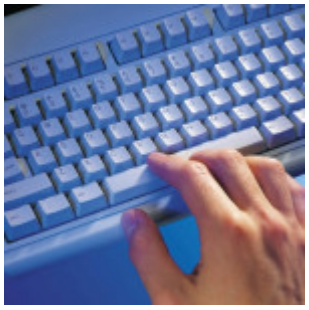
# La nuova edizione della norma ISO 27002 (seconda parte)



In questo articolo (cfr. precedente articolo) passiamo ad esaminare la seconda parte della norma La norma UNI CEI ISO/IEC 27002:2014 – *Raccolta di prassi sui controlli per la sicurezza delle informazioni* (che sostituisce la ISO 27002:2005).

**12 Sicurezza delle attività operative**

Questa area comprende ben 7 categorie:

- **Procedure operative e responsabilità (12.1)**: devono essere predisposte procedure per documentare lo svolgimento di una serie di attività inerenti la sicurezza, occorre gestire i cambiamenti all'organizzazione e la capacità delle risorse (di *storage*, di banda, infrastrutturali ed anche umane), infine è necessario mantenere separati gli ambienti di sviluppo da quelli di produzione.
- **Protezione dal malware (12.2)**: un solo controllo in questa categoria (protezione dal malware) che prescrive tutte le misure di sicurezza da attuare contro il malware. Non solo antivirus per prevenire ed eliminare malware, ma anche azioni di prevenzione tecnica e comportamentali (consapevolezza degli utenti).
- **Backup (12.3)**: devono essere documentate ed attuate procedure di backup adeguate a garantire il ripristino dei dati in caso di perdita dell'integrità degli stessi e la continuità operativa (vedasi anche punto 17).
- **Raccolta di log e monitoraggio (12.4)**: devono essere registrati, conservati e protetti i log delle attività degli utenti normali e di quelli privilegiati (si ricorda che per apposita disposizione del Garante Privacy italiano i log degli accessi in qualità di Amministratore di Sistema devono essere mantenuti in modo "indelebile" per almeno 6 mesi), occorre inoltre mantenere sincronizzati gli orologi dei sistemi con una fonte attendibile.
- **Controllo del software di produzione (12.5)**: particolari attenzioni devono essere adottate nell'installazione ed aggiornamento del software di produzione (non solo per organizzazioni del settore ICT, banche o assicurazioni, ma anche per aziende manifatturiere!).
- **Gestione delle vulnerabilità tecniche (12.6)**: viene fornita dalla norma un'ampia guida attuativa sulla gestione delle vulnerabilità tecniche conosciute (occorre mantenere un censimento dell'hardware e del relativo software installato su ogni elaboratore, installare le *patch* di sicurezza in modo tempestivo, mantenersi aggiornati sulle vulnerabilità di sicurezza conosciute, ecc.), oltre alle

indicazioni sulla limitazione nell'installazione dei software (è opportuno, infatti, ridurre al minimo la possibilità per gli utenti di installare applicativi software autonomamente, anche se leciti come le utility gratuite che, a volte, possono essere il veicolo di *adware* o altre minacce alla sicurezza).
- **Considerazioni sull'audit dei sistemi informativi (12.7)**: gli audit sui sistemi informativi dovrebbero avere un impatto ridotto sulle attività lavorative e le evidenze raccolte dovrebbero essere raccolte senza alterare i dati dei sistemi (accessi in sola lettura) e dovrebbero essere mantenute protette.

Questi elementi nella precedente versione della norma erano in gran parte all'interno della sezione 10 "*Communications and Operations Management*" (ma la gestione delle vulnerabilità tecniche era, invece, al paragrafo 12.6, per puro caso lo stesso della versione attuale della norma), il quale comprendeva anche i controlli del punto 13 seguente.

**13 Sicurezza delle comunicazioni**

Questa sezione contiene due sole categorie:

- **Gestione della sicurezza della rete (13.1)**: occorre adottare alcuni accorgimenti per garantire la sicurezza delle reti interne (responsabilità, autenticazioni, ecc.); viene anche citata la ISO/IEC 27033 nelle sue parti da 1 a 5 sulla sicurezza delle reti e delle comunicazioni per ulteriori informazioni. Deve, inoltre, essere gestita la sicurezza dei servizi di rete, compresi i servizi acquistati presso fornitori esterni, e la segregazione delle reti (separazione delle VLan, gestione delle connessioni Wi-Fi, …).
- **Trasferimento delle informazioni (13.2)**: occorre stabilire ed attuare politiche e procedure per il trasferimento delle informazioni con qualsiasi mezzo (posta elettronica, fax, telefono, scaricamento da internet, ecc.), nel trasferimento di informazioni con soggetti esterni occorre stabilire accordi sulle modalità di trasmissione, le informazioni trasmesse tramite messaggistica elettronica dovrebbero essere adeguatamente controllate e protette (non solo e-mail, ma anche sistemi EDI, *instant messages*, *social network*, ecc.) e, infine, occorre stabilire e riesaminare periodicamente accordi di riservatezza e di non divulgazione con le parti interessate.

I 7 controlli di quest'area sono sicuramente molto dettagliati e migliorano, oltre ad aggiornare, la precedente versione della norma, includendo controlli (un po' sparsi nella versione 2005 della ISO 27002) che recepiscono le nuove modalità di comunicazione, tra cui i social network, professionali e non.

**14 Acquisizione, sviluppo e manutenzione dei sistemi**

Quest'area tratta la sicurezza dei sistemi informativi impiegati per le attività aziendali e comprende tre categorie:

- **Requisiti di sicurezza dei sistemi informativi (14.1)**: la sicurezza dei sistemi informativi- acquistati o sviluppati ad hoc – deve essere stabilita fin dall'analisi dei requisiti, deve essere garantita la sicurezza dei servizi applicativi che viaggiano su reti pubbliche (ad esempio attraverso trasmissioni ed autenticazioni sicure crittografate), infine occorre garantire la sicurezza delle transazioni dei servizi applicativi.
- **Sicurezza nei processi di sviluppo e supporto (14.2)**: devono essere definite ed attuate politiche per lo sviluppo (interno o esterno all'organizzazione) sicuro dei programmi applicativi, devono essere tenuti sotto controllo tutti i cambiamenti ai sistemi (dagli aggiornamenti dei sistemi operativi alle modifiche dei sistemi gestionali), occorre effettuare un riesame tecnico sul funzionamento degli applicativi critici a fronte di cambiamenti delle piattaforme operative (sistemi di produzione, database, ecc.) e si dovrebbero limitare le modifiche (personalizzazioni) ai pacchetti software, cercando comunque di garantirne i futuri aggiornamenti. Inoltre dovrebbero essere stabiliti, documentati ed attuati principi per l'ingegnerizzazione sicura dei sistemi informatici e per l'impiego di ambienti di sviluppo sicuri. Nel caso in cui attività di sviluppo software fossero commissionate all'esterno, dovrebbero essere stabilite misure per il controllo del processo di sviluppo esternalizzato. Infine dovrebbero essere eseguiti test di sicurezza dei sistemi durante lo sviluppo e test di accettazione nell'ambiente operativo di utilizzo, prima di rilasciare il software.
- **Dati di test (14.3)**: i dati utilizzati per il test dovrebbero essere scelti evitando di introdurre dati personali ed adottando adeguate misure di protezione, anche al fine di garantirne la riservatezza.

Nel complesso i 13 controlli di questa sezione sono molto dettagliati e comprendono una serie di misure di sicurezza informatica ormai consolidate che riguardano tutti gli aspetti del ciclo di vita del software impiegato da un'organizzazione per la propria attività. Alcuni principi vanno commisurati ad una attenta valutazione dei rischi, poiché una stessa regola di sicurezza informatica (ad es. l'aggiornamento sistematico e tempestivo del software di base) potrebbe non garantire sempre l'integrità e la disponibilità dei sistemi (ad es. errori o malfunzionamenti introdotti dagli ultimi aggiornamenti di un sistema operativo).

**15 Relazioni con i fornitori**

Questo punto di controllo tratta tutti gli aspetti di sicurezza delle informazioni che possono legati al comportamento dei fornitori. Sono state individuate due categorie:

- **Sicurezza delle informazioni nelle relazioni con i fornitori (15.1)**: è necessario stabilire una politica ed accordi su tematiche inerenti la sicurezza delle informazioni con i fornitori che accedono agli asset dell'organizzazione; tali accordi devono comprendere requisiti per affrontare i rischi relativi alla sicurezza associati a prodotti e servizi nella filiera di fornitura dell'ICT

(cloud computing compreso).

- **Gestione dell'erogazione dei servizi dei fornitori (15.2):** occorre monitorare – anche attraverso audit se necessario – e riesaminare periodicamente le attività dei fornitori che influenzano la sicurezza delle informazioni, nonché tenere sotto controllo tutti i cambiamenti legati alle forniture di servizi.

**16 Gestione degli incidenti relativi alla sicurezza delle informazioni**

L'area relativa agli incidenti sulla sicurezza delle informazioni (sezione 13 della precedente versione della norma) comprende una sola categoria (erano 2 nella precedente edizione):

- **Gestione degli incidenti relativi alla sicurezza delle informazioni e dei miglioramenti (16.1)**: devono essere rilevati e gestiti tutti gli incidenti relativi alla sicurezza delle informazioni (viene qui richiamata la ISO/IEC 27035 – *Information security incident management*), ma anche rilevate ed esaminate tutte le segnalazioni di eventi relativi alla sicurezza che potrebbero indurre a pensare che qualche controllo è risultato inefficace senza provocare un vero e proprio incidente e pure tutte le possibili debolezze dei controlli messi in atto. In ogni caso ogni evento relativo alla sicurezza delle informazioni va attentamente valutato per eventualmente classificarlo come incidente vero e proprio o meno. Occorre poi rispondere ad ogni incidente relativo alla sicurezza delle informazioni in modo adeguato ed apprendere da quanto accaduto per evitare che l'incidente si ripeta. Infine dovrebbero essere stabilite procedure per la raccolta di evidenze relative agli incidenti e la successiva gestione (considerando anche eventuali azioni di analisi forense).

**17 Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa**

In quest'area (corrispondente al punto 14 sella precedente versione della norma) viene trattata la ***business continuity*** in 5 controlli suddivisi in due categorie:

- **Continuità della sicurezza delle informazioni (17.1)**: la continuità operativa per la sicurezza delle informazioni dovrebbe essere pianificata a partire dai requisiti per la business continuity, piani di continuità operativa (*business continuity plan*) dovrebbero essere attuati, verificati e riesaminati periodicamente.
- **Ridondanze (17.2)**: per garantire la disponibilità (e la continuità operativa) occorre prevedere architetture e infrastrutture con adeguata ridondanza.

Naturalmente sull'argomento esiste la norma specifica UNI EN ISO 22301:2014 – *Sicurezza della società – Sistemi di gestione della continuità operativa – Requisiti.*

**18 Conformità**

Questo ultimo punto di controllo (era il punto 15 nella ISO 27002:2005) tratta la gestione della cosiddetta "*compliance*", ovvero la conformità a leggi, regolamenti ed accordi contrattuali con i clienti. Sono identificate due categorie:

- **Conformità ai requisiti cogenti e contrattuali (18.1)**: occorre innanzitutto identificare i requisiti cogenti, quindi attuare controlli per evitare di ledere i diritti di proprietà intellettuale, proteggere adeguatamente le registrazioni che permettono di dimostrare la conformità a tutti i requisiti cogenti, in particolare devono essere rispettati leggi e regolamenti sulla privacy (in Italia il D.Lgs 196/2003 in attesa del nuovo Regolamento Europeo, ma nella norma viene citata come riferimento la ISO/IEC 29100:2011 "*Information technology – Security techniques – Privacy framework*"). Infine occorre considerare eventuali limitazioni all'uso dei controlli crittografici vigenti in alcune nazioni.
- **Riesami della sicurezza delle informazioni (18.2)**: dovrebbe essere svolto periodicamente un riesame indipendente sulla sicurezza delle informazioni dell'organizzazione, i processi di elaborazione delle informazioni e le procedure dovrebbero essere riesaminate periodicamente per valutarne la continua conformità ed adeguatezza alla politica ed alle norme ed infine dovrebbero essere eseguite delle verifiche tecniche della conformità dei sistemi informativi a politiche e standard di sicurezza (ad esempio *penetration test* e *vulnerability assessment*). Su quest'ultimo controllo si fa riferimento alla ISO/IEC TR 27008 – *Guidelines for auditors on information security management systems controls*.

---

# 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.

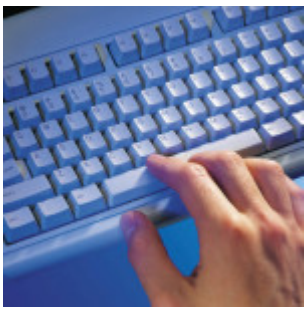
- **Cessazione e variazione del rapporto di lavoro (7.3)**: vengono presi in esame tutti gli aspetti e le attività da svolgere quando si chiude un rapporto di lavoro o avviene un'assegnazione ad altro incarico, come ad esempio il prolungamento della validità degli accordi di riservatezza, i passaggi 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).

# La nuova versione della ISO 27001 arriverà a fine 2013

La **ISO/IEC 27001**, norma contenente i requisiti per un **sistema di gestione della sicurezza delle informazioni**, è in corso di revisione e la sua pubblicazione è prevista per l'autunno del 2013. La revisione riguardeà essenzialmente l'armonizzazione della norma alla **ISO Guide 83** che prevede uno schema univoco per tutte le norme sui sistemi di gestione, a cui si stanno man mano adeguando gli standard di recente e futura pubblicazione.

Tale allineamento comporterà che tutte le norme riporteranno un significativo testo comune e ciò porterà un indubbio vantaggio per le organizzazioni che risparmieranno tempo nell'applicare le norme stesse, grazie **all'integrazione tra i vari Sistemi di Gestione**. Naturalmente ciò comporterà – per le organizzazioni già certificate per più sistemi – la necessità di revisionare la documentazione del sistema di gestione (integrato).

Il testo comune prevede i seguenti capitoli  a struttura comune : Introduzione, Norme di riferimento, Termini e definizioni, Contesto dell'organizzazione, Guida e Direzione (Leadership), Pianificazione, Supporto, Operatività (Operation), Valutazione delle Prestazioni e Miglioramento.

Altre modifiche riguarderanno la S.O.A., la comprensione del contesto dell'organizzazione, la **Business Continuity**, l'allineamento del **Risk Assessment** alla **ISO 31000** e l'aggiornamento dei **controlli di sicurezza** dell'Annex A. Proprio per quest'ultimo motivo si prevede l'emissione congiunta della **nuova ISO 27002** che rappresenta la linea guida per l'attuazione dei controlli.

Finora la ISO 27001 (pubblicata anche in versione italiana dall'UNI come **UNI CEI ISO/IEC 27001**) ha avuto un numero limitato di certificazioni in Italia, soprattutto se consideriamo che la certificazione di molet organizzazione è multisito e, quindi, il numero di certificati emessi è molto superiore alle aziende certificate.

Da un lato questo può essere imputabile ad un approccio un po' "high-level" della norma che, pertanto, può essere applicata in modo completo solo dalle organizzazioni più grandi che dispongono di risorse e di personale dalle competenze adeguate.

Dall'altro la scarsa propensione delle PMI a tutto ciò che può ridurre i rischi del

business, ma che richiede risorse dedicate per farlo ne ha impedito la diffusione capillare come è avvenuto per altri schemi. In questo contesto anche la **privacy,** a seguito dell'eliminazione dell'obbligo di redigere il DPS, è stata dimenticata da molte organizzazioni di medio-piccole dimensioni.

Il filo conduttore è sempre la sopravvivenza a cui mirano molte PMI in questo momento di crisi, trascurando diversi aspetti di miglioramento dell'efficienza e di riduzione dei rischi. Proprio i **rischi legati alla sicurezza delle informazioni** sono tra quelli trascurati, oggi che da un lato stanno crescendo i crimini informatici ed i reati legati al furto di informazioni di valore, dall'altro le aziende sono sempre più dipendenti dai sistemi informatici.

Sicuramente arrivare alla certificazione ISO 27001 è impegnativo e costoso (il numero di giornate di audit previste dallo schema di accreditamento è molto superiore a  quello della ISO 9001, a parità di dimensioni dell'organizzazione), ma questo non vuol dire che non si possa recepire l'approccio della norma in modo più semplificato ed attuare comunque i controlli che si ritiene adeguati a seconda del rapporto costo/beneficio (=riduzione del rischio) che essi possono portare.

Un sistema di gestione per la sicurezza delle informazioni ISO 27001 richiede, poi, un approccio culturalmente avanzato ed una conoscenza profonda dei processi aziendali e dell'impatto della sicurezza delle informazioni su di essi.

Purtroppo molte realtà ignorano che sicurezza delle informazioni non significa soltanto sicurezza dei sistemi informatici garantita attraverso l'adozione di un buon antivirus. Gli aspetti trattati dal SGSI ISO 27001 (e dai controlli della ISO 27002) sono molteplici e degni di nota: si va dalla sicurezza fisica dei locali (prevenzione e mitigazione degli effetti di incendi, allagamenti, inondazioni ed altri fenomeni naturali, prevenzione di furti ed altri atti criminosi) a quella logica dei sistemi informativi. Soprattutto si considerano tutti gli aspetti che possono minare la continuità dell'operatività aziendale (che genera profitti): dal furto di informazioni importanti all'interruzione dei servizi per le cause più disparate, il tutto considerando che le minacce più pericolose non sempre vengono dall'esterno dell'azienda, ma talvolta sono rappresentate da dipendenti e collaboratori infedeli o semplicemente incauti.

Ma quali sono le organizzazioni che più si avvantaggerebbero – sia dal punto di vista della riduzione dei rischi operativi, sia da quello dell'immagine sul mercato dall'applicazione di un sistema di gestione per la sicurezza delle informazioni ISO 27001? Sicuramente anzitutto Banche ed Istituti di Credito, Società finanziarie, Assicurazioni; insomma chi tratta flussi di denaro ed operazioni ad essi correlate tramite sistemi informatici. Tra esse forse le Compagnie di Assicurazioni (che trattano anche dati sensibili legati a polizze infortuni e malattie) sono probabilmente più lontane dallo standard ISO 27001, anche perchè sono costituite anche da piccole Agenzie che, di fatto, sono realtà con poco personale e con un'infrastruttura informatica ridotta per cui non dispongono di mezzi propri

sufficienti per approcciare lo standard ISO 27001.

Per il resto tutte le realtà che trattano dati ed informazioni, anche riservate, in outsourcing per conto di organizzazioni più grandi, come quelle sopra citate, oppure Enti Pubblici potrebbero trovare nell'applicazione dei principi della ISO 27001 (e ISO 27002) valore aggiunto per garantire al cliente un servizio più sicuro. Dunque i vantaggi sarebbero sia dal punto di vista di riduzione del rischio di business, sia dal punto di vista commerciale e di marketing, presentandosi come organizzazione certificata per la sicurezza delle informazioni.

Infine tutte le organizzazioni che forniscono servizi amministrativi, legali e di assistenza fiscale o consulenza del lavoro trattano dati sensibili o comunque riservati per conto dei propri clienti, ma non sempre attuano quelle misure di sicurezza che sono auspicate anche dal Codice della Privacy nel Disciplinare dell'Allegato B. Per esse – parliamo di Studi Legali, Studi di Commercialisti o Società di Professionisti nel medesimo settore, Consulenti del Lavoro, ecc. – l'impatto della ISO 27001 potrebbe essere eccessivamente oneroso, soprattutto per le realtà più piccole, ma applicarne i principi, gli obiettivi di controllo ed i controlli delle ISO 27001/27002 potrebbe ridurre sensibilmente i rischi di business legati alla perdita di Riservatezza, Integrità e Disponibilità delle Informazioni.

Leggi il documento ACCREDIA sulla nuova norma

Al sito http://www.iso27001security.com/index.html (in lingua inglese) sono disponibili numerosi documenti, liberamente scaricabili, sull'implementazione del sisttema di gestione della sicurezza delle informazioni (o ISMS, Information Security Management System).