SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI - REQUISITI

Per conto di AICQ CN[1] - Autore dr. Giovanni Mattana Presidente AICQ CentroNord

Peculiarità della Norma

Scopo della presente scheda è quello di attirare l'attenzione sull'importanza di questa norma e sintetizzarne i contenuti in modo molto schematico. La norma sarà presto pubblicata da UNI in lingua italiana.

Questa norma tratta i requisiti del sistema di gestione della Sicurezza Informazioni (spesso identificato con la sigla ISMS, Information Security Management System oppure in italiano SGSI, Sistema di Gestione della Sicurezza Informatica). La ISO/IEC 27001:2013 è la seconda edizione della norma (prima edizione nel 2005) ed **adotta la nuova struttura derivata dall'ANNEX SL**. L''ANNEX SL fa parte delle ISO/IEC Directives Supplement ove sono definite le direttive per lo sviluppo di tutti i nuovi standard sui sistemi di gestione. Anche le nuove edizioni di altri sistemi di gestione si adegueranno a questo schema.

Nello specifico la norma 27001 fornisce i requisiti per il sistema di gestione della sicurezza informazioni e quindi può essere utilizzata per certificare la conformità di un sistema informativo a questo standard.

Per sicurezza del sistema informativo (che oggi si identifica in larga parte con il sistema informatico) si intende, secondo la definizione data nella norma 27000, 'preservation of confidentiality integrity and availability of information' (in italiano riservatezza, integrità e disponibilità delle informazioni).In queste tre caratteritiche si considera anche inclusa la *compliance* (conformità) a leggi e regolamenti (es. leggi sulla privacy, sui crimini informatici oppure prescrizioni regolamentari sulla disponibilità di sistemi critici a supporto di servizi pubblici ecc.). A conferma dell'importanza di questo argomento la norma dedica un capitolo intero ai controlli di compliance nell'Annex A.

La norma, già dalla prima edizione, utilizza i concetti del risk management come base per decidere azioni e contromisure (controls) da mettere in atto. In sostanza le decisioni su come e quanto investire nella sicurezza delle informazioni debbono avvenire in base al rischio cioè alla valutazione della probabilità di un evento dannoso, attribuibile al sistema informativo, e della severità delle sue conseguenze.

SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI - REQUISITI

La norma 27001 può essere utilizzata da qualsiasi impresa (pubblica o privata, profit o noprofit, culturale o sociale, collettiva o individuale) che intende gestire i rischi relativi alla sicurezza delle informazioni.

La lunghezza della Norma è di circa 30 pagine.

Caratteristica della norma è la sua 'specificità': infatti nell'Annex A (lungo circa 14 pagine) è raccolto un catalogo molto completo delle contromisure ('controls in inglese) che possono essere adottate per contrastare i rischi del sistema informativo.

Si segnala che oltre alla norma 'base' 27001 esistono altri standard ISO che approfondiscono i vari aspetti della sicurezza informatica e di cui citiamo i principali:

- **ISO/IEC 27000:2012** Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary .

- **ISO/IEC 27002:2013** (seconda edizione emessa contemporaneamente alla 27001-2013) Information technology -- Security techniques -- Code of practice for information security controls La norma fornisce alle organizzazioni le linee guida per selezionare i controlli da realizzare nell'implementazione di un SGSI conforme alla ISO/IEC 27001 e le best practices per realizzarli.

- **ISO/IEC 27005:2011** Information technology -- Security techniques -- Information security risk management. La norma fornisce linee guida specifiche sulla gestione del rischio relativo alla sicurezza delle informazioni.

Da notare che, come linea guida generale per la gestione del rischio, le nuove norme ISO fanno riferimento allo standard **ISO 31000, Risk Management — Principles and Guidelines** citato quindi anche nella 27001-2013.

INDICE DELLA NORMA

0 INTRODUZIONE

0.1 Generalità

La presente norma internazionale è stata elaborata allo scopo di fornire i requisiti per stabilire, attuare, mantenere e migliorare in modo continuo un sistema di gestione per la sicurezza delle informazioni.

L'adozione di un sistema di gestione per la sicurezza delle informazioni dovrebbe essere una decisione strategica per un'organizzazione.

Il progetto e l'attuazione un sistema di gestione per la sicurezza delle informazioni di un'organizzazione è influenzato dalle necessità e obiettivi dell'organizzazione, dai suoi requisiti di sicurezza, dai suoi processi organizzativi, dalla sua dimensione e struttura. E' previsto che tutti questi fattori si modifichino nel tempo.

Il sistema di gestione per la sicurezza delle informazioni preserva la riservatezza, l'integrità e la disponibilità dalle informazioni mediante l'applicazione di un processo di gestione del rischio e dà fiducia alle parti interessate sull'adeguatezza della gestione dei rischi.

E' importante che il sistema di gestione per la sicurezza delle informazioni sia parte integrante dei processi e della struttura gestionale complessiva dell'organizzazione e che la sicurezza delle informazioni sia considerata nella progettazione dei processi, dei sistemi informativi e dei controlli. Ci si attende che un sistema di gestione per la sicurezza delle informazioni sia commisurato alle necessità dell'organizzazione.

La presente norma internazionale può essere utilizzata da parti interne ed esterne al fine di valutare la capacità di un'organizzazione di soddisfare i propri requisiti relativi alla sicurezza delle informazioni.

0.2 Compatibilità con altre norme relative a sistemi di gestione

La presente norma internazionale **utilizza la struttura ad alto livello,** gli stessi titoli per i punti, il testo identico, i termini comuni e le definizioni fondamentali definite nell'Annex SL delle ISO/IEC Directives, Part 1, Consolidated ISO Supplement, e mantiene quindi la compatibilità con le altre norme relative ai sistemi di gestione che hanno adottato l'Annex SL.

1 SCOPO E CAMPO DI APPLICAZIONE

La presente norma internazionale specifica i requisiti per stabilire, attuare, mantenere e migliorare in modo continuo un sistema di gestione per la sicurezza delle informazioni nel contesto di un'organizzazione. La presente norma internazionale include anche i requisiti per la valutazione e il trattamento dei rischi relativi alla sicurezza delle informazioni adattati alle necessità dell'organizzazione. I requisiti stabiliti dalla presente norma internazionale sono di carattere generale e predisposti per essere applicabili a tutte le organizzazioni, indipendentemente dalla loro tipologia, dimensione e natura. L'esclusione di qualunque requisito specificato nei punti dal 4 al 10 non è accettabile quando un'organizzazione dichiara la sua conformità alla presente norma internazionale.

4 CONTESTO DELL'ORGANIZZAZIONE

4.1 Comprendere l'organizzazione e il suo contesto

L'organizzazione deve stabilire, attuare, gestire, monitorare, riesaminare, conservare e migliorare un SGSI documentato entro il contesto delle attività complessive dell'organizzazione e dei rischi a cui far fronte.

Per lo scopo di questa Norma il processo usato è basato su un modello PDCA.

4.2 Comprendere le necessità e le aspettative delle parti interessate

L'organizzazione deve determinare:

a) le parti interessate pertinenti al sistema di gestione per la sicurezza delle informazioni; e

b) i requisiti di tali parti interessate attinenti la sicurezza delle informazioni.

4.3 Determinare il campo di applicazione del sistema di gestione per la sicurezza delle informazioni

L'organizzazione deve determinare i confini e l'applicabilità del sistema di gestione per la sicurezza delle informazioni per stabilirne il campo di applicazione.

Nel determinare il campo di applicazione, l'organizzazione deve considerare:

a) i fattori esterni ed interni di cui al punto 4.1;

b) i requisiti di cui al punto 4.2; e

c) le interfacce e le interdipendenze tra le attività svolte dall'organizzazione, e quelle svolte da altre organizzazioni.

Il campo di applicazione deve essere disponibile come insieme di informazioni documentate

4.4 Sistema di gestione per la sicurezza delle informazioni

L'organizzazione deve stabilire, attuare, mantenere e migliorare in modo continuo un sistema di gestione per la sicurezza delle informazioni, in conformità ai requisiti della presente norma internazionale.

5 LEADERSHIP

5.1 Leadership e impegno

La clausola tratta i requisiti per l'alta direzione

Da segnalareil requisito assicurando l'integrazione dei requisiti del sistema di gestione per la sicurezza delle informazioni nei processi dell'organizzazione;

5.1 Leadership e impegno

L'alta direzione deve dimostrare leadership e impegno nei riguardi del sistema di gestione per la sicurezza delle informazioni:

a) assicurando che la politica e gli obiettivi per la sicurezza delle informazioni siano stabiliti e siano compatibili con gli indirizzi strategici dell'organizzazione;

b) assicurando l'integrazione dei requisiti del sistema di gestione per la sicurezza delle informazioni nei processi dell'organizzazione;

c) assicurando la disponibilità delle risorse necessarie al sistema di gestione per la sicurezza delle informazioni;

d) comunicando l'importanza di un'efficace gestione della sicurezza delle informazioni e dell'essere conforme ai requisiti del sistema di gestione per la sicurezza delle informazioni;

e) fornendo sufficienti risorse per stabilire, attuare, gestire, monitorare, riesaminare, manutenere e migliorare i SGSI;

f) fornendo guida e sostegno alle persone per contribuire all'efficacia del sistema di gestione per la sicurezza delle informazioni;

g) promuovendo il miglioramento continuo; e

h) fornendo sostegno ad altri pertinenti ruoli gestionali nel dimostrare la propria leadership come opportuno nelle rispettive aree di responsabilità.

5.2 Politica

La politica deve:

1) essere appropriata rispetto alle finalità dell'organizzazione;

2) fornire un quadro di riferimento per stabilire gli obiettivi …;

3) comprendere un impegno a soddisfare le norme e i requisiti applicabili;

4) comprendere un impegno per il miglioramento continuo del SGSI;

Viene richiesto che sia documentata, comunicata e disponibile.

5.3 Ruoli, responsabilità e autorità nell'organizzazione

L'alta direzione deve definire e comunicare i ruoli dell'organizzazione.
A ciascun ruolo deve assegnare responsabilità e poteri per:

a) assicurare che il sistema di gestione per la sicurezza delle informazioni sia conforme ai requisiti della presente norma internazionale; e

b) riferire all'alta direzione sulle prestazioni del sistema di gestione per la sicurezza delle informazioni

Nota: questo requisito è molto importante perché la sicurezza si realizza con il contributo di tutti coloro che sono coinvolti nell'utilizzo e gestione del sistema informativo. Spesso la sicurezza è considerata come un tema per specialisti.

6 PIANIFICAZIONE

6.1 Azioni per affrontare rischi e opportunità

6.1.1 Generalità

a) Occorre un piano ai fini di assicurare che il sistema di gestione per la sicurezza delle informazioni possa conseguire il/i proprio/i esito/i previsto/i;

b) prevenire, o ridurre, gli effetti indesiderati; e

c) realizzare il miglioramento continuo.

L'organizzazione deve pianificare:

d) le azioni per affrontare questi rischi e opportunità; e le modalità per

- integrare e attuare le azioni nei processi del proprio sistema di gestione per la sicurezza delle informazioni; e
- valutare l'efficacia di tali azioni.

Da notare il punto a) dove si richiede di valutare un tipo di rischio specifico del piano (e non del sistema informativo).

6.1.2 Valutazione del rischio relativo alla sicurezza delle informazioni

Il risk assessment relativo al sistema informativo è un attività che :

a) stabilisca e mantenga i criteri di rischio relativo alla sicurezza delle informazioni, che includano:
- i criteri per l'accettazione del rischio; e
- i criteri per effettuare valutazioni del rischio relativo alla sicurezza delle informazioni;

b) assicuri che ripetute valutazioni del rischio relativo alla sicurezza delle informazioni producano risultati coerenti, validi e confrontabili tra loro;

c) identifichi i rischi relativi alla sicurezza delle informazioni:
- applicando il processo di valutazione del rischio relativo alla sicurezza delle informazioni per identificare i rischi associati alla perdita di riservatezza, di integrità e di disponibilità delle informazioni incluse nel campo di applicazione del sistema di gestione per la sicurezza delle informazioni; e
- identificando i responsabili dei rischi;

d) analizzi i rischi relativi alla sicurezza delle informazioni:
   - valutando le possibili conseguenze che risulterebbero se i rischi identificati al punto 6.1.2 c) si concretizzassero;
   - valutando la verosimiglianza realistica del concretizzarsi dei rischi identificati al punto 6.1.2 c); e
   - determinando i livelli di rischio;

e) ponderi i rischi relativi alla sicurezza delle informazioni:
   - comparando i risultati dell'analisi del rischio con i criteri di rischio stabiliti al punto 6.1.2.a); e
   - stabilendo le priorità dei rischi analizzati per il trattamento del rischio.

L'organizzazione deve conservare informazioni documentate sul processo di valutazione del rischio relativo alla sicurezza delle informazioni

6.1.3 Trattamento del rischio relativo alla sicurezza delle informazioni

Il capitolo prevede le seguenti attività:
a) selezionare le opzioni del processo di trattamento del rischio(accettare, trasferire, mettere in atto provvedimenti di mitigazione);
b) determinare le misure di controllo che realizzano i trattamenti selezionati;
c) comparare i controlli con le indicazioni dell'annex A;
d) produrre una dichiarazione di applicabilità in cui giustificare quali dei 114 controlli sono stati utilizzati per il trattamento del rischio e la motivazione dell'esclusione di alcuni controlli;
e) formulare un piano di trattamento;
f) ottenere l autorizzazione della direzione x attuare il piano e accettare il rischio residuo.

6.2 Obiettivi per la sicurezza delle informazioni e pianificazione per conseguirli

Si richiede di fissare obiettiv:

a) consistenti con la politica;
b) misurabili;
c) allineati all'analisi dei requisiti e ai risultati di rm;
d) comunicati;
e) aggiornati.

In base agli obiettivi occorre definire:

1) cosa fare,
2) con quali risorse,
3) chi è responsabile,
4) tempi di completamento,
5) modalità di valutazione dei risultati

7 SUPPORTO

7.1 Risorse

L'organizzazione deve determinare e mettere a disposizione le risorse necessarie per l'istituzione, implementazione, manutenzione e continuo miglioramento del SGSI.

7.2 Competenza

Viene richiesto di
1)determinare le necessarie competenze di persone che in autonomia influenzano le prestazioni SGSI;
2) garantire giusti livelli di competenza con adeguata istruzione, formazione, addestramento esperienza;
3)adottare misure per acquisire le competenze necessarie e valutare l'efficacia di tali misure;
4) mantenere evidenza delle competenze.

7.3 Consapevolezza

Coloro che operano ina azienda debbono conoscere la policy di sicurezza, loro responsabilità specifiche e implicazioni derivanti dalla non ottemperanza alle regole del sistema di sicurezza.

7.4 Comunicazione

Sono richiamati i criteri da utilizzare per la comunicazione :

a) ciò su cui comunicare;
b) quando comunicare;
c) con chi comunicare;
d) chi deve comunicare; e
e) i processi attraverso i quali devono essere effettuate le comunicazioni.

7.5 Informazioni documentate

Questo paragrafo sostituisce le richieste delle procedure di documentazione precedentemente preenti nelle norme ISO. La formulazione è la stessa che per altre norme recentemente emesse.
Documenti richiesti

- quelli indicati nello standard (in alcuni paragrafi è indicate la necessità di un documento specifico)
- documenti che l'azienda ritiene necessari

Sono poi indicati i criteri per creare/approvare la documentazione, per conservarla, per gestirne le versioni, ecc.

8 ATTIVITÀ OPERATIVE

Questo capitolo corrisponde al 'DO' nello schema PDCA. Consiste in tutte le attività realizzative

8.1 Pianificazione e controllo operativi

L'organizzazione deve pianificare, attuare e tenere sotto controllo i processi necessari per soddisfare i requisiti di sicurezza delle informazioni e per mettere in atto le azioni determinate al punto 6.1. L'organizzazione deve anche attuare i piani per conseguire gli obiettivi per la sicurezza delle informazioni determinati al punto 6.2.

Tutta l'attività realizzativa (il 'do' del ciclo PDCA) è 'collassata' in questo sottoparagrafo di poche righe. L'organizzazione deve assicurare che i processi affidati all'esterno siano determinati e tenuti sotto controllo.

8.2 Valutazione del rischio relativo alla sicurezza delle informazioni

Si richiede di ripetere il risk assessment a 'planned intervals or when significant changes are proposed or occur'.

8.3 Trattamento del rischio relativo alla sicurezza delle informazioni

L'organizzazione deve

1) attuare il piano di trattamento del rischio;
2) conservare informazioni documentate sui risultati del trattamento del rischio.

9 VALUTAZIONE DELLE PRESTAZIONI

In questo capitolo rientrano alcuni requisiti che nelle norme precedenti erano oggetto di capitoli dedicati

9.1 Monitoraggio, misurazione, analisi e valutazione

L'organizzazione deve valutare le prestazioni e determinare

a) cosa – grandezze da misurare;

b) come – i metodi di misura…

c) quando e chi – piani delle attività sia x raccolta dati di monitoraggio e misura, sia x analisi e valutazione dei dati raccolti.

d) conservare informazioni documentate sui risultati delle misure.

9.2 Audit interno

Sono fornite le indicazioni classiche sull'attività di auditing
L'audit deve verificare la conformità allo std 27001 ed alle regole/procedure interne
Sono previsti i programmi, gli obiettivi, la scelta di auditor competenti, la comunicazione dei risultati al management, la documentazione dell'attività di audit.

9.3 Riesame di direzione

Anziché definire input ed output sono definiti gli argomenti da trattare
a lo stato delle azioni definite nei i precedenti riesami …;
b) i cambiamenti interni-esterni
c) le informazioni di ritorno sulle prestazioni (nc, ac, audit, risultati attesi-effettivi, …)
d) le informazioni di ritorno dalle parti interessate;
e) i risultati valutazione del rischio e lo stato del piano di trattamento del rischio; e
f) le opportunità

10 MIGLIORAMENTO

10.1 Non conformità e azioni correttive

Contenuti

1)reagire alle non conformità : attivare controllo-correzione, trattarne le conseguenze.
2) eliminare le cause di nc: riesaminare la nc, determinando le cause di nc e determinare se esistono o potrebbero verificarsi nc simili.
3) attuare le azioni correttive (ac) necessarie;
4) riesaminare l'efficacia di ogni ac intrapresa;
5) cambiare le parti del SGSI non adeguate

10.2 Miglioramento continuo

L'organizzazione deve migliorare in modo continuo l'idoneità, l'adeguatezza e l'efficacia del sistema di gestione per la sicurezza delle informazioni.

L'ANNEX A

L'Annesso A (che si estende per circa 14 pagine) risulta particolarmente utile ed importante. Contiene i controlli cioè il catalogo delle contromisure . Gli obiettivi di controllo e i controlli elencati nel prospetto A.1 sono ripresi direttamente dai punti da 5 a 18 nella ISO/IEC 27002:2013 [1] e allineati ad essi.