Quaderno UNINFO

LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI E DELLA PRIVACY NELLE PMI

Gruppo di Lavoro UNINFO sulla serie di norme ISO/IEC 27000

Edizione 1.0 – 27 Settembre 2012

0 Premessa

L'**UNINFO**, libera associazione a carattere tecnico, ha lo scopo di promuovere e di partecipare allo sviluppo della normativa nel settore delle tecniche informatiche. Rientrano nel suo campo di attività i sistemi di elaborazione e di trasmissione delle informazioni e le loro applicazioni nelle più diverse aree, quali, ad esempio, le attività bancarie, le carte intelligenti, la telematica del traffico, l'automazione industriale.
In questo ambito l'UNINFO, ente federato all'UNI, opera con delega UNI, a livello nazionale ed internazionale e rappresenta l'Italia presso l'ISO, l'ISO/IEC JTC 1 e il CEN.

Il presente quaderno è stato concepito **dal Gruppo di Lavoro UNINFO sulla serie di norme ISO/IEC 27000** come libera iniziativa volta principalmente a diffondere la cultura dell'uso pratico degli standard relativi alla sicurezza delle informazioni in contesti di qualsiasi dimensione e non solo nelle grandi aziende.

In tale prospettiva il quaderno viene liberamente messo a disposizione attraverso il sito internet di UNINFO e tramite qualsiasi altro canale di altri soggetti che vogliano redistribuirlo, rispettando la seguente **licenza Creative Commons "*Attribuzione - Non opere derivate 3.0*"**, adottata per la presente opera:

Il testo integrale della sopracitata licenza è disponibile su: http://creativecommons.org/licenses/by-nd/3.0/it/legalcode

Indice

1 Introduzione

La tutela dei dati personali è regolamentata in Italia dal Decreto Legislativo 196 del 2003 "Codice in materia di protezione dei dati personali" (indicato anche come "Codice privacy") e dalla normativa secondaria ad esso collegata ed emessa dal Garante per la protezione dei dati personali (indicato anche come Garante privacy). Il Codice privacy italiano costituisce il recepimento della Direttiva Europea 95/46/CE.

Le norme più importanti in quest'area e a cui questo Quaderno fa riferimento sono le seguenti:

- D.lgs. 196/03 (Codice in materia di protezione dei dati personali);
- Allegato B del D.lgs. 196/03;
- Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema – Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 (con modifiche introdotte dai Provvedimenti del 12 febbraio 2009 e 25 giugno 2009).

Nell'ultima parte del 2011 e nei primi mesi del 2012, la normativa italiana è stata investita da modifiche che hanno cambiato e cambieranno, almeno in parte, le modalità di trattamento dei dati personali e la valutazione della loro liceità. Si prevede che ulteriori modifiche saranno apportate nel corso del 2012 e 2013. Non ci soffermiamo sulle motivazioni che hanno indotto il legislatore ad introdurre queste modifiche; possiamo però affermare che sono orientate alla semplificazione, a una maggiore armonizzazione a livello UE e all'adeguamento allo sviluppo tecnologico.

Le principali modifiche introdotte sono:

- nuova definizione di dato personale, ora applicabile alle sole persone fisiche;
- eliminazione dell'obbligo di redigere e aggiornare periodicamente il Documento programmatico per la sicurezza (DPS).

Per quanto riguarda gli scenari futuri, la Commissione europea ha presentato la proposta di un *Regolamento generale sulla protezione dei dati*, che andrà a sostituire, oltre alla direttiva 95/46/CE, lo stesso Codice privacy; introducendo identiche regole nei Paesi che compongono la UE. Infatti, i Regolamenti UE, a differenza delle direttive, sono immediatamente esecutivi e non necessitano di recepimento da parte degli Stati membri.

Il nuovo Regolamento, al momento solo in bozza, non è previsto che apporterà riduzioni o stravolgimenti dei requisiti rispetto all'attuale Codice privacy, ma semplificazioni nell'applicazione e miglioramenti degli effetti generali.

La normativa privacy si occupa, come è noto, di sicurezza delle informazioni, anche se limitatamente a quelle di carattere personale. E' quindi naturale volerla associare allo standard internazionale ISO/IEC 27001, che definisce i requisiti di un Sistema di gestione per la sicurezza delle informazioni (SGSI). Questo standard è applicabile in modo generale ad aziende di qualsiasi dimensione e riguarda la sicurezza di qualunque tipo di dato e informazione.

Questo Quaderno ha l'obiettivo di facilitare la realizzazione di un Sistema di gestione per la sicurezza delle informazioni (SGSI) che integri al suo interno le misure di sicurezza, incluse le procedure documentate o non documentate, previste dalla normativa italiana sulla tutela dei dati personali e costituisca un quadro di riferimento per mantenerle e migliorarle nel tempo.

Un secondo obiettivo, non meno importante, è quello di mostrare come la costruzione di un SGSI, anche in contesti aziendali di ridotte dimensioni (piccole e medie imprese, PMI), preponderanti nel tessuto economico del nostro Paese, sia un obiettivo raggiungibile con uno sforzo modesto. Tale sforzo, se correttamente indirizzato, può trasformare da costo a valore l'impegno per l'adeguamento al Codice privacy e la realizzazione e manutenzione delle misure di sicurezza delle informazioni.

La realizzazione di un SGSI e la sua integrazione con quanto descritto nel presente Quaderno non assicura la completa conformità al Codice privacy né ai diversi Provvedimenti emanati dal Garante; può tuttavia costituire un valido modo per dimostrare di aver affrontato in modo coerente e sistematico l'individuazione e la gestione delle misure di sicurezza minime e idonee (di cui agli artt. 31-36 del Codice).

E' importante ricordare che *la protezione dei dati personali*, come regolata dalle disposizioni contenute nel D.lgs. 196/03, *non attiene solamente alla gestione della sicurezza dei dati personali* per garantirne riservatezza, integrità e disponibilità, ma anche alla definizione di specifiche modalità di trattamento che ne determinano la liceità. In questo Quaderno sono presi in considerazione ed approfonditi gli aspetti che riguardano la sicurezza dei dati personali.

In questo documento è utilizzato il termine "azienda" al posto di altri termini più generali (quali "organizzazione", "ente" o "impresa") perché ritenuto di più facile comprensibilità. Questo non deve indicare una limitazione d'uso del Quaderno per le sole aziende private.

2 Sistemi di gestione della sicurezza delle informazioni

2.1 Introduzione ai sistemi di gestione

Il modello noto come "Plan-Do-Check-Act" (PDCA), descritto anche in [3], è caratterizzato dalla ripetizione ciclica delle fasi di pianificazione, realizzazione, verifica e adozione di azioni ed è orientato al miglioramento continuo. Esso si colloca alla base di tutti i moderni sistemi di gestione, da quelli per la qualità a quelli per la sicurezza delle informazioni.

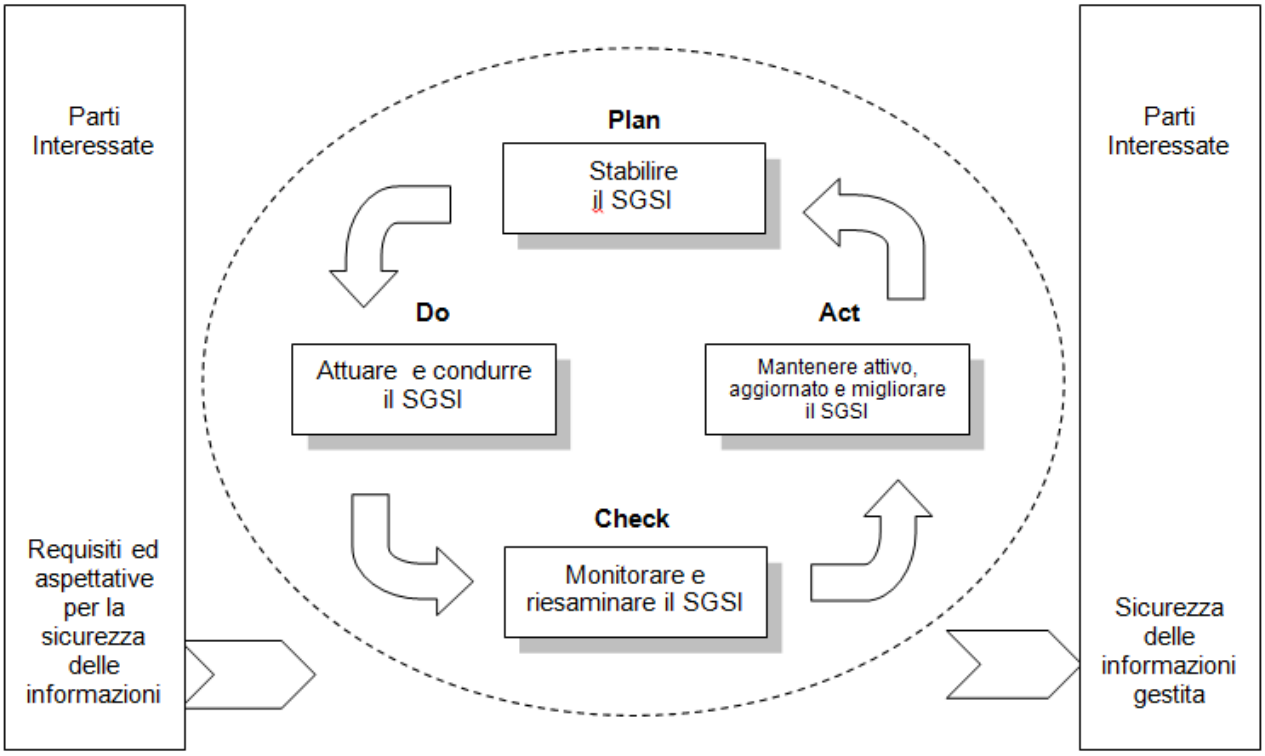

Figura 1 - Modello PDCA

I sistemi di gestione sono finalizzati a stabilire delle politiche e degli obiettivi e a operare per il loro raggiungimento nel tempo, anche attraverso la modifica delle attività aziendali. Un sistema di gestione, perché sia tale, richiede che le attività siano strutturate in una serie di processi opportunamente correlati tra loro, in modo da organizzare correttamente e coerentemente quanto necessario per raggiungere gli obiettivi stabiliti.

L'applicazione di un sistema di gestione, a maggior ragione in contesti aziendali snelli e flessibili, può e deve essere un fattore abilitante e non un fattore debilitante. Per forza di cose esso richiede degli sforzi e delle attenzioni, ma questi devono essere coerenti ai rischi d'impresa e bilanciare l'efficacia con l'efficienza nella gestione delle informazioni, inclusi i dati personali, in conformità ai requisiti normativi e alle aspettative delle parti interessate.

Un Sistema per la gestione della sicurezza delle informazioni, quindi, può e dovrebbe includere i requisiti per la sicurezza dei dati personali, di cui fanno parte quelli stabiliti per legge. Nel caso di sistemi che intendono essere conformi alla UNI CEI ISO/IEC 27001, tale scelta non è opzionale.

2.2 Elementi fondamentali per la gestione dei dati personali

La gestione dei dati personali, come già detto, è regolata in Italia da un insieme di normative e provvedimenti emessi sia dal Parlamento sia dal Garante per la Privacy. Questi documenti fissano dei requisiti senza però inserirli in un quadro organico, con il rischio concreto che i principi stessi a cui si ispirano vadano disattesi anche in caso di loro completo adempimento.

Per questa ragione sono elencati di seguito alcuni elementi considerati fondamentali per stabilire un quadro organico che garantisca la coerenza dell'approccio seguito con i principi sottostanti la tutela dei dati personali:

- coordinamento delle diverse aree aziendali in materia di gestione dei dati personali;
- definizione di regole interne per la gestione dei dati personali, da rispettare nelle procedure, formalizzate o meno, seguite nell'operatività;
- chiara e precisa definizione dei trattamenti di dati personali, specificandone le finalità, le modalità di trattamento e le categorie di interessati e predisponendo le relative informative e notifiche, se necessario;
- gestione delle attribuzioni di responsabilità interne ed esterne e delle comunicazioni rese da esse necessarie;
- controllo e dimostrabilità sia delle azioni sia dell'approccio complessivo mantenuto per la gestione dei dati personali.

2.3 Sistema di gestione

Sono di seguito riportate le raccomandazioni, suddivise per fase del ciclo PDCA, da tenere in considerazione per raggiungere e mantenere nel tempo un'adeguata gestione della sicurezza delle informazioni, tra cui i dati personali.

2.3.1 Plan

2.3.1.1 Ruoli e responsabilità

Il primo passaggio propedeutico alla creazione di un Sistema per la gestione della sicurezza delle informazioni, compresi i dati personali, una volta definita in modo preliminare la sua estensione rispetto ai processi aziendali, consiste nell'individuare un membro della Direzione con adeguate competenze relative al tema della privacy e della sicurezza delle informazioni, a cui assegnare la responsabilità di coordinamento (d'ora innanzi citato come *Responsabile del sistema* o del SGSI).

Questa figura, a seconda delle dimensioni e della complessità dei trattamenti di dati personali e dell'azienda, può essere dedicata completamente o meno a questo compito. Può però capitare, specie nelle PMI, che non esistano all'interno dell'azienda figure di competenza adeguata. In questo caso si presentano due possibili alternative:

- assegnazione della responsabilità ad una persona interna, che si appoggia, anche con continuità, ad un esperto esterno;
- assegnazione della responsabilità ad un esperto esterno, che opera con continuità e piena visibilità all'interno dell'azienda.

Qualunque sia la scelta adottata, non dovrà mancare al Responsabile il pieno sostegno della Direzione e la necessaria autorità per garantire una corretta ed efficace gestione del sistema. Il primo passo è la formalizzazione della sua nomina.

Va sottolineato che non dovrà mai mancare da parte della Direzione, che ha comunque la titolarità dei trattamenti, un adeguato e visibile supporto anche economico alle azioni proposte dal Responsabile del sistema, un continuo monitoraggio del suo operato e una costante condivisione degli obiettivi e delle finalità del SGSI.

In molte realtà, è d'uso associare alla nomina di Responsabile del sistema la nomina a Responsabile del trattamento. Poiché al Responsabile del sistema potrebbe non essere assegnato alcun particolare trattamento, tale scelta può essere intesa come non prevista dal Codice. Cionondimeno, il comma 2 dell'articolo 29, in virtù dell'elevato livello di responsabilità assegnato al soggetto, rende giustificata la prima interpretazione. Si ricorda inoltre che la nomina del Responsabile del sistema, anche ai sensi del comma 3 dell'articolo 29 del Codice, non impedisce la nomina di altri Responsabili del trattamento, mediante opportuna suddivisione dei compiti.

Ulteriori responsabilità, ricoperte dal Responsabile di sistema in contesti aziendali di ridotte dimensioni o da personale a suo supporto, possono essere introdotte in base alla dimensione e alla complessità dei trattamenti effettuati e comprendono:

- verifica periodica (audit interno) dello stato di conformità del SGSI;
- gestione della documentazione del SGSI e del suo aggiornamento;
- supporto all'applicazione delle procedure del SGSI
- erogazione di interventi di formazione e consapevolezza;
- gestione delle comunicazioni in materia di privacy con gli interessati;
- risposta alle richieste di informazione, cancellazione o modifica di dati personali da parte degli interessati (esterni e interni all'azienda);
- sorveglianza dei nuovi obblighi normativi e delle sentenze in materia.

Gli altri ruoli aziendali normalmente coinvolti nella sicurezza delle informazioni sono il responsabile del Sistema informativo, il responsabile dell'Ufficio personale e, nel caso ci siano trattamenti di dati personali che presentano rischi specifici o per i quali è richiesta la notifica (ad es. carta fedeltà, gestione automezzi con GPS, ecc.), i responsabili delle aree aziendali coinvolte da tali trattamenti (eventualmente anche loro nominati Responsabili di tali trattamenti, ai sensi dell'art. 29 del Codice).

E' importante sottolineare che non devono necessariamente essere coinvolti tutti i responsabili delle funzioni aziendali, ma solo coloro che sono specificamente dedicati a garantire, in vari modi e con diverse professionalità, la sicurezza delle informazioni e la protezione dei dati personali. In altri termini, l'*organigramma della sicurezza* non deve necessariamente replicare la struttura dell'organigramma aziendale. E' indispensabile però che il Responsabile del sistema sia un efficace canale di comunicazione con la Direzione aziendale che, a sua volta, deve fornire tutto il proprio appoggio affinché i diversi Responsabili dei trattamenti abbiano risorse e autorità adeguate a garantire un efficiente funzionamento del sistema.

2.3.1.2 Documentazione per la sicurezza delle informazioni

Definire e documentare una *Politica per la gestione della sicurezza delle informazioni e dei dati personali*, finalizzata a definire gli indirizzi e le regole generali da applicare in materia all'interno di tutta l'azienda è la base di partenza di tutto il sistema di gestione. La politica, sintetica ed estremamente comprensibile nella sua stesura, deve includere:

- una definizione di cosa si intende come *sicurezza delle informazioni*, dei suoi obiettivi e della sua importanza, in linea con gli obiettivi aziendali e la normativa sulla privacy;

- un indirizzo generale e i principi di azione concernenti la protezione dei dati personali;
- la descrizione dei processi necessari alla gestione della sicurezza delle informazioni e dei dati personali;
- la formalizzazione di ruoli e responsabilità;
- i criteri rispetto ai quali ponderare i rischi.

Tale Politica deve essere riesaminata almeno con cadenza annuale e venire approvata dalla Direzione affinché sia garantito e visibile il necessario appoggio.

Alla Politica deve essere associato un *Elenco della documentazione aziendale* (procedure) rilevante sul tema.

Il Documento programmatico per la sicurezza, se già presente, può essere convenientemente aggiornato e inserito nel suddetto elenco, anche se non più richiesto dall'attuale normativa privacy. Si raccomanda comunque di descrivere in un documento i meccanismi di sicurezza implementati.

Le procedure operative che guidano in maniera puntuale l'attuazione di quanto indicato nella politica possono essere definite in modo informale nelle aziende di più ridotte dimensioni mentre, con il crescere del numero delle persone, delle sedi e della complessità del business, aumenta la necessità di averle formalizzate all'interno di un unico documento o come oggetti separati per un più facile aggiornamento. Anche tali procedure dovrebbero essere riesaminate con cadenza annuale, in occasione degli audit interni.

I temi da trattare nelle procedure sono legati alla realtà aziendale e ai rischi che incombono su di essa. Quelli più frequentemente indirizzati sono:

- gestione della documentazione;
- gestione degli asset;
- controllo degli accessi fisici e logici;
- gestione delle utenze;
- gestione degli incidenti;
- back-up e ripristino;
- modalità di conduzione degli audit interni.

E' opportuno sottolineare come le procedure siano funzionali all'esecuzione di azioni specifiche, sovente legate a flussi operativi. In tale prospettiva possono anche essere formalizzate in modo estremamente schematico indicando la sequenza delle attività e i corrispondenti ruoli degli attori coinvolti.

Si ricorda che l'Allegato B del D.lgs. 196/03 richiede esplicitamente la descrizione scritta di alcune attività: si raccomanda di includerle nelle procedure sopra elencate.

Si raccomanda inoltre di documentare per iscritto le regole per la corretta gestione delle informazioni e dei dati personali e degli strumenti aziendali connessi al loro trattamento. Esse dovrebbero essere mantenute aggiornate e distribuite a tutti gli incaricati o ai soggetti interessati dove rilevante. Tali regole, aggregabili anche in un solo documento, possono includere:

- le modalità di classificazione e etichettatura dei dati (vanno ad esempio identificati i dati personali di natura sensibile o le informazioni rilevanti per garantire la loro disponibilità, integrità o riservatezza) considerando i diversi supporti (per esempio, cartacei ed elettronici) su cui possono essere mantenuti;

- le regole di trattamento di informazioni e dati personali lungo tutto il loro ciclo di vita;
- le regole di accesso fisico e logico e le relative richieste ed assegnazioni dei diritti di accesso alle informazioni;
- le regole per l'uso di Internet e della posta elettronica;
- le regole per l'uso di computer, telefoni e altre tecnologie in dotazione.

Le suddette regole dovrebbero trovare applicazione nelle procedure operative.

2.3.1.3 Consolidamento dell'ambito

La definizione iniziale dei processi aziendali da considerarsi in ambito, effettuata prima dell'assegnazione dei ruoli e delle responsabilità, deve essere consolidata, sotto la guida del Responsabile del sistema, con maggiore precisione ed approfondimento.

Prima di effettuare le azioni successive è necessario infatti definire e documentare schematicamente le informazioni, tra cui i dati personali (indicando se sensibili), e i relativi trattamenti, in termini di processi, persone coinvolte e strumenti utilizzati.

Questo lavoro permetterà ad ogni responsabile di avere la visione d'insieme necessaria per poter gestire correttamente le informazioni, tra cui i dati personali, trattati dalla sua area di responsabilità secondo le indicazioni della politica e con il coordinamento del responsabile del SGSI.

Dovrebbe essere garantito l'aggiornamento, su base periodica e in occasione di modifiche organizzative, degli ambiti di trattamento individuati.

2.3.1.4 Analisi del Rischio

L'analisi del rischio può avere diverse finalità, tra le quali: determinare i rischi strategici di un'azienda, quelli finanziari, quelli sulla sicurezza dei lavoratori e, ovviamente, quelli sulla sicurezza dei dati e delle informazioni. In questo documento si tratta di quest'ultima. E' comunque necessario avere ben chiara tale finalità, in modo da individuare i corretti metodi da seguire e non rendere il lavoro troppo oneroso perché non ben finalizzato.

Per le finalità di questo documento non si ritiene utile proporre alcun modello specifico per condurre l'analisi del rischio. Alcuni modelli sono accompagnati da software acquistabili sul mercato, altri si basano su semplici formulari su fogli di calcolo. La scelta del modello dipende dall'azienda che lo vuole adottare: le piccole e medie imprese sceglieranno modelli semplici ed economici, mentre quelle più grandi dovranno sceglierne di più complessi e, probabilmente, costosi. ENISA ha comunque effettuato un inventario dei principali oggetti utilizzati in questo ambito [5].

Per quanto riguarda l'analisi del rischio per la sicurezza delle informazioni, dovrebbero essere seguiti i seguenti passi:

1. *Stabilire il contesto:* descrivere lo scenario di riferimento (ossia, l'azienda analizzata specificando le attività svolte, le responsabilità designate, i confini fisici e informatici, le relazioni con terze parti, le tecnologie in uso) utilizzando anche quanto definito nel paragrafo precedente in merito al consolidamento dell'ambito;
2. *Identificare i rischi*:
    - elencare tutte le minacce che incombono sulle informazioni e valutare la loro verosimiglianza di accadimento: l'esperienza della Direzione e dei responsabili dei sistemi informativi normalmente rende veloce questo compito (possono considerare

casi già successi nella stessa azienda o in imprese vicine geograficamente o dello stesso settore merceologico);
- identificare le possibili conseguenze di ogni minaccia (per esempio, quale potrebbe essere il danno per l'azienda nel caso in cui si manifestino dei virus sulla rete aziendale o nel caso in cui si danneggino dei file contenenti dati personali o i documenti dei progetti);
- stabilire il livello di vulnerabilità o, viceversa, la robustezza delle misure di sicurezza (in particolare quelle richieste dalla normativa applicabile); questo ultimo passaggio richiede alle persone coinvolte la massima oggettività nell'attribuzione dei valori, senza sottostimare eventuali carenze o sovrastimarle per ottenere più risorse economiche per i progetti di loro riduzione;

3. *Calcolare i livelli dei rischi:* combinare la verosimiglianza delle minacce, le possibili conseguenze e il livello di vulnerabilità, in modo da assegnare dei valori per ciascun rischio.

Per l'identificazione e valutazione dei rischi è necessario basarsi quanto più possibile su scale di valori stabilite in precedenza, anche per garantire la ripetibilità del processo..

2.3.1.5 Trattamento del rischio

Affinché l'analisi del rischio sia poi utile al processo decisionale, deve essere seguita dai seguenti passi:

1. *Ponderare i rischi:* valutare se i rischi individuati sono accettabili;
2. *Identificare e ponderare le opzioni di trattamento dei rischi*: a fronte dei rischi valutati come inaccettabili, è necessario individuare le possibili azioni da intraprendere e valutarne la fattibilità (per esempio, in alcuni casi le azioni potrebbero introdurre più rischi di quelli attuali oppure avere costi eccessivi);
3. *Pianificare il trattamento dei rischi*: stabilire scadenze, budget e responsabilità per le azioni che si è deciso di intraprendere.

Le azioni di miglioramento individuate devono essere elencate in un unico documento, detto *Piano di trattamento dei rischi*, per avere un quadro d'insieme delle attività in corso. E' importante mantenere il collegamento tra azioni intraprese e minacce contrastate, anche al fine di fornire una giustificazione per le scelte compiute.

Le misure di sicurezza dovranno essere controllate nel tempo; in particolare, ne dovrà essere verificata la corretta realizzazione e, periodicamente, il loro buon funzionamento, anche attraverso attività di manutenzione ordinaria o straordinaria (per esempio, a seguito di incidenti).

2.3.2 Do

2.3.2.1 Nomine e profili

L'allocazione delle responsabilità per la sicurezza delle informazioni, così come le nomine richieste dalla normativa in materia di Privacy, devono essere mantenute aggiornate in modo che tutti gli inserimenti di nuovo personale, i cambiamenti di ruolo e le dimissioni siano immediatamente e correttamente riflessi nel quadro della gestione delle informazioni e dei dati personali dell'azienda.

In particolare, si deve curare la corretta attribuzione delle nomine di:

- responsabili per il trattamento dei dati personali.
- incaricati per il trattamento dei dati personali;

- amministratori di sistema (ai sensi di [2]).

Si osservi che le nomine possono riguardare sia personale con contratto da dipendente, sia altro personale con rapporto di lavoro regolamentato da altre forme contrattuali, inclusa quella di stage.

Normalmente, in una azienda l'area delle risorse umane e quella dei sistemi informativi si occupano di gestire questo processo nel tempo, tenendo anche conto dei profili di accesso fisico e logico alle informazioni. Tali profili sono creati in base all'area aziendale di appartenenza, ai dati da essa trattati e alla funzione svolta dalla singola persona, sempre rispettando il principio di conferire il minimo livello di accesso necessario per permettere di svolgere le proprie mansioni. E' opportuno effettuare un riesame periodico, con cadenza almeno annuale, della correttezza delle nomine e dei corrispondenti profili di accesso.

Per facilitare la gestione delle nomine e dei profili di accesso, è possibile mantenerne un elenco (in forma di documento o di database) in cui sono registrati tutti i ruoli assegnati al personale. Vanno considerate secondo gli stessi principi le nomine a Responsabile di trattamento e i rapporti con altri Titolari autonomi (quali ad es. fornitori di servizi di data center o di videosorveglianza). Con queste terze parti è opportuno attivare un canale di comunicazione necessario ad impartire (nel caso di Responsabili esterni) o concordare (nel caso di Titolari autonomi) le misure di corretto trattamento dei dati e per coordinare al meglio le azioni volte a garantirne la sicurezza.

2.3.2.2 Informative

Ad ogni trattamento di dati personali deve essere associata una informativa indirizzata agli interessati, che può essere realizzata in forme diverse (con maggiore o minore dettaglio) e che lega il trattamento ad una specifica finalità.

Le informative sono i principali documenti da creare e mantenere aggiornati in relazione all'acquisizione dei dati personali. Le necessità di trasmissione di nuove informative agli interessati devono essere valutate di conseguenza all'evoluzione dei trattamenti.

2.3.2.3 Formazione e consapevolezza

Il personale deve essere sempre consapevole delle corrette modalità di trattamento delle informazioni e dei dati personali e dei rischi che incombono su di essi.

Oltre a predisporre una formazione iniziale sul tema (ai neo-assunti), l'azienda deve periodicamente predisporre delle sessioni di aggiornamento, anche attraverso strumenti elettronici, che permettano di ricordare i concetti inizialmente espressi e di allinearli all'evoluzione del contesto aziendale.

Necessità puntuali di formazione specifica, in particolar modo per il personale con responsabilità in merito di sicurezza delle informazioni, devono inoltre essere rilevate e fatte confluire nei piani di formazione dell'azienda.

Iniziative quali articoli interni, poster o concorsi, possono utilmente complementare il mantenimento della consapevolezza sulle nozioni di corretta gestione delle informazioni e dei dati personali, contribuendo anche a mantenere alta la cultura sulla sicurezza in azienda. ENISA ha recentemente prodotto e distribuito materiale funzionale a questo obiettivo in tutte le lingue dell'Unione Europea [7].

2.3.3 Check

2.3.3.1 Verifiche interne

Con cadenza periodica, personale esterno a quello coinvolto nelle operazioni di trattamento delle informazioni (il responsabile del SGSI, il suo staff oppure la funzione di audit interna o, eventualmente, esterna) dovrebbe effettuare delle verifiche sulla correttezza del trattamento delle informazioni e dei dati personali, sul livello di conformità delle attività effettuate rispetto alle regole e procedure stabilite dall'azienda e, più in generale, sull'efficacia del SGSI. Queste verifiche dovrebbero inoltre includere la valutazione della conformità rispetto alla normativa cogente con particolare attenzione a quella relativa alla privacy.

Nell'ambito dell'esecuzione di tali verifiche è necessario includere quelle sull'operato degli amministratori di sistema, in modo da controllare la sua rispondenza alle misure organizzative e tecniche stabilite per i trattamenti dei dati personali, così come richiesto dalla normativa vigente [2].

I risultati delle attività di verifica dovrebbero essere documentati e utilizzati come base per decidere quali azioni mettere in atto per rimediare eventuali criticità riscontrate.

La Direzione stessa può essere utilmente coinvolta nella presentazione di tali attività di verifica e in periodiche relazioni sulla sicurezza delle informazioni all'interno dell'azienda.

2.3.4 Act

2.3.4.1 Monitoraggio azioni, raccolta e riesame delle proposte di miglioramento

Durante il normale ciclo di vita del SGSI possono emergere delle opportunità per migliorare la gestione delle informazioni e dei dati personali o aggiornarla a nuovi sviluppi. Dovrebbero quindi essere fissati dei meccanismi, controllati del Responsabile del sistema, per poter identificare, valutare, stabilire, attuare e controllare azioni di miglioramento del sistema.

Aspetti significativi per il miglioramento continuo possono emergere dalle analisi degli incidenti, dai risultati delle verifiche interne ma anche dalle semplici attività di monitoraggio della sicurezza delle informazioni o da suggerimenti del personale.

Per ogni azione definita dovrebbero essere stabiliti i responsabili e le scadenze. Le decisioni dovrebbero essere documentate e lo stato di avanzamento delle azioni monitorato.

3 Bibliografia e autori

[1]. D.lgs. 196/2003 (Codice in materia di protezione dei dati personali), e successive modifiche e integrazioni (questo documento è aggiornato alle modificazioni e integrazioni introdotte dal D.lgs. 69/2012

[2]. Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema – Provvedimento a carattere generale del Garante per la protezione dei dati personali del 27 novembre 2008, aggiornato in base al successivo provvedimento del 25 giugno 2009.

[3]. UNI CEI ISO/IEC 27001:2006 - Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni – Requisiti

[4]. ISO/IEC 27002:2005 - Information technology -- Security techniques - Code of practice for information security management

[5]. ENISA; Inventory of Risk Management / Risk Assessment Methods; http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory

[6]. ENISA; Material for raising information security awareness; http://www.enisa.europa.eu/activities/cert/security-month/material

I membri del Gruppo di Lavoro UNINFO sulla serie di norme ISO/IEC 27000 che hanno contribuito alla stesura del presente quaderno sono:

Mauro Bert, Schmidt Consulting – *Consulente Senior per Sicurezza delle Informazioni e Privacy*

Cesare Gallotti – *Consulente per la Sicurezza delle Informazioni, LA ISO/IEC 27001, LA ISO 9001, LA ISO/IEC 20000, CISA, ITIL Expert, CBCI*

Fabio Guasconi, @ Mediaservice.net – *Senior Security Advisor, Presidente UNINFO SC27, LA ISO/IEC27001, CISA, CISM, ITIL, ISFS, PCI-QSA*

Marco Simoncini, ENAV – *Responsabile policy e procedure SIG*, PMP, *ITIL, LA ISO 9001, LA ISO 27001, LA ISO 20000*

Con un sentito ringraziamento per l'opera di revisione ad **Attilio Rampazzo**.

4 Allegati

4.1 Workflow

Si riporta di seguito una sintesi dei principali punti illustrati nel presente documento, al fine di avere una comoda lista di riscontro per la corretta realizzazione di un SGSI. Sono riportati in corsivo i punti non sempre necessari per delle aziende di piccole o medie dimensioni:

a) definire i processi aziendali su cui sviluppare il sistema per la gestione della sicurezza delle informazioni (cfr. 2.3.1.1);
b) individuare un Responsabile del sistema che coordini la sicurezza delle informazioni (cfr. 2.3.1.1);
c) definire le altre responsabilità per la sicurezza delle informazioni (cfr. 2.3.1.1);
d) definire e diffondere una politica per la sicurezza delle informazioni (cfr. 2.3.1.2);
e) definire e diffondere le procedure per la sicurezza delle informazioni (cfr. 2.3.1.2);
f) definire e diffondere le regole per la corretta gestione delle informazioni e dei dati personali (cfr. 2.3.1.2);
g) consolidare i flussi delle informazioni aziendali (cfr. 2.3.1.3);
h) effettuare un'analisi del rischio per la sicurezza delle informazioni (cfr. 2.3.1.4);
i) definire ed attuare le azioni di trattamento del rischio rese evidenti dall'analisi (cfr. 2.3.1.5);
j) riesaminare periodicamente e mantenere aggiornate le nomine e i profili di accesso alle informazioni (cfr. 2.3.2.1);
k) mantenere aggiornate le informative per il trattamento di dati personali (cfr. 2.3.2.2);
l) includere la formazione sulla sicurezza delle informazioni ai programmi di formazione aziendali (cfr. 2.3.2.3);
m) realizzare programmi per la sensibilizzazione del personale in materia di sicurezza delle informazioni (cfr. 2.3.2.3);
n) effettuare delle verifiche periodiche sull'efficacia del SGSI (cfr. 2.3.3.1);
o) informare periodicamente la Direzione sullo stato della sicurezza delle informazioni (cfr. 2.3.3.1);
p) implementare meccanismi per abilitare un miglioramento continuo della sicurezza delle informazioni (cfr. 2.3.4.1).

4.2 Corrispondenze tra ISO/IEC 27002 e Normativa privacy

La seguente tabella permette di associare, quando possibile, ad ogni controllo della norma ISO/IEC 27002:2005 le relative misure di sicurezza della normativa privacy.

Ciò permette di trovare nei controlli della ISO/IEC 27002 una chiave interpretativa delle misure da applicare, nonché utili indicazioni per una loro adeguata attuazione.

Come già annunciato nella premessa al Quaderno, le norme a cui si fa riferimento sono le seguenti:

- D.lgs 196/2003, "Codice in materia di protezione dei dati personali" e successive modifiche e integrazioni (questo documento è aggiornato alle modificazioni e integrazioni introdotte dal D.lgs. 69/2012);
- Allegato B del D.lgs 196/2003;
- Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema – Provvedimento a carattere generale del Garante per la protezione dei dati personali del 27 novembre 2008, aggiornato in base al successivo provvedimento del 25 giugno 2009.

Va specificato che sono stati presi in considerazione solo gli articoli e le prescrizioni applicabili ad una generica azienda, tralasciando pertanto tutto ciò che si riferisce a Titolari che operano in particolari settori, come ad esempio le telecomunicazioni o la sanità.

Nella colonna "Testo" vengono, quando necessario e per chiarezza, identificati i commi degli articoli che in modo specifico rimandano al controllo individuato.

Controllo		*Misura*		*Testo*	*Commenti*
A.5	Politica per la sicurezza				
A.5.1	Politica per la sicurezza delle informazioni				
A.5.1.1	Documento relativo alla politica per la sicurezza delle informazioni	CP art. 31	Obblighi di Sicurezza		L'art. 31 fornisce, in termini generali, indicazioni circa la politica di sicurezza da attuare nei confronti dei dati personali
A.5.1.2	Riesame della politica per la sicurezza delle informazioni	N.A.			
A.6	Organizzazione della sicurezza delle informazioni				
A.6.1	Organizzazione interna				
A.6.1.1	Impegno della Direzione per la sicurezza delle informazioni	CP art. 28	Titolare del Trattamento		
A.6.1.2	Coordinamento della sicurezza delle informazioni	N.A.			
A.6.1.3	Assegnazione delle responsabilità di sicurezza delle informazioni	CP art. 29	Responsabile del trattamento	in particolare: 2. Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. 4. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.	
		CP art. 30 comma 1	Incaricati del trattamento	1. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite	

Controllo		*Misura*		*Testo*	*Commenti*
		AdS punto 2 lett. b	Designazioni individuali	b) La designazione quale amministratore di sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.	
A.6.1.4	Processo di autorizzazione per le strutture di elaborazione delle informazioni	CP art. 3	Principio di necessità nel trattamento dei dati		
A.6.1.5	Accordi di riservatezza	CP art. 29	Responsabile del trattamento		
		CP art. 30	Incaricati del trattamento		
A.6.1.7	Contatti con gruppi di interesse specifico	N.A.			
A.6.1.8	Riesame indipendente della sicurezza delle informazioni	N.A.			
A.6.2	Parti esterne				
A.6.2.1	Identificazione dei rischi derivanti da parti esterne	CP art. 29	Responsabile del trattamento		E' bene che la scelta di trasferire a parti esterne (in qualità di titolari, responsabili o incaricati) un trattamento sia accompagnata da un'adeguata analisi dei rischi
		CP art. 30	Incaricati del trattamento		
		CP artt. 42 - 45	Trasferimento dei dati all'estero		
A.6.2.2	Sicurezza nel trattare con i clienti	N.A.			
A.6.2.3	Sicurezza negli accordi con terze parti	CP art. 29 comma 5	Responsabile del trattamento	5. Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.	

Controllo		*Misura*		*Testo*	*Commenti*
		All.B punto 25	Misure di tutela e garanzia		
		AdS punto 2 lett. d	Servizi in outsourcing	d) Nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare o il responsabile esterno devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.	
A.7	Gestione dei beni				
A.7.1	Responsabilità dei beni				
A.7.1.1	Inventario dei beni	CP art. 34 comma 1 lett. d	Trattamenti con strumenti elettronici	d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;	Per assicurare che i trattamenti di dati personali siano corretti e legittimi ne dovrà prima di tutto essere fatto un inventario
A.7.1.2	Responsabilità dei beni	CP Art. 29	Responsabile del trattamento		
A.7.1.3	Utilizzo accettabile dei beni	N.A.			
A.7.2	Classificazione delle Informazioni				
A.7.2.1	Linee guida per la classificazione	CP art. 4	Definizioni		
A.7.2.2	Etichettatura e trattamento delle informazioni	CP art. 11 comma 1	Modalità di trattamento e requisiti dei dati	1. I dati personali oggetto di trattamento sono: a) trattati in modo lecito e secondo correttezza; b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre	

Controllo		*Misura*		*Testo*	*Commenti*
				operazioni del trattamento in termini compatibili con tali scopi; c) esatti e, se necessario, aggiornati; d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.	
A.8	Sicurezza delle risorse umane				
A.8.1	Primo impiego				
A.8.1.1	Ruoli e Responsabilità	CP art. 29	Responsabile del trattamento		
		CP art. 30	Incaricati del trattamento		
		AdS punto 2 lett. c	Elenco degli Amministratori di Sistema		
		AdS punto 2 lett. d	Servizi in outsourcing	d) Nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare o il responsabile esterno devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.	
A.8.1.2	Profilo del personale (Screening)	AdS punto 2 lett. a	Valutazione delle caratteristiche soggettive	a) L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.	

Controllo		*Misura*		*Testo*	*Commenti*
A.8.1.3	Termini e condizioni di impiego	CP art. 29	Responsabile del trattamento		
		CP art. 30	Incaricati del trattamento		
A.8.2	Durante l'impiego				
A.8.2.1	Responsabilità della direzione	N.A.			
A.8.2.2	Consapevolezza, formazione e addestramento per la sicurezza delle informazioni	N.A.			
A.8.2.3	Processi disciplinari	N.A.			
A.8.3	Interruzione o variazione d'impiego				
A.8.3.1	Responsabilità di interruzione del rapporto di lavoro	N.A.			
A.8.3.2	Restituzione dei beni	N.A.			
A.8.3.3	Rimozione dei diritti di accesso	All.B punto 14	Sistema di autorizzazione		
		All.B punto 15	Altre misure di sicurezza		
A.9	Sicurezza fisica e ambientale				
A.9.1	Aree sicure				
A.9.1.1	Perimetro di sicurezza fisica	CP art. 31	Obblighi di Sicurezza		
		All.B punto 24	Ulteriori misure in caso di trattamento di dati sensibili o giudiziari		

Controllo		*Misura*		*Testo*	*Commenti*
A.9.1.2	Controlli di accesso fisico	CP art. 31	Obblighi di Sicurezza		
		All.B punto 29	Trattamento senza l'ausilio di strumenti elettronici		
A.9.1.3	Rendere sicuri uffici, locali e strutture	CP art. 31	Obblighi di Sicurezza		
A.9.1.4	Protezione contro minacce esterne e ambientali	CP art. 31	Obblighi di Sicurezza		
A.9.1.5	Lavoro in aree sicure	N.A.			
A.9.1.6	Aree pubbliche di accesso, carico e scarico	N.A.			
A.9.2	Sicurezza delle apparecchiature				
A.9.2.1	Disposizione delle apparecchiature e loro protezione	CP art. 34 comma 1 lettera e	Trattamenti con strumenti elettronici	e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;	
A.9.2.2	Infrastrutture di supporto	N.A.			
A.9.2.3	Sicurezza dei cablaggi	N.A.			
A.9.2.4	Manutenzione delle apparecchiature	N.A.			
A.9.2.5	Sicurezza delle apparecchiature all'esterno dell'organizzazione	N.A.			
A.9.2.6	Dismissione o riutilizzo sicuri delle apparecchiature	All.B punto 22	Ulteriori misure in caso di trattamento di dati sensibili o giudiziari		

Controllo		*Misura*		*Testo*	*Commenti*
A.9.2.7	Trasferimento di proprietà	All.B punto 21	Ulteriori misure in caso di trattamento di dati sensibili o giudiziari		
		All.B punto 24	Ulteriori misure in caso di trattamento di dati sensibili o giudiziari		
A.10	Gestione delle comunicazioni e dell'operatività				
A. 10.1	Procedure operative e responsabilità				
A. 10.1.1	Procedure operative documentate	All.B punto 4	Sistema di autenticazione informatica		
		All.B punto 9	Sistema di autenticazione informatica		
		All.B punto 10	Sistema di autenticazione informatica		
		All.B punto 18	Altre misure di sicurezza		
		All.B punto 21	Ulteriori misure in caso di trattamento di dati sensibili o giudiziari		

Controllo		*Misura*		*Testo*	*Commenti*
		All.B punto 27	Trattamenti senza l'ausilio di strumenti elettronici	Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.	Le istruzioni scritte si ritrovano al punto 28 "Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate"
A. 10.1.2	Tenuta sotto controllo dei cambiamenti	N.A.			
A. 10.1.3	Separazione dei compiti	N.A.			
A. 10.1.4	Separazione delle strutture di sviluppo, di test e operative	N.A.			
A. 10.2	Gestione dell'erogazione di servizi di terze parti.				
A.10.2.1	Erogazione di servizi	CP art. 29 punto 4	Responsabile del trattamento	4. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.	
		CP art. 32bis comma 8	Adempimenti conseguenti ad una violazione di dati personali	8. Nel caso in cui il fornitore di un servizio di comunicazione elettronica accessibile al pubblico affidi l'erogazione del predetto servizio ad altri soggetti, gli stessi sono tenuti a comunicare al fornitore senza indebito ritardo tutti gli eventi e le informazioni necessarie a consentire a quest'ultimo di effettuare gli adempimenti di cui al presente articolo.	

Controllo		*Misura*		*Testo*	*Commenti*
A.10.2.2	Monitoraggio e riesame dei servizi di terze parti	AdS punto 2 lett. e	Verifica delle attività	e) L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento o dei responsabili, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.	
		CP art. 29 punto 5	Responsabile del trattamento	5. Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.	
		CP art. 34 comma 1 lettera d	Trattamenti con strumenti elettronici	d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici.	
A.10.2.3	Gestione dei cambiamenti dei servizi di terza parte				
A.10.3	Pianificazione e approvazione dei sistemi				
A.10.3 .1	Gestione della capacità	N.A.			
A.10.3 .2	Approvazione dei sistemi	N.A.			
A.10.4	Protezione contro software dannosi e codici autoeseguibili				
A.10.4.1	Controlli contro software dannosi	CP art. 34 comma 1 lettera e	Trattamenti con strumenti elettronici	e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici.	

Controllo		*Misura*		*Testo*	*Commenti*
		All.B punto 16	Altre misure di sicurezza	I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.	
A.10.4.2	Controlli contro codici autoeseguibili	N.A.			
A.10.5	Back-up				
A.10.5.1	Back-up delle informazioni	CP art. 31	Obblighi di Sicurezza		
		CP art. 34 comma 1 lettera f	Trattamenti con strumenti elettronici	f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;	
		All.B punto 18	Altre misure di sicurezza		
		All.B punto 23	Ulteriori misure in caso di trattamento di dati sensibili o giudiziari		
A.10.6	Gestione della sicurezza della rete				
A.10.6.1	Controlli di rete	CP art. 31	Obblighi di Sicurezza		
A.10.6.2	Sicurezza dei servizi di rete	CP art. 34 lettera h	Trattamenti con strumenti elettronici	h. adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.	
A.10.7	Trattamento dei supporti				
A.10.7.1	Gestione dei supporti rimovibili	All.B punto 21	Ulteriori misure in caso di trattamento di dati sensibili o giudiziari		

Controllo		*Misura*		*Testo*	*Commenti*
A.10.7.2	Dismissione dei supporti	All.B punto 22	Ulteriori misure in caso di trattamento di dati sensibili o giudiziari		
A.10.7.3	Procedure di trattamento delle informazioni	CP art. 11 comma 1	Modalità di trattamento e requisiti dei dati	1. I dati personali oggetto di trattamento sono: a) trattati in modo lecito e secondo correttezza; b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; c) esatti e, se necessario, aggiornati; d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.	
A.10.7.4	Sicurezza della documentazione di sistema	N.A.			

Controllo		***Misura***		***Testo***	***Commenti***
A.10.8	Trasmissione delle informazioni				
A.10.8.1	Politiche e procedure di trasmissione delle informazioni	CP artt. 42 - 45	Trasferimento dei dati all'estero		
		All.B punto 24	Ulteriori misure in caso di trattamento di dati sensibili o giudiziari	Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.	
A.10.8.2	Accordi per la trasmissione	N.A.			

Controllo		*Misura*		*Testo*	*Commenti*
A.10.8.3	Trasporto dei supporti fisici	All.B punto 24	Ulteriori misure in caso di trattamento di dati sensibili o giudiziari	Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato	
A.10.8.4	Messaggistica elettronica	N.A.			
A.10.8.5	Sistemi informativi relativi al business	N.A.			
A. 10.9	Servizi di commercio elettronico				
A. 10.9 .1	Commercio elettronico	N.A.			
A. 10.9 .2	Transazioni on-line	N.A.			
A. 10.9 .3	Informazioni disponibili al pubblico	N.A.			
A.10.10	Monitoraggio				
A.10.10.1	Log di audit	N.A.			

Controllo		*Misura*		*Testo*	*Commenti*
A.10.10.2	Monitoraggio dell'utilizzo dei sistemi	AdS punto 2 lett. e	Verifica delle attività		
A.10.10.3	Protezione dei log	AdS punto 2 lett. f	Registrazione degli accessi	f) Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste.	
A.10.10.4	Log degli amministratori e degli operatori	AdS punto 2 lett. f	Registrazione degli accessi	f)…. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi	
A.10.10.5	Log degli errori	N.A.			
A.10.10.6	Sincronizzazione degli orologi	N.A.			

Controllo		*Misura*		*Testo*	*Commenti*
A.11	Controllo degli accessi				
A.11.1	Requisiti relativi al business per il controllo degli accessi				
A.11.1.1	Politica per la tenuta sotto controllo degli accessi	All.B punti da 1 a 11	Sistema di autenticazione informatica		
A.11.2	Gestione dell'accesso degli utenti				
A.11.2.1	Registrazione degli utenti	CP art. 34 comma 1 lettere a, b	Trattamenti con strumenti elettronici	a) autenticazione informatica; b) adozione di procedure di gestione delle credenziali di autenticazione;	
		All.B punti 2, 3, 6, 7, 8	Sistema di autenticazione informatica		
		All.B punto 3	Sistema di autenticazione informatica		
A.11.2.2	Gestione dei privilegi	CP art. 34 comma 1 lettera c	Trattamenti con strumenti elettronici	c) utilizzazione di un sistema di autorizzazione;	
		All.B punto 12	Sistema di autorizzazione		
		All.B punto 13	Sistema di autorizzazione		
A.11.2.3	Gestione delle password degli utenti	All.B punti da 1 a 11	Sistema di autenticazione informatica		

Controllo		*Misura*		*Testo*	*Commenti*
A.11.2.4	Riesame dei diritti di accesso degli utenti	All.B punto 14	Sistema di autorizzazione		
		All.B punto 15	Altre misure di sicurezza		
		CP art. 34 comma 1 lettera d	Trattamenti con strumenti elettronici	d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici.	
A. 11.3	Responsabilità degli utenti				
A.11.3.1	Utilizzo delle password	All.B punto 4	Sistema di autenticazione informatica		
		All.B punto 5	Sistema di autenticazione informatica		
		All.B punto 6	Sistema di autenticazione informatica		
A.11.3.2	Apparecchiature incustodite degli utenti	All.B punto 9	Sistema di autenticazione informatica		
A.11.3.3	Politica di schermo e scrivania puliti	N.A.			

Controllo		*Misura*		*Testo*	*Commenti*
A. 11.4	Controllo degli accessi alla rete				
A.11.4.1	Politica per l'utilizzo dei servizi di rete	All.B punti da 1 a 11 e punto 20	Trattamenti con strumenti elettronici Ulteriori misure in caso di trattamento dei dati sensibili e giudiziari		
A.11.4.2	Autenticazione dell'utente per le connessioni esterne	N.A.			
A.11.4.3	Autenticazione dell'apparecchiatura in rete	N.A.			
A.11.4.4	Protezione delle porte per la diagnostica remota e la configurazione	N.A.			
A.11.4.5	Separazione in reti	N.A.			
A.11.4.6	Controllo di connessione della rete	N.A.			
A.11.4.7	Controllo di instradamento di rete	N.A.			
A. 11.5	Controllo degli accessi al sistema operativo				
A.11.5.1	Procedure di log-on sicure	N.A.			
A.11.5.2	Identificazione e autenticazione degli utenti	CP art. 34 lettera a	Trattamenti con strumenti elettronici	a) autenticazione informatica;	
		All.B punti 2 e 3	Sistema di autenticazione informatica		
A.11.5.3	Sistema per la gestione delle password	All.B punto 5	Sistema di autenticazione informatica		

Controllo		***Misura***		***Testo***	***Commenti***
A.11.5.4	Utilizzo di programmi di utilità del sistema	N.A.			
A.11.5.5	Time-out della sessione	N.A.			
A.11.5.6	Limitazione del tempo di connessione	N.A.			
A. 11.6	Controllo degli accessi ad applicazioni e informazioni				
A.11.6.1	Limitazione all'accesso alle informazioni	All.B punto 1	Sistema di autenticazione informatica		
		All.B punto 13	Sistemi di autorizzazione		
		CP art. 3	Principio di necessità nel trattamento dei dati		

Controllo		*Misura*		*Testo*	*Commenti*
A.11.6.2	Isolamento dei sistemi sensibili	All.B punto 24	Ulteriori misure in caso di trattamento di dati sensibili o giudiziari	Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.	
		CP art. 3	Principio di necessità nel trattamento dei dati		
A.11.7	Utilizzo di dispositivi portatili e telelavoro				
A.11.7.1	Utilizzo di dispositivi portatili e comunicazioni	N.A.			
A.11.7.2	Telelavoro	N.A.			

Controllo		***Misura***		***Testo***	***Commenti***
A.12	Acquisizione, sviluppo e manutenzione dei sistemi informativi				
A.12.1	Requisiti di sicurezza dei sistemi informativi				
A.12.1.1	Analisi e formalizzazione dei requisiti di sicurezza	CP art. 31	Obblighi di Sicurezza		
		CP art. 3	Principio di necessità nel trattamento dei dati		
A.12.2	Corretta elaborazione nelle applicazioni				
A.12.2.1	Registrazione degli utenti	N.A.			
A.12.2.2	Gestione dei privilegi	N.A.			
A.12.2.3	Gestione delle password degli utenti	N.A.			
A.12.2.4	Riesame dei diritti di accesso degli utenti	N.A.			

Controllo		*Misura*		*Testo*	*Commenti*
A.12.3	Controlli crittografici				
A.12.3.1	Politica per l'utilizzo dei controlli crittografici	CP art. 22 commi 6 e 7	Principi applicabili al trattamento di dati sensibili e giudiziari	6. I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità. 7. I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici.	
		CP art. 34 comma 1 lettera h	Trattamenti con strumenti elettronici	h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.	
A.12.3.2	Gestione delle chiavi	N.A.			
A.12.4	Sicurezza dei file di sistema				
A.12.4.1	Controllo del software in funzione	N.A.			
A.12.4.2	Protezione dei dati di test di sistema	N.A.			
A.12.4.3	tenuta sotto controllo degli accessi al codice sorgente dei programmi	N.A.			

Controllo		*Misura*		*Testo*	*Commenti*
A.12.5	Sicurezza nei processi di sviluppo e supporto				
A.12.5.1	Procedure di tenuta sotto controllo dei cambiamenti	N.A.			
A.12.5.2	Riesame tecnico delle applicazioni in seguito ai cambiamenti nei sistemi operativi	N.A.			
A.12.5.3	Limitazioni ai cambiamenti nei pacchetti software	N.A.			
A.12.5.4	Fuga di informazioni	N.A.			
A.12.5.5	Sviluppo di software affidato all'esterno	All.B punto 25	Misure di tutela e garanzia		
A.12.6	Gestione delle vulnerabilità tecniche				
A.12.6.1	Tenuta sotto controllo delle vulnerabilità tecniche	All.B punto 17	Altre misure di sicurezza		
A.13	Gestione degli incidenti relativi alla sicurezza delle informazioni				
A.13.1	Segnalazione degli eventi e dei punti di debolezza relativi alla sicurezza delle informazioni				
A.13.1.1	Segnalazione degli eventi relativi alla sicurezza delle informazioni	N.A.			
A.13.1.2	Segnalazione di debolezze nella sicurezza	N.A.			

Controllo		*Misura*		*Testo*	*Commenti*
A.13.2	Gestione degli incidenti relativi alla sicurezza delle informazioni e dei miglioramenti				
A.13.2.1	Responsabilità e procedure	N.A.			
A.13.2.2	Apprendimento dagli incidenti relativi alla sicurezza delle informazioni	CP art. 32bis comma 7	Adempimenti conseguenti ad una violazione di dati personali	7. I fornitori tengono un aggiornato inventario delle violazioni di dati personali, ivi incluse le circostanze in cui si sono verificate, le loro conseguenze e i provvedimenti adottati per porvi rimedio, in modo da consentire al Garante di verificare il rispetto delle disposizioni del presente articolo. Nell'inventario figurano unicamente le informazioni necessarie a tal fine.	
A.13.2.3	Raccolta di evidenze oggettive (prove)	N.A.			
A.14	Gestione della continuità operativa				
A.14.1	Aspetti di sicurezza delle informazioni relativi alla gestione della continuità operativa				
A.14.1.1	Inclusione della sicurezza delle informazioni nel processo di gestione della continuità operativa	N.A.			
A.14.1.2	Continuità operativa e valutazione del rischio	N.A.			
A.14.1.3	Sviluppo e attuazione di piani di continuità operativa comprensivi della sicurezza delle informazioni	All.B punto 10	Sistema di autenticazione informatica		
		All.B punto 18	Altre misure di sicurezza		

Controllo		*Misura*		*Testo*	*Commenti*
		All.B punto 23	Ulteriori misure in caso di trattamento di dati sensibili o giudiziari		
A.14.1.4	Struttura di supporto per la pianificazione della continuità operativa	N.A.			
A.14.1.5	Testare, mantenere attivi e sottoporre a ri-valutazione i piani di continuità operativa	N.A.			
A.15	Conformità				
A.15.1	Conformità alle prescrizioni legali				
A.15.1.1	Identificazione della legislazione applicabile	N.A.			
A.15.1.2	Diritti di proprietà intellettuale (IPR)	N.A.			
A.15.1.3	Protezione delle registrazioni dell'organizzazione	N.A.			
A.15.1.4	Protezione dei dati e privacy delle informazioni personali	N.A.			
A.15.1.5	Prevenzione dell'utilizzo non appropriato delle strutture di elaborazione delle informazioni	N.A.			
A.15.1.6	Regolamentazione dei controlli crittografici	N.A.			

Controllo		*Misura*		*Testo*	*Commenti*
A.15.2	Conformità a politiche e norme di sicurezza e conformità tecnica				
A.15.2.1	Conformità a politiche e norme di sicurezza	AdS punto 2 lett. e	Verifica delle attività	e) L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento o dei responsabili, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.	
		CP art. 29 punto 5	Responsabile del trattamento		
A.15.2.2	Verifica della conformità tecnica	N.A.			
A.15.3	Considerazioni sull'audit dei sistemi informativi				
A.15.3.1	Controlli di audit dei sistemi informativi	N.A.			
A.15.3.2	Protezione degli strumenti per gli audit dei sistemi informativi	N.A.			