Linee guida sulla qualità dei beni e dei servizi ICT per la definizione ed il governo dei contratti della Pubblica Amministrazione

Manuale di riferimento

Ricognizione di alcune Best Practice

applicabili ai contratti ICT

ISO IEC 27001:2005

Sistema di Gestione della Sicurezza delle Informazioni

INDICE

1. GENERALITÀ SUL DOCUMENTO

Questo documento descrive uno dei lemmi del Manuale di riferimento "Dizionario delle Best Practice e degli Standard" delle Linee Guida sulla qualità dei beni e dei servizi ICT per la definizione ed il governo dei contratti della Pubblica Amministrazione.
Con le espressioni Best Practice e Standard, nel seguito indicate con il termine Framework, si intende rispettivamente :

- **Best practice :** raccolta organizzata di raccomandazioni derivanti dalla selezione delle pratiche migliori per l'erogazione dei servizi;
- **Standard :** insieme di elementi predeterminati (requisiti) che fissano le caratteristiche di un prodotto, o processo, o servizio, o sistema organizzativo e che, se applicati, ne consentono la comparazione, la misura e la valutazione.

Ogni lemma del Dizionario è autoconsistente ed indipendente; esso prevede il seguente indice :

- **obiettivi e ambito**, dove vengono descritti gli obiettivi e l'ambito di applicazione entro cui il frame work si colloca (ICT sevice acquisition, IT sevice Management, IT Governance, SW development & system integration, Project Management, Quality Assurance);
- **storia**, che ha portato alla versione ultima del framework;
- **destinatari**, dove sono riportati i destinatari principali quali la PA che appalta, l'organizzazione che eroga un servizio o realizza un progetto, la funzione interna ad una organizzazione, l'organizzazione che sviluppa SW e fa system integration, l'organizzazione che gestisce un sistema produttivo di qualità;
- **specificità** , dove sono indicati le specificità del FW rispetto alle forniture ICT, alla pubblica amministrazione ed alla relazione cliente-fornitore;
- **contenuti**, dove viene riportato lo schema di come il FW è strutturato e la relazione esistente tra gli elementi della struttura;
- **modalità di applicazione**, dove vengono riportate le eventuali modalità di applicazione dei singoli FW nell'ambito della Pubblica Amministrazione (acquisizione forniture ICT, gestione progetti ICT, erogazione servizi ICT, erogazione di procedimenti amministrativi) ;
- **documentazione disponibile**, dove vengono elencati i documenti disponibili, indicando per ognuno gli elementi della struttura del FW interessati;
- **certificazioni esistenti**, riferite sia alle persone che alle organizzazioni;
- **formazione disponibile**;
- **estratto del glossario**;
- **associazioni di riferimento**;
- **indicazioni bibliografiche**;

La versione digitale di ogni lemma è singolarmente scaricabile dal sito CNIPA.

Scopo di questo documento è quello di diffondere la conoscenza in ambito pubblico di questo Framework, dandone una sintetica descrizione e fornire nello stesso tempo tutte le informazioni utili per potersi procurare la relativa documentazione ed approfondirne i contenuti.

Per informazioni relative al contesto di utilizzo nell'ambito del ciclo di vita di acquisizione delle forniture ICT e per una comparazione con gli altri FW, lemmi del medesimo dizionario, si può far riferimento al manuale applicativo numero 9 delle Linee Guida : "Dizionario delle Best Practice e degli Standard".

2. OBIETTIVI E AMBITO

Dopo la certificazione dei sistemi di gestione aziendale relativi alla qualità secondo la Norma EN ISO 9001:2000, per le Organizzazioni che si occupano di servizi ICT, si profilano delle nuove sfide tra cui quella relativa alla certificazione del SGSI (Sistema di Gestione della Sicurezza delle Informazioni).
Infatti sono sempre più numerosi gli "incidenti" sulla sicurezza delle informazioni.
Alcuni esempi sono:

- i casi di fuga di notizie ed informazioni riservate,
- i continui tentativi di intrusione ed attacchi da "virus", "cavalli di troia", "worm" , ecc.
- "i furti e le truffe" basate sull'uso di informazioni e/o altri strumenti informatici.

Occorre considerare che viviamo in una società dove è fondamentale per la nostra attività possedere e gestire le informazioni necessarie per valutare e prendere decisioni quotidianamente su eventi specifici..
Questo significa poter disporre di un'ampia base informativa da cui selezionare di volta in volta le informazioni giuste.
Significa, inoltre, che le informazioni hanno un valore di tipo economico e che la loro perdita può causare danni significativi.
Il motivo è dovuto al fatto che le informazioni sono una risorsa preziosa per le Organizzazioni, e costituiscono un patrimonio importante che deve essere opportunamente ed adeguatamente difeso. Per questo la sicurezza delle informazioni ha lo scopo di proteggere le informazioni da una ampia serie di minacce, allo scopo di garantire il regolare svolgimento delle attività della Organizzazione, minimizzando gli eventuali danni che possono essere economici e relativi alla immagine, massimizzando il ritorno sugli investimenti eseguiti. Le informazioni da difendere possono presentarsi in varie forme : su carta, in formato elettronico, trasmesse per posta elettronica, scambiate a voce durante conversazioni, su filmati. In qualunque forma o mezzo in cui vengono trattate le informazioni, esse devono sempre essere adeguatamente protette.
La sicurezza delle informazioni è caratterizzabile come salvaguardia della:

- Riservatezza (garanzia che le informazioni siano accessibili solo da parte delle persone autorizzate);
- Integrità (salvaguardia dell'accuratezza e della completezza);
- Disponibilità (assicurazione che gli utenti autorizzati abbiano accesso alle informazioni ed alle risorse associate quando ne hanno bisogno).

Tali requisiti vanno garantiti attraverso la messa in atto di un efficace sistema di misure :

Organizzative
Consistono in Politiche, in Procedure, in Regolamenti atti ad ottenere un livello di sicurezza e protezione delle informazioni coerente con gli Obiettivi e le strategie della Organizzazione.

Fisiche
Consistono nell' impiego di mezzi ed infrastrutture per prevenire l' accesso a personale non autorizzato, e misure di rilevazione fisica. Inoltre sono previste tutte quelle misure di supporto per garantire la continuità delle attività prevenendo interruzioni dovute a cause esterne ed eventi ambientali.

Logiche
Consistono in misure tecnologiche atte a prevenire la possibilità di accesso alle risorse informatiche da parte di programmi software o personale non autorizzato. Inoltre misure di rilevazione di attività relative a violazioni e tentativi di intrusione delle informazioni.

Bisogna considerare, per la sicurezza delle informazioni, tutti gli aspetti derivanti dalla legislazione corrente in maniera di Privacy e trattamento dei dati, Proprietà Industriale, Criminalità Informatica, Responsabilità Amministrativa, per comprendere tutte le possibili implicazione ed i benefici nella applicazione dello Standard di riferimento.
Per rendere adeguatamente comparabili i livelli di capacità tecnica, le Amministrazioni che intendano appaltare servizi ICT per la sicurezza dovrebbero prevedere, come uno tra i requisiti idonei a dimostrare il possesso della capacità tecnica, la disponibilità, da parte delle imprese, di una certificazione dei loro sistemi di gestione per la Sicurezza delle Informazioni, rilasciata sulla base della norma ISO/IEC 27001:2005 da organismi accreditati.
La necessità di proteggere le informazioni è dimostrata anche dalle numerose leggi emesse nei vari paesi su questo tema.
E' importante rilevare che talvolta si pensa che il problema della protezione delle informazioni sia un tema specifico che riguarda le aziende di servizi informatici; questo non è vero il tema riguarda tutti coloro che gestiscono informazioni riservate, da proteggere e da garantire integre.
Da queste brevi considerazioni si può capire perchè le informazioni hanno un valore, in quanto possono costituire: il vantaggio competitivo per l'Organizzazione, il patrimonio culturale da preservare, le regole e le guide da applicare alla propria Organizzazione oppure sono dati sensibili/riservati che devo assolutamente proteggere in quanto fanno parte del servizio offerto agli utenti/clienti (o possono essere informazioni di proprietà del cliente) e che la loro perdita rappresenterebbe un danno per loro e per il gestore del servizio..
In conclusione tutte le informazioni hanno un valore economico diretto o indiretto in quanto una loro perdita o danneggiamento o indisponibilità può essere causa di danni ingenti.
Non esiste però "la protezione ideale o assoluta" ed inoltre anche la protezione ha un costo. Occorre perciò trovare il giusto equilibrio tra il valore di ciò che si vuol proteggere e il costo della protezione.
Da tempo sono state predisposte norme che indicano quali sono i requisiti di base per costruire un sistema di gestione della sicurezza delle informazioni. Queste norme, inizialmente emesse dal BSI (British Standard Institution), sono state ora adottate internazionalmente e pubblicate come norme ISO/IEC, e successivamente pubblicate dalla UNI in Italia.
Un elemento fondamentale per costruire un sistema di sicurezza adeguato è la determinazione e la valutazione dei rischi. Infatti attraverso questa valutazione, non solo si rilevano i rischi che l'Organizzazione che gestisce informazioni sta correndo per quanto riguarda la sicurezza, ma si determinano gli elementi di base per poter prendere anche le contromisure necessarie a mitigare i rischi individuati.
Questo è uno degli elementi più impegnativi nella costruzione e nella gestione di un Sistema di Sicurezza Informazioni.

Per quanto riguarda l'ambito di Applicazione, lo Standard ISO/IEC 27001:2005 Information Technology – Security techniques – Information security management systems – Requirements, costituisce uno dei riferimenti per impostare un sistema organizzativo che comprende tutti gli aspetti della Sicurezza delle informazioni e che si inserisce in uno scenario

di Governance dei Processi ICT in interazione con altri modelli di riferimento per la gestione ICT quali: COBIT, ITIL, ISO/IEC 20000.
E' uno standard certificabile (dai vari Organismi di Certificazione accreditati dal SINCERT), e non fa riferimento a nessun contesto specifico. Cioè lo standard è applicabile a qualsiasi contesto a qualsiasi Organizzazione di diversa natura pubblica o privata, di piccola media o grande complessità, con elevato o basso livello di informatizzazione. Fino ad oggi le Organizzazioni che hanno utilizzato maggiormente lo standard sono state quelle in cui l' ICT costituisce un aspetto primario e molto significativo.
Nella eventuale Certificazione del Sistema di gestione per la sicurezza delle informazioni possono essere previsti diversi ambiti di applicazione che vanno formalizzati in un Documento specifico chiamato "Campo di applicazione" che può prevedere :

- Tutti i processi dell' Organizzazione;
- Uno o più processi primari e relative interfacce;
- Un processo critico e relative interfacce;
- Uno o più processi primari e uno o più processi di supporto e relative interfacce.

Il campo di applicazione costituisce il testo che viene inserito all' interno del certificato e che comunica all' esterno quali attività, processi, servizi, applicazioni sono previste nella certificazione del sistema di gestione.

3. STORIA

Il DTI (Department of Trade and Industry) del Governo Britannico nell' anno 1990 ha istituito un Gruppo di lavoro con il compito di realizzare e fornire alle Organizzazioni una linea guida per la gestione della sicurezza e di tutto il patrimonio informativo.
Nell' anno 1993 viene pubblicato il Documento "Code of Practice for Information Security Management" che conteneva una raccolta di pratiche per aiutare nella implementazione della sicurezza nelle varie Organizzazioni.
British Standard Institution nel 1995 recepisce e pubblica lo stesso Documento come Standard BS 7799-1:1995 Code of Practice for Information Security Managemnt.
La ISO (International Standard Organization) nel 1996 costituisce il Comitato JTC1 SC27 assegnadoli il compito di trasformare lo Standard BS 7799-1:1995 in uno standard mondiale.
British Standard Institution nel 1998 pubblica lo Standard BS 7799-2:1998 Specification for Information Security Management System che costituisce l' elemento di riferimento per i Sistemi di Gestione per la Sicurezza delle Informazioni e da l' avvio alla certificazione secondo lo Standard British Standard Institution per i paesi che vogliono aderire volontariamente ai contenuti della norma.
Nel 1999 British Standard Institution pubblica un aggiornamento di entrambe le norme dando luogo ad una versione aggiornata allineata e coerente dei documenti :BS 7799-1:1999 e BS 7799-2:1999.
Lo Standard BS 7799, nasce con l' obiettivo di fornire un insieme di requisiti comprendenti le "best Practices" nell' ambito della sicurezza delle informazioni. Il suo intento è quello di rappresentare un riferimento univoco per identificare l' insieme delle misure che sono necessarie nella maggior parte delle Organizzazioni che devono proteggere le informazioni.

Le norme sono state articolate in due parti distinte :

- Parte 1, fornisce le raccomandazioni per la gestione della sicurezza delle informazioni da utilizzare da parte di coloro che vogliono istituire, realizzare e mantenere un sistema di gestione per la sicurezza delle informazioni;
- Parte 2, definisce i requisiti per istituire, realizzare e mantenere un sistema di gestione per la sicurezza delle informazioni;

Il Comitato ISO nell' anno 2000 emette la prima versione del documento ISO/IEC 17799:2000 che costituisce la emissione ISO dello Standard BS7799-1:1995.

Versione attuale e Prospettive
Lo stesso Comitato ISO nell' anno 2005 recepisce la versione dello standard BS 7799-2:1999, pubblica la versione definitiva ed attuale dello Standard ISO/IEC 27001:2005 e della ISO/IEC 17999:2005, rendendo internazionali entrambi le norme, e definendo l' utilizzabilità in ambito di certificazione internazionale.
L' ISO attraverso il recepimento delle norme normalizza tutte le certificazioni emesse fino a quella data, definendo anche un periodo di transizione. Cioè stabilisce dei criteri e dei tempi per convertire le certificazioni esistenti secondo la norma BS 7799-2 in ISO/IEC 27001:2005 con data ultima fissata a livello mondiale al 20 Aprile 2007.
Nell' anno 2007 viene pubblicata la norma ISO/IEC 27002:2005 corrispondente alla ISO/IEC 17799:2005, il suo contenuto è identico a quello della ISO/IEC 17799:2005. La norma ISO/IEC 17799:2005 cambia il suo numero di riferimento da ISO/IEC 17799 a ISO/IEC 27002.

In autunno 2007 l'UNI (Ente Nazionale Italiano di Unificazione) ha rilasciato e pubblicato la **UNI CEI ISO/IEC 27001** in italiano.

Code of Practice of Information Security Management	ISMS requirements
BS7799-1:1995	BS7799-2:1998
	
BS7799-1:1999	BS7799-2:1999
	
ISO/IEC 17799:2000	BS7799-2:2002
	
ISO/IEC 17799:2005 ISO/IEC 27002:2005 (rinumerata luglio 2007)	ISO/IEC 27001:2005

Il Comitato ISO (International Standard Organization) JTC1 SC27 WG1 ha previsto per la famiglia delle ISO 27000 tutta una serie di norme delle quali si citano quelle emesse :

- ISO 27000 Principi e vocabolario;

- ISO 27001 Requisiti per un Sistema di Gestione per La Sicurezza delle Informazioni (pubblicata in ottobre 2005) ;
- ISO 27002 Linea guida – Raccomandazioni per un Sistema di Gestione per La Sicurezza delle Informazioni (è la rinumerazione della ISO 17999:2005 effettuata in luglio 2007);
- ISO 27003 Guida alla implementazione;
- ISO 27004 Misura della sicurezza delle informazioni;
- ISO 27005 Gestione del Rischio per i SGSI (Sistemi di Gestione per la Sicurezza delle Informazioni);
- ISO 27006 Guida per gli Organismi di Certificazione/Organismi di Accreditamento alla valutazione di conformità dei SGSI (pubblicata nella primavera 2007);
- ISO 27007 Linee guida per gli audit dei Sistemi di Gestione per la Sicurezza delle Informazioni;

4. DESTINATARI

La norma **ISO/IEC 27001:2005** è indirizzata a:

- organizzazioni private piccole, medie e grandi operanti sia nei settori commerciali che industriali: finanza, banche, assicurazioni, telecomunicazioni, servizi, trasporti, farmaceutiche (e ospedaliere), …
- agenzie governative,
- amministrazioni e enti governativi,
- organizzazioni pubbliche sia centrali che locali,
- organizzazioni senza scopo di lucro.

I destinatari sono quindi tutte le aziende od organizzazioni che effettuano o forniscono servizi di trattamento delle informazioni, sia all'interno che all'esterno e a tutti coloro che intendono occuparsi della sicurezza delle informazioni. L'applicazione della norma da parte di un'impresa o Organizzazione rappresenterà una garanzia per le parti interessate, le quali sapranno con certezza che il problema della Sicurezza delle Informazioni viene affrontato e gestito seriamente nell'ambito dell'impresa stessa
Ne consegue che essendo i requisiti della ISO/IEC 27001 generici, questi si possono applicare a tutte le Organizzazioni siano esse private o pubbliche, ed oltretutto indipendentemente dal tipo, dalla dimensione e dalla natura del business (considerando tale anche l'erogazione di prestazioni o servizi pubblici).

Le culture presenti nella norma sono ricondicibili a :

- Manageriale (gestione aziendale);

- Processi (gestione del servizio);
- Tecnica-Applicativa (gestione delle tecnologie dell'informazione e della comunicazione ICT).

Profili professionali

Per avviarsi nel modo giusto un progetto di innovazione, così come si può configurare un progetto di adozione della norma, si deve poter contare sulla disponibilità iniziale delle opportune risorse di conoscenza e finanziarie. Per concludersi con successo il progetto deve poi necessariamente comportare un soddisfacente ritorno economico e di conoscenza per le parti interessate all'Organizzazione. Conoscenze e competenze distintive dell'Organizzazione sono fondamentalmente localizzate nelle persone che interpretano ruoli chiave nei processi tipici della gestione dei servizi IT.

Parallelamente e funzionalmente all'evoluzione della certificazione per la Sicurezza delle Informazioni, specie in settori che gestiscono informazioni riservate, è sorta l'esigenza di disporre di figure professionali dotate di elevata e dimostrata competenza per lo svolgimento di attività particolarmente critiche ai fini dei processi di implementazione ed assicurazione della Sicurezza delle Informazioni. Ha avuto quindi origine la prassi della qualificazione del personale, che ha inizialmente riguardato operazioni strettamente tecniche (es. tecnici informatici) e si è poi estesa ad altre figure professionali correlate con la valutazione e realizzazione dei sistemi di gestione (auditor e consulenti/progettisti).
Queste figure hanno il compito di garantire, secondo le proprie competenze, che le caratteristiche "tecniche e qualitative dei prodotti/servizi" forniti siano quelle desiderate e che tutte le relative attività produtive siano svolte in modo conforme alle Procedure.

Di seguito sono elencati e messi in relazione alcuni profili professionali oggi definiti ma sicuramente in continua evoluzione:

- SGSI Manager,
- Responsabili del coordinamento e della Gestione dell'attuazione di un SGSI,
- Progettisti e Consulenti SGSI,
- SGSI Auditor.

L' **SGSI Manager** è un esperto in possesso delle competenze necessarie per gestire con efficacia la Sicurezza delle Informazioni (SGSI) nelle Organizzazioni, tenendo conto anche degli aspetti economici e di efficienza, della missione e delle strategie aziendali e con la piena consapevolezza dei principi dell'etica negli affari e della deontologia professionale.

I **Responsabili del coordinamento e della Gestione dell'attuazione di un SGSI** sono degli esperti che coadiuvano l'SGSI Manager nella conduzione ed attuazione del Sistema di Gestione della Sicurezza delle Informazioni.

I **Progettisti e Consulenti SGSI** sono degli esperti in grado di comprendere e applicare le pertinenti norme internazionali che incidono sulle organizzazioni e gli idonei strumenti gestionali utili e necessari per l'erogazione dei servizi di progettazione, di attuazione, di

gestione e di miglioramento continuo del Sistema di Gestione della Sicurezza delle Informazioni dell'Organizzazione.

L' **SGSI Auditor** è un esperto in possesso delle competenze necessarie alla conduzione di audit indipendenti o di terza parte su Sistemi di Gestione per la Sicurezza delle Informazioni (S.G.S.I.) conformi alla ISO/IEC 27001:2005 ed a supportare efficacemente gli interlocutori impegnati nell'iter di certificazione del SGSI.

Stakeholder

Per quanto riguarda i vari portatori di interesse nel sistema di gestione della sicurezza delle informazioni si può citare :

- La Direzione dell'Organizzazione che ha il compito di definire la Politica e gli Obiettivi, Ruoli e Responsabilità del personale, e mettere a disposizione tutte le risorse per il SGSI
- Il Personale nell'Organizzazione che utilizza la norma e mette in atto le politiche ed i requisiti di sicurezza per raggiungere gli obiettivi prefissati;
- i clienti dell'Organizzazione intesi come coloro che usufruiscono dei vari servizi che vengono garantiti con le esigenze di sicurezza, in misura conforme agli impegni assunti;
- i fornitori dell'Organizzazione che contribuiscono, in quanto partner, agli obiettivi dell' organizzazione, accettando le politiche di sicurezza ed i rischi connessi alla fornitura;

5. SPECIFICITÀ

Ambito Pubblico (PAC, PAL)

Le Pubbliche Amministrazioni, sia centrali (Ministeri e relativi Organi Tecnici), sia periferiche (Regioni, Province, Comuni, Enti locali), sono chiamate:

- da un lato, a tutelare i bisogni di Sicurezza delle Informazioni dei cittadini (dati sulla salute, educazione, mobilità, lavoro, giustizia, … ...), tramite la funzione loro propria di regolamentazione e controllo delle attività di produzione di beni e servizi e della vita sociale in genere;
- dall'altro, ad applicare la Sicurezza delle Informazioni, in quanto fornitrici di servizi di pubblica utilità (sanità, scuola, trasporti, ambiente, energia, servizi pubblici tecnologici ed amministrativi vari … …).

Per l'espletamento di tali funzioni le Pubbliche Amministrazioni si avvalgono poi di lavorazioni, beni, prodotti e servizi acquisiti da terzi.
Esse sono pertanto tenute a svolgere il delicato compito di:

- promotori e regolatori di Sicurezza delle Informazioni (funzione "politica"),
- committenti di Sicurezza delle Informazioni (funzione "amministrativa")
- fornitori di Sicurezza delle Informazioni (funzione "tecnica").

Si noti che, nel caso delle Pubbliche Amministrazioni, tali funzioni sono fra loro strettamente interdipendenti ancor più che per altre Organizzazioni, con conseguenze di particolare criticità.
Infatti, l'inadeguatezza di una sola di esse o la mancanza di coordinamento fra le medesime possono compromettere gravemente l'efficacia del ruolo istituzionale complessivamente svolto dalle Pubbliche Amministrazioni, reso già arduo dalle inerzie culturali e dai vincoli burocratici ad esse non estranei, con l'insorgere di meccanismi perversi di degradamento.
Si noti che la cultura e la prassi della Sicurezza delle Informazioni stanno entrando anche nel mondo della Pubblica Amministrazione specialmente dopo l'avvento dell'informatizzazione globale con l'utilizzo di Internet.
È invece rimasta, sostanzialmente, estranea al mondo delle Pubbliche Amministrazioni la cultura di ottenere la "certificazione di conformità", sia in quanto assicurazione della applicazione della Sicurezza delle Informazioni nei beni e servizi acquisiti, sia, soprattutto, come dimostrazione dell'applicazione della Sicurezza delle Informazioni alle opere realizzate ed ai servizi forniti.
Suddetti strumenti invece devono diventare parte integrante della cultura della Pubblica Amministrazione ed essere applicati in modo sostanziale e consapevole, adattandoli alle specifiche esigenze e caratteristiche delle molteplici attività svolte. Essi devono essere, in particolare:

- assunti a riferimento nell'opera di promozione, regolamentazione e controllo svolta dalle Amministrazioni;
- utilizzati per la valutazione/assicurazione dell'applicazione della Sicurezza delle Informazioni (a tutto campo) dei fornitori e dei beni e servizi acquisiti;
- applicati per garantire la Sicurezza delle Informazioni dei servizi forniti dalle Amministrazioni medesime.

A tale riguardo, va tenuto presente il ruolo fondamentale delle risorse umane (personale dell'Amministrazione) che devono essere adeguatamente formate, sensibilizzate e motivate al fine di acquisire la necessaria competenza e consapevolezza in tema di Sicurezza delle Informazioni ed in particolar modo nell'implementazione di un Sistema di Gestione per la Sicurezza delle Informazioni.

Forniture ICT

La nascita delle forniture ICT può farsi risalire alle prime offerte di servizi EDP della fine anni '70, in genere costituite da applicazioni e da tempo di calcolo.
Dagli anni '90 ha visto poi evolversi in modo rilevante un fenomeno chiamato "outsourcing IT", con l'affermarsi di nuove forme di "esternalizzazione" dei servizi ICT intesi anche come forniture.
In questo scenario non è comunque consueto oggi osservare, a parte poche eccezioni, che un'Organizzazione conferisca in outsourcing più del 70-80% dell'attivita' del reparto IT.
Con l'avvento della globalizzazione informatica e specialmente di Internet una delle forniture ICT più richieste specialmente nella Pubblica Amministrazione è la "Sicurezza delle Informazioni o meglio Sicurezza ICT".

L'applicazione della norma che prevede, tra l'altro, l'uso dei consigli di implemenazione previsti nella norma ISO/IEC 27002:2005, ovvero vengono trattate le forniture ICT come acquisizione di servizi in outsourcing/terze parti, quindi è applicabile da parte di che ha implementato il Sistema di Gestione per la Sicurezza delle Informazioni.

Esemplificando, se la PA o PAL si avvale di un S.G.S.I. può, anzi deve, garantirsi tramite una serie di controlli specifici nell'acquisizione della fornitura in outsourcing o terza parte. Mentre se la PA non si avvale di un SGSI ma richiede che chi effettua la fornitura sia certificato secondo la norma ISO/IEC 27001, ha l'assicurazione che il fornitore applica un Sistema di Gestione per la Sicurezza delle Informazioni. In questo caso è molto importante verificare lo scopo per cui il fornitore è certificato per constatare se l'ambito è quello relativo alla fornitura.

La PA e/o PAL dovrebbe assicurare che i prodotti hardware o software nonché i servizi approvvigionati per la sicurezza siano conformi ai requisiti specificati per l'approvvigionamento. Il tipo e l'estensione del controllo eseguito sul fornitore e sul prodotto o servizio acquistato dovrebbe essere correlato agli effetti che quanto acquistato potrà avere sulla sicurezza delle informazioni. L'organizzazione dovrebbe valutare e selzionare i fornitori in base alle loro capacità di fornire servizi o prodotti conformi ai requisiti dell'organizzazione stessa. Dovrebbero pertanto essere stbiliti i criteri per la selezione, valutazione e rivalutazione del fornitore. I risultati delle valutazioni e delle azione necessarie andranno conservate.

Relazione Contrattuale

Quando si intraprende il percorso verso una relazione con un fornitore identificato, con l'obiettivo di concretizzarlo in un contratto di servizio, occorre minimizzare il rischio di insuccessi, e ciò lo si deve perseguire assumendo l'ottica tipica della sana gestione dei progetti, e cioè dotandosi di una metodologia strutturata (esempio PDCA …)
Come accennato nel paragrafo precedente, è possibile applicare in un contratto di fornitura le best practice previste dalla norma ISO/IEC 27002 relative alla gestione dei rapporti con le terze parti.
I contratti con terze parti che coinvolgono l'accesso, gestione, comunicazione delle informazioni dell'organizzazione o strumenti di gestione dell'informazione, o l'implementazione/manutenzione di prodotti e/o servizi per gli strumenti di gestione dell'informazione dovrebbero prendere in considerazione i requisiti di sicurezza in essere nell'organizzazione.

PUNTO DI VISTA DEL CLIENTE

Durante il periodo di fruizione del servizio è opportuno che il cliente (PA o PAL) mantenga un controllo costante del rispetto delle clausole contrattuali e del corretto andamento delle relazioni con il fornitore/terza parte. Le clausole contrattuali devono almeno rispettare i controlli previsti nell'annex A relativamente all'applicazione dell'obiettivio A.6.2 Parti Esterne (Outsourcing).

Queste attività, saranno particolarmente importanti per gestire, ad esempio, il manifestarsi di esigenze interne diverse da requisiti contrattuali iniziali, oppure il perdurare di carenze nel servizio fruito rispetto agli SLA, con modalità che possano evitare il deteriorarsi dei rapporti tra le due controparti.

PUNTO DI VISTA DEL FORNITORE

Sicuramente il fornitore avrà tutto l'interesse di rafforzare la sua posizione di mercato quale fornitore di servizi di outsourcing ICT e si opererà nel mantenere aggiornato il suo SGSI.

Sviluppo Progetti / Sviluppo Servizi

I Sistemi Informativi IT includono i sistemi operativi, le infrastrutture, le applicazioni di business, i prodotti disponibili immediatamente i servizi e le applicazioni sviluppate

dall'utente. La progettazione e l'implementazione del Sistema Informativo che supportano il processo di business di una Pubblica Amministrazione possono essere cruciali per quanto riguarda la Sicurezza delle Informazioni. I requisiti di Sicurezza dovrebbero essere identificati e concordati prima dello sviluppo e/o della realizzazione dei Sistemi Informativi
Tutti i requisiti di Sicurezza dovrebbero essere identificati nella fase di realizzazione/ implementazione di un progetto e dovrebbero essere giustificati, concordati e documentati.
Nella progettazione e sviluppo delle applicazioni informatiche il processo di valutazione del software viene eseguito per assicurare la conformità ai requisiti di sicurezza specificati. Inoltre le modifiche alla progettazione dovrebbero essere tenute strettamente sotto controllo mediante l'utilizzo di formali procedure.

Anche per questi argomenti vengono trattati ampliamente con best practice nella norma ISO 27002 mentre nella norma ISO 27001 sono previsti i controlli per l'applicazione dei requisiti.

Erogazione dei Servizi
Per l' **erogazione dei servizi** si rimanda alla Norma ISO/IEC 20000 più specifica per il contesto e dove la ISO 27002:2005 è inserita come processo per la Sicurezza delle Informazioni e la ISO/IEC 27001:2005 è considerata come soddisfazione del requisito di applicazione della Sicurezza delle Informazioni.

Politica
L' Organizzazione deve definire, comunicare e diffondere a tutte le parti interessate una politica per la sicurezza delle informazioni, che indichi il bisogno di soddisfare :

- requisiti di sicurezza del cliente;
- requisiti contrattuali;
- regolamenti e requisiti cogenti.

Rischi
L' Organizzazione deve mettere in atto una serie di attività per la valutazione, misura e gestione dei rischi :

- definizione di un modo sistematico per la valutazione dei rischi;
- classificazione dei beni del sistema con i relativi proprietari;
- Valutazione dei rischi;
- Trattamento dei rischi;
- Accettazione del rischio residuo.

Controlli di sicurezza (trattamento dei rischi)
L' Organizzazione deve mettere in atto una serie di controlli e misure di sicurezza definendo :

- Ruoli e responsabilità;
- La disponibilità e la garanzia della competenza, consapevolezza e formazione del personale;

- Tipologie di misure e controlli : organizzativi, logici, fisici;
- Metodologie per monitorare e misurare l' efficacia delle politiche della sicurezza e dei relativi controlli messi in atto.

Documentazione dei controlli di sicurezza
L' Organizzazione deve emettere documentazione per :

- Descrivere i rischi;
- Descrivere i controlli;
- Valutazione degli impatti dei cambiamenti dei controlli.

Accordi con terze parti
L' Organizzazione deve considerare e mettere in atto misure per la gestione delle terze parti attraverso :

- Politiche;
- Gestione dei rischi;
- Requisiti contrattuali riguardo la sicurezza;
- Accordi contrattuali;
- Indicatori e monitoraggio.

Gestione degli incidenti
L' Organizzazione deve descrivere e mettere in atto una procedura per la gestione degli incidenti allo scopo di :

- Classificarli;
- Comunicarli e registrarli;
- Investigarli;
- Gestirli attraverso contromisure;

L' Organizzazione deve mettere in atto a seguito della gestione degli incidenti e malfunzioni una serie di azioni proattive per migliorare i servizi erogati.

6. CONTENUTI

La ISO/IEC 27001:2005 riconduce ai principi generali riconosciuti a livello internazionale.
Si fa riferimento alle "Linee guida sulla sicurezza dei sistemi e delle reti di informazione. Verso una cultura della Sicurezza" adottate sotto forma di raccomandazione in occasione

della Sessione del Consiglio OCSE (Organizzazione per la Cooperazione e lo Sviluppo Economico) il 25/07/2002. Gli obiettivi della guida sono :

- Estendere alle parti interessate una cultura della sicurezza quale mezzo di protezione dei sistemi e delle reti di informazione
- Rafforzare la sensibilità rispetto ai rischi per i sistemi e le reti di informazioni, alle politiche, pratiche, azioni e procedure disponibili per affrontare tali rischi, nonché la necessità di adottarli ed attuarli.
- Favorire una maggiore fiducia delle parti nei confronti dei sistemi e delle reti di informazione e nel modo in cui sono forniti ed utilizzati.
- Creare un assetto generale di riferimento che aiuti le parti interessate a comprendere la natura dei problemi legati alla sicurezza a rispettare i valori etici nell' elaborazione e nell' attuazione di politiche, pratiche, azioni e procedure coerenti per la sicurezza dei sistemi e reti di informazione.
- Incoraggiare fra tutte le parti interessate la cooperazione e la condivisione di informazioni adeguate alla elaborazione e all' attuazione di politiche, pratiche, azioni e procedure intese alla sicurezza.
- Promuovere la presa in considerazione della sicurezza quale obiettivo rilevante per tutte le parti interessate associate all' elaborazione e attuazione di norme.

La ISO/IEC 27001 contiene i requisiti per istituire realizzare e documentare un SGSI, ad essa è affiancata come copia coerente la ISO/IEC 27002 linea guida e fonte di raccomandazioni per l' attuazione e la gestione operativa del SGSI. Pertanto la Norma non entra nel dettaglio della classificazione dei processi, delle attività, delle istruzioni operative, della documentazione operativa e degli indicatori.

Lo norma ISO/IEC 27001prevede che una Organizzazione istituisca e mantenga un SGSI del tipo documentato, definendo gli obiettivi di sicurezza, identificando le risorse da proteggere, gestendo i rischi relativi al sistema, implementando le misure da attuare.

Specificità dello standard

Chiave di volta dello standard è la valutazione dei rischi sulla base della quale viene organizzato un SGSI.
Lo standard introduce però altri aspetti caratteristici tipici di un SGSI:

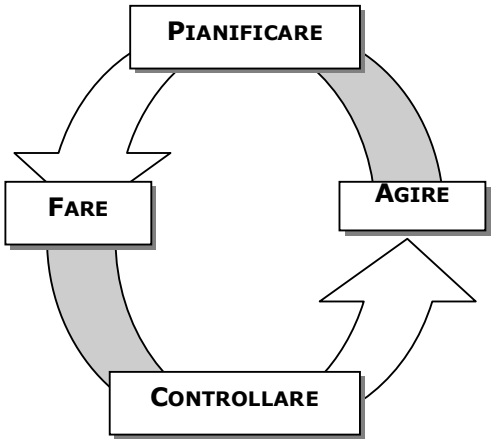
- il concetto di asset (o bene) con relativa valorizzazione;
- gli aspetti economico-finanziari inerenti la sicurezza delle informazioni;
- l'aspetto organizzativo (e non solo tecnologico) della sicurezza delle informazioni;
- l'efficacia del SGSI e delle contromisure adottate per trattare i rischi.

In tal senso siamo di fronte ad uno standard che pone le basi per una reale utilizzabilità e comprensione all'interno di una organizzazione.
Altra importante caratterizzazione è l'insieme di nuove norme/standard (linee guida) che a breve affiancheranno la ISO/IEC 27001:05 per supportare le organizzazioni nell'attuazione dello stesso.

La norma è stata progettata in modo da rendere agevole l'iterazione con altri standard relativi a sistemi di gestione quali ISO 9001 e ISO 14001.

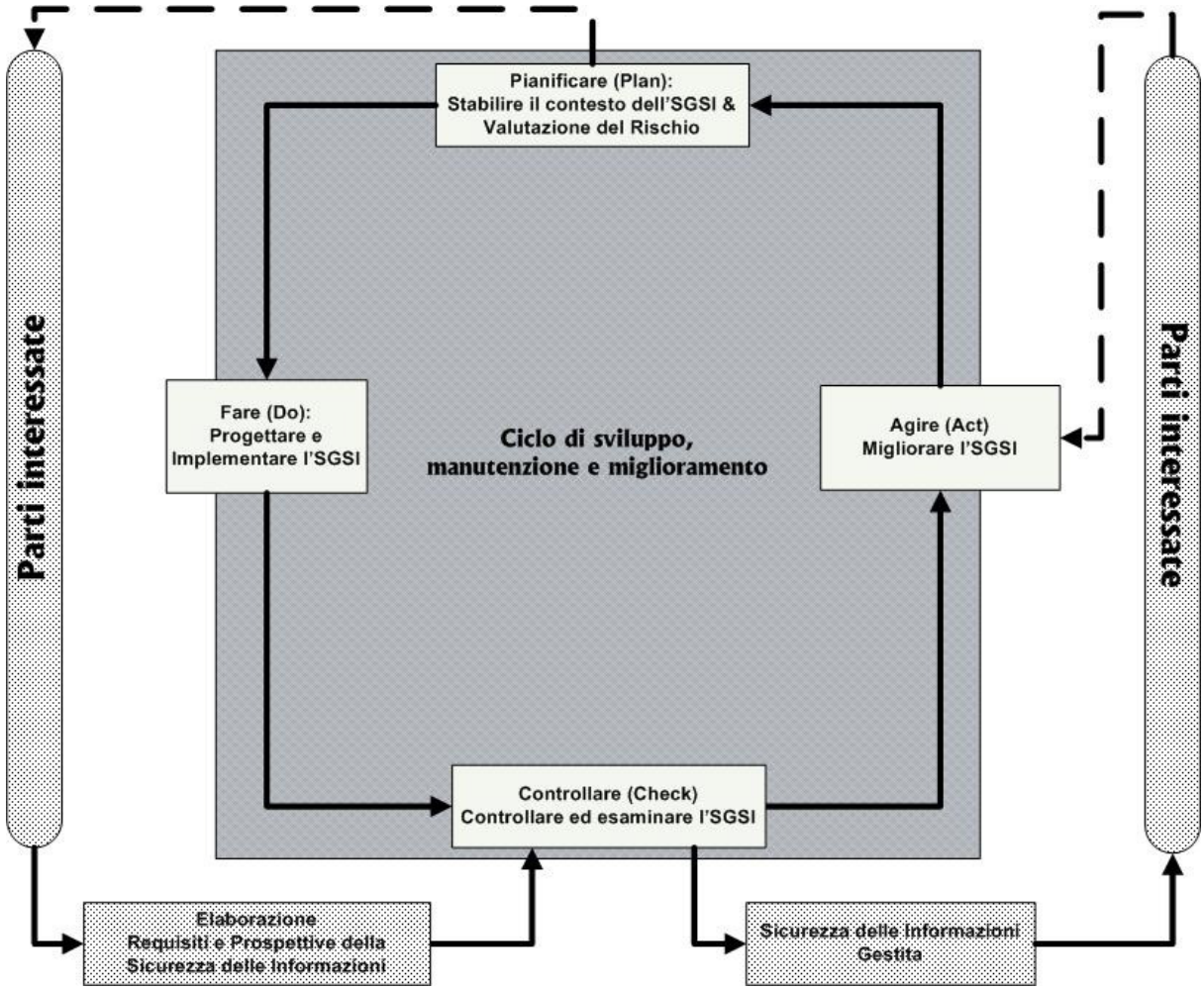
L'obiettivo di fondo della ISO 27001:2005 è il medesimo della versione BS 7799-2:2002: definire un modello internazionale in tema di gestione della sicurezza delle informazioni, ovvero una serie di linee guida per definire, progettare, realizzare, implementare, revisionare, mantenere e migliorare un S.G.S.I. o Information Security Management System (I.S.M.S)..
In tal senso viene utilizzato il modello PDCA (Plan-Do-Check-Act) o ciclo di Deming, già introdotto dalla BS7799-2:002, che definisce il processo di controllo e miglioramento continuo dell'ISMS.

Il ciclo di Deming è una metodologia che guida il processo di miglioramento continuativo e che si realizza attraverso un'azione ciclica basata sulla reiterazione sequenziale delle quattro fasi che costituiscono la "cosiddetta ruota" di Deming:

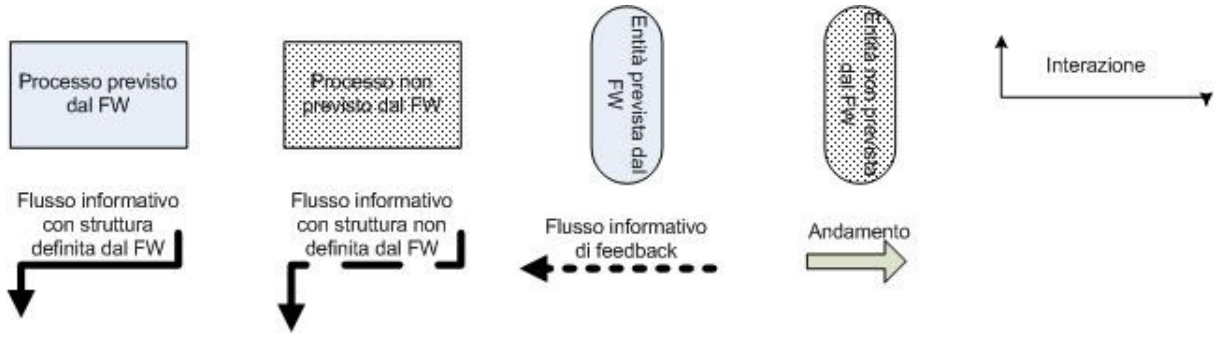


che si traduce per i Sistemi di Gestione della Sicurezza delle Informazioni nel seguente modello di rappresentazione:

Fasi del ciclo di vita del SGSI : Plan-Do-Check-Act



legenda :



Processi- Attività ed Output delle fasi del ciclo di vita di un S.G.S.I.

FASI del CDV	PROCESSI	ATTIVITA'
Pianificare (Plan) *descritta nella norma nel paragrafo 4.2.1*	**Stabilire il contesto dell'SGSI & Valutazione del Rischio**	• Definire lo scopo dell'SGSI e le regole • Definire un approccio sistematico alla valutazione del rischio • Identificare i rischi • Applicare l'approccio sistematico per valutare i rischi • Identificare e valutare le scelte per il trattamento dei rischi • Scegliere controlli oggettivi e controlli per il trattamento dei rischi
Fare (Do) *descritta nella norma nel paragrafo 4.2.2 (poche righe, ma sono le attività più importanti cioè quelle realizzative del Sistema di Gestione della Sicurezza)*	***Progettare e Implementare l'SGSI***	• Misurare le performance dell'SGSI • Identificare i miglioramenti nell'SGSI e implementarle effettivamente • Prendere azioni correttive e preventive appropriate • Comunicare i risultati e le azioni e consultarsi con tutte le parti coinvolte • Revisionare l'SGSI dove necessario • Assicurarsi che le revisioni raggiungano gli scopi loro designati
Controllare (Check) *descritta nella norma nel paragrafo 4.2.3*	***Controllare ed esaminare l'SGSI*** -	• Eseguire le procedure e altri controlli (p.e. per scoprire errori, identificare breccie riuscite e non riuscite) • Intraprendere regolari revisioni dell'efficacia dell'SGSI • Esaminare il livello di rischio residuo e del rischio accettabile • Eseguire procedure • Implementare un programma specifico di controllo • Implementare controlli che sono stati scelti • Gestire le operazioni • Gestire le risorse • Implementare le procedure e altri controlli dei procedimenti • re di gestione • Esaminare una revisione formale del proprio SGSI su base regolare • Registrare e scrivere il report di tutte le azioni ed eventi

Agire (Act) *descritta nella norma nel paragrafo 4.2.1*	**Migliorare l'SGSI**	• Implementare un programma specifico di controllo • Implementare controlli che sono stati scelti • Gestire le operazioni • Gestire le risorse • Implementare le procedure e altri controlli dei procedimenti

Requisiti

La ISO/IEC 27001: 2005 ha la seguente struttura :

- Dal Capitolo 0 al Capitolo 3 : Introduzione, Scopo della Norma, Termini e Definizioni;
- Dal cap. 4 al cap. 8: requisiti applicativi del Sistema di Gestione per la Sicurezza delle Informazioni
- Allegati: normativi e descrittivi a supporto di quanto citato nei capitoli precedenti. L'allegato A, in particolare, ricopre un ruolo fondamentale nelle fasi di implementazione operativa e audit del S.G.S.I., come vedremo di seguito.

All'interno dei capitoli (detti anche *requisiti* o *clausole)* dal 4 all'8 sono distribuiti i requisiti applicativi per i SGSI.

Requisito: 4 INFORMATION SECURITY MANAGEMENT SYSTEM SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI
Requisito: 5 MANAGEMENT RESPONSIBILITY RESPONSABIITA' DELLA DIREZIONE
Requisito: 6 INTERNAL ISMS AUDITS VERIFICHE ISPETTIVE INTERNE (AUDIT)
Requisito: 7 MANAGEMENT REVIEW OF THE ISMS RIESAME DELL'S.G.S.I. DA PARTE DELLA DIREZIONE
Requisito: 8 ISMS IMPROVEMENT MIGLIORAMENTO DELL'S.G.S.I.

Macrorequisito 4 : Sistema di Gestione per la Sicurezza delle Informazioni

Il Sistema di Gestione per la Sicurezza delle Informazioni è attuato attraverso i processi del sistema di gestione dell'organizzazione. Questi, qualora facenti parte con la politica e con gli obiettivi per la sicurezza delle informazioni, nonché con la sicurezza delle esigenze e delle aspettative delle parti interessate, dovrebbero essere protetti contro le proprie vulnerabilità e contro le minacce.
La sicurezza delle informazioni stabilita con la politica e gli obiettivi viene impostata durante la progettazione del sistema, viene creata durante il suo sviluppo e viene esercitata durante il funzionamento del sistema.

MACROREQUISITO 4.1: REQUISITI GENERALI
E' un requisito di tipo generale che richiede che il sistema di gestione sia coerente con il ciclo PDCA (Plan,Do,Act,Check)
Il Macrorequisito. 4.1 definisce le caratteristiche del SGSI che deve essere :

- stabilito;
- documentato;
- attuato;
- aggiornato;
- migliorato

in conformità con i requisiti normativi, tenendo conto dei rischi associati al businnes.

MACROREQUISITO 4.2 : STABILIRE E GESTIRE L' S.G.S.I.

Requisito 4.2.1 Stabilire l'S.G.S.I.
Descrive gli adempimenti che nello schema concettuale precedente abbiamo identificato con il titolo PLAN
In particolare il Requisito 4.2.1 definisce i vari passi per la fase di pianificazione (Fase Plan) del SGSI:

- definizione dell' ambito e dei confini;
- definizione della Politica per la sicurezza delle informazioni;
- Valutazione dei rischi;
- Trattamento dei rischi;
- Definizione delle contromisure;
- Accettazione da parte della Direzione dei rischi residui;
- Approvazione da parte della Direzione per l' attuazione del SGSI;
- Stesura di una Dichiarazione di applicabilità.

Requisito 4.2.2: Attuare e Condurre l'S.G.S.I.
Descrive gli adempimenti che nello schema concettuale precedente abbiamo identificato con il titolo DO:

- Stesura ed attuazione di un piano di trattamento dei rischi;
- Attuazione delle contromisure definite;
- Definizione dei criteri per la misurazione dell' efficacia dei controlli;
- Attuazione dei programmi di formazione ;
- Gestione delle attività operative del SGSI;
- Rilevazione e registrazione degli incidenti e pronta risposta.

Requisito 4.2.3: Monitorare e Riesaminare l'S.G.S.I.
Descrive gli adempimenti che nello schema concettuale precedente abbiamo identificato con il titolo CHECK:

- Attuazione delle attività di monitoraggio del SGSI;
- Conduzione di riesami per l' efficacia del SGSI;
- Misurazione della efficacia delle contromisure attuate;
- Riesame del livello di rischio residuo ed accettabile;
- Conduzione degli Audit interni pianificati;
- Conduzione del riesame della Direzione sul SGSI ad intervalli stabiliti;
- Aggiornamento dei Piani di sicurezza in relazione ai dati raccolti e riesami condotti;
- Registrazione di azioni ed eventi inerenti l' efficacia e le prestazioni del SGSI.

Requisito 4.2.4: Mantenere attivo, aggiornato e migliorare l'S.G.S.I.
Descrive gli adempimenti che nello schema concettuale precedente abbiamo identificato con il titolo ACT:

- Attuazione dei miglioramenti individuati;
- Attuazione di Azioni Correttive e Preventive stabilite;
- Comunicazione alle parti interessate dei risultati delle azioni di miglioramento;
- Assicurazione che i risultati del miglioramento raggiungano gli obiettivi prefissati.

MACROREQUISITO 4.3 : REQUISITI RELATIVI ALLA DOCUMENTAZIONE

Il Requisito 4.3 definisce la struttura della documentazione necessaria per la definizione del SGSI.

La documentazione comprende due tipologie :

- Descrizione di attività da condurre per la sicurezza delle informazioni : politiche, procedure, istruzioni operative)
- Tracciamento e registrazione della effettiva attuazione di quanto prescritto (registrazioni).

Sono elencate tutte le attività che devono essere messe in atto per assicurare un controllo efficace sia sui documenti che sulle registrazioni del SGSI.

Requisito 4.3.1 : Generalità

Il Requisito 4.3.1 definisce nel dettaglio la documentazione obbligatoria del SGSI :

- Politica per la sicurezza ed Obiettivi;
- Scopo (Perimetro) del SGSI;
- Metodologia per la valutazione dei rischi;
- Piano di trattamento dei rischi;
- Procedure documentate per : Gestione della documentazione, Verifiche Ispettive interne, Azioni Correttive e Preventive;
- Registrazioni inerenti il SGSI;
- Dichiarazione di Applicabilità : quale elenco delle misure adottate contenute nell' Allegato A della norma, compresi i motivi della scelta od eventuale esclusione dei controlli;
- Valutazioni dell' efficacia del SGSI e delle contromisure attuate.

Requisito 4.3.2 Tenuta sotto controllo dei documenti

Il requisito richiede:

- Che i documenti dell'ISMS siano approvati e mantenuti aggiornati nel tempo
- Che le modifiche siano identificate nel documento aggiornato e venga gestita la versione
- Che sia rese disponibili ai possibili utenti solo le versioni aggiornate all'ultimo livello
- Che la documentazione sia sempre leggibile ed identificabile (indice della documentazione con livelli delle versioni correnti dei documenti)
- Che la distribuzione (ove ciò avvenga) sia controllata in modo da sostituire le copie obsolete in possesso dei riceventi
- Che i documenti obsoleti siano segregati ed identificati(esw con sovrimpressione di apposita dicitura del tipo 'superato/annullato')

Requisito 4.3.3 Tenuta sotto controllo delle registrazioni

Non viene dato un elenco preciso di questa documentazione, ma si lascia all'Azienda l'identificazione di tutte le registrazioni utili a dimostrare la congruenza con la norma.

Solo otto tipi di documenti vengono tassativamente richiesti:

1. *quelli relativi alle prestazioni del sistema di gestione della sicurezza ed al trattamento degli incidenti di sicurezza (par- 4.3.3. Records shall be kept of the performance of the process as outlined in 4.2 and of all occurrences of significant security incidents related to the ISMS)*
2. *documentazione di azioni ed eventi che possono avere un impatto sull'ISMS*
3. *quelli relativi all'addestramento (profili di competenze necessarie,corsi programmati ed effettuati dal personale)*
4. *i verbali del riesame periodico da parte dell'alta direzione*
5. *documentazione delle azioni correttive*
6. *documentazione delle azioni preventive*
7. *documentazione relativa alle prestazioni dell'ISMS*
8. *documentazione delle visite ispettive (piano, consuntivo attività, relazioni)*

MACROREQUISITO 5: RESPONSABILITÀ DELLA DIREZIONE

*L'alta Direzione dell'organizzazione dovrebbe fornire evidenza del suo impegno nello sviluppo, nell'attuazione, nel funzionamento, nel monitoraggio, nel riesame, nel mantenimento e nel miglioramento continuo del S.G.S.*I.

Requisito 5.1: Impegno della Direzione

- Definire policy
- Assicurare la predisposizione di obiettivi e piani
- Stabilire ruoli e responsabilità
- Comunicare all'azienda l'importanza dell'ISMS
- Fornire le risorse necessarie per ISMS
- Stabilire i livelli max di rischio accettabile (v la metodologia descritta sopra)
- Assicurare audit periodici dell'ISMS
- Condurre i riesami dell'ISMS come richiesto dalla norma

Requisito 5.2 : Gestione delle Risorse

E' composto dai sottorequisiti:

- 5.2.1 Provision of resources

  Il management deve fornire le risorse necessarie a realizzare,mantenere e controllare l'ISMS.

- 5.2.2 Training, Awareness and competence

  Consiste nel classico processo di identificazione dei ruoli e delle competenze, della valutazione dei singoli dipendenti addetti all'ISMS, della pianificazione e realizzazione dell'addestramento a copertura dei gap individuati per ogni dipendente

MACROREQUISITO 6 : VERIFICHE ISPETTIVE INTERNE (AUDIT)

Il concetto di audit nell'ambito della sicurezza delle informazioni viene utilizzato per esprimere diverse modalità di controllo. La norma prevede per audit un controllo che dovrebbe essere eseguito per assicurare la continuità dei processi di business.
La direzione deve provvedere a effettuare degli audit interni o visite ispettive dell'ISMS (SGSI) ad intervalli pianificati per determinare se gli obiettivi di controllo, i controlli, i processi e le procedure dell'ISMS:

- sono conformi ai requisiti di questo standard ed alla legislazione e/o alla normativa inerente (cogente)
- sono conformi ai requisiti di sicurezza delle informazioni identificati
- sono efficacemente implementati e mantenuti
- funzionano come atteso.

Il programma di audit necessita di essere pianificato, prendendo in considerazione lo stato e l'importanza dei processi e delle aree in oggetto, come anche i risultati degli audit precedenti.
I criteri per l'audit, l'ambito, la frequenza e i metodi devono essere ben definiti rispettando le definizioni, principi e gestione di un programma di audit previsti dalla ISO 19011.
La selezione degli auditors e la condotta dell'audit deve garantire obiettività ed imparzialità dei processi. Gli auditors non possono effettuare audit sul loro proprio lavoro.

Le responsabilità e i requisiti per pianificare e condurre gli audit, nonché per presentare i risultati e mantenere le annotazioni (vedi 4.3.3), devono essere definiti in una procedura documentata.

Il management responsabile dell'area soggetta all'audit deve garantire che si agirà senza ritardo per eliminare le non conformità individuate e le loro cause. Le attività di miglioramento devono includere la verifica delle azioni intraprese e la presentazione dei risultati di verifica (vedi sezione macrorequisito 8).

MACROREQUISITO 7 : RIESAME DEL S.G.S.I. DA PARTE DELLA DIREZIONE

La direzione dovrebbe impostare i propri riesami in modo di andare oltre la verifica della continua idoneità, adeguatezza ed efficacia del S.G.S.I., per estendersi a verificare tutta l'organizzazione ed a valutare il grado di efficienza del sistema stesso. Questo riesame può valutare il grado di efficienza del sistema stesso. Questo riesame può valutare di adattare la politica e gli obiettivi della stessa.
I riesami dovrebbero comprendere la valutazione delle opportunità per il miglioramento e le esigenze di modifiche del S.G.S.I., della politica e degli obiettivi per la sicurezza dell'informazione.

Requisito 7.1 Generalità
La direzione deve riesaminare ad intervalli pianificati l'ISMS per assicurare il ciclo di miglioramento e la verifica del corretto funzionamento delle regole / standard aziendali in materia di ISMS

Requisito 7.2 Elementi in ingresso per il riesame (molto simile a ISO 9001)
L'input è composto di seguenti elementi:

- Risultato dei controlli/visite ispettive
- Informazioni di ritorno da tute le parti interessate
- Tecnologie/procedure che sono proposte dai vari responsabili dell'ISMS in ottica di miglioramento
- Stato delle azioni preventive/correttive
- Minacce e vulnerabilità non soddisfacentemente trattate nei precedenti risk assessments
- Follow up sulle iniziative decise nei precedenti riesami
- Qualsiasi evento interno/esterno all'azienda ce debba essere riflesso nell'ISMS
- Raccomandazioni per il miglioramento

Requisito 7.3 Elementi in uscita dal riesame (molto simile a ISO 9001)
L'output tratterà i seguenti argomenti:

- programmi di miglioramento
- aggiornamento del piano di trattamento del rischio
- requisiti di aggiornamento delle procedure sulla base di: bus requirement /security requirements, business processes (nuovi,variati), normativa,obblighi contrattuali, variazioni dei livelli di rischio accettabili
- dimensionamento risorse
- miglioramenti nei sistemi di monitoraggio delle prestazioni del sistema

MACROREQUISITO 8 : MIGLIORAMENTO DEL S.G.S.I.

L'organizzazione dovrebbe migliorare con continuità l'efficacia del sistema di gstione per la sicurezza dell'informazione, utilizzando la politica per la sicurezza, gli obiettivi per la sicurezza, i risultati delle verifiche ispettive (audit), l'analisi degli eventi, le azioni correttive e preventive ed i riesami da parte della direzione.
Le varie attività del processo di miglioramento, a partire dalla individuazione delle opportunità di miglioramento, all'analisi degli eventi, alla ricerca delle cause, alla definizione delle azioni correttive o azioni preventive fino all'attuazione ed alla verifica dell'efficacia dell'azione, dovrebbero essere effettuate con la massima obiettività senza preconcetti ma basandosi sui fatti.
Affinché la soluzione attuata sia completamente efficace, è necessario provvedere all'adeguato addestramento e formazione del personale coinvolto nel processo.

Requisito 8.1: Miglioramento continuo
Si richiamano tutte le possibili azioni per questo obiettivo e precisamente:

- utilizzo della policy
- assegnazione di obiettivi di sicurezza
- risultati delle visite ispettive
- analisi degli eventi monitorati
- azioni correttive e preventive
- riesami della direzione

Requisito 8.2: Azioni correttive
Sono le azioni adottate per eliminare le cause che sono alla base delle non conformità
Queste azioni debbono mirare alle 'cause prime' e non solo alla sistemazione estemporanea di un inconveniente/ gestione di un incidente

Requisito 8.3: Azioni preventive
Sono le iniziative che vengono attivate per prevenire un inconveniente/incidente
Un esempio può essere l'introduzione di strumenti automatici al posto di controlli manuali che possono risultare incompleti o condizionati da situazioni particolari di carico di lavoro,conoscenze ecc

A completamento dei Requisti della norma troviamo l'allegato A che è l'unico allegato "normativo" cioè obbligatorio per la corretta implementazione e certificazione del SGSI.
In esso sono rappresentati:

- **11 Domini** di aspetti inerenti la sicurezza delle informazioni
- **39 Obiettivi** (a loro volta suddivisi in 133 contromisure o controlli) utili per la riduzione/mitigazione dei rischi individuati nella fase di valutazione dei rischi.

Ciascun Dominio fissa un argomento (ad esempio A.7 Gestione degli Asset) ed all'interno di questo definisce gli obiettivi per la sicurezza (nel nostro esempio definisce 2 obiettivi di controllo: Responsabilità per gli asset e Classificazione delle Informazioni). Ciascun obiettivo è quindi esploso in dettagli operativi (ad esempio: A.7.1.1 Inventario degli asset).
Quindi una struttura logica orientata ad individuare potenziali soluzioni organizzative (e talvolta tecniche) a fronte di rischi valutati e relativi danni potenziali alle informazioni.

Eccone l'esempio di quanto sopra citato:

A.7 Gestione degli asset		
A.7.1 Responsabilità per gli asset Obiettivo: Raggiungere e mantenere un'adeguata protezione degli asset dell'organizzazione		
A.7.1.1	**Inventario degli asset**	**Controllo** **Tutti gli asset devono essere chiaramente identificati e deve essere creato e mantenuto un inventario di tutti gli asset importanti.**
A.7.1.2	**Detenzione degli asset**	**Controllo** **Tutte le informazioni e gli asset associati con le strutture di elaborazione delle informazioni devono essere "detenute" da una parte designata dell'organizzazione.**
A.7.1.3	**Uso accettabile degli asset**	**Controllo** **Le regole per un uso accettabile delle informazioni e degli asset associati alle strutture di elaborazione delle informazioni devono essere identificate, documentate ed implementate.**
A.7.2 Classificazione delle informazioni **Obiettivo: Garantire che gli asset informativi ricevano una protezione adeguata**		
A.7.2.1	**Linee guida per la classificazione**	**Controllo** **Le informazioni devono essere classificate in base al loro valore, ai requisiti legali, alla sensibilità e criticità verso l'organizzazione.**
A.7.2.2	**Etichettatura e manipolazione delle informazioni**	**Controllo** **In base allo schema di classificazione adottato dall'organizzazione, deve essere sviluppato ed implementato un appropriato insieme di procedure per l'etichettatura e la manipolazione delle informazioni.**

Inoltre l'allegato A costituisce il collegamento con lo standard ISO/IEC 27002:05, l'uso di quest'ultimo standard deve essere considerato come una raccolta di best practice cui riferirsi per trarre idee e spunti in tema di contromisure.
Lo standard ISO/IEC 27002:05 *non è in alcun modo certificabile,* pertanto la sua utilizzazione è assolutamente libera e priva di legami obbligatori nei confronti di ISO/IEC 27001:05. Anzi, in tal senso è possibile utilizzare standard diversi per coprire gli aspetti citati nell'allegato A della ISO/IEC 27001:05.

L'appendice A è particolarmente importante perché elenca tutte le protezioni (la norma dice 'Control objectives an controls') che debbono essere prese in considerazione per essere applicate alle risorse che si debbono proteggere dalle minacce esterne.
A rinforzare l'obbligo di analizzare tutti questi controlli la norma dice al paragrafo 4.2.1

- Punto g) la scelta dei controlli (da Appendice A) utilizzati deve essere giustificata
- Punto h) i motivi della scelta di alcuni dei controlli (da Appendice A) e della esclusione degli altri debbono essere giustificati

Pertanto non risultano accettabili dichiarazioni del tipo:

- Il trasferimento in produzione non è regolamentato perché l'attuale prassi va bene (…salvo poi sentire ammissioni sui problemi relativi)
- La crittografia non è applicabile al ns ambiente

- Nella ns azienda non si usa conferire incarichi formali (e quindi neanche per la sicurezza)
- …….

I controlli dell'appendice A

L'appendice inizia con il paragrafo o sezione A5 per allineare la numerazione alla norma 27002:2005
Quindi i paragrafi o sezioni da 5 a 15 della ISO 27002:2005 forniscono consigli sull'implementazione e indicazioni sullo stato dell'arte nel supportare i controlli specificati tra A.5 e A.15.

I Domini, che possiamo identificare anche come processi, sono:

- Politiche di sicurezza
- Organizzazione per la sicurezza;
- Classificazione e controlli delle risorse
- Sicurezza del personale
- Sicurezza fisica e ambientale
- Comunicazione e gestione delle operazioni
- Controllo degli accessi
- Sviluppo e manutenzione dei sistemi
- Gestione degli incidenti
- Gestione della continuità delle attività aziendali
- Conformità

Vengono di seguito sintetizzati i Processi relativi alla sicurezza riportati nell' Allegato A

A.5 POLITICA PER LA SICUREZZA

A.5.1 POLITICA DELLA SICUREZZA DELLE INFORMAZIONI
Fornire indicazioni e direttive manageriali e supportare la sicurezza delle informazioni, in conseguenza dei requisiti di business, cogenti e regolamenti. *CONTROLLI* *A.5.1.1 Documento della Politica per la sicurezza delle informazioni* *A.5.1.2 Riesame e valutazione della Politica*

A.6 ORGANIZZAZIONE PER LA SICUREZZA

A.6.1 ORGANIZZAZIONE DELLA SICUREZZA

Gestire la sicurezza delle informazioni nell' ambito dell' Organizzazione.

CONTROLLI
A.6.1.1 Impegno della direzione per la sicurezza
A.6.1.2 Coordinamento della sicurezza
A.6.1.3 Responsabilità per la sicurezza
A.6.1.4 Processo d' autorizzazione per servizi informativi
A.6.1.5 Impegno alla riservatezza
A.6.1.6 Contatti con le autorità
A.6.1.7 Contatti con gruppi interessati
A.6.1.8 Riesame indipendente della sicurezza

A.6.2 PARTI ESTERNE (OUTSOURCING)

Mantenere attiva la sicurezza delle applicazioni e dei servizi aziendali nel caso che siano coinvolte altre Organizzazioni (Outsourcing).

CONTROLLI
A.6.2.1 Identificazione dei rischi derivanti da parti esterne
A.6.2.2 Indirizzi di sicurezza negli accordi con i clienti
A.6.2.3 Indirizzi di sicurezza negli accordi con le parti esterne

A.7 GESTIONE DEI BENI

A.7.1 RESPONSABILITA' DEI BENI

Verifica del mantenimento di una adeguata protezione di tutte i beni dell' Organizzazione.

CONTROLLI
A.7.1.1 Inventario dei beni
A.7.1.2 Proprietario dei beni
A.7.1.3 Uso accettabile dei beni

A.7.2 CLASSIFICAZIONE DELLE INFORMAZIONI

Garantire che le risorse informative ricevano un adeguato livello di protezione. Le informazioni dovrebbero essere classificate per indicare esigenze, priorità e livello di protezione.

CONTROLLI
A.7.2.1 Linee guida per la classificazione
A.7.2.2 Identificazione e trattamento delle informazioni.

A.8 SICUREZZA DEL PERSONALE

A.8.1 PRIMA DELL' IMPIEGO

Assicurare che gli impiegati, personale a contratto, e terze parti conoscano le loro responsabilità, e siano adatti per il loro ruolo a loro assegnato, per ridurre il rischio di furto e frode.

CONTROLLI
A.8.1.1 Ruoli e responsabilità
A.8.1.2 Selezione
A.8.1.3 Termini e condizioni di impiego

A.8.2 DURANTE L' IMPIEGO

Assicurare che gli impiegati, personale a contratto, e terze parti conoscano le loro responsabilità, e sono addestrati per la loro normale attività riducendo i rischi di errori.

CONTROLLI
A.8.2.1 Responsabilità della direzione
A.8.2.2 Consapevolezza, competenza e formazione
A.8.2.3 Processi disciplinari

A.8.3 TERMINE O CAMBIO DI IMPIEGO

Assicurare che gli impiegati, personale a contratto e terze parti che escono dall' Organizzazione o cambiano impiego lo facciano in maniera controllata.

CONTROLLI
A.8.3.1 Responsabilità
A.8.3.2 Restituzione dei beni
A.8.3.3 Rimozione dei diritti di accesso

A.9 SICUREZZA FISICA ED AMBIENTALE

A.9.1 AREE DI SICUREZZA

Prevenire accessi non autorizzati, danni ed interferenze alle infrastrutture ed alle informazioni.

CONTROLLI
A.9.1.1 Perimetro di sicurezza
A.9.1.2 Controlli accesso fisico

A.9.1.3 Sicurezza negli uffici, nelle stanze e nelle strutture
A.9.1.4 Protezione contro minacce esterne ed ambientali
A.9.1.5 Lavoro nelle aree di sicurezza
A.9.1.6 Accesso pubblico, aree di carico e scarico

A.9.2 SICUREZZA NEGLI IMPIANTI

Prevenire la perdita, il danno o la compromissione delle risorse aziendali o l'interruzione delle attività aziendali.

CONTROLLI
A.9.2.1 Ubicazione e protezione degli impianti
A.9.2.2 Infrastrutture di supporto
A.9.2.3 Sicurezza nel cablaggio
A.9.2.4 Manutenzione negli impianti
A.9.2.5 Sicurezza nelle attrezzature fuori sede
A.9.2.6 Smaltimento e riuso delle attrezzature
A.9.2.7 Trasferimento di proprietà

A.10 COMUNICAZIONE E GESTIONE DELLE OPERAZIONI

A.10.1 RESPONSABILITA' E PROCEDURE OPERATIVE

Verificare la corretta e sicura gestione delle informazioni nei processi.

CONTROLLI
A.10.1.1 Procedure documentate
A.10.1.2 Controllo modifiche
A.10.1.3 Separazione tra compiti e mansioni
A.10.1.4 Separazione tra ambiente di sviluppo ed ambiente operativo

A.10.2 GESTIONE DELL' EROGAZIONE DEI SERVIZI IN OUTSOURCING

Implementare e mantenere un adeguato livello di sicurezza nella erogazione dei servizi in accordo con i requisiti contrattuali definiti per i servizi .

CONTROLLI
A.10.2.1 Erogazione del servizio
A.10.2.2 Monitoraggio e riesame del servizio
A.10.2.3 Gestione delle modifiche

A.10.3 PIANIFICAZIONE ED ACCETTAZIONE DEL SISTEMA

Ridurre il rischio di guasti del sistema.

CONTROLLI
A.10.3.1 Pianificazione delle capacità
A.10.3.2 Accettazione dei sistemi

A.10.4 PROTEZIONE DA SOFTWARE DANNOSO E CODICI AUTOESEGUIBILI

Proteggere l'integrità del software e delle informazioni.

CONTROLLI
A.10.4.1 Controlli contro software dannosi
A.10.4.2 Controlli contro codici autoeseguibili

A.10.5 BACK UP

Garantire l' integrità e la disponibilità dei processi d' informazione e dei servizi di comunicazione.

CONTROLLI
A.10.5.1 Back up delle informazioni

A.10.6 GESTIONE DELLE RETI

Assicurare la salvaguardia delle informazioni nelle reti di comunicazione e la protezione delle infrastrutture di supporto.

CONTROLLI
A.10.6.1 Controlli di rete
A.10.6.2 Sicurezza della rete

A.10.7 GESTIONE E SICUREZZA DEI SUPPORTI RIMOVIBILI

Prevenire il danneggiamento delle proprietà e l' interruzione delle attività aziendali .

CONTROLLI
A.10.7.1 Gestione dei supporti
A.10.7.2 Eliminazione dei supporti
A.10.7.3 Procedure per il trattamento delle informazioni
A.10.7.4 Sicurezza della documentazione di sistema

A.10.8 SCAMBIO DI INFORMAZIONI

Mantenere la sicurezza nello scambio di informazioni all' interno dell' Organizzazione con altre entità esterne.

CONTROLLI
A.10.8.1 Politiche e procedure per lo scambio di informazioni
A.10.8.2 Accordi per lo scambio di software e di dati
A.10.8.3 Trasporto di supporti fisici
A.10.8.4 Posta elettronica
A.10.8.5 Sistemi informativi relativi al business

A.10.9 COMMERCIO ELETTRONICO

Assicurare la sicurezza dei servizi di commercio elettronico e il loro uso sicuro .

CONTROLLI
A.10.9.1 Commercio elettronico
A.10.9.2 Transazioni on -line
A.10.9.3 Informazioni disponibili al pubblico

A.10.10 MONITORAGGIO

Rilevare attività non autorizzate.

CONTROLLI
A.10.10.1 Log di Audit
A.10.10.2 Monitoraggio dell ' utilizzo dei sistemi
A.10.10.3 Protezione dei log
A.10.10.4 Log degli amministratori e operatori
A.10.10.5 Log di errori
A.10.10.6 Sincronizzazione degli orologi

A.11 CONTROLLO DEGLI ACCESSI

A.11.1 REQUISITI PER IL CONTROLLO

Garantire che l' accesso alle informazioni avvenga in modo controllato.

CONTROLLI
A.11.1.1 Politica di controllo degli accessi

A.11.2 GESTIONE DEGLI ACCESSI UTENTE

Assicurare che i diritti di accesso alle informazioni siano opportunamente autorizzati, definiti e mantenuti.

CONTROLLI
A.11.2.1 Registrazione degli utenti
A.11.2.2 Gestione dei privilegi
A.11.2.3 Gestione delle password degli utenti
A.11.2.4 Revisione dei diritti di accesso degli utenti

A.11.3 RESPONSABILITA' DELL' UTENTE

Prevenire accessi di utenti non autorizzati.

CONTROLLI
A.11.3.1 Uso delle password
A.11.3.2 Postazioni di lavoro non presidiate
A.11.3.4 Gestione del posto di lavoro

A.11.4 CONTROLLO DEGLI ACCESSI IN RETE

Proteggere i servizi in rete.

CONTROLLI
A.11.4.1 Politica sull'uso dei servizi della rete
A.11.4.2 Autenticazione dell' utente per connessioni esterne
A.11.4.3 Autenticazione dell' apparecchiatura in rete
A.11.4.4 Protezione per le porte diagnostiche remote e la configurazione
A.11.4.5 Separazione delle reti
A.11.4.6 Controllo di connessione della rete
A.11.4.7 Controllo dell' instradamento di rete

A.11.5 CONTROLLO DI ACCESSO AL SISTEMA OPERATIVO

Prevenire l'utilizzo non autorizzato di risorse informatiche.

CONTROLLI
A.11.5.1 Procedura di log on sicure
A.115.2 Identificazione ed autenticazione degli utenti
A.115.3 Sistema di gestione delle password
A.115.4 Utilizzo dei programmi di utilità del sistema
A.115.5 Temporizzazione della sessione (Time out)
A.11.5.6 Limitazioni del tempo di connessione

A.11.6 CONTROLLO DEGLI ACCESSI ALLE APPLICAZIONI

Prevenire accessi non autorizzati alle informazioni contenute nei sistemi informativi.

CONTROLLI
A.11.6.1 Limitazione degli accessi alle informazioni
A.11.6.2 Isolamento dei sistemi con dati sensibili

A.11.7 COMPUTER PORTATILI E TELELAVORO

Assicurare la sicurezza delle informazioni quando sono utilizzati computer portatili e attività svolte in telelavoro.

CONTROLLI
A.11.7.1 Computer portatili
A.11.7.2 Telelavoro

A. 12 SVILUPPO E MANUTENZIONE DEI SISTEMI

A.12.1 REQUISITI DI SICUREZZA DEI SISTEMI

Assicurare la sicurezza intrinseca dei sistemi.

CONTROLLI
A.12.1.1 Analisi e specifiche

A.12.2 SICUREZZA NEI SISTEMI APPLICATIVI

Prevenire perdite, modifiche o usi scorretti dei dati degli utenti nei sistemi applicativi.

CONTROLLI
A.12.2.1 Validazione dei dati in ingresso
A.12.2.2 Controllo dell' elaborazione interna
A.12.2.3 Integrità dei messaggi
A.10.2.4 Validazione dei dati in uscita

A.12.3 CONTROLLI CRITTOGRAFICI

Proteggere la riservatezza, l' autenticità e/o l'integrità delle informazioni.

CONTROLLI
A.12.3.1 Politica d' uso dei controlli crittografici
A.10.3.2 Gestione delle chiavi

A.12.4 SICUREZZA DEI FILE DI SISTEMA

Assicurare che le attività di progettazione e supporto siano condotte in maniera sicura.

CONTROLLI
A.12.4.1 Controllo del software operativo
A.12.4.2 Protezione dei dati per il test di sistema
A.12.4.3 Controllo degli accessi alle librerie codici sorgenti dei programmi

A.12.5 SICUREZZA NEI PROCESSI DI SVILUPPO

Mantenere la sicurezza dei software applicativi e delle informazioni .

CONTROLLI
A.12.5.1 Procedure di controllo di configurazione
A.12.5.2 Riesame tecnico delle modifiche al sistema operativo
A.12.5.3 Limitazioni alle modifiche dei pacchetti software
A.12.5.4 Fuga di informazioni
A.12.5.5 Sviluppo software in outsourcing

A.12.6 GESTIONE DELLE VULNERABILITA'

Ridurre il rischio dalle esplosioni di vulnerabilità tecniche pubblicate .

CONTROLLI
A.12.6.1 Controllo delle vulnerabilità tecniche

A.13 GESTIONE DEGLI INCIDENTI

A.13.1 RAPPORTI SUGLI EVENTI DELLA SICUREZZA E VULNERABILITA'

Assicurare che le informazioni sugli eventi riguardanti la sicurezza e le relative vulnerabilità associate siano comunicate ed a disposizione per consentire tempestive azioni da intraprendere .

CONTROLLI
A.13.1.1 Rapporti di incidenti
A.13.1.2 Segnalazioni sulle vulnerabilità

A.13.2 GESTIONE DEGLI INCIDENTI SULLA SICUREZZA E MIGLIORAMENTO

Assicurare che venga applicato un approccio costante ed efficace alla gestione degli incidenti

CONTROLLI
A.13.2.1 Responsabilità e procedure
A.13.2.2 Analisi degli incidenti
A.13.2.3 Raccolta evidenze

A. 14 GESTIONE DELLA CONTINUITA' DELL' ATTIVITA' AZIENDALE

A.14.1 ASPETTI DI GESTIONE DELLA CONTINUITA'

Contrastare interruzioni della attività, e proteggere i processi critici dal punto di vista aziendale dagli effetti causati da malfunzionamento o disastri.

CONTROLLI
A.14.1.1 Processo di gestione della continuità operativa
A.14.1.2 Analisi d'impatto
A.14.1.3 Stesura ed attuazione dei piani di continuità
A.14.1.4 Struttura di supporto per la pianificazione della continuità
A.14.1.5 Prova, manutenzione e rivalutazione dei piani di continuità

A. 15 CONFORMITA'

A.15.1 CONFORMITA' CON LA LEGISLAZIONE CORRENTE

Ridurre il rischio dovuto al mancato rispetto delle leggi e le azioni da intraprendere a causa del mancato rispetto degli obblighi contrattuali ai fini della sicurezza.

CONTROLLI
A.15.1.1 Identificazione della legislazione applicabile
A.15.1.2 Diritto di proprietà intellettuale
A.15.1.3 Salvaguardia delle registrazioni aziendali
A.15.1.4 Protezione dei dati e riservatezza delle informazioni personali
A.15.1.5 Prevenzione da usi impropri dei sistemi informativi
A.15.1.6 Regolamento dei controlli crittografici

A.15.2 RIESAME DELLA POLITICA DELL' IS

Il personale direttivo deve assicurarsi che tutte le procedure di sicurezza, all' interno della propria area di competenza, siano applicate correttamente.

CONTROLLI
A.15.2.1 Conformità con le politica e norme di sicurezza
A.15.2.2 Verifica di conformità tecnica

A.15.3 CONSIDERAZIONI SUGLI AUDIT DI SISTEMA

Massimizzare l' efficacia e minimizzare le interferenze causate dalle attività di audit di sistema.
CONTROLLI
A.15.3.1 Controlli di audit sui sistemi informativi
A.15.3.2 Protezione dedli strumenti per gli audit dei sistemi informativi

7. MODALITÀ DI APPLICAZIONE

Possibili usi della norma in ambito PA

Come per altre certificazioni di sistemi di gestione (es. Qualità ISO 9001) riconosciuti in ambito internazionale l' utilizzo della ISO/IEC 27001:2005 costituisce un mezzo per un rapporto di fiducia tra le diverse componenti che intervengono nella acquisizione, gestione progetti fornitura ed erogazione di un servizio ICT.
L' utilizzo della certificazione può essere stimolata nelle situazioni ed ambiti di elevata criticità che possono essere individuate nella PA.

Gli ambiti, nei quali è possibile utilizzare lo standard trattato, sono quelli in cui possono essere presenti criticità nella gestione delle informazioni quali :

- Tutela della salute ed incolumità dei cittadini;
- Danni elevati di tipo economico per il cittadino e la PA;
- Danni per perdita di dati (Archivi, Dati Anagrafici, ecc)

Il compito è quello di verificare all' interno della PA se esistono e sono individuabili servizi IT e trattamento dati ed informazioni tali da classificarli in situazioni ad elevato rischio.
In questi casi dopo l' esecuzione di una verifica di valutazione, si può decidere l' opportunità di una eventuale modalità di certificazione sulla Sicurezza delle Informazioni.

Acquisizione di forniture ICT

Nella acquisizione di forniture ICT occorre considerare oltre i requisiti di qualità anche i requisiti di sicurezza. I requisiti di sicurezza contemplano la garanzia ed il raggiungimento degli obiettivi fissati anche in situazione in cui si presentano eventi anomali non previsti dalle condizioni di esercizio ordinario, quali incidenti di sicurezza, calamità naturali, attacchi ai sistemi.
I requisiti di sicurezza definiscono anche le modalità di attuare contrasto e contromisure in un certo numero di casi anomali, che sono stati preventivamente analizzati e considerati per gli aspetti strategici ed economici. Tale considerazioni provengono dai risultati di un processo definito, analitico, riproducibile e confrontabile nel tempo che viene definito gestione dei rischi.
Pertanto in ogni fornitura di servizi ICT bisognerebbe considerare tutti gli aspetti previsti in una gestione dei rischi, in funzione dell' importanza e dalla natura della fornitura considerata.
Nell' ambito di contratti di acquisizione dovrebbero essere considerati gli aspetti :

- Obblighi e responsabilità dei contraenti nella gestione di casi anomali vedi misure di sicurezza;
- Modalità di gestione con cui devono essere gestiti eventi anomali imprevisti, ruoli e obblighi che le controparti dovranno assumere in tali circostanze.

Gestione progetti ICT

La gestione dei progetti ICT una volta ritenuta soltanto utile, oggi è indispensabile non solo per le organizzazioni ma anche per la PA/PAL. Per gestire il lavoro come progetto è necessario, però, rivedere l'organizzazione e ottimizzare l'impiego delle risorse**.**
Lo standard ISO/IEC 27001:2005 prende in considerazione l'intero processo di gestione delle informazioni e prevede il coinvolgimento e l'integrazione di tutti gli elementi della catena del valore dell'organizzazione, ovvero le persone, i processi, le tecnologie, al fine di consentire una corretta gestione delle informazioni e ridurre il rischio di danneggiamenti, furti … anche nella gestione dei progetti ICT.
Un servizio ICT che viene acquisito dovrebbe prevedere la gestione della sicurezza, gli eventuali casi anomali, e prevedere un livello di sicurezza adeguato.
Per questo motivo si procede :

- Scegliendo fornitori di provata affidabilità;
- Verificando le caratteristiche di sicurezza;

- Richiedendo e necessario la certificazione sul sistema di sicurezza delle informazioni.

E' pertanto molto importante prevedere la scelta di fornitori che hanno ottenuto un riconoscimento da parte di un ente terzo sulla gestione della sicurezza.
Nel caso di gestione progetti di servizi ICT ancora oggi sono pochi i fornitori che dispongono di tale certificazione. Pertanto rimangono aperte le altre alternative di scegliere fornitori affidabili e valutare opportunamente le caratteristiche di sicurezza preventivamente.
A questo punto la PA dovrà analizzare il grado di sicurezza informatica del fornitore , a partire dalle procedure e dalle infrastrutture adottate; identificare gli ambiti specifici su cui mettere a punto un piano d'azione; sviluppare soluzioni concrete in grado di rispondere alle reali esigenze di sicurezza basandosi sugli standard internazionali di riferimento e sul rispetto della normativa vigente.
Si rimanda al Macrorequisito 4 dello standard ISO/IEC 27001:2005 sui processi che un fornitore dovrebbe implementare per dirsi compliant all'applicazione di un Sistema di Gestione per la Sicurezza delle Informazioni.

Erogazione di servizi ICT

Nella erogazione di servizi ICT è compreso anche il caso in cui il contratto viene erogato da un fornitore in outsourcing, in cui la responsabilità della gestione dei processi è demandata ad un'altra Organizzazione.
Anche gli aspetti della sicurezza e della gestione dei casi anomali viene demandata al fornitore. I requisiti di sicurezza riguardano la gestione attraverso contromisure sugli aspetti di eventi previsti e non previsti.
I requisiti di sicurezza dovrebbero essere espressi come caratteristiche intrinseche del servizio. Previste dal contratto che dovrebbe specificare gli obblighi del fornitore del servizio in relazione ad una serie di casistiche ed aspetti, e definire quali sono le prestazione e le misure a seguito di tali eventi.
Gli aspetti della sicurezza sono particolarmente critici nel caso che vengano erogati in outsourcing, e gli aspetti fondamentali a cui attenersi sono :

- Clausole di riservatezza e non divulgazione delle informazioni riservate;
- Modalità in cui il fornitore deve attenersi alle politiche di sicurezza stabilite dal committente;
- Obbligo del fornitore in merito alla registrazione e bollettini periodici sui problemi di sicurezza;
- Procedure che il fornitore deve utilizzare in caso di incidenti di sicurezza;
- Diritto del committente di eseguire Audit sul rispetto dei requisiti e clausole contrattuali.

Il fornitore ha la decisione e la scelta delle soluzioni tecniche, organizzative e fisiche per messa in atto delle misure di sicurezza.
Una volta definiti i requisiti di sicurezza contrattuali, la responsabilità di attuare le politiche di sicurezza è a carico del fornitore che deve metterle in atto per soddisfare ai requisiti contrattuali. In questo caso il contratto si configura come un elemento in ingresso alla implementazione dei requisiti di sicurezza che daranno poi con il raggiungimento degli obiettivi il risultato atteso.
Un approccio diverso è quello di richiesta al fornitore della certificazione secondo la ISO/IEC 27001:2005 dove i requisiti di sicurezza, le misure organizzative, tecnologiche e fisiche sono

dettati dalla norma applicata e pertanto facente parte del Sistema di Gestione della Sicurezza delle Informazioni.

Possibili opportunità e difficoltà in ambito PA

La certificazione dei SGSI secondo la ISO/IEC 27001:2005 non è richiesta per partecipare a gare o come requisito contrattuale. Per questo la sua valenza per ora si estende alla sola Organizzazione che la vuole utilizzare senza ulteriori possibilità di sfruttamento per altri fini.
Naturalmente essendo un riferimento internazionale a livello ISO (International Standard Organization) la rende quanto mai attuale per eventuali prossimi utilizzi anche a scopi contrattuali.
La certificazione di un Sistema di gestione per la sicurezza delle informazioni è una opportunità per qualunque tipo di Organizzazione ed ovviamente anche per la PA.
E' un passo necessario per consentire alla Organizzazione di avere una visione sistemica della sicurezza delle informazioni, che viene riferita a degli standard riconosciuti a livello internazionale.
La certificazione è intesa anche come conoscenza della sicurezza interna della Organizzazione, valutazione e misura degli sforzi per attuare il SGSI, e come mezzo per il miglioramento dei processi di sicurezza.
I vantaggi possono essere elencati :

- Riferirsi ad uno standard riconosciuto;
- Rendere documentato tutto quanto viene eseguito per quanto riguarda la sicurezza delle informazioni;
- Coinvolgere il personale e le parti interessate allo sforzo comune per la sicurezza;
- Attuare e dimostrare in maniera evidente con registrazioni la conformità allo standard;
- Misurare le prestazioni del SGSI attraverso indicatori atti a dimostrare l' efficacia del SGSI a raggiungere gli obiettivi definiti dalla politica per la sicurezza.

Le difficoltà per l' implementazione della norma ISO/IEC 27001:2005 ha diversi aspetti tra i quali si evidenzia la carenza di personale competente nella materia di sicurezza delle informazioni, di gestione dei rischi, di misure tecnologiche.
Inoltre il percorso di implementazione del SGSI richiede una forte volontà politica ad alto livello, competenze, coinvolgimento del personale e sforzo implementativo di tutte le misure : logiche, fisiche ed organizzative.

Caratteristiche del progetto di adozione del SGSI

Le attività per l' implementazione di un SGSI sono indicate dalla norma ISO/IEC 27001:2005 (Cap. 4.2.1) e riassunte di seguito :

- Definizione dei confini del SGSI (ambito o perimetro);
- Definizione di una Politica per la sicurezza;
- Identificazione di un metodo di valutazione dei rischi;
- Definizione dei criteri di accettazione dei rischi;
- Identificazione del livello di rischio accettabile;

- Identificare i beni (assett) all' interno dell' ambito del SGSI;
- Identificazione delle minacce, vulnerabilità, impatti che la perdita di riservatezza, integrità e disponibilità possono avere sugli assett;
- Valutazione delle probabilità che si verifichino malfunzionamenti dovuti alle minacce ed alle vulnerabilità;
- Stimare il livello dei rischi;
- Determinare se il rischio è accettabile o richiede un trattamento;
- Identificare e valutare le opzioni per il trattamento del rischio;
- Ottenimento dell' approvazione da parte della direzione per i rischi residui;
- Approvazione da parte della direzione per attuare il SGSI;
- Preparazione di una Dichiarazione di Applicabilità.

Documentazione obbligatoria prevista

La documentazione prevista del SGSI prevede :

- Politica ed obiettivi per la sicurezza;
- Descrizione dei confini del SGSI (ambito o perimetro);
- Metodologia e Rapporto di valutazione dei rischi;
- Piano di trattamento dei rischi;
- Procedure documentate per : Gestione della Documentazione, Verifiche Ispettive Interne (Audit), Azioni Correttive, Azioni Preventive;
- Registrazioni del SGSI;
- Valutazioni sull' efficacia del SGSI;
- Dichiarazione di Applicabilità : l' elenco di tutte le contromisure adottate con inclusi i motivi di scelta ed eventuale esclusione dei n° 133 Controlli riportati nell' Allegato della norma;
- Altra documentazione dell' Organizzazione per la definizione di ruoli e responsabilità, pianificazione e gestione del SGSI.

L'adozione del Sistema di Gestione per la Sicurezza delle Informazioni a fronte della norma ISO/IEC 27001:2005 è relativa alla protezione di Beni Informativi dell'organizzazione ed assicura la continuità del Business.
L'esigenza di dotarsi di un Sistema di Gestione per la Sicurezza delle Informazioni è legata alla globalizzazione dei mercati, dell'evoluzione dei sistemi ITC e della tecnologia a supporto e, in particolare, alla necessità di assicurare:

- Credibilità, fiducia e confidenza da parte del committente nel garantire la riservatezza, l'integrità e la disponibilità delle sue informazioni

- Conformità alle leggi, ai regolamenti ed alle direttive
- Riduzione dei rischi economici dovuti a perdite di informazioni rilevanti per la continuità del business e per l'interesse degli stakeholders
- Dimostrazione e assicurazione dell'impegno assunto dalla direzione e da tutti i livelli dell'organizzazione.

Tempi, costi, sponsorship, impatto organizzativo, formazione e impatto sul personale

Il processo di certificazione ha come primo passo quello di scegliere l' Organismo di Certificazione che naturalmente deve essere tra quelli accreditati dal Sincert. La scelta può essere fatta in funzione delle referenze dell' Organismo intese come numero e tipologie di certificati emessi.
I tempi per lo sviluppo e implementazione di un SGSI dipende dalla natura e dalla complessità della Organizzazione, così come i relativi costi. Per un progetto di medie dimensioni si può ipotizzare un periodo di 12 mesi.
Per gli aspetti che riguardano l' ambito organizzativo, di formazione ed impatto sul personale, così come per altri sistemi di gestione, il lavoro e le attività sono molteplici.
E' necessario ricondurre le informazioni ai vari Processi aziendali che le utilizzano, ed individuare le modalità di gestione e gli asset coinvolti.
Pertanto nella fase iniziale è necessario utilizzare un modello di riferimento per processi allo scopo di :

- Identificare i Processi aziendali e dei sistemi informativi di supporto a tali processi, definendo la struttura dei vari flussi informativi;
- Classificare le Informazioni, in riferimento al valore che le stesse hanno all' interno della Organizzazione. La classificazione in termini di valore relativo determina il livello di criticità che l' Organizzazione attribuisce alle stesse.
- Identificazione e classificazione degli asset

Un "asset" è qualcosa che ha valore o utilità per l' Organizzazione, per il suo business, e per la continuità del servizio. Gli assets necessitano protezione per assicurare il corretto funzionamento delle attività di business e la continuità. Ogni asset all' interno del confine definito, dovrà essere identificato e opportunamente valutato dal responsabile secondo una Classificazione. (Esempio di classificazione) :

- **Dati/Informazioni** : data base o datafile, documentazione di sistema, manuale utente, materiale didattico, procedure operative, piano di continuità ;
- **Documenti cartacei** : contratti, linee guida,documentazione aziendale ;
- **Software asset** : software applicativo, software di sistema, tools di sviluppo, utilities ;
- **Hardware/Apparecchiature di comunicazione** : computer, mezzi di trasmissione dati, supporti fisici, apparati (alimentatori, aria condizionata) ;
- **Persone** : dipendenti, clienti,collaboratori, abbonati;

- Immagine aziendale e reputazione ;
- **Servizi** : servizi di comunicazione, energia, aria condizionata, ecc.

Personale (Ruoli e Responsabilità)

Individuare i Ruoli del personale dell' Organizzazione coinvolto nel SGSI a cui deputare specifici compiti, e le relative Responsabilità individuate nel SGSI. L' importanza di tale assegnazione si riflette nel garantire:

- che le attività previste dalla Norma di gestione della sicurezza siano sotto la responsabilità di persone qualificate ed idonee
- una divisione dei ruoli e delle responsabilità tra le diverse figure operanti nella gestione ed esecuzione e controllo dei processi del SGSI.

Formazione

Per gli aspetti di addestramento, consapevolezza e competenza occorre mettere in atto :

- la definizione delle competenze richieste per i ruoli relativi ai processi della sicurezza;
- la definizione di azioni di formazione ed addestramento per assicurare la necessaria competenza attraverso un Piano di addestramento;
- la misura dell' efficacia della formazione effettuata;
- la verifica dell' effettiva coerenza e finalizzazione dell'addestramento tecnico agli strumenti, ambienti, tecniche e metodologie utilizzate;

Processo di certificazione

Il processo di Audit per la certificazione di un SGSI è diviso in due fasi ciascuna della quale produce un rapporto di valutazione che consente il passaggio alla fase successiva.
Fase 1 (Audit sui Documenti)
Durante questa prima fase viene eseguita una valutazione sul sistema documentale dell' Organizzazione in conformità al Cap. 4.3.1 della Norma e anche del regolamento dell' Organismo di Certificazione, ed i relativi aspetti cogenti applicabili.
Il risultato della valutazione determina se sussistono le condizioni per proseguire il processo di certificazione. In caso di esito positivo viene stabilito il piano per le attività della Fase 2.
Fase 2 (Audit di certificazione)
In questa fase il gruppo di audit dell' Organismo di Certificazione valuta la conformità e l' efficacia del SGSI in campo, cioè nei processi. Vengono raccolte evidenze oggettive ed al termine dell' audit viene redatto un rapporto di valutazione che contiene l' esito della valutazione eseguita. Il rapporto di audit viene poi sottoposto al Comitato di Certificazione dell' Organismo, che è preposto alla decisione finale sulla certificazione.

I tempi ed i relativi costi per la conduzione di un audit di Certificazione dipendono da diversi fattori: numero di persone, numero delle sedi, complessità dei processi dell' Organizzazione. Esistono delle tabelle di giorni/persone a cui gli Organismi devono attenersi, e sono suscettibili di variazioni.
Pertanto è bene rivolgersi agli Organismi di Certificazione accreditati per avere Regolamenti, Tariffari e preventivi di spesa.

8. DOCUMENTAZIONE DISPONIBILE

Riportiamo di seguito la documentazione disponibile per l'approfondimento sulle tematiche relative allo standard ISO/IEC 27001.

ISO/IEC 27001					
Argomento / Titolo	**Autore**	**Editore**	**Anno**	**Pagamento**	**Lingua**
UNI CEI ISO/IEC 27001:2006	**ISO/IEC**	**UNI**	**2006**	**Euro 64**	**Italiana**

Elenco commentato documenti

Lo standard ISO/IEC 27001 è entrato in vigore e pubblicato in Italia in data 28/03/2006 come UNI CEI ISO/IEC 27001:2006 Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni – Requisiti.
La norma copre tutte le tipologie di Organizzazioni (imprese commerciali, agenzie governative, Organizzazioni senza scopo di lucro). Essa specifica i requisiti per impostare, mettere in opera, utilizzare, monitorare, rivedere, manutenere e migliorare un sistema documentato all'interno di un contesto di rischi legati alle attività centrali dell'Organizzazione. Dettaglia inoltre i requisiti per i controlli di sicurezza personalizzati in base alle necessità di una singola Organizzazione o di una sua parte.Il sistema è progettato per garantire la selezione di controlli di sicurezza adeguati e proporzionati.

Come e dove acquisire la documentazione

La pubblicazione ufficiali dello standard UNI CEI ISO/IEC 27001:2006 può essere reperita presso la UNI : Ente Nazionale Italiano di Unificazione .
Visita: www.uni.com

9. CERTIFICAZIONI ESISTENTI

Tipologie

Lo Standard ISO /IEC 27001: 2005 riguarda la certificazione di Sistemi di gestione per la Sicurezza delle Informazioni.
Nella Certificazione del Sistema i gestione per la sicurezza possono essere previsti :

- Tutti i processi dell' Organizzazione;
- Uno o più processi primari e relative interfacce;
- Un processo critico e relative interfacce;
- Uno o più processi primari e uno o più processi di supporto e relative interfacce.

Ad ottobre 2007 la diffusione mondiale della certificazione consta di 4047 certificati ISMS (fonte www.iso27001certificates.com vers. 175 october 2007). Di questi 2059 sono aggiornamenti o nuove certificazioni ISO/IEC 27001.
L'Italia si trova all'undicesima posizione per certificati rilasciati e riconosciuti dall'International Register of ISMS Certificates.

Certificazioni rilasciate suddivise per settore

Settore	Percentuale
Telecomunicazioni	**25**
Finanza	**21**
Servizi Terze Parti	**17**
Industria IT	**15**
Manifatture	**11**
Organizzazioni Governative	**7**
Utilities	**4**

Diffusione in Italia

Situazione certificati ISO/IEC 27001 rilasciati da Organismi Italiani accreditati SINCERT

Organismo di Certificazione	*Certificati ISO/IEC 27001:2005 rilasciati in ITALIA*	*Certificati ISO/IEC 27001:2005 rilasciati all'Estero*
TUV	**74**	
DNV	**58**	**2**
RINA	**27**	**2**
IMQ	**27**	
CERTIQUALITY	**12**	
LLOYD's	**4**	**6**
CERMET	**4**	
totali	**206**	**10**

Fonte SINCERT data : 30/9/2007

Organismi di Certificazione ed enti di Accreditamento (Italia ed Europa)

La certificazione di un SGSI è un passo importante che viene eseguito da un Organismo di certificazione. Tali Organismi di certificazione possono essere accreditati o non accreditati.
L' accreditamento viene eseguito dagli Organismi di accreditamento presenti in ogni paese.
Come detto prima non tutti gli Organismi di certificazione che operano sul mercato sono accreditati, questo vuol dire che non sono soggetti a loro volta da un organo di controllo corrispondente a quello che avviene sulle Organizzazioni certificate.
Infatti l' Organismo di accreditamento esegue degli Audit sugli Organismi di Certificazione accreditati attraverso uno standard di riferimento.
Se ne deduce che un Organismo di Certificazione accreditato assicura una garanzia maggiore nella emissione di un certificato secondo la ISO /IEC 27001:2005.
In Italia come Organismo di accreditamento esiste il SINCERT costituito dal 1991 come associazione senza scopo di lucro, riconosciuta legalmente dallo Stato Italiano con Decreto Ministeriale del 16 Giugno 1995.

La compagine associativa di SINCERT comprende attualmente 47 Associati, fra cui rientrano i principali Soggetti istituzionali, scientifici e tecnici, economici e sociali aventi interesse diretto e indiretto nelle attività di accreditamento e certificazione, quali: le Pubbliche Amministrazioni e i maggiori Enti Pubblici Tecnici e di Ricerca, le Associazioni dei Consumatori, le Associazioni di categoria della industria, commercio e agricoltura, le Camere di Commercio, i grandi Fornitori di servizi di pubblica utilità (energia e trasporti), le Associazioni rappresentative degli Organismi di Certificazione e Ispezione e delle Società e Professionisti della consulenza, nonché numerosi altri Soggetti facenti riferimento alle attività di accreditamento.

L'Associazione ha come finalità l'accreditamento di:

- Organismi di Certificazione di sistemi di gestione aziendale, quali sistemi di gestione per la qualità, sistemi di gestione ambientale, sistemi di gestione per la sicurezza e salute sul lavoro, sistemi di gestione per la sicurezza delle informazioni, sistemi di gestione per la sicurezza alimentare;
- Organismi di Certificazione di prodotti/servizi;
- Organismi di Certificazione di personale;
- Organismi di Ispezione..

A tal fine, valuta ed accredita suddetti Operatori, accertandone la conformità ai requisiti istituzionali, organizzativi, tecnici e morali stabiliti dalle Norme Tecniche consensuali e da altre Prescrizioni applicabili, in termini tali da ingenerare, in tutte le parti sociali ed economiche interessate e, in particolare, nel mercato degli utenti e consumatori, un elevato grado di fiducia nel loro operato e nei corrispondenti risultati. SINCERT opera tradizionalmente nel settore dell'accreditamento volontario, ma un numero crescente di Pubbliche Amministrazioni ed Organi Tecnici dello Stato, competenti per gli accreditamenti nel settore cogente e regolamentato, fanno esplicito riferimento all'accreditamento SINCERT, sia come fattore di garanzia nell'ambito di procedimenti regolamentati per legge, sia come utile elemento di valutazione ai fini del rilascio di autorizzazioni, riconoscimenti e notifiche di loro spettanza.

Organismi di Certificazione e Ispezione accreditati in Italia

In data agosto 2007, operano sotto accreditamento SINCERT ben **118 Organismi di Certificazione e Ispezione**, per complessivi **217 accreditamenti rilasciati**,.

Gli schemi di Certificazione attualmente accreditati sono 7 (Fonte SINCERT data : 31/8/2007)

In Europa è presente dal 2000 l' EA nata dalla fusione di EAC (European Accreditation of Certification) e EAL (European co-operation for Accreditation of Laboratories) ed è una entità legale con sede in Olanda.
Possono diventare membri associati tutti gli Organismi di Accreditamento riconosciuti a livello nazionale di stati Europei che possono dimostrare di operare in conformità alle normative per l' accreditamento dei laboratori e per l'accreditamento degli organismi di certificazione.

A livello mondiale è presente l' IAF (International Accreditation Forum) che costituisce l' associazione mondiale degli Organismi di Accreditamento di Organismi di Certificazione.

Possibili utilizzi delle certificazioni
Fornire alle Amministrazioni e alle commissioni di gara un elemento aggiuntivo di valutazione e di riferimento nella identificazione che le imprese hanno messo in atto un sistema conforme ed efficace per garantire i requisiti fondamentali : Riservatezza, Integrità e Disponibilità delle informazioni che sono comprese nell' ambito di riferimento (perimetro) del Sistema di gestione della sicurezza.

10. FORMAZIONE DISPONIBILE

In Italia sono disponibili parecchi momenti formativi relativi alla Sicurezza delle Informazioni. Vengono offerti tra l'altro corsi introduttivi sulle norme ISO/IEC 27001 e ISO/IEC 27002, sull'implementazione di un Sistema di Gestione per la Sicurezza delle Informazioni e di qualificazione Auditor/Lead Auditor ISO/IEC 27001.
Le Organizzazioni che effettuano la formazione specialmente sulle prime due tipologie normalmente sono società che in qualche modo hanno legami con la consulenza sui Sistemi di Gestione secondo la norma ISO/IEC 27001. Per avere una visione aggiornata basta effettuare una ricerca con un buon motore su Internet.
Sulla tipologia dei corsi di qualificazione per Auditor/Lead Auditor ISO/IEC 27001 bisogna fare invece una precisazione: è conveniente, nel caso si voglia intraprendere un corretto percorso per intraprendere questa attività, rivolgersi alle Organizzazioni che offrono formazione riconosciuta da uno degli enti di certificazione del personale.
Ricordiamo che in Italia gli enti di certificazione del personale che hanno attivi i registri per Audtor/Lead Auditor ISO/IEC 27001 e riconosciuti dal SINCERT sono AICQ-SICEV, CEPAS e KHC.
Queste Organizzazioni, nel rispettivo sito, elencano le Organizzazioni di formazione riconosciute e che rilasciano titoli di qualificazione validi per l'iscrizione al rispettivo registro.
Si riportano di seguito le principali Organizzazioni di formazione riconosciute che offrono formazione su ISO/IEC 27001:

- AICQ formazione — Via Cornalia, 19 - 20124 Milano
- RINA training factory — Via Corsica, 9/7 E - 16128 Genova
- DNV Italia Training (Mi) — Viale Colleoni, 9 - 20041 Agrate Brianza
- Bureau Veritas Italia — Viale Monza, 261 – 20126 Milano

Esistono poi altri enti di certificazione del personale con registri per Auditor/Lead Auditor ISO/IEC 27001 attivi in Italia che sono il RICEC con sede nella Repubblica di San Marino (riconosciuto dal SAS) e l'I.R.C.A. di Londra.
Le principali Organizzazioni di formazione riconosciute da questi ultimi sono:

- BSI Management System — Corso Milano 21, 20052 Monza (MI)
- STR srl — Via Tre Settembre, 99 47891 Dogana (RSM)

Sarà comunque utile prima di effettuare una scelta sull'Organizzazione di formazione controllare sui siti dei vari enti di certificazione del personale menzionati quali siano i corsi riconosciuti e le Organizzazioni che li erogano.

Sul panorama esistono anche i Master e i Corsi di Alta Formazione organizzati da Università o Enti collegati che offrono una formazione molto più ampia ed impegnativa in termini di tempo.

I più conosciuti sono:

- Information Security Management organizzato da CEFRIEL e MIP Politecnico Milano
- Gestione della sicurezza informatica nell'impresa e nella Pubblica Amministrazione organizzato dal Dipartimento di Informatica dell'Università degli Studi di Roma "La Sapienza".

11. ESTRATTO DEL GLOSSARIO

Le definizioni riportate sono state estratte dalla ISO/IEC 27001 e ISO/IEC 27002.

ACCETTAZIONE DEI RISCHI : Decisione di accettare i rischi

ANALISI DEL RISCHIO : Attività volta ad identificare minacce e vulnerabilità di un sistema allo scopo di definire gli obiettivi di sicurezza e di permettere la gestione del rischio.

ASSET : Qualsiasi cosa di valore per l 'Organizzazione

ATTACCO : Azione od evento che può pregiudicare la sicurezza di un sistema

AUDIT : Processo sistematico indipendente e documentato per ottenere evidenze della verifica ispettiva e valutarle con obiettività, al fine di stabilire in quale misura i criteri di verifica ispettiva sono stati soddisfatti

BEST PRACTICE : Migliore approccio possibile per affrontare una determinata situazione; è basato sull' osservazione su quanto fatto dalle Organizzazioni leader in circostanze analoghe

COMUNICAZIONE DEL RISCHIO : Scambio o condivisione di informazioni riguardo il rischio tra la Direzione e le parti interessate.

CONSEGUENZE : Risultato di un evento

CONTINUITA' OPERATIVA : Insieme DI attività volte a minimizzare gli effetti distruttivi di un evento che ha colpito una Organizzazione o parte di essa con l'obiettivo di garantire la continuità delle attività in generale. Include il Disaster Recovery.

CONTROLLO ACCESSI : Funzione di sicurezza volta a controllare che un utente possa espletare le sole operazioni di loro competenza.

CONTROMISURE : Strumento di natura tecnologica, organizzativa o fisica, atto a contrastare un attacco nei confronti di un sistema.

CONTROLLO DEI RISCHI : Azioni implementate dalle decisioni della gestione dei rischi

DANNO : Effetto che può essere prodotto da una minaccia.

DICHIARAZIONE DI APPLICABILITA' : Dichiarazione documentata che descrive gli obiettivi di controllo e i controlli rilevanti ed applicabili al SGSI della Organizzazione.

DISPONIBILITA' : Assicurazione che gli utenti autorizzati abbiano accesso alle informazioni e agli assets quando ne fanno richiesta.

DISASTER RECOVERY : Insieme di attività volte a ripristinare lo stato del sistema informatico o parte di esso, compresi gli aspetti fisici e organizzativi e le persone necessarie per il suo funzionamento, con l' obiettivo di riportarlo alle condizioni antecedenti ad un evento disastroso.

EVENTO DI SICUREZZA DELLE INFORMAZIONI : Identificata occorrenza dello stato di un sistema, servizio o rete indicante una possibile vulnerabilità della politica di sicurezza delle informazioni, un' avaria delle contromisure o una situazione non osservata in precedenza ma rilevante per la sicurezza.

EVITARE I RISCHI : Decisione di non coinvolgimento, o azione di ritiro da una situazione di rischio

GARANZIA : Fiducia nella capacità di un sistema di protezione di soddisfare i requisiti di sicurezza.

GESTIONE DEGLI INCIDENTI : Insieme delle attività, dei processi e procedure, dell' Organizzazione e delle misure di sicurezza volti al rilevamento, alla risposta e alla risoluzione degli incidenti di sicurezza.

GESTIONE DEI RISCHI : Attività coordinate per dirigere e controllare una Organizzazione per quanto riguarda i rischi.

IDENTIFICAZIONE : Atto per cui un soggetto dichiara di essere se stesso; è il primo passo per l' autenticazione.

IDENTIFICAZIONE DEI RISCHI: Processo per trovare, elencare e caratterizzare elementi di rischio

IDENTIFICAZIONE DELLE SORGENTI: Processo per trovare, elencare e caratterizzare sorgenti di rischio

INCIDENTE DI SICUREZZA DELLE INFORMAZIONI : Evento o serie di eventi di sicurezza delle informazioni non voluti o inattesi che hanno una probabilità significativa di compromettere operazioni di business e di minacciare la sicurezza delle informazioni.

INTEGRITA': Assicurazione circa l' accuratezza e la completezza delle informazioni e i metodi di processo.

LIVELLO DI SERVIZIO : Indicatore che traduce le attese qualitative in obiettivi quantitativi misurabili sulla base dei quali è possibile verificare il rispetto delle clausole contrattuali ed in particolare dei livelli di qualità pattuiti.

LOG : File o altro documento elettronico che registra informazioni dettagliate sugli eventi di un sistema, di solito nella stessa sequenza in cui si verificano.

MECCANISMI DI SICUREZZA : Strumenti, apparati, software, algoritmi, procedure organizzative e operative che realizzano le funzioni di sicurezza.

MINACCIA : Una potenziale causa o un incidente che può causare danni ad un sistema o alla Organizzazione.

MISURAZIONE DEI RISCHI : Processo di comparazione tra il rischio stimato su i criteri definiti dei rischi per determinare l' importanza del rischio

MITIGAZIONE : Limitazione di alcune conseguenze negative di un particolare evento

OBIETTVI DI SICUREZZA : Esigenza di protezione da determinati attacchi contro i dati e le risorse del sistema informativo.

OTTIMIZZAZIONE DEI RISCHI : Processo, relativo al rischio per minimizzare le conseguenze negative e massimizzare le conseguenze positive e le loro rispettive probabilità

PAROLA CHIAVE : Password.

PASSWORD : Stringa di caratteri, generalmente cifrata dall' elaboratore, che autentica un utente ad un sistema.

PDCA (Plan-Do-Check-Act) : Modello dei sistemi di gestione articolato attraverso le fasi della definizione, realizzazione, esercizio, monitoraggio, revisione, manutenzione e miglioramento continuo dei processi.

PIANO DELLA SICUREZZA : Documento per la pinificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell' ambito, in genere di una Organizzazione.

POLITICA : Intenzione totale e strategie formalmente espresse dalla Direzione.

POLITICHE DELLA SICUREZZA : Costituiscono l' insieme dei principi, norme, regole, consuetudini che regolano la gestione delle informazioni di una Organizzazione in termni di protezione e distribuzione. Si possono classificare in politiche di alto livello e funzionali.

PRIVACY : Tratta la riservatezza in merito alle informazioni riguardanti la persona. In Italia il concetto di Privacy è correlato al Decreto Legislativo 30 giugno 2003. n. 196 "Codice in materia di protezione di dati personali".

PROBABILITA': dimensione che un evento possa accadere.

REQUISITI DI SICUREZZA : Esprimono ciò che si intende per sicurezza : riservatezza, integrità e disponibilità.

RIDUZIONE DEI RISCHI : Azioni prese per diminuire le probabilità negative e le conseguenze o entrambe associate al rischio

RIPRISTINO : Attività che consiste nel riportare un sistema al suo stato precedente a un errore. Nel caso di perdita di dati, permette di rigenerarli come erano prima dell' evento, in genere partendo da un back up.

RISCHIO : Combinazione della probabilità di un evento e le sue conseguenze.

RISCHI RESIDUI : Rischio rimanente dopo il trattamento

RISERVATEZZA (CONFIDENZIALITA') : Assicurazione che le informazioni siano accessibili solo da utenti autorizzati.

RUOLI E RESPONSABILITA' : Definisce la categoria delle funzioni organizzative all' interno di un' Organizzazione er la sicurezza che hanno lo scopo di specificare le figure operative che pianificano e gestiscono il sistema di protezione evidenziando le responsabilità e le attività di loro competenza.

SGSI (SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI) : La parte del sistema di gestione, basata su un approccio dei rischi, per stabilire, implementare, monitorare, riesaminare, mantenere e migliorare il sistema di sicurezza delle informazioni.

STATMENT OF APPLICABILITY : Dichiarazione documentata che descrive gli obiettivi di controllo e i controlli rilevanti ed applicabili al SGSI della Organizzazione.

STIMA DEI RISCHI: Processo usato per assegnare valori alle probabilità e conseguenze

TRASFERIMENTO DEI RISCHI : Condividere con altre parti il valore della perdita o benefici di guadagni, per un rischio

TRATTAMENTO DEI RISCHI : Processo di selezione ed implementazione di misure per modificare il rischio

VALUTAZIONE DEI RISCHI : Processo di analisi dei rischi e misurazione dei rischi

VULNERABILITA' : Una debolezza di un asset o gruppo di asset che può determinare una o più minacce.

12. ASSOCIAZIONI DI RIFERIMENTO

Gli utilizzatori della ISO 27001 (e delle linee guida collegate) sono riuniti all'interno di un Gruppo Utenti Internazionali (IUG) con sede a Londra, gestito dal "padre" della norma Ted Humphreys. Ogni nazione può esprimere un Capitolo locale coordinato da un chair di riferimento. L'Organizzazione dei Capitoli può essere diversa di nazione in nazione ma le finalità sono comuni.
I Capitoli si incontrano una volta l'anno in occasione dell'International Meeting che si svolge a Londra nel mese di dicembre.
Ciascun Capitolo ha come obiettivo principale sostenere la diffusione e l'utilizzazione della ISO 27001 supportando e/o organizzando eventi in materia di sicurezza delle informazioni.

Il Capitolo italiano, attivo dal settembre 2005, provvede a tale scopo mediante il proprio sito **www.ismsiugitaly.net** e le proprie iniziative, spesso in collaborazione con altre associazioni.
In Italia nel campo della Sicurezza delle Informazioni esistono molte entità che si interessano dell'argomento.
Di seguito si riporta un elenco che, anche se non esaustivo, comunque evidenzia le associazioni più riconosciute ed in qualche modo più attive:

- **Clusit** Via Complico, 39 – 20135 Milano
- **AICQ** Comitato "Qualità del Software e Servizi IT" Via Macchi, 42 - 20124 Milano
- **AIEA** capitolo ISACA Via Valla, 16 20141 MILANO
- **AIPSI** Associazione Italiana Professionisti Sicurezza Informatica capitolo di ISSA
- **ANSSAIF** Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Finanziaria
- **ISACA** Roma capitolo ISACA

13. INDICAZIONI BIBLIOGRAFICHE

Testi

ISO/IEC 27002:2005
Information Tecnology – Code of practice for information security management

ISO/IEC 27001:2005
Information Security management systems – Specification with guidance for use

ISO/IEC 27006:2005
Requirements for the accreditation of bodies operating certification of ISMS

ISO Guide 73:2002
Risk management – Vocabulary – Guidelines for use in standards

Elio Molteni – Francesco Faenzi

La Sicurezza dei SISTEMI INFORMATIVI
Teoria e pratica a confronto
Ed. Mondadori Informatica

Cesare Gallotti
SICUREZZA DELLE INFORMAZIONI
Analisi e Gestione del Rischio
Franco Angeli Editore

Ioanis Tsiouras
LA SICUREZZA DELL'INFORMAZIONE
Dal sistema di gestione alla sicurezza dei Sistemi Informatici
Le norme BS 7799-2 e ISO/IEC 15408 (Common Criteria)
Franco Angeli Editore

G.Cantù – A. Rampazzo – L. Polo
Quaderno n° 20 - Comitato per la Qualità del Software e dei Servizi IT
Gestione della Sicurezza delle Informazioni: guida alla lettura della norma ISO 27001
AICQ Centro Nord – AICQ Triveneta

F. Cirilli
Implementazione e certificazione dei sistemi di gestione per la sicurezza delle informazioni
Quaderni Clusit

Vito Trinetta
Sicurezza informatica in azienda
Strategie di prevenzione e tecniche di controllo
IPSOA

Bruce Schneider
SICUREZZA DIGITALE
Le decisioni giuste per la sicurezza aziendale
Tecniche nuove

Kevin Day
SECURITY JUNGLE
Le decisioni giuste per la sicurezza aziendale
Mondadori Informatica

Gruppo di Sviluppo M5
EUCIP IT Administrator – Modulo 5
Sicurezza Informatica
Mc Graw Hill Ed.

Alessandro Sinibaldi
Risk Management
Hoepli Informatica

Riviste

Qualità : Associazione Italiana Cultura Qualità – Federazione Nazionale
Via Cornalia 19
Milano

CSO La Guida per i responsabili della Sicurezza - Network Italia
Via Zante 16/2
20136 Milano

ICT Security – Nuovo Studio Tecna
Viale Adriatico 147
00141 Roma

ICT Professional La rivista dei Professionisti dei Sistemi Informativi delle Telecomunicazioni e dell' Organizzazione
Soiel International srl
Via Martiri Oscuri 3
2015 Milano.

Siti Internet

www.aicq.it
www.aicqsw.it
www.aicqci.it
www.aicqtv.it
www.clusit.it
www.uni.com
www.iso.org
www.sincert.it