tali contesti. Un malfunzionamento, accidentale o provocato, di tali sistemi può infatti in molti casi produrre gravissimi danni alle persone, se non addirittura la perdita di numerose vite umane.

Altri contesti a priorità molto elevata dal punto di vista della certificazione di sicurezza sono quelli in cui il danno, pur essendo solo di tipo economico, può essere comunque molto rilevante sia per il cittadino sia per lo stato. Per alcuni di questi contesti esistono dei precedenti nella legislazione italiana, come dimostra il caso della firma digitale. Affinché a quest'ultima possa essere riconosciuto il valore legale, infatti, alcuni dei dispositivi ICT che la gestiscono devono essere obbligatoriamente sottoposti ad un processo di valutazione/certificazione. Altre situazioni nelle quali si possono verificare ingenti danni per lo stato sono ad esempio quelle riferibili a eventuali mancate entrate attraverso imposte e tributi o al mancato conseguimento di benefici in termini di contenimento della spesa pubblica. Per quanto riguarda quest'ultimo aspetto la certificazione di sicurezza può sicuramente svolgere un ruolo importante, ad esempio, nel generare fiducia nei cittadini circa la fruizione in forma telematica di servizi della PA normalmente erogati nella forma tradizionale, la quale molto spesso risulta sensibilmente più onerosa in termini economici per lo stato. In alcuni di questi casi, quali ad esempio il voto elettronico o i servizi nei quali vengono trattati dati personali sensibili, oltre al beneficio in termini economici per lo stato si può peraltro ravvisare anche quello di aver sottoposto a verifica di terza parte la tutela che gli apparati ICT sono in grado di assicurare al cittadino quando quest'ultimo li utilizza per esercitare le proprie libertà ed i propri diritti fondamentali.

Altri contesti critici

Altre situazioni nelle quali la certificazione, sia pure con minore forza rispetto ai casi trattati nel precedente paragrafo, può essere consigliata sono quelle per le quali si possano prevedere danni considerevoli a seguito di incidenti informatici. Ad esempio nel caso di archivi elettronici contenenti ingenti quantità di dati, eventuali alterazioni o cancellazioni (accidentali o intenzionali) di tali dati possono produrre, oltre al danno derivante dall'interruzione più o meno lunga dei servizi correlati, anche il danno rappresentato dal costo di reinserimento dei dati stessi nell'archivio. A tal proposito andrebbe anche considerato che alcuni dati potrebbero essere non recuperabili, qualora non esistesse per essi una copia cartacea o elettronica (back-up) nel momento in cui l'incidente informatico si è verificato. Un altro tipo di danno può essere quello di immagine che lo Stato potrebbe subire qualora si dimostrasse che non è stato in grado di tutelare adeguatamente le informazioni ed i servizi gestiti. Anche questo danno può avere ovviamente dei risvolti economici, in quanto il cittadino, come già osservato, potrebbe rinunciare ad avvalersi di tali servizi per via telematica impedendo così di realizzare le economie consentite dall'automazione dei processi. Anche il singolo cittadino peraltro può subire danni diretti nel caso in cui la PA non protegga adeguatamente, sotto il profilo della riservatezza, dell'integrità e della disponibilità, i dati che utilizza per offrirgli i servizi. Anche questi danni dovrebbero quindi essere stimati per decidere se sia opportuno prevedere una certificazione di sicurezza, che questa volta andrebbe a garantire i singoli cittadini piuttosto che lo Stato nel suo complesso.

2 - Schemi di certificazione e di accreditamento

In questo paragrafo si descriveranno, con riferimento alla situazione italiana, gli schemi di certificazione che fanno riferimento allo standard ISO27001, e allo standard ISO15408 (Common Criteria). La descrizione verrà effettuata con le finalità principali sia di descrivere i suddetti schemi, sia di far emergere le differenze terminologiche e "di metodo".

2.1 La sicurezza ICT in un'organizzazione

Normalmente, quando si parla in generale di "sicurezza ICT" ci si riferisce ad una molteplicità di aspetti tecnici, organizzativi e procedurali che tendono a proteggere l'hardware, il software, le informazioni, i servizi.

In particolare, per quanto riguarda le informazioni, le caratteristiche principali che devono essere protette sono:

- la riservatezza (o confidenzialità), che tende a garantire che le informazioni non possano essere accedute da soggetti non autorizzati, sia in modo intenzionale, sia in modo accidentale;

- l'autenticità, che tende a garantire che le informazioni appaiano come generate da un'entità che sia quella che le ha effettivamente generate;
- l'integrità, che tende a garantire che le informazioni non possano subire alterazioni non autorizzate, siano esse accidentali o intenzionali;
- la disponibilità, che mira a garantire che i soggetti autorizzati possano effettivamente accedere alle informazioni ogniqualvolta sia necessario, anche in presenza di fenomeni ostativi accidentali o in presenza di azioni ostili deliberate che tendano ad impedirne l'accesso.

Ovviamente, nei casi reali potrebbe essere estremamente complesso, se non addirittura impossibile, garantire con certezza assoluta le suddette caratteristiche. E' pertanto necessario individuare dei compromessi che tengano in conto, tra gli altri, anche gli aspetti economici della realizzazione della sicurezza ICT. L'importante è che tali compromessi siano individuati in modo esplicito e consapevole da parte di ogni Ente. Questo risultato lo si può ottenere solamente adottando un processo organico e strutturato di analisi e di realizzazione della sicurezza ICT. Questo processo è stato standardizzato in varie normative internazionali, tra cui la ISO 27001, ed è conosciuto con il termine "Analisi dei rischi".

Per quanto riguarda la descrizione dettagliata delle finalità e delle metodologie di realizzazione di una corretta analisi dei rischi, si rimanda alla copiosa letteratura in materia, tra cui è opportuno segnalare anche la Linea Guida "La sicurezza delle reti - Dall'analisi del rischio alle strategie di protezione" redatta dal Gruppo di lavoro sulle infrastrutture critiche coordinato dall'ISCOM (Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione) e disponibile all'indirizzo web www.iscom.gov.it..

Nel contesto di questa Linea Guida, si vuole sottolineare che tra le altre "conclusioni" di una corretta Analisi dei rischi dovrebbe esserci anche l'individuazione di quelle parti della realizzazione della sicurezza ICT che necessitano, nel caso particolare, di una certificazione di sicurezza di terza parte. Con riferimento alla figura seguente, che

descrive in modo sintetico l'approccio di sicurezza "globale" che dovrebbe essere realizzato da una specifica Organizzazione, i possibili ambiti in cui potrebbe essere richiesta una certificazione di sicurezza ICT sono:

- il processo di gestione della sicurezza (ISMS), che può essere certificato in accordo allo standard ISO27001;
- le contromisure tecniche (sistemi e prodotti ICT), le cui funzionalità di sicurezza possono essere certificate facendo riferimento allo standard Common Criteria (ISO15408);
- la competenza del personale, certificabile in accordo a vari criteri, quali il CISSP/SSCP, il CISA/CISM ed altri;
- le contromisure fisiche ambientali, quali i sistemi antincendio, i sistemi di accesso ai locali, ecc.

Vogliamo sottolineare che le certificazioni di per sé non riescono ad aumentare la sicurezza se non sono accompagnate da una sensibilità ed attenzione alla cultura organizzativa in cui si innestano. E' dunque importante considerare le certificazioni come condizione necessaria ma non sufficiente: è solo attraverso un lavoro continuo di sensibilizzazione ed attenzione che parte dai più elevati livelli del management che l'organizzazione può essere mobilitata alla difesa del "bene conoscenza" e del valore economico e istituzionale che essa rappresenta.

2.2 Gli Schemi di certificazione della sicurezza in Italia

Gli Schemi della certificazione della sicurezza ICT, attualmente operanti in Italia, possono essere suddivisi in due categorie:

1. Le certificazioni regolate da DPCM (Decreto della Presidenza del Consiglio dei Ministri):
   - Schema Nazionale del 1995 aggiornato nel 2002 (DPCM 11 aprile 2002 – GU n. 131 del 6 giugno 2002) applicabile nel contesto della sicurezza interna e esterna dello Stato. Si occupa di certificazione di prodotto/sistema ICT. L'Ente di Certificazione/Accreditamento (EC) è l'ANS/UCSI. Attualmente in questo schema sono accreditati 5 Centri di Valutazione, 3 privati e due pubblici;
   - Schema Nazionale del 2003 (DPCM 30 ottobre 2003 – GU n. 98 del 27 aprile 2004) che si occupa di certificazione di prodotto/sistema ICT in tutti i contesti non coperti dal primo Schema. Con il DPCM 30 ottobre 2003 presso l'ISCOM[7] è stato istituito l'OCSI, Organismo di certificazione della sicurezza di sistemi e prodotti ICT, che non trattano informazioni classificate concernenti la sicurezza interna ed esterna dello Stato. L'OCSI, che si avvale del suppor-

to della Fondazione Ugo Bordoni (FUB), svolge un duplice ruolo di accreditatore e di certificatore. Infatti l'OCSI accredita Laboratori di Valutazione della Sicurezza informatica (LVS), i quali operano in base ai criteri di valutazione ISO 15408 (*Common Criteria for Information Technology Security Evaluation*) e ITSEC (*Information Technology Security Evaluation Criteria*) Inoltre l'OCSI è l'unico soggetto abilitato all'emissione dei certificati, i quali sono rilasciati a seguito dell'approvazione dei risultati della valutazione effettuata dagli LVS. Attualmente in questo schema sono accreditati tre laboratori per la valutazione della sicurezza (LVS).

2. Altre certificazioni:
   - per la certificazione del processo di gestione (ISMS) che fa riferimento alla ISO27001:2005 (ovvero BS7799-2:2002 nel periodo transitorio definito con apposita comunicazione posta sul sito www.sincert.it) SINCERT è l'Ente di Accreditamento Nazionale per gli Organismi di Certificazione e per gli Organismi di Ispezione. In questa veste opera le attività di accreditamento degli Organismi di Certificazione che valutano le Organizzazioni per l'eventuale rilascio delle certificazioni di conformità alla Norma ISO27001:2005
   - per la certificazione del personale, i criteri di verifica della competenza sono sviluppati per quanto riguarda l'Italia da CEPAS (in particolare per le figure di

7 - ISCOM è l'Istituto Superiore per le Comunicazioni e le Tecnologie dell'Informazione, che opera nell'ambito del Ministero delle Comunicazioni in qualità di organo tecnico-scientifico. La sua attività, rivolta specificatamente verso le aziende operanti nel settore ICT, le Amministrazioni pubbliche e l'utenza, riguarda fondamentalmente i servizi alle imprese, la normazione, la sperimentazione e la ricerca di base e applicata, la formazione e l'istruzione specializzata nel campo delle telecomunicazioni. Il ruolo di organismo tecnico scientifico assieme alla garanzia di indipendenza da parti terze, porta l'Istituto ad essere riferimento per favorire lo sviluppo delle telecomunicazioni semplificando l'immissione sul mercato di nuovi prodotti e l'applicazione di tecnologie innovative.

ICT Security Manager, ICT Security Auditor, ICT Security Responsabile Gruppo di Audit), ovvero da KHC (in particolare per le figure del Security Auditor Interno, del Security Auditor e Lead Auditor e del Privacy Auditor). A livello internazionale alcune certificazioni sono state sviluppate da ISC2 (per quanto riguarda CISSP/SSCP) e da ISACA (per quanto riguarda CISA/CISM): queste due organizzazioni operano anche in Italia attraverso le relative affiliazioni nazionali. Va ricordato che queste ultime certificazioni (CISA/CISM e CISSP/SSCP) sono gestite sotto Accreditamento statunitense, emesso da ANSI/RAB[8]

E' da evidenziare che le norme ISO27001e ISO15408/ITSEC, pur essendo state sviluppate con finalità completamente diverse, prevedono in alcuni casi requisiti e, verifiche riguardanti aspetti similari. Quando ciò avviene, un'adeguata interpretazione delle norme può consentire da un lato di rendere del tutto complementari e sinergiche le relative certificazioni, dall'altro di evitare la possibile duplicazione di attività da parte degli Auditor ISO27001 e dei valutatori ISO15408/ITSEC. L'uso congiunto delle due certificazioni risulta così ottimizzato dal punto di vista sia dell'efficienza sia dell'efficacia, dal momento che diviene possibile conseguire, con un minor impegno di risorse, un più elevato livello di sicurezza globale.

Con queste finalità ISCOM ha affiancato SINCERT nella produzione di un Regolamento Tecnico, in corso di emanazione, avente lo scopo di integrare i requisiti di accreditamento generali già definiti nei Regolamenti SINCERT, nonché quelli individuati nelle Linee Guida EA 7/01 ed EA 7/03 con quei criteri operativi che possono fornire un vero valore aggiunto per tutte le parti interessate al processo di certificazione: in primis le Organizzazioni, con le proprie risorse umane, i Clienti, i Fornitori e la collettività tutta, come appropriato. In particolare, il Regolamento Tecnico dovrebbe prevedere che[9] :

8 Negli Stati Uniti, ANSI/RAB è l'equivalente di SINCERT; tra i due Enti di Accreditamento esiste il mutuo riconoscimento.

9 Le informazioni sotto riportate dovranno essere verificate all'emanazione effettiva del Regolamento Tecnico che dovrebbe avvenire entro breve tempo..

- nel caso dello svolgimento di certificazioni dei prodotti informatici, secondo gli schemi ANS ovvero OCSI, in presenza di una vigente certificazione del Sistema di Gestione della Sicurezza delle Informazioni, emessa sotto accreditamento SINCERT o di Ente da questi riconosciuto, gli ispettori dei laboratori Ce.Va., ovvero LVS, provvederanno a valutare la coerenza tra la documentazione di sistema richiesta per tali certificazioni e quella del Sistema di Gestione della Sicurezza delle Informazioni, limitatamente agli aspetti organizzativi di loro competenza, registrando le eventuali incoerenze come "non conformità".
- nel caso dello svolgimento del processo di valutazione di Organizzazioni che richiedano la certificazione del proprio Sistema di Gestione della Sicurezza delle Informazioni in presenza di certificazioni di prodotti informatici (secondo gli schemi nazionali gestiti da ANS o da OCSI), gli Auditor dell' Organismo di Certificazione provvederanno a richiedere a tali Organizzazioni le evidenze relative alla struttura organizzativa dichiarata ai Laboratori (Ce.Va., ovvero LVS) e verificheranno la coerenza di tale documentazione relativa alla struttura dell' Organizzazione sotto valutazione con la documentazione di sistema presentata all'Organismo di Certificazione. Le eventuali discrepanze dovranno essere gestite come "non conformità" della documentazione di sistema in parola.

2.3 Schema di certificazione e accreditamento ISO27001

2.3.1 Lo schema di accreditamento di SINCERT

Da quanto illustrato finora, appare chiaro che l'oggetto della certificazione secondo lo standard ISO27001 (ovvero BS7799-2 nel periodo transitorio) è il processo di gestione della sicurezza (ISMS).

Riprendendo i concetti espressi nel paragrafo 1, tale certificazione, in Italia, si fonda sui seguenti attori fondamentali:

- La norma di riferimento ISO27001:2005;
- Lo schema di certificazione costituito dalla Linea Guida EA7/03 e dai Regolamenti Tecnici di SINCERT;
- SINCERT, che definisce le regole per la gestione dello schema e che rappresenta l'ente Accreditatore, cioè colui che dà "credibilità" al Certificatore vigilando sulla corretta applicazione dello schema, sia dal punto di vista formale, sia da quello delle competenze, sia nella correttezza delle offerte che nella completa assenza di conflitti di interessi tra le parti in causa. Il processo di accreditamento si svolge sulla base della Norma UNI CEI EN45012:1998[10], delle prescrizioni del Regolamento Generale di Accreditamento (RG – 01) e delle Linee Guida EA7/01 ed EA7/03. Attualmente il SINCERT ha accreditato 5 Organismi di certificazione.
- il Certificatore, che rilascia i certificati applicando correttamente lo schema. Fatti salvi i controlli interni, la vigilanza sull'organismo di certificazione è effettuata da SINCERT che controlla anche che l'organismo sia gestito attuando gli indirizzi dati da un comitato di parti interessate, costituito in modo equilibrato tra gli stakeholders;
- il Valutatore, che esegue la valutazione di sicurezza. Qui la criticità sta nella competenza e nell'approccio etico di tale "braccio operativo": garanzia che viene data da apposita certificazione della professionalità di tale figura, con tutti gli aspetti connessi (esami, mantenimento della competenza nel tempo, rispetto del codice etico e gestione dei possibili reclami);

il Committente della certificazione, cioè l'azienda che richiede volontariamente tale atto.

10 A breve, tale Norma sarà sostituita dalla ISO IEC 17021

2.3.2 Le competenze del personale di valutazione

Come detto, tutto il personale addetto alle attività di valutazione utilizzato dall'Organismo di Certificazione, nei vari ruoli di Responsabile del Programma di Audit, Responsabile dei Gruppi di Audit e di Auditor, deve possedere particolari competenze nell'ambito della ICT e, in modo particolare, nella Sicurezza delle Informazioni e aver superato un corso di formazione sulla norma ISO27001 e sulla ISO19011 qualificato da un Organismo di Certificazione del Personale accreditato o riconosciuto da SINCERT.

I requisiti particolareggiati di tali competenze sono descritti nel documento "Prescrizioni per l'accreditamento degli Organismi di Certificazione operanti la certificazione dei Sistemi di Gestione della Sicurezza delle Informazioni" in corso di emanazione da parte di SINCERT/ISCOM.

A partire dalla seconda metà del 2007, i Responsabili dei Gruppi di Auditing dovranno essere in possesso della Certificazione professionale per lo schema in parola, rilasciata da un Organismo di Certificazione del Personale accreditato o riconosciuto da SINCERT: sono considerate certificazioni idonee allo scopo anche le certificazioni CISA (Certified Information Systems Auditor), CISM (Certified Information Security Manager), o CISSP (Certified Information Systems Security Professional), ove il titolare abbia anche superato un corso di 40 ore sulla norma ISO27001:2005, qualificato da un Organismo di Certificazione del Personale accreditato o riconosciuto da SINCERT.

A questo proposito è bene evidenziare che BSI (British Standard Institution) ha disegnato un corso di formazione intensivo di 40 ore allo scopo di preparare i partecipanti alla conduzione di audit di terza parte su Sistemi di Gestione per la Sicurezza delle Informazioni conformi alla norma BS7799-2:2002. Nella giornata finale del corso è previsto un esame: ai partecipanti che lo superano viene consegnato un "certificato BSI" con la qualifica di Lead Auditor BS7799. Una versione tradotta di tale corso viene erogata anche in Italia su licenza BSI (www.bsi-italy.com). La partecipazione richiede almeno una buona conoscenza teorica-pratica della norma, oltre ad una discreta cono-

scenza nel campo della sicurezza informatica.

Alcune società accreditate dal Sincert quali enti certificatori di Sistemi di Gestione della Sicurezza delle Informazioni conformi alla norma ISO/IEC 27001:2005 (BS7799-2:2002 nel periodo transitorio del 2006), erogano analoghi corsi di formazione (non licenziati dal BSI) indirizzati a coloro i quali vogliano prepararsi per il ruolo di Lead Auditor BS7799. Tali corsi forniscono attestati di partecipazione e superamento dell'eventuale esame; in alcuni casi tali attestati vengono denominati "certificati".

In Italia non è attualmente disponibile uno schema di certificazione del personale in relazione alla qualifica di Lead Auditor BS7799. Pertanto né il "certificato BSI", né gli attestati (o "certificati") emessi da altri enti dopo il superamento di prove d'esame relativi a corsi di formazione sull'argomento, possono essere considerati certificati nel senso pieno del termine.

Dunque, rimane aperta la questione della stima del livello di garanzia che può essere riposto sul fatto che una persona che abbia partecipato con successo a tali corsi sia effettivamente in possesso dei requisiti necessari ad assolvere il compito di Lead Auditor BS7799. Una possibile scelta consiste nello stimare l'autorevolezza delle organizzazioni che li erogano.

Tale scenario risulta molto utile a comprendere il valore di uno schema di certificazione!

Proprio per ovviare alle possibili anomalie derivanti dall' assenza di un riferimento certo sulle competenze che deve avere il Lead Auditor per i Sistemi di Gestione della Security delle Informazioni, SINCERT ha definito, in collaborazione con ISCOM, i requisiti minimi, che sono stati inseriti nel Regolamento Tecnico di prossima pubblicazione. In assenza di questi, stante la non esaustività della Linea Guida europea EA 7/03, SINCERT ha effettuato delle valutazioni di merito sui profili dei singoli Auditor degli Organismi di Certificazione accreditati, sulla base del possesso di adeguate qualifiche nello specifico settore della ICT Security e del superamento del corso di qualificazione sulle norme di riferimento.

Inoltre, vale la pena di riportare il successo che tali corsi di for-

mazione stanno riscontrando negli ultimi anni. Titolari di aziende, consulenti, IT e quality manager; personale coinvolto nell'implementazione di un ISMS, professionisti dell'IT si stanno rivolgendo a tali corsi allo scopo di comprendere principi e meccanismi della certificazione ISO 27001 (BS7799-2), pur non essendo intenzionati a ricoprire il ruolo di Lead Auditor ISMS. Entrando nel ruolo dell' Auditor è infatti possibile arricchire le competenze necessarie a progettare al meglio un Sistema di Gestione della Sicurezza delle Informazioni che dovrà essere sottoposto all'iter di certificazione. Inoltre, occorre specificare che, al di la del percorso di certificazione, nelle diverse Organizzazioni aventi dei Sistemi di Gestione della Security delle Informazioni attivi, debbono essere svolti gli Audit Interni. Il processo di Auditing Interno per tali Sistemi di Gestione richiede una competenza ottenibile,in parte, anche attraverso la frequenza a tali corsi di formazione.

Infine, c'è da osservare che quando ci si rivolge ad un ente accreditato dal SINCERT per la certificazione ISO 27001 (ex BS7799-2) non è necessario che l' Organizzazione certificanda richieda essa stessa delle certificazioni di competenza del personale del team di audit che si occuperà di portare avanti l'iter. Lo schema di certificazione ISO 27001 di SINCERT prevede infatti specifici requisiti sul personale dell'ente di certificazione, a garanzia della qualità del processo medesimo, pertanto rivolgendosi ad un ente accreditato si ottengono anche garanzie sul personale chiamato alla certificazione.

2.3.3 L'iter di certificazione

Un'organizzazione che desideri ottenere la certificazione di un suo ISMS deve seguire un iter ben preciso. Il primo passo consiste nella definizione e nell'implementazione del Sistema di Gestione, così come è definito dalla norma. Una volta che l'organizzazione abbia raggiunto la ragionevole fiducia nella stabilità e nella maturità del proprio ISMS, ed abbia come commitment direzionale quello della certificazione dello stesso, può procedere all'individuazione di uno tra gli enti di certificazione accreditati alla valutazione delle Organizzazioni ed alla loro eventuale certificazione, secondo la norma ISO/IEC 27001:2005

(BS7799-2:2002 nel periodo transitorio del 2006).

Da un punto di vista strettamente pratico, l'organizzazione richiederà all'ente di certificazione una proposta commerciale che, oltre ai servizi di valutazione nel seguito descritti, può prevedere elementi opzionali quali una visita cosiddetta "precertificativa". Solitamente si tratta di un momento informale in cui il certificatore, prima di iniziare l'iter vero e proprio, effettua un primo esame del Sistema di Gestione allo scopo di verificarne consistenza e maturità. L'esito può portare alla conferma del calendario previsto nella proposta economica, o allo slittamento dell'inizio dell'iter al momento in cui l'ISMS sarà giudicato sufficientemente maturo.

Una volta scelto l'ente certificatore, l'organizzazione condividerà con quest'ultimo la documentazione completa del Sistema di Gestione della Sicurezza delle Informazioni, con particolare riguardo a: Obiettivi del sistema di gestione; Policy di sicurezza; Ambito di validità dell'ISMS; Metodologia e risultati dell'analisi del rischio; Obiettivi di controllo e giustificazione dei controlli attuati.

L'iter di certificazione è articolato come segue:

- Valutazione iniziale – Fase 1: - Esame della documentazione e di congruità del sistema;
- Valutazione iniziale – Fase 2: - Attuazione dell'ISMS;
- Certificazione;
- Valutazione continua.

Dal punto di vista dell'organismo di certificazione, le attività prendono il via dalla designazione di un gruppo di valutazione ("team di audit") che studia la documentazione di riferimento e convoca, di concerto con l'organizzazione, una riunione introduttiva in cui vengono condivisi principi, metodologia, tempi e modi della verifica.

Valutazione iniziale – Fase 1 – Esame della documentazione e di congruità del sistema

Gli obiettivi che tale fase si propone di raggiungere sono:

- la comprensione del contesto in relazione alla politica di sicurezza dell'organizzazione;
- l'attuale livello di aderenza rispetto al punto precedente.

La valutazione iniziale si sostanzia nell'esame della documentazione disponibile e, secondo il Regolamento SINCERT, deve essere condotta presso il sito dell' Organizzazione certificanda.

E' questo il momento in cui si svolgono attività focali quali:

- verifica della metodologia di analisi e gestione del rischio scelta dall'organizzazione;
- valutazione della coerenza del campo di applicazione dell'ISMS e dello scopo che comparirà sul certificato quando emesso;
- verifica dello Statement of Applicability.

Lo Stage 1 è composto di un'attività di valutazione documentale ed una di raccolta di informazioni e di pre valutazione che deve essere svolta necessariamente sul campo, presso i siti delle Organizzazioni. Anche la valutazione documentale deve essere svolta presso l'Organizzazione Cliente, vuoi per evitare la trasmissione di documenti critici da e per gli uffici dell'Organismo di Certificazione, vuoi per avere immediata possibilità di una migliore interpretazione della documentazione stessa, in particolare per gli aspetti tecnologici. Comunque, prima delle attività di Stage 2, dovrà essere stato effettuato un sopralluogo ai siti dell'Organizzazione, a fronte della documentazione di sistema, con le finalità e modalità indicate nella LG EA 7/03 per lo Stage 1. Di tale sopralluogo dovrà essere redatto un adeguato rapporto, da consegnare al Responsabile del Programma di Audit, per la pianificazione delle attività di Stage 2.

Valutazione iniziale – Fase 2 – Verifica di attuazione dell'ISMS

Sulla base delle informazioni reperite nel corso della fase precedente, gli obiettivi sono:

- verificare la conformità dell'organizzazione alle proprie politiche/procedure;
- verificare e confermare che l'ISMS sia conforme alla norma oltre che ai documenti operativi;
- verificare l'efficacia dell'ISMS.

A differenza della fase precedente, focalizzata sulla documentazione, la *Verifica di attuazione* dell'ISMS prevede molte interazioni con il personale coinvolto nel Sistema di Gestione, che potrà essere intervistato a discrezione del certificatore.

La fase si conclude con l'emissione di un rapporto con indicati i risultati della verifica. All'interno del rapporto sono evidenziate eventuali non conformità ed il relativo livello di gravità.

Tale documento, detto "Rapporto di Verifica Ispettiva", conterrà:

- il riepilogo delle risultanze della verifica;
- gli obiettivi di controllo e controlli della norma sottoposti a verifica;
- le eventuali dichiarazioni di non conformità;
- il tracciamento dei reparti organizzativi coinvolti nella verifica e i nominativi del personale interpellato.

Certificazione

Costituisce la fase conclusiva della verifica e si conclude con successo se le eventuali non conformità rilevate in precedenza sono state eliminate tramite "azioni correttive". L'ISMS deve risultare aderente ai dettami della norma per ciò che concerne il campo di applicabilità. La conclusione prevede il rilascio del certificato ad opera dell'organismo di Certificazione.

La struttura di un certificato ISO 27001 (ex BS7799-2) è molto

simile a quella di un certificato di Quality Assurance ISO9001.

Pertanto contiene, sia in lingua italiana sia in lingua inglese, le seguenti informazioni:

- il nome (logo) della società che ha effettuato la certificazione (Organismo di Certificazione);
- la dicitura "ISMS Certificate" (generalmente in lingua inglese);
- il numero univoco di certificato;
- il nome, il focus e l'indirizzo dell'organizzazione che ha terminato positivamente l'iter di verifica ed ottenuto la certificazione;
- la dichiarazione di "compliance" alla norma ISO/IEC 27001:2005 (BS7799-2:2002 nel periodo transitorio del 2006);
- il campo di applicazione dell'ISMS. Il campo di applicazione definisce l'area dell'organizzazione che è stata sottoposta a verifica. L'identificazione di tale perimetro è utile al fine di individuare i controlli durante la verifica;
- la dichiarazione di aderenza allo Statement of Applicability;
- il luogo e la data di emissione;
- il nome e il cognome del Lead Auditor;
- il nome e il cognome, nonché la firma autografa del responsabile dell'organismo di certificazione;
- il simbolo dell'organismo preposto all'accreditamento (ad es. SINCERT);
- le regole per la validità e per le visite di sorveglianza periodica per il mantenimento della certificazione stessa (in calce).

Valutazione continua

Una volta ottenuta la certificazione sarà necessario procedere alla pianificazione di un certo numero di visite ispettive finalizzate al mantenimento. Tali visite mirano a garantire che quanto raggiunto in merito all'aderenza allo standard non venga meno nel corso del tempo.

In linea di massima, in base ai singoli regolamenti adottati dai diversi enti certificatori, le visite di mantenimento sono programmate a 6, 12, 18/24 mesi con una validità generale del certificato di 3 anni decorsi i quali tutte le operazioni vanno ripetute dal principio.

2.4 Schema di certificazione e accreditamento secondo i Common Criteria (e ITSEC)

Lo "Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione" raccoglie l'insieme delle procedure e delle regole necessarie per la valutazione e certificazione di sistemi e prodotti ICT, in conformità ai criteri europei ITSEC o ai Common Criteria[11] che, quindi, costituiscono le norme di riferimento.

Nello schema nazionale, i soggetti coinvolti nel processo di valutazione e certificazione della sicurezza sono[12]:

- l'Organismo di Certificazione (OCSI), che sovrintende alle attività operative di valutazione e certificazione nell'ambito dello Schema nazionale, svolgendo, in particolare, il ruolo di Certificatore e di Accreditatore dei Laboratori di valutazione della Sicurezza;

11 Lo standard Common Criteria è normalmente considerato come una "evoluzione" di ITSEC e, pertanto, nel seguito si darà maggiore spazio ai CC rispetto ad ITSEC. Purtuttavia, ITSEC rappresenta ancora una realtà rilevante in alcuni contesti specifici e, quindi, si ritiene opportuno fornire in questa linea guida indicazioni dettagliate anche per questo standard. Le informazioni di dettaglio su ITSEC sono riportate in Appendice.

12 L'elenco completo delle attività svolte dai vari soggetti è riportato nelle Linee Guida dell'OCSI, descritte brevente nel seguito e disponibili al sito web www.ocsi.gov.it.

- la Commissione di Garanzia, che ha il compito di dirimere ogni tipo di controversia inerente alle attività svolte all'interno dello Schema nazionale quando nella controversia sia coinvolto anche l'Organismo di Certificazione o quando quest'ultimo, pur non essendo coinvolto, non sia riuscito a dirimerla. La Commissione di Garanzia è presieduta da un membro prescelto dal Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri e vede rappresentati al suo interno il Ministro per l'Innovazione e le Tecnologie, il Ministero delle Comunicazioni, il Ministero delle Attività Produttive, il Ministero dell'Economia e delle Finanze, altri Ministeri che risultino interessati al funzionamento dello Schema nazionale, l'ISCOM, gli LVS, i Fornitori, le Associazioni dei Consumatori;
- i Laboratori per la Valutazione della Sicurezza (LVS) che, essendo accreditati dall'Organismo di Certificazione, effettuano le valutazioni di prodotti, sistemi e di profili di protezione in accordo allo Schema nazionale e sotto il diretto controllo dell'Organismo di Certificazione;
- i Committenti, cioè le persona fisiche, giuridiche o qualsiasi altro organismo che commissionano le valutazioni;
- i Fornitori, cioè le persona fisiche, giuridiche o qualsiasi altro organismo che forniscono gli oggetti da valutare. Il Fornitore può anche rivestire il ruolo di Committente della valutazione;
- gli Assistenti, persone formate, addestrate e abilitate dall'Organismo di Certificazione per fornire supporto tecnico al Committente o al Fornitore che ne faccia richiesta.

Le procedure relative allo Schema nazionale devono essere osservate dall'Organismo di Certificazione (OC), dai Laboratori per la Valutazione della Sicurezza (LVS), nonché 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 certifica-

zione di sicurezza conforme ai criteri europei e agli standard internazionali Common Criteria e ITSEC.

Lo Schema nazionale non si applica per i sistemi e prodotti che trattino informazioni classificate.

Lo Schema, gestito dall'ISCOM, è descritto in varie Linee Guida (disponibili al sito www.ocsi.gov.it), alle quali si rimanda per una comprensione dettagliata di tutte le procedure previste. Attualmente sono operative sette Linee Guida:

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

La LGP1, dopo aver introdotto il concetto di Schema nazionale, di sicurezza IT e di accreditamento dei laboratori, affronta una descrizione sintetica del processo di valutazione, identificando le finalità e i requisiti generali per svolgere una valutazione e certificazione di un sistema/prodotto o Profilo di Protezione (PP). Nella terminologia OCSI, il sistema, il prodotto o il profilo di protezione che deve essere valutato e certificato viene sinteticamente denominato "Oggetto della Valutazione" (ODV). Successivamente, nella LGP1 vengono definiti e descritti i ruoli dei soggetti coinvolti nel processo di valutazione e certificazione, con particolare enfasi per l'Organismo di Certificazione, il Laboratorio per la Valutazione della Sicurezza, il Committente, il Fornitore e l'Assistente. Inoltre, vengono delineate le tre fasi che caratterizzano il processo di valutazione: la preparazione, la conduzione e la conclusione. Infine, viene delineata la fase di certificazione e si forniscono delle informazioni per quanto concerne la gestione dei Certificati e il loro mantenimento.

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 Laboratorio per la Valutazione della Sicurezza informatica secondo lo Schema nazionale per la valutazione e certificazione della sicurezza nel settore della tecnologia dell'informazione. Inoltre, vengono specificati gli ambiti di attività di un Laboratorio per la Valutazione della Sicurezza 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 sistema/prodotto o di un Profilo di Protezione, così come definiti in ITSEC o 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.

LGP4-Attività di valutazione secondo i Common Criteria

La LGP4 si prefigge l'obiettivo di definire la terminologia di riferimento in lingua italiana per descrivere, discutere e analizzare l'insieme minimo di unità di lavoro in cui possono essere decomposte le azioni di valutazione richieste per svolgere la valutazione di un Profilo di Protezione e la valutazione di un sistema/prodotto ai livelli di garanzia EAL1, EAL2, EAL3 e EAL4 secondo i Common Criteria. Tutti i punti relativi alla valutazione di un ODV o di un Profilo di Protezione contenuti nella LGP4 sono stati sviluppati tenendo conto dello stato della normativa a gennaio 2004.

La LGP4 contiene 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 for-

nisce 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.

LGP5-Il Piano di Valutazione: indicazioni generali

La LGP5 fornisce ai Valutatori gli elementi fondamentali per definire, in base ai Criteri di valutazione ITSEC e Common Criteria, un Piano Di Valutazione (PDV) della Sicurezza di un sistema/prodotto o di un Profilo di Protezione. Il PDV è il documento che contiene la descrizione di tutte le attività che i Valutatori debbono eseguire durante la valutazione e le modalità secondo le quali queste attività risultano organizzate, pianificate, correlate e suddivise nell'ambito del periodo di valutazione.

La necessità di fornire delle istruzioni per la definizione di un PDV nasce dall'esigenza di soddisfare più requisiti, quali:

- armonizzare tutta la documentazione e le procedure di valutazione alla normativa internazionale e nazionale in vigore;
- rendere omogenei e confrontabili i PDV prodotti da Laboratori per la Valutazione della Sicurezza diversi;
- garantire, mediante il rispetto delle Linee Guida, l'obiettività, l'imparzialità, la ripetitività e la riproducibilità delle attività di valutazione indicate in un PDV.

LGP6-Guida alla scrittura dei Profili di Protezione e dei Traguardi di Sicurezza

Nella LGP6 sono fornite indicazioni per la scrittura dei Profili di Protezione (PP) e dei Traguardi di Sicurezza (TDS) secondo le norme fissate dai Common Criteria.

Questa LGP è indirizzata principalmente a coloro che sono coinvolti nello sviluppo dei PP/TDS. Tuttavia, può anche essere utile ai Valutatori e ai responsabili della definizione e del controllo della metodologia per la valutazione dei PP/TDS. Gli utenti finali possono

altresì trovare utile questo documento per comprendere i PP/TDS o per individuare le parti di loro interesse.

Viene dapprima fornita una panoramica sui PP/TDS, che comprende un indice di riferimento; vengono quindi descritte in dettaglio le sezioni del PP/TDS.

Infine, sono riportate alcune appendici che approfondiscono aspetti di particolare rilievo, tra cui la descrizione di esempi di minacce, politiche di sicurezza, assunzioni e obiettivi di sicurezza, e l'identificazione di adeguati componenti funzionali per specificare i requisiti funzionali di sicurezza.

LGP7-Glossario e terminologia di riferimento

Nella LGP7 sono raccolte tutte le definizioni in uso nello Schema nazionale. Inoltre, è fornito un elenco di termini di uso comune che assumono un significato specifico nei Common Criteria

2.4.1 L'iter di certificazione

Come riportato in dettaglio nella LGP3, l'iter di certificazione è composto da due fasi: quella di valutazione e quella di certificazione.

La fase di valutazione comprende le seguenti attività:

- *Preparazione*. La fase di preparazione vede coinvolti il Committente e l'LVS, che esamina il Traguardo di Sicurezza (TDS) o il PP del Committente e produce un Piano di Valutazione (PDV), dettagliando come deve essere effettuata la valutazione. I Valutatori produrranno anche un elenco di materiali per la valutazione, individuando la documentazione necessaria e l'eventuale supporto richiesto al Fornitore dell'ODV. Prima di definire un rapporto contrattuale, il Committente e l'LVS potranno contattare, sia pure in modo informale, l'OC per accertare la possibilità di condurre la valutazione nell'ambito dello Schema. Una volta definito l'accordo tra Committente e

LVS, quest'ultimo deve sottoporre una richiesta perché la valutazione sia formalmente accettata nello Schema. A tal fine, l'LVS sottopone all'OC

- un TDS o un PP completo;
- un PDV completo;
- una descrizione dell'estensione e della natura dell'attività di preparazione svolta con il Committente, compresi i nomi delle persone coinvolte;

- *Conduzione*. La fase di conduzione inizia quando l'OC, esaminato il materiale ricevuto, approva il PDV e accetta formalmente la valutazione nello Schema. L'OC, l'LVS e il Committente devono rispettivamente designare un responsabile per ogni valutazione. Nel corso della fase di conduzione possono essere prodotti rapporti di vario tipo:
  - Rapporti di Attività (RA)
  - Rapporti di Osservazione (RO)
  - Rapporti di Osservazione sullo Schema (ROS)
  - Rapporto delle Metodologie (RM)
- *Conclusione*. Nella fase di conclusione della fase di valutazione, l'LVS produce un Rapporto Finale di Valutazione (RFV) che riassume tutti i risultati ottenuti durante la valutazione e che verrà utilizzato dall'OC come base per la stesura del Rapporto di Certificazione.

La fase di certificazione prevede, nella sua parte iniziale, la revisione dell'RFV da parte dell'OC. Terminata questa parte, l'OC è nella condizione di produrre il Rapporto di Certificazione e il Certificato. Entro trenta giorni dall'approvazione dell'RFV, l'OC redige una bozza di Rapporto di Certificazione (RC), che invia all'LVS e al Committente per avere conferma dell'assenza di errori materiali e della volontà dello stesso di ottenere il rilascio del Rapporto di Certificazione e del relativo Certificato, nonché dell'assenza di elementi che contengano informazioni riservate. L'LVS e il Committente si pronunciano sulla richiesta entro i successivi cinque giorni. Acquisita

la conferma da parte dell'LVS e del Committente l'OC emette entro i successivi trenta giorni il Rapporto di Certificazione. Tale rapporto riassume i risultati della valutazione e contiene commenti e raccomandazioni da parte dell'OC. L'RC non deve contenere informazioni riservate, può essere utilizzato esclusivamente dall'OC e dal Committente e reso pubblico solo integralmente. In caso di valutazione positiva, l'OC allega all'RC il relativo Certificato, cioè l'attestazione che l'ODV o il PP è stato valutato da un LVS accreditato in conformità con i criteri di valutazione (CC/ITSEC) e con le procedure dello Schema. Il Certificato si applica soltanto alla specifica versione dell'ODV o del PP nella configurazione valutata ed attesta che il livello di garanzia richiesto è stato raggiunto, facendo esplicito riferimento al TDS o al PP e all'RC.

2.4.2 Validità dei certificati emessi dall'OCSI in ambito internazionale

I certificati di sicurezza rilasciati da un organismo di certificazione che fa riferimento ai Common Criteria possono essere riconosciuti a livello internazionale a patto che l'organismo stesso abbia sottoscritto il Common Criteria Recognition Arrangement (CCRA) e si sia sottoposto a un processo di valutazione effettuato dagli attuali membri del CCRA stesso.

I principali obiettivi dei firmatari CCRA sono:

- Assicurarsi che le valutazioni dei sistemi/prodotti e dei Profili di Protezione siano effettuate secondo modalità che contribuiscano in modo significativo ad aumentare la sicurezza IT;
- Aumentare la disponibilità di sistemi/prodotti e Profili di Protezione valutati
- Evitare la duplicazione di valutazioni degli stessi sistemi/prodotti e Profili di Protezione

Attualmente l'Italia ha sottoscritto il CCRA impegnandosi a

riconoscere i certificati di sicurezza emessi da altri organismi di certificazione, ma non si è ancora sottoposta al processo di valutazione richiesto dal CCRA. Per aggiornamenti rispetto a tale argomento si rimanda al sito dell'OCSI (www.ocsi.gov.it)

3 Le tipologie di certificazione di sicurezza

3.1 Certificazione di processo secondo gli standard tipo ISO27001

Di solito quando si ragiona intorno agli standard ISO/IEC 17799-1:2005 e ISO/IEC 27001:2005, ci si riferisce genericamente allo "standard BS7799". Questo perché quando nel 1998 il BSI (British Standards Institution) pubblicò la seconda parte, erano già trascorsi tre anni dalla pubblicazione della prima, tre anni in cui lo standard si era imposto come una delle più importanti novità nel settore della sicurezza delle informazioni. Un successo che nel 2000 ha condotto la prima parte allo status di standard ISO, e che nel 2002 ha comportato un significativo aggiornamento della seconda parte, con particolare riguardo all'approccio metodologico. Grazie alle novità del 2002, lo "standard BS7799" può essere ora considerato appartenente alle norme che regolano i "sistemi di gestione". Le altrettanto importanti novità del 2005 (vedi par. "Le principali differenze tra BS7799-2:2002 e ISO/IEC 27001:2005") rafforzano la precedente considerazione e porteranno all'abbandono della denominazione BS7799 in favore di quella più estesa della serie 27000.

3.1.1 Storia

Agli inizi degli anni 90', il DTI (Department of Trade and

Industry) britannico ha istituito un gruppo di lavoro, in risposta ad un'esigenza emersa in ambito industriale, finalizzato a fornire alle aziende una guida per il governo della sicurezza del loro patrimonio informativo. Il gruppo ha pubblicato nel 1993 una raccolta di "best practice" (Code of Practice for Information Security Management) che costituì la base per lo standard britannico BS7799 pubblicato dal BSI (British Standard Institution) nel 1995. Nel 1998 fu aggiunta una seconda parte allo standard (Specification for Information Security Management Systems) che fu poi sottoposto ad una revisione complessiva conclusasi con la pubblicazione, nell'aprile del 1999, di una nuova versione delle sue due parti. Lo standard BS7799 riguarda nominalmente ogni forma di gestione dell'informazione, pur essendo stato redatto tenendo al centro dell'attenzione la gestione mediante il mezzo informatico. Chi ha redatto lo standard, comunque, ha tenuto ben presente che, secondo un approccio ormai universalmente affermato, per implementare un sistema di gestione della sicurezza delle informazioni è indispensabile creare ben precise condizioni: la sicurezza dell'informazione si ottiene mediante la realizzazione di un insieme di misure logiche, organizzative e fisiche che nel loro complesso riducono i rischi cui sono sottoposte le informazioni.

Nel 1995 la Gran Bretagna sottopose lo standard BS7799 all'ISO/IEC JTC1 SC27 (il sotto-comitato 27 del Joint Technical Committee 1 attivo nell'ambito di International Organization for Standardization/ International Electrotechnical Commission) affinché venisse approvato come standard ISO ma, seppure di stretta misura, la proposta non fu accettata. Nel frattempo però l'Australia, la Nuova Zelanda e l'Olanda svilupparono schemi nazionali di certificazione basati sullo standard BS7799 e l'interesse intorno a tale standard crebbe anche in molti altri paesi (tra i quali: Brasile, Danimarca, Giappone, Norvegia, Polonia, Sud Africa, Svezia, Svizzera, ecc.) tanto che la proposta di trasformarlo in uno standard internazionale è stata nuovamente presentata all'ISO nell'autunno del 1999 e la parte 1 dello standard BS7799 è divenuta uno standard internazionale ISO (ISO17799-1) alla fine del 2000. La parte 2 è stata aggiornata nel 2002 (diventando standard BS7799-2:2002) soprattutto per quanto riguarda l'approccio: questa revisione prevede chiari punti di contatto con ISO9001:2000. Nel giugno 2005 è stata pubblicata una revisione della prima parte: ISO/IEC 17799:2005. Alla fine del 2005 è stata pubblica-

ta la versione ISO della BS7799 Parte 2 che ha preso la denominazione di ISO/IEC 27001. Tale versione prevede la riorganizzazione degli annessi e alcuni cambiamenti che permettono di chiarire e migliorare i requisiti relativi al processo PDCA (Plan, Do, Check, Act). La nuova denominazione rivela la definizione di una nuova serie, la 27000, interamente dedicata ai sistemi di gestione della sicurezza delle informazioni. Nei prossimi anni è in programma la pubblicazione delle seguenti norme:

- ISO/IEC 27000 Principi & Vocabolario (in fase di sviluppo);
- ISO/IEC 27001 Requisiti per i ISMS (basata su BS7799-2);
- ISO/IEC 27002 (ISO/IEC 17799:2005, prenderà tale denominazione nel 2007);
- ISO/IEC 27003 ISMS: gestione dei rischi (in fase di sviluppo);
- ISO/IEC 27004 ISMS: metrica e misurazione (prevista per il 2007);
- ISO/IEC 27005 ISMS: guida per l'attuazione (prevista per il 2007);
- ISO/IEC 270006 … ISO/IEC 27010 da definire.

Da notare che prima e seconda parte saranno invertite, come è giusto che sia se si considera che la 27001 specifica il modello e elenca i controlli, mentre la 27002 riporterà una descrizione più approfondita dei controlli stessi.

La tabella che segue sintetizza la storia dello standard

	1995	1998	1999	2000	2002	2005	2007 in avanti
Standard unico	BS7799						
Parte 2		BS7799 2:1998	BS7799 2:1999		BS7799 2:2002	ISO/IEC 27001	
Parte 1			BS7799 1:1999	ISO/IEC 17799 - 1:2000		ISO/IEC 17799 - 1:2005	ISO/IEC 27002
Gestione dei rischi							ISO/IEC 27003
Metrica e misurazione							ISO/IEC 27004
Guida per l'attuazione							ISO/IEC 27005

3.1.2 Lo standard ISO/IEC 27001:2005 e il modello PDCA

Lo standard ISO/IEC 27001:2005 è basato sul modello PDCA (Plan, Do, Check, Act), ovvero progettare, implementare e utilizzare, controllare e revisionare, aggiornare e migliorare (nel senso di effettuare eventuali azioni correttive). Il modello PDCA, conosciuto anche come ciclo di Deming, è anche alla base delle norme internazionali sui sistemi di gestione (ISO9001:2000; ISO 14001:2004; OHSAS 18001:1999). In entrambi i contesti l'approccio è quello dell'analisi "per processi", e uno degli obiettivi principali è l'implementazione di un sistema di gestione ciclico capace di migliorare continuamente i processi gestiti. La frase di Bruce Schneier "la sicurezza non è un prodotto ma un processo" è ormai celebre tra le persone che si occupano di sicurezza informatica, e molto spesso viene messa in relazione con lo "standard BS7799" che mette al centro dell'attenzione tutti quei processi che concorrono alla gestione della sicurezza delle informazioni. Tale approccio per processi è esplicitamente definito in ISO/IEC 27001:2005 che definisce anche i concetti fondamentali di Sistema di Gestione della Sicurezza dell'Informazione (ISMS, che è l'acronimo di Information Security Management System) e di Politica di Sicurezza.

L'ISMS viene definito come quell'insieme di responsabilità, ruoli organizzativi, modalità operative, procedure, istruzioni di lavoro, tecnologie e ambienti fisici che consentono ad un'organizzazione di tenere sotto controllo e di migliorare la sicurezza delle informazioni, adeguando continuamente le proprie componenti all'evoluzione tecnologica, in armonia con la Politica di Sicurezza.

I sistemi di gestione definiti secondo questi principi sono in grado quindi di mantenere e migliorare nel tempo le proprie caratteristiche. Una certificazione secondo uno standard basato su questi principi non solo fornisce garanzie sul sistema di gestione così come è stato verificato al momento della certificazione ma fornisce anche garanzie sul futuro del sistema, posto che le previste verifiche periodiche accertino che il meccanismo di revisione continua sia in atto.

Il modello PDCA raccomandato è costituito da quattro fasi:

- Progettare: stabilire la politica di sicurezza, gli obiettivi, i

processi e le procedure rilevanti per la gestione del rischio e per il miglioramento della sicurezza delle informazioni, secondo le politiche e gli obiettivi dell'organizzazione.

- Implementare e utilizzare: implementare e utilizzare la politica di sicurezza, i controlli, i processi e le procedure.
- Controllare e revisionare: valutare e, dove applicabile, misurare le prestazioni dei processi di sicurezza rispetto alla politica di sicurezza, agli obiettivi e all'esperienza pratica; riferire i risultati alla direzione per la revisione.
- Aggiornare e migliorare: intraprendere azioni correttive e preventive basate sui risultati della revisione della direzione, allo scopo di ottenere il miglioramento continuo dell'ISMS.

La figura seguente, estratta dall'introduzione della norma ISO/IEC 27001: 2005, illustra il modello.

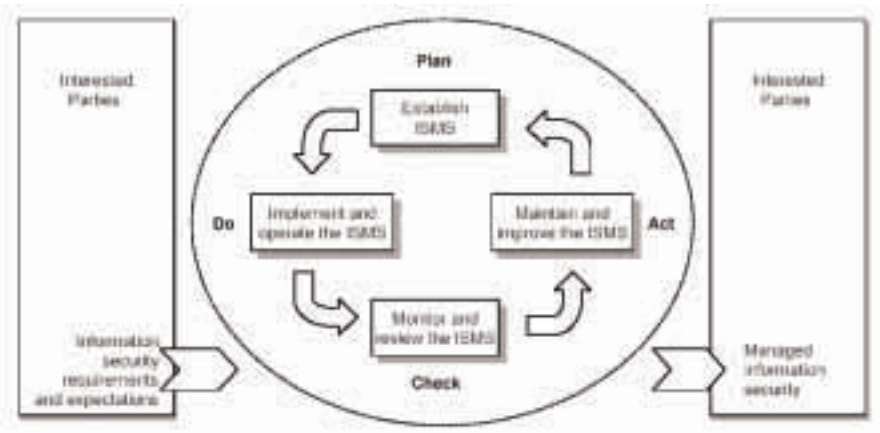


Figure 1 — PDCA model applied to ISMS processes

I riferimenti ad altri sistemi di gestione (basati sul modello PDCA) già presenti in BS7799-2:2002 sono stati posti in maggiore evidenza nella versione del 2005. In sintesi, alle organizzazioni che hanno già in essere un sistema di gestione e che vogliano definirne uno ulteriore rispetto ad un altro standard, si raccomanda di gestirli tutti in

maniera coordinata. In altre parole è ormai possibile definire un unico sistema di gestione che faccia contemporaneamente riferimento a: ISO/IEC 27001:2005, ISO 9001:2000, ISO 14001:2004. L'Annesso C allo standard ISO/IEC 27001:2005 è dedicato alle corrispondenze tra i tre standard appena citati.

L'annesso A della 27001 è dedicato all'elenco dei controlli (specificati in maggiore dettaglio in ISO/IEC 17799:2005, la futura 27002), mentre l'annesso B enuncia i principi definiti nelle linee guida OECD (Organization for Economic Co-operation and Development) sulla sicurezza nei sistemi informativi e nelle reti (OECD Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security, Paris: OECD, July 2002. www.oecd.org).

La norma BS7799-2:2002 dedicava uno degli annessi (Annex B - informative) ad una guida per l'utilizzo che descrive i documenti da redigere e le attività da svolgere affinché il modello PDCA possa essere applicato seguendo le quattro fasi previste. In futuro, lo standard "ISO/IEC 27005 ISMS: guida per l'attuazione" (previsto per il 2007) sarà interamente dedicato all'argomento.

Nel seguito, sono descritte le attività previste nel corso delle quattro fasi del ciclo PDCA.

3.1.2.1 Fase "Progettare"

La progettazione del ciclo PDCA prevede che:

- sia definita la Politica di Sicurezza;
- siano individuati ambito e frontiera dell'ISMS rispetto all'organizzazione che lo include;
- siano identificati e misurati i rischi della sicurezza delle informazioni;
- sia sviluppato un piano per il trattamento di questi rischi[13].

13 La principale misura di controllo per i rischi relativi alla Security delle Informazioni è la consapevolezza delle risorse umane aziendali e la loro competenza in materia

La definizione dell'ambito è fondamentale e la norma richiede che le eventuali esclusioni (rispetto all'intera organizzazione) siano motivate. Se l'ambito della certificazione corrisponde ad una parte dell'organizzazione, è necessario che presenti caratteristiche di omogeneità in termini di processi, siti fisici e missione; la frontiera e le interfacce devono essere ben definite. Tutti i passi dell'attività di pianificazione devono essere documentati per mantenere la tracciabilità e per gestire i cambiamenti.

Politica di Sicurezza delle Informazioni

L'organizzazione deve definire la Politica di Sicurezza delle Informazioni ed assegnare le responsabilità per la sicurezza delle informazioni, tenendo conto dei requisiti legali e normativi, e della missione dell'organizzazione stessa.

In ISO/IEC 27001:2005 si chiarisce in una nota (par. 4.2.1) che nell'ambito di questo standard la politica di sicurezza riferita all'ISMS, oggetto della certificazione, deve contenere la Politica di Sicurezza delle Informazioni dell'organizzazione.

Ambito dell'ISMS

L'ISMS può riguardare tutta l'organizzazione o una o più parti di essa (suddivisione a volte necessaria per facilitare la gestione del rischio). Per tale ragione è importante stabilire i confini entro cui l'ISMS è inserito in termini di organizzazione, localizzazione dei beni e tecnologie.

L'ambito dell'ISMS deve specificare:

- i processi inclusi nell'ambito;
- il contesto strategico e organizzativo;
- l'approccio dell'organizzazione alla gestione del rischio relativo alla sicurezza delle informazioni;
- i criteri per la valutazione del rischio e il grado di fiducia richiesto;
- l'identificazione dei beni appartenenti all'ambito.

Identificazione e valutazione del rischio

I documenti relativi alla valutazione del rischio devono illustrare l'approccio, la metodologia e le tecniche scelte per tale attività. Devono essere documentate le motivazioni che hanno spinto a tali scelte, evidenziando la coerenza con i requisiti di sicurezza, con la missione e la dimensione dell'organizzazione e con i rischi da affrontare. L'approccio adottato deve prevedere un'efficace gestione degli impegni e delle risorse sia dal punto di vista economico che organizzativo.

Un'appropriata valutazione del rischio prevede:

- l'identificazione dei beni e la stima del loro valore, che deve essere calcolato in funzione del business sotteso e non solo dei parametri di inventario;
- l'identificazione delle minacce e delle vulnerabilità associate a questi beni;
- la valutazione delle minacce potenzialmente in grado di sfruttare le vulnerabilità, e degli impatti conseguenti agli eventuali danni causati;
- il calcolo del rischio basato su tali valutazioni e l'identificazione del rischio residuo;
- la confrontabilità dei risultati ottenuti mediante differenti metodologie di analisi (esplicitamente richiesta in ISO/IEC 27001:2005);
- la riproducibilità dei risultati (esplicitamente richiesta in ISO/IEC 27001:2005).

Piano del trattamento del rischio

L'organizzazione deve definire un piano di trattamento del rischio che mostri per ogni rischio identificato:

- il metodo scelto per il trattamento del rischio (accettazione, trasferimento, riduzione);
- i controlli che sono già implementati;
- i controlli addizionali raccomandati a seguito della valutazione del rischio;
- i tempi entro cui si pensa di implementare tali controlli.

Il piano si basa sull'identificazione del livello di rischio accettabile. Per ogni rischio si deve agire secondo una delle seguenti strategie:

- accettare il rischio, ad esempio perché altre azioni non sono possibili o risultano troppo dispendiose;
- trasferire il rischio (verso una terza parte o un'assicurazione);
- ridurre il rischio (mediante l'implementazione delle misure raccomandate).

Allo scopo di individuare quale sia il livello di rischio accettabile per l'organizzazione, è necessario effettuare un bilancio tra i costi di implementazione legati ai controlli che l'analisi del rischio raccomanda, e l'impatto che deriverebbe dal verificarsi degli eventi dannosi.

Dichiarazione di Applicabilità

La fase "Progettare" prevede infine l'elaborazione della Dichiarazione di Applicabilità (Statement of Applicability, o SOA in inglese) che deve includere l'elenco dei controlli della norma in cui si specificano e si motivano le scelte e le eventuali esclusioni. Tale documento riassume le scelte fatte nel corso della fase di pianificazione.

3.1.2.2 Fase "Implementare e utilizzare"

La fase di implementazione del ciclo PDCA prevede la realizzazione dei controlli selezionati durante la fase di pianificazione e la realizzazione delle strategie necessarie per gestire i rischi (accettazione, trasferimento, riduzione) che mettono in pericolo la sicurezza delle informazioni. Ciò si realizza tramite:

- la scelta di personale adeguato da coinvolgere nell'ISMS mediante la formazione e la sensibilizzazione sulla gestione del rischio e sulla cultura della sicurezza;
- lo stanziamento di risorse, in termini di tempo e denaro, adeguate all'implementazione dei controlli;

- il trattamento del rischio relativamente all'implementazione dei controlli corrispondenti ai rischi definiti in riduzione, e alla messa in atto delle modalità di trasferimento (contratti con terze parti, stipula di polizze assicurative, ecc.);
- formazione continua delle risorse umane sul tema della Security;
- la definizione di una metrica per l'efficacia dei controlli selezionati.

L'ultimo punto rappresenta una delle più rilevanti novità presenti in ISO/IEC 27001:2005, ed è da mettere in diretta correlazione con ISO/IEC 27004 ISMS: metrica e misurazione (prevista per il 2007). La misura dell'efficacia è pensata per permettere ai manager e al personale coinvolto nell'ISMS di determinare quanto i controlli sono in grado di raggiungere gli obiettivi.

3.1.2.3 Fase "Controllare e revisionare"

In questa fase si verifica che i controlli siano effettivamente operativi come previsto, e che l'ISMS sia efficace. Eventuali modifiche nelle assunzioni o nell'ambito della valutazione del rischio devono essere prese in considerazione in modo da individuare i controlli che non sono più adeguati e le eventuali azioni correttive. L'esecuzione di tali azioni è prevista nella fase successiva.

ISO/IEC 27001:2005 chiede anche di misurare l'efficacia dei controlli secondo la metrica definita nella fase precedente. La nuova versione inoltre pone maggiore enfasi sulla gestione degli incidenti.

L'attività di controllo dipende dalle caratteristiche del ciclo PDCA considerato. Alcuni esempi di controllo e revisione sono:

- controlli di routine, da effettuarsi con una certa frequenza, al fine di controllare i processi, prevenire eventuali errori nei risultati e limitare i danni (riconciliazione di conti correnti bancari, verifica dell'inventario, risoluzione dei reclami dei clienti, ecc.);
- ricerca di informazioni concernenti altre organizzazioni

che hanno problemi, tecnologici e gestionali, analoghi a quelli della propria organizzazione, che sono però in grado di risolverli in modo più efficace; ad esempio, si può imparare dagli altri sia in termini di efficacia nell'aggiornamento del software, sia di tecniche gestionali che possono essere di aiuto per accelerare la soluzione dei problemi;

- audit interno da effettuarsi in un periodo di tempo predefinito (non più di un anno) per verificare che tutti gli aspetti del ISMS funzionino come stabilito. La direzione deve garantirsi che esistono evidenze sulle seguenti questioni:
  - la politica di sicurezza delle informazioni rifletta ancora i requisiti dettati dalla missione dell'organizzazione;
  - la metodologia di valutazione del rischio che si sta usando sia appropriata;
  - le procedure documentate siano seguite in modo da incontrare gli obiettivi desiderati;
  - i controlli tecnici (firewall, controlli di accesso fisico, ecc.) siano installati, configurati correttamente e funzionino come previsto;
  - i rischi residui siano stati correttamente valutati e siano ancora accettabili per la direzione;
  - le azioni definite nel corso degli audit e delle revisioni precedenti siano state implementate;
  - il ISMS sia conforme allo standard BS7799-2:2002.

3.1.2.4 Fase "Aggiornare e migliorare"

L'attività svolta durante questa fase è diretta conseguenza dei risultati della precedente fase "Controllare e revisionare". Tali risultati possono portare a individuare una "non conformità" o a effettuare "azioni correttive" che potrebbero avere come conseguenza la definizione di attività relative alle fasi "Progettare" e "Implementare e utilizzare".

Può considerarsi una non conformità:

- l'assenza, la fallita implementazione o il fallito mantenimento di uno o più requisiti dell'ISMS;
- una situazione che sulla base di prove oggettive porta ad avere dubbi significativi sulla capacità dell'ISMS di soddisfare la politica di sicurezza delle informazioni e gli obiettivi di sicurezza.

Una volta identificata una non conformità è importante capire la causa che l'ha originata in modo da evitare il ripetersi della situazione critica e le eventuali ripercussioni sull'intero equilibrio nel medio e lungo termine.

Le azioni correttive devono essere proporzionate alla gravità della non conformità e al rischio che l'ISMS non verifichi i requisiti specificati.

3.1.3 Best Practice per l'introduzione dell'ISMS in una Organizzazione

Di seguito viene presentata una panoramica delle Best Practice legate alla introduzione degli ISMS all'interno di un'Amministrazione, Ente o Azienda[14].

Queste sono presentate come raccomandazioni di carattere generale contenenti fattori di indirizzo strutturale che sono determinanti per il successo delle attività di implementazione degli ISMS.

3.1.3.1 Ottenere il commitment del Top Management per l'introduzione dell'ISMS

Un programma per la gestione della sicurezza delle informa-

14 Le best Practice sono state raccolte dalla esperienze sul campo dei componenti del Gruppo di Ricerca dell'AIEA sugli ISMS e contenute nel White Paper "Information Security Management System. Un valore aggiunto per le aziende", pubblicato dall'AIEA a giugno 2005.

zioni ha conseguenze sull'intera organizzazione: coinvolge persone, tecnologie, processi, procedure, comporta la presa di decisioni di ordine strategico e l'impegno di adeguate risorse economiche.

Questo potrebbe generare resistenze al cambiamento dovute a barriere di natura culturale, organizzativa ed economica.

Per superarle, è fondamentale disporre di un forte commitment da parte del vertice che comunichi a tutta l'organizzazione il fermo convincimento e la determinazione nel raggiungere i risultati stabiliti dal programma di sicurezza.

3.1.3.2 Diffondere, al proprio interno e a tutti gli stakeholder, la cultura della sicurezza delle informazioni e l'importanza degli ISMS

E' fondamentale far crescere, in tutti coloro che trattano ed utilizzano informazioni, sia internamente sia all'esterno (clienti, fornitori, terze parti), la consapevolezza circa:

- la presenza delle minacce che gravano sul patrimonio informativo e dei conseguenti potenziali impatti;
- l'importanza del rigoroso rispetto delle policy, delle norme e delle procedure di sicurezza vigenti;
- la rilevanza del contributo dei singoli nel prevenire il verificarsi di eventi anomali ed incidenti al fine di innalzare il livello complessivo di protezione dei dati e delle informazioni.

3.1.3.3 Calcolare il valore degli Information Asset

Le Amministrazioni, gli Enti o le aziende utilizzano dati ed informazioni di cui spesso non riescono ad acquisire consapevolezza del valore economico. Classificare ed elevare a valore il patrimonio da difendere costituisce un passo preliminare di fondamentale importanza per abilitare il processo di protezione. Occorre responsabilizzare gli 'owner' di dati e informazioni affinché associno un valore monetario

agli information asset di competenza.

3.1.3.4 Nel condurre l'analisi dei rischi valutare sempre la gravità del danno potenziale in termini di impatto economico

E' indispensabile condurre regolarmente l'Analisi dei Rischi gravanti sugli information asset del patrimonio aziendale.

Ma per avviare un sistema di sicurezza efficace e giustificabile dal punto di vista economico, è necessario che l'Analisi dei Rischi sia corredata con una analisi di impatto che evidenzi per ogni minaccia il valore economico esposto a rischio (Business Impact Analysis)

3.1.3.5 Tenere conto degli impatti legati ad eventuali esternalizzazioni di attività o ad attività di 'merging/acquisition'.

Nel disegno degli ISMS occorre tenere conto degli impatti derivanti da eventuali operazioni di 'merging/acquisition' e di 'outsourcing'.

Al fine di non creare pericolose discontinuità nella gestione della sicurezza è necessario assicurare che le funzionalità ed i requisiti degli ISMS si adeguino al nuovo contesto organizzativo.

Negli accordi contrattuali con terze parti debbono essere inoltre introdotti specifici riferimenti al rispetto del framework dell'ISMS adottato e dei relativi indici di performance definiti (Security Service Level Agreement).

3.1.3.6 Valutare i benefici legati all'introduzione degli ISMS

Valutare i risultati economici conseguibili con l'introduzione degli ISMS. Utilizzare indicatori che consentono di rapportare gli investimenti effettuati in sicurezza a misure quali:

- il valore economico degli asset sottratto al rischio di perdita;
- l'incremento delle performance del Business conseguenti l'adozione del sistema di protezione.

3.1.3.7 Disegnare ed implementare gli ISMS partendo dalle esigenze e dalle caratteristiche delle attività e del business

Gli ISMS devono essere integrati nei processi interni organizzativi e di business. Devono costituire un fattore di miglioramento e non di limitazione o di eccessivo aumento della complessità del processo produttivo.

Se è stato adottato un Sistema di certificazione della Qualità, è opportuno, laddove applicabile, collegare il sistema di gestione della sicurezza delle informazioni al Sistema di Qualità.

3.1.3.8 Cercare di recepire in maniera organica tutti i vincoli di legge e normativi rilevanti per la sicurezza delle informazioni

Gli ISMS consentono di perseguire la conformità ai vari adempimenti di legge, regolamenti di settore, regole e standard produttivi, razionalizzando i controlli di sicurezza ed evitando duplicazioni e dispendio di risorse umane, tecniche e organizzative.

Molti sono, ad esempio, i requisiti di sicurezza logica imposti dagli Accordi di Basilea, dal Codice in Materia di Protezione dei Dati Personali, dal Decreto Legge sulla Responsabilità Amministrativa,

piuttosto che dal Sistema di Qualità interno: non avrebbe senso mettere in campo strumenti, procedure e controlli 'separatamente' per ciascuno di questi adempimenti.

3.1.3.9 La sicurezza si basa, in larga parte, sulle persone. Tenere conto della rilevanza del fattore umano nel disegno del sistema di gestione della sicurezza

Nel disegno dei sistemi di gestione della sicurezza va posta particolare attenzione agli aspetti legati alla qualità dell'interfaccia con l'uomo: l'usabilità delle tecnologie, l'applicabilità delle procedure ed il disegno razionale dei processi costituiscono fattori critici di successo degli ISMS.

3.1.3.10 Reperire nell'ambito della cultura e dell'esperienza dell'Auditing gli schemi di riferimento per il coordinamento ed il controllo dei sistemi di gestione della sicurezza

Per gli aspetti inerenti la sicurezza delle informazioni il ruolo dell'Internal Auditor non dovrà più essere circoscritto meramente alle sole attività di 'verifica ispettiva' ma è opportuno che si estenda anche alle fasi di costruzione del sistema di gestione, acquisendo un nuovo e rilevante ruolo di 'consulente' all'interno dell'organizzazione per il framework di gestione della sicurezza. Ciò nel consueto rispetto di specifiche procedure e norme di condotta, che garantiscono l'indipendenza e la professionalità dell'auditor.

3.1.3.11 Nell'implementazione degli ISMS procedere per gradi. Partire dagli asset più critici e poi estendere progressivamente il sistema di gestione agli altri asset

Gli ISMS possono essere applicati a domini di riferimento di varia estensione e complessità. In fase iniziale e comunque nel caso di risorse limitate, è opportuno identificare il dominio degli asset più critici e procedere a partire da quello. Man mano che si rendono disponibili nuove risorse e che si consolidano le prassi gestionali si amplierà il campo di applicazione agli altri asset.

Ciò consente di:

- intervenire con priorità sulle situazioni a maggior rischio;
- minimizzare i disagi legati ad una eventuale frammentazione temporale del budget disponibile;
- garantire interventi in linea con la filosofia dell'approccio 'integrato' degli ISMS anche a fronte di disponibilità limitata di risorse;
- rendere graduale l'introduzione delle novità introdotte dall'ISMS nell'organizzazione.

3.1.3.12 Partire con l'obiettivo di mettere in campo un sistema di gestione della sicurezza e una volta realizzato, valutare l'opportunità di certificarlo

E' consigliabile che le organizzazioni mettano in piedi un ISMS in quanto consapevoli dei vantaggi di un sistema di governo della sicurezza. La certificazione offre il vantaggio di un riconoscimento dei risultati raggiunti spendibile internamente ed esternamente.

Mettere in campo un ISMS col solo fine di perseguire la certificazione, ad esempio per fini commerciali, può essere pericoloso. Il rischio è che, una volta ottenuta la certificazione, diminuisca l'attenzione verso la sicurezza; si indebolisce così il "circolo virtuoso" della revisione e del miglioramento continuo con conseguente riduzione dell'efficacia di tutto il sistema di protezione inizialmente messo in campo.

3.1.3.13 Nell'implementazione degli ISMS, curare con attenzione la descrizione dei processi e delle procedure di sicurezza

Privilegiare la chiarezza e la sinteticità rendendo palesi i principi di controllo sottostanti e concordando, con le strutture operative, la descrizione dei flussi di dettaglio per garantire un miglior riscontro operativo delle contromisure pianificate.

I processi di sicurezza debbono essere ben strutturati in relazione allo scopo prefissato, chiari, essenziali, considerati dall'organizzazione come 'scolpiti nella pietra' e parte integrante dei processi di riferimento.

La stabilità, la larga applicabilità e la non derogabilità dei processi di sicurezza costituiscono un fattore fondamentale per il successo del sistema di protezione.

A riprova di ciò e' frequente il caso di policy di sicurezza che arrivano a considerare le violazioni delle procedure o le varianze di processo occorse come 'incidenti di sicurezza'.

3.1.3.14 Nell'analisi dei rischi tenere conto non solo delle minacce correnti ma effettuare anche delle analisi prospettiche individuando i rischi legati a nuove tipologie di minacce

Nell'analisi dei rischi conviene assumere che il futuro sarà sempre più complesso del passato: ad esempio, possono essere già alla porta minacce di cui non abbiamo ancora conoscenza.

Per questo è fortemente consigliabile procedere nell'analisi, non solo valutando i rischi sulla base del nostro corrente set di informazioni disponibili (es.: tabelle standard di minacce, storia degli incidenti occorsi), ma basandosi su attività di previsione che tengano conto di nuove possibili minacce e valutandone, nel contempo, l'ordine d'impatto sull'operatività e le possibili strategie di contrasto.

3.1.3.15 L'implementazione degli ISMS richiede attenzione nelle relazioni internet e nei processi di comunicazione

Una corretta comunicazione circa gli obiettivi legati all'implementazione del sistema di gestione, favorisce un clima di apertura e collaborazione da parte di tutte le componenti interne. Particolarmente prezioso, in tal senso, sono i contributi delle strutture operative: in fase di costruzione dell'ISMS queste non debbono avere la sensazione di divenire unità sotto 'audit'. Va invece instaurata una relazione di tipo 'win-win' facendo comprendere la rilevanza del loro contributo nella costruzione del sistema ed i vantaggi di cui la struttura stessa potrà godere a seguito dell'avvio dell'ISMS. In tal senso può risultare particolarmente utile identificare, per ogni struttura operativa, un referente che assuma il ruolo di 'facilitatore' per le tematiche di sicurezza delle informazioni.

3.1.3.16 Cogliere l'occasione di significativi progetti di change management (es: revisione di applicazioni strategiche, adeguamento delle infrastrutture tecnologiche) per partire con l'avvio o l'ampliamento di un ISMS

L'avvio di un ISMS può comportare revisioni nell'organizzazione, nei processi e nelle infrastrutture dell'ICT.

L'occasione di revisioni tecniche e organizzative, già previste per altre esigenze, può costituire una buona opportunità per introdurre o ampliare gli ISMS, riducendo l'impatto complessivo del programma sia in termini di tempi che di risorse impiegate. Tanto più i requisiti del progetto di costituzione degli ISMS diverranno parte integrante del progetto di change management, tanto più robusto ed affidabile diventerà il sistema di governance della sicurezza.

3.1.4 Lo standard ISO/IEC 17799-1:2005 (dal 2007 ISO/IEC 27002)

La Parte 1 dello standard è un elenco di misure di sicurezza (che lo standard chiama "controls", controlli) di tipo logico, fisico e organizzativo, che costituiscono la prassi corrente adatta a gestire la sicurezza delle informazioni in ambito industriale. Di seguito vengono riportate le categorie che erano presenti nella vecchia versione dello standard, che ne prevedeva 10, e quelle presentate nella nuova versione, che ne prevede invece 11.

Edizione del 2000	Edizione del 2005
Politica per la sicurezza	Politica per la sicurezza
Organizzazione della sicurezza	Organizzare la sicurezza delle informazioni
Classificazione e controllo dei beni	Gestione dei beni
Sicurezza del personale	Sicurezza delle risorse umane
Sicurezza fisica e ambientale	Sicurezza fisica e ambientale
Gestione delle comunicazioni e delle operazioni	Gestione delle comunicazioni e delle operazioni
Controllo accessi	Controllo accessi
Sviluppo e manutenzione del sistema	Acquisizione, sviluppo e manutenzione dei sistemi di informazione
	Gestione degli incidenti inerenti la sicurezza delle informazioni
Gestione della continuità aziendale	Gestione della continuità aziendale
Conformità	Conformità

Queste 11 categorie si articolano in 133 controlli dei quali 9 sono stati modificati rispetto alla vecchia versione e 17 sono nuovi .

Ovviamente, le 11 categorie (e i 133 controlli) corrispondono a quelle indicate in ISO/IEC 27001 (del 2005), mentre le 10 categorie (e i 127 controlli) dell'edizione del 2000 corrispondono a quelle indicate in BS7799-2:2002.

Un'organizzazione che volesse definire un suo regolamento di sicurezza può riferirsi alla "best practice" presentata dallo standard e scegliere l'insieme dei controlli che si adattano alla propria realtà. I controlli prescelti dovranno, pertanto, essere realizzati attraverso:

- meccanismi hardware o software (sistemi di autenticazione tramite password e/o smart-card, prodotti per la protezione crittografica dei dati, firewall, etc.), nel caso dei controlli attuati mediante misure di sicurezza di tipo logico;
- meccanismi quali sistemi anti-intrusione, telecamere, casseforti, contenitori ignifughi, ecc., nel caso dei controlli che richiedono misure di sicurezza fisiche;
- strutture o cariche aziendali create appositamente e precise procedure definite per la messa in atto dei controlli di tipo procedurale (ad esempio l'istituzione del forum aziendale per la gestione della sicurezza dell'informazione, l'affidamento dell'incarico di aggiornamento periodico del personale, le procedure per l'accettazione di visitatori all'interno dell'organizzazione, ecc.).

La revisione del 2005 della ISO/IEC 17799 prevede l'aggiornamento di parte dei controlli allo scopo di adeguare la "best practice" alle nuove realtà aziendali, e di rispondere ai nuovi sviluppi in ambito sia tecnologico sia organizzativo, includendo nuovi controlli gestionali e prassi aggiornate, mantenendo sempre la compatibilità con il passato, e cercando di facilitare l'utilizzazione da parte dell'utente. Infatti, nella vecchia versione dello standard ogni controllo è seguito da una descrizione dalla quale emergono indicazione per l'attuazione. Oggi invece il testo che definisce il controllo è esplicitamente separato dalla guida all'implementazione e da altre informazioni utili (riferimenti ad altri standard e norme).

La novità più importante è relativa alla gestione degli incidenti. Per questa problematica è stata introdotta una nuova categoria che include tutti i controlli pertinenti presenti nella precedente versione dello standard in altre categorie, e prevede aggiornamenti nelle definizioni e nelle guide all'implementazione. L'organizzazione deve poter identificare ed individuare gli incidenti, analizzarli ed essere quindi in grado di reagire e applicare azioni correttive. Facendo tesoro di eventuali incidenti avvenuti, da una lato si deve continuamente controllare,

riesaminare e rivalutare i rischi, dall'altro devono essere intraprese azioni che finalizzate a tenere sotto controllo tali rischi.

Le novità relative alla misura dell'efficacia dei controlli (di cui si è detto al par. 3.1.2.2) e la nuova categoria dedicata alla gestione degli incidenti costituiscono le due fondamentali innovazioni della norma.

3.1.5 Le principali differenze tra BS7799-2:2002 e ISO/IEC 27001:2005

Tale paragrafo è dedicato alla presentazione di una tabella che riassume le principali differenze tra BS7799-2:2002 e ISO/IEC 27001:2005.

BS7799-2:2002 (Paragrafo n°)	ISO/IEC 27001:2005	Commenti e interpretazione sui cambiamenti e sulle differenze
1.2 Application	1.2 Application	Il contenuto e i requisiti in questo paragrafo non sono stati modificati. Tuttavia il paragrafo è stato riorganizzato in modo da mettere in evidenza che non è possibile accettare l'esclusione dei requisiti espressi nei paragrafi 4-8 dello standard ISO/IEC 27001. Si spiegano inoltre le condizioni sotto cui l'esclusione dei controlli è possibile.
3 Terms and definition	3 Terms and definition	Sono state aggiunte nuove definizioni dagli standard. ISO/IEC 13335-1:2004, ISO/IEC TR 18044:2004, ISO/IEC Guide 73:2002.Alcune definizioni già esistenti sono state modificate per allinearle con quelle presenti nello standard ISO/IEC 13335-1:2004. Le definizioni di "risk treatment" e "statement of applicability" sono state modificate per maggiore chiarezza

BS7799-2:2002 (Paragrafo n°)	ISO/IEC 27001:2005 (Paragrafo n°)	Commenti e interpretazione sui cambiamenti e sulle differenze
4.2.1 Establish the ISMS	4.2.1 Establish the ISMS	
a) "Define the scope of the ISMS"	a) "Define the scope and boundaries of the ISMS"	L'aggiunta della parola "boundaries" chiarisce che devono essere definiti l'ambito e i confini del perimetro dell'ISMS per assicurare la presenza di dettagli che giustifichino ogni esclusione dall'ambito, facendo riferimento al paragrafo 1.2 Application di questo standard.
c) "Define a systematic approach to risk assessment"	Nel punto c) è stata cancellata la frase "define the risk assessment approach of the organization" ed è stata aggiunta una nuova frase	È stata cancellata la seconda frase del punto c). Il resto del testo è rimasto invariato con l'aggiunta di una nuova frase che chiarisce ed estende i requisiti esistenti, affermando che il metodo di "risk assessment" selezionato deve produrre risultati comparabili e riproducibili.
g) "Select control objectives and controls for the treatment of risks"	È stato esteso il punto g) "Select control objectives and controls for the treatment of risks"	Questo chiarimento ed estensione del requisito esistente assicura che la selezione tenga conto dei criteri per l'accettazione dei rischi [vedere par. 4.2.1c)] come pure dei requisiti legali, normativi e contrattuali

BS7799-2:2002 (Paragrafo n°)	ISO/IEC 27001:2005	Commenti e interpretazione sui cambiamenti e sulle differenze
h) "Prepare a Statement of Applicability"	Nel punto j) "Prepare a Statement of Applicability" è stato aggiunto un nuovo punto j) 2)	Questo chiarimento ed estensione del requisito esistente, che riguarda lo Statement of Applicability, enfatizza che tale documento deve includere gli obiettivi di controllo e i controlli generalmente implementati. Inoltre c'è un riferimento al paragrafo 4.2.1 punto e) 2).
4.2.2 Implement and operate the ISMS	4.2.2 Implement and operate the ISMS	
	È stato aggiunto il punto d) "Define how to misure the effectiveness"	Questa estensione del requisito relativo all'implementazione e alla realizzazione dell'ISMS, afferma che deve essere definito in che modo si misura l'efficacia dei controlli o dei gruppi di controlli, e che deve essere specificato come queste misurazioni devono essere usate per valutare l'efficacia dei controlli con lo scopo di produrre risultati comparabili e riproducibili.

BS7799-2:2002 (Paragrafo n°)	ISO/IEC 27001:2005 (Paragrafo n°)	Commenti e interpretazione sui cambiamenti e sulle differenze
4.2.3 Monitor and review the ISMS	4.2.3 Monitor and review the ISMS	
a) "Execute monitoring procedures and other controls"	Nel punto a) è stato aggiunto il punto a) 4) "Execute monitoring and review procedures and other controls to detect security events"	Questo chiarimento ed estensione del requisito esistente aiuta a scoprire gli eventi legati alla sicurezza e perciò a prevenire incidenti sulla sicurezza tramite l'uso di indicatori
	È stato aggiunto il punto c) "Measure the effectiveness of controls"	Questa estensione del requisito di monitoraggio e revisione dell'ISMS permette di misurare l'efficacia dei controlli per verificare che i requisiti di sicurezza siano stati soddisfatti.
c) "Review the level of residual risk and acceptance risk"	Nel punto d) è stato aggiunto il punto d) 5) "Review risk assessments at planned intervals and the level of residual risk and acceptable risk, taking into account changes to effectiveness of implemented controls	Questo chiarimento ed estensione del requisito esistente è stato aggiunto per includere l'efficacia dei controlli implementati.

BS7799-2:2002 (Paragrafo n°)	ISO/IEC 27001:2005 (Paragrafo n°)	Commenti e interpretazione sui cambiamenti e sulle differenze
4.3.1 General	4.3.1 General	
	1° paragrafo	Questo chiarimento ed estensione dei requisiti relativi alla documentazione afferma che la documentazione deve includere note relative alle decisioni della direzione. Inoltre deve assicurare che le azioni siano riconducibili alle decisioni dell'organizzazione e alle politiche e che i risultati registrati siano riproducibili.
	2° paragrafo	È stata aggiunta una nuova frase sulla possibilità di dimostrare la coerenza dei controlli selezionati con i risultati del "risk assessment" e del trattamento del rischio, con la politica dell'ISMS e gli obiettivi.
	È stato aggiunto il punto d) "Description of risk assessment methodology"	Questo chiarimento ed estensione dei requisiti relativi alla documentazione assicura che deve essere inclusa nella documentazione una descrizione della metodologia di "risk assessment" [vedere par 4.2.1 c)]

BS7799-2:2002 (Paragrafo n°)	ISO/IEC 27001:2005 (Paragrafo n°)	Commenti e interpretazione sui cambiamenti e sulle differenze
Punto e) "Documented procedures	È stato aggiornato il punto g) "Documented procedures	Questo chiarimento ed estensione del requisito permette di descrive come misurare l'efficacia dei controlli [vedere il par. 4.2.3 c)]
4.3.2 Control of documents	4.3.2 Control of documents	
	È stato aggiunto il punto f) "Ensure that documents are available"	Questo chiarimento ed estensione del requisito esistente permette di controllare i documenti, per assicurare che tali documenti siano disponibili a chi ne ha bisogno e siano trasferiti, memorizzati ed in fine distribuiti in conformità alle procedure applicabili secondo il loro livello di classificazione.
5.1 Management commitment	5.1 Management commitment	
	È stato aggiunto il punto g) "Ensuring that internal ISMS audits are conducted"	Questo chiarimento ed estensione del requisito esistente relativo all'impegno della direzione aziendale permette di assicurare lo svolgimento dell'audit interno dell'ISMS.

BS7799-2:2002 (Paragrafo n°)	ISO/IEC 27001:2005 (Paragrafo n°)	Commenti e interpretazione sui cambiamenti e sulle differenze
Paragrafi 6.1, 6.2, 6.3	Paragrafi 7.1, 7.2, 7.3	Cambio di numerazione
Paragrafi 7.1, 7.2, 7.3	Paragrafi 8.1, 8.2, 8.3	Cambio di numerazione
6.2 Review input	7.2 Review input	Cambio di numerazione
	È stato aggiunto il punto g) "Ensuring that internal ISMS audits are conducted	Questa estensione dell'esistente requisito relativo all'input della revisione permette di includere i risultati delle misurazioni dell'efficacia
6.3 Review output	7.3 Review output	Cambio di numerazione
	È stato aggiunto il punto b) "update of the risk assessment and risk treatment plan"	Questa estensione dell'esistente requisito relativo all'output della revisione permette di aggiornare il "risk assessment" e il piano di trattamento del rischio.
b) "Modification of procedures that effect information security, as necessary, to respond to internal or external events that may impact on the ISMS"	Nel punto c) (ex punto b)) è stato aggiunto il punto c) 5): "Modification of procedures and controls that effect information security, as necessary, to respond to internal or external events that may impact on the ISMS, including changes to contractual obligations"	Questo chiarimento ed estensione dell'esistente requisito di output della revisione permette di includere gli obblighi contrattuali

BS7799-2:2002 (Paragrafo n°)	ISO/IEC 27001:2005	Commenti e interpretazione sui cambiamenti e sulle differenze
	È stato aggiunto il punto e) "Improvement to how the effectiveness of controls is being measured"	Questo è un chiarimento ed una estensione dell'esistente requisito di output dell'analisi che permette di includere il miglioramento di come si sta misurando l'efficacia dei controlli.
6.4 Internal ISMS audits	6 Internal ISMS audits	Cambio di numerazione: "Internal ISMS audits" è stato spostato in un nuovo paragrafo di primo livello. Il testo in questo paragrafo deriva da quello del paragrafo 6.4 del BS7799-2:2002.
7.3 Preventive	8.3 Preventive	Cambio di numerazione
	Punto b) "Evaluating the need for action to prevent occurrence of nonconformities"	Questo chiarimento ed estensione dei requisiti è relativo alle azioni preventive che riguardano la valutazione della necessità di intraprendere azioni di prevenzione del verificarsi di non conformità.
Annex A	Annex A	Questa appendice è stata aggiornata per prendere in considerazione la versione aggiornata dello standard ISO/IEC 17799:2005

BS7799-2:2002	ISO/IEC 27001:2005	Commenti e interpretazione sui cambiamenti e sulle differenze
Annex B e Table B.1	Annex B	La maggior parte del vecchio Annex B è proposto come base di nuove linee guida che devono essere sviluppate da ISO/IEC chiamate "ISMS Implementation Guide" (ISO/IEC 27005) ed è quindi stato rimosso. Solo la tavola che mostra la mappatura tra i principi OECD e questo standard internazionale è rimasta. Questa Tavola forma il nuovo Annex B.
Annex C	Annex C	Questa appendice è stata aggiornata
Annex D		Questa appendice è stata rimossa

3.2 Valutazione e Certificazione di sistema/prodotto secondo lo standard ISO 15408 (Common Criteria)

Come detto in precedenza, i processi di valutazione e certificazione in accordo allo standard dei Common Criteria sono gestiti, in

Italia, dall'Organismo per la Certificazione della Sicurezza Informatica (OCSI). Tutte le considerazioni seguenti riguardanti i vari aspetti della certificazione Common Criteria effettuata dall'OCSI derivano da documenti ufficiali prodotti dall'OCSI stesso e disponibili sul sito www.ocsi.gov.it.

Le considerazioni e le informazioni contenute in questo paragrafo fanno riferimento alla versione 2.2 dei CC, che è stata recepita dallo standard ISO15408, e della relativa metodologia CEM (Common Evaluation Methodology). I CC versione 2.2 sono costituiti da tre parti contenenti, il modello generale, il catalogo dei requisiti funzionali di sicurezza e il catalogo dei requisiti di assurance, rispettivamente. La CEM, invece, è costituita da un solo documento che descrive, appunto, la metodologia di valutazione della sicurezza effettuata in accordo con i CC.

E' ormai in fase di edizione finale la versione 3.1 dei CC che conterrà delle variazioni anche sostanziali su alcuni aspetti anche rilevanti. Per le finalità di questa Linea Guida si ritiene opportuno fare comunque riferimento alla versione 2.2 "ufficiale" al momento e consigliare al lettore una verifica periodica presso il sito dell'OCSI (www.ocsi.gov.it) per gli aggiornamenti.

Tutti i documenti ufficiali dei CC sono riportati nel sito www.commoncriteriaportal.org

3.2.1 Generalità sui Common Criteria

In questo paragrafo ci si limiterà a descrivere l'approccio secondo il quale i CC sono stati sviluppati, mirando principalmente a fornire quegli elementi informativi che consentono una adeguata comprensione delle argomentazioni svolte in questo lavoro.

La filosofia che è alla base dei CC è stata ripresa dai precedenti criteri europei ITSEC (Information Technology Security Evaluation Criteria) che per primi l'hanno introdotta. In base a tale filosofia non ha senso verificare se un sistema/prodotto è sicuro se non si specifica:

- "sicuro" per fare cosa (obiettivi di sicurezza)

- "sicuro" in quale contesto (ambiente di sicurezza)
- "sicuro" a fronte di quali verifiche (requisiti di assurance).

Tra parentesi sono stati indicati alcuni termini che sono utilizzati nell'ambito dei CC e che consentono di esprimere nel seguente modo lo scopo di una valutazione secondo tali criteri: offrire garanzie, che vengono prodotte dal soddisfacimento dei requisiti di assurance e che risultano crescenti con il livello di valutazione, sulla capacità del sistema/prodotto di soddisfare i propri obiettivi di sicurezza nell'ambiente di sicurezza per esso ipotizzato.

Nel contesto dei Common Criteria[15] , con il termine "prodotto" si intende "un insieme di elementi software, hardware e/o firmware che svolge una funzione che può essere utilizzata da molti sistemi ", mentre con il termine "sistema" si intende "una specifica installazione IT (software, firmware o hardware), caratterizzata da uno scopo e da un ambiente operativo ben definiti". Il Profilo di Protezione (PP) è invece "il documento che descrive per una certa categoria di ODV ed in modo indipendente dalla realizzazione, gli obiettivi di sicurezza, le minacce, l'ambiente ed i requisiti funzionali e di fiducia, definiti secondo i Common Criteria. Un PP ha la finalità di definire un insieme di requisiti che si è dimostrato efficace per raggiungere gli obiettivi individuati, sia per quanto riguarda le funzioni di sicurezza, sia per quanto riguarda la garanzia. Un PP fornisce agli utenti uno strumento per fare riferimento ad uno specifico insieme di esigenze di sicurezza, e facilita lo svolgimento di future valutazioni di Prodotti o Sistemi che soddisfino tali esigenze".

Un obiettivo di sicurezza viene definito, secondo i CC, come l'intenzione di contrastare una minaccia o quella di rispettare leggi, regolamenti o politiche di sicurezza preesistenti. Il conseguimento degli obiettivi avviene attraverso l'adozione di misure di sicurezza tecniche (funzioni di sicurezza) e non tecniche (fisiche, procedurali e relative al personale).

L'ambiente di sicurezza viene descritto in termini di:

- uso ipotizzato del sistema/prodotto (applicazioni, utenti,

[15] *Le definizioni successive sono tratte dalla LGP7 emanata dall'OCSI*

informazioni trattate ed altri beni con specifica del relativo valore)

- ambiente di utilizzo (misure di sicurezza non tecniche, collegamento con altri apparati ICT)
- minacce da contrastare, specificando caratteristiche dell'attaccante (conoscenze, risorse disponibili e motivazione), metodi di attacco (citando, tra l'altro, lo sfruttamento di eventuali vulnerabilità note del sistema/prodotto ICT), beni colpiti
- politiche di sicurezza dell'Organizzazione.

Le verifiche previste durante il processo di valutazione mirano ad accertare che siano stati soddisfatti, da parte del sistema/prodotto, del suo sviluppatore e del valutatore, opportuni requisiti di assurance che diventano sempre più severi al crescere del livello di valutazione. I CC definiscono una scala di 7 livelli di valutazione (EAL1, EAL2,..., EAL7) o livelli di assurance, precisando, per ogni livello di tale scala uno specifico insieme di requisiti di assurance. Il livello EAL1, cui corrisponde il livello di sicurezza più basso, non ha corrispondenti nei precedenti criteri di valutazione.

Le verifiche, eseguite in base ai requisiti di assurance del livello di valutazione considerato, hanno lo scopo di fornire garanzie circa:

1. l'idoneità delle funzioni di sicurezza a soddisfare gli obiettivi di sicurezza del sistema/prodotto;
2. l'assenza di errori nel processo che dalle specifiche iniziali di sicurezza (ambiente e obiettivi di sicurezza) porta alla pratica realizzazione delle funzioni di sicurezza (errori di interpretazione delle specifiche tecniche, errori di programmazione, ecc);
3. l'adeguatezza delle procedure di sicurezza previste per la consegna e per l'installazione del sistema/prodotto (per evitare che il sistema/prodotto che perviene all'utente finale possa differire, magari anche di poco, da quello sottoposto a valutazione/certificazione), la chiarezza dei manuali d'uso e d'amministrazione (questi ultimi potrebbero infatti indurre gli utilizzatori a comportamenti che introducono vulnerabilità nell'utilizzo di un

prodotto/sistema dotato di funzioni di sicurezza del tutto idonee e realizzate senza errori), il supporto che lo sviluppatore si impegna a fornire a chi usa il sistema o prodotto per rimediare ad eventuali vulnerabilità emerse dopo la valutazione.

Con riferimento al punto 2) può essere interessante precisare che le garanzie circa l'assenza di errori nel processo di realizzazione delle funzioni di sicurezza non vengono ottenute solamente ricercando direttamente gli errori stessi (analizzando la documentazione presentata dal richiedente della valutazione e sottoponendo il sistema/prodotto a test funzionali e ad attacchi), bensì anche verificando che nel processo di realizzazione sia stato previsto l'impiego di strumenti, metodologie e procedure finalizzati alla riduzione della probabilità di errori.

Al crescere del livello di valutazione:

- vengono richieste specifiche realizzative più dettagliate (ad esempio progetto ad alto livello, progetto a basso livello, codice sorgente)
- il livello di rigore con il quale le specifiche devono essere descritte aumenta (descrizione informale, semiformale, formale).

Il rigore della valutazione, così come nei criteri ITSEC, non viene individuato solo dal livello di valutazione bensì anche da un altro parametro. Infatti per le funzioni che devono essere realizzate con meccanismi probabilistici o di permutazione (password, funzioni hash, ecc.), i CC richiedono (a partire da EAL2) che venga specificato un livello minimo di robustezza (SOF - Strength Of Functionality) su una scala a tre valori (basic, medium, high).

Le funzioni di sicurezza del sistema/prodotto vengono descritte in base ai requisiti cui devono soddisfare. Tali requisiti, denominati requisiti funzionali, così come i già citati requisiti di assurance, devono essere espressi (a meno di possibili eccezioni che occorre comunque giustificare) utilizzando un catalogo di componenti fornito nei CC. Più precisamente il catalogo delle componenti funzionali costituisce la parte 2 dei CC, mentre quello delle componenti di assurance la parte 3. I cataloghi sono strutturati su più livelli gerarchici in modo

da raccogliere componenti di tipo omogeneo. A titolo di esempio, per quanto riguarda le componenti funzionali, al livello gerarchico più elevato è previsto un raggruppamento secondo le 11 classi di seguito specificate: Audit, Communication, Cryptographic Support, User Data Protection, Identification and Authentication, Security management, Privacy, Protection of the TOE Security Function, Resource Utilization, TOE Access, Trusted Path/Channels (l'acronimo TOE ricorrente in alcuni nomi di classi funzionali indica il sistema/prodotto ICT da valutare).

Tra i numerosi documenti che il richiedente della valutazione deve/può consegnare ai valutatori, unitamente al sistema/prodotto ICT da valutare, due meritano un particolare cenno. Il primo, denominato Traguardo di Sicurezza (Security Target), deve essere obbligatoriamente fornito e rappresenta il documento principale della valutazione. Nel Traguardo di Sicurezza devono essere descritti l'ambiente di sicurezza, gli obiettivi di sicurezza, i requisiti funzionali e di assurance (e quindi il livello di valutazione), la robustezza minima delle funzioni di sicurezza ed una prima descrizione ad alto livello delle funzioni di sicurezza. Quest'ultima sezione non è invece contenuta nel secondo documento, il Profilo di Protezione (Protection Profile), che per il resto ha una struttura del tutto simile a quella del Traguardo di Sicurezza. Il Profilo di Protezione può essere opzionalmente sviluppato con riferimento ad un'intera classe di prodotti (per la quale si lascia la libertà di realizzare le funzioni di sicurezza in un qualsiasi modo che soddisfi i requisiti funzionali) piuttosto che con riferimento ad uno specifico sistema/prodotto ICT (come è il caso, invece, del Traguardo di Sicurezza). Il Profilo di Protezione può essere registrato e anche valutato per verificarne la coerenza interna.

3.2.2 Vantaggi e svantaggi dei Common Criteria

In questo paragrafo verranno descritti i principali vantaggi e svantaggi derivanti dall'applicazione dei CC. In realtà, come apparirà più chiaro nel seguito, gran parte di essi possono essere considerati

comuni a tutte le raccolte di criteri di valutazione fin qui sviluppate. Per quanto riguarda i vantaggi si possono citare:

1. la verifica, eseguita da una terza parte per la quale viene riconosciuto il possesso di conoscenze specialistiche, che le funzionalità di sicurezza del sistema/prodotto ICT, affiancate alle contromisure non tecniche previste, siano adeguate al soddisfacimento degli obiettivi di sicurezza;
2. lo svolgimento di un'azione di contrasto preventivo degli incidenti di sicurezza ICT;
3. le maggiori garanzie che i CC offrono rispetto ad altri strumenti di contrasto di tipo preventivo;
4. la disponibilità di vasti cataloghi relativamente alle funzionalità di sicurezza ICT e ai requisiti di assurance adottabili;
5. la possibilità di esprimere in forma standardizzata requisiti di sicurezza per sistemi e prodotti ICT.

Con riferimento al punto 1) si può osservare che, qualora non si utilizzino i CC, qualcosa di simile può essere ottenuto mediante consulenze di sicurezza svolte da soggetti di comprovata capacità nel campo della sicurezza ICT che selezionino opportunamente le contromisure tecniche e non tecniche da adottare nell'ambito di un opportuno processo di analisi e gestione dei rischi ICT.

Per quanto concerne invece il punto 2) può essere utile evidenziare che strutture quali i CERT (Computer Emergency Response Team) hanno la caratteristica di svolgere una funzione preventiva solo rispetto alla ripetizione di attacchi a sistemi ICT che siano già stati eseguiti e che risultino quindi già noti. Tramite la valutazione compiuta avvalendosi dei CC, invece, non ci si limita a verificare che il sistema/prodotto ICT sia in grado di contrastare gli attacchi di tipo noto che potrebbero minacciarlo (ad esempio controllando, con l'eventuale ausilio di strumenti automatizzati quali i vulnerability scanners, che siano state installate le patch a tale scopo sviluppate), ma ci si preoccupa anche di ottenere adeguate garanzie circa il fatto che non sia possibile violare le funzionalità di sicurezza del sistema/prodotto ICT secondo modalità non ancora conosciute. Per quanto riguarda tali garanzie si può inoltre affermare, arrivando così a trattare il punto c), che risultano maggiori di quelle ottenibili con altri strumenti che

potrebbero essere impiegati. Utilizzando infatti i CC, soprattutto quando il livello di valutazione è elevato, si dispone di informazioni che non sono altrimenti accessibili (ad esempio i valutatori possono avere accesso al codice sorgente di un prodotto commerciale). Conseguentemente eventuali tentativi di violazione, messi in atto a scopo preventivo dall'organizzazione utilizzando risorse specializzate interne o esterne (i cosiddetti tiger-team), avrebbero minori probabilità di successo rispetto alle stesse attività eseguite nel contesto di una valutazione (ciò assumendo, naturalmente, che il livello di specializzazione dei valutatori non sia inferiore a quello delle risorse citate).

Relativamente al punto 4) si può affermare che i cataloghi funzionali e di assurance messi a disposizione dai CC possono avere un'utilità considerevole anche fuori del contesto di una valutazione, ad esempio nella fase di progettazione della sicurezza di un sistema/prodotto ICT sicuro.

Infine si può osservare, per quanto riguarda il punto e), che l'utilizzazione dei cataloghi sopra citati prevista dai CC ai fini della specificazione dei requisiti di sicurezza di un sistema/prodotto ICT da valutare, può anche trovare applicazione nella stesura di capitolati per l'acquisizione di sistemi/prodotti ICT di sicurezza (esempi di tale tipo di utilizzazione possono essere trovati nel settore della pubblica amministrazione statunitense con lo sviluppo di un certo numero di Protection Profile per varie tipologie di prodotti ICT), indipendentemente dal fatto che sia poi pianificata una loro valutazione. Inoltre la descrizione in forma standardizzata dei requisiti di sicurezza consente un più agevole confronto di sistemi/prodotti ICT certificati, sia dal punto di vista funzionale sia dal punto di vista del rigore della valutazione (requisiti di assurance).

Detto questo riguardo ai vantaggi che l'applicazione dei CC può portare, vediamo ora quelli che sono comunemente considerati gli svantaggi. Essi derivano essenzialmente da come è stata utilizzata fino ad ora la certificazione CC. Nel prossimo paragrafo vedremo che questi svantaggi possono essere fortemente mitigati, se non addirittura annullati, utilizzando una diversa strategia di applicazione dei CC.

I principali svantaggi della certificazione secondo i CC potrebbero essere:

1. i lunghi tempi di esecuzione del processo di valutazione/certificazione;
2. il costo elevato del processo;
3. la perdita della certificazione non appena ci si discosta anche lievemente dalla configurazione certificata.

Lo svantaggio citato al punto 1) deriva dall'obbligo per chi richiede la valutazione di predisporre una notevole mole di documentazione e dal tempo necessario ai valutatori per analizzare tale documentazione ed eseguire tutte le numerose e complesse azioni che i criteri pongono a loro carico. Conseguenza di questo stato di cose è che non di rado quando il processo termina è già disponibile una nuova versione del sistema/prodotto ICT. Inoltre possono nascere difficoltà relativamente all'utilizzazione di prodotti certificati nelle architetture hw/sw più recenti.

Per quanto riguarda il punto 2) si può dire che il costo elevato risulta una diretta conseguenza, oltre che dei lunghi tempi di esecuzione, anche delle risorse non trascurabili dal punto di vista sia qualitativo sia quantitativo che durante l'esecuzione del processo è necessario impegnare. Il fattore costo ha fatto sì che finora i criteri di valutazione in generale, ed i CC in particolare, siano stati prevalentemente impiegati nel campo della sicurezza nazionale (i budget sono in questo caso piuttosto elevati ed inoltre in vari paesi è obbligatoria in tale campo la certificazione di sistema/prodotto), oppure per la valutazione di sistemi/prodotti ICT per i quali sia ipotizzabile un fatturato particolarmente elevato (o perché è elevato il costo unitario del sistema/prodotto ICT, o perché se ne prevede la vendita in un elevato numero di esemplari, come è il caso, ad esempio, dei sistemi operativi dei computer).

E' evidente che i limiti descritti ai punti 1) e 2) diventano meno marcati quando risulti adeguato utilizzare livelli di valutazione bassi. Al riguardo si può peraltro ricordare che proprio con i CC è stato aggiunto un livello iniziale di valutazione che non trova corrispondenze nei precedenti criteri di valutazione e che è caratterizzato da tempi e costi alquanto contenuti. Questa considerazione sarà meglio sviluppata nel paragrafo successivo, quando verrà descritta la strategia di approccio alla certificazione CC in corso di attuazione da parte dell'OCSI.

Riguardo al punto 3) è opportuno invece sottolineare che una

delle implicazioni più dirette che crea notevoli difficoltà è l'impossibilità di installare patch senza prevedere una nuova certificazione del sistema/prodotto ICT. Quest'ultima può essere però resa relativamente veloce e non troppo costosa seguendo le indicazioni che i criteri stessi forniscono relativamente al mantenimento nel tempo della certificazione nell'apposita classe di assurance denominata Maintenance of assurance. In taluni casi, peraltro, ossia quando mediante una opportuna analisi si sia potuto stabilire che gli aggiornamenti hw/sw non possono compromettere il buon funzionamento delle parti più critiche del sistema/prodotto ICT, può essere sufficiente una integrazione della documentazione di valutazione, piuttosto che una riesecuzione di attività da parte dei valutatori. Proprio la classe Maintenance of assurance, a dimostrazione dell'importanza che riveste, è stata quella maggiormente studiata dopo l'emanazione della prima versione dei CC.

A completamento di quanto esposto per il punto 3) può essere interessante osservare che l'esigenza di aggiornare i sistemi/prodotti ICT pur mantenendo valide le garanzie relative al livello di sicurezza che sono in grado di offrire può essere parzialmente soddisfatta con approcci alternativi a quello della certificazione, ottenendo in tali casi vantaggi e svantaggi. Ad esempio si potrebbe prevedere che, dopo aver scelto alcune fonti di riferimento (tipicamente i cosiddetti CERT – Computer Emergency Response Team, che raccolgono le segnalazioni relative agli incidenti di sicurezza e le divulgano unitamente alle eventuali contromisure utilizzabili per evitarli) dalle quali acquisire informazioni relative alle nuove vulnerabilità scoperte e alle patch eventualmente disponibili per ridurle o eliminarle, si proceda direttamente all'installazione delle patch stesse. Tale approccio si baserebbe in pratica sulla filosofia di attribuire un maggior peso alla riduzione o eliminazione di vulnerabilità già note rispetto alla possibilità che proprio la patch produca anche, come effetto indesiderato, la creazione di nuove, ed eventualmente anche più gravi, vulnerabilità (ovviamente non ancora note nel momento in cui la patch viene resa disponibile). Un simile approccio, peraltro, qualora si desideri che almeno per alcuni aspetti dia garanzie analoghe a quelle della certificazione, dovrebbe anche prevedere che un soggetto interno o esterno all'organizzazione verifichi l'avvenuta installazione delle patch di sicurezza sui prodotti/sistemi ICT. E' evidente che il vantaggio principale dell'approccio descritto

consisterebbe nei ridotti tempi con i quali si provvederebbe a dotare i sistemi/prodotti ICT delle contromisure in grado di contrastare nuove modalità di attacco utilizzate in almeno un incidente di sicurezza che sia stato segnalato alla comunità dei CERT. Lo svantaggio è invece quello, già anticipato, di non prevedere una accurata analisi della modifica del sistema/prodotto ICT, analisi che tenda a verificare l'assenza di elementi sfruttabili per realizzare con successo attacchi diversi da quelli contrastati dalla modifica stessa.

3.2.3 La strategia dell'OCSI per la certificazione CC

L'individuazione della suddetta strategia deve necessariamente tenere in conto le esperienze recenti in materia di certificazione di sicurezza, al fine di individuare sia gli errori commessi, sia la possibilità di attuare possibili migliorie. Nel seguito, si effettueranno le due analisi e, alla fine, si descriveranno alcune direttrici di sviluppo della certificazione di sicurezza che verrà attuata dall'OCSI.

Gli standard internazionali prevedono che la certificazione e la valutazione di sicurezza possa essere effettuata a vari livelli di garanzia: nel caso dei Common Criteria, sono previsti sette livelli di garanzia denominati EALx, essendo EAL1[16] il livello a garanzia più bassa, EAL7 quello a garanzia più elevata. Al crescere del livello di garanzia crescono sia i controlli e le verifiche di sicurezza effettuati, sia gli oneri economici e tecnici a carico del Fornitore. E' opportuno evidenziare, che già il livello EAL1, pur essendo il più basso livello di garanzia previsto dai Common Criteria, garantisce l'assenza di vulnerabilità note e sfruttabili nel sistema/prodotto certificato. Tale garanzia è già da considerarsi molto apprezzabile, almeno nei sistemi e prodotti ICT destinati alle applicazioni commerciali, soprattutto rispetto alla diffusa situazione attuale in cui molti sistemi/prodotti sono vulnerabili ad attacchi informatici già noti da tempo[17] .

---

16 Si prevede che la nuova versione dei Common Criteria modificherà la definizione del livello EAL1 introducendo verifiche di sicurezza aggiuntive che miglioreranno significativamente il livello di sicurezza garantito rispetto a quanto previsto dalla attuale versione dello standard.

Analizzando la tipologia delle certificazioni fino ad ora effettuate dagli Schemi esteri, emergono alcune considerazioni, che possono essere riassunte come descritto nel seguito.

- E' prevalentemente utilizzata la certificazione di prodotto a livelli di garanzia medi ed elevati (da EAL4 in sù), mentre sono raramente eseguite le certificazioni di sistema (se non nell'ambito della sicurezza nazionale) e le certificazioni a bassi livelli di garanzia (EAL1 e EAL2). Tale situazione è essenzialmente favorita dalle politiche commerciali dei Fornitori, che ritengono svantaggioso proporre agli utenti prodotti certificati con bassi livelli di garanzia.
- Essendo in generale le certificazioni a livelli medio alti di garanzia, molto costose e richiedendo tempi lunghi rispetto al ciclo di vita del prodotto, la diffusione della certificazione di sicurezza risulta alquanto limitata. Si osserva, in particolare, che le certificazioni eseguite all'estero hanno riguardato prevalentemente prodotti quali, ad es, smart cards e dispositivi impiegati per la protezione perimetrale delle reti.
- Sono abbastanza diffuse le certificazioni dei documenti denominati Profili di Protezione (PP)[18] . Si possono individuare diverse applicazioni di PP certificati. A titolo di esempio, negli USA, i PP vengono utilizzati come riferi-

---

17 Potrebbe apparire che il livelli di garanzia previsti nei Common Criteria siano stati "mal progettati", in quanto sono fortemente sbilanciati a favore di una elevata sicurezza garantita. Tale situazione, che effettivamente esiste, è però motivata, almeno in parte, dal fatto che la certificazione di sicurezza è stata inizialmente introdotta e utilizzata per molti anni quasi esclusivamente per sistemi/prodotti destinati ad essere utilizzati nell'ambito della sicurezza nazionale. Anche nell'ambito della sicurezza nazionale, comunque, i livelli di garanzia EAL6 e EAL7 sono utilizzati in rarissimi casi, in quanto molto onerosi. Con il diffondersi della certificazione di sicurezza anche nell'ambito commerciale tale sbilanciamento è divenuto più evidente, senza però nulla togliere all'efficacia e alla utilità degli standard.

18 Il Profilo di Protezione (PP) è un documento che descrive gli obiettivi di sicurezza, le minacce, l'ambiente ed i requisiti funzionali e di fiducia per una certa categoria di prodotto/sistema ed in modo indipendente dalla realizzazione. Un PP può essere utilizzato, ad esempio, per definire un insieme standard di requisiti di sicurezza ai quali uno o più prodotti possono dichiarare la conformità, o che devono essere soddisfatti dai sistemi usati per uno scopo particolare all'interno di un'organizzazione.

mento per definire i capitolati di approvvigionamento delle dotazioni di sicurezza ICT delle Agenzie Federali: storicamente, i primi PP certificati hanno riguardato soprattutto i firewall. Nella UE, sono stati predisposti alcuni PP riguardanti i dispositivi sicuri da utilizzare per i servizi di firma elettronica[19] : questi documenti costituiscono evidentemente un riferimento per i fornitori che intendono certificare prodotti appartenenti a tale categoria di prodotti.

- Non sono per nulla diffuse le procedure di mantenimento nel tempo dei certificati di sicurezza. In assenza di una procedura di mantenimento, formalmente il Certificato ha valore solo nel momento in cui viene emesso e, di fatto, le garanzie che può offrire vengono meno non appena si rilevino nuove vulnerabilità o vengano rilasciate nuove "patch" di sicurezza o nuove versioni del prodotto. E' evidente che, a tutela dell'utilizzatore finale del prodotto/sistema certificato, sarebbe opportuno che l'Organismo di Certificazione vigilasse sull'eventuale uso a fini promozionali della certificazione soprattutto nei casi in cui le garanzie da essa offerte siano effettivamente venute meno.

D'altra parte, analizzando la situazione attuale della sicurezza ICT, sembra opportuno esplicitare le seguenti considerazioni. Innanzitutto, dalle statistiche disponibili sugli incidenti informatici e dall'esperienza pratica risulta che il maggior numero di incidenti deriva dallo sfruttamento di vulnerabilità note per le quali spesso esistono le patch (cioè gli aggiornamenti del software che risolvono la vulnerabilità stessa). Per migliorare tale situazione sembrerebbe logico, quindi, attuare una politica di utilizzo dei prodotti che ponga la giusta atten-

19 CWA 14167-2 Cryptographic Module for CSP Signing Operations – Protection Profile (CMCSO-PP);
CWA 14167-3 Cryptographic Module for CSP Key Generation Services – Protection Profile (CMCKG-PP);
CWA 14167-4: Security requirements for trustworthy systems managing certificates for electronic signatures - part 4 : cryptographic module for CSP signing operations - protection profile (CMCSO-PP).

zione all'aspetto di disponibilità nella generazione delle patch da parte del fornitore e di test e inserimento delle patch stesse nelle applicazioni e nei sistemi software.

La seconda considerazione è che non ha molto senso utilizzare prodotti "molto sicuri" in sistemi complessivamente molto vulnerabili o in organizzazioni in cui non si sia provveduto a certificare l'intero processo organizzativo che ruota attorno all'uso del prodotto ICT certificato. Queste considerazioni portano a dedurre che è preferibile una uniformità di attenzioni alla sicurezza, eventualmente anche a bassi livelli di garanzia, ma estesa ai vari ambiti che caratterizzano un 'processo completo' (cioè, il sistema/prodotto, l'ambiente, i ruoli del personale, le procedure di amministrazione e gestione della sicurezza, etc.) piuttosto che utilizzare un prodotto certificato ad alti livelli di garanzia e lacune di sicurezza in tutti gli altri ambiti. La suddetta uniformità di sicurezza garantita si ottiene innanzitutto favorendo la certificazione secondo i Common Criteria di sistemi completi, piuttosto che il semplice assemblaggio di prodotti certificati e di prodotti non certificati[20] . Inoltre, sarebbe opportuno superare l'attuale conflittualità tra la certificazione di prodotto/sistema effettuata secondo i Common Criteria e la certificazione di processo aziendale secondo lo standard BS7799: i due tipi di certificazione, pur mantenendo le loro specificità, dovrebbero essere maggiormente integrati e coordinati, al fine di raggiungere un miglioramento complessivo della sicurezza dei sistemi ICT.

Inoltre, attualmente l'utente finale non risulta essere un soggetto fondamentale nella richiesta di certificazione, almeno non tanto quanto lo è il fornitore. Infatti, le certificazioni risultano essere richieste in modo pressoché esclusivo dai fornitori per i loro prodotti, ma non esiste ancora la cultura della Certificazione del Sistema, a cui dovrebbero essere molto più interessati sia l'acquirente del sistema certificato, sia l'utente finale dei servizi erogati con sistemi certificati. A

---

20 *Ovviamente, la certificazione di sistema è generalmente più onerosa della certificazione, allo stesso livello di garanzia, dei singoli prodotti costituenti il sistema. A questa circostanza si può ovviare abbassando il livello di garanzia desiderato, eventualmente anche fino al livello EAL1 che, come detto in precedenza, è già da considerarsi largamente sufficiente in molte applicazioni commerciali*

titolo di esempio, consideriamo una applicazione di e-banking: in questo caso, da una parte dovrebbe essere interesse della banca certificare i sistemi acquistati dal fornitore, al fine di avere garanzie che le funzionalità di sicurezza desiderate (e acquistate) siano affidabili[21], dall'altra il cliente della banca che vuole utilizzare i servizi di e-banking dovrebbe pretendere che i sistemi utilizzati dalla banca stessa siano certificati da una parte terza rispetto sia alla banca, sia al fornitore del sistema.

Considerando quanto accaduto negli altri Paesi (come brevemente descritto in precedenza), bisogna riconoscere che la certificazione non ha avuto la diffusione che ci si sarebbe potuto attendere, sia per gli elevati costi, sia per i lunghi tempi di valutazione, sia per il fatto che la stragrande maggioranza degli Organismi esteri non vigilano sufficientemente sull'utilizzo di certificati non più validi sia formalmente, sia praticamente. Come conseguenza di questo approccio, il certificato emesso perde rapidamente la sua reale utilità per l'utente finale a causa, ad esempio, del presentarsi sistematico di nuove vulnerabilità che non sono contrastate dal sistema/prodotto nella versione in cui è stato certificato. Nel contempo, quasi nessun fornitore intraprende autonomamente[22] il percorso del mantenimento della certificazione, con azioni che, sotto la verifica dell'Organismo, garantirebbero una elevata tempestività nel contrastare le nuove minacce e gli eventuali malfunzionamenti che influenzino la sicurezza del sistema-prodotto.

Infine, un ultimo elemento che è bene tenere presente è legato alla peculiarità del mercato italiano per i fornitori di prodotti e sistemi ICT. Infatti, l'Italia è caratterizzata da una molteplicità di aziende medie e piccole che si occupano, con ottimi risultati sul piano nazionale e internazionale, principalmente dell'integrazione del software e dell'hardware esistente, piuttosto che della loro produzione (le aziende produttrici sono concentrate tipicamente negli USA). Questo scenario fa si che, di fatto, potrebbe non esserci un mercato in Italia per la

21 Tali garanzie potrebbero consentire alla banca sia di incrementare il numero di clienti che si avvalgono del servizio di e-banking, sia di attenuare le proprie responsabilità nei confronti dei clienti a seguito del verificarsi di incidenti informatici.

22 Il fornitore, d'altronde, potrebbe non avere alcun interesse economico e commerciale ad intraprendere un percorso di mantenimento del certificato, una volta che il suo uso a fini pubblicitari non venga, di fatto, impedito.

Certificazione di Prodotti agli alti livelli di garanzia (EAL3 e 4 tipicamente) come negli USA, ma che esista un potenziale mercato molto ampio per la certificazione di sistemi, che eventualmente integrino prodotti già certificati. Tale certificazione potrebbe risultare molto appetibile soprattutto se eseguita in modo tale da fornire garanzie circa l'assenza di vulnerabilità note sfruttabili nei sistemi stessi (ciò può essere ottenuto già con una certificazione al primo livello di garanzia EAL1 e aderendo a un processo di mantenimento del certificato).

Alla luce delle analisi sopra delineate, l'OCSI ha intenzione di intraprendere una azione di comunicazione e di operatività incentrata sui seguenti punti:

1. promozione della certificazione ai primi livelli di garanzia (EAL1 e EAL2);
2. promozione della certificazione di interi sistemi ICT;
3. promozione del mantenimento sistematico dei certificati;
4. stimolo della domanda di sistemi certificati agendo anche (e soprattutto) sugli utilizzatori finali dei servizi;
5. diffusione della certificazione di sistema a bassi livelli di garanzia nella Pubblica Amministrazione, al fine di innescare il meccanismo virtuoso conosciuto come "government by example";
6. utilizzazione della certificazione di Profili di Protezione che possano essere utilizzati come capitolati nella fornitura di sistemi/prodotti con specifiche funzionalità di sicurezza; tali capitolati potranno essere utilizzati sia dalla PA, sia dalle imprese private;
7. diffusione, congiuntamente alla certificazione secondo i Common Criteria, della certificazione di tipo BS7799/ISO27001 almeno per ciò che concerne i processi di gestione della sicurezza direttamente correlati con l'operatività dei sistemi certificati secondo i CC.

In particolare, per quanto riguarda i punti 1), 2) e 3) si può affermare che per il caso dei livelli di garanzia EAL1 e EAL2:

- la valutazione di sicurezza si può condurre in modo relativamente semplice sull'intero sistema ICT, riducendo, tra l'altro, gli oneri tecnici a carico del Fornitore (ad esempio, produzione di una complessa documentazione di corredo

al prodotto da certificare);
- i tempi di valutazione risultano mediamente dell'ordine di alcune settimane, garantendo un adeguato 'time to market' per il prodotto-sistema;
- in considerazione dei tempi rapidi, la valutazione e il processo di mantenimento del certificato dovrebbero risultare sufficientemente economici, così da poter essere affrontati anche nelle situazioni di bassi budget di produzione del sistema/prodotto;
- per quanto riguarda la diffusione del processo di mantenimento della certificazione si può osservare che tale processo potrebbe costituire una interessante opportunità di lavoro per un vasto numero di professionisti della sicurezza, per i quali risulterebbe alquanto agevole ricoprire ruoli riconosciuti dall'OCSI, come, ad esempio, quello di Assistente[23]

3.3 Certificazione di competenza del personale

Lo standard ISO17799 prevede che all'atto della verifica di un ISMS sia verificata anche la competenza e il processo formativo del personale che riveste un qualche ruolo nella attuazione delle politiche di sicurezza delle informazioni. Tale verifica, però, si limita a controllare se è stato previsto e/o attuato un processo formativo, ma non entra eccessivamente nel merito riguardo alla adeguatezza del processo formativo stesso rispetto alle effettive esigenze, né - peraltro - il Lead Auditor verifica puntualmente l'effettiva competenza del personale.

Nel caso un ente ritenga necessario avvalersi di personale con competenza certificata nel settore della sicurezza ICT, ha a disposizio-

[23] L'Assistente è una persona abilitata a fornire assistenza al Committente della valutazione, al Fornitore o a un Laboratorio per la Valutazione della Sicurezza (LVS) nella fase di stesura della documentazione per la valutazione di un sistema/prodotto/PP. Inoltre, l'Assistente può curare la fase di gestione/mantenimento del Certificato. L'Assistente deve garantire l'imparzialità, l'indipendenza, la riservatezza e l'obiettività nello svolgimento del proprio ruolo, nonché la capacità di mantenere nel tempo i requisiti in virtù dei quali è stato abilitato

ne una varietà di scelte che cercheremo di illustrare nel seguito, senza, peraltro, la pretesa di essere esaustivi, anche considerando la notevole varietà di "certificazioni" di competenza attualmente disponibili sul mercato.

In particolare, non entreremo nel merito di quale tipologia di certificazione di competenza sia necessaria per poter svolgere un particolare ruolo aziendale, in quanto questo argomento richiederebbe una analisi approfondita dei vari ruoli che esula dagli obiettivi primari del presente documento.

Analogamente a quanto avviene per le altre tipologie di certificazione di terza parte, anche nel caso della certificazione di competenza del personale è opportuno fare riferimento innanzitutto a quanto previsto dalle norme internazionali. Nel campo specifico, è stata emanata la norma ISO/IEC 17024, "General requirements for bodies operating certification of persons", che stabilisce quali dovrebbero essere le caratteristiche di un Organismo di Certificazione abilitato a certificare la competenza professionale del personale, indipendentemente dalla competenza specifica che si vuole certificare. Tali requisiti sono, sostanzialmente, quelli riportati nel seguente elenco:

- Indipendenza
- Trasparenza
- Imparzialità
- Assenza di conflitti di interesse
- Partecipazione nel Consiglio Direttivo dell'Ente di Certificazione delle "parti del mercato interessate"
- Equilibrio nelle decisioni: non deve essere possibile che prevalgano interessi particolari
- Competenza
- Riservatezza
- individuazione di un Codice Deontologico da far sottoscrivere ai professionisti prima della certificazione e da far rispettare nel tempo
- Durata delle certificazioni limitata e controllata nel tempo (e non a vita come per gli iscritti negli albi professionali)
- Concessione del rinnovo della certificazione (dopo un limitato periodo di tempo) solo se il professionista:
- ha curato l'aggiornamento professionale previsto;
- ha continuato a svolgere, nel periodo di tempo stabilito,

l'attività professionale per la quale è stato certificato;
- ha rispettato il codice deontologico sottoscritto

La verifica che un Organismo di Certificazione possieda le suindicate caratteristiche dovrebbe essere verificata da un Organismo "super partes" che, a sua volta, abbia una legittimazione ad operare nel campo specifico.

In Italia, il ruolo di Organismo "super partes" è svolto dal SINCERT che effettua l'accreditamento degli organismi di certificazione di competenza in base alla ISO17024 e con riferimento alla Guida EA IAF ILAC A4 Ed 2004 (disponibile al sito web www.sincert.it/documentisincert.asp?id=142). La legittimazione di SINCERT ad effettuare tali accreditamenti risiede nel fatto che ha aderito agli accordi multilaterali EA[24] (European Cooperation for Accreditation,) e IAF [25] (International Accreditation Forum).

Al momento, comunque, SINCERT ha accreditato 9 Organismi di certificazione di competenza del personale[26] in vari settori (ad esempio, esperti in prove non distruttive, di saldatura, di gestione ambientale, esperti in sistemi di qualità) ma nessuno di essi è accreditato specificatamente per erogare certificazioni di competenza nel settore della sicurezza ICT.

In questo contesto, meritano una particolare citazione sia CEPAS (www.cepas.it), sia KHC (www.khc.it) che hanno attivato degli specifici "schemi di certificazione" denominati, rispettivamente:

(vedi www.cepas.it/persec.html):
- Security Manager/ Senior Security Manager
- Consulenti di Sistemi di Gestione della Security
- ICT Security Manager/ ICT Senior Security Manager
- ICT Security Auditor/ ICT Security Responsabili Gruppo di Auditn (vedi www.khc.it)
- Auditor Interno per Sistemi di Gestione della Security delle Informazioni

24 Per maggiori informazioni, vedi sito web www.european-accreditation.org/default_flash.htm
25 Per maggiori informazioni, vedi sito web
www.compad.com.au/clients/iaf/indexPrev.php?updaterUrlPrev=articles&artId=5
26 Per maggiori informazioni, vedi sito web
www.sincert.it/RisultatiRicerche.asp?id=259&root=elenchi

- Auditor / Lead Auditor per Sistemi di Gestione della Security delle Informazioni
- Auditor per la Privacy

Pur consapevoli che sia Cepas, sia KHC, che hanno già ottenuto l'accreditamento SINCERT per altri schemi di certificazione della competenza del personale, non sono ancora stati accreditati ad erogare (al momento della scrittura del presente documento) specificatamente le suddette certificazioni di competenza nel campo specifico della sicurezza delle informazioni, si consiglia il Lettore di verificare l'evoluzione di un possibile accreditamento di questi Organismi di Certificazione anche per lo specifico schema, direttamente nei siti indicati.

In assenza, almeno in Italia, di un Organismo di certificazione di terza parte nel settore della sicurezza ICT, ci si può avvalere di altre tipologie di "certificazione" che possono essere suddivise in due grandi categorie: le certificazioni "vendor neutral" e le certificazioni "vendor specific"[27] . La valutazione dell'affidabilità di ciascun tipo di certificazione dovrebbe tenere in conto anche delle modalità di attuazione dei requisiti stabiliti dalla ISO17024 che hanno comunque validità generale anche in assenza di un accreditamento formale in base alla norma ottenuto dall'ente erogante il particolare certificato di competenza.

Le certificazioni vendor neutral sono normalmente gestite o riferibili ad associazioni nazionali o internazionali senza scopo di lucro e, sostanzialmente, fondano la loro credibilità sulla maggiore o minore diffusione delle loro certificazioni di competenza, sulla riconosciuta affidabilità dei certificati di competenza emessi e sul comportamento deontologico delle persone che hanno acquisito e mantengono nel tempo quel particolare tipo di certificazione. Fanno parte di questa categoria, ad esempio, le certificazioni CISSP, SSCP, CISA, CISM, EUCIP, di cui si daranno maggiori dettagli nel seguito. Ciò nonostante, va detto che recentissimamente, sia ISACA (CISA/CISM) sia ISP2 (CISSP/SSCP) hanno ottenuto l'accreditamento, negli Stati Uniti, da parte di ANSI/RAB.

Le certificazioni vendor specific sono invece normalmente erogate da produttori di hardware e software, e sono finalizzate alla formazione di personale specializzato ad operare su prodotti specifici. La loro affidabilità è, ovviamente, unicamente legata alla affidabilità del

"vendor" che, peraltro, ha forti interessi commerciali e "di immagine" connessi alla concreta possibilità di utilizzare in modo sicuro i propri prodotti e, quindi, alla disponibilità sul mercato di un rilevante numero di professionisti abilitati e realmente esperti. Fanno parte di questa categoria, ad esempio, i corsi che fanno riferimento alle aziende Microsoft, Cisco, Symantec, Check Point, ISS, etc. Per maggiori dettagli su questo tipo di certificazioni si rimanda all'ottima pubblicazione del CLUSIT "Certificazioni professionali in sicurezza informatica", disponibile all'indirizzo web www.clusit.it/download/index.htm, oltreché, ovviamente, ai siti web delle aziende che erogano certificazioni di competenza riguardanti i loro prodotti.

Per quanto riguarda le associazioni vendor neutral che si occupano delle professionalità legate alla sicurezza delle informazioni a livello internazionale, abbiamo scelto di fornire alcuni dettagli di alcune tra quelle più note prediligendo una chiave di lettura basata sull'analisi delle componenti fondamentali in termini di :

- Organizzazione che promuove la Certificazione, comprensivo di sito web
- Certificazione
- Aggiornamenti

così da fornire un quadro di insieme utile per orientarsi ed i riferimenti necessari per approfondire i contenuti specifici di ciascun percorso di Certificazione tramite i link di pertinenza anch'essi riportati. Inoltre, in Appendice sono riportati, a titolo di esempio, i Codici Deontologici di $(ISC)^2$ e di ISACA.

Organizzazione	Certificazione	Aggiornamento Certificazione
ISACA (Information Systems Audit and Control Association) www.isaca.org	CISM (Certified InformationSecurity Manager).La Certificazione si pone l'obiettivo di qualificare professionisti dell'Information Security che abbiano maturato una sostanziale esperienza manageriale nell'Information Security e che siano quindi in grado di operare efficacemente nell'ambito delle 5 job practice analysis areas considerate quali knowledge statement di Security Management. Il Programma di Certificazione è costituito da un Corso facoltativo, da un esame, dall'attestazione di specifiche referenze che garantiscano un'adeguata esperienza del candidato nell'Information Security Management, e dall'adesione al codice di condotta professionale.	La Certificazione va mantenuta attraverso un rinnovo annuale ed il rispetto del Programma di Formazione Continua che richiede un minimo di 20 ore l'anno e di almeno 120 ore ogni 3 anni di formazione professionale nell'ambito della sicurezza
ISACA (Information Systems Audit and Control Association) www.isaca.org	CISA (Certified InformationSecurity Auditor).La Certificazione si pone l'obiettivo di qualificare professionisti che operano nella verifica, nel controllo e nella governance dei sistemi informativi, con particolare attenzione alla sicurezza. I professionisti debbono aver maturato una sostanziale esperienza nel settore e debbono essere quindi in grado di operare efficacemente nell'ambito dei 6 domini considerati quali knowledge statement per la verifica , il controllo e la sicurezza dei sistemi informatici. Il Programma di Certificazione è costituito da un Corso facoltativo, da un esame, dall'attestazione di specifiche referenze che garantiscano un'adeguata esperienza del candidato nell'Auditing dei Sistemi Informativi, e dall'adesione al codice di etica professionale	La Certificazione va mantenuta attraverso un rinnovo annuale ed il rispetto del Programma di Formazione Continua che richiede un minimo di 20 ore l'anno e di almeno 120 ore ogni 3 anni di formazione professionale nell'ambito della sicurezza.

Organizzazione	Certificazione	Aggiornamento Certificazione
(ISC)² (International Information Systems Security Certification Consortium) www.isc2.org	CSSP (Certified Information Systems Security Professional)La Certificazione si pone l'obiettivo di qualificare professionisti che operano nella sicurezza informatica che abbiano maturato una sostanziale esperienza in almeno uno dei 10 domini considerati quali knowledge statement relativi alla sicurezza dei sistemi informatici. Il Programma di Certificazione è costituito da un Seminario facoltativo, da un esame, dall'attestazione di specifiche referenze che garantiscano un'adeguata esperienza operativa del candidato negli aspetti implementativi della Sicurezza Informatica, dall'adesione al codice di etica professionale e dall'endorcement di un CISSP o di altra persona riconosciuta che possa essere garante del candidato.	Il Mantenimento della Certificazione è basato sulla Formazione continua, e richiede un minimo di 120 crediti di Formazione Professionale Continua in 3 anni
(ISC)² www.isc2.org	CISA (Certified InformationSecurity SSCP (Systems Security Certified Practitioner)La Certificazione si pone l'obiettivo di qualificare professionisti che operano nell'implementazione della sicurezza informatica che abbiano maturato una sostanziale esperienza in almeno uno dei 7 domini considerati quali knowledge statement relativi alla sicurezza dei sistemi informatici.Il Programma di Certificazione è costituito da un Seminario facoltativo, da un esame, dall'attestazione di specifiche referenze che garantiscano un'adeguata esperienza operativa del candidato nella Sicurezza Informatica, e dall'adesione al codice di etica professiona	Il Mantenimento della Certificazione è basato sulla Formazione continua, e richiede un minimo di 60 crediti di Formazione Professionale Continua in 3 anni

Organizzazione	Certificazione	Aggiornamento Certificazione
ISECOM (Institute for Security and Open Methodologies) www.isecom.org	OPSA (OSSTMM Professional Security Analyst) è la Certificazione per l'analisi della sicurezza dal punto di vista delle procedure di esecuzione di security test (penetration testing e vulnerability scanning in particolare), nonché dell'elaborazione.e comprensione dei risultati finali, conforme alla metodologia OSSTMM (Open Source Security Testing Methodology Manual) dell'ISECOM Lo scopo della certificazione OPSA è fornire una specializzazione, di tipo sia teorico che pratico, ai professionisti che operano nell'analisi dei sistemi informatici dal punto di vista delle violazioni di sicurezza. Il Programma di Certificazione è costituito da un Corso e dal superamento di un esame finale	Non ci sono particolari requisiti per il mantenimento della Certificazione
ISECOM (Institute for Security and Open Methodologies) www.isecom.org	OPST (OSSTMM Professional Security Tester) è la Certificazione per l'esecuzione di test di sicurezza (penetration testing e vulnerability scanning in particolare) preventiva conformi alla metodologia OSSTMM (Open Source Security Testing Methodology Manual) dell'ISECOM.Il Programma di Certificazione è costituito da un Corso che richiede quale prerequisito obbligatorio la conoscenza preventiva ed approfondita di alcuni temi di base (ad es. architetture e protocolli di rete, tecniche e software per le attività di security test) e dal superamento di un esame finale. Il corso prevede molte ore di pratica nella verifica delle vulnerabilità dei sistemi.I partecipanti al corso sono inoltre tenuti a leggere, comprendere e sottoscrivere il Codice Etico Isecom che li impegna a far uso delle proprie competenze solo per scopi legali.	Non ci sono particolari requisiti per il mantenimento della Certificazione

3.3.1 Certificazioni professionali nazionali: la tendenza nel contesto italiano

Il panorama italiano delle iniziative volte ad assicurare un elevato standard qualitativo nella preparazione dei professionisti che operano nel campo dell'Information Security è caratterizzato da alcuni progetti che puntano all'identificazione di un percorso formativo completo sulle diverse aree di competenza.

Tra le iniziative omai consolidate si segnala, ad esempio, il "Corso Avanzato in Information Security Management" organizzato dal Cefriel (Consorzio per la Formazione e la Ricerca in Ingegneria dell'Informazione , sito web www.cefriel.it) e dal MIP (Politecnico di Milano) finalizzato a formare la figura dell'Information Security Manager attraverso la focalizzazione su competenze sia di natura tecnica, sia organizzativa e legale. L'ammissione al Corso è a numero chiuso ed è basata su una valutazione dei curricula e dell'esperienza lavorativa attraverso una fase di colloquio individuale. Maggiori informazioni di dettaglio sul Corso possono essere reperite al link: www. securman.it.

Una menzione particolare merita la patente europea del computer (ECDL), in quanto, pur non essendo specifica per certificare la competenza in materia di sicurezza informatica, dovrebbe assicurare che il soggetto certificato sia in possesso dei concetti ritenuti di base per l'informatica e che, quindi, dovrebbe possedere le nozioni minime per poter contribuire ad attuare, sia pure a basso livello, le politiche di sicurezza dell'ente di appartenenza. Per ottenere l'ECDL è necessario acquistare una "Skill card" e sostenere 7 esami presso uno qualsiasi dei Centri accreditati (Test Center) in Italia o nel resto d'Europa. L'ISCOM (www.iscom.gov.it) è un Test Center accreditato dall'AICA (Associazione Italiana per l'Informatica e il Calcolo Automatico) ed è abilitato al rilascio delle "Skills card" e ad organizzare sessioni di esame.

Infine, si segnala che l'OCSI ha organizzato appositi Corsi di Formazione sui Common Criteria e sullo Schema Nazionale di certificazione della sicurezza di prodotti e sistemi finalizzati alla formazione delle figure di Valutatore e di Assistente (vedi www.ocsi.gov.it). Ricordiamo che:

- Il **Valutatore** può svolgere tutte le attività di valutazione

all'interno di un Laboratorio di Valutazione. Esso è formato, addestrato ed abilitato dall'Organismo di Certificazione a condurre una valutazione in accordo ai Common Criteria e alla relativa metodologia CEM

- L'**Assistente** è una persona formata, addestrata e abilitata dall'Organismo di Certificazione per fornire supporto tecnico al Committente o al Fornitore che ne faccia richiesta. All'Assistente può essere richiesta, tra l'altro, un'analisi del Traguardo di Sicurezza o del Profilo di Protezione al fine di accertare, sulla base anche di eventuale ulteriore documentazione richiesta al Committente, che lo stesso costituisca una solida base per la conduzione del processo di valutazione.

3.4 Certificazioni di sicurezza fisica

Per quanto riguarda la certificazione di sicurezza fisica, la situazione attuale è nettamente più complessa rispetto ai casi trattati in precedenza. Questa complessità è essenzialmente dovuta alla numerosità e alla varietà degli elementi coinvolti nella scelta, nel progetto, nella realizzazione, nella configurazione e nel mantenimento di un sito fisico e/o di sistemi che ospitano informazioni.

Ciò implica che opportuni controlli debbano essere effettuati affinché la struttura fisica risulti adeguata (es. parametri di costruzione) ed anche sia possibile garantire che quanto contenuto all'interno venga opportunamente protetto (es. impianto antincendio e porte tagliafuoco, rispetto dei requisiti elettrici, protezione fisica da accessi non autorizzati). A tutto questo si aggiunge che se i predetti locali sono destinati ad accogliere sistemi di elaborazione dati, i cablaggi dovranno rispettare norme precise, alcune delle quali dipendono dalla tipologia di sistemi ospitati piuttosto che da altri parametri intrinseci nella scelta dei collegamenti.

Tali considerazioni forniscono una prima e non esaustiva idea della complessità che sottende a quanto viene compreso nella definizione di "Sicurezza Fisica".

Quanto descritto nel seguito di questa Linea Guida in merito all'argomento non può e non vuole essere una trattazione completa ma

mira soltanto a fornire alcune indicazioni che possano essere di ausilio per iniziare ad orientarsi ed affrontare il problema della sicurezza fisica.

3.4.1 Lo standard BS7799 (ISO/IEC 17799:2005 e ISO/IEC 27001:2005) e la sicurezza fisica

Anche per la sicurezza fisica, la norma a cui si può fare riferimento, almeno nella fase iniziale, è la ISO/IEC 17799:2005. Alcuni dei controlli previsti all'interno dello standard si focalizzano proprio sulla verifica dei meccanismi preposti sì alla protezione fisica ma comunque nell'ottica della garanzia della sicurezza del processo di gestione delle informazioni e della missione istituzionale dell'organizzazione.

Nella ISO/IEC 17799 viene evidenziata la specifica voce "Sicurezza fisica ed ambientale": più precisamente nel capitolo 9, "Physical and environmental security", si suddivide il problema generale in aree, a loro volta articolate in sottoaree di indagine, secondo lo schema indicato di seguito.

- **Secure areas**, il cui obiettivo è prevenire accessi non autorizzati, danneggiamenti ed interferenze nei confronti delle finalità del business e delle informazioni. Tale sezione si compone di:
  - Physical security perimeter (garanzia dell'adeguatezza delle protezioni fisiche);
  - Physical entry controls (garanzia dell'impossibilità di accesso da parte di persone non autorizzate);
  - Securing offices, rooms, and facilities (garanzia dell'adeguatezza delle protezioni dei componenti della Secure area);
  - Protecting against external and environmental threats (garanzia di protezione da minacce esterne sia ambientali sia ad opera di umani);
  - Working in secure areas (garanzia che protezioni fisiche ed adeguate linee guida siano poste in atto per tutti i soggetti che stabilmente o periodicamente debbano accedere all'area ristretta);
- Public access, delivery, and loading areas (garanzia che

aree contenenti informazioni riservate siano mantenute ben distinte da aree pubbliche);

- **Equipment security** che mira a prevenire la perdita, il danneggiamento, l'asportazione o la compromissione di beni nonché l'interruzione delle attività, e si compone di:
  - Equipment siting and protection (garanzia che la localizzazione e la protezione delle apparecchiature sia tale da ridurre il rischio di minacce ambientali, pericoli ed opportunità di accessi indesiderati);
  - Supporting utilities (garanzia che le apparecchiature siano protette da interruzioni di corrente causate da eventuali guasti nelle apparecchiature di supporto);
  - Cabling security (garanzia che le connessioni atte al trasferimento di informazioni e dati siano protette da danneggiamento ed intercettazione);
  - Equipment maintenance (garanzia che le apparecchiature vengano sottoposte regolarmente a manutenzione al fine di prevenire la mancata "disponibilità ed integrità");
  - Security of equipment off-premises (garanzia che le apparecchiature utilizzate fuori sede siano adeguatamente protette);
  - Secure disposal or re-use of equipment (garanzia che tutte le apparecchiature contenenti dati sensibili e prodotti software sottoposti a licenza, vengano opportunamente controllate prima della dismissione);
  - Removal of property (garanzia che apparecchiature, informazioni o software non possano essere portati fuori il sito senza preventiva autorizzazione).

Tali indicazioni si sostanziano in altrettanti "controlli" indicati nella sezione A.9 della norma ISO/IEC 270001:2005.

Va comunque tenuto conto che seppure la BS7799 comprenda controlli inerenti al contesto fisico, è pur vero che la verifica ad opera di un Lead Auditor BS7799 si sostanzia nell'analizzare che le soluzioni di protezione adottate siano adeguate ai requisiti specifici del contesto in esame.

Ciò in alcuni casi può risultare sufficiente mentre in altri casi

potrebbe essere necessario avvalersi di ulteriori garanzie fornite sia da parte delle aziende produttrici, tramite autocertificazione, sia - eventualmente - ad opera di una "terza parte" che "certifichi" la qualità del prodotto finale, come richiesto, d'altra parte, dalla nuova ISO/IEC 270001:2005 in termini di misura dell'efficacia dei controlli.

Generalmente nel campo della sicurezza fisica vengono utilizzati anche altri tre termini: Conformità, Omologazione e Certificazione delle prestazioni. Le omologazioni ed i certificati di conformità sono spesso obbligatori, mentre i certificati di prestazione sono volontari ed esiste una grande varietà di istituti ed associazioni di privati che in grado di rilasciarli.

Conformità

Il termine conformità, prevede che i locali fisici, gli impianti e le apparecchiature ICT debbano essere conformi alle normative di legge, non ultima la sicurezza del lavoro. Nel Decreto Legislativo sulla Tutela della Salute e della Sicurezza dei Lavoratori (626/1994) viene stabilito un principio di fondo: la sicurezza del lavoro non è rigorosamente legata alle norme ma è delegata ad un tecnico progettista che operi un'analisi della situazione e individui le condizioni di rischio ed i criteri per minimizzarlo. Una volta raggiunto il livello di sicurezza identificato, è previsto che quest'ultimo venga periodicamente controllato ad opera di un responsabile (non necessariamente una figura tecnica) che ne garantisca il mantenimento nel tempo. Secondo questo schema, il primo soggetto ha la responsabilità di identificare le condizioni di rischio potenziale ed individuare le opportune contromisure in fase progettuale, mentre il secondo deve garantire la costante attività di minimizzazione del "rischio incidenti" per l'azienda. In questa architettura le norme, complicatissime, devono essere applicate sulla base del "buon senso". E' compito, quindi, delle due figure professionali individuate precedentemente determinare quali siano le giuste norme da applicare rispetto alla situazione in esame.

Nel caso di una società di installazione di impianti antincendio il certificato principale è quello di conformità alla legge sulla Sicurezza degli Impianti (46/1990). Quest'ultimo può essere rilasciato da una ditta iscritta alla camera di commercio come ditta abilitata a fornire la

specifica tipologia di impianti in esame e dotata di un tecnico responsabile con l'abilitazione a firmare il progetto dell'impianto.

E' importante controllare, in questi casi, l'iscrizione alla camera di commercio che deve necessariamente essere aggiornata ogni tre mesi.

La ditta è obbligata a rilasciare la certificazione di conformità e, durante l'esecuzione dei lavori, è inoltre obbligata a dimostrare che il personale sia dotato di DPI (Dispositivi di Protezione Individuale) omologati. Alle società fornitrici di impianti può essere richiesta una copertura assicurativa che tuteli il committente in caso di guasti o malfunzionamenti agli impianti installati.

Certificati di conformità sono richiesti non solo per gli impianti ma anche per alcuni prodotti e componenti. Ad esempio negli impianti elettrici tutti i componenti utilizzati nella realizzazione devono essere conformi alle norme CEI (Comitato Elettrotecnico Italiano). Il CEI è il rappresentante italiano dei principali organismi di normazione internazionale. Le norme CEI hanno lo scopo di stabilire i requisiti a cui devono rispondere impianti elettrici, apparecchi, macchinari, circuiti, materiali ma anche processi e programmi, per essere rispondenti all'indicazione di "regola dell'arte".

Sono i produttori a dichiarare che un loro prodotto è conforme a determinate norme tramite l'applicazione della marcatura CE.

Infatti attraverso la marcatura CE il produttore dichiara, sotto la propria responsabilità, la conformità del prodotto ai requisiti essenziali previsti dalle direttive europee. applicabili.

Per poter applicare la marcatura, il produttore deve effettuare delle prove di laboratorio, produrre una documentazione e conservarla per almeno 10 anni successivi all'immissione sul mercato dell'ultimo esemplare, ciò in quanto è previsto che i prodotti, possano essere sottoposti a controlli da parte delle Autorità competenti

Omologazione

Il termine omologazione identifica la condizione in cui un istituto indipendente (di terza parte) verifica la rispondenza di un prodotto ad una serie di norme e requisiti obbligatori e ne certifica la rispondenza. Solo in tal caso il produttore può dichiarare di possedere un certificato di omologazione.

Certificazione in base alle prestazioni

Il temine Certificazione in base alle prestazioni vuol dire che un sistema/prodotto, a seguito di specifici test, è stato riconosciuto rispondente a determinate norme di legge. Tale rispondenza viene evidenziata in opportuni documenti rilasciabili dal produttore/installatore a seguito dell'attività. Per poter meglio comprendere il significato della certificazione in base alle prestazioni si ritiene opportuno presentare un esempio specifico relativo alla sicurezza del cablaggio strutturato.

3.4.2 Certificazioni di prestazione nel cablaggio strutturato

La velocità di trasmissione delle informazioni tra due apparati è imposta dalla velocità che tali apparati supportano e dalla velocità trasmissiva supportata dal collegamento. Per ottimizzarla è utilizzato un meccanismo di autonegoziazione della velocità di trasmissione tra i due apparati, meccanismo in grado di determinare di volta in volta la massima velocità di trasmissione possibile.

Per quanto appena detto, il collegamento fisico tra due apparati può limitare pesantemente le prestazioni di trasmissione. I vincoli imposti possono essere determinati sia dai materiali utilizzati, sia dal modo in cui tali materiali sono assemblati ed installati. I materiali sono suddivisi in categorie o classi e per ognuna di queste sono definiti dei parametri di prestazione misurabili, codificati in opportuni standard. Si vuole sottolineare che non è sufficiente fornirsi di apparati molto "rapidi"; non è nemmeno sufficiente utilizzare materiali che, presi singolarmente, garantiscono una elevata banda passante. È necessario che tutti gli elementi siano assemblati a regola d'arte. L'unico modo per garantire chi commissiona l'impianto è quello di misurare le caratteristiche trasmissive a installazione ultimata e verificare che tali caratteristiche siano quelle previste, ossia collaudare i collegamenti realizzati. I documenti che attestano l'avvenuto collaudo sono chiamati certificazioni di prestazione dell'impianto.

Come esempio si intende analizzare le procedure di certificazione che attestano che un collegamento soddisfa a determinati stan-

dard. Per far ciò si introdurranno gli standard di riferimento del cablaggio strutturato, si accennerà alle norme di sicurezza da osservare, si indicherà la documentazione che l'installatore dovrebbe rilasciare al committente.

Prendiamo in esame il collegamento tra due punti in uno stesso piano, detto Permanent Link, che è di norma un collegamento di lunghezza massima pari a 90m.

3.4.3 Standard

Gli standard generali di cablaggio cui fare riferimento sono il documento americano ANSI/TIA/EIA-568-B (ratificato in maggio 2001, e aggiornato con diversi Addendum), il documento internazionale ISO/IEC 11801 2nd Edition (ratificato in settembre 2002), la versione europea CENELEC EN 50173 2nd Edition (ratificata in novembre 2002), e la versione italiana CEI 306-6.

Può essere corretto fare riferimento a tutti gli standard quando si specificano i componenti, ma non è corretto quando si specifica il sistema che si vuole implementare: infatti, tra i vari standard (in special modo tra la versione americana e le altre) esistono leggere differenze sui limiti prestazionali (ad esempio tra Categoria 6 e Classe E) che possono dare valutazioni diverse in fase di test e collaudo. Per il sistema da realizzare è quindi importante definire a quale standard si vuole fare riferimento.

Per il cablaggio in rame le prestazioni più elevate attualmente definite sono: la Categoria 6 con l'addendum ANSI/TIA/EIA-568-B.2.1 (ratificato a giugno 2002) e la Classe E con lo standard ISO/IEC 11801:2002. Le prestazioni dei singoli componenti sono state definite successivamente alle specifiche di Canale (ossia del collegamento end2end), per cui esistono potenziali problemi di compatibilità tra componenti provenienti da costruttori di cablaggio che hanno fatto scelte ingegneristiche iniziali non in linea con le indicazioni finali. I costruttori, per i cablaggi Categoria 6, sulla loro documentazione ufficiale devono fare riferimento a questi standard nelle loro versioni definitive e approvate.

Esistono infine altri standard specifici di vari aspetti che consentono di implementare e utilizzare correttamente un sistema di

cablaggio strutturato:

- sistemi di distribuzione (spazi, canalizzazioni, percorsi cavi, ecc.): TIA/EIA-569-A e ISO/IEC 18010 (in questo caso la versione americana è più completa, e si consiglia di fare riferimento ad essa);
- installazione e grounding: TIA/EIA-607, ISO/IEC-14763-2 e CENELEC EN 50174-2;
- integrazione di sistemi di Building Automation nel cablaggio strutturato: TIA/EIA-862;
- identificazione dei componenti del cablaggio, registrazione e amministrazione delle informazioni, loro aggiornamento durante l'uso da parte dell'utenza: TIA/EIA-606-A e ISO/IEC 14763-1.

3.4.4 Sicurezza

Il parametro di sicurezza più considerato è il rischio d'incendio. I componenti del cablaggio strutturato, in particolare le guaine dei cavi, hanno vari gradi di resistenza al fuoco e differenti comportamenti in caso di combustione. È' fortemente raccomandato utilizzare cavi conformi alla norma di Propagazione dell'Incendio/della Fiamma CEI 20-22 parte 3°, corrispondente alla norma internazionale IEC 60332-3a ed europea CENELEC HD 405-3. E' auspicabile inoltre utilizzare cavi LSZH (Low Smoke Zero Halide, poco fumo zero alogenuri) che, in caso di combustione, siano conformi alle seguenti norme:

- emissione di fumi: CEI 20-37 parti 4°-6°, IEC 61034-2, CENELEC HD 606.2
- acidità e corrosività: CEI 20-37 parte 3°, IEC 60754-2, CENELEC HD 602
- tossicità dei fumi: CEI 20-37 parte 7°, NES 713

Un altro aspetto fondamentale per la sicurezza riguarda la messa a terra degli elementi di supporto, distribuzione e networking dell'impianto. E' necessario che ogni elemento metallico che possa venire a contatto con un operatore sia collegato al sistema di protezione e messa terra dell'edificio. Un adeguato riferimento comune di terra è anche utile per garantire il buon funzionamento dei sistemi di telecomunicazione e del trasferimento dei segnali. La soluzione consiste in

un impianto di terra per telecomunicazioni, ampiamente descritto nella norma TIA/EIA-607.

3.4.5 Compatibilità elettromagnetica

Le Direttive Europee sulla Compatibilità Elettromagnetica (la 89/336/CEE più successive modifiche e la 2004/108/CE) stabiliscono i requisiti essenziali relativi agli aspetti della compatibilità elettromagnetica, rimandando alle norme armonizzate per la verifica della conformità ai suddetti requisiti.

Un sistema di cablaggio è passivo, di per sé non emette segnali non è soggetto a problemi di immunità, e non è soggetto alla direttiva di cui sopra.

La nuova Direttiva, 2004/108/CE, prevede la possibilità di certificare l'intero impianto prescindendo dalle singole apparecchiature.

3.4.6 Competenza dell'installatore

Particolare importanza riveste in questo ambito il ruolo della ditta installatrice. La competenza delle società di installazione e integrazione infatti è essenziale per conseguire le prestazioni attese dal cablaggio. La necessaria formazione può essere fornita da enti di formazione indipendenti (ad esempio BICSI) o dai costruttori di cablaggio, che possono fornire dettagli tecnici specifici della propria soluzione.

I costruttori supportano sul mercato i loro sistemi di cablaggio tramite società integratrici, che vengono qualificate tecnicamente. Le attività interessate da questa formazione sono: la fase progettuale del cablaggio e della sua distribuzione (canalizzazioni), l'integrazione con gli altri sistemi, l'installazione e il successivo collaudo.

E' utile valutare come gli installatori vengano addestrati dai costruttori di soluzioni di cablaggio strutturato, quali siano i requisiti che questi ultimi pongono per il personale che esegue le installazioni (numero di addetti qualificati), e cosa sia previsto per mantenere nel tempo l'aggiornamento di progettisti e installatori. A questo proposito sarebbe opportuno che la società installatrice fornisca documentazione (ad esempio attestati di partecipazione a corsi) dell'avvenuta formazione del personale che interverrà sul sistema di cablaggio.

È bene che un eventuale committente sappia che i costruttori di soluzioni di cablaggio strutturato rilasciano alle società di installazione le seguenti certificazioni:

- Certificazione della qualifica dell'azienda installatrice;
- Certificazione dell'avvenuta formazione tecnica del responsabile dei lavori dell'azienda installatrice;
- Certificazione dell'avvenuta formazione tecnica del progettista dell'impianto.

3.4.7 Collaudi e certificazioni

Terminata l'installazione del sistema si deve procedere con il collaudo ed il test per verificare la corretta installazione e funzionalità di quanto realizzato.

E' ragionevole che l'installatore verifichi quanto effettivamente di sua competenza, cioè la parte permanente del cablaggio strutturato. Per quanto riguarda il rame, il test preposto a ciò è il test di Permament Link, che esclude i cordoni alle estremità, risultando più stringente. Le nuove categorie di performance richiedono strumenti certificatori di cablaggio secondo gli standard TIA/EIA e ISO/IEC di Livello III o superiore.

I risultati dei test non devono essere in nessun caso manipolabili dall'installatore.

In conformità alle procedure ISO 9001 lo strumento certificatore deve essere stato precedentemente calibrato da un laboratorio indipendente. Le procedure di calibrazione per gli strumenti certificatori devono essere ripetute almeno una volta l'anno.

Il collaudo di un collegamento consiste nel connettere lo stru-

mento certificatore ai due capi del collegamento da collaudare. Lo strumento certificatore è composto da due unità, una principale e una remota che comunicano tra loro attraverso il collegamento sotto test. Una unità dello strumento emette segnali dalle caratteristiche note e l'altra rileva il segnale e il rumore generato (cavo, pannelli di connessione connettori eventuali cordoni, eventuali interferenze esterne).

A meno che non sia richiesto diversamente da parte del committente, di norma il collaudo è effettuato dalla società di installazione del cablaggio.

Dalla certificazione dovrà risultare:

- nominativo dell'azienda che effettua il collaudo;
- nominativo dell'operatore;
- marca, modello e numero di serie dello strumento utilizzato;
- versione software dello strumento;
- data dell'ultima taratura;
- specifiche sulle quali si basa il collaudo (es. classe EIA/TIA oppure categoria secondo ISO11801).

Per ogni collegamento realizzato deve essere rilasciato un documento che indichi l'esito del collaudo, sul quale in particolare per la categoria 6 devono essere riportati:

- la lunghezza del collegamento;
- attenuazione;
- frequenza di test;
- ritardo di propagazione del segnale;
- skew di ritardo (differenza di propagazione del segnale all'interno di una singola coppia);
- resistenza (in funzione della frequenza);
- ACR (Attenuation to Crosstalk Ratio);
- PSACR (ACR indotto da tutte le altre coppie su quella in esame);
- NEXT (diafonia);
- PSNEXT (diafonia indotta da tutte le altre coppie su quella in esame);
- ELFEXT (Equal Level FEXT. È l'ACR utilizzando il valore di FEXT, ossia il NEXT al ricevitore);
- PSELFEXT (ELFEXT indotto da tutte le altre coppie su

quella in esame);
- RL (return loss).

Per ognuno dei campi si deve riportare il valore di soglia e il valore misurato.

È necessario che l'impianto sia consegnato completo di etichette in modo da mantenere una corrispondenza uno a uno tra identificazione e certificazione.

3.4.8 Assicurazione delle prestazioni del cablaggio

L'utente può avere ulteriori assicurazioni della bontà di una soluzione di cablaggio facendo effettuare il collaudo dell'impianto da laboratori indipendenti e riconosciuti a livello internazionale (ad esempio ISCOM).

3.4.9 Garanzia

Alcuni costruttori garantiscono i loro prodotti per un tempo ragionevolmente lungo (20-25 anni), in particolare è garantita la conformità allo standard dell'intero impianto. Queste garanzie sono applicate quando l'installatore dell'impianto abbia effettuato dei corsi di formazione presso il costruttore.

4 - Appendice A: Applicazione degli standard tipo BS7799

4.1 Introduzione

Nella presente appendice è mostrato un esempio reale delle attività necessarie per realizzare un ISMS basato sullo standard BS7799:2 2002, nonché la documentazione che è prodotta.

La realizzazione di un ISMS rappresenta una scelta di carattere strategico per un'azienda, e deve essere presa dalla direzione aziendale per creare processi più sicuri e nel contempo efficaci che fungano da abilitatori del business, ottenendo quindi anche un vantaggio competitivo.

Come per ogni tipo di processo, deve sempre valere la regola della semplicità, specialmente per le piccole aziende, caratterizzate da sistemi informativi non complessi; il relativo ISMS dovrà essere semplice e facilmente gestibile. Nel caso di realtà più complesse, contraddistinte da numerose interazioni e processi, nonché da un sistema informativo aziendale complesso, anche il relativo ISMS rifletterà tale complessità.

Una volta presa la determinazione da parte della direzione aziendale di certificare il proprio sistema informativo, utilizzando lo standard BS7799:2, sarà necessario procedere per passi, creando un sistema documentale della sicurezza che sia costituito da politiche, standard e procedure di sicurezza.

Esiste di fatto una gerarchia delle informazioni che vanno a comporre un ISMS. Nella figura sottostante sono riportati sei livelli differenti di documentazione. La figura rappresenta solo un possibile esempio di organizzazione del sistema documentale. I documenti che vanno dal primo al quinto livello, possono essere raccolti in un unico "Manuale della Sicurezza", che, con collegamenti ipertestuali, punta ai documenti specifici; tale organizzazione facilita, per altro, il compito di eventuali valutatori.

Nella realtà sono possibili delle variazioni: per esempio il primo livello ed il secondo possono essere collassati in un unico documento di politiche di sicurezza. Oltre che verticalmente tale opera di sintesi si può realizzare anche orizzontalmente, per es. raggruppando tutti gli standard di sicurezza: architetturali, HW, SW, controllo accessi, etc. in un unico documento. Ciò è stato realizzato in particolare nell'esempio descritto nella presente Appendice, riferita al caso dell'azienda ACME, che ha un unico standard di sicurezza, chiamato ITCS104, suddiviso in vari capitoli a seconda delle aree di applicazione.

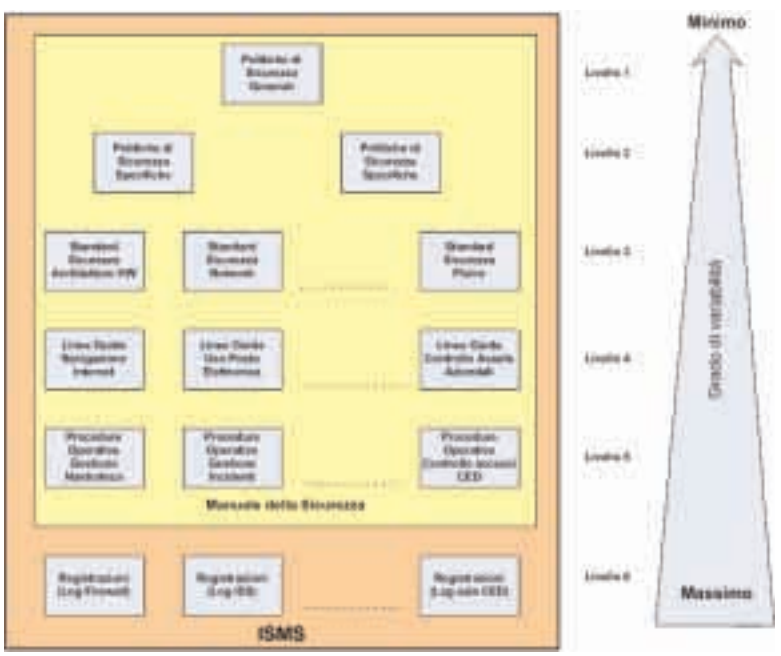


Figura 1 La gerarchia della documentazione all'interno del sistema documentale.

Il grado di variabilità della documentazione è massimo ai livelli più bassi (si pensi a tutti i log che giornalmente vengono prodotti) e minimo ai livelli più elevati (le politiche di sicurezza sono di solito riviste ogni anno, oppure se dovessero intervenire dei cambiamenti normativi).

Esistono ulteriori documenti che devono essere prodotti per permettere una corretta valutazione del sistema documentale; il primo è lo Statement of Applicability (SOA). In esso a partire dalle politiche di sicurezza, conoscendo gli asset da proteggere ed i rischi principali cui sono sottoposti la direzione aziendale sceglie i controlli che devono essere messi in essere. Il SOA delimita, quindi, l'ambito cui si applica l'ISMS. E' necessario condurre un'attenta valutazione dei rischi che agiscono sugli asset. La direzione aziendale decide se controllare, trasferire o rifiutare il rischio e a fronte delle azioni prescelte si deve realizzare un Piano di Gestione del Rischio dove per ogni rischio riscontrato viene descritto le azioni e gli eventuali controlli messi in atto per ridurlo, la data di realizzazione di questi controlli e il responsabile.

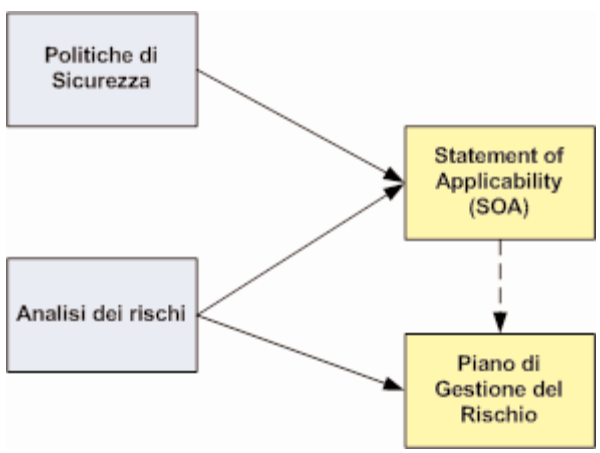


Figura 2 Documenti per la produzione del SOA e il Piano di Gestione del Rischio

Nell'esempio considerato si esamina il caso di un'azienda multinazionale fittizia di nome ACME che opera nel campo dei servizi di Information Technology. La Business Unit di ACME in Italia, che offre servizi di Business Continuity e Disaster Recovery (BCRS) ha deciso di certificare il proprio ISMS secondo BS7799:2 2002.

Per fare questo ha analizzato le politiche di sicurezza di cui era già dotata, ha valutato i controlli proposti dallo standard BS7799:2, determinando quale di quelli proposti erano adeguati ai bisogni aziendali, creando lo Statement of Applicability. Ha quindi proceduto all'analisi dei rischi, e come output finale ha generato il Risk Management Treatment Plan, dove vengono pianificate le azioni da intraprendere, per adeguare i controlli di sicurezza al livello desiderato.

Nella seguenti tabelle sono illustrate, in forma schematica, le varie attività da intraprendere per creare un ISMS. Il progetto è stato suddiviso in tre fasi principali. La fase uno è propedeutica all'implementazione dell'ISMS, ed è seguita dalle fasi due e tre, composte varie attività. Si deve ricordare che il processo di sviluppo dell'ISMS è iterativo, le attività non sono mai esaustive, ma vanno viste nella logica di Deming (Plan-Do-Check-Act). La colonna Deliverables riporta semplicemente i documenti che vengono citati all'interno di questa appendice. Essa non è dunque esaustiva di tutta la documentazione che deve essere prodotta, in quanto questa appendice riporta solo i controlli relativi alle aree di Organizzazione e di Sicurezza Fisica dello Standard BS7799:2 2002.

Nella tabella sotto riportata sono evidenziate le attività principali da svolgere durante la fase uno

Cod. Attività	Attività (principale)	Descrizione dell'attività	Responsabili	Deliverables
000	Project management	Assegnare le risorse per il project management del progetto.	Direzione Aziendale Project Manager	Business Case e piano delle attività
100	Information management fulfillment	Protezione degli asset importanti e loro classificazione in accordo con le regole, chiara assegnazione dell'ownership degli asset.	Business Owner ISMS Core team (Consulenti Esterni)	CMT: gestione ordine ed inventario asset Service Level Agreement
200	Risk Assessment	Definizione di una prima iterazione del Risk Assessment e relativa Gap Analysis	ISMS Core Team (Consulenti Esterni)	Risk Management Doc.
300	Politiche di sicurezza	Revisione e/o preparazione delle Politiche di Sicurezza	ISMS COre team Direzione Aziendale	ACME Information Security Policies

Tabella 1 Attività da svolgere nella fase uno

Nella tabella sotto riportata sono evidenziate le attività principali da svolgere durante la fase due

Cod. Attività	Attività (principale)	Descrizione delle attività	Responsabili	Deliverables
400	Pianificazione dell'ISMS per l'Organizzazione Obiettivo di questa fase è quello di costruire un ISMS che sia conforme al framework ISO e rispetti le normative nazionali e dell'Organizzazione,	Definizione dell'ambito dell' ISMS Definizione delle politiche dell' ISMS Completamento Risk assessment e management plan Selezione dei controlli di sicurezza Preparazione Statement of Applicability (SOA) Formulazione del Piano di controllo del rischio (risk treatment plan) Implementazione dei controlli di sicurezza (I° revisione)	Mgr. Organizzazione ISMS Core Team	SOA ACME Risk Management ACME Information Security Manual
500	Implementazione dei controlli ISMS, inizio delle operazioni e verifica dei risultati, con eventuali azioni di retroazione , per migliorare l'ISMS	Implementazione dei controlli di sicurezza (seconda revizione) Gestione delle operazione (registrazione degli eventi) Esecuzione audit interni Manutenzione e miglioramento dell'ISMS	Mgr. Organizzazione ISMS Core Team	

Tabella 2 Attività da svolgere nella fase due

Nella tabella successiva sono evidenziate le attività principali da svolgere durante la fase tre

Cod. Attività	Attività (principale)	Descrizione dell'attività	Responsabili	Deliverables
600	Preparazione delle Organizzazioni relative alla sicurezza	Nomina del CISO, creazione dell' Information Security Committee, dello Staff di Sicurezza ed altri cambiamenti relativi all'organizzazione..	Direzione Aziendale	Management Security Responsibility Organizations and Contacts ACME BCRS Organizational Model Security Roles Job Descriptions
700	Realizzazione delle Politiche di sicurezza e relative procedure	Revisione e/o preparazione delle Politiche di Sicurezza e dei relativi standard. I consulenti valuteranno/prepareranno anche le relative procedure operative e le linee guida	ISMS Core Team (Consulenti Esterni) CISO	ACME Security Guidelines ITCS104- BB100: Purchasing requisition approval for goods/services Global Logistics Guidelines ITCS 300 Security and Use standards for ACME employees QMX-IT-PRC-00629
800	Realizzazione dei piani e attività di educazione alla sicurezza	Stabilire i piani e le attività per l'education dei manager, gli specialisti di sicurezza e gli impiegati.	HR	Security pamphlet 2004 ITCS 300 Security and Use standards for ACME employees
900	Implementazione misure di sicurezza fisica	Seguire le regole per ciascuna area classificata e implementare le eventuali misure di sicurezza fisica richieste.	Management aziendale	ACME Information Security Manual (cap 7 Physical Security) ITCS104 (Physical Access Control) Procedura controllo accessi centro BCRS Roma (QMX:IT-PRC-00619) ITCS104 (Information Technology Security Standard Global Logistics Guidelines
1000	System Development	Adeguare il sistema informativo, riducendone le vulnerabilità e stabilire le regole di sicurezza da seguire nei nuovi sviluppi.	Management Aziendale ISMS Core team (Consulenti Esterni)	ACME Information security Manual (Cap. 4)
1100	Business continuity management	Stabilire i piani di business continuity	Management Aziendale	ACME Business Continuity Plan

Cod. Attività	Attività (principale)	Descrizione dell'attività	Responsabili	Deliverables
1200	Audit & Self assessment	Stabilire dei processi o piani di self-check, audit interno e operazioni di follow up	Audit team interno	
1300	Ottenimento della certificazione per l'ISMS	Richiedere la certificazione Revisione preliminare Fase 1(revisione della documentazione) Fase 2 (Visita presso l'Azienda/Organizzazione) Risultati della certificazione	Direzione Aziendale ISMS Core Team (Consulenti esterni) Valutatori	

Tabella 3 Attività da svolgere durante la fase tre

Per realizzare un progetto di questo tipo un azienda o una PA di dimensioni medie o grande può ricorrere ad un'organizzazione simile a quella mostrata nella figura sottostante.

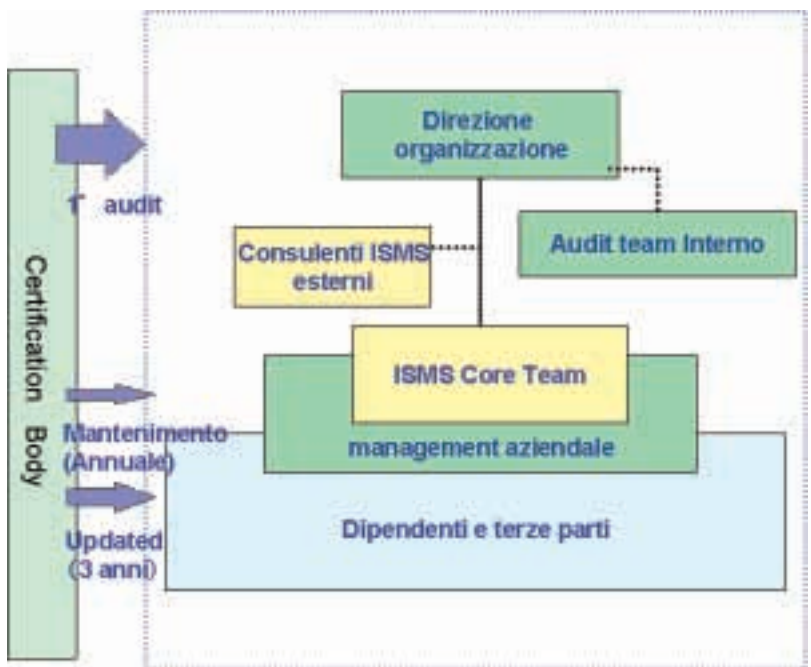


Figura 3 Schema di organizzazione aziendale per la realizzazione di un ISMS

All'interno dell'azienda, sfruttando le competenze presenti, si è costituito un Core team che, con l'aiuto di consulenti esterni specializzati nella realizzazione di ISMS, ha il compito di eseguire tutti i passi che portano alla messa in produzione di un ISMS efficiente. Fatto questo si dovrà procedere alla certificazione. Il management aziendale guida le operazioni dell'ISMS all'interno di ogni divisione/direzione aziendale e coopera nell'introduzione dell'ISMS con le persone che fanno parte del team di implementazione (ISMS core team e consulenti esterni).

4.2 Organizzazione dei documenti presenti in Appendice.

Il documento è organizzato in paragrafi che distinguono logicamente le varie attività che devono essere svolte, secondo la loro sequenza operativa. Il paragrafo 4.3 che copre le Politiche di Sicurezza di alto livello dell'ACME BCRS.

Nel paragrafo 4.4 vengono descritte delle Politiche di Sicurezza specifiche, ovvero quelle relative alla protezione fisica degli asset.

Il paragrafo 4.5 presenta l'esempio di una procedura specifica, in questo caso quella di accesso alla sala CED dell'ACME.

Il paragrafo 4.6 è il documento dove viene descritto il processo di Risk Assessment e Risk management per i processi e gli asset di ACME BCRS.

Un ulteriore output si ha al paragrafo 4.7, che è di fondamentale importanza, e rappresenta il Manuale della Sicurezza. Esso è il cuore dell'ISMS, poiché in questo documento gli attori dei processi di ITC, trovano le motivazioni dei controlli messi in essere, nonché i riferimenti, mediante collegamenti ipertestuali alle normative (politiche specifiche, standard, linee guida o procedure di sicurezza) il cui rispetto assicura il mantenimento dei livelli di sicurezza prescelti. Il manuale della Sicurezza copre tutti i dieci domini del BS7799:2002, ma per motivi di spazio vengono riportati come esempio solo i domini riferiti alla sicurezza organizzativa e a quella fisica.

Infine, nel paragrafo 4.8, si riporta un esempio di SOA anche di questo vengono, per congruenza mostrati solo i controlli relativi alle aree della sicurezza organizzativa e di quella fisica.

4.3 Information Security policy

Sono le politiche di sicurezza di alto livello da cui derivano gli eventuali standard di sicurezza e le procedure di sicurezza.

4.3.1 Ente emittente

L'Information Security Policy di ACME BCRS è:

- proposta da l'Information Security Manager di ACME BCRS;
- condivisa con l'ISSF;
- approvata dall'ACME BCRS, South Leader;
- emessa e diffusa dall'Information Security Manager di ACME BCRS
- comunicata al BCRS Security Committee.

Sono individuati di seguito i principali ruoli e le principali responsabilità di carattere decisionale previsti per la gestione della sicurezza delle informazioni all'interno di ACME BCRS.

Per i rimanenti ruoli di sicurezza di carattere operativo e per il dettaglio dei compiti di sicurezza, si rimanda ad apposito documento facente parte dell'ISMS.

4.3.2 ACME BCRS South Leader

Il ACME BCRS South Leader promuove la realizzazione e l'applicazione dell'ISMS

4.3.3 Information Security Manager

L'Information Security Manager rappresenta il referente e la guida principale per le tematiche inerenti la Sicurezza delle informazioni.

4.3.4 Proprietario dell'asset

Il proprietario dell'asset è la figura di alto livello, inteso genericamente come il responsabile del processo che genera o acquisisce o comunque detiene le principali responsabilità sull'asset.

4.3.5 Information Security Steering Forum BCRS

L' Information Security Steering Forum BCRS, sotto la guida del BCRS South Leader, dell'Information Security Manager, e con le figure aventi rilevanti responsabilità sui temi della sicurezza delle informazioni in ACME BCRS, si riunisce periodicamente per valutare lo stato attuale della sicurezza e promuovere trasversalmente su tutta la Business Unit le azioni necessarie.

L'ISSF è composto dalle seguenti figure:

- ACME BCRS South Leader;

- Information Security Manager;
- Site Manager della sede di Roma

In aggiunta, per particolari tematiche, possono essere richieste competenze ulteriori.

4.3.6 Information Security Commitee BCRS

L'Information Security Commitee BCRS, sotto la guida dell'Information Security Manager, e con le figure professionali esterne a ACME BCRS che per competenza verranno di volta in volta coinvolte, si riunisce periodicamente per valutare lo stato di implementazione della sicurezza e pianificare le attività necessarie.

L'ISCC è composto dalle seguenti figure:

- Information Security Manager;
- Organizational Security Referent;
- Technological Security Referent;
- Delivery Security Referent;
- Referenti esterni a ACME BCRS, specialisti nel loro ambito di competenza

In aggiunta, per particolari tematiche, possono essere richieste competenze ulteriori.

4.3.7 Security Referent

Il Security Referent costituisce, secondo le proprie competenze reali all'interno della struttura organizzativa di ACME BCRS, elemento di raccordo per tutte le tematiche legate alla definizione, all'implementazione ed al controllo delle misure di sicurezza aziendali.

Il Security Referent rappresenta per tutti gli utenti la figura di riferimento per la proposizione di problematiche e suggerimenti in tema di sicurezza aziendale.

4.3.8 Utenti

Gli utenti condividono le responsabilità per la protezione dei beni aziendali loro affidati, incluse le informazioni e gli strumenti informatici.

Tutto il personale deve essere accuratamente informato sulle politiche di sicurezza adottate e deve prontamente evidenziarne ogni violazione, anche sospetta, all'Information Security Manager.

Principi di sicurezza

Di seguito vengono enunciati i principi fondamentali su cui ACME BCRS fonda la propria gestione della sicurezza delle informazioni. Tali principi, secondo quanto riunito e strutturato all'interno dell'ISMS, possono essere perseguiti ed implementati sia mediante la emissione di apposite linee guida o procedure organizzative sia mediante il perseguimento di standard o best practice di comune adozione.

4.3.9 Organizzazione di sicurezza

L'implementazione ed il controllo della sicurezza degli asset all'interno di ACME BCRS devono essere regolati da una struttura organizzativa e conseguenti responsabilità assegnate

In particolare, la struttura organizzativa, secondo ruoli, responsabilità, e quanto definito nella mission assegnata, deve provvedere a:

- definire, approvare e applicare le politiche di sicurezza aziendale e le relative procedure;
- definire le modalità di valutazione del rischio e la scelta delle contromisure per la sua riduzione;
- implementare i controlli di sicurezza;
- monitorare la correttezza e l'efficacia del sistema implementato.

4.3.10 Inventario e classificazione degli asset

Gli asset aziendali creati o utilizzati a supporto delle attività di business, indipendentemente dal tipo, dal formato e dai supporti di memorizzazione o di comunicazione, devono essere gestiti al fine di preservare la loro riservatezza e criticità

Da tale principio discende che deve:

- essere predisposto e mantenuto un inventario degli asset aziendali;
- essere individuato un proprietario per ogni asset aziendale;
- essere classificato ogni asset aziendale, secondo modello unico e condiviso, al fine di permettere l'adozione di misure di sicurezza commisurate al valore dell'asset stesso.

4.3.11 Personale

Il personale di ACME BCRS è parte attiva del processo di gestione del rischio di sicurezza e quindi deve essere a conoscenza dell'Information Security Policy e delle procedure di sicurezza adottate.

Ne consegue che il personale deve:

- essere informato circa le proprie responsabilità in tema di sicurezza;
- essere adeguatamente formato e sensibilizzato, secondo appositi piani di formazione in funzione dei ruoli e delle responsabilità di sicurezza attribuiti, per il rispetto puntu le dei principi e l'applicazione delle regole adottate
- operare seguendo scrupolosamente le regole di sicurezza definite, facendosi portatore nei confronti del managment di suggerimenti e richieste;
- segnalare ogni incidente o sospetto tale, e ogni comporta mento non in linea con quanto definito, secondo le proce dure di comunicazione predisposte.

4.3.12 Sicurezza fisica

Gli asset fisici aziendali devono essere protetti tramite la predisposizione e il mantenimento di un ambiente materiale (fisico) che impedisca la fuoriuscita di materiali ed il verificarsi di danni ad ACME BCRS.

Tale principio deve essere perseguito attraverso misure di controllo, correlate ai rischi e al valore degli asset. Ne fanno parte le

seguenti componenti:

- la definizione e la classificazione dei perimetri di sicurezza;
- l'implementazione di misure di sicurezza negli ambienti definiti;
- il corretto posizionamento degli asset fisici all'interno dei perimetri in relazione alla classificazione di sicurezza;
- la tempestiva rilevazione di eventi anomali.

4.3.13 Gestione operativa e delle comunicazioni

L'infrastruttura tecnica deve essere gestita in modo efficace ed efficiente nel tempo al fine di garantire che all'utente sia fornito il livello di servizio richiesto e che gli asset informativi (materiali e immateriali) siano gestiti, anche nel trasferimento, in modo da preservarne la riservatezza e la criticità.

Ne consegue che:

- gli aggiornamenti dell'hardware, del software di base e degli applicativi devono essere pianificati e autorizzati al fine di minimizzare gli impatti sul livello di servizio;
- le procedure di autorizzazione e di implementazione devono essere rispondenti ai differenti requisiti di sicurezza e di continuità in relazione alla diversa tipologia di intervento;
- la gestione del change deve essere disciplinata da apposita procedura, inserita e gestita nell'ISMS;
- I test di modifiche strutturali o evolutive devono essere effettuati in un ambiente dedicato a tale scopo. Il proce so di collaudo del software è condotto secondo le

speciche di test;

- I dati di produzione non devono essere utilizzati per scopi di test senza che ogni informazione riservata e ogni dato personale sia prima rimosso o modificato in modo da preservare i dati stessi;
- gli incidenti (malicious software, virus, etc.) devono essere gestiti tramite procedure formalizzate;
- il trasferimento e la comunicazione dell'asset devono essere normate tramite apposite procedure documentate.

4.3.14 Controllo accessi logici

La sicurezza deve essere un elemento costitutivo nella fase di sviluppo e di progettazione di nuovi prodotti/sistemi/servizi di ACME BCRS. Ne consegue come i prodotti/servizi, sviluppati da o per conto di ACME BCRS, devono rispettare requisiti di sicurezza definiti sulla base di una specifica analisi dei rischi.

Ne consegue che:

- l'accesso agli asset informatici deve essere autorizzato formalmente in base alle reali esigenze operative;
- la gestione delle credenziali degli utenti e dei loro profili di accesso alle risorse aziendali devono essere definite tramite procedure, supportate da appositi strumenti software e/o hardware;
- gli utenti autorizzati devono essere responsabilizzati all'osservanza delle procedure e delle misure di sicurezza definite.

4.3.15 Progettazione e sviluppo prodotti/servizi

La disponibilità dei servizi erogati deve essere garantita, in funzione della loro criticità, al fine di assicurare il ripristino dei processi critici entro termini tollerabili, per quanto riguarda l'operatività sia interna sia esterna

Durante le fasi di sviluppo e di progettazione di nuovi prodotti/sistemi/servizi devono essere eseguite le seguenti attività:

- per i prodotti/sistemi/servizi che richiedano un elevato livello di sicurezza, deve essere svolta una adeguata valutazione del rischio di sicurezza che porti alla definizione controlli atti a diminuire il rischio;
- implementazione dei controlli organizzativi, procedurali e tecnologici necessari;
- gestione del sistema di sicurezza implementato, che comprenda anche la manutenzione correttiva ed evolutiva.

4.3.16 Continuità del business

Qualsiasi comportamento deve essere conforme alla normativa di legge inerenti all'ambito dei sistemi informativi e dell'ambiente ICT nonché al trattamento di dati personali, alla disposizioni interne e, in generale, e a quanto richiesto dalla norma BS 7779:2 2002, e deve essere verificato e garantito nel tempo.

Le misure di sicurezza organizzative, procedurali e tecnologiche a tutela della continuità del servizio devono essere formalizzate all'interno di una struttura documentale basata sul Business Continuity Plan che preveda l'individuazione dei:

- ruoli e responsabilità coinvolte nel mantenimento della continuità;

- criteri al fine di individuare i processi/servizi critici;
- requisiti di continuità.

Il piano inoltre deve fornire le linee guida in merito a:

- le misure preventive (organizzative e tecnologiche);
- la procedura di escalation, sulla base dei livelli di gravità del danno emergente.

4.3.17 Conformità

Il principio racchiude i seguenti aspetti:

- definizione e documentazione dei requisiti normativi e contrattuali;
- adozione delle misure richieste per rispettare gli obblighi contrattuali sul copyright;
- conformità ai requisiti di legge delle registrazioni da presentare in contenziosi legali;
- adozione delle misure richieste per la protezione dei dati personali;
- adozione delle precauzioni necessarie per evitare l'uso illecito delle risorse di elaborazione e comunicazione;
- verifica del rispetto della norma BS 7779:2 2002.

4.4 Politiche di sicurezza fisica

Sono le politiche non più di carattere generale, ma specifiche rispetto ad una ben determinata area. In questo caso viene riportato l'esempio della politica di sicurezza per la protezione fisica degli assets

Di seguito sono enunciati i principi fondamentali su cui

ACME BCRS fonda il proprio approccio alla sicurezza fisica:

- protezione delle risorse umane
- individuazione dei perimetri di sicurezza;
- controllo degli accessi fisici;
- protezione dei cablaggi
- protezione delle apparecchiature informatiche;

4.4.1 Protezione delle risorse umane

La tutela della sicurezza e della salute delle persone fisiche è obiettivo prioritario del management di ACME BCRS e viene perseguito con l'ausilio ed il supporto delle strutture appositamente dedicate.

ACME BCRS distribuisce a tutti i dipendenti un apposito opuscolo informativo conforme ai requisiti del D.Lgs 626/94 e successive modifiche e integrazioni.

4.4.2 Individuazione dei perimetri di sicurezza

Per prevenire i rischi di perdita o sottrazione degli asset informativi aziendali si richiede che vengano individuati perimetri fisici di sicurezza ad accesso selezionato in funzione del valore degli asset trattati all'interno delle aree aziendali

Tali perimetri sono definiti in relazione al grado di criticità delle attività che vi si svolgono e del valore degli asset informativi che vi vengono conservati secondo quanto seguito indicato:

- ❒ **Aree pubbliche** - sono le zone in cui il pubblico può accedere liberamente (es. reception);

- **Aree interne** - sono zone che ACME BCRS mette a disposizione dei dipendenti per l'espletamento delle normali attività di lavoro, e per il carico / scarico delle merci in entrata
- **Aree riservate** – sono le aree riservate all'interno delle sedi, i control center e le sale macchine, vale a dire i locali nei quali sono collocati beni, apparecchiature, informazioni.
  - le risorse informatiche
  - dispositivi di trasmissione (modem, unità di controllo, routers, etc.),
  - centraline elettriche,
  - impianti di condizionamento,
  - gruppi di continuità,
  - gruppi elettrogeni.

Le aree suddette vengono identificate in modo preciso e mantenute adeguatamente separate tra loro: l'accesso alle aree interne dalle aree pubbliche e aree riservate, avviene unicamente mediante punti di controllo.

4.4.3 Controlli degli accessi fisici

La sussistenza di adeguata autorizzazione è verificata e controllata, anche tramite strumenti automatizzati e non, prima di concedere l'accesso alle aree fisiche ai perimetri aziendali

Aree pubbliche

L'accesso alle aree pubbliche è gestito e regolamentato dalle apposite strutture centrali mediante apposite procedure cui si rimanda nel loro complesso.

Aree interne

L'accesso alle aree interne è permesso unicamente previa identificazione del soggetto e, se esterno, mediante registrazione delle

generalità e avviso dell'ospite ACME BCRS secondo modalità definite e regolamentate dalla struttura centrale di riferimento mediante apposite procedure cui si rimanda nel loro complesso.

In ogni caso, a tutela della sicurezza degli asset informativi di ACME BCRS, all'interno delle aree interne sono attivati controlli di tipo "clear desk" e "clear screen"

Aree di carico / scarico

Le aree di consegna e carico sono isolate rispetto alle aree riservate al fine di evitare accessi non autorizzati. L'accesso alle aree di carico e scarico è consentito unicamente a personale identificato ed autorizzato.

Aree riservate

Sono aree ad accesso ristretto e controllato. La protezione delle aree riservate è basata sulla selezione e restrizione delle persone che hanno l'autorità di accedervi mediante il ricorso a dispositivi e tecniche di controllo.

In questo senso:

- ❒ l'accesso alle aree riservate è fisicamente possibile solo da aree interne dell'azienda e non direttamente dall'esterno; le uscite di emergenza devono essere dotate di impianti di allarme.
- ❒ l'accesso alle aree riservate è autorizzato dal responsabile competente e limitato alle persone che ne hanno una effettiva necessità.
- ❒ il personale addetto ai servizi (pulizia, manutenzioni, ecc..) è identificato sulla base di comunicazioni (liste di riconoscimento) specifiche fatte dall'Ente fornitore e munito di appositi badge e sorvegliato da un dipendente dell'area.

L'accesso alle aree riservate di ACME BCRS è regolamentato dall'apposita procedura Physical Access Procedure.

4.4.4 Protezione delle apparecchiature informatiche

La collocazione delle apparecchiature informatiche è eseguita in modo da ridurre al minimo gli accessi non necessari nelle aree di lavoro e da ottimizzare l'attivazione delle misure di sicurezza necessarie alla protezione dell'effettivo valore delle risorse.

Da ciò deriva che:

Allestimento delle aree pubbliche

- ❒ all'interno delle aree pubbliche non sono posizionate apparecchiature informatiche se non destinate all'uso del personale di sorveglianza.

Allestimento delle aree interne

- ❒ laddove le aree interne sono organizzate con layout di tipo "open space", il management seleziona degli appositi spazi da dedicare agli uffici che svolgono operazioni a maggior riservatezza (es. controllo di gestione, sicurezza informatica,..);

Allestimento delle aree riservate

- ❒ le apparecchiature informatiche classificate al massimo livello sono allocate all'interno delle aree riservate salvo le seguenti eccezioni:
  - o i notebook aziendali - che sono gestiti e tutelati dai rischi di uso improprio, furto, alterazione dei dati, danneggiamento/distruzione del notebook e/o dei dati secondo apposite istruzioni cui si fa riferimento
  - o i PC - desktop aziendali eventualmente contenitori di informazioni classificate al massimo livello - che sono gestiti e tutelati dai rischi di uso improprio, furto, alterazione dei dati, danneggiamento/distruzione dell'apparecchiatura e/o dei dati secondo apposite istruzioni cui si fa riferimento.
- ❒ le aree riservate sono dotate di:
  - o impianti privilegiati di condizionamento, telefonici e di

collegamento;

- impianti anti-incendio e anti-allagamento;
- gruppi di continuità;
- gruppi elettrogeni.

Fornitura elettrica

- le aree riservate sono provviste di adeguati impianti di fornitura di energia che consentano di garantire la continuità di erogazione, attraverso gli opportuni strumenti (punti di alimentazione multipli, generatori di emergenza, generatori di corrente, luci di emergenza, interruttori di sicurezza, parafulmini, ..); tali strumenti sono oggetto di adeguanti piani di verifica e manutenzione periodica, che ne garantiscono l'efficienza nel tempo.

Manutenzione apparecchiature

- le apparecchiature informatiche sono periodicamente sottoposte a adeguati interventi di manutenzione, al fine di garantirne l'efficienza nel tempo e per osservare le disposizioni dei contratti assicurativi.
- le suddette manutenzioni sono espletate in base alle indicazioni del produttore ed effettuate da apposito personale specializzato.

4.4.5 Protezione dei cablaggi

I cablaggi elettrici e quelli relativi alla trasmissione dati sono protetti da danneggiamenti o interruzioni al fine di evitare impatti sui servizi forniti.

Da ciò deriva che:

- i terminali di controllo delle linee elettriche e di trasmissione dati sono opportunamente posizionate nelle aree dedicate alle apparecchiature informatiche;
- le linee elettriche sono separate dalle linee dati al fine di evitare interferenze;
- le linee di trasmissione dati sono protette da eventuali intercettazioni o danni anche tramite misure di sicurezza fisica (es. canaline, passaggi riservati)

4.5 Procedura di accesso fisico alla sala macchine

E' un esempio di una procedura specifica che serve a gestire l'accesso alla sala CED dell'ACME BCRS

L'ISMS di ACME BCRS recepisce come procedura di accesso alla sala macchine quanto già aziendalmente definito ed attivato tramite la procedura riportata nelle pagine seguenti.

E' compito del Responsabile IT Security provvedere, a seguito di eventuali modifiche al form, all'aggiornamento della presente procedura.

E' sempre suo compito operare per verificare che la procedura sia attesa dal comportamento del personale e per un sempre maggiore allineamento e razionalizzazione delle procedure di gestione degli accessi fisici alle aree riservate.

4.5.1 Procedura di Controllo accessi alla sala macchine

Scopo della procedura è:

- Limitare e autorizzare l'accesso al personale ACME, del personale di società terze e di visitatori alla Sala Macchine

- Individuare e controllare le attività condotte sui sistemi e infrastrutture
- Informare il personale delle regole di condotta da osservare

L'accesso nei locali macchine è regolato dal badge magnetico assegnato dal coordinatore, solo dopo verifica e accertamento della/e operazioni richieste.

Per l'accesso di personale non ACME, è necessario che il responsabile delle operazioni, mandi comunicazione scritta al coordinatore, il quale successivamente concederà un tesserino provvisorio di accesso al CED.

Un limitato numero di badge è assegnato in maniera fissa al personale ACME, continuamente impegnato in lavori dentro ai locali del CED.

La lista dei tesserini assegnati è inclusa all'interno della procedura.

A tutto il personale ACME ICT è consentito l'accesso in Sala Macchine solo per la realizzazione di attività definite nella riunione di programmazione settimanale, oppure in caso di necessità ed urgenza, su richiesta del Responsabile della Sala di Controllo.

L'autorizzazione di accesso in Sala Macchine è di responsabilità del responsabile della Sala Macchine.

Per l'autorizzazione di accesso è richiesto il riempimento di un form in cui dovranno essere comunicate le seguenti informazioni:

1. Nr. Tessere Magnetica
2. Nome, Cognome, Matr. ACME
3. Attività da svolgere in base alla programmazione settimanale
4. Tipo di attività: (modifica hardware, software, ripristino di un apparato, nuova installazione hardware, etc.)
5. Motivazione del carattere di necessità/urgenza della richiesta di accesso in caso di attività non programmata
6. Durata dell'attività, ora inizio, ora fine.

Il form deve essere firmato dal personale nuovamente in uscita, con la riconsegna del badge assegnato.

I form informativi saranno archiviati per il periodo di due mesi presso la postazione del Responsabile della Sala Macchine.

Tessere Fisse.	Nominativo assegnatario
Nr. 1	Tizio Caio
Nr. 2	Lucio Sempronio
Nr. 3	Domitilla Flavia

4.6 BCRS Risk Management

Rappresenta il documento dove viene descritto il processo di Risk Assessment e Risk management per i processi e gli asset di ACME BCRS

4.6.1 Premessa

In accordo alle strategie di sicurezza del patrimonio informativo dichiarate nella propria Politica di sicurezza delle informazioni [rif. ACME BCRS Servizi di certificazione della sicurezza ICT], ACME BCRS ritiene fondamentale conoscere e gestire i rischi cui i propri asset informativi sono sottoposti, al fine di tutelarne adeguatamente il livello di sicurezza aziendale. Conseguentemente, ACME BCRS riconosce la necessità di comprendere chiaramente la composizione del proprio patrimonio informativo nonché il preciso valore di ognuna delle sue componenti e quindi di eseguire una corretta analisi dei rischi per selezionare i controlli più appropriati a contrastare le minacce relative. Ai risultati delle suddette attività ACME BCRS intende applicare le proprie strategie di gestione del rischio al fine di ottimizzare, governare e controllare il livello di rischio cui è sottoposto il proprio patrimonio informativo.

4.6.2 Responsabilità Operative

È compito dell'ISM accertarsi che i contenuti del presente documento, e le modalità di loro implementazione, siano applicati nel corso di tutte le attività di risk assessment e risk management eseguite all'interno di ACME BCRS.

Scopo

Scopo principale del presente documento è quello di definire un approccio sistematico al rischio, conforme all'ISMS di ACME BCRS che definisca:

- la metodologia di valutazione e gestione del rischio
- le modalità di individuazione del rischio,
- le modalità di valutazione del rischio,
- la strategia di gestione del rischio,
- le modalità di individuazione dei controlli e delle contromisure di sicurezza a riduzione dei rischi evidenziati,
- le modalità di approvazione manageriale dei risultati delle precedenti attività.

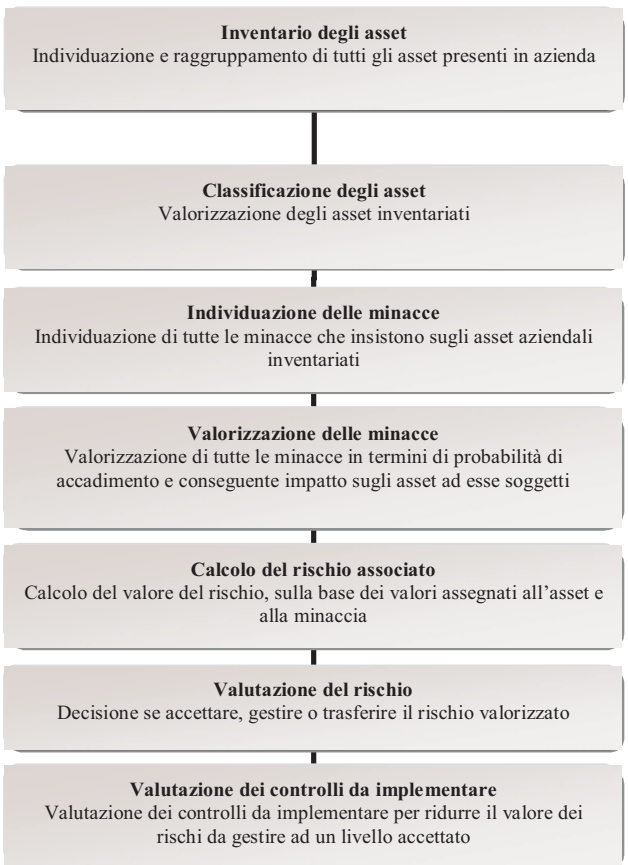
4.6.3 Introduzione al concetto di rischio

4.6.3.1 Concetto di rischio

ACME BCRS recepisce, all'interno del proprio approccio al "risk management" la terminologia così come definita nel documento ISO Guide 73:2002 [3]. Di conseguenza, operativamente, ACME BCRS contestualizza le suddette definizioni al proprio ambiente operativo rendendole efficaci al raggiungimento degli obiettivi della propria strategia di sicurezza delle informazioni.

I risultati della suddetta attività sono riportati nell'apposito glossario.

4.6.3.2 Metodologia di risk assessment e di risk management



ACME BCRS intende come risk assessment (o analisi dei rischi) il processo avente lo scopo di individuare le minacce relative agli asset informativi, e a qualificare coerentemente i controlli e le contromisure a loro protezione.

Ne deriva che il processo di analisi dei rischi è preceduto dall'inventario e dalla classificazione degli asset informativi.

ACME BCRS intende come risk management (o gestione dei rischi) il processo avente lo scopo di ottimizzare, governare e controllare il livello di rischio cui sono sottoposti i propri asset informativi.

Obiettivo principale dei suddetti processi risulta quindi essere quello di aiutare il management di ACME BCRS ad individuare:

1. le corrette strategie di protezione del proprio patrimonio informativo
2. il corretto equilibrio tra i costi connessi all'implementazione delle misure di sicurezza ed i benefici da esse derivanti.
3. le adeguate contromisure di sicurezza

I suddetti processi prevedono secondo la norma BS7799-2:2002 lo svolgimento ordinato di una serie di fasi distinte approfonditi nei successivi capitoli.

Per ottenere questi risultati, la metodologia di analisi dei rischi adottata rispetta le seguenti caratteristiche:

- Ripetibilità e riproducibilità. è possibile ottenere, a parità di condizioni, lo stesso risultato, sia da parte dello stesso operatore in tempi successivi, sia da parte di operatori diversi nello stesso momento;
- Comprensibilità. I criteri adottati nell'espressione dei parametri che compongono il rischio (es. probabilità di accadimento) sono trasparenti e comprensibili;
- Condivisione. I valori attribuiti agli asset sono condivisi tra le varie funzioni aziendali per le quali tali valori sono di interesse;
- Coerenza. I valori attribuiti agli asset sono coerenti con quanto stabilito dalle politiche di sicurezza di ACME BCRS ;
- Attinenza al dominio di applicazione. La definizione del dominio di applicazione del ISMS è coerente con il dominio definito per l'analisi dei rischi;

- Riutilizzabilità. I risultati (finali o anche intermedi) dell'analisi dei rischi possono essere riutilizzabili in caso di variazioni (es.: modifica delle minacce) in modo da garantire economie nella ripetizione dell'analisi;
- Sintesi nei risultati. I risultati sono sintetici e facilmente leggibili

4.6.4 Attivazione del processo (trigger)

E' responsabilità dell'ISM pianificare ed eseguire il processo di analisi e gestione dei rischi con una periodicità almeno annuale; la revisione è tracciata e giustificata formalmente.

I contenuti dello strumento (es. parametri di classificazione, elenco minacce, checklist di assessment, …) ed i risultati dell'analisi e della gestione dei rischi, nonché i deliverable del processo (es. Risk treatment Plan, SOA, ...) sono comunque aggiornati al variare delle seguenti condizioni:

- variazioni delle strategie di business di ACME BCRS
- variazione delle politiche di sicurezza di ACME BCRS
- variazioni legislative
- decisioni dell'ISM a fronte dei risultati della Security Checklist compilata dai solution designer in fase di disegno delle soluzioni di delivery – vedi paragrafo successivo
- risultati delle attività di incident management e conseguente storicizzazione degli incidenti atta a sostenere la ponderazione delle minacce

4.6.4.1 Gestione della SECURITY CHECKLIST

- Nella fase di disegno della soluzione ACME BCRS richiede al solution designer di compilare una security checklist atta ad individuare tutte le variazioni dell'ambiente di delivery di ACME BCRS.con impatto significativo sulla sua sicurezza delle informazioni.

4.6.5 Individuazione degli asset

L'individuazione degli asset è la base di partenza senza cui non è possibile poter procedere ad una corretta ed efficace gestione della sicurezza aziendale. L'inventario è infatti il punto di partenza per la classificazione degli asset aziendali e per l'analisi del livello di rischio cui sono essi sono sottoposti.

Il mantenimento e l'aggiornamento nel tempo dell'inventario diventa quindi parte integrante e fondamentale della gestione del rischio.

Le modalità e le responsabilità di svolgimento delle suddette attività sono definite all'interno dei processi di analisi e gestione dei rischi

In particolare, inoltre, avendo valutato la criticità dei singoli asset secondo specifici requisiti di business, contrattuali e di legge, ACME BCRS decide di considerare Mission Critical tutti gli asset che abbiano almeno uno dei tre requisiti "High", ovvero tutti e tre i requisiti valutati "Medium".

La tabella successiva mostra alcuni dei principali tipi di asset presenti (la lista non è esaustiva) e l'importanza degli stessi rispetto alle tre categorie di requisiti individuate (Biz Business, Ctr Contrattuali e Legal)

				Mission critical			
				Requirement			Mission Critical
id	Asset Category	Type of asset		Biz	Ctr	Legal	
1	Data	1 Client's applications or data		H	H	NO	yes
2	Data	2 Application in Lotus Notes environment		H	H	M	yes
3	Data	3 Other ACME BCRS application		M	M	M	yes
4	Hardware/Firmware	4 Network infrastructure		H	H	NO	yes
5	Hardware/Firmware	5 Data containers		H	H	M	yes
6	Hardware/Firmware	6 Working set		H	H	M	yes
7	Hardware/Firmware	7 Management device		H	H	NO	yes
8	Hardware/Firmware	8 Facilities		H	H	NO	yes
9	Hardware/Firmware	9 Phone		H	H	M	yes
10	Mobile Hardware	10 Mobile phone		H	NO	NO	yes
11	Mobile Hardware	11 Data containers		H	H	M	yes
12	Site	12 Building		H	H	M	yes
13	Services	13 Connectivity		H	H	L	yes
14	Services	14 Other 3rd parties services		H	H	L	yes
15	Services	15 Other ACME BCRS services		H	H	M	yes
16	Human Resources	16 Well Being		H	L	H	yes
17	Human Resources	17 Skills		H	H	NO	yes

Tabella 4 Esempio di categorizzazione degli asses e loro

4.6.6 Individuazione delle minacce

Obiettivo di questa attività è l'individuazione delle minacce che insistono sugli asset di ACME BCRS individuati e recepiti all'interno del processo di analisi e gestione del rischio.

Una minaccia è un evento potenziale, accidentale (es.: allagamento) o deliberato (es.: furto) che, nel caso si esplicitasse, produrreb-

be un danno per ACME BCRS determinato dalla violazione dei livelli di riservatezza e integrità e disponibilità attribuito ai propri asset.

L'individuazione delle minacce prende in considerazione, per lo meno, le seguente categorie:

- eventi accidentali;
- minacce derivanti da interventi umani di tipo volontario;
- minacce derivanti da errori accidentali da parte degli utenti.

Al fine di garantire un accurata individuazione delle minacce da gestire, ACME BCRS procede per step successivi:

- individuazione delle minacce rilevanti per gli asset, gli ambienti, e le modalità operative inserite nell'ambito di certificazione. Operativamente è possibile partire da liste consolidate o "best practice" di riferimento. In questo caso, qualora una minaccia non fosse ritenuta rilevante è necessario motivarne le cause.
- Attribuzione della minaccia selezionata ad una delle seguenti tipologie:
    1. S (Security) = minaccia che impatta sulla sicurezza degli asset
    2. B (Business) = minaccia che impatta sul business aziendale
    3. L (Legal) = minaccia che impatta sugli adempimenti legali
    4. G (General) = una minaccia che impatta su almeno due delle precedenti tipologie contemporaneamente

E' compito dell'ISM, anche tramite persona delegata per competenza, aggiornare periodicamente almeno annualmente, l'elenco delle minacce che insistono sugli asset di ACME BCRS, sulla base di:

- esperienza personale;
- contatti con enti e associazioni, governative e private, che operano nel campo della sicurezza;
- risultati dell'incident management;
- suggerimenti e condivisioni da parte dell'ISSC

A garanzia dell'esaustività dell'elenco, e considerando la fase di attivazione del processo, ACME BCRS adotta una lista di minacce basata inizialmente sul BSI Protection Model, analizzato e rivisto in funzione delle esperienze e delle competenze specifiche di sicurezza delle informazioni di ACME, e dei principali tool di analisi dei rischi disponibili sul mercato. L'elenco è poi integrato con minacce derivanti dal modello di business, dalle attività e dalle strategie aziendali, dalla localizzazione geografica delle strutture aziendali, dalle caratteristiche dell'architettura informativa.

4.6.6.1 Ponderazione delle minacce

Le minacce individuate sono ponderabili su due fattori

- probabilità strutturale di accadimento;
- impatto derivante dall'accadimento della minaccia.

L'ISM, avvalendosi anche del supporto dei Security Referent per competenza, assegna ad ogni fattore di ponderazione della minaccia una valutazione qualitativa. È' compito dell'ISM definire e mantenere aggiornato un modello unico e condiviso di ponderazione della probabilità e dell'impatto.

La figura a lato mostra una classificazione di alcune delle minacce riscontrate (la lista non è esaustiva), se è applicabile (Relevant) il tipo di minaccia (S Security, B Business, L legal, G General) e infine la probabilità e l'impatto.

id	Threat	Relevant	Threat type	Probab.	Impact
1	Lack of compilance whit security policy	↓ yes	↓ S	↓ L	↓ L
2	Damage from or re-occurrence of incidents because of lake of a good reporting scheme	↓ yes	↓ S	↓ L	↓ M
3	Security breaches (deliberate or accidental) because employees are not aware of the impotance of security	↓ yes	↓ S	↓ L	↓ M
4	Security breaches because of lake of management support (e.g. When allocating resources of security)	↓ yes	↓ S	↓ L	↓ L
5	Security breaches because security policy is not up to date	↓ yes	↓ S	↓ L	↓ L
6	Security breaches because nobody feels responsible for maintaning the security policy	↓ yes	↓ S	↓ L	↓ L
7	Higher costs than necessary for security	↓ no	↓		
8	Security breaches because of unclear aims of security within the organisation	↓ yes	↓ S	↓ L	↓ L
9	Security breaches because of not up date controls	↓ yes	↓ S	↓ L	↓ H
10	Damage because of not correcly handled incidents	↓ yes	↓ G	↓ L	↓ H

Tabella 5 Esempio di alcune minacce (Threat) e loro ponderazione

4.6.6.2 Attribuzione delle minacce agli asset

Una volta selezionate le minacce è necessario procedere alla loro mappatura sugli asset al fine di individuare le corrette relazioni tra gli asset e le effettive minacce da essi subite.

Operativamente, ACME BCRS procede per step successivi:

- attribuzione delle minacce alle categorie di asset
- attribuzione delle minacce alle tipologie di asset.

Nella figura sotto riportata è evidenziata la relazione tra alcu-

ne delle minacce (threat) applicabili all'ambiente da certificare. Si noti che la lista è stata troncata per motivi di spazio e non è, quindi, esaustiva.

Pis, select with "x" all the threats referable to each asset category		1 Data	2 Hardware/Firmware	3 Services	4 Human Resources	5 Mobile hardware	6 Site
9	Security breaches because of not up to date con-	x	x	x	x	x	x
10	Damage because of not correctly handled inci-	x	x	x	x	x	x
14	Lack of asset protection because of wrongly handled ownership and delegation of responsibility	x	x	x	x	x	x
17	Unauthorides installation of new software (e.g.	x					
18	Wrong or ineffective reaction to incidents because of a lack of contact to the appropriate organisa-	x		x	x	x	x
19		x	x		x	x	
21			x			x	x

Tabella 6 La matrice di attribuzione delle minacce (threat agli asset)

4.6.7 Individuazione delle vulnerabilità

Definendo come vulnerabilità una scopertura di sicurezza di un asset o di un gruppo di essi che può essere sfruttato da una minaccia, che di fatto consiste nell'assenza o nella carenza di controlli di sicurezza adeguati ad impedire l'accadimento della minaccia, in ossequio alla metodologia di risk assessment e risk management adottata, ACME BCRS individua le vulnerabilità mediante la valutazione dei

controlli BS7799 in essere.

In altre parole, al fine del mantenimento nel tempo della certificazione BS7799 dell'ISMS adottato e della ripetibilità del metodo, ACME BCRS valuta i controlli in essere mediante l'uso di un apposito tool strutturato che evidenzi le scoperture di sicurezza rispetto ai singoli controlli dello standard di riferimento.

La suddetta valutazione avviene secondo passi successivi:

1. Selezionare i controlli BS7799 eventualmente non applicabili allo scope dell'ISMS di ACME BCRS. La selezione dei controlli avviene sulla base della conoscenza dell'ambiente operativo di ACME BCRS e del perimetro di applicabilità del proprio ISMS. Qualora un controllo non fosse ritenuto applicabile è necessario motivarne le cause mediante loro formalizzazione all'interno del SOA di ACME BCRS.
2. Individuare gli ambienti operativi per i quali i controlli possono essere implementati con modalità diverse.
3. La contestualizzazione dei controlli BS7799 all'interno delle attività oggetto dello scope dell'ISMS permette, infatti, a ACME BCRS di pianificare e valutare l'attivazione dei controlli con modalità separate in funzione delle diverse infrastruttura IT utilizzate per il delivery delle attività di ACME BCRS.
4. Attribuire gli specifici controlli agli ambienti operativi individuati.
5. Selezionare i controlli BS7799 eventualmente non applicabili ai singoli ambienti operativi.
6. Selezionare il livello di implementazione dei controlli in essere.
7. In funzione delle precedenti attività è compito dell'ISM procedere, anche tramite il supporto di altre figure, alla personalizzazione del tool, quale ad esempio la duplicazione dei capitoli dello standard di riferimento per gli ambienti individuati secondo applicabilità.
8. Selezionare il livello di implementazione dei controlli in essere
9. L'attività si svolge mediante una ponderazione, sia sulla base delle evidenze che sulla base dell'esperienza del rilevatore, del livello di implementazione dei controlli secondo una scala: di valori progressiva da 0 a 10, dove:
10. 0 = livello di attivazione nullo
11. 10 = livello di attivazione Best Practice

12. Individuare i livelli target di implementazione dei controlli.
13. L'attività si svolge contemporaneamente alla precedente e permette, in funzione anche dei suggerimenti e del benchmarking supportato dai membri dell'ISSC, di individuare a priori i controlli ritenuti migliorabili al fine di raggiungere un livello di sicurezza delle informazioni che possa essere ritenuto dal mercato di assoluta garanzia.
14. Attribuire i singoli controlli alle minacce individuate.
15. L'attività è funzionale alla possibilità di calcolare per ogni minaccia il livello di controlli attivati al fine di mitigarne gli effetti e, conseguentemente, di calcolare il rischio effettivo

4.6.8 Individuazione degli impatti sugli asset

Scopo di questa fase è la classificazione degli asset informativi di ACME BCRS, precedentemente identificati e definiti come "Mission Critical".

Tale attività viene svolta dal proprietario dell'asset, che procede alla valutazione dello stesso mediante la valutazione delle conseguenze che il medesimo potrebbe subire a causa dell'incapacità di garantirne gli obiettivi del Riservatezza, Integrità e Disponibilità, dove:

- **Riservatezza:** concetto cardine della sicurezza il cui rispetto garantisce che l'asset informativo è accessibile solamente a coloro che hanno l'autorizzazione ad accedervi.
- **Integrità**: concetto cardine della sicurezza il cui rispetto garantisce l'accuratezza e la completezza dell'asset informativo e dei metodi di elaborazione. .
- **Disponibilità:** concetto cardine della sicurezza il cui rispetto garantisce che gli utenti autorizzati possono accedere all'asset informativo quando vi è necessità.

Il valore deve essere misurato a prescindere dalle eventuali contromisure già in atto.

È compito dell'ISM definire e mantenere aggiornato un modello unico e condiviso di classificazione degli asset.

4.6.9 Calcolo del rischio totale

Scopo di questa fase è la valutazione del danno di business che potrebbe risultare da una scopertura di sicurezza e conseguente perdita delle caratteristiche di riservatezza, integrità e disponibilità degli asset.

Conseguentemente è necessario calcolare il Rischio Totale sul singolo asset, inteso come prodotto scalare della minaccia per il valore dell'asset su cui la minaccia infierisce:

$$R^{tot}(n)=A(n) \times T(n)$$

4.6.10 Calcolo del valore effettivo delle minacce

Scopo di questa fase è la valutazione della reale probabilità di accadimento delle suddette scoperture di sicurezza.

Conseguentemente è necessario calcolare il valore effettivo della minaccia inteso come il valore di partenza della minaccia decurtata del valore risultante della ponderazione dei controlli in essere:

$$T^{eff}(n)= (T(n)-C^{eff}(n))$$

Per ogni minaccia, sulla base della propria mappatura verso i controlli della norma descritta precedentemente, sono quindi individuati i controlli che possono essere utilizzati per gestire il rischio ad essa connesso, in altre parole, sono individuati tutti i controlli che, se attivati, sono in grado di diminuire la probabilità di accadimento della minaccia o il relativo impatto.

4.6.11 Calcolo del rischio effettivo

Scopo dell'attività è quello di calcolare il rischio effettivo cui è sottoposto un asset mediante il prodotto scalare del valore dell'asset per la minaccia decurtata del valore risultante della ponderazione dei controlli in essere:

$$R^{eff}(n)=A(n) \times T^{eff}(n)$$

E' proprio sul valore del rischio effettivo che fornisce al management di ACME BCRS le corrette informazioni per procedere alle attività di valutazione del rischio.

Infine si riporta in figura un esempio di asset aziendali e il rischio totale, nonché quello effettivo dopo aver messo in essere i controlli stabiliti per mitigare le varie minacce.

			V(a)	V(t)	R(t)	C(e)	V(te)	R(e)	
			Value	threats value	TOTAL RISK R(t)= V(a)*V(t)	existing controls value	effective threats value V(te)= V(t)*C(e)	EFFECTIVE RISK R(e)= V(a)*V(te)	
Dati e applicativi dei clienti			4,7	0,77	3,61	0,71	0,07	0,31	Accepted
Configurazioni degli ambienti			7,3	0,77	5,68	0,71	0,07	0,49	Accepted
Configurazioni degli ambienti			10,0	0,77	7,75	0,82	-0,05	-0,47	Accepted
CMT			10,0	0,77	7,75	0,82	-0,04	-0,41	Accepted
mail			8,0	0,77	6,20	0,82	-0,04	-0,33	Accepted
problem management			10,0	0,77	7,75	0,82	-0,04	-0,41	Accepted
blue pages			6,0	0,77	4,65	0,82	-0,04	-0,25	Accepted
infrastruttura hw e firmware			10,0	0,77	7,75	0,77	0,00	-0,04	Accepted
informatica individuale			10,0	0,77	7,75	0,82	-0,04	-0,44	Accepted
HW in uso			7,3	0,77	5,68	0,77	0,00	-0,03	Accepted

4.6.12 Determinazione del livello di rischio accettabile

ACME BCRS ritiene accettabile, a priori, un livello di rischio pari al principio di efficienza sopra definito.

Al momento ACME BCRS in funzione dei propri obiettivi strategici di business e di sicurezza delle informazioni, al fine inoltre di verificare l'effettiva efficienza del proprio sistema di gestione della sicurezza delle informazioni, decide di non intervenire in diminuzione sui rischi effettivi negativi (ovvero i controlli al momento implementati risultano essere maggiori rispetto a quelli richiesti)

4.6.13 Strategia di gestione del rischio

In funzione dei risultati delle attività sopra svolte ACME BCRS stabilisce la sua strategia di gestione del rischio che si concretizza nella tabella alla pagina successiva..

4.6.14 Selezione dei controlli

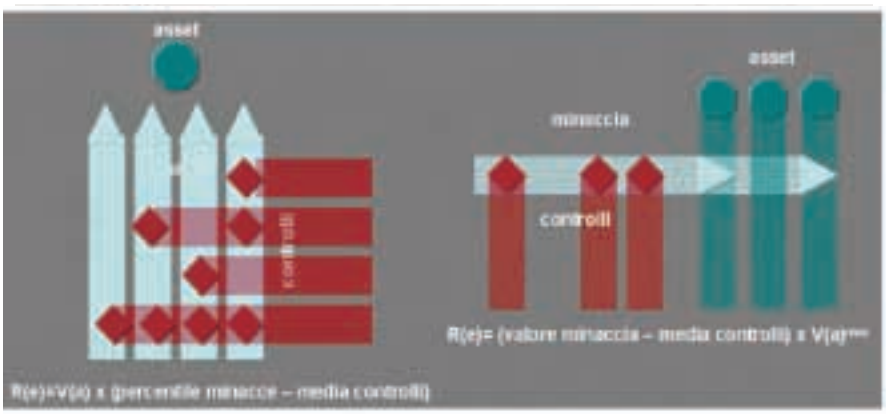
In funzione della strategia di sicurezza delle informazioni sopra descritta, ACME BCRS decide di procedere alla selezione dei controlli unicamente per quei rischi che risultano essere maggiori o uguali al livello di rischio accettato.

La selezione dei controlli avviene con l'obiettivo di ricondurre l'attuale esposizione di sicurezza al suddetto livello accettato.

Accettare il rischio	ACME BCRS è conscia che esiste un rischio che insiste sull'asset ma decide, o per lo scarso impatto del rischio, oppure dopo la valutazione costi-benefici, di non intervenire	Il Rapporto di efficienza si traduce nella definizione di un rischio accettato (Ra) pari al principio di efficienza sopra definitoIn tutti gli altri casi il rischio è ridotto ad un valore non superiore al livello di rischio accettato salvo che il rapporto costi-benefici dei singoli controlli non risulti eccessivo.
Evitare il rischio	ACME BCRS decide che la rischiosità è tale da rendere preferibile una modifica della propria strategia di business. Si pensi ad un'azienda che decida di dismettere attività di business oggetto di atti ostili (es.: allevamento di animali da pelliccia).	ACME BCRS non prevede al momento alcuna modifica alla propria strategia di business tale da permetterle di evitare dei rischi evidenziati nel corso dell'analisi.
Trasferire il rischio	ACME BCRS ritiene più economico, o comunque preferibile, trasferire il rischio, magari mediante assicurazione, ad altra azienda, senza dismettere l'attività che ne è causa.	ACME BCRS ritiene di poter trasferire parte del proprio rischio limitatamente al valore economico storico o al valore iscritto a bilancio aziendale dei singoli beni materiali nonché ai costi sostenuti in caso di disastro del cliente. In questo si avvale anche delle apposite strutture centrali a livello corporate.Per le collaborazioni con soggetti terzi con modalità di outsourcing di attività di ACME BCRS, sono valutati gli specifici rischi al fine di individuare adeguate strategie di condivisione degli stessi con le controparti.Ogni altro rischio non è trasferito, ed è gestito direttamente da ACME BCRS.
Ridurre il rischio	ACME BCRS decide, dopo l'analisi costi-benefici, di implementare dei controlli aggiuntivi per ridurre il rischio ad un livello accettabile.	Il rischio è ridotto mediante l'individuazione e attivazione di specifici controlli di sicurezza.Le attività di valutazione del rischio sono demandate all'ISM che agisce conformemente alle strategie di sicurezza definite dall'ISSF. Ogni eccezione è da questi valutata.La fase di valutazione del rischio, tuttavia, per una realtà come ACME BCRS, che, svolgendo attività consolidate nel tempo, ha già consolidato l'attivazione ed implementazione di controlli di sicurezza a tutela dei propri asset informativi e conseguenti obiettivi di business, non può basarsi unicamente sulla valutazione del rischio totale.

4.6.15 Verifica del livello di rischio effettivo

A garanzia dell'effettiva gestione di tutti i rischi cui sono sottoposti gli asset di ACME BCRS, e poiché il valore del rischio effettivo sugli asset risulta essere mediato sia sulle minacce che sui controlli, si valutano anche i rischi sui singoli asset partendo dalle minacce come esplicitato nelle seguenti figure:



In funzione dello stato attuale dei controlli implementati è così possibile evidenziare tutti i rischi effettivi con un valore maggiore o uguale al livello di rischio accettato.

A maggior copertura di tutti i rischi individuati, ACME BCRS stabilisce il proprio registro dei rischi organizzato secondo la presente modalità.

4.6.16 Valutazione dei controlli da implementare

Sulla base dei risultati dell'attività di valutazione dei rischi, relativamente ai rischi che ACME BCRS intende ridurre, si definisce l'elenco dei controlli da implementare per ridurre il rischio ad un livello accettabile procedendo al calcolo del Rischio Residuo inteso come il prodotto scalare del valore dell'asset per la minaccia decurtata del valore dei controlli di sicurezza selezionati al fine di ricondurre il rischio effettivo ai livelli desiderati:

$$R^{res}(n)=A(n) \times (T(n) - C^{sel}(n))$$

individuando il valore di $\mathbf{C}^{sel}(n)$ secondo le modalità discusse per il calcolo del rischio effettivo. Chiaramente, in questo caso, l'input non è dato dalla valutazione dei controlli in essere, ma dall'individuazione automatica del livello di attivazione dei controlli necessario al raggiungimento del livello di rischio definito accettabile.

Per ogni valore di rischio risultante è compito dell'ISM, avvalendosi se necessario di competenze specialistiche, ottenere una valutazione sul costo connesso all'implementazione dei singoli controlli, in modo da consentire una loro corretta valutazione.

Quando possibile, è fornita anche una valutazione del costo associato al trasferimento del rischio, in modo da consentire una valutazione completa delle opzioni.

Conseguentemente, per ogni rischio, è compito dell'ISM selezionare i controlli maggiormente efficienti nella gestione dei rischi cui sono connessi.

4.6.17 Modalità di selezione dei controlli

ACME BCRS seleziona i propri controlli mediante il controllo di gestione della sicurezza delle informazioni fornito dal tool utilizzato nelle fasi di risk assessment e risk management.

Attraverso i "cruscotti" di gestione della sicurezza delle informazioni, separati per ambiente infrastrutturale, è possibile infatti selezionare e ponderare i controlli necessari a gestire le minacce di cui al momento non è gestito il rischio entro i limiti accettati.

Fattivamente, per ogni minaccia o rischio evidenziato si individuano i controlli attivabili al fine di ridurne la dannosità. La scelta dei controlli, condivisa con l'ISSF, è formalizzata nell'apposita sezione del Risk Treatment Plan.

4.7 Manuale della Sicurezza IT

E' il manuale della sicurezza IT, analogo al manuale della qualità, in esso i vari attori dei processi di ITC, trovano le motivazioni dei vari controlli messi

in essere, nonché i riferimenti alle normative (politiche specifiche, standards, linee guida o procedure di sicurezza) il cui rispetto assicura il mantenimento dei livelli di sicurezza prescelti.

Esso copre tutti i dieci domini del BS7799:2002, ma per motivi di spazio vengono riportati come esempio solo i domini riferiti alla sicurezza organizzativa e a quella fisica.

4.7.1 Information security infrastructure

A.4.1 Information security infrastructure	4.1
Control objective: To manage information security within the organization.	

La protezione del personale e degli asset informativi dell'ACME è una responsabilità fondamentale del management di ACME. Fra gli asset che ACME si prefigge di proteggere ci sono sia gli asset fisici che finanziari, sia le tecnologie che tutte le altre informazioni concernente la conduzione del business di ACME. I programmi di protezione di ACME sono stati sviluppati per aiutare il management a questo proposito. L'esecuzione e la conformità a questi programmi è responsabilità di tutti i manager, e la loro efficacia dipende dall'applicazione del programma di sicurezza da parte di ogni manager.

Le responsabilità di ciascun manager in tema di sicurezza sono espresse chiaramente nella sezione dedicata del sito Management Security Responsibilities. L'elenco e la distribuzione geografica dei contatti regionali di sicurezza (EMEA Director of Security, Manager of Investigations, Case Mgr. Investigations, Department Secretary) è presente nella pagina sul web di cui si fornisce qui il link: Organization and Contacts

Il sistema di gestione della sicurezza delle informazioni di ACME BCRS, quindi, partendo dall'organizzazione di sicurezza già presente in ACME, si fonda su una struttura già collaudata, nella quale ACME BCRS ha ulteriormente specificato i ruoli di sicurezza che ha ritenuto opportuno per gestire al meglio la sicurezza dei propri asset e rispondere ai requisiti della BS7799.

ACME BCRS all'interno del documento ACME BCRS Organizational Model definisce un modello organizzativo di sicurezza di riferimento implementato nell'attuale organigramma di ACME BCRS.

Sulla base del modello vengono attribuite le responsabilità e i ruoli per la sicurezza delle informazioni, come approfondite nel documento Security Roles Job description

4.7.1.1 Management information security forum

Rif. BS7799 4.1.1	A management forum to ensure that there is clear direction and visible management support for security initiatives shall be in place. The management forum shall promote security through appropriate commitment and adequate resourcing.	

ACME BCRS ha individuato e nominato un comitato per il coordinamento delle iniziative di sicurezza (ISSF - Information Security Steering Forum), composto di persone provenienti da diverse aree aziendali. Il BCRS Information Security Steering Forum si riunisce periodicamente per valutare lo stato attuale della sicurezza e promuovere trasversalmente su tutta ACME BCRS le azioni necessarie.

L'ISSF è composto dalle seguenti figure:

- ACME BCRS South Leader;
- Information Security Manager;
- Site Manager di Roma.

Sarà inoltre possibile, all'occorrenza, invitare altre figure che per competenza e ruolo ricoperto, possano fornire il supporto necessario.

- Per i dettagli sulle responsabilità e le funzioni coinvolte nel forum si rimanda al documento BCRS Job Description.

4.7.1.2 Information security co-ordination

Rif. BS7799 4.1.2	In large organizations, a cross-functional forum of management representatives from relevant parts of the organization shall be used to coordinate the implementation of information security controls.	

ACME BCRS ha individuato e nominato un comitato per l'implementazione delle misure di sicurezza (ISCC - Information Security Cross-functional Committee), composto di persone provenienti da diverse aree aziendali. L'Information Security Commitee BCRS si riunisce periodicamente per valutare lo stato di implementazione della sicurezza e pianificare le attività necessarie.

L'ISCC è composto dalle seguenti figure:

- Information Security Manager;
- Organizational Security Referent;
- Technological Security Referent;
- Delivery Security Referent;
- Referenti esterni a ACME BCRS, specialisti nel loro ambito di competenza.

Per i dettagli sulle responsabilità e le funzioni coinvolte nel committee si rimanda al documento BCRS Job Description.

4.7.1.3 Allocation of information security responsibilities

Rif. BS7799 4.1.3	Responsibilities for the protection of individual assets and for carrying out specific security processes shall be clearly defined.	

ACME BCRS adotta un modello organizzativo di sicurezza delle informazioni sulla base del quale attribuire le responsabilità di sicurezza delle informazioni.

Sono stati individuati i principali ruoli e le principali responsabilità di carattere decisionale previsti per la gestione della sicurezza delle informazioni all'interno di ACME BCRS, di cui si riporta sotto un breve elenco dei principali:

- ACME BCRS South Leader, promuove la realizzazione e l'applicazione dell'ISMS e si occupa in prima persona di approvare la Security Policy e della nomina delle altre persone designate;
- L'Information Security Manager, rappresenta il referente e la guida principale per le tematiche inerenti la Sicurezza delle informazioni.
- Security Referent, costituisce, secondo le proprie competenze reali all'interno della struttura organizzativa di ACME BCRS, l'elemento di raccordo per tutte le tematiche legate alla definizione, all'implementazione ed al controllo delle misure di sicurezza aziendali. A seconda della propria responsabilità e ruoli sono stati individuati i seguenti referenti di sicurezza:
- Organizational Security Referent
- Technological Security Referent
- Delivery Security Referent

Il documento che formalizza i suddetti ruoli e responsabilità di sicurezza, nonché tutti gli altri ruoli e responsabilità necessari per garantire l'adeguata protezione degli asset informativi di ACME BCRS è il seguente: ACME BCRS Job Description.

4.7.1.4 Authorization process for information processing facilities

Rif. BS7799 4.1.4	A management authorization process for new information processing facilities shall be established.	

ACME ritiene fondamentale per la protezione degli asset

informativi aziendali una corretta gestione delle autorizzazioni alle processing facilities. A tal fine ha pubblicato regole ben definite all'interno dello standard di sicurezza ITCS104 - Authorization. La procedura descritta nel documento applica la strategia di sicurezza dell'ACME, che intende gestire l'assegnazione e il diniego dell'accesso ai servizi ed alle informazioni, basandosi su un'identità autenticata, in funzione del bisogno specifico di business delle persone interessate.

A completezza del processo, ACME gestisce, con modalità formalizzata e controllata, anche l'acquisizione delle information processing facilities mediante la seguente procedura :

BB100: Purchasing requisition approval for goods/services

ACME BCRS oltre a recepire i principi e le procedure che la corporate ACME applica nella gestione delle autorizzazioni agli asset informativi, ha previsto ulteriori disposizioni puntuali.

Sono stati previsti pertanto processi di autorizzazione per l'installazione di nuove componenti IT (hardware e software) e formalizzati nel documento presente sul database CMT- Gestione ordini ed inventario Asset BCRS. All'interno del processo sono stati previsti i seguenti Task:

1. approvazione manageriale (di linea)
2. approvazione tecnica (compatibilità tecnologica)
3. approvazione di sicurezza (risposta ai requisiti di sicurezza)
4. utilizzo di asset personali (modem, pc a casa, software di proprietà dei singoli, ..)

Per quanto attiene al punto 3, non è prevista un'autorizzazione in quanto le nuove componenti IT devono rispettare gli standard definiti a priori.

4.7.1.5 Specialist information security advice

Rif. BS7799 4.1.5	Specialist advice on information security shall be sought from either internal or external advisors and coordinated throughout the organization.	

ACME BCRS, riconosce alla propria organizzazione di sicurezza (comprensiva, quindi di ISSF e Sec Committee) specifiche com-

petenze di sicurezza ritenute sufficienti per la gestione corrente e continuativa della sicurezza dei propri asset informativi. Tuttavia ACME BCRS riconosce che, a fronte di particolari problematiche, tali competenze possano non risultare esaustive e debbano essere integrate secondo specifiche esigenze mediante l'utilizzo di risorse esterne a ACME BCRS.

A tal fine all'ISM è assegnata la responsabilità di gestire i rapporti con terze parti che possano di volta in volta rendersi necessarie per approfondire o gestire direttamente particolari tematiche di sicurezza. In questo, è sua responsabilità gestire le convocazioni dell'ISCC, invitando i responsabili, interni ed esterni ad ACME, dei reparti, o loro delegati, investiti dalle competenze richieste, in funzione delle finalità rilevanti.

In particolar modo ACME BCRS, a titolo d'esempio non esaustivo, può avvalersi di specialisti esterni alla propria struttura o a quella di ACME, ovvero di consulenze esterne, per le seguenti attività:

- Analisi dei rischi
- Supporto all'adozione delle misure di sicurezza
- Formazione
- Specifici servizi (es. sorveglianza delle sedi, ..)
- …

4.7.1.6 Co-operation between organizations

Rif. BS7799 4.1.6	Appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunications operators shall be maintained.	

All'ISM è assegnata la responsabilità di gestire i rapporti con terze parti che possano di volta in volta rendersi necessarie per approfondire o gestire direttamente particolari tematiche di sicurezza. In questo, inoltre, riceve guida funzionale dall'ISSF e si incarica di mantenere costanti contatti con i principali enti esterni di sicurezza (enti regolamentari, autorità legislative, service providers, operatori in ambi-

to telecomunicazioni) al fine di garantire un continuo interscambio di informazioni relative agli elementi utili a prevenire o risolvere incidenti di sicurezza.

4.7.1.7 Independent review of information security

Rif. BS7799 4.1.7	The implementation of the information security policy shall be reviewed independently.	

ACME BCRS ha schedulato un esame indipendente della politica di sicurezza da parte della funzione di audit ACME. Inoltre l'aderenza della politica agli standard di riferimento è verificata annualmente nel corso delle attività di rinnovo della certificazione da parte di terze parte abilitate

4.7.2 Physical and environmental security

A.7.1 Secure areas	7.1
Control objective: To prevent unauthorized physical access, damage and interference to business premises and information.	

ACME reputa da sempre fondamentale la sicurezza fisica degli asset aziendali.

ACME ha dedicato all'interno del sito Intranet una sezione su tutto il materiale di riferimento per la corretta gestione della sicurezza fisica : ACME Security Manual – Phisical Security (PS)

Il già menzionato Security Manual, così come il Security Guidelines, ha una sezione dedicata , Physical Security (PS), che dettaglia al suo interno i seguenti argomenti:

- Risk Analysis - Additional Evaluated Controls (PS00)
- Exterior Security (PS01)
- Building Perimeters and Interior Security (PS02)

- Mail Services Security (PS03)
- Lock and Key Controls (PS04)
- ACME Access Controls and Badge Designs (PS05)
- Security Control Center (PS06)
- ACME Search Policy (PS11)

Lo standard ITCS104, Physical Access Controls, enuncia con chiarezza la strategia di sicurezza IT dell'ACME: attenuare il rischio di furto o danneggiamento degli asset informativi, rilevazione o cancellatura non autorizzata delle informazioni dell'ACME ed interruzione dei processi di ACME che possono derivare da accesso fisico non autorizzato alle risorse legate all'informazione e agli asset informativi.

ACME BCRS, quindi, recependo quanto riportato nella documentazione Corporate ACME in tema di protezione delle informazione e degli asset informativi, e le regole predisposte da Telco Provider, ha definito per il Sito di Roma ulteriori regole per l'accesso al sito e agli asset. Tali regole sono raccolte all'interno di un documento controllato, cui dovranno attenersi sia i dipendenti che le terze parti (clienti, outsourcer, ecc...): BCRS - Procedura accessi Centro BCRS Roma

4.7.2.1 Physical Security Perimeter

Rif. BS7799 7.1.1	Organizations shall use security perimeters to protect areas that contain information processing facilities.	

Le linee guida per il controllo del perimetro di sicurezza fisico sono state implementate nel ITCS104 Information Technology Security Standards .

In particolare è stata fatta una chiara definizione del perimetro di sicurezza. Il perimetro di un sito che ospita una sala CED è fisicamente isolato (non esistono varchi che consentono intrusioni), i muri esterni sono di solida costruzione e le porte esterne sono protette contro accessi non autorizzati (es. meccanismi di controllo, allarmi, serrature).

Esiste una reception atta a controllare gli accessi fisici al sito delle sole persone autorizzate. Le porte antincendio dentro il perime-

tro di sicurezza sono allarmate e dotate di un meccanismo di blocco automatico (le porte sono sempre apribili per far fronte alle emergenze.

L'obiettivo primario è il controllo dell'ingresso (controllare che non entri nessuno), non dell'uscita (motivo di tutela della safety).

4.7.2.2 Physical Entry Controls

Rif. BS7799 7.1.2	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	

ACME ha prodotto una brochure per dare le principali informazioni di sicurezza a tutto il personale e terze parti che devono accedere all'interno di siti ACME: Security pamphlet 2004.

L'opuscolo è dato solitamente al personale ed alle terze parti dell'ACME durante l'induction di sicurezza, in occasione del rilascio del badge ACME.

Sono stati implementati all'interno delle aree classificate come riservate i seguenti controlli :

- I visitatori sono identificati e viene registrata l'ora di ingresso ed uscita dal sito
- I diritti di accesso alle aree riservate sono assegnati sulla base di una procedura formalizzata
- I diritti di accesso alle aree riservate sono regolarmente verificati ed aggiornati
- Il personale adotta misure di riconoscimento a vista (es. Badge sempre visibilmente esposto) ed è invitato a chiedere l'identità di chiunque non adotti tali misure

I log alle aree riservate sono crittografati e non resi leggibili a tutti per motivi sindacali.

La videosorveglianza è presente solo in aree pubbliche, le relative registrazioni sono conservate per una settimana: la loro visione è accessibile solo ai responsabili della sicurezza in caso di incidenti

Periodicamente, ogni 3 mesi, viene rivista la lista delle autorizzazioni.

4.7.2.3 Securing offices, rooms and facilities

Rif. BS7799 7.1.3	Secure areas shall be created in order to protect offices, rooms and facilities with special security requirements.	

ACME ha previsto, così come richiesto dalle sue policies e procedure (Information Technology Security Standards (ITCS104), l'insieme di controlli sotto riportati per tutelare la sicurezza degli edifici, degli uffici e delle apparecchiature:

- Meccanismi atti ad impedire l'accesso a persone non autorizzate
- Porte e finestre chiuse in assenza di presidio dei locali
- Protezioni esterne applicate alle finestre (in particolare per quelle al piano terra) (In base alla classificazione delle aree le finestre possono essere antisfondamento, oppure soltanto a doppio vetro e regolarmente chiuse).
- Le porte esterne, le finestre facilmente raggiungibili, e le aree non presidiate sono dotate di sistemi antintrusione progettati secondo standard internazionali certificati, e regolarmente testati. Il perimetro esterno è protetto H24 (ad eccezione delle due portinerie), alcune aree sono presidiate con sensori e grigliati con sistema di antintrusione.
- La documentazione inerente la sala CED (localizzazione, ubicazione dei server, ecc.) è protetta in modo da impedire la consultazione/sottrazione da parte di persona non autorizzate
- I materiali pericolosi od infiammabili sono collocati in aree distanti dalle aree riservate (es. sala CED)
- I dati di backup e le risorse atte a garantire il ripristino sono collocate in un edificio diverso da quello in cui sono principalmente gestiti i dati
- Videosorveglianza esterna per i perimetri critici

4.7.2.4 Working in secure areas

Rif. BS7799 7.1.4	Additional controls and guidelines for working in secure areas shall be used to enhance the security of secure areas.	

ACME prevede, come descritto nello standard Information Technology Security Standards (ITCS104), per consentire al suo personale di lavorare in aree sicure, che il personale sia a conoscenza delle attività svolte all'interno dell'area in funzione del "need to know".

Le aree protette non presidiate devono essere chiuse e sono oggetto di periodici controlli.

Le terze parti (es. personale delle pulizie) hanno accesso autorizzato alle aree protette limitato all'espletamento del servizio (Alle aree più ristrette è vietato l'ingresso anche al personale delle pulizie).

Barriere aggiuntive sono attivate in presenza di aree, all'interno del perimetro di sicurezza, con differenti diritti di accesso.

Attrezzature quali macchine fotografiche, videocamere sono vietate. Le eccezioni sono gestite event by event.

4.7.2.5 Isolated delivery and loading areas

Rif. BS7799 7.1.5	Delivery and loading areas shall be controlled, and where possible, isolated from information processing facilities to avoid unauthorized access.	

ACME ha deciso, a livello Corporate, di redigere delle linee guida sui processi logistici aziendali ed in particolare delle specifiche istruzioni sui controlli delle aree di carico e scarico delle merci: Global Logistics Guidelines.

Le aree di consegna e carico sono isolate rispetto alle aree protette al fine di evitare accessi non autorizzati.

I requisiti di sicurezza per le aree di consegna e carico sono stati definiti sulla base di un'analisi dei rischi realizzata con frequenza annuale per tutti i siti. Il Database è gestito a livello emea

Per tutelare la sicurezza nelle aree di consegna e carico sono stati implementati i seguenti controlli:

- o L'accesso alle aree di attesa dall'esterno del sito è consentito solo al personale identificato ed autorizzato
- o L'area è strutturata in modo tale che lo scarico delle merci in entrata non consente agli addetti alle consegne di accedere ad altre parti dell'edificio
- o Gli accessi esterni alle aree di consegna e carico sono chiusi quando le porte interne sono aperte
- o Il materiale in entrata è soggetto ad ispezioni prima della sua collocazione nelle postazioni di utilizzo
- o Il materiale in entrata è registrato all'atto dell'ingresso nel sito

4.7.3 Equipment security

A.7.2 Equipment security	7.2
Control objective: To prevent loss, damage or compromise of assets and interruption to business activities.	

4.7.3.1 Equipment siting and protection

Rif. BS7799 7.2.1	Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	

Per quanto riguarda la collocazione e protezione degli asset aziendali, ACME implementa quanto segue:

- o Gli elaboratori per il trattamento e la conservazione di dati riservati e/o sensibili sono posizionati in modo da ridurre i rischi di accessi a letture non autorizzate durante il loro utilizzo

- Le apparecchiature che richiedono particolari misure di sicurezza sono isolate per abbassare il livello di protezione richiesto
- Sono implementati controlli per minimizzare il rischio di potenziali minacce come, furti, incendi, esplosivi, fumo, acqua, polvere, vibrazioni, effetti chimici, interferenze delle forniture elettriche, radiazioni elettromagnetiche
- E' stata definita una policy che disciplina la possibilità di mangiare, bere e fumare in prossimità di elaboratori che processano le informazioni
- E' stato valutato il potenziale impatto di eventi disastrosi che si verifichino in prossimità delle aree protette (es. incendio nell'edificio adiacente)
- Nella risk analisys è valutato il rischio anche sull'ambiente esterno

4.7.3.2 Power supplies

Rif. BS7799 7.2.2	Equipment shall be protected from power failures and other electrical anomalies.	

Sono presenti i seguenti sistemi di continuità nella fornitura di energia:

- Alimentazione multipla per ovviare a possibili "point of failure" del sistema di alimentazione
- Alimentazione di emergenza (UPS) per le attrezzature che supportano le attività critiche di business
- Generatore di riserva per ovviare a una prolungata caduta di tensione elettrica
- Interruttori della corrente posizionati in vicinanza dell'uscita di emergenza delle aree contenenti le attrezzature per consentire una rapida interruzione della corrente in

caso di emergenza

- Luci di emergenza in caso di black-out
- Parafulmini in tutti i siti

4.7.3.3 Cabling security

Rif. BS7799 7.2.3	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.	

Come tutti i siti dove ACME ha una sede, il sito di Roma è conforme alla norma ITCS 104.

4.7.3.4 Equipment maintenance

Rif. BS7799 7.2.4	Equipment shall be correctly maintained to enable its continued availability and integrity.	

Per quanto attiene alla manutenzione delle attrezzature:

- La manutenzione avviene in conformità alle istruzioni dei produttori
- Le riparazioni sono effettuate solo da personale specialistico
- I guasti sospetti o effettivi e la manutenzione preventiva e correttiva sono registrati
- Accurati controlli sono effettuati quando le attrezzature sono manutenute all'esterno dei locali aziendali

4.7.3.5 Security of equipment off-premises

Rif. BS7799 7.2.5	Any use of equipment for information processing outside an organization's premises shall require authorization by management.	

Per tutelare la sicurezza delle attrezzature utilizzate all'esterno dei locali aziendali ACME implementa i seguenti controlli:

- Le attrezzature portate all'esterno sono custodite con particolare attenzione nelle aree pubbliche ed i laptop sono trasportati in apposite valigie durante il trasporto
- Le istruzioni del produttore sono osservate per proteggere le attrezzature da minacce esterne (es. protezione da campi elettromagnetici)
- La necessità dell'home-working è valutata in funzione dei rischi che ne potrebbero derivare
- Esistono coperture assicurative adeguate

4.7.3.6 Secure disposal or re-use of equipment

Rif. BS7799 7.2.6	Information shall be erased from equipment prior to disposal or re-use.	

I dati memorizzati sono cancellati senza possibilità di recupero degli stessi in occasione della dismissione o riutilizzo delle attrezzature e dei supporti.

4.7.4 General controls

A.7.4 General controls	7.2
Control objective: To prevent compromise or theft of information and information processing facilities	

4.7.4.1 Clear desk and clear screen policy

Rif. BS7799 7.3.1	Organizations shall have a clear desk and a clear screen policy aimed at reducing the risks of unauthorized access, loss of, and damage to information.	

ACME BCRS ha deciso di raccogliere tutte le istruzioni di sicurezza, che ritiene indispensabili per la protezione dei suoi asset informativi, da mettere in atto da parte di tutto il personale, in uno standard: Security and Use Standards for ACME Employees (ITCS300).

Fra le altre istruzioni è stata definita una adeguata clear desk and screen policy.

Inoltre sono implementati, come da ITCS 300, i seguenti controlli:

- La documentazione ed i supporti informatici sono riposti in armadi chiusi a chiave quando non usati, in particolare al di fuori dell'orario di lavoro
- I PC, i terminali e le stampanti sono protetti da accessi non autorizzati mediante chiavi di chiusura, password.
- Le fotocopiatrici sono spente o comunque protetti da un loro utilizzo non autorizzato al di fuori dell'orario di lavoro

Le informazioni riservate, una volta stampate, vengono ritirate con sollecitudine dalla stampante

4.7.4.2 Removal of property

Rif. BS7799 7.3.2	Equipment, information or software belonging to the organization shall not be removed without authorization of the management.	

ACME, ritenendo fondamentale per la protezione delle informazioni che la riguardano una corretta e puntuale gestione del trasfe-

rimento degli asset informativi, ha deciso di regolamentare il trasferimento/spostamento degli asset aziendali (attrezzature, informazioni, software, ecc.) attraverso delle linee guida a livello Corporate specifiche sull'argomento: Global Logistics Guidelines.

4.8 Statement of applicability (SOA)

E' il documento che va preparato per definire quali dei controlli individuati dallo standard sono applicabili al contesto da certificare.

Anche in questo caso si riporta solo un estratto del SOA, ed in particolare si riportano le aree relative all'organizzazione della sicurezza e alla sicurezza fisica.

Controllo	Selezionato	Dettagli di Applicazione	Requisiti e Giustificazione	Documentazione a supporto
A.4 Information Security Infrastructure				
A.4.1 Organizational security				
A.4.1.1 Management information security forum (Comitato di gestione della sicurezza delle informazioni)	YES	Controllo normato e implementato a livello di intero Scope di certificazione	ACME BCRS seleziona il controllo per istituire un Forum cui attribuire, tra le altre, le responsabilità di promuovere l'applicazione della Politica di Sicurezza delle Informazioni e, in generale, dell'ISMS, di valutare e monitorare lo stato attuale della sicurezza all'interno dello Scope, di pianificare le azioni di miglioramento	L'applicazione del controllo è regolamentata dai seguenti documenti: ACME BCRS Information Security Policy ACME BCRS Security Guidelines ACME BCRS IS Security Roles & Job Descriptions
A.4.1.2 Information security co-ordination (Coordinamento in materia di sicurezza delle informazioni)	YES	Controllo normato e implementato a livello di intero Scope di certificazione	ACME BCRS seleziona il controllo per istituire un Comitato cui attribuire, tra le altre, le responsabilità di definire metodologie e processi di audit della sicurezza delle informazioni, di proporre, supportare e coordinare iniziative di sicurezza su tutta l'ACME e di verificarne la corretta implementazione a livello BCRS	ACME BCRS Information Security Policy ACME BCRS Security Guidelines ACME BCRS IS Security Roles & Job Descriptions

Controllo	Selezionato	Dettagli di Applicazione	Requisiti e Giustificazione	Documentazione a supporto
A.4.1.3 Allocation of information security responsibilities (Attribuzione delle responsabilità in materia di sicurezza delle informazioni)	YES	Controllo normato e implementato a livello di intero Scope di certificazione	Il controllo è selezionato per rispondere all'esigenza di individuare in modo puntuale ed esaustivo le responsabilità attinenti alla sicurezza delle informazioni.	L'applicazione del controllo è regolamentata dai seguenti documenti: ACME BCRS Security Guidelines ACME BCRS IS Security Roles & Job Descriptions
A.4.1.4 Authorization process for information processing facilities (Processo autorizzativo per i nuovi componenti hardware e software)	YES	Controllo normato e implementato a livello di intero Scope di certificazione	BCRS seleziona il controllo al fine di implementare un corretto presidio della propria infrastruttura di elaborazione delle informazioni. In recepisce le procedure ACME di autorizzazione all'inserimento di nuove componenti hardware e software	L'applicazione del controllo è regolamentata dai seguenti documenti: ACME BCRS IS Manual (cap.4) Gestione ordini ed inventario Asset BCRS

Controllo	Selezionato	Dettagli di Applicazione	Requisiti e Giustificazione	Documentazione a supporto
A.4 Information Security Infrastructure				
A.4.1.5 Specialist information security advice (Consulenza di specialisti in materia di sicurezza delle informazioni)	YES	Controllo normato e implementato a livello di intero Scope di certificazione, e implementato in funzione delle specifiche esigenze progettuali, e in base alle valutazioni contenute negli nei documenti inerenti i singoli progetti	A causa della complessità del panorama che caratterizza le problematiche correlate alla sicurezza delle informazioni, e a garanzia di un'efficace implementazione dell'ISMS, BCRS considera opportuno il ricorso all'ausilio di consulenti esterni allo scope in funzione delle specifiche esigenze di sicurezza delle informazioni.	L'applicazione del controllo è regolamentata dai seguenti documenti: ACME BCRS IS Manual (cap.4) ACME BCRS Risk Management
A.4.1.6 Co-operation between organizations (Collaborazione fra organizzazioni)	YES	Controllo normato e implementato a livello di intero Scope di certificazione	BCRS considera opportuno, anche ai fini di un continuo aggiornamento in materia, cooperare con organizzazioni che si occupano di aspetti della sicurezza delle informazioni.	L'applicazione del controllo è regolamentata dai seguenti documenti: ACME BCRS IS Security Roles & Job Descriptions

Controllo	Selezionato	Dettagli di Applicazione	Requisiti e Giustificazione	Documentazione a supporto
Independent review of information security (Revisione indipendente in materia di sicurezza delle informazioni)	YES	Controllo normato e implementato a livello di intero Scope di certificazione	BCRS considera opportuno, in linea con il principio della separazione delle responsabilità, la pianificazione e svolgimento, con il supporto di personale qualificato esterno, di attività di revisione dello stato di formalizzazione e applicazione dell'ISMS. In questo senso, è previsto lo svolgimento di audit annuali (mediamente due volte l'anno)	L'applicazione del controllo è regolamentata dai seguenti documenti: QMX: IT-PRC-00629
A.4.2 Security of third part access				
A.4.2.1 Identification of risks from third party access (Identificazione dei rischi di accesso da parte delle terze parti)		Non trattato nell'esempio	Non trattato nell'esempio	Non trattato nell'esempio
A.4.2.2 Security requirements in third party contracts (Requisiti di sicurezza nei contratti con terze parti)		Non trattato nell'esempio	Non trattato nell'esempio	Non trattato nell'esempio

Controllo	Selezionato	Dettagli di Applicazione	Requisiti e Giustificazione	Documentazione a supporto
A.4.3 Outsourcing				
A.4.3.1 Security requirements in outsourcing (Requisiti di sicurezza nei contratti di outsourcing)		Non trattato nell'esempio	Non trattato nell'esempio	Non trattato nell'esempio
A.7 Physical and environmental security				
A.7.1 Secure Areas				
A.7.1.1 Physical security perimeter (Perimetro di sicurezza fisica)	YES	La specificazione delle misure di sicurezza fisica è giustificata dall'esigenza di salvaguardare gli asset informativi.	La specificazione delle misure di sicurezza fisica è giustificata dall'esigenza di salvaguardare gli asset informativi.	L'applicazione del controllo è regolamentata dai seguenti documenti: ACME BCRS Security Guidelines Procedura di gestione accessi fisici Centro BCRS (QMX: IT-PRC-00619) ACME BCRS IS Manual (cap.7)
A.7.1.2 Physical entry controls (Controllo degli accessi fisici)	YES	Controllo normato e implementato a livello di intero Scope di Certificazione	La specificazione della misura di sicurezza fisica è giustificata dall'esigenza di salvaguardare in modo opportuno le risorse informative consentendo l'accesso in modo selettivo al solo personale esplicitamente autorizzato.	L'applicazione del controllo è regolamentata dai seguenti documenti: ACME BCRS Security Guidelines Procedura di gestione accessi fisici Centro BCRS (QMX: IT-PRC-00619) ACME BCRS ISManual (cap.7)

Controllo	Selezionato	Dettagli di Applicazione	Requisiti e Giustificazione	Documentazione a supporto
A.7.1.3 Securing offices, rooms and facilities (Sicurezza degli uffici, delle stanze e delle apparecchiature)		Controllo normato e implementato a livello di intero Scope di Certificazione	La specificazione della misura di sicurezza fisica è giustificata dall'esigenza di salvaguardare in modo opportuno le risorse informative consentendo l'accesso in modo selettivo al solo personale esplicitamente autorizzato.	L'applicazione del controllo è regolamentata dai seguenti documenti: ACME BCRS Security Guidelines Procedura di gestione accessi fisici Centro BCRS (QMX: IT-PRC-00619) ACME BCRS IS Manual (cap.7)
A.7.1.4 Working in secure areas (Lavoro in aree protette)	YES	Controllo normato e implementato a livello di intero Scope di Certificazione	BCRS attiva tale controllo per migliorare il livello di sicurezza delle aree aziendali. Tale controllo include le attività di terze parti svolte all'interno di tali aree.	L'applicazione del controllo è regolamentata dai seguenti documenti: ACME BCRS Security Guidelines ACME BCRS IS Manual (cap.7)
A.7.1.5 Isolated delivery and loading areas (Aree isolate per il carico e lo scarico)	YES	Controllo normato e implementato a livello di intero Scope diCertificazione.Nell'ambito del sito di Settimo si applicano modalità condivise tra BCRS e Telco Provider	La specificazione della misura di sicurezza fisica è giustificata dall'esigenza di salvaguardare in modo opportuno le risorse informative concedendo l'accesso in modo selettivo al solo personale esplicitamente autorizzato.	L'applicazione del controllo è regolamentata dai seguenti documenti: ACME BCRS IS Manual (cap.7)

Controllo	Selezio-nato	Dettagli di Applicazione	Requisiti e Giustificazione	Documentazione a supporto
A.7.2 Equipment security				
A.7.2.1 Equipment siting and protection (Posizionamento e protezione delle apparecchiature)	YES	Controllo normato e implementato a livello di intero Scope di Certificazione Nell'ambito del sito di Settimo si applicano modalità condivise tra BCRS e Telco Provider	BCRS attiva tale controllo per prevenire la perdita, il danneggiamento o l'alterazione degli asset aziendali e l'interruzione delle attività di business. Le apparecchiature devono essere collocate o protette in modo tale da ridurre il rischio da minacce ambientali e accessi non autorizzati. In questo BCRS verifica il livello di servizio garantito dal contratto con Telco Provider	L'applicazione del controllo è regolamentata dai seguenti documenti: Service level Agreement ACME –ISP ACME BCRS IS Manual (cap.7)
A.7.2.2 Power supplies (Alimentazione d'emergenza)	YES	Controllo normato e implementato a livello di intero Scope di Certificazione Nell'ambito del sito di Settimo si applicano modalità condivise tra BCRS e Telco Provider	Il controllo viene applicato al fine di garantire in modo opportuno la continuità dei servizi erogati e l'attività produttiva e proteggere le apparecchiature da cadute di tensione elettrica o altre anomalie. In questo BCRS verifica il livello di servizio garantito dal contratto con Telco Provider	L'applicazione del controllo è regolamentata dai seguenti documenti: Service level Agreement ACME –ISP ACME BCRS IS Manual (cap.7)

Controllo	Selezionato	Dettagli di Applicazione	Requisiti e Giustificazione	Documentazione a supporto
A.7.2 Equipment security				
A.7.2.1 Equipment siting and protection (Posizionamento e protezione delle apparecchiature)	YES	Controllo normato e implementato a livello di intero Scope di Certificazione Nell'ambito del sito di Settimo si applicano modalità condivise tra BCRS e Telco Provider	BCRS attiva tale controllo per prevenire la perdita, il danneggiamento o l'alterazione degli asset aziendali e l'interruzione delle attività di business. Le apparecchiature devono essere collocate o protette in modo tale da ridurre il rischio da minacce ambientali e accessi non autorizzati. In questo BCRS verifica il livello di servizio garantito dal contratto con Telco Provider	L'applicazione del controllo è regolamentata dai seguenti documenti: Service level Agreement ACME –ISP ACME BCRS IS Manual (cap.7)
A.7.2.2 Power supplies (Alimentazione d'emergenza)	YES	Controllo normato e implementato a livello di intero Scope di Certificazione Nell'ambito del sito di Settimo si applicano modalità condivise tra BCRS e Telco Provider	Il controllo viene applicato al fine di garantire in modo opportuno la continuità dei servizi erogati e l'attività produttiva e proteggere le apparecchiature da cadute di tensione elettrica o altre anomalie. In questo BCRS verifica il livello di servizio garantito dal contratto con Telco Provider	L'applicazione del controllo è regolamentata dai seguenti documenti: Service level Agreement ACME –ISP ACME BCRS IS Manual (cap.7)

Controllo	Selezionato	Dettagli di Applicazione	Requisiti e Giustificazione	Documentazione a supporto
A.7.2.3 Cabling security (Sicurezza del cablaggio)	YES	Controllo normato e implementato a livello di intero Scope di Certificazione Nell'ambito del sito di Settimo si applicano modalità condivise tra BCRS e Telco Provider	Il controllo viene applicato al fine di garantire in modo opportuno la continuità dei servizi erogati e l'attività produttiva. In questo BCRS verifica il livello di servizio garantito dal contratto con Telco Provider	L'applicazione del controllo è regolamentata dai seguenti documenti: Service level Agreement ACME –ISP ACME BCRS IS Manual (cap.7)
A.7.2.4 Equipment maintenance (Manutenzione delle apparecchiature)	YES	Il controllo viene applicato al fine di garantire in modo opportuno la continuità dei servizi erogati e l'attività produttiva. In questo BCRS segue le policies ACME e verifica il livello di servizio garantito dal contratto con Telco Provider	Il controllo viene applicato al fine di garantire in modo opportuno la continuità dei servizi erogati e l'attività produttiva e proteggere le apparecchiature da cadute di tensione elettrica o altre anomalie. In questo BCRS verifica il livello di servizio garantito dal contratto con Telco Provider	L'applicazione del controllo è regolamentata dai seguenti documenti: Service level Agreement ACME –ISP ACME BCRS IS Manual (cap.7) ACME BCRS Business Continuity Plan

Controllo	Selezionato	Dettagli di Applicazione	Requisiti e Giustificazione	Documentazione a supporto
A.7.2.5 Security of equipment off-premises (Sicurezza delle apparecchiature dislocate all'esterno dei locali aziendali)	NO		Non esistono nell'ambito di BCRS impianti e/o apparecchiature poste all'esterno dei locali aziendali	
A.7.2.6 Secure disposal or re-use of equipment (Controllo sul riutilizzo e sull'eliminazione delle apparecchiature)	YES	Controllo normato e implementato	Il controllo si rende necessario in quanto nel contesto del sistema informativo aziendale viene fatto uso di media device e di dispositivi per il trattamento delle informazioni.	L'applicazione del controllo è regolamentata dai seguenti documenti: ACME BCRS IS Manual (cap.7)
A.7.3 General controls				
A.7.3.1 Clear desk and clear screen policy (Politica per il clear desk e il clear screen)	YES	Controllo normato e implementato	Il controllo è selezionato BCRS per evitare un accesso alle informazioni non autorizzato . In questo, BCRS segue le policies ACME	L'applicazione del controllo è regolamentata dai seguenti documenti: ACME BCRS IS Manual (cap.7)
A.7.3.2 Removal of property (Trasferimento di beni aziendali)	YES	Controllo normato e implementato	BCRS attiva tale controllo affinché gli asset informativi non fuoriescano dal sito di Settimo senza specifica autorizzazione. In questo, BCRS segue le policies ACME	L'applicazione del controllo è regolamentata dai seguenti documenti: ACME BCRS IS Manual (cap.7)

Controllo	Selezio-nato	Dettagli di Applicazione	Requisiti e Giustificazione	Documentazione a supporto
A.7.2 Equipment security				
A.7.2.1 Equipment siting and protection (Posizionamento e protezione delle apparecchiature)	YES	Controllo normato e implementato a livello di intero Scope di Certificazione Nell'ambito del sito di Settimo si applicano modalità condivise tra BCRS e Telco Provider	BCRS attiva tale controllo per prevenire la perdita, il danneggiamento o l'alterazione degli asset aziendali e l'interruzione delle attività di business. Le apparecchiature devono essere collocate o protette in modo tale da ridurre il rischio da minacce ambientali e accessi non autorizzati. In questo BCRS verifica il livello di servizio garantito dal contratto con Telco Provider	L'applicazione del controllo è regolamentata dai seguenti documenti: Service level Agreement ACME –ISP ACME BCRS IS Manual (cap.7)
A.7.2.2 Power supplies (Alimentazione d'emergenza)	YES	Controllo normato e implementato a livello di intero Scope di Certificazione Nell'ambito del sito di Settimo si applicano modalità condivise tra BCRS e Telco Provider	Il controllo viene applicato al fine di garantire in modo opportuno la continuità dei servizi erogati e l'attività produttiva e proteggere le apparecchiature da cadute di tensione elettrica o altre anomalie. In questo BCRS verifica il livello di servizio garantito dal contratto con Telco Provider	L'applicazione del controllo è regolamentata dai seguenti documenti: Service level Agreement ACME –ISP ACME BCRS IS Manual (cap.7)

5 - Appendice B: Codici deontologici delle certificazioni di competenza del personale

5.1 ISACA® Code of Professional Ethics (www.isaca.org/codeofethics.htm)

ISACA® sets forth this Code of Professional Ethics to guide the professional and personal conduct of members of the association and/or its certification holders.

Members and ISACA certification holders shall:

1. Support the implementation of, and encourage compliance with, appropriate standards, procedures and controls for information systems.
2. Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards and best practices.
3. Serve in the interest of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and not engage in acts discreditable to the profession.
4. Maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.

5. Maintain competency in their respective fields and agree to undertake only those activities, which they can reasonably expect to complete with professional competence.
6. Inform appropriate parties of the results of work performed; revealing all significant facts known to them.
7. Support the professional education of stakeholders in enhancing their understanding of information systems security and control.

Failure to comply with this Code of Professional Ethics can result in an investigation into a member's, and/or certification holder's conduct and, ultimately, in disciplinary measures.

5.2 (ISC)² Code of Professional Ethics (https://www.isc2.org/cgi/content.cgi?category=12#code)

All information systems security professionals who are certified by (ISC)² recognize that such certification is a privilege that must be both earned and maintained. In support of this principle, all (ISC)² members are required to commit to fully support this Code of Ethics (the "Code"). (ISC)² members who intentionally or knowingly violate any provision of the Code will be subject to action by a peer review panel, which may result in the revocation of certification.

There are only four mandatory canons in the code. By necessity, such high-level guidance is not intended to be a substitute for the ethical judgment of the professional.

Additional guidance is provided for each of the canons. While this guidance may be considered by the board of directors in judging behaviour, it is advisory rather than mandatory. It is intended to help professionals identify and resolve the inevitable ethical dilemmas that they will confront during the course of their information security career.

Code of Ethics Preamble:

- Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behaviour.
- Therefore, strict adherence to this Code is a condition of certification.

Code of Ethics Canons:

- Protect society, the commonwealth, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principals.
- Advance and protect the profession.

The following additional guidance is given regarding pursuit of these goals.

Objectives for Guidance

In arriving at the following guidance, the committee is mindful of its responsibility to:

- Give guidance for resolving good versus good and bad versus bad dilemmas.
- To encourage right behaviour such as:
- Research
- Teaching
- Valuing the certificate
- To discourage such behaviour as:
    - Raising unnecessary alarm, fear, uncertainty, or doubt
    - Giving unwarranted comfort or reassurance
    - Consenting to bad practice

- Attaching weak systems to the public network
- Professional association with non-professionals
- Professional recognition of or association with amateurs
- Associating or appearing to associate with criminals or criminal behaviour

These objectives are provided for information only; the professional is not required or expected to agree with them.

In resolving the choices that confront him or her, the professional should keep in mind that the following guidance is advisory only. Compliance with the guidance is neither necessary nor sufficient for ethical conduct.

Compliance with the preamble and canons is mandatory. Conflicts between the canons should be resolved in the order of the canons. The canons are not equal and conflicts between them are not intended to create ethical binds.

- Protect society, the commonwealth, and the infrastructure
- Promote and preserve public trust and confidence in information and systems.
- Promote the understanding and acceptance of prudent information security measures.
- Preserve and strengthen the integrity of the public infrastructure.
- Discourage unsafe practice.

Act honorably, honestly, justly, responsibly, and legally

- Tell the truth; make all stakeholders aware of your actions on a timely basis.
- Observe all contracts and agreements, express or implied.
- Treat all members fairly. In resolving conflicts, consider public safety and duties to principals, individuals, and the profession in that order.

- Give prudent advice; avoid raising unnecessary alarm or giving unwarranted comfort. Take care to be truthful, objective, cautious, and within your competence.
- When resolving differing laws in different jurisdictions, give preference to the laws of the jurisdiction in which you render your service.

Provide diligent and competent service to principals

- Preserve the value of their systems, applications, and information.
- Respect their trust and the privileges that they grant you.
- Avoid conflicts of interest or the appearance thereof.
- Render only those services for which you are fully competent and qualified.

Advance and protect the profession

- Sponsor for professional advancement those best qualified. All other things equal, prefer those who are certified and who adhere to these canons. Avoid professional association with those whose practices or reputation might diminish the profession.
- Take care not to injure the reputation of other professionals through malice or indifference.
- Maintain your competence; keep your skills and knowledge current. Give generously of your time and knowledge in training others.

6 - Appendice C: Case Studies sulla sicurezza fisica

In questa Appendice vengono sviluppati due Case Studies con l'obiettivo di evidenziare la complessità della verifica della sicurezza fisica, che, ad un primo livello di certificazione, dovrebbe essere verificato da un Lead Auditor BS7799.

6.1 Case study: sicurezza dell'alimentazione elettrica e condizioni ambientali in un data center

Pur non essendo possibile minimizzare la dipendenza dall'energia elettrica è, invece, possibile minimizzare la dipendenza da sorgenti che non garantiscono i livelli di affidabilità desiderati.

La disponibilità dell'energia elettrica può essere affidata a sistemi locali che si occupano di generare energia, in quegli istanti in cui la rete di distribuzione non è presente. Disponibilità è il concetto chiave che guida la progettazione dei sistemi ad alto rischio: non è ammessa nessuna interruzione nell'erogazione dell'energia elettrica.

Un altro aspetto che non va trascurato riguarda le condizioni ambientali in un data center. La temperatura e l'umidità infatti possono essere una sorgente di guasti e pertanto vanno opportunamente monitorate

A. Infrastruttura

Le infrastrutture che garantiscono il suddetto tipo di alimentazione non interrompibile sono tanto più complesse quanto più complessi sono i sistemi da alimentare. E' sempre richiesta un'attenta progettazione e analisi dell'ambiente elettrico e dei dispositivi che devono essere alimentati.

Ricordiamo che la normativa di riferimento di tipo generale per gli impianti elettrici è il documento CEI64-8.

Massimizzare la disponibilità significa minimizzare il "down-time" (vedi anche prossima figura), ovvero il tempo di non funzionamento del sistema. E' un fenomeno non programmato e non programmabile che può incidere negativamente sulle prestazioni globali. Minimizzare il "down-time" significa minimizzare i disservizi.

L'obiettivo è diminuire quanto più possibile le cause di guasto interne ed esterne che possono causare il collasso del sistema: mancanza di alimentazione elettrica, bassa qualità della stessa, guasti sui generatori,

guasti nella distribuzione e mancato coordinamento delle sorgenti sono alcune di esse.

Al fine di evitare l'accesso non autorizzato ai sistemi per la somministrazione di energia per il Data Center, si suggerisce di contenerli in armadi che tengano conto dei seguenti requisiti :

- l'armadio deve essere provvisto di accesso tramite chiave elettronica o badge, in possesso del solo personale autorizzato;
- ogni accesso deve essere rilevato e registrato dal sistema, a disposizione del responsabile della sicurezza;
- all'interno dell'armadio e associata ad ogni apertura della porta di accesso, si attiverà una fotocamera o videocamera che invierà e registrerà le immagini conseguenti per la identificazione dell'eventuale intruso non autorizzato da parte del responsabile della sicurezza;
- le pareti laterali dovranno essere fisse e non asportabili a posa in opera conclusa, così come la porta anteriore dovrà essere totalmente metallica , solo opportunamente forata o fessurata per consentire una corretta ventilazione degli apparati installati all'interno dell'armadio (salvo necessità di condizionamento forzato);
- l'accesso dei cavi all'interno dell'armadio, sia dal basso che dall'alto, dovrà essere provvisto di passa paratie meccanici, che non consentono l'accesso, dall'esterno, di altro ad eccezione del cavo .

Attuando i livelli di protezione, sopra descritti, l'attestazione dei cavi, la permutazione e l'interconnessione fra apparati dello stesso armadio può essere realizzata senza particolari ulteriori accorgimenti antintrusione.

Sono da prendere in considerazione soluzioni di gestione intelligente e da remoto degli armadi e di tutto l'hardware in essi contenuto, che sovrintendono a tutte le attività preventive e correttive che li riguardano.

B. I sistemi per la qualità dell'energia elettrica

I gruppi statici di continuità (UPS) sono dispositivi che oltre a garantire la continuità dell'alimentazione a fronte di assenza della rete elettrica permettono di avere costantemente un'alta qualità dell'energia elettrica stessa. Alta qualità significa erogazione elettrica con parametri perfetti nella quasi totalità del tempo di funzionamento del sistema. Ricordiamo che la normativa di riferimento per gli UPS è il documento EN62040/1,2,3. Il committente deve assicurarsi la piena rispondenza dell'UPS allo standard sopraccitato, chiedendo la certificazione dei prodotti eseguita da laboratori indipendenti riconosciuti a livello internazionale.

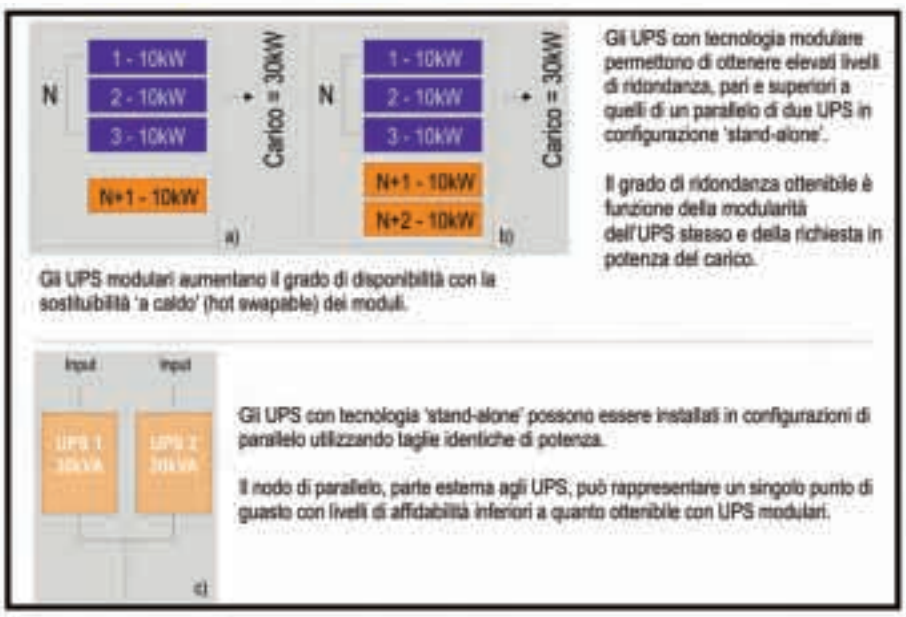
Esistono tre grandi famiglie di UPS:

- Stand-by o Off-line
- Interattivi o Line Interactive
- On-Line

I gruppi di continuità possono essere singoli, "stand-alone", o modulari, "power array"(vedi prossima figura).Un gruppo di continuità deve essere scelto in funzione delle necessità di affidabilità del sistema, in funzione della disponibilità richiesta.

Un singolo gruppo di continuità è legato all'affidabilità di una singola macchina; per aumentare l'affidabilità è necessario creare ridondanza di UPS, aggiungere una seconda unità.

Un UPS modulare garantisce una ridondanza intrinseca tale da essere pari o superiore a quella di due UPS stand-alone in parallelo.



Disponibilità di un sistema in funzione dei tempi di ripristino

E' possibile ottenere architetture modulari ad alti livelli di disponibilità. In questi casi tutti i componenti hardware sono ridondanti, modulari e sostituibili a caldo. E' una vera e propria infrastruttura comprendente tutti gli elementi necessari ad una struttura inserita in un contesto "Information Technology". Pertanto essa permette di installare UPS, quadro e distribuzione elettrica, armadi rack per l'alloggiamento degli apparati IT, distribuzione (eventualmente schermata) dei cavi di segnale, aria condizionata, controllo locale e remoto, etc.

Infrastrutture di questo tipo, nascendo già perfettamente pronte ad essere integrate in differenti configurazioni, garantiscono livelli di ingegnerizzazione difficilmente ottenibili con soluzioni tradizionali che, inoltre, richiedono rischiosi test sul campo per verificarne la funzionalità La possibilità di controllare da remoto i dispositivi, attraverso l'infrastruttura di rete, permette di conoscere in tempo reale eventuali anomalie del sistema e di porvi rimedio prima di ulteriori instabilità del sistema globale.

Gli strumenti di connettività vengono abbinati a strumenti di

reportistica. Conoscere l'andamento degli stati del sistema nel tempo consente l'identificazione di eventi ordinari o straordinari, esterni o interni al sistema che ne potrebbero pregiudicare la stabilità.

Il controllo da globale si diffonde fino al particolare permettendo l'analisi e la segnalazione di eventi associati sia a macro aree che a micro aree.

Il controllo può essere effettuato in maniera locale, remota autonoma o remota gestita dal costruttore e da diverse postazioni ridondanti, così da avere il controllo completo e sicuro del sistema ad ogni ora del giorno e della notte.

C. Sicurezza delle condizioni ambientali di un Data Center

L'hardware IT produce un inconsueto carico di calore concentrato e, al contempo, è molto sensibile alle variazioni di temperatura o di umidità. Un ambiente di sala tecnologica non ottimale può avere effetti negativi sia sull'elaborazione dei dati sia nell'archiviazione degli stessi. Uno sbalzo di temperatura o di umidità può causare problemi che variano dalla generazione di dati "senza senso" all'arresto completo del sistema.

- Effetti della temperatura sui componenti ICT: una temperatura ambiente diversa da quella di esercizio o rapide variazioni di temperatura possono alterare le caratteristiche dei componenti elettronici e fisici del pannello. Tali alterazioni possono provocare guasti transitori o permanenti nel sistema. In particolare i problemi transitori possono risultare molto difficili da diagnosticare e riparare.
- Effetti dell'umidità dell'aria sui componenti ICT. Elevata umidità dell'aria: condizioni di elevata umidità possono causare il deterioramento delle superfici, dei nastri magnetici, la rottura delle testine, fenomeni di condensa, corrosione, difficoltà di gestione della carta con conseguente guasto dei componenti e del pannello.

- Bassa umidità dell'aria: condizioni di bassa umidità aumentano la possibilità di scariche elettriche statiche, che possono provocare la corruzione dei dati e danneggiare l'hardware.

Per mantenere le apparecchiature di una sala tecnologica in condizioni ideali di esercizio la temperatura e l'umidità relativa (RH) dovrebbero essere rispettivamente pari a 22-24°C ed al 35-50%RH. L'hardware viene lasciato sempre acceso anche per prevenire rapide variazioni di temperatura.

I sistemi di condizionamento dell'aria di precisione sono progettati per mantenere la temperatura in un intervallo di 0,56°C (±1°F) e l'umidità a ±3-5% RH, 24 ore su 24, inoltre garantiscono un'elevata affidabilità per il funzionamento continuo durante tutto l'anno e la ridondanza necessaria a mantenere in funzione le sale tecnologiche. All'opposto, i sistemi di tipo "comfort" sono progettati per mantenere la temperatura a 27°C (80°F) e l'umidità relativa al 50% solo in condizioni estive di 35°C e RH esterna del 48%. Solitamente non sono dotati di dispositivi dedicati per il controllo dell'umidità e le semplici unità di controllo non sono in grado di garantire la tolleranza necessaria del punto di regolazione, consentendo l'instaurarsi di variazioni di temperatura e di umidità potenzialmente dannose. Per queste ragioni all'interno dei Data Center è preferibile l'adozione di Unità di condizionamento di Precisione, opportunamente progettate per mantenere le condizioni ideali per l'elaborazione dei dati ed in grado di gestire, attraverso l'apporto del corretto quantitativo di aria, i "punti caldi" presenti con l'adozione di particolari tecnologie come Server ad alta densità o Server Blade.

6.2 Case Study : Sicurezza del cablaggio di un data center

La protezione delle apparecchiature e dei dispositivi di interconnessione è necessaria per ridurre il rischio di accesso non autorizzato ai dati e per prevenire perdite o danni (vedi paragrafo B3 parte

prima).

L'interconnessione fra le macchine attive e la rete di edificio, deve essere già all'interno di una infrastruttura che comprende il controllo degli accessi e soluzioni tecnologiche appropriate per la realizzazione del suo perimetro di sicurezza.

Bisognerebbe avere più percorsi di collegamento differenti e altrettanti carrier differenti per garantire la continuità di funzionamento del datacenter in caso di emergenza.

Il cablaggio è il tessuto connettivo della infrastruttura di rete e deve essere realizzato in conformità agli standard nazionali e internazionali che ne garantiscono qualità e prestazioni.

A. Gli standard generali di cablaggio

Gli standard generali di cablaggio cui fare riferimento sono il documento americano ANSI/TIA/EIA-568-B (ratificato in maggio 2001, e aggiornato con diversi Addendum), il documento internazionale ISO/IEC 11801 2nd Edition (ratificato in settembre 2002), la versione europea CENELEC EN 50173 2nd Edition (ratificata in novembre 2002), e la versione italiana CEI 306-6.

In particolare per le infrastrutture standard sono previste le seguenti norme.

1) A livello Americano Draft TIA/EIA- 942 (SP-3-0092) che include:

· ANSI/TIA/EIA-568-B.2.1 per la cat.6;

ANSI/TIA/EIA-568-B.3.1 per le fibre OM3 ottimizzate con Laser multimodali;

· ANSI/TIA/EIA-568-B.3. per le fibre monomodali.

2) A livello Europeo Draft EN 50173-5: Information Technology- Generic Cabling System, Part 5: Data Center.

Per le fibre multimodali di nuova generazione OM3 gli standard sono.

Il TIA/EIA-492AAAC-A Annex C.1 e l'IEC 60793-2-10 Type A1a.2, a cui l'addendum ANSI/TIA/EIA-568-B.3.A1 (ratificato a luglio 2002), ISO/IEC 11801:2002 e ISO/IEC 60793-1-49 (per la certificazione delle prestazioni delle fibre OM3 con il test DMD).

Il committente deve assicurarsi la piena rispondenza della soluzione di cablaggio agli standard sopraccitati, chiedendo la certificazione dei prodotti eseguita da laboratori indipendenti riconosciuti a livello internazionale (es.: UL, ETL, ISCOM).

B. Standard specifici

Esistono infine altri standard specifici per i vari aspetti che consentono di implementare e utilizzare correttamente un sistema di cablaggio strutturato:

- sistemi di distribuzione (spazi, canalizzazioni, percorsi cavi, ecc.): TIA/EIA-569-A e ISO/IEC 18010 (in questo caso la versione americana è più completa, e si consiglia di fare riferimento ad essa);
- installazione, compatibilità elettromagnetica e grounding: TIA/EIA-607, ISO/IEC-14763-2 e CENELEC EN 50174-2;
- identificazione dei componenti del cablaggio, registrazione e amministrazione delle informazioni, loro aggiornamento durante l'uso da parte dell'utenza: TIA/EIA-606-A e ISO/IEC 14763-1;

Il parametro di sicurezza più considerato è il rischio di incendio. I componenti del cablaggio strutturato, in particolare le guaine dei cavi, hanno vari gradi di resistenza al fuoco e differenti comportamenti in caso di combustione. E' preferibile indicare cavi conformi alla norma di Propagazione dell'Incendio/della Fiamma CEI 20-22 parte 3°, corrispondente alla norma internazionale IEC 60332-3 ed europea CENELEC HD 405-3. Inoltre è auspicabile utilizzare cavi LSZH che,

in caso di combustione, siano conformi alle seguenti norme:

- emissione di fumi: CEI 20-37 parti 4°-6°, IEC 61034-2, CENELEC HD 606.2
- acidità e corrosività: CEI 20-37 parte 3°, IEC 60754-2, CENELEC HD 602
- tossicità dei fumi: CEI 20-37 parte 7°, NES 713
- Norme armonizzate previste dalle direttive sulla compatibilità elettromagnetica (EMC):

  89/336/CEE e successive modifiche,

  2004/108/CE

C. La fibra ottica

E' auspicabile, dal punto di vista prestazionale per un Data Center, avere a disposizione una banda ridondante con soluzioni di cablaggio sia in rame che in fibra ottica.

La minore o totale capacità di non essere suscettibile ad attacchi condotti direttamente o radiati (con sorgenti RF), depone a favore di una soluzione in fibra ottica che trasporta le informazioni su fasci di luce. Per questo l'eventuale intrusione può essere messa in atto solo mettendo a nudo la singola fibra ottica e dopo averla opportunamente curvata, spillando parte del segnale ottico trasportato. Questa tecnica dello splitting comporta la necessità di accedere in modo evidente alla interconnessione e non è di facile attuazione. Per ovviare a ciò è necessario proteggere l'interconnessione, lungo tutto il suo percorso, dall'accesso fisico non controllato. In particolare ciò vale per armadi, apparati e fibra ottica. A favore di una soluzione in fibra ottica, c'è anche la totale capacità di condividere percorsi anche molto ravvicinati e paralleli con la rete di energia elettrica all'interno del data center; cosa non attuabile anzi da evitare optando per un cablaggio in rame.

Si ha l'impressione che, fino al giorno d'oggi, la scelta di utilizzare un materiale piuttosto che un altro, ovvero di utilizzare la fibra

ottica piuttosto che il rame, è determinata esclusivamente dalle caratteristiche del collegamento in questione in termini di banda passante e non in termini di sicurezza del collegamento.

C.1 Armadi, apparati e attestazioni fibra ottica.

Gli armadi per il contenimento degli apparati e del relativo cablaggio di interconnessione degli stessi dovranno avere requisiti simili a quelli elencati nella sezione A della parte seconda.

C.2 Percorso all'interno del data center.

Indipendentemente che si scelga un percorso per il cablaggio all'interno del pavimento flottante o nel contro soffitto, i cavi dovrebbero essere protetti con cavidotti metallici, canaline metalliche chiuse o cavi ibridi anti taglio o rottura parziale dello strato di protezione, anch'esso metallico e controllato dal sistema .

Ad ogni potenziale soluzione si associano vantaggi e svantaggi che dovranno essere tenuti in considerazione.

Stato dell'arte su utilizzazione e Certificazione delle connessioni a fibra ottica

Il modo e il tipo di utilizzo della fibra ottica da parte di un operatore di telecomunicazioni autorizzato (come TELECOM o TIM), in mancanza di una standardizzazione univocamente accettata, sono imposti dalle prestazioni end2end.

Le scelte sul tipo di cablaggio utilizzato sono determinate dall'hardware che si utilizza, sia a livello di dorsale, sia a livello di cablaggio orizzontale. La fibra monomodale si utilizza solo nel collegamento geografico; all'interno delle centrali si usa la fibra OM1 (fibra multimodale con 200 MHz*km @850 nm di banda passante) o OM3 (fibra multimodale con 2000 MHz*km @850 nm di banda passante). La fibra OM2 praticamente mai. Infatti conviene spendere un po' di più nella fibra e meno nei generatori di segnale che sono molto economici per la fibra 50/125 (OM3).

Gli impianti installati sono certificati per le loro prestazioni, non per la Sicurezza nell'Informazione. La certificazione di conformi-

tà alle caratteristiche prestazionali viene effettuata dalla ditta che esegue l'impianto, con la strumentazione in suo possesso. Non esistono, di norma, controlli dell'impianto eseguiti da terze parti.

Cavidotto metallico

Può essere applicato sul singolo cavo o su più cavi ed ha conformazione corrugata al fine di consentire una gestione meno difficoltosa nei percorsi di posa. Fornisce un elevato grado di protezione all'accesso fisico ai cavi ma comporta maggiori oneri in caso di sostituzione dei cavi o infilaggio di nuovi. Deve comunque essere messo a terra, almeno alle estremità, attraverso appositi collegamenti equipotenziali. Non consente ispezioni visive lungo il percorso del cavo, che può essere infilato prima della posa in opera; si può, comunque posare il cavidotto con pilota predisposto per l'infilaggio del cavo dopo la posa.

Canalina metallica chiusa

Utilizzata diffusamente nei percorsi a contro soffitto ma aperta dal lato superiore e poco utilizzata nei pavimenti flottanti. In molti casi è installata, con appositi sostegni metallici ancorati al soffitto, al di sopra degli armadi del Data Center a vista. Deve comunque essere messa a terra, almeno alle estremità, attraverso appositi collegamenti equipotenziali. Consente ispezioni visive lungo tutto il percorso del cavo, evitando fori o fessurazioni di dimensioni tali da consentire accessi fisici dannosi o non consentiti. Sono disponibili anche delle canaline in plastica chiuse, che però non assolvono a pieno le problematiche legate alla sicurezza fisica dei cavi.

Cavi protetti e allarmati

Sono cavi particolari che prevedono, durante il processo costruttivo, l'inserimento di conduttori all'interno della guaina esterna, o immediatamente sotto. Vengono percorsi, in operatività, da un segnale continuo. In caso di taglio doloso del cavo, il segnale si interrompe attivando appositi allarmi predisposti.

7 - Appendice D: Lo standard ITSEC

In questa appendice si riportano informazioni relative allo standard ITSEC che riveste ancora oggi una rilevanza nella valutazione e certificazione di sistemi e prodotti ICT e viene utilizzato in contesti specifici.

Con il progredire dell'evoluzione tecnologica nel settore delle tecnologie delle comunicazioni e dell'informazione (ICT), sin dai primi anni '60 si era consolidata sempre più la consapevolezza, in particolare negli USA, che la sicurezza diventasse un elemento essenziale e che, in particolare, la valutazione della sicurezza delle nuove tecnologie dell'informazione richiedesse una analisi, condotta da terze parti indipendenti dal produttore, sulla base dell'applicazione di criteri e metodologie predefinite.

Negli anni successivi fu accettato e si consolidò che:

- la nozione di sicurezza ICT dovesse comprendere: la riservatezza, l'integrità e la disponibilità delle informazioni;
- i requisiti dei sistemi/prodotti ICT contenessero elementi per garantire riservatezza, integrità e disponibilità delle informazioni;
- per soddisfare tali requisiti fossero necessarie adeguate misure tecniche di sicurezza;
- gli utenti dei sistemi/prodotti dovessero poter confidare nella sicurezza del sistema/prodotto da loro utilizzato, disporre di un parametro di riferimento per poter con-

frontare le prestazioni, in materia di sicurezza, dei vari prodotti ICT nonché poter effettuare da soli una serie di test ed affidarsi ad un esame imparziale effettuato da un organismo indipendente.

Si rese pertanto necessario disporre di criteri di valutazione della sicurezza obiettivi e ben definiti nonché di un organismo di certificazione che possa confermare la correttezza di tale valutazione. Fu stabilito, inoltre, che gli obiettivi (target) di sicurezza dei sistemi dovessero corrispondere alle esigenze specifiche degli utenti dei sistemi, mentre i target di sicurezza dei prodotti potevano avere carattere più generale in modo che il prodotto ad essi conforme potesse essere integrato in vari sistemi aventi requisiti di sicurezza simili ma non necessariamente identici.

Lo standard ITSEC (*Information Tecnology Security Evaluation Criteria*) è stato uno dei primi standard sviluppati per corrispondere alla sempre più sentita esigenza di poter valutare e certificare come sicuri sia un intero sistema di governo della sicurezza dell'informazione che prodotti e sistemi informatici.

Detto standard, in particolare, individua dei livelli di garanzia per la valutazione del prodotto/sistema i quali vanno da **E1** ad **E6**, in scala crescente: **E1** rappresenta il livello minimo, **E6** rappresenta il livello massimo. Lo standard ITSEC è uno standard nato dal lavoro di armonizzazione condotto da Francia, Germania, Gran Bretagna (G.B.) ed Olanda ed è stato pubblicato in G.B. in versione finale nel giugno del 1991 con pieno successivo recepimento della Commissione della Comunità Europea (CE). Nel 1993 è stato seguito dal documento "*IT Security Evaluation Manual*" (ITEM) della Commissione CE che definisce la metodologia da applicare nelle valutazioni secondo i criteri ITSEC.

Lo standard ITSEC può considerarsi la risposta europea allo standard TCSEC (Trusted Computer Security Evaluation Criteria), anche noto con il nome di "*Orange Book*" emanato, sin dal 1985, dal Dipartimento della Difesa USA. Anche detto standard definisce dei criteri di valutazione e classificazione dei sistemi operativi ed individua

quattro livelli con i quali esaminare i sistemi operativi: **A** (protezione verificata), **B** (protezione obbligatoria), **C** (protezione discrezionale) e **D** (protezione minima); all'interno delle suddivisioni viene definito anche un sistema di classificazione con le classi: **A1, A+,B1, B2,C1,C2** e **C3**.

Entrambi gli standard, come altri sviluppati ed applicati in seguito, sono quindi delle metodologie approvate da organismi istituzionali, riconosciute dalla comunità internazionale, da tempo largamente applicate e sperimentate con le quali è possibile esprimere un giudizio su quanto sia sicuro un sistema od un prodotto informatico.

Lo standard TCSEC presentava, tuttavia, alcuni svantaggi quali:

- le protezioni menzionate nello standard sono tipiche di elaboratori non connessi in rete;
- lo standard non consente flessibilità nella modalità di valutazione: la complessità è proporzionale al livello di sicurezza;
- ci sono pochi livelli per cui quasi tutti i prodotti sono stati valutati con livello medio-alto (C2)
- un costo di applicazione elevato.
- Rispetto ai criteri TCSEC, i criteri ITSEC, invece, presentavano i seguenti miglioramenti:
- la definizione dell'oggetto (prodotto o sistema) della valutazione (Target Of Evaluation - TOE);
- la definizione dell'obiettivo della valutazione (Security Target - ST);
- la valutazione con diversi livelli di severità (Assurance Level - AL).

7.1 Fondamenti dei criteri ITSEC

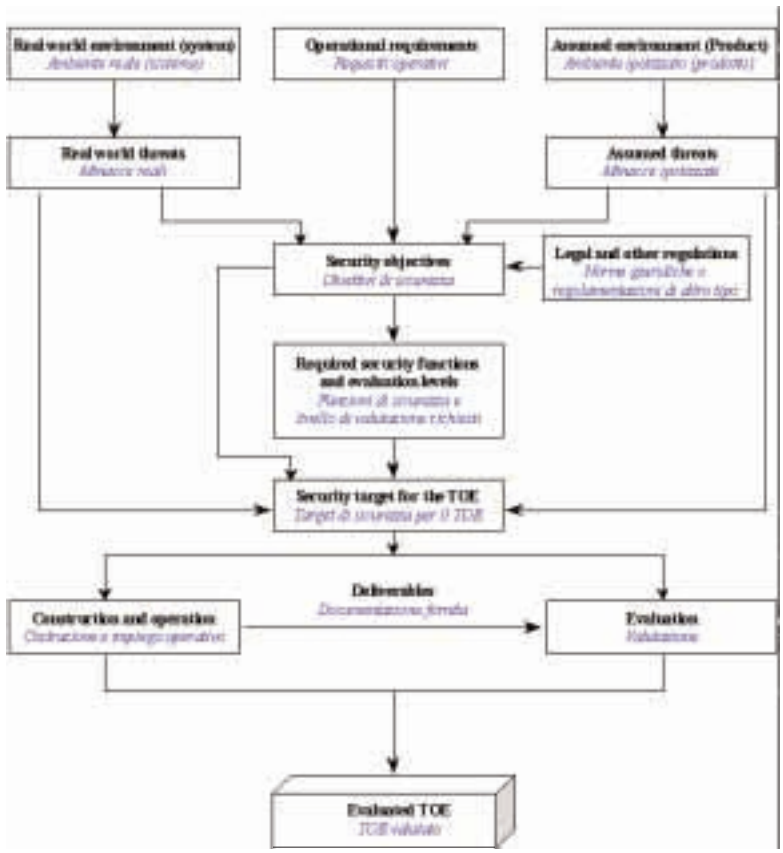
I criteri di sicurezza ITSEC:

- riguardano non solo principalmente misure di carattere tecnico ma anche alcuni aspetti non tecnici quali le disposizioni per un impiego operativo sicuro relative al personale, alla sicurezza fisica e organizzativa del sistema o dei prodotti quando tali aspetti si ripercuotono direttamente sulle misure di sicurezza tecniche;
- sono stati definiti in modo tale da poter essere in gran parte applicati, allo stesso modo, alle misure di sicurezza tecniche implementate sia sull'hardware, sia sul software, sia sul firmware;
- identificano chiaramente chi richiede la valutazione (persona od organizzazione) denominato "sponsor";
- individuano un ente di valutazione[28] del sistema che deve essere accreditato per effettuare la valutazione dei sistemi.

Nello schema che segue è riportato il flusso logico seguito dai criteri ITSEC nel processo di sviluppo e di valutazione il cui obiettivo del processo di valutazione è di consentire al responsabile della valutazione di redigere un rapporto imparziale che indichi se il TOE realizza o meno il suo Security Target con il grado di fiducia richiesto dal livello di valutazione indicato.

In base ai requisiti operativi noti di un prodotto o di un sistema ed al loro ambiente fisico di collocazione sono identificabili delle politiche di sicurezza e degli obiettivi di sicurezza in termini di riserva-

[28] *Negli Schemi nazionali per la valutazione e la certificazione della sicurezza per la tutela delle informazioni classificate e della sicurezza di sistemi/prodotti non coperti dal primo Schema corrispondono , rispettivamente ai Centri di valutazione (Ce.Va.) ed ai Laboratori di valutazione (LVS).*



tezza, integrità e disponibilità nonché uno scenario di minacce a cui il sistema può essere sottoposto.

La definizione delle funzioni di sicurezza, le minacce e gli obiettivi di sicurezza individuati, nonché ogni specifico meccanismo di sicurezza da utilizzare costituiscono il processo di definizione del target di sicurezza per la fase di sviluppo.

La valutazione del *TOE* è effettuata rispetto al *Security Target* che specifica l'ambiente in cui il sistema deve operare e le misure di sicurezza che esso adotta contro le minacce presenti nel suo ambiente. Il *Security Target* per l'approccio ITSEC è un documento composto da quattro parti:

- la *politica di sicurezza del sistema* (*System Security Policy* - SSP), in caso di sistemi, o la descrizione del prodotto (*Product Rationale* - PR) nel caso di prodotti;
- la *specifica delle funzioni di sicurezza* richieste (*Security Enforcing Functions* - SEF) che consentono di conseguire gli obiettivi individuati;
- il livello minimo dichiarato di robustezza dei meccanismi cioè la loro efficacia in termini di resistenza ad un attacco diretto (*Strength of mechanism*);
- il livello di valutazione desiderato.

La SSP identifica le minacce al sistema informatico, gli obiettivi di riduzione delle minacce e l'insieme delle leggi, regole e prassi che stabiliscono come le informazioni e le risorse critiche per la sicurezza devono essere gestite, protette e distribuite all'interno del sistema.

Nel caso di prodotti, invece, la PR, poiché l'ambiente preciso all'interno del quale il TOE sarà utilizzato non è noto al suo sviluppatore perché il prodotto potrebbe essere impiegato in più di un sistema ed in diversi ambienti operativi, descrive le capacita di un prodotto in termini di sicurezza, e fornisce le informazioni necessarie al potenziale acquirente per poter decidere se il prodotto consente o meno di realizzare gli obiettivi di sicurezza del suo sistema.

Le SEF identificano che cosa il TOE garantisce ai propri utenti in termini di sicurezza. L'approccio ITSEC non impone l'adozione di alcuna funzione di sicurezza specifica, a differenza dei criteri TCSEC, perché è lo sponsor che deve decidere quali funzioni intende fornire agli utenti e quali, pertanto, devono essere valutate. I criteri ITSEC raccomandano l'uso di otto categorie generiche (*Generic headings*) di SEF:

- *identificazione ed autenticazione* (*Identification and authentication*), che raccoglie tutte le funzioni che consentono di verificare l'identità di un utente che chiede l'accesso al sistema informatico;
- *controllo degli accessi* (*Access control*), che racchiude tutte le funzioni che controllano il flusso di informazioni fra i processi del sistema informatico e l'uso delle risorse da parte dei processi stessi;
- *attribuibilità delle azioni* (*Accountability*), che contiene tutte le funzioni che tengono traccia delle azioni delle varie entità

(utenti o processi) in modo che esse possono essere attribuite a chi le ha svolte;

- *ispezionabilità* (*Audit*), che riguarda tutte le funzioni che permettono la registrazione ed analisi degli eventi che possono rappresentare una minaccia alla sicurezza del sistema;
- *riuso degli oggetti* (*Object reuse)*, che racchiude le funzioni che permettono di riutilizzare le risorse del sistema senza che ciò costituisca una minaccia alla sua sicurezza;
- *accuratezza* (*Accuracy*), che include le funzioni che evitano le modifiche illecite ai dati;
- *affidabilità del servizio* (Reabilty of service), che include le funzioni atte a garantire che le risorse siano accessibili ed utilizzabili entro tempi prefissati da parte di qualsiasi entità autorizzata;
- *scambio di dati* (*Data exchange*), che include le funzioni che assicurano la sicurezza dei dati durante la loro trasmissione su canali di comunicazione non sicuri.

Nei criteri ITSEC, il processo di valutazione del livello di sicurezza di un sistema o di un prodotto informatico ha lo scopo di stabilire se le SEF previste dalle specifiche:

- garantiscono in modo efficace la sicurezza del sistema/prodotto rispetto alle minacce previste (*valutazione dell'efficacia*);
- siano state realizzate senza commettere errori (volontari od involontari) che ne possano minare l'efficacia (*valutazione della correttezza*)

Il raggiungimento dei suddetti obiettivi garantisce il conseguimento della fiducia nelle capacità di un TOE ad assicurare i previsti requisiti di sicurezza.

I processi di *valutazione dell'efficacia* e della *correttezza* consentono, rispettivamente, di verificare se le SEF fornite dal TOE sono:

- *idonee agli scopi,* specificati nel Security Target, per cui sono state scelte e se i meccanismi che realizzano tali funzioni sono capaci di contrastare attacchi diretti ovvero se corrispondono a livelli di robustezza di base (il meccanismo assicura protezione solo per attacchi senza particolare determinazione e conoscenze specifiche), media (il mecca-

nismo resiste ad attacchi portati con conoscenze e risorse limitate) ed alta (il meccanismo garantisce da attacchi portati con conoscenze e risorse al di sopra della norma);
- stati realizzate correttamente insieme ai corrispondenti meccanismi.

La *valutazione della correttezza* è espressa con la scala di sette livelli da E0 (nessuna fiducia) fino ad E6 (fiducia massima) che rappresentano il livello globale di fiducia nella sicurezza del TOE e, pertanto, il livello di valutazione.

La *valutazione dell'efficacia* delle SEF è svolta nel corso della progettazione del sistema e nella sua messa in opera e deve essere effettuata usando la documentazione fornita dallo sponsor ed i risultati provenienti dalla valutazione della correttezza.

Con la valutazione della progettazione del sistema si intende verificare l'efficacia dei meccanismi del TOE, così come sono stati progettati, di resistere ad un attacco diretto contro il sistema. Tale controllo avviene mediante la verifica:

- delle capacità delle SEF di contrastare le minacce alla sicurezza identificate nel Security Target;
- delle capacità delle SEF e dei corrispondenti meccanismi di sicurezza di funzionare in modo sinergico;
- delle capacità dei meccanismi di sicurezza di resistere ad attacchi diretti, in funzione delle risorse a disposizione dell'aggressore;
- che le vulnerabilità costruttive dichiarate dallo sponsor o scoperte durante la valutazione non costituiscano pregiudizio per la sicurezza del TOE.
- Con la valutazione della messa in opera del sistema si intende verificare se il sistema:
- non diventi insicuro ad insaputa dei suoi utenti;
- le SEF siano di facile utilizzo;
- non contenga delle vulnerabilità note tali da compromettere la sicurezza del TOE.

Qualora la *valutazione dell'efficacia* porti alla scoperta di gravi vulnerabilità ed incongruenze rispetto al Security Target, il TOE riceverà la classifica E0.

La *valutazione della correttezza* garantisce all'utente che le SEF sono corrispondenti alle loro specifiche e prende in esame, separata-

mente, il processo di sviluppo e la messa in opera del TOE.

Il processo di sviluppo considerato nei criteri ITSEC è suddiviso in quatto fasi: la definizione dei requisiti di sicurezza (*Requirements*); il progetto architetturale (*Architectural design*); il progetto dettagliato (*Detailed design*) e la realizzazione (*Implementation*). Per ciascuna fase, lo sponsor deve presentare la documentazione adeguata al livello di valutazione desiderato; nelle tre prime fasi, inoltre, il valutatore si limita a verificare che la documentazione fornita rispetti, con il variare del livello di valutazione desiderato, i requisiti previsti mentre nella quarta fase il valutatore ha un ruolo più complesso che prevede:

- ai livelli più bassi, la semplice analisi dei risultati delle prove effettuate dallo sponsor;
- per i livelli più elevati, la verifica della correttezza delle SEF con effettuazione delle prove già eseguite dallo sponsor e di ogni altra prova ritenuta utile.

La disponibilità e la completezza della documentazione a corredo del sistema o prodotti da valutare costituiscono uno degli aspetti fondamentali dei criteri ITSEC in quanto:

- *la valutazione dell'efficacia* deve esser svolta usando sia la documentazione fornita dallo sponsor che i risultati della valutazione della correttezza;
- *la valutazione della correttezza* è effettuata sulla base della conoscenza dell'ambiente di sviluppo, della documentazione per l'uso (*User documentation*), destinata all'utente, e della documentazione per gli amministratori (*Administration documentation*) del TOE, delle procedure di distribuzione ed installazione (Delivery and configuration) e di start-up e gestione (*start-up and operation*).

La conoscenza dell'ambiente di sviluppo è considerata importante per la valutazione del livello di affidabilità della correttezza di un sistema informatico. Gli aspetti che il valutatore deve prendere in considerazione sono tre: il controllo di configurazione (configuration control), i linguaggi di programmazione ed i compilatori (programming languages and compilers), la sicurezza dell'ambiente di sviluppo (developers security). Più precisamente:

- il controllo di configurazione riguarda i controlli imposti dallo sviluppatore del sistema sui suoi processi di produzione e di gestione; dal livello E2 in poi il sistema di con-

trollo di configurazione deve assicurare che il sistema sotto esame sia esattamente quello descritto nella documentazione e che soltanto modifiche autorizzate sono possibili;

- i linguaggi di programmazione e i compilatori non hanno particolari requisiti fino al livello E2, al livello E3 è richiesto l'uso di linguaggi di programmazione ben definiti (ad esempio linguaggi per i quali esistono standard ISO) mentre dal livello E4 in avanti i requisiti diventano più stringenti e riguardano anche i compilatori e le run-time libraries utilizzate;
- la sicurezza dell'ambiente di sviluppo riguarda le misure di sicurezza (fisiche, procedurali, tecniche e relative al personale) adottate per proteggere l'integrità del sistema informatico durante il suo sviluppo; in particolare: al livello E2 è richiesta solo una descrizione per sommi capi delle misure di sicurezza; al livello E3, lo sponsor deve descrivere dettagliatamente tali misure mentre dal livello E5 in avanti le misure adottate devono essere dettagliatamente spiegate.

7.2 Impiego, vantaggi e svantaggi dei criteri ITSEC

I criteri ITSEC hanno costituito un deciso miglioramento ed un approccio più flessibile del rigido standard TSEC il quale, nel tempo, ha presentato i difetti di considerare protezioni tipiche di elaboratori non in rete, di non consentire flessibilità di valutazione con una complessità che è proporzionale al livello di sicurezza nonché di presentare pochi livelli di sicurezza.

Lo standard ITSEC, in quanto sviluppato in Europa, è stato recepito dalla Comunità Europea ed ha costituito in Europa un valido riferimento per la valutazione di sicurezza, migliore dello standard TCSEC, soprattutto per la valutazione dei sistemi e prodotti utilizzati nel settore militare e per la valutazione di dispositivi e dei sistemi connessi con la firma digitale.

Lo standard ITSEC, pur costituendo un sensibile miglioramento rispetto a quello TCSEC, ha tuttavia mantenuto una certa complessità perché i valutatori possono mescolare ed abbinare le valutazioni di funzionalità e garanzia, facendo proliferare le classificazioni e mantenendo complicato il processo di valutazione. Lo standard ITSEC, inoltre, non è evoluito ulteriormente così come avvenuto per i Common Criteria i quali sono diventati, invece, uno standard a maggiore diffusione internazionale ed adottato dall'ISO (ISO/IEC 15408).

In Italia, entrambi gli schemi nazionali che regolano la valutazione e la certificazione di sistemi e prodotti informativi, da applicare a sistemi militari l'uno ed a sistemi di tipo civile l'altro, lasciano la facoltà di applicazione di uno dei due possibili insiemi di criteri si valutazione citati in precedenza. I criteri ITSEC, tuttavia all'atto pratico, presentano i seguenti svantaggi rispetto allo standard ISO/IEC 15408:

- minore flessibilità, perché lo standard ISO/IEC 15408 valuta un prodotto a fronte di un certo profilo di protezione che è strutturato in modo da soddisfare specifici requi

TCSEC		ITSEC		ISO/IEC 15408 (C.C.)	
D	Sicurezza assente	E0	Garanzia inadeguata	EAL0	Garanzia inadeguata
-				EAL1	Testato funzionalmente
C1	Sicurezza media discrezionale	E1	Descrizione informale ODV	EAL2	ODV strutturalmente testato
C2	Sicurezza media obbligatoria	E2	Descrizione informale ODV	EAL3	ODV metodicamente testato e controllato
B1	Sicurezza medio - altamodifica dei permessi di accesso ai file non consentita	E3	Descrizione informale dell'ODV e del progetto, testati con metodo	EAL4	ODV metodicamente testato, progettato e controllato
B2	Sicurezza medio - altaclassificazione del livello di sicurezza dei dispositivi HW	E4	ODV testato metodicamente con descrizione informale del progetto	EAL5	ODV progettato e testato semi-informalmente

TCSEC		ITSEC		ISO/IEC 15408 (C.C.)	
B3	Sicurezza medio - alta impiego di HW specifico per proteggere risorse importanti	E5	Progetto semiformale con modello formale delle politiche di sicurezza	EAL6	Test e verifica del progetto semi-informale
A1	Sicurezza massima-certificata	E6	ODV progettato e testato formalmente in accordo con il modello formale delle politiche di sicurezza	EAL7	Test e verifica formale del progetto

siti di protezione con ampie funzionalità e requisiti di garanzia che rendono più formale e ripetibile la compilazione del Security Target;

- gli elementi che qualificano la valutazione sono scelti dal committente e se non si leggono i documenti della valutazione non si hanno informazioni sulle caratteristiche di sicurezza al contrario dello standard ISO/IEC 15408 il quale fa riferimento a profili di protezione predefiniti e certificati, i Protection Profile, relativi a tipologie omogenee di prodotti;
- non consentono di mantenere l'attualità e la garanzia della certificazione;
- non considerano la necessità di escludere il coinvolgimento dello sviluppatore del TOE ai fini della certificazione;
- Nello schema successivo è riportata, infine, la corrispondenza tra i livelli di valutazione ITSEC, i livelli e le classi di valutazione TCSEC ed i livelli di sicurezza di valutazione dei Common Criteria.

8 - Glossario

8.1 Glossario di riferimento nel contesto delle certificazioni BS7799/ISO27001

Analisi dei Rischi	insieme di attività aventi lo scopo di determinare, tramite l'individuazione delle minacce, la valutazione delle vulnerabilità e la quantificazione dell'impatto, il livello di esposizione degli asset informativi considerati rilevanti per il conseguimento degli obiettivi e della mission, e a qualificare coerentemente i controlli e le contromisure a loro protezione
Asset	componente materiale o immateriale utilizzato per il raggiungimento degli obiettivi di un processo cui è possibile attribuire un valore
Asset Informativo	Informazione o strumento mediante il quale le informazioni sono trattate, avente un valore specifico e riconosciuto, utilizzato per il raggiungimento degli obiettivi dei propri processi.
Disponibilità	concetto cardine della sicurezza il cui rispetto garantisce che gli utenti autorizzati possono accedere all'asset informativo quando vi è necessità. Relativamente alle informazioni, perdite di disponibilità possono avvenire a seguito di una loro erronea o dolosa cancellazione o distruzione nonché di una loro organizzazione, conservazione, interconnessione o blocco non coerente con le esigenze dei processi di business aziendali
Gestione dei Rischi	insieme di attività aventi lo scopo di ottimizzare, governare e controllare il livello di rischio cui sono sottoposti gli asset informativi

Information Security Management System	(it. Sistema di gestione della sicurezza delle informazioni) È la componente del più ampio processo di gestione delle attività aziendali, basata sull'approccio di gestione del rischio di business, finalizzata a stabilire, implementare, perseguire operativamente, controllare, rivedere, manutenere e migliorare la sicurezza delle informazioni garantendo nel tempo il soddisfacimento della politica di sicurezza. Fattivamente si compone di strutture organizzative, di documenti (policy, procedure, linee guida, etc.), di progetti e attività, nonché di risorse e usi.
Integrità	concetto cardine della sicurezza il cui rispetto garantisce l'accuratezza e la completezza dell'asset informativo e dei metodi di elaborazione. Relativamente alle informazioni, perdite di integrità possono avvenire a seguito di raccolta, registrazione, elaborazione, modificazione delle stesse da parte di soggetti non competenti o non autorizzati
Minaccia	modalità di manifestazione di un evento dannoso collegata ad una vulnerabilità di una risorsa aziendale.
Patrimonio informativo	insieme di informazioni e strumenti mediante i quali queste sono trattate, sia esso riconducibile ad asset prettamente immateriali sia non
Proprietario dell'Asset	Indica la persona fisica che detiene la responsabilità dei livelli di servizio richiesti all'asset dal servizio o dal processo che lo utilizza e sulle modalità con cui questi vengono garantiti.
Rischio	Combinazione della probabilità del verificarsi di un evento e della sua conseguenza
Rischio Accettato	il valore del rischio sull'asset ritenuto accettabile dalle strategie di sicurezza delle informazioni ovvero il livello di rischio obiettivo delle sue attività di risk management.
Rischio Effettivo	il prodotto scalare del valore dell'asset per la minaccia decurtata del valore risultante della ponderazione dei controlli in essere
Rischio Residuo	il prodotto scalare del valore dell'asset per la minaccia decurtata del valore dei controlli di sicurezza selezionati al fine di ricondurre il rischio effettivo ai livelli desiderati
Rischio Totale	il prodotto scalare della minaccia per il valore dell'asset su cui la minaccia infierisce

Riservatezza	concetto cardine della sicurezza il cui rispetto garantisce che l'asset informativo è accessibile solamente a coloro che hanno l'autorizzazione ad accedervi. Relativamente alle informazioni, perdite di riservatezza possono avvenire a seguito di consultazione, selezione, estrazione, raffronto delle stesse da parte di soggetti non autorizzati nonché della loro comunicazione o diffusione ai medesimi (es. concorrenza, pubblico, dipendenti non autorizzati, …)
Sicurezza	processo di gestione del rischio che, a partire da un'analisi dei requisiti di business, legali e di sicurezza, permette l'individuazione dei controlli e delle contromisure atte a gestire tale rischio
Sicurezza delle Informazioni	insieme delle attività di sicurezza aventi la responsabilità di proteggere il patrimonio informativo mediante la definizione di una serie di misure organizzative, normative e tecniche di protezione controllo e verifica, fondate sul rispetto dei tre concetti cardine di Riservatezza, Integrità e Disponibilità
Vulnerabilità	una scopertura di sicurezza di un asset o di un gruppo di essi che può essere sfruttato da una minaccia.

8.2 Glossario di riferimento nel contesto delle certificazioni Common Criteria (ISO15408)[29]

Accreditamento	Riconoscimento formale dell'indipendenza, dell'affidabilità e della competenza tecnica di un Laboratorio per la Valutazione della Sicurezza
Algoritmo crittografico	Un insieme di regole matematiche per trasformare i dati di input in un output sulla base di altri parametri di input quali le chiavi crittografiche ed i vettori di inizializzazione
Analisi dell'impatto sulla sicurezza	Analisi delle modifiche apportate all'ODV effettuata al fine di stabilire se le modifiche apportate all'ODV risultino tali da richiedere una ri-valutazione o se possano dare luogo ad un aggiornamento del Certificato nell'ambito del PGC
Analisi di vulnerabilità	Processo che consiste nello svolgere una ricerca sistematica di vulnerabilità nell'ODV, e nel valutare le vulnerabilità eventualmente individuate allo scopo di determinare la loro rilevanza nell'ambiente operativo che è stato previsto per l'ODV.
Assistente	Persona formata, addestrata e abilitata dall'Organismo di Certificazione a fornire assistenza
Assistenza	Attività di supporto tecnico, inerente la sicurezza nel settore della tecnologia dell'informazione, fornita durante la fase di preparazione alla valutazione di un sistema/prodotto/PP
Assurance	vedi *Garanzia*
Beni	Informazioni o risorse che devono essere protette mediante le contromisure realizzate da un OdV
Certificato	Documento formale e pubblico che conferma i risultati di una valutazione e la corretta applicazione dei Criteri ITSEC e della relativa Metodologia, o dei Common Criteria e della Common Evaluation Methodology
Certificato di Accreditamento	Documento formale e pubblico che attesta l'idoneità di un LVS ad operare all'interno dello Schema nazionale
Certificatore	Persona facente parte dell'organico dell'Organismo di Certificazione e da quest'ultimo formata, addestrata e abilitata a condurre le attività di certificazione
Certificazione	L'attestazione da parte dell'Organismo di Certificazione che conferma i risultati della Valutazione, la corretta applicazione dei criteri adottati e della relativa metodologia
Committente	La persona fisica, giuridica o altro organismo o associazione che commissiona e sostiene gli oneri economici della valutazione e certificazione e che può anche rivestire il ruolo di Fornitore
Disponibilità delle informazioni	Proprietà tesa a consentire l'accesso e l'utilizzo di informazioni su richiesta di entità autorizzate

[29] Il seguente glossario è un estratto del glossario ufficiale dell'OCSI riportato nella LGP7, disponibile nel sito web www.ocsi.gov.it

Fiducia	vedi *Garanzia*
Formale	Espresso in un linguaggio dalla sintassi ristretta con una semantica ben definita basate su concetti matematici consolidati
Fornitore	Persona fisica, giuridica o altro organismo o associazione che fornisce l'ODV e che può rivestire il ruolo di Committente
Funzioni di sicurezza (FS)	Contromisure di tipo tecnico di cui è dotato l'ODV sulle quali si fa affidamento per realizzare un sottoinsieme di regole contenute nella politica di sicurezza dell'ODV stesso.
Garanzia	Il termine garanzia (o fiducia), è utilizzato con riferimento alla capacità che l'ODV mostra nel soddisfare i propri obiettivi di sicurezza, considerando le minacce e l'ambiente descritti nel TDS. La garanzia è tipicamente assicurata a vari livelli da un processo di valutazione formale.
Identità	Una rappresentazione (ad esempio una stringa alfanumerica) che identifica in maniera univoca un utente autorizzato
Informale	Espresso in un linguaggio naturale
Ispettore	Figura abilitata dall'OC per condurre le verifiche previste nella procedura di accreditamento di un LVS.
Laboratorio per la Valutazione della Sicurezza (LVS)	Organizzazione indipendente che ha ottenuto l'Accreditamento e che pertanto è abilitata ad effettuare valutazioni e a fornire assistenza
Linee Guida	Pubblicazione tecnica che fornisce informazioni dettagliate relative alla conduzione ed allo svolgimento delle attività inerenti il processo di Valutazione e Certificazione
Livello di garanzia	La misura della garanzia espressa mediante identificatori alfanumerici la cui parte numerica cresce con il crescere della fiducia (in ITSEC: da E1 a E6; nei Common Criteria: da EAL1 ad EAL7).
Materiale per la Valutazione	Risorse per la valutazione di tipo materiale, cioè, la documentazione tecnica o le componenti software, hardware, firmware realizzati durante lo sviluppo del sistema o del prodotto. Può contenere informazioni riservate.
Meccanismo di sicurezza	Le specifiche soluzioni hardware, software e firmware che realizzano le funzioni di sicurezza di cui è dotato l'ODV.
Metodologia	Il sistema di principi, procedure e processi che è applicato a una valutazione della sicurezza IT
Non ripudio	L'impossibilità per una entità di negare di aver preso parte ad una comunicazione

Obiettivo di sicurezza	Una dichiarazione d'intenti, fatta in un PP o in un TDS, al fine di contrastare minacce identificate e/o verificare ipotesi e politiche di sicurezza ben specificate
Oggetto della Valutazione (ODV)	Un prodotto o un sistema IT che, unitamente alla documentazione destinata agli utenti e agli amministratori, è sottoposto al processo di valutazione secondo i criteri e la metodologia adottati.
Organismo di Certificazione (OC)	Organizzazione nazionale indipendente e imparziale che esegue la Certificazione di sistemi, prodotti, PP e l'accreditamento dei Laboratori per la Valutazione della Sicurezza
Penetration testing	vedi *Test di intrusione*
Piano Di Valutazione (PDV)	Documento che descrive le attività che saranno svolte dall'LVS durante il processo di valutazione, i tempi di esecuzione e le risorse necessarie
Politiche di sicurezza di un'organizzazione (PSO)	Una o più regole, procedure, pratiche o linee guida di sicurezza adottate da un'organizzazione
Prodotto	Un insieme di elementi software, hardware e/o firmware che svolge una funzione che può essere utilizzata da molti sistemi
Profilo di Protezione (PP)	Il documento che descrive per una certa categoria di ODV ed in modo indipendente dalla realizzazione, gli obiettivi di sicurezza, le minacce, l'ambiente ed i requisiti funzionali e di fiducia, definiti secondo i Common Criteria. Un PP ha la finalità di definire un insieme di requisiti che si è dimostrato efficace per raggiungere gli obiettivi individuati, sia per quanto riguarda le funzioni di sicurezza, sia per quanto riguarda la garanzia. Un PP fornisce agli utenti uno strumento per fare riferimento ad uno specifico insieme di esigenze di sicurezza, e facilita lo svolgimento di future valutazioni di Prodotti o Sistemi che soddisfino tali esigenze.
Protection Profile	vedi *Profilo di Protezione*
Rapporto di Attività (RA)	Documento che l'LVS invia all'Organismo di Certificazione, nel quale sono indicati dettagliatamente i risultati raggiunti e le attività svolte dal Laboratorio stesso durante le varie fasi della valutazione. Può contenere informazioni riservate
Rapporto di Certificazione (RC)	Documento emesso dall'Organismo di Certificazione, che conferma i risultati della valutazione e la corretta applicazione dei criteri
Rapporto di Certificazione dell'accreditamento	Rapporto redatto dalla Commissione Tecnico-consultiva che, sulla base del Rapporto Finale di Accreditamento, esprime l'esito motivato di una procedura di accreditamento
Rapporto di Classificazione delle Componenti dell'ODV (RCC)	Documento che fornisce una classificazione delle componenti dell'ODV secondo la loro rilevanza in termini di sicurezza.
Rapporto di Mantenimento	Documento che viene allegato al Rapporto di Certificazione al fine di attestare il buon esito dell'attività di mantenimento effettuata

Rapporto di Osservazione (RO)	Rapporto dell'LVS per l'OC e il Committente, finalizzato alla segnalazione di anomalie o errori. Può contenere informazioni riservate.
Rapporto Finale di Accreditamento	Rapporto redatto dal Responsabile della Sezione Accreditamento che, sulla base del Rapporto Finale di Visita Ispettiva, descrive l'iter della pratica di accreditamento di un laboratorio.
Rapporto Finale di Valutazione (RFV)	Rapporto prodotto dall'LVS, contenente i risultati della valutazione, che costituisce la base per la Certificazione dell'ODV o del PP. Può contenere informazioni riservate.
Rapporto Finale di Visita Ispettiva	Rapporto redatto dagli Ispettori contenente la descrizione delle attività ispettive effettuate e il loro esito.
Requisiti di garanzia	Requisiti su cui si basa la fiducia che l'ODV raggiunga gli obiettivi di sicurezza specificati nel TDS. Normalmente, nel caso dei CC, i requisiti di garanzia sono raggruppati in pacchetti predefiniti (EAL) corrispondenti a livelli di garanzia standard.
Requisiti di sicurezza	L'insieme dei requisiti funzionali e di garanzia specificati in un PP, in un TDS o in un pacchetto.
Requisiti funzionali di sicurezza	I Requisiti funzionali di sicurezza descrivono il comportamento di sicurezza che viene richiesto ad un ODV, ed hanno l'obiettivo, se correttamente realizzati, di consentire il raggiungimento degli obiettivi di sicurezza enunciati in un PP o in un TDS.
Responsabile per la Gestione del Certificato (RGC)	Persona (o gruppo di persone) che ha il compito di verificare che i processi e le procedure di gestione del Certificato dichiarate nel PGC siano applicati dal Fornitore.
Riservatezza delle informazioni	Proprietà tesa ad impedire l'accesso e la divulgazione non autorizzata di informazioni
Robustezza di una funzione	La misura della capacità di una Funzione di Sicurezza di contrastare attacchi diretti condotti con risorse predefinite.
Ruolo	Un insieme predefinito di regole che stabilisce le interazioni consentite tra l'utente e l'ODV
Schema	L'insieme delle procedure e delle regole nazionali necessarie per la Valutazione e Certificazione, in conformità ai criteri europei ITSEC o agli standard internazionali ISO/IEC IS-15408 (Common Criteria) e alle relative metodologie ITSEM e CEM
Schema di Gestione dei Certificati (SGC)	L'insieme delle procedure che permettono di mantenere nel tempo la validità del Cerificato
Semiformale	Espresso in un linguaggio dalla sintassi ristretta con una semantica ben definita

Sistema	Una specifica installazione IT (software, firmware o hardware), caratterizzata da uno scopo e da un ambiente operativo ben definiti.
Target of evaluation (TOE)	vedi *Oggetto della valutazione*
Test di intrusione	Test che sono eseguiti con l'obiettivo di determinare se le vulnerabilità potenziali dell'ODV possono essere sfruttate nell'ambiente operativo che è stato previsto per quest'ultimo.
Traguardo di Sicurezza (TDS)	Il documento, utilizzato come base per la Valutazione di un ODV, che contiene gli obiettivi di sicurezza, la descrizione dell'ambiente in cui l'ODV è utilizzato e le minacce alle quali è soggetto, i requisiti funzionali e di garanzia, la specifica delle funzioni di sicurezza
Utente	Ogni entità (utente umano o entità IT) esterna all'ODV che interagisce con l'ODV stesso
Utente autorizzato	Un Utente che, in accordo con la Politica di Sicurezza dell'ODV, può eseguire un'operazione
Utente umano	Qualsiasi persona che interagisca con l'ODV
Valutatore	Persona nell'organico dell'LVS formata, addestrata ed abilitata dall'Organismo di Certificazione a condurre le attività di valutazione
Valutazione	L'analisi di un sistema, prodotto, PP condotta in base a predefiniti criteri applicati secondo una predefinita metodologia.
Verdetto	Una dichiarazione di esito positivo, negativo o in sospeso prodotta da un Valutatore e riferita a un elemento che descrive un'azione che deve essere svolta dal Valutatore, a un componente di garanzia o a una classe. Si veda anche la voce verdetto complessivo.
Verdetto complessivo	Una dichiarazione di esito positivo o negativo che viene prodotta dal Valutatore e che riguarda il risultato di una valutazione.
Vulnerabilità	Elemento di debolezza che è presente nell'ODV e che può essere sfruttato, in un determinato ambiente operativo, per violare una politica di sicurezza.
Vulnerabilità evidente	Vulnerabilità che può essere sfruttata disponendo di un livello minimo di comprensione dell'ODV, di competenza tecnica minima e di risorse minime.
Vulnerabilità potenziale	Vulnerabilità di cui, postulando la disponibilità di un percorso d'attacco, si sospetta l'esistenza nell'ODV, ma la cui effettiva presenza non è stata confermata.

Vulnerabilità residua	Vulnerabilità che potrebbe essere sfruttata da un attaccante che fosse in possesso di un potenziale d'attacco superiore a quello che è stato previsto nell'ambiente operativo che è stato ipotizzato per l'ODV. Si tratta, quindi, di un particolare tipo di vulnerabilità che non può essere sfruttata.
Vulnerabilità sfruttabile	Vulnerabilità che può essere sfruttata nell'ambiente operativo che è stato previsto per l'ODV.

10 - Bibliografia

Normative

D.P.C.M. 11 aprile 2002 – 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.

D.P.C.M. 30 ottobre 2003 – Approvazione dello schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione, ai sensi dell'art. 10, comma 1, del decreto legislativo n. 10 del 23 gennaio 2002

Raccomandazione del Consiglio dell'Unione Europea (95/144/CE) in data 7 aprile 1995, "Applicazione dei criteri per la valutazione della sicurezza della tecnologia dell'informazione ITSEC";

Direttiva 1999/93/CE del Parlamento europeo e del Consiglio del 13 dicembre 1999 Relativa ad un quadro comunitario per le firme elettroniche;

Decisione della Commissione Europea del 6 novembre 2000 (2000/709/CE) "Criteri minimi di cui devono tener conto gli Stati membri all'atto di 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";

Risoluzione del Consiglio dell'Unione Europea del 6 dicembre 2001 "Approccio comune e azioni specifiche nel settore della sicurezza delle reti e dell'informazione";

Decreto del Presidente del Consiglio dei Ministri 11 aprile 2002, "Approvazione dello schema nazionale per la valutazione e la certificazione della sicurezza nel settore delle tecnologie dell'informazione per la tutela delle informazioni classificate, concernenti la sicurezza interna ed esterna dello Stato";

Decreto del Presidente del Consiglio dei Ministri 30 ottobre 2003 "Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione, ai sensi dell'art. 10, comma 1, del decreto legislativo 23 febbraio 2002, n. 10";

Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 "Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale dei documenti informatici";

Presidenza del Consiglio dei Ministri/Autorita' Nazionale per la Sicurezza, "Linea Guida -Procedure di Valutazione" P.C.M.-A.N.S. / LG – VAL";

Decreto del Ministro per l'Innovazione e le Tecnologie e del ministro delle Comunicazioni 17 febbraio 2005 " Linee guida provvisorie per l'applicazuione dello schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione".

Standard

ISO/IEC 17799 Information technology – Code of practice for information security management

ISO/IEC 27001 Information technology – Security techniques – Information security managementsystems – Requirements

ISO/IEC 15408-1:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model. Disponibile gratuitamente al sito web "webstore.ansi.org/".

ISO/IEC 15408-2:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements. Disponibile gratuitamente al sito web "webstore.ansi.org/".

ISO/IEC 15408-3:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model. Disponibile gratuitamente al sito web "webstore.ansi.org/".

UNI CEI EN 45012 Ed. 1998, Guida EA-7/01 rev 2 Ed. 2003, Accreditamento di Organismi di Certificazione di sistemi di gestione per la qualità (SGQ) in conformità alla norma UNI EN ISO 9001:2000. Disponibile al sito web http://www.sincert.it/documentisincert.asp?id=142.

ISO IEC Guide 66 Ed. 1999 Guida EA-7/02 rev 4 Ed. 2003, Accreditamento di Organismi di Certificazione di sistemi di gestione ambientale (SGA) in conformità alla norma: UNI EN ISO 14001:2004. Disponibile al sito web http://www.sincert.it/documentisincert.asp?id=142.

ISO IEC Guide 66 Ed. 1999 Guida EA-7/02 rev 4 Ed. 2003, Accreditamento di Organismi di Certificazione di sistemi di gestione per la salute e sicurezza dei lavoratori (SCR) in conformità alla norma: OHSAS 18001:1999. Disponibile al sito web http://www.sincert.it/documentisincert.asp?id=142.

UNI CEI EN 45012 Ed. 1998 Guida EA-7/03 rev 0 Ed. 2000, Accreditamento di Organismi di Certificazione di sistemi di gestione per la sicurezza delle informazioni (SSI) in conformità alle norme:BS7799:1999; Parte 2 e ISO 27001. Disponibile al sito web http://www.sincert.it/documentisincert.asp?id=142.

UNI CEI EN 45011 Ed. 1999 Guida EA-6/01 rev 0 Ed. 1999, Accreditamento di Organismi di Certificazione di prodotti (PRD) . Disponibile al sito web http://www.sincert.it/documentisincert.asp?id=142.

UNI CEI EN ISO/IEC 17024 Ed. 2004 Guida EA-8/01 rev 1 Ed. 2004, Accreditamento di Organismi di Certificazione di personale (PRS) . Disponibile al sito web http://www.sincert.it/documentisincert.asp?id=142.

UNI CEI EN ISO/IEC 17020 Ed. 2005 Guida EA IAF ILAC A4 Ed 2004, Accreditamento di Organismi di ispezione (ISP). Disponibile al sito web http://www.sincert.it/documentisincert.asp?id=142.

UNI CEI EN 45011 Ed. 1999 Guida EA-6/01 rev 0 Ed. 1999 ISO/TR 14025:2000 SEMEC MSR 1999:2, Accreditamento di Organisimi di Certificazione operanti la verifica e convalida delle Dichiarazioni Ambientali di Prodotto (DAP) . Disponibile al sito web http://www.sincert.it/documentisincert.asp?id=142.

ISO/IEC 17024, "General requirements for bodies operating certification of persons"

Common Criteria e ITSEC

CCIMB-2004-01-001, "Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model", version 2.2, 1/2004

CCIMB-2004-01-002, "Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional requirements", version 2.2, 1/2004

CCIMB-2004-01-003, "Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance requirements", version 2.2, 1/2004

CCIMB-2004-02-09 "Assurance Continuity: CCRA Requirements"; 2/2004

CEM-97/017, "Common Evaluation Methodology for Information Technology Security Evaluation, Part 1 – Introduction and general model"; version 0.6, 1/1997

CCIMB-2004-01-004, "Common Evaluation Methodology for Information Technology Security Evaluation, Part 2 – Evaluation Methodology", version 2.2, 1/2004

ISO/IEC TR 15446 "Information technology – Security techniques – Guide for the production of Protection Profiles and Security Targets", 12/2003

Information Technology Security Evaluation Criteria, version 1.2, 6/1991

Information Technology Security Evaluation Manual, version 1.0, 9/1993

Varie

CNIPA, "i Quaderni", n. 23 marzo 2006, "Linee Guida per la sicurezza ICT nelle Pubbliche Amministrazioni. Piano Nazionale della sicurezza delle ICT per la PA. Modello organizzativo nazionale di sicurezza ICT per la PA", disponibile in formato elettronico all'indirizzo web www.cnipa.gov.it/site/_files/Quaderno%20n%2023.pdf., pagg 52 e 53.

Pubblicazione ISCOM, "LA SICUREZZA DELLE RETI - Dall'analisi del rischio alle strategie di protezione", disponibile all'indirizzo web http://www.iscom.gov.it/news.asp?ID=9

Pubblicazione ISCOM, "LA SICUREZZA DELLE RETI - Nelle infrastrutture critiche" ", disponibile all'indirizzo web http://www.iscom.gov.it/news.asp?ID=10

Tutte le Linee Guida Iscom sono scaricabili dal sito
www.iscom.gov.it

realizzazione GRAPHICLAB
SETTORE DIVULGAZIONE E COMUNICAZIONE ESTERNA ISCOM

Finito di stampare agosto 2006 PGE - Roma

Ministero delle Comunicazioni

ISCOM

DIVULGAZIONE E COMUNICAZIONE ESTERNA

LINEE GUIDA ISCOM PUBBLICATE

SICUREZZA DELLE RETI DALL'ANALISI DEL RISCHIO ALLE STRATEGIE DI PROTEZIONE

SICUREZZA DELLE RETI NELLE INFRASTRUTTURE CRITICHE

LA QUALITÀ DEI SERVIZI NELLE RETI ICT

GESTIONE DELLE EMERGENZE LOCALI

RISK ANALYSIS APPROFONDIMENTI

QUALITÀ DEL SERVIZIO SU UMTS

QUALITÀ DEL SERVIZIO SU BANDA LARGA

CERTIFICAZIONE DELLA SICUREZZA ICT

OUTSOURCING E SICUREZZA