Rubrica

Nuovo Impulso per la Sicurezza delle Informazioni con la Revisione delle Norme

A. Piva - A. Rampazzo

Le informazioni sono cruciali per il funzionamento e talvolta persino per la sopravvivenza di un'organizzazione, pertanto la loro gestione e tutela sono aspetti cruciali soprattutto quando si tratta di dati critici in termini di proprietà industriale e di tutela degli stakeholders.

E' necessario proteggere le informazioni, attraverso un opportuno Sistema di Gestione per la Sicurezza delle Informazioni, da accessi non autorizzati e dal rischio che esse vengano corrotte o rese non disponibili, cosa che avrebbe un impatto negativo su diversi aspetti del business.

Introduzione

Il valore delle informazioni gestite da un'organizzazione richiede un continuo impegno per misurare, controllare e migliorare la sicurezza dei servizi offerti, garantendo il rispetto delle norme e delle direttive per la tutela della riservatezza, integrità e disponibilità delle informazioni stesse. Per garantire la protezione del patrimonio informativo aziendale ogni organizzazione dovrebbe aver definito un proprio Sistema di Gestione per la Sicurezza delle Informazioni (SGSI)[1], modellato sulla base di uno standard. In questo contesto l'elemento centrale è costituito dalla "Gestione del Rischio", che permette di analizzare i rischi tramite la loro identificazione, stima e misurazione, di individuare le vulnerabilità che potrebbero compromettere la riservatezza, l'integrità e la disponibilità delle informazioni, di definire le contromisure per contrastare le minacce ed infine di pianificare gli interventi da attuare per la riduzione dei rischi stessi. Un'attenzione particolare è posta nell'adozione di misure organizzative

---

[1] Vedi articolo "La sicurezza delle informazioni e le Norme ISO 27000" pubblicato su "Mondo Digitale" nr. 3 di settembre 2008

che rendano efficaci gli interventi tecnici, nella strutturazione dei processi di lavoro, nell'individuazione di soluzioni tecnologiche innovative, nella formazione e nella sensibilizzazione del personale in merito ai problemi della sicurezza. L'attuazione del Sistema di Gestione per la Sicurezza delle Informazioni porta alla definizione di ruoli, di responsabilità e di regole specifiche della sicurezza, di attività di pianificazione e realizzazione di politiche e procedure, nonché alla verifica dei processi attuati secondo quanto previsto dal modello indicato dallo standard.

Cosa sono i sistemi di gestione della sicurezza delle informazioni

Il Sistema di Gestione della Sicurezza delle informazioni (Information Security Management System - ISMS) è regolato dalle norme della famiglia ISO 27000 e nasce allo scopo di custodire e proteggere l'insieme di informazioni di una organizzazione.

Il Sistema di Gestione della Sicurezza dell'informazione è dunque fondamentale per proteggere i dati ed evitare possibili violazioni e divulgazioni di notizie private. Un'organizzazione dovrebbe dunque tenere in particolare considerazione la sicurezza del proprio protocollo comunicativo attraverso sistemi di gestione della sicurezza delle informazioni validi, efficaci ed efficienti sia nel confronto dell'interno che dall'esterno.

Pertanto ISMS sono necessari per monitorare il flusso delle informazioni, per proteggerle e controllarle in qualunque momento anche dal punto di vista degli accessi alla rete. Essi possono quindi essere fondamentali anche per migliorare e accrescere l'efficienza della propria azienda.

Sistemi di gestione della sicurezza delle informazioni: le norme ISO/IEC 27001 e ISO/IEC 27002

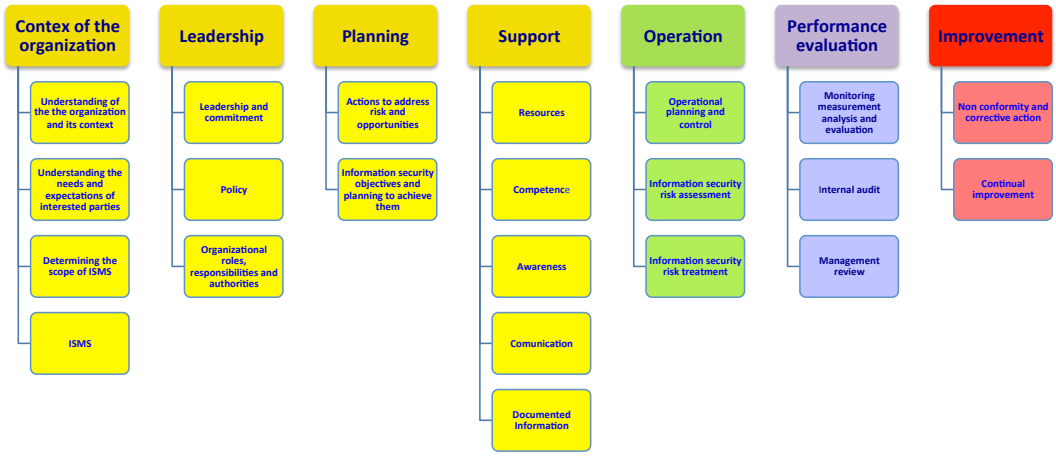
La norma ISO/IEC 27001 è adatta a diverse tipologie di aziende ed organizzazioni ed è una certificazione importante soprattutto quando l'azienda divulga o utilizza un ampio numero di informazioni anche con soggetti terzi.

La nuova ISO/IEC 27001 rivista e pubblicata nella sua seconda versione il 1 ottobre 2013, segue le nuove direttive definite dalla ISO e descritte nel MSS HLS (Management system standards - High level structure). Il primato in questo senso va alla ISO 22301:2012, essendo stata la prima norma pubblicata con la nuova strutturazione dei contenuti.

L'obiettivo di questo modello uniforme è sostanzialmente l'allineamento di tutte le norme dei sistemi di gestione ad una medesima organizzazione dei contenuti, avviando così il progetto di integrabilità concettuale degli schemi. L'integrabilità di fatto, sempre possibile in linea teorica, deve essere oggetto di valutazione da parte delle singole organizzazioni interessate, anche per individuare le migliori modalità applicabili.

Sinteticamente i contenuti della nuova ISO/IEC 27001, espandendone i punti principali dell'indice (si veda figura 1 struttura della norma), si possono riassumere:

- Il contesto dell'organizzazione - Capire l'organizzazione ed il suo contesto - Comprendere le necessità e le aspettative delle parti interessate - Determinare il campo di applicazione del sistema di gestione per la sicurezza delle informazioni - Sistema di gestione per la sicurezza delle informazioni
- Guida e direzione (Leadership) - Guida, direzione e impegno - Politica - Ruoli, responsabilità e poteri dell'organizzazione
- Pianificazione - Azioni per fronteggiare rischi e opportunità - Valutazione del rischio relativo alla sicurezza delle informazioni - Trattamento del rischio relativo alla sicurezza delle informazioni — Obiettivi per la sicurezza delle informazioni e piani per conseguirli
- Supporto - Risorse - Competenze - Consapevolezza - Comunicazione - Informazioni documentate - Creazione e aggiornamento - Controllo delle informazioni documentate
- Operatività - Pianificazione e controllo operativo - Valutazione del rischio relativo alla sicurezza delle informazioni - Trattamento del rischio relativo alla sicurezza delle informazioni
- Valutazione delle prestazioni - Monitoraggio, misurazione, analisi e valutazione - Audit interni - Riesame della Direzione
- Miglioramento - Non conformità e azioni correttive - Miglioramento continuo
- Annex A - Riferimenti alla ISO/IEC 27002



Struttura della norma ISO/IEC 27001:2013

Si può quindi notare una nuova organizzazione delle tematiche con alcune novità. A titolo di esempio: si parla di informazioni documentate e non più di procedure documentate e registrazioni; le azioni preventive sono state eliminate, perché incluse nelle "azioni per fronteggiare rischi e opportunità"; la valutazione e il trattamento del rischio sono presenti sia nella pianificazione del Sistema sia nella sua operatività.

Non è sicuro che l'eliminazione del concetto di azione preventiva possa essere del tutto un beneficio, ma l'attuazione efficace del sistema di gestione è di per sé l'origine della prevenzione di qualsiasi possibile fattore di instabilità organizzativa.

Va evidenziato il forte richiamo alla comprensione del "contesto" nel quale opera l'organizzazione ed alle aspettative delle parti interessate, che dello stesso sistema possono essere le promotrici.

Con la precedente edizione della norma questo aspetto era poco sviluppato, concentrando da subito l'attenzione in modo troppo immediato sui beni e sulle pratiche di gestione della sicurezza. Oggi l'esigenza di definire le finalità, le opportunità ed i rischi relativi al sistema di gestione nel suo complesso, sia strategico aziendale che tecnico, risulta ben chiara, e permetterà di focalizzare con maggiore efficacia ed efficienza lo sviluppo dei controlli di sicurezza non solo da un punto di vista tecnico, ma anche e soprattutto da un punto di vista organizzativo e gestionale.

Vi è un nuovo approccio anche alla gestione del rischio: uno dei cambiamenti più importanti della norma è quello di definire un nuovo approccio per l'applicazione di valutazione del rischio, sia nella fase di "pianificazione" che nella fase di “attuazione”. I requisiti di valutazione del rischio sono generici e sono allineati alla norma ISO 31000:2009[2]. La gestione del rischio è un obiettivo a cui ogni impresa attenta agli aspetti preventivi dovrebbe tendere e che ogni cliente dovrebbe pretendere, in particolare in settori caratterizzati da alta vulnerabilità. La Linea Guida ISO 31000:2009 ci propone un modello di gestione del rischio e di integrazione dello stesso nel sistema di gestione aziendale. Essa è applicabile a tutte le tipologie di rischio (da quelli strategici a quelli operativi, valutari, di mercato, di compliance, di paese, ecc.).

Pertanto, non è più necessario individuare le attività, le minacce e le vulnerabilità al fine di individuare i rischi. Se la metodologia di valutazione del rischio utilizzata per l'organizzazione utilizza questo metodo e funziona, è possibile mantenerla e non c'è bisogno di cambiarla. Tuttavia, se si vuole, ci sono metodi alternativi che possono essere perfettamente validi da usare, che non utilizzano asset, minacce e/o vulnerabilità per identificare i rischi.

E’ stata introdotta anche una nuova funzione nel processo di valutazione del rischio, che è il proprietario del rischio (o risk owner).

Complessivamente (si veda figura 2 confronto requisiti), l'edizione 2005 della ISO/IEC 27001 aveva 102 requisiti obbligatori contenuti nelle clausole da 4 a 8

---

[2] Nel novembre del 2010 è stata pubblicata la norma UNI ISO 31000:2010 “Gestione del rischio”, traduzione italiana della corrispondente norma internazionale ISO 31000 del novembre 2009.

mentre ora nella versione 2013 sono stati aggiunti 28 requisiti, portando ad un totale di 130 requsiti presenti nelle nuove clausole da 4 a 10.

ISO/IEC 27001:2013			
§ requisito		Descrizione	Controlli
Mandatory	4	Contesto dell'organizzazione	8
	5	Leadership	19
	6	Pianificazione	39
	7	Supporto	28
	8	Operatività	9
	9	Valutazione delle prestazioni	29
	10	Miglioramento	26
		Controlli	**148**
ISO/IEC 27001:2005			
§ requisito		Descrizione	
Mandatory	4	Sistema di Gestione per la Sicurezza delle Informazioni	50
	5	Responsabilità della direzione	18
	6	Audit interni del SGSI	4
	7	Riesame del SGSI da parte della direzione	16
	8	Miglioramento del SGSI	14
		Controlli	**102**

Confronto requisiti ISO/IEC 27001

Sono state revisionate anche le norme ISO/IEC 27000 e la ISO/IEC 27002.

Tutte le definizioni presenti nella versione precedente della norma ISO/IEC 27001 sono state eliminate , e quelle che sono ancora rilevanti, sono state trasferite alla norma ISO/IEC 27000 pubblicata nel mese di gennaio 2014 e scaricabile gratuitamente per uso personale all'indirizzo: http://standards.iso.org/ittf/licence.html

Questo trasferimento ad una unica norma garantisce la coerenza dei termini e delle definizioni a tutti gli standard della famiglia ISO/IEC 27000.

La revisione della ISO/IEC 27002 ha previsto una nuova struttura dell'Annex A (si veda figura 3 - confronto Annex A): i controlli dell'annex A diminuiscono rispetto alla versione del 2005, passando da 133 a un totale di 114, vale a dire 19 controlli vengono rimossi in questo allegato. Tuttavia, nonostante questa diminuzione, il nuovo annex A che era composto nella versione 2005 da 11 domini, da A.5 a A.15, nella nuova versione 2013 è composto da 14 domini da A.5 a A.18.

Nella nuova versione sono stati separati due domini e creato uno nuovo su "Provider Relations" in risposta alla popolarità del "Cloud Computing" e gli sforzi per proteggere le catene di approvvigionamento.

Questo miglioramento della struttura dell'annex A, ha un impatto sulla chiarezza e l'allineamento con le politiche, i processi e le procedure aziendali esistenti.

Annex A ISO/IEC 27001:2013				
Area controllo		Descrizione	Obiettivi	Controlli
Discrezionale	A5	Politica per la sicurezza	1	2
	A6	Organizzazione della sicurezza delle informazioni	2	7
	A7	Sicurezza delle risorse umane	3	6
	A8	Gestione dei beni	3	10
	A9	Controllo degli accessi	4	14
	A10	Crittografia	1	2
	A11	Sicurezza fisica ed ambientale	2	15
	A12	Sicurezza delle operazioni	7	14
	A13	Sicurezza delle comunicazioni	2	7
	A14	Acquisizione, sviluppo e manutenzione dei sistemi	3	13
	A15	Rapporti con i fornitori	2	5
	A16	Gestione degli incidenti relativi alla sicurezza delle informazioni	1	7
	A17	Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa	2	4
	A18	Conformità	2	8
		Controlli	**35**	**114**

Annex A ISO/IEC 27001:2005				
Area controllo		Descrizione	Obiettivi	Controlli
Discrezionale	A5	Politica per la sicurezza	1	2
	A6	Organizzazione della sicurezza delle informazioni	2	11
	A7	Gestione dei beni	2	5
	A8	Sicurezza delle risorse umane	3	9
	A9	Sicurezza fisica ed ambientale	2	13
	A10	Gestione delle comunicazioni e dell'operatività	10	32
	A11	Controllo degli accessi	7	25
	A12	Acquisizione , sviluppo e manutenzione dei sistemi informativi	6	16
	A13	Gestione degli incidenti relativi alla sicurezza delle informazioni	2	5
	A14	Gestione della continuità operativa	1	5
	A15	Conformità	3	10
		Controlli	**39**	**133**

Confronto Annex A ISO/IEC 27001

Oltre ad avere cambiato il numero di controlli, un altro cambiamento importante di cui all'annex A ha a che fare con l'applicazione: nella nuova versione della norma ISO 27001 non è più necessario "selezionare" i controlli invece, le organizzazioni devono "stabilire" quali sono i controlli necessari, come parte del trattamento dei rischi, e di confrontare i controlli con l'annex A, al fine di garantire che non venga dimenticato alcun controllo importante.

Nel complesso, gli attuali Sistemi di Gestione della Sicurezza delle Informazioni non dovranno essere completamente reingegnerizzati per soddisfare i nuovi requisiti, anche se saranno, da un lato necessarie, e dall'altro lato possibili, delle modifiche significative a quanto attualmente implementato dalle diverse organizzazioni.

Comunque da questa revisione ne consegue la necessità di rimodulare le attuali Dichiarazioni di Applicabilità (SoA) che verrà comunque facilitata dalla presenza di un'apposita tabella di correlazione scaricabile all'indirizzo: http://www.jtc1sc27.din.de/sbe/wg1sd3

Impatto sulle organizzazioni già certificate

Tutti questi cambiamenti avranno un impatto su migliaia di aziende già certificate: dalla pubblicazione della norma ISO/IEC 27001:2013 tutte le organizzazioni avranno un periodo di tempo di due anni per provvedere all'adeguamento del Sistema di Gestione. L'adeguamento può essere fatta su qualsiasi revisione di audit annuale programmata, o da una verifica speciale concordata con l'Organismo di Certificazione.

Dalla prima pubblicazione della norma ISO/IEC 27001 nel 2005, il numero di aziende certificate è passato da 5.800 a circa 20.000 a fine del 2012 (survey ISO 2012). Tra i paesi con le aziende certificate in questo standard sono inclusi Giappone, Romania, Cina, Inghilterra, India e Italia. L'Italia ha circa 500 aziende certificate.

Certamente la revisione di queste norme porterà un nuovo impulso alle organizzazioni nella gestione della sicurezza delle informazioni un tema di vera attenzione in un continuo scenario nel quale le informazioni sono diventate la moneta del nuovo millennio.

Bibliografia

- ISO/IEC 27000:2014 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
- ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements
- ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls

Biografie

Antonio Piva,Laureato in Scienze dell'Informazione, Vice Presidente dell'ALSI (Associazione Nazionale Laureati in Scienze dell'Informazione ed Informatica) e Presidente della commissione di informatica giuridica. Ingegnere dell'Informazione, docente a contratto di diritto dell'ICT, qualità e comunicazione all'Università di Udine. Consulente su Governo Elettronico, Agenda Digitale ed innovazione nella PA locale, Auditor Sistemi informativi e 231, è consulente e valutatore di sistemi di qualità ISO9000, Privacy e Sicurezza presso Enti pubblici e privati. Ispettore AICA presso scuole ed enti di formazione. Membro del Consiglio Nazionale del Forum Competenze Digitali, è Presidente della Sezione Territoriale AICA del Nord Est.

E-mail: antonio@piva.mobi

Attilio Rampazzo, *CISA CRISC*, *C|CISO CMC* consulente di Sistemi Informativi e Sicurezza delle Informazioni in primaria azienda di Servizi Informatici italiana. Ha maturato un'esperienza pluriennale nello sviluppo e conduzione di progetti informatici in ambito bancario e finanziario, nei quali la qualità e la sicurezza hanno ricoperto un ruolo determinante.
E' Vice Presidente di AICA sez. Nord Est, AICQ Triveneta e CISA Coordinator e Research Director in ISACA Venice chapter. Svolge attività come Valutatore di Sistemi di Sicurezza delle Informazioni e di Sistemi di Gestione dei Servizi (cert. AICQ Sicev) presso CSQA Certificazioni. Trainer accreditato APMG per ITIL, ISO 20000 e Cobit 5.
Socio AICA, AICQ, ISACA Venice chapter, ASSOVAL, ANIP.

E-mail: attilio.rampazzo@gmail.com