La sicurezza delle informazioni in caso di calamità naturali e non naturali

In caso di catastrofi e calamità naturali quali terremoti, alluvioni, inondazioni, incendi, eruzioni vulcaniche, uragani oppure atti terroristici, uno dei danni collaterali dopo la perdita di vite umane e i danni materiali ad edifici ed infrastrutture, occorre considerare il blocco dei sistemi informativi che può rallentare notevolmente la ripresa delle normali attività.

Le metodologie da impiegare per prevenire e mitigar i danni che possono compromettere la ripresa delle attività dopo un evento catastrofico riguardano la tematica della business continuity (continuità operativa).

Nell'intervento presentato lo scorso 17/11 al Convegno EVENTI SISMICI: PREVENZIONE, PROTEZIONE, SICUREZZA, EMERGENZA, le cui slide sonono scaricabili in questa pagina, si sono presentate tutte le attività da porre in essere per controllare tali situazioni indesiderate, in particolare sono stati trattati i seguenti argomenti:

- business continuitymanagement
- normative ISO 22301, ISO 2001/27002 e ISO 27031 per la gestione della business continuity, con particolare riferimento ai sistemi informatici
- gestione dei rischi per la continuità operativa
- disaster recovery
- obiettivi ed indicatori di business continuity
- business continuity plan (piano di continuità operativa).

La sicurezza dei dati in caso di terremoto (180 download)

La nuova edizione della norma ISO 27002 (prima parte)

La norma UNI CEI ISO/IEC 27002:2014 "*Raccolta di prassi sui controlli per la sicurezza delle informazioni*" (che sostituisce la ISO 27002:2005) è stata progettata per essere impiegata nelle organizzazioni che intendono implementare un sistema di gestione della sicurezza delle informazioni ISO 27001 e la prendono come riferimento per la scelta dei controlli di sicurezza da attuare.

Struttura della norma

La norma contiene **14 punti di controllo di sicurezza** (erano 11 nella precedente versione della norma) che riuniscono un totale di **35 categorie principali di sicurezza** (erano 39 nella versione precedente) e **114 controlli** (erano 133 nella versione precedente).

Ogni punto che definisce controlli di sicurezza contiene una o più categorie principali di sicurezza, al cui interno sono raggruppati i controllo relativi. Nella norma viene precisato che l'ordine dei punti è indipendente dalla loro importanza, infatti, a seconda delle circostanze, i controlli di sicurezza appartenenti ad uno o a tutti i punti di controllo potrebbero rivelarsi più o meno importanti ed ogni organizzazione che impiega la norma dovrebbe identificare i controlli applicabili al proprio interno, la loro importanza ed il loro impiego in ogni processo di business.

Ogni **categoria principale** di controllo di sicurezza contiene:

- L'**obiettivo di controllo** che dichiara cosa si vuole raggiungere
- I **controlli** che possono essere applicati per raggiungere l'obiettivo di controllo.

La descrizione dei controlli sono strutturate come segue:

- Controllo: definisce nello specifico il controllo funzionale alla soddisfazione dell'obiettivo di controllo.
- Guida attuativa: fornisce informazioni più dettagliate per supportare l'attuazione del controllo. La guida può risultare completamente attinente o sufficiente a tutte le situazioni oppure potrebbe non soddisfare i requisiti specifici di controllo dell'organizzazione.
- Altre informazioni: fornisce informazioni aggiuntive che potrebbe essere

necessario considerare, per esempio considerazioni legali e riferimenti ad altre norme. Nel caso non vi siano informazioni aggiuntive da considerare questa parte non è riportata nel testo.

Elenco dei controlli

I punti di controllo definiti dalla norma sono i seguenti:

5 POLITICHE PER LA SICUREZZA DELLE INFORMAZIONI

Al suo interno viene individuata la categoria "**Indirizzi della direzione per la sicurezza delle informazioni**" (5.1), in cui viene indicata la necessità di stabilire una politica per la sicurezza delle informazioni coerente con gli obiettivi e gli indirizzi dell'organizzazione in merito all'Information Security, anche in funzione del contesto di riferimento (mercato, esigenze dei clienti, leggi e regolamenti applicabili). Tale politica dovrà essere mantenuta aggiornata attraverso riesami periodici.

6 Organizzazione della sicurezza delle informazioni

In questa sezione sono definiti le seguenti categorie principali:

- **Organizzazione interna (6.1)**: è necessario definire tutti i ruoli e le responsabilità per la sicurezza delle informazioni, separazioni dei compiti, modalità di contatto con le autorità e con gruppi specialistici ed infine le modalità di gestione dei progetti con riferimento alla sicurezza delle informazioni.
- **Dispositivi portatili e telelavoro (6.2)**: in questa categoria sono raggruppati due controlli molto importanti che, forse, meriterebbero una trattazione separata, anche se poi i controlli relativi sono descritti in modo dettagliato. I dispositivi portatili da gestire e mantenere sotto controllo sono di diverse tipologie (notebook, tablet, smartphone, …) ed ognuna di essa meriterebbe una trattazione a sé, così come la proprietà del dispositivo (azienda, dipendente o collaboratore, o semplice visitatore) ed il tipo di impiego (esclusivamente aziendale, esclusivamente privato o misto come nel caso del BYOD, *Bring Your Own Device*). Per quanto riguarda il telelavoro occorre tenere sotto controllo diversi parametri ed aspetti di sicurezza fisica e logica, non trascurando il fatto che ora il telelavoro è inteso in senso più ampio rispetto alla precedente versione della norma.

Quest'area è nel complesso più ridotta rispetto alla sezione 6 della precedente versione della norma che, tra l'altro, riportava la medesima categoria riferita a dispositivi portatili e telelavoro alla sezione 11, quella del controllo accessi. Del resto questa seconda categoria deve essere considerata in senso un po' più ampio perché la sicurezza dei dispositivi portatili e del telelavoro deve essere valutata insieme alla gestione delle connessioni wi-fi e degli accessi a siti web aziendali e ad eventuali servizi cloud.

Francamente ci si poteva aspettare qualcosa di più in quest'area ove al 6.2 l'evoluzione tecnologica in questi ultimi 9 anni trascorsi dalla precedente versione della ISO 27002 ha fatto passi da gigante moltiplicando anche le possibili vulnerabilità e qualche citazione più specifica del problema del BYOD e dell'autenticazione a due fattori (2FA) sarebbe stata gradita.

7 Sicurezza delle risorse umane

In questa sezione sono descritte le attività da considerare per garantire la sicurezza nella gestione del personale prima, durante ed al termine del rapporto di lavoro:

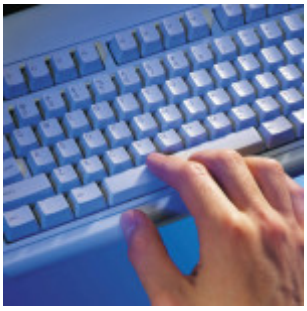
- **Prima dell'impiego (7.1)**: in due controlli vengono esposte tutte le cautele da intraprendere al momento dell'assunzione di una persona o dell'incarico ad un collaboratore esterno, non solo accordi di riservatezza e clausole contrattuali sul futuro rapporto lavorativo, ma anche – per quanto reso possibile dalla legislazione applicabile – un'accurata indagine conoscitiva sul passato, lavorativo e non, del futuro dipendente/collaboratore.
- **Durante l'impiego (7.2)**: nel corso della normale attività lavorativa viene data enfasi all'applicazione delle procedure stabilite e le responsabilità della Direzione nell'applicazione delle stesse, alla formazione-addestramento e sensibilizzazione del personale ed al ricorso ad eventuali processi disciplinari. Dunque regole da rispettare, ma anche motivazione ed incentivazione del personale, oltre che sanzioni a chi infrange le regole.
- **Cessazione e variazione del rapporto di lavoro (7.3)**: vengono presi in esame tutti gli aspetti e le attività da svolgere quando si chiude un rapporto di lavoro o avviene un'assegnazione ad altro incarico, come ad esempio il prolungamento della validità degli accordi di riservatezza, i passaggi di consegne e la comunicazione all'altro personale interessato della cessazione del rapporto di lavoro.

Qualche perplessità desta la traduzione UNI in quest'area: viene utilizzato il termine "soffiare" in senso di "soffiata", "spiata", "delazione", "informazione anonima su un comportamento non corretto" ed il termine "inazioni" probabilmente intendendo "omissioni" o il contrario di azioni, ovvero il "non agire".

I contenuti sono analoghi a quelli della precedente versione della norma alla sezione 8, anche se i controlli sono in numero minore.

8 Gestione degli asset

In quest'area viene trattata la gestione degli asset (tradotti come "beni" nella precedente versione della norma ISO 27001) all'interno di tre categorie:



- **Responsabilità per gli asset (8.1)**: tutti gli asset aziendali vanno inventariati, ne deve essere definito un responsabile e le regole per l'utilizzo e la gestione durante tutto il ciclo di vita.
- **Classificazione delle informazioni (8.2)**: le informazioni dovrebbero essere classificate in funzione del livello di riservatezza richiesto e conseguentemente etichettate in funzione della loro classificazione. Le procedure per il trattamento degli asset dovrebbero essere una logica conseguenza della classificazione degli stessi e delle informazioni in essi trattate.
- **Trattamento dei supporti (8.3)**: al fine di garantire riservatezza, integrità e disponibilità delle informazioni contenute nei supporti rimovibili (hard-disk esterni, chiavi USB, DVD, ecc.) occorre prevedere opportune procedure di gestione degli stessi durante tutto il loro ciclo di vita (impiego, dismissione, trasporto, ecc.).

Nella presente sezione – praticamente immutata rispetto alla corrispondente sezione 7 della precedente versione della norma, salvo l'aggiunta di due controlli – viene richiamata la classificazione degli asset finalizzata alla valutazione dei rischi contenuta nella ISO 27005.

9 Controllo degli accessi

Questa sezione tratta l'importante aspetto del controllo degli accessi alle aree dove sono custodite informazioni, in formato digitale o su supporto cartaceo, sia dal punto di vista degli accessi fisici, sia dal punto di vista degli accessi logici ai sistemi informatici. Le categorie prese in esame sono le seguenti:

- **Requisiti di business per il controllo degli accessi (9.1)**: occorre definire una politica di controllo degli accessi basata sull'accesso alle sole informazioni necessarie per svolgere il proprio lavoro (come impone anche la normativa sulla privacy in vigore in Italia) e regolamentare l'accesso alle reti (soprattutto evitare l'uso incontrollato delle reti wi-fi senza autenticazione utente).
- **Gestione degli accessi degli utenti (9.2)**: è necessario regolamentare il processo di registrazione (tramite credenziali di autenticazione univoche) e de-registrazione degli utenti, la fornitura delle credenziali di accesso (*provisioning*), la gestione degli accessi privilegiati (ad es. quelli in qualità di "amministratore di sistema", cfr. apposita disposizione del Garante della

Privacy), la gestione delle informazioni segrete per l'autenticazione (password, smartcard, ecc.), il riesame periodico dei diritti di accesso, la rimozione degli stessi al termine del rapporto (o la revisione in caso di cambio mansioni).
- **Responsabilità dell'utente (9.3)**: è importante regolamentare ed istruire il personale sull'uso della password.
- **Controllo degli accessi ai sistemi e alle applicazioni (9.4)**: è opportuno limitare l'accesso alle informazioni, predisporre procedure di log-on sicure, procedure di gestione delle password, limitare l'impiego di programmi di utilità privilegiati, limitare gli accessi al codice sorgente dei programmi.

Nei controlli esposti sono illustrati molti principi di sicurezza delle informazioni abbastanza noti ai più, ma spesso non recepiti nelle PMI per scarsa competenza dei responsabili IT (spesso esterni), richieste di gestioni semplificate da parte degli utenti e dei responsabili, mancanza di consapevolezza da parte della Direzione e, soprattutto, la ricerca del minor costo nelle apparecchiature e nella formazione del personale. Per questo motivo molte regole basilari, ad esempio relative ad una corretta gestione della rete wi-fi (creazione di accessi "ospite" per gli esterni, impiego di autenticazioni per singolo utente tramite protocollo Radius o da pannello di controllo del router, segmentazione delle reti in Vlan, …) e delle password (impiego di password complesse e memorizzate in modo sicuro tramite utility apposite, uso non promiscuo delle password, variazione delle password al primo accesso,…) spesso non vengono implementate.

Nel complesso sono presenti molti meno controlli rispetto alla precedente versione della norma alla sezione 11, ma i contenuti, opportunamente aggiornati, sono equivalenti.

10 Crittografia

Questo punto di controllo prevede una sola categoria **"Controlli crittografici" (10.1)** all'interno della quale sono descritti due controlli inerenti la politica relativa all'impiego dei controlli crittografici e la gestione delle chiavi crittografiche. La trattazione è molto dettagliata e comprende diversi aspetti da non sottovalutare come cosa fare in caso di indisponibilità, temporanea o permanente, delle chiavi crittografiche. In Italia occorre considerare la normativa specifica sulla firma digitale e la gestione dei certificati tramite le *certification authority* accreditate. Viene richiamata la norma ISO/IEC 11770 per ulteriori informazioni sulle chiavi.

Questa che era prima una categoria (cfr. punto 12.3 della norma ISO 27002:2005) ora è salito a livello di punto di controllo.

11 Sicurezza fisica e ambientale

La sezione comprende due categorie:

- **Aree sicure (11.1)**: devono essere definiti dei perimetri che delimitano aree con diversi livelli di sicurezza, nei quali occorre prevedere adeguate protezioni per prevenire accessi indesiderati e *safety* (viene citata la normativa antincendio), devono essere attivati sistemi di controllo e registrazione degli accessi alle aree sicure, devono essere implementate particolari misure di sicurezza fisica per proteggere aree chiave e devono essere adottate misure di protezione contro disastri e calamità naturali (incendi, alluvioni, terremoti, ecc.). Inoltre devono essere progettate ed attuate procedure per permettere il lavoro in aree sicure e protette e, infine, devono essere implementati controlli particolari nelle aree di carico/scarico materiali.
- **Apparecchiature (11.2)**: particolari accorgimenti devono essere intrapresi per proteggere le apparecchiature impiegate (per elaborazione o archiviazione di informazioni in genere) rispetto ad accessi non consentiti o minacce di possibili danneggiamenti, anche provenienti dalle infrastrutture di supporto (connettività di rete, energia elettrica, gas, acqua, ecc.) o da carenze di sicurezza dei cablaggi. Inoltre le apparecchiature devono essere sottoposte a regolare manutenzione, dispositivi hardware e software devono essere mantenuti sotto controllo in caso di trasferimenti all'esterno dell'organizzazione, adottando, nel caso particolari misure di sicurezza ed in caso di dismissione di apparecchiature o supporti di memorizzazione le informazioni in essi contenute devono essere cancellate in modo sicuro. Infine è necessario definire istruzioni affinché le apparecchiature non siano lasciate incustodite quando con esse è possibile accedere ad informazioni riservate ed occorre definire politiche di "scrivania pulita" per prevenire la visione di informazioni riservate da parte di personale non autorizzato.

fine I parte ….continua…

Le novità della UNI ISO 27001:2014

La norma ISO 27001 pubblicata nel 2013 è stata tradotta in italiano e convertita in norma UNI nel marzo 2014 come UNI CEI ISO/IEC 27001:2014 – *Tecnologie informatiche – Tecniche per la sicurezza – Sistemi di gestione per la sicurezza delle informazioni – Requisiti*. Essa 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, includendo anche i requisiti per **valutare e trattare i rischi** relativi alla sicurezza delle informazioni adattati alle necessità dell'organizzazione.

La nuova ISO 27001 non riporta termini e definizioni, ma richiama la ISO 27000.2014 (scaricabile gratuitamente da http://www.iso27001security.com/html/27000.html e curiosamente venduta dall'UNI a € 138) per tutti i termini utilizzati nelle norme della serie ISO 27k.

Si segnala che nel capitolo introduttivo della ISO 27001 è scomparso il paragrafo "Approccio per processi", sebbene venga sottolineata l'importanza che il sistema di gestione per la sicurezza delle informazioni sia parte integrante dei processi e della struttura gestionale complessiva dell'organizzazione.

La norma ISO 27001 riprende la nuova struttura di tutte le norme sui sistemi di gestione e, pertanto, al capitolo 4 tratta il "contesto dell'organizzazione". In questo capitolo viene esposto che per **comprendere l'organizzazione e il suo contesto** (4.1) occorre determinare i fattori esterni ed interni pertinenti alle finalità dell'organizzazione stessa e che influenzano la sua capacità di conseguire i risultati previsti per il proprio sistema di gestione per la sicurezza delle informazioni e che per **comprendere le necessità e le aspettative delle parti interessate** (4.2) occorre individuare le parti interessate al sistema di gestione per la sicurezza delle informazioni ed i requisiti delle stesse attinenti ad esso.

Anche la determinazione del **campo di applicazione del Sistema di Gestione per la Sicurezza delle Informazioni** (SGSI o ISMS, *Information Security Management System*) è un'attività inerente la comprensione dell'organizzazione ed il suo contesto. In questo ambito l'organizzazione deve determinare i **confini di applicabilità** del sistema di gestione per la sicurezza delle informazioni ISO 27001 al fine di stabilirne il campo di applicazione, in modo analogo a quanto avveniva nella versione precedente della norma, considerando anche i **fattori esterni ed interni** ed i **requisiti delle parti interessate** esposti ai paragrafi precedenti.

Il capitolo 5 **"Leadership"** rispecchia anch'esso la nuova struttura delle norme sui sistemi di gestione. In esso, al paragrafo 5.1, viene indicato quali modalità l'alta direzione deve attuare per dimostrare leadership e impegno nei riguardi del sistema di gestione per la sicurezza delle informazioni. In analogia con altri sistemi di gestione, l'alta direzione deve stabilire **politica** ed **obiettivi**, mettere a disposizione le **risorse necessarie** per l'attuazione del SGSI, **comunicare** l'importanza di **un'efficace gestione della sicurezza delle informazioni** e dell'essere **conforme ai requisiti** del SGSI stesso; deve, inoltre, assicurare che il SGSI ISO 27001 consegua i risultati previsti, fornire guida e sostegno al personale per contribuire all'efficacia del sistema di gestione della sicurezza delle informazioni e, naturalmente, deve promuovere il miglioramento continuo.

Il paragrafo 5.2 tratta della **politica per la sicurezza delle informazioni** per la quale i requisiti sono analoghi a quelli presenti negli altri sistemi di gestione: naturalmente la politica deve essere documentata, comunicata all'interno dell'organizzazione ed essere disponibile a tutte le parti interessate.

Anche il paragrafo 5.3 – che riguarda **ruoli, responsabilità e autorità nell'organizzazione** – è molto simile a quanto riportato nelle altre norme sui sistemi di gestione; in particolare, il fatto che la l'alta direzione debba assegnare responsabilità e autorità per assicurare che il sistema di gestione per la sicurezza delle informazioni sia conforme ai requisiti della norma e per riferire alla direzione stessa sulle prestazioni del sistema di gestione per la sicurezza delle informazioni, se non definisce la **nomina di un responsabile per il sistema di gestione della sicurezza delle informazioni** poco ci manca. Pur non essendo richiesto un rappresentante della direzione (non lo era neanche nella versione 2005 ISO e 2006 UNI della norma) viene rafforzato il concetto che è necessario assegnare responsabilità precise, all'interno o all'esterno dell'organizzazione (consulente), per garantire la conformità del SGSI.

Il capitolo 6 "**Pianificazione**" tratta, nel paragrafo 6.1, quali azioni occorre attuare per affrontare **rischi ed opportunità**. Infatti sulla base di quanto emerso dall'analisi del contesto dell'organizzazione occorre determinare i rischi e le opportunità che è necessario affrontare per assicurare che il sistema possa conseguire i risultati previsti, possa prevenire, o almeno ridurre, gli effetti indesiderati e realizzare il miglioramento continuo. Le **azioni per affrontare rischi ed opportunità** devono essere **pianificate**, così come le modalità per **integrare ed attuare** le azioni stesse nei processi del proprio sistema di gestione per la sicurezza delle informazioni e per **valutare l'efficacia** di tali azioni.

La **valutazione dei rischi relativi alla sicurezza delle informazioni** è trattata al paragrafo 6.1.2, dove sono riportati i requisiti per il **processo di valutazione del rischio** relativo alla sicurezza delle informazioni. Il processo di valutazione del rischio dovrà comprendere le seguenti attività

- Stabilire e mantenere i criteri di rischio relativo alla sicurezza.
- Assicurare che le ripetute valutazione del rischio producano risultati coerenti, validi e confrontabili tra loro (il metodo usato deve essere ripetibile e riproducibile con risultati coerenti come se fosse un dispositivo di misurazione sotto conferma metrologica).
- Identificare i rischi relativi alla sicurezza.
- Analizzare i rischi individuati, valutando le possibili conseguenze che risulterebbero se tali rischi si concretizzassero e valutando la verosimiglianza realistica di concretizzarsi dei rischi identificati, ovvero la probabilità che essi accadono, e, infine, determinando i livelli di rischio.
- Ponderare i rischi comparando i risultati dell'analisi dei rischi con i criteri stabiliti e definendo le priorità di trattamento dei rischi precedentemente valutati.

Naturalmente **la valutazione dei rischi deve essere documentata.**

Il **trattamento del rischio** relativo la sicurezza delle informazioni (6.1.3) deve essere definito ed applicato attraverso un processo del tutto similare a quello

stabilito nella versione precedente della norma, anche se esposto in modo differente. Oltre a selezionare l'opzione di trattamento dei rischi consuete occorre determinare i controlli necessari per attuare le opzioni selezionate per il trattamento del rischio, tenendo presente controlli riportati nell'appendice A e meglio dettagliati nella norma ISO 27002 (anch'essa tradotta finalmente in italiano come UNI CEI ISO/IEC 27002:2014 – *Tecnologie informatiche – Tecniche per la sicurezza – Raccolta di prassi sui controlli per la sicurezza delle informazioni*) al fine di non omettere controlli che potrebbero essere necessari.

Resta la necessità di redigere una **Dichiarazione di Applicabilità** che riporti:

- i controlli selezionati come necessari (che siano attuati o meno) e la relativa giustificazione per l'inclusione;
- i controlli presenti nell'Appendice A della ISO 27001 stessa eventualmente esclusi con le giustificazioni per la loro esclusione
- i controlli selezionati attualmente applicati.

Quest'ultimo punto costituisce una novità nel testo della norma che chiarisce e sancisce una prassi comunemente adottata dagli Organismi di Certificazione, ovvero quella di accettare una dichiarazione di applicabilità di determinati controlli di sicurezza la cui attuazione è stata pianificata, ma deve ancora venire.

Infine occorre predisporre un **piano di trattamento dei rischi** relativi alla sicurezza delle informazioni che dovrà essere approvato dalla Direzione, comprendente anche l'accettazione dei rischi residui che si è deciso di non trattare.

Anche questo **processo di trattamento del rischio dovrà essere documentato**.

Il sistema di gestione per la sicurezza delle informazioni ISO 27001 dovrà porsi degli **obiettivi** e **pianificare le azioni adeguate per conseguirli** (paragrafo 6.2). Le caratteristiche degli obiettivi sono le stesse degli altri sistemi di gestione (devono essere coerenti con la politica, misurabili, ecc.).

La pianificazione delle azioni poste in essere per conseguire gli obiettivi per la sicurezza delle informazioni deve comprendere le **azioni** pianificate, le **risorse** necessarie, le **responsabilità**, i **tempi** di completamento delle azioni, e le **modalità** di **valutazione dei risultati**.

Il capitolo 7 "**Supporto**" non presenta novità significative rispetto all'analogo capitolo delle altre norme relative ad altri sistemi di gestione. Pertanto i paragrafi **Risorse** (7.1), **Competenza** (7.2) Consapevolezza (7.3) e **Comunicazione** (7.4) non presentano sorprese di sorta, ma solo una esplicitazione più chiara rispetto al passato di cosa ci si dovrebbe attendere da un sistema di gestione per la sicurezza delle informazioni.

Il paragrafo 7.5 “**Informazioni documentate**” con i suoi sotto paragrafi descrive i requisiti relativi a **documenti** e **registrazioni,** secondo la dizione delle precedenti norme sui sistemi di gestione. Anche in questo caso i requisiti non presentano novità rispetto al passato, ma solo un diverso ordine di esposizione ed una maggior chiarezza nel descrivere che cosa ci si aspetta da un sistema di gestione documentato.

Non sono richieste procedure particolari, né un manuale del sistema di gestione ISO 27001, ma solo le informazioni documentate indicate nei vari punti della norma.

Il capitolo 8 “**Attività operative**” dispone requisiti relativi ai punti:

- pianificazione e controlli operativi (8.1);
- valutazione del rischio relativo la sicurezza delle informazioni (8.2);
- trattamento del rischio relativo la sicurezza delle informazioni (8.3).

In questo capitolo non ci sono novità rispetto alla versione precedente della norma, ma solo una riscrittura secondo la nuova struttura delle norme sui sistemi di gestione di quanto era già prescritto in passato. I contenuti, in verità, sono alquanto scarni, infatti viene prescritto di mantenere sotto controllo i processi operativi dell’organizzazione (processo produttivo o erogazione del servizio, approvvigionamenti, commerciale, ecc.) attraverso l’attuazione di tutti i controlli di sicurezza pianificati, monitorando ogni cambiamento e rivalutando periodicamente i rischi secondo le modalità già descritte nei paragrafi deò capitolo 6.

Il capitolo 9 “**Valutazione delle prestazioni**”, riporta i requisiti per il **monitoraggio**, la **misurazione**, **l’analisi** e la **valutazione** (9.1) del SGSI, per gli **audit** interni (9.2) e per il **riesame della direzione** (9.3). Anche in questo capitolo non sono presenti novità sostanziali rispetto alla precedente versione della norma, ma solo una riscrittura del testo in modo più chiaro. In particolare viene indicata la necessità di monitorare e misurare l’efficacia dell’attuazione dei controlli di sicurezza e tutti i processi che forniscono evidenza del buon funzionamento del SGSI.

Nel capitolo 10 “**Miglioramento**” sono trattate **non conformità**, **azioni correttive** e **miglioramento continuo**. Anticipando quello che avverrà per la prossima versione della norma ISO 9001:2015, si rileva l’eliminazione delle requisito riguardante le **azioni preventive** che vanno a confluire insieme a tutte le azioni di miglioramento non legate a non conformità o incidenti sulla sicurezza delle informazioni.

È curioso il fatto che mentre nella versione precedente la norma ISO 27001 non dedicava un paragrafo alle non conformità, che venivano citate nel testo, ma erano citati anche gli **incidenti** per la sicurezza delle informazioni, questa nuova versione non tratta gli incidenti – se non nei controlli dell’appendice A – e dedica il paragrafo 10.1 alle non conformità ed alle azioni correttive attuate per eliminarle.

Si ricorda che ACCREDIA ha disposto che Tutte le certificazioni emesse sotto accreditamento a fronte della ISO/IEC 27001:2005 dovranno essere ritirate entro il 1° ottobre 2015; oltre tale data potranno sussistere solo certificazioni secondo la nuova ISO 27001:2013. Pertanto restano pochi mesi per convertire i vecchi SGSI alla nuova norma. Probabilmente la stragrande maggioranza delle organizzazioni con SGSI certificato o certificando ISO 27001 dispongono già della certificazione ISO 9001 per la qualità, ma la nuova norma ISO 9001:2015, la cui struttura è allineata alla ISO 27001:2013 deve ancora essere ufficialmente emessa.

Il consiglio per le organizzazioni che si stanno adeguando alla 27001:2013 è quello di strutturare il sistema di gestione integrato secondo il nuovo schema, dunque allineare anche il sistema di gestione per la qualità sulla base delle indicazioni disponibili dalla bozza di ISO 90001:2015. Così facendo si avrà un sistema di gestione integrato ISO 9001-27001 omogeneo e meglio gestibile nell'immediato.

Questo probabilmente comporterà ristrutturare il manuale del sistema di gestione, anche se non esplicitamente richiesto dalla nuova norma, al fine di mantenere una continuità con il passato e garantire il controllo su tutta la documentazione del sistema di gestione.

Le modifiche al SGSI non sono sostanziali e riguardano più che altro i 114 controlli di sicurezza dell'appendice A e della ISO 27002 che naturalmente impattano sul trattamento dei rischi e sulla Dichiarazione di Applicabilità (*Statement of Applicability*, SoA).

Una metodologia di valutazione dei rischi per la sicurezza delle informazioni

La norma UNI CEI ISO 27001 (*Sistemi di gestione della sicurezza delle informazioni – Requisiti*), recentemente pubblicata in nuova versione 2013 dall'ISO, richiede una valutazione preliminare dei rischi sulla sicurezza delle informazioni (punto 4.2.1) al fine di implementare un sistema di gestione della sicurezza delle informazioni idoneo a trattare i rischi che l'organizzazione effettivamente corre in merito all'Information Security.

Gli approcci possibili alla valutazione dei rischi possono essere diversi ed i

metodi per effettuare il cosiddetto ***Risk Assessment*** possono variare di caso in caso, in funzione della dimensione, della complessità e del tipo di organizzazione che si sta esaminando.

La ISO 27005 (*Information security risk management*) è il principale riferimento per la gestione del rischio in ambito sicurezza delle informazione, ma anche altre norme quali la ISO 31000 (*Risk management – Principles and guidelines*) – recepita in Italia come UNI ISO 31000 (Gestione del rischio – Principi e linee guida) – e ISO 31010 (*Risk management – Risk assessment techniques*) possono essere prese a riferimento.

Vediamo un esempio di possibile approccio alla gestione del rischio finalizzato a preparare una valutazione dei rischi sulla sicurezza delle informazioni.

Il processo di **gestione dei rischi** comprende le seguenti fasi, descritte nel seguito:

1) Identificazione dei rischi

2) Analisi e ponderazione dei rischi

3) Identificazione e valutazione delle opzioni per il trattamento dei rischi

4) Scelta degli obiettivi di controllo ed i controlli per il trattamento dei rischi

5) Accettazione dei rischi residui.

Le attività suddette vengono descritte nel **Rapporto di valutazione dei rischi** (*Risk assessment report*).

L'**identificazione dei rischi** che incombono sulla sicurezza delle informazioni avviene attraverso:

a) L'identificazione degli asset significativi all'interno del SGSI: tale attività avviene come descritto nella procedura *Identificazione e valutazione degli asset*.

b) La valorizzazione ai fini del SGSI degli asset rilevati: tale attività avviene come descritto nella procedura *Identificazione e valutazione degli asset*. La valorizzazione degli asset in termini di riservatezza, integrità e disponibilità avviene per singolo asset oppure per gruppi di asset omogenei ai fini del SGSI; nel seguito in entrambe le situazioni si utilizzerà il termine *asset* intendendosi anche "raggruppamento di *asset*".

c) Identificazione delle minacce/pericoli che incombono sugli asset: tale

attività viene svolta valutando le minacce note della letteratura e quelle ipotetiche specifiche in relazione ai servizi svolti dall'organizzazione. Le minacce vengono associate agli asset (e quindi alle informazioni che essi gestiscono) e vengono valorizzate in una scala da 1 a 3 (Bassa, Media, Alta). La stessa minaccia può assumere un livello di gravità diverso a seconda dell'asset cui si applica..

d) Identificazione delle vulnerabilità: tale attività viene svolta valutando le vulnerabilità note della letteratura, quelle ufficiali comunicate da fonti autorevoli e quelle ipotetiche specifiche in relazione ai servizi svolti dall'organizzazione. Le vulnerabilità vengono associate agli asset (e quindi alle informazioni che essi gestiscono) e vengono valorizzate in una scala da 1 a 3 (Bassa, Media, Alta). La stessa vulnerabilità può assumere un livello di gravità diverso a seconda dell'asset cui si applica.

e) Identificazione degli impatti o conseguenze che la perdita dei requisiti di riservatezza, integrità e disponibilità possono avere sugli asset. Le conseguenze del concretizzarsi di una minaccia in grado di sfruttare una vulnerabilità vengono anch'esse valorizzate attraverso la formula seguente:

Impatto = Valore Asset x Gravità Minaccia x Gravità Vulnerabilità.

L'analisi e ponderazione dei rischi per la sicurezza delle informazioni identificati avviene attraverso:

a) La valutazione della probabilità che si verifichino i singoli rischi identificati nella fase precedente. La probabilità di accadimento di un rischio avviene considerando gli **incidenti** verificatisi in passato e statistiche eventualmente disponibili. L'assegnazione di una livello di probabilità attraverso una scala qualitativa avviene secondo il seguente schema:

Valore	Descrizione	Esempio
1	Mai verificatosi ma possibile	Non è mai accaduto nella storia dell'organizzazione
2	Raro	Accaduto una volta all'anno
3	Periodico	Accaduto circa 3 volte l'anno
4	Regolare	Accaduto circa una volta al mese
5	Frequente	Si verifica settimanalmente

b) Determinazione dell'indice di esposizione al rischio moltiplicando la gravità dell'impatto per la probabilità. Il risultato ottenuto sarà un valore da 3 a 81.

c) Definizione dei criteri di accettazione dei rischi: si stabilisce un livello minimo di tolleranza dei rischi al di sotto del quale i rischi vengono accettati ed al di sopra del quale i rischi devono essere trattati con azioni mirate.

Relativamente alla **identificazione e valutazione delle opzioni per il trattamento dei rischi, per i rischi** che si è deciso di trattare, in ordine decrescente dal maggiore al minore, vengono scelte delle azioni di mitigazione del rischio, che possono consistere nelle seguenti opzioni:

- Ridurre il rischio attraverso l'applicazione di obiettivi di controllo e controlli preventivi e correttivi, finalizzati alla riduzione degli effetti (impatto) del verificarsi del rischio e/o alla riduzione della probabilità che si verifichi.
- Evitare il rischio attraverso l'applicazione di obiettivi di controllo e controlli finalizzati ad evitare che si concretizzino le situazioni che permettono al rischio di concretizzarsi, ovvero ridurre a zero la probabilità che l'incidente paventato si verifichi.
- Trasferire il rischio attraverso la stipula di polizze assicurative oppure l'esternalizzazione a fornitori di processi ed attività con la relativa presa in carico da parte del fornitore dei relativi rischi.

Tali azioni vengono documentate nel **Piano di trattamento dei rischi**. Esso deve definire le singole azioni da intraprendere, i tempi e le relative responsabilità e risorse per gestire i singoli rischi. L'efficacia delle azioni pianificate porterà ad un ricalcolo della valutazione dei rischi, ottenendo nuovi indici.

La **scelta degli obiettivi di controllo e dei controlli per il trattamento dei rischi** da attuare avviene in base dall'elenco dei controlli applicabili definito a partire dai controlli identificati a livello normativo (norme della famiglia ISO 27000) a cui si possono aggiungere altri controlli ritenuti utili.

I controlli vengono ritenuti applicabili o non applicabili, se applicabili possono essere attuati in modo completo o parziale. L'applicazione dei controlli può infatti essere ritenuta conveniente solo su alcuni processi/attività, in funzione della diversa esposizione al rischio che possiedono le varie attività svolte dall'organizzazione.

L'attuazione del **piano di trattamento dei rischi** porta all'**accettazione dei rischi residui**, ovvero ad evidenziare i rischi residui ritenuti accettabili, dato dall'insieme dei rischi valutati accettabili in sede di prima valutazione dei rischi ed i rischi residui trattati dalle azioni contenute nel **piano di trattamento dei rischi**.

Il piano di trattamento dei rischi riporta le seguenti informazioni:

1) Elenco dei rischi da trattare;

2) Descrizione delle relazioni fra il rischio e l'azione di trattamento del rischio prescelta;

3) Descrizione delle relazioni fra il rischio e gli obiettivi di controllo ed i controlli selezionati per gestire il rischio.

Lo scopo della procedura *Identificazione e valutazione degli asset* (predisposta con riferimento alla ISO 27005 – *Information technology – Security techniques – Information security risk management – Annex B – Identification and valuation of assets and impact assessment*) dovrebbe essere quello di definire le modalità operative e le responsabilità per l'effettuazione e l'aggiornamento del censimento dei beni (*asset*) aziendali e la relativa valutazione, in termini di riservatezza, integrità e disponibilità delle stesse. In essa vengono stabiliti:

- la classificazione degli asset;
- l'identificazione di ogni asset che ha impatto sulla sicurezza delle informazioni;
- la valutazione quantitativa di ogni asset in relazione alla sua importanza per la sicurezza delle informazioni.

La **classificazione degli asset** potrebbe distinguere due categorie principali di asset:

1. Asset primari: processi/attività ed informazioni;
2. Asset di supporto: hardware, software, reti, personale, sito, struttura organizzativa.

Gli asset possono essere delle seguenti tipologie:

1. *Information asset*: dati digitali e non digitali, sistemi operativi, software applicativo, beni intangibili (conoscenza, marchi, brevetti, …).
2. *Asset fisici*: infrastruttura IT, Hardware, Sistemi di controllo, Servizi IT.
3. *Risorse Umane*: dipendenti, collaboratori esterni e consulenti.

L'**identificazione** e ed il **censimento degli asset** aziendali (*asset inventory*) ha lo scopo di identificare i requisiti di sicurezza (riservatezza, integrità e disponibilità) degli stessi e valutarne possibili vulnerabilità.

Ad ogni *information asset* deve essere associato un valore in termini di **Riservatezza**, **Integrità** e **Disponibilità**; tale valore viene espresso in termini qualitativi attraverso l'attribuzione di un livello di importanza (Basso, Medio, Alto) a cui è associato un valore numerico crescente (1,2,3).

Ad ogni *asset* di supporto o *asset* non informativo (risorse fisiche e risorse umane) viene associato un valore in termini di criticità dell'asset, dato dalla somma dei valori di importanza dei requisiti *dell'asset* in termini di Riservatezza, Integrità, Disponibilità in funzione delle informazioni che esso gestisce. Dunque l'importanza di una risorsa per la sicurezza dipende dai requisiti di Riservatezza, Integrità e Disponibilità, espressi in livelli (Basso/Medio/Alto) a cui corrisponde il valore

1/2/3.

Di conseguenza il valore associato all'asset potrà variare da un minimo di 3 (Riservatezza=Basso + Integrità=Basso + Disponibilità=Basso) ad un massimo di 9 (Riservatezza=Alto + Integrità=Alto + Disponibilità=Alto).

Poiché gli asset possono essere di diversi tipi (risorse fisiche e risorse umane), la metodologia di valutazione dei requisiti di sicurezza delle informazioni è differente per ogni tipo di asset.

Il Valore *dell'Asset* in termini di sicurezza delle informazioni viene utilizzato nel ***Risk Assessment*** in combinazione con:

- le minacce che incombono sugli *asset* che possono sfruttare le vulnerabilità rilevate degli *asset* stessi;
- la probabilità che la minaccia si concretizzi in un incidente di sicurezza (delle informazioni);
- la gravità dell'impatto associato all'incidente.