Un documento ENISA

Pacchetto informativo per le PMI

Con esempi di
valutazione e gestione del rischio
per due PMI

(disponibile anche all'indirizzo www.enisa.europa.eu/rmra)

Realizzato dal
Dipartimento tecnico dell'ENISA
Sezione Gestione del rischio
in collaborazione con

George Patsis
Obrela Security Industries (OSI)
www.obrela.com

Febbraio 2007

Avvertenza legale

Sintesi

Questo è il secondo documento menzionato nel programma di lavoro 2006 dell'ENISA. Il materiale si ricollega in parte all'esigenza, manifestata all'ENISA, di approntare un modello semplificato di valutazione del rischio.

Il documento intende fornire un quadro d'insieme, semplificato ed esauriente, della gestione e della valutazione del rischio ad uso e consumo delle piccole e medie imprese (PMI). Per conseguire questo obiettivo il documento è stato strutturato in maniera modulare, con moduli specificatamente dedicati alle diverse esigenze delle parti coinvolte nel processo di valutazione e gestione del rischio.

L'approccio filosofico alla base del documento consiste nell'aiutare gli utenti (non esperti) a districarsi nella complessità delle attività legate alla gestione ed alla valutazione del rischio. Nel far ciò, alcuni aspetti particolarmente complessi sono stati semplificati quanto basta per conseguire un livello di sicurezza accettabile.

Non vi è dubbio che se occorre un livello di sicurezza elevato, bisogna tener conto di tutta la complessità della gestione della sicurezza, fra cui un affinamento dei dati, delle misure e delle tecnologie corrispondenti. A questo proposito, le idee e il modello qui presentati sono ritenuti coprire un livello di sicurezza accettabile per le piccole organizzazioni, i cui investimenti in sicurezza sono più ridotti. Forme più avanzate di sicurezza (ad esempio, componenti infrastrutturali critiche) richiederebbero una trattazione più ampia che va al di là dello scopo del presente documento.

Il materiale è stato predisposto prevedendo tutta la gamma delle competenze delle parti coinvolte nella valutazione del rischio. Il processo di valutazione del rischio che qui si propone è articolato in un modello semplificato di valutazione, in quattro fasi, partendo dal presupposto che gli utenti di questo documento non abbiano conoscenze avanzate delle problematiche relative alla sicurezza. Qualora queste conoscenze siano necessarie, il presente modello non è altro che un "congegno" che offre un numero limitato di scelte globali.

Un altro criterio di cui si è tenuto conto è il rapporto costi/benefici in tutte le fasi della valutazione e della gestione del rischio. Il materiale può aiutare i responsabili decisionali a decidere quale sia il modello di valutazione del rischio più consono alla propria organizzazione, sulla base dei costi e degli indicatori di performance. Inoltre, nel caso in cui si scelga l'autovalutazione, il documento fornisce gli strumenti per realizzarla, senza richiedere una precedente esperienza specifica.

Il modello semplificato di valutazione del rischio qui presentato è un esempio di buona prassi per valutare i rischi cui è esposto il patrimonio informativo. Si parte dal presupposto che esistano delle alternative, cioè modelli analoghi o buone prassi similari. Questo modello non vuole essere né un tentativo di sostituire gli standard esistenti, né il tentativo di ridefinire le buone prassi. Il documento è stato concepito piuttosto per dare alle PMI interessate uno strumento di non facile reperibilità altrove.

L'applicazione delle idee qui presentate è stata dimostrata mediante degli esempi. Sono state prescelte due tipologie di PMI rappresentative, i cui rischi sono stati valutati utilizzando questo modello di valutazione. Gli esempi sono presentati nell'ambito del modello semplificato di valutazione del rischio qui proposto.

Vale la pena rilevare che questo documento è il primo di una serie di documenti che l'ENISA produrrà per sensibilizzare le PMI sul tema della gestione e della valutazione del rischio. In quanto tale, sarà oggetto di ulteriori migliorie, adeguamenti ed ampliamenti. Le future attività dell'ENISA comprendono la convalida del materiale tramite progetti pilota presso le PMI, la valutazione/revisione tramite gruppi di esperti e la divulgazione, anche mediante organizzazioni che si occupano di formazione e/o associazioni professionali. L'obiettivo ultimo consiste nell'avere una versione del documento che possa essere utilizzata dalle PMI "così com'è", vale a dire senza ulteriori migliorie/spiegazioni/adeguamenti. Per questo motivo, ci riferiamo al presente documento come alla "versione beta", intendendo con questo che dopo vari progetti pilota, applicazioni e divulgazioni, ad essa seguiranno rettifiche e versioni più avanzate, portando così il materiale qui presentato, nel medio periodo, ad uno stadio di maturità.

Contatto: Dipartimento tecnico dell'ENISA, sezione Gestione del rischio, L. Marinos, esperto senior in gestione del rischio, e-mail: RiskMngt@enisa.europa.eu

Indice

1. FINALITÀ E CAMPO DI APPLICAZIONE 6

2. STRUTTURA DEL DOCUMENTO 7

3. GUIDA PER IL RESPONSABILE DECISIONALE 8

3.1 COSA DEVE CONSIDERARE IL RESPONSABILE DECISIONALE 8
3.2 COSA DEVE SAPERE IL RESPONSABILE DECISIONALE 9
3.3 COME METTERE IN SICUREZZA LE INFORMAZIONI 11
3.3.1 Personale interno 12
3.3.2 Esternalizzazione totale 13
3.3.3 Esternalizzazione parziale 15

4. UN MODELLO SEMPLIFICATO: PANORAMICA 18

4.2 IPOTESI DI LAVORO 20
4.3 UN APPROCCIO IN QUATTRO FASI 20
4.3.1 Fase 1: selezione del profilo di rischio 22
4.3.2 Fase 2: identificazione degli elementi critici 23
4.3.3 Fase 3: selezione delle schede di controllo 25
Selezione delle schede di controllo organizzativo 26
Selezione delle schede di controllo tecnico 26
4.3.4 Fase 4: implementazione e gestione 27

5. LINEE GUIDA PER L'AUTOVALUTAZIONE, CORREDATE DA DUE ESEMPI 29

FASE 2: IDENTIFICAZIONE DEGLI ASSET CRITICI 33
Passaggio 1. Selezionare i cinque asset critici più importanti dell'organizzazione 33
Passaggio 2. Registrare la logica di selezione di ciascun asset critico 34
Passaggio 3. Identificare i requisiti di sicurezza degli asset critici 34
FASE 3: SELEZIONE DELLE SCHEDE DI CONTROLLO 38
Passaggio 1. Selezionare le schede di controllo organizzativo 39
Passaggio 2. Selezionare le schede di controllo tecnico 39
Passaggio 3. Elenco documentato dei controlli selezionati e delle relative logiche 39
FASE 4: IMPLEMENTAZIONE E GESTIONE 44
Passaggio 1. Analisi delle non-conformità 44
Passaggio 2. Elaborare piani di riduzione del rischio 45
Passaggio 3. Implementazione, monitoraggio e controllo 45

ALLEGATO A. SCHEDE DI CONTROLLO ORGANIZZATIVO 52

ALLEGATO B. SCHEDE DI CONTROLLO TECNICO 53

ALLEGATO C. CONTROLLI ORGANIZZATIVI 67

ALLEGATO D. CONTROLLI TECNICI 71

ALLEGATO E. ALCUNI SEMPLICI CONSIGLI 76

Password 76
Virus, worm e trojan 77
Spamming 78
Spyware 79
Firewall 79
Patch 80
Backup 81
Furto di informazioni e identità 82
Reti wireless 83
Soggetti terzi 84
Provider di servizi 86

Protezione dei dati e privacy *86*

RIFERIMENTI **88**

Elenco delle figure

Figura 1. Gestione del rischio relativo alla sicurezza delle informazioni - Attività di valutazione del rischio 10
Figura 2. Le quattro fasi del modello di valutazione del rischio qui proposto 21
Figura 3. Fase 1: flusso di lavoro per la selezione del profilo di rischio 30
Figura 4. Fase 2: flusso di lavoro per l'identificazione degli asset critici 33
Figura 5. Fase 3: flusso di lavoro per la selezione delle schede di controllo 38
Figura 6. Fase 4: flusso di lavoro per l'implementazione e la gestione 44
Figura 7. Opzioni relative all'esternalizzazione della gestione o dell'implementazione 46

Elenco delle tabelle

Tabella 1. Opzioni per l'implementazione della valutazione del rischio 12
Tabella 2. Valutazione del profilo di rischio 22
Tabella 3. Elenco degli asset 23
Tabella 4. Selezione dei requisiti di sicurezza 24
Tabella 5. Controlli utilizzati nel modello qui presentato 25
Tabella 6. Schede di controllo organizzativo 26
Tabella 7. Schede di controllo tecnico 26
Tabella 8. Esempio di scheda di controllo per un'applicazione con profilo di rischio alto 27
Tabella 9. Valutazione del profilo di rischio: esempio A 31
Tabella 10. Profilo di rischio dell'organizzazione: esempio A 31
Tabella 11. Valutazione del profilo di rischio: esempio B 32
Tabella 12. Profilo di rischio dell'organizzazione: esempio B 32
Tabella 13. Selezione dei requisiti di sicurezza: esempio A 35
Tabella 14. Logica dei requisiti di sicurezza 36
Tabella 15. Selezione dei requisiti di sicurezza: esempio B 36
Tabella 16. Logica dei requisiti di sicurezza 37
Tabella 17. Selezione dei controlli organizzativi: esempio A 40
Tabella 18. Selezione delle schede di controllo tecnico: esempio A 41
Tabella 19. Scheda di controllo tecnico: esempio A (CC-1A) 41
Tabella 20. Logica di selezione dei controlli: esempio A 42
Tabella 21. Selezione dei controlli organizzativi: esempio B 42
Tabella 22. Selezione delle schede di controllo tecnico: esempio B 43
Tabella 23. Scheda di controllo tecnico: esempio B (CC-2S) 43
Tabella 24. Logica di selezione dei controlli: esempio B 43
Tabella 25. Elenco derivante dall'analisi delle non-conformità: esempio A 48
Tabella 26. Elenco delle azioni: esempio A 49
Tabella 27. Piano di implementazione: esempio A 50
Tabella 28. Elenco derivante dall'analisi delle non-conformità: esempio B 50
Tabella 29. Elenco delle azioni: esempio B 50
Tabella 30. Piano di implementazione: esempio B 51

1. Finalità e campo di applicazione

Le piccole e medie imprese (PMI) rappresentano un'area prioritaria per la politica economica dei governi e sono considerate di importanza essenziale per la crescita socioeconomica dell'Unione europea. Le PMI hanno solitamente un retroterra di passione imprenditoriale e risorse finanziarie limitate, con sistemi aziendali spesso eterogenei ed indipendenti. Inoltre, il patrimonio materiale ed immateriale delle PMI è definito in maniera rudimentale ed il loro valore è spesso noto soltanto in parte. Questo è tipicamente il caso di uno degli asset più importanti, vale a dire, le informazioni.

Come qualsiasi altro bene aziendale, le informazioni devono essere gestite e protette in maniera strategica. La sicurezza delle informazioni consiste nella protezione delle informazioni all'interno dell'azienda, ivi compresi i sistemi e l'hardware utilizzati per salvarle, elaborarle e trasmetterle. È indispensabile che i responsabili delle PMI comprendano il valore delle informazioni contenute all'interno del proprio sistema aziendale e dispongano di un quadro entro il quale valutare ed implementare la sicurezza delle informazioni. Per salvaguardare un'organizzazione dalla perdita di informazioni e da potenziali responsabilità si possono adottare svariati schemi di sicurezza approvati a livello internazionale. Poiché questi schemi sono complessi, onnicomprensivi ed in ultima analisi di costosa implementazione, essi sono adottati per lo più dalle grandi organizzazioni.

Di solito, in considerazione dello sviluppo dinamico e del tutto specifico di molte PMI, nella fase di avvio dell'attività le questioni dell'integrazione o della sicurezza non sono affrontate in maniera sistematica. Ne segue che le politiche e gli schemi per la pianificazione della sicurezza delle informazioni e per il disaster recovery sono di solito estremamente rudimentali o perfino inesistenti. Accade spesso che nelle PMI la comprensione del rischio relativo alla sicurezza delle informazioni non vada molto al di là dei virus e dei software antivirus. Le minacce di natura involontaria rappresentano alcuni dei massimi rischi di sicurezza per le PMI, eppure la formazione del personale ed i programmi di sensibilizzazione sono spesso trascurati.

Dai risultati dell'indagine emerge che il livello di sensibilizzazione al tema della sicurezza delle informazioni tra i responsabili delle PMI è estremamente variabile, al pari della situazione dei sistemi informativi, delle tecnologie e dei dispositivi di sicurezza di cui dispongono. Anche se una minoranza di PMI ha adottato standard di sicurezza quali l'ISO/IEC 27001, oppure il suo equivalente internazionale ISO 17799, la maggior parte dei dirigenti delle PMI non ha mai sentito parlare di standard di sicurezza e ritiene che la sicurezza delle informazioni consista soltanto in interventi tecnici tesi a contrastare la minaccia dei virus e ad effettuare il backup dei dati.

Lungi dal biasimare i dirigenti delle PMI che non sono consapevoli delle criticità relative alla sicurezza delle informazioni, la ricerca conclude affermando che i vertici delle PMI devono avviare, comprendere ed attuare processi formali di sicurezza del patrimonio informativo, comprendenti anche misure tecniche ed organizzative. Senza misure di questo tipo, l'azienda può risultare seriamente danneggiata da minacce involontarie/attacchi deliberati ai propri sistemi informativi, tali da poter determinare in ultima analisi la cessazione dell'attività.

Sulla base del presente pacchetto informativo le PMI saranno in grado di valutare il rischio rispetto al proprio ambiente, selezionando ed applicando misure adeguate per affrontare e gestire i rischi per la sicurezza delle informazioni. Con questo documento, assistiamo le PMI nella definizione di questo impegno, nella decisione di come iniziare e di come procedere e, se le PMI dispongono di risorse sufficienti, forniamo linee guida per effettuare l'autovalutazione dei rischi informatici. A tal fine, offriamo un metodo semplice di valutazione del rischio, che porta ad una veloce ed ampia identificazione e riduzione dei rischi informatici.

Il metodo di valutazione qui presentato si basa su un modello semplificato, messo a punto per piccole organizzazioni che condividono alcune caratteristiche in comune. In primo luogo, le strutture organizzative sono relativamente piatte e le persone inquadrate in livelli diversi dell'organizzazione sono abituate a lavorare l'una a fianco dell'altra. In secondo luogo, alle persone si chiede spesso di svolgere una molteplicità di compiti, facendo partecipare il personale all'insieme dei processi e delle procedure in uso all'interno dell'organizzazione.

2. Struttura del documento

Per coprire le esigenze di svariate tipologie di PMI, abbiamo scelto per questo documento una struttura modulare. A seconda delle esigenze di una specifica PMI e di quanto essa cerchi di affrontare la valutazione del rischio, si rivelano utili parti diverse del medesimo documento. Alle PMI che desiderino una panoramica della gestione del rischio allo scopo di definire la propria strategia futura, sarà utile la parte generale del presente documento (cfr. capitolo 3. Guida per il responsabile decisionale e capitolo 4. Un modello semplificato: panoramica).

Qualora una PMI decida di implementare in proprio la gestione del rischio, si rimanda alle parti del documento che contengono la descrizione dettagliata del metodo di valutazione del rischio e degli esempi (cfr. capitolo 5. Linee guida per l'autovalutazione, corredate da due esempi). Nel caso dell'autovalutazione, servono anche i documenti dettagliati che si trovano negli allegati, allo scopo di definire le misure che devono essere implementate nell'organizzazione (cfr. Allegato A. Schede di controllo organizzativo, Allegato B. Schede di controllo tecnico). Per fornire un'idea più precisa di come questo documento possa essere utilizzato, forniamo alcuni esempi di possibile uso, a seconda del ruolo dei lettori:

- **le persone aventi un background manageriale** possono prendere in esame il capitolo 3, che è dedicato ai responsabili decisionali. Esso spiega i retroscena della sicurezza informatica e la necessità della gestione del rischio. Il capitolo 3 fornisce possibili opzioni per l'implementazione della gestione del rischio e definisce i criteri decisionali. I dirigenti interessati potrebbero voler capire anche la struttura del processo di valutazione del rischio, qui proposto al capitolo 4;
- **i componenti non esperti di un gruppo di valutazione del rischio** dovranno comprendere il modello semplificato di valutazione del rischio qui proposto, dovranno leggere i dettagli e gli esempi presentati (cfr. capitolo 4. Un modello semplificato: panoramica);
- **i componenti esperti di un gruppo di valutazione del rischio** dovranno leggere il metodo e comprenderne i dettagli. Essi saranno anche in grado di consultare il materiale che figura negli allegati, con particolare riferimento alla scelta delle misure (denominate anche, nel documento, contromisure, controlli o controlli di sicurezza). In alternativa, agli asset esistenti si possono assegnare nuove misure, ma si possono anche aggiungere nuovi asset (cfr. Allegato A. Schede di controllo organizzativo, Allegato B. Schede di controllo tecnico, Allegato C. Controlli organizzativi).

3. Guida per il responsabile decisionale

3.1 Cosa deve considerare il responsabile decisionale

Oggi, le informazioni create, elaborate ed utilizzate da un'organizzazione rappresentano uno dei suoi asset di maggior valore. La divulgazione delle informazioni, la loro compromissione o indisponibilità possono determinare un **grave impatto** sull'organizzazione, rappresentare **una violazione delle leggi e dei regolamenti** e possono **incidere** negativamente **sul buon nome dell'azienda.**

L'adeguatezza dei sistemi di sicurezza delle informazioni e di elaborazione delle informazioni rientra tra le responsabilità fondamentali della direzione. I proprietari ed i responsabili decisionali devono comprendere qual è la situazione del programma di sicurezza delle informazioni per poter emettere giudizi motivati ed effettuare investimenti che riducano i rischi ad un livello accettabile. I rischi correlati alle informazioni possono portare a situazioni critiche, quando vanno ad investire l'essenza dell'organizzazione, sul piano aziendale e legale. I rischi correlati alle informazioni possono portare pertanto a categorie di rischio più generali e a maggiore criticità quali:

- **rischio legale/legato agli adempimenti** è il rischio derivante da violazioni o mancato rispetto di leggi, norme contabili, regolamenti, prassi o norme etiche. I rischi legali o correlati agli adempimenti possono esporre l'organizzazione a pubblicità negativa, ammende, sanzioni penali e civili, pagamento dei danni e annullamento dei contratti. Il furto di informazioni relative ai clienti, come le informazioni sulle carte di credito, le informazioni finanziarie, le informazioni sanitarie o altri dati personali possono anche sollevare rischi potenziali in termini di rivendicazioni di terzi. **In riconoscimento del fatto che la sicurezza delle informazioni è una problematica crescente e composita, ma anche per tutelare i diritti civili e coinvolgere la responsabilità delle aziende, i governi dell'UE e l'Unione europea hanno stabilito leggi e regolamenti il cui rispetto è previsto da parte di tutte le organizzazioni, a prescindere dalle dimensioni o dal settore. Queste norme obbligano le società ad implementare controlli interni volti a proteggere l'azienda dai rischi informatici. Esse mirano anche a migliorare le prassi e le procedure di gestione del rischio;**
- **rischi di stabilità finanziaria**. La mancanza di adeguate infrastrutture di produzione, di infrastrutture gestionali o di personale per perseguire la strategia aziendale può far sì che la società non sia in grado di conseguire gli obiettivi dichiarati e gli obiettivi finanziari in un ambiente ben gestito e controllato. Una **inadeguata gestione della sicurezza delle informazioni può ricadere sui rischi relativi alla stabilità finanziaria dell'organizzazione, i quali rischi a loro volta, possono aprire la porta a frode, riciclaggio di denaro, instabilità finanziaria, ecc.;**
- **il rischio produttività** è il rischio di riportare perdite operative e di erogare **servizi carenti alla clientela** per effetto del mancato rispetto delle procedure di lavorazione di base e dei relativi controlli. Questo rischio si riferisce solitamente a tutte le attività di produzione che contribuiscono in qualche modo alla consegna complessiva di un prodotto o di un servizio. Il rischio produttività non è limitato all'uso delle tecnologie: può anche essere il risultato di attività organizzative. In questa famiglia di rischio rientrano i rischi derivanti da sistemi inadeguati o scarsamente controllati, dal software utilizzato a supporto del front office alle operazioni di gestione del rischio, dalla contabilità ad altre unità aziendali. Una inadeguata gestione della sicurezza delle informazioni può determinare rischi di produttività elevati, fra cui elevati costi operativi, carenze operative, debolezza delle decisioni manageriali (prezzo, liquidità ed esposizione al rischio del credito), nonché mancanza **di privacy ed interruzione del servizio alla clientela**;
- **reputazione e fiducia nella clientela.** Forse il rischio più difficile da comprendere, ma anche uno dei più importanti, è il rischio di danno alla reputazione, un bene immateriale ma importante. I clienti, che hanno magari letto sul giornale che la banca dati della società, che

contiene i numeri delle carte di credito, è stata aggredita dagli hacker, saranno disposti a fornire in seguito il numero della propria carta di credito? I vertici aziendali rimarranno al loro posto, in una società così danneggiata? Quale sarà la reazione degli azionisti? Qual è la prevista perdita di reddito futuro? Qual è la perdita prevista in termini di capitalizzazione di mercato?

Molti titolari di PMI pensano di non essere a rischio, in virtù della ridotta dimensione della propria azienda e del patrimonio informativo. La maggior parte ritiene che soltanto le grandi società, quelle che hanno un patrimonio di grande rilievo, siano a rischio. Questo non è vero. In primo luogo, la sensitività delle informazioni si applica alla qualità e non alla quantità delle informazioni. In secondo luogo, le PMI non dispongono delle risorse o del personale necessari per affrontare la sicurezza in maniera intensiva, come fanno le grandi società: sono pertanto più esposte. Di fatto, le nuove tecnologie consentono alle piccole aziende di utilizzare una buona parte dei medesimi sistemi informativi utilizzati dalle grandi imprese. Nel fare questo, le piccole aziende si espongono a molte delle minacce che tradizionalmente si associano alle grandi società. **Infatti, nell'arco dell'ultimo anno, il 56% delle piccole aziende ha registrato almeno un incidente relativo alla sicurezza**. Sfortunatamente, una percentuale non irrilevante delle aziende colpite da inconvenienti che hanno messo fuori uso i computer non riesce a recuperare il danno e l'azienda stessa è costretta a chiudere. Affinché il successo sia continuativo, è imperativo pertanto che i titolari ed i responsabili decisionali delle PMI ammettano queste insidie e prendano misure atte ad affrontare le questioni relative alla sicurezza delle informazioni.

Le misure volte a attenuare il rischio di sicurezza delle informazioni (controlli) dovrebbero essere rapportate ai rischi affrontati dalle informazioni in questione. Tuttavia, il processo volto a determinare quali siano i controlli di sicurezza più appropriati e con il miglior rapporto qualità/prezzo è abbastanza spesso complesso ed a volte soggettivo. **Una delle funzioni primarie per collocare questo processo su una base più oggettiva è una valutazione permanente del rischio di sicurezza.**

3.2 Cosa deve sapere il responsabile decisionale

La sicurezza delle informazioni riguarda l'identificazione, la riduzione e la gestione dei rischi pertinenti al patrimonio informativo. La valutazione del rischio è il primo passo necessario per comprendere i rischi: si tratta di effettuare l'**identificazione** e la **valutazione** dell'insieme dei rischi di quella determinata organizzazione. Il risultato di questa attività è essenziale per poter gestire l'azienda, in quanto i rischi coinvolti possono influenzare significativamente la riservatezza, l'integrità e la disponibilità del patrimonio informativo e **possono essere di rilevanza critica per conservare il vantaggio competitivo, la stabilità finanziaria, il rispetto delle leggi ed una forte immagine commerciale**.

In quanto tale, la valutazione del rischio può aiutare i responsabili decisionali:

- **a valutare le prassi organizzative e la piattaforma tecnologica installata;**
- **ad introdurre forme di protezione delle informazioni basate sul potenziale impatto sull'organizzazione;**
- **a concentrarsi sugli aspetti importanti della sicurezza; le misure che sono associate a rischi accettabili possono essere tralasciate;**
- **a garantire che le misure attuate ed il relativo costo siano del tutto rapportati ai rischi ai quali l'organizzazione è esposta. In questo modo si può conservare un equilibrio tra i costi legati ad un rischio da contrastare ed i benefici derivanti dall'evitare l'eventuale impatto negativo.**

Nel corso della valutazione del rischio, l'organizzazione deve intervenire per a) individuare i rischi per la sicurezza delle informazioni, b) valutare i rischi per determinare le priorità e c) decidere come provvedere a ridurre i rischi (cfr. anche la Figura 1).

La valutazione del rischio relativo alla sicurezza delle informazioni, tuttavia, è soltanto il primo passo verso la gestione del rischio, la quale consiste in un processo continuo di individuazione dei rischi e di implementazione dei piani per affrontarli. La figura 1 illustra il processo di gestione del rischio relativo

alla sicurezza delle informazioni e la "porzione" che, rispetto a questo processo, è rappresentata dalla valutazione del rischio.

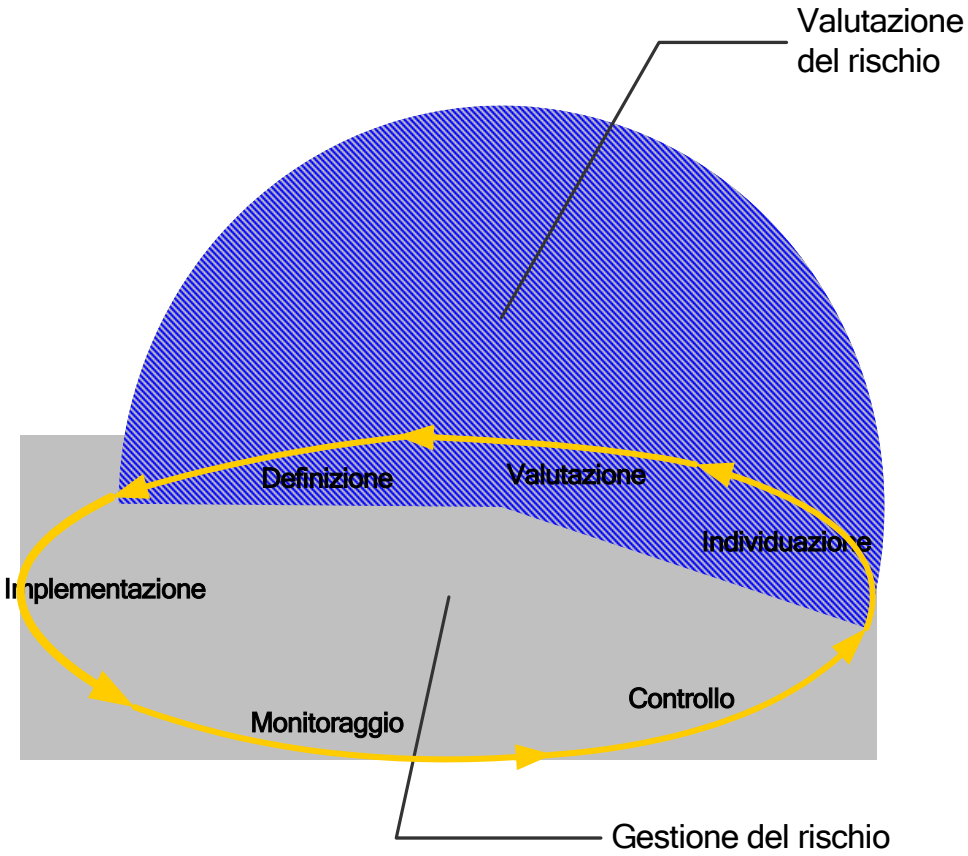

Figura 1. Gestione del rischio relativo alla sicurezza delle informazioni - Attività di valutazione del rischio

Chiaramente, la valutazione del rischio indica di per sé soltanto una direzione per le attività dell'organizzazione in materia di sicurezza dell'informazione; **non comporta necessariamente miglioramenti significativi a meno che non si provveda ad adottare alcune misure**. Come in qualsiasi altra disciplina gestionale, l'implementazione di una sola parte del ciclo di vita della gestione non porta gli effetti desiderati. Nessuna valutazione, sia essa più o meno dettagliata o più o meno esperta, è in grado *ipso facto* di migliorare la posizione in termini di sicurezza, se l'organizzazione non fa seguito alla valutazione con una fase di implementazione. Oltre alla valutazione del rischio, un'efficace gestione del rischio comprende i **passi seguenti**:

- **pianificazione** delle modalità di implementazione della strategia di protezione e dei piani di riduzione del rischio, partendo dalla fase valutativa e sviluppando piani d'azione dettagliati. Questa attività può comprendere un'analisi dettagliata dei costi/benefici delle strategie e delle azioni possibili;
- **implementazione** dei piani d'azione dettagliati precedentemente selezionati;
- **monitoraggio** dei piani per verificarne i progressi e l'efficacia; questa attività comprende l'osservazione degli eventuali cambiamenti avvenuti nei livelli di rischio;
- **controllo** delle variazioni rispetto all'esecuzione dei piani, adottando appropriate azioni correttive.

3.3 Come mettere in sicurezza le informazioni

Una parte della responsabilità dei dirigenti delle PMI consiste nel garantire la sicurezza del proprio ambiente aziendale. Secondo le norme di legge per lo più applicabili, la responsabilità per eventuali violazioni della sicurezza risiede in capo ad essi. Proprio come essi devono fornire un ambiente fisico sicuro da ogni punto di vista, essi devono anche assicurarsi che le informazioni siano protette. Tuttavia, i computer non sono strumenti definiti una volta per tutte: la tutela delle informazioni è una problematica costante.

I responsabili decisionali possono cominciare a valutare il rischio rispetto al proprio ambiente e promuovere l'introduzione di misure atte a far fronte a rischi che l'organizzazione non può accettare. Questo è un prerequisito per la gestione della sicurezza delle informazioni. Si possono seguire modalità di approccio diverse, a seconda delle risorse da dedicare (la decisione del "fare o comprare"). Noi distinguiamo fra tre modalità di approccio:

- **la valutazione del rischio con personale interno,** compresa l'identificazione delle misure necessarie. La valutazione si basa su un approccio prescelto dall'organizzazione stessa (ad esempio una buona prassi, uno standard noto, ecc.). Ciò può aiutare l'organizzazione a padroneggiare l'approccio per le successive valutazioni;
- **l'esternalizzazione totale della valutazione del rischio**: con questo approccio, l'intera valutazione del rischio è demandata ad un contraente esterno. La valutazione segue l'approccio prescelto dal contraente esterno. Il contraente può farsi carico anche delle valutazioni periodiche future. Per l'intero ciclo di vita della valutazione e della gestione del rischio della PMI, non si prevede alcun trasferimento di know-how al personale interno;
- **l'esternalizzazione parziale della valutazione del rischio**: questo approccio parte dal presupposto che la valutazione iniziale del rischio sia demandata ad una società esterna, ma seguendo un approccio noto alla PMI. Conseguentemente, ulteriori valutazioni del rischio potranno essere effettuate dal personale interno. La valutazione iniziale eseguita dalla società esterna funge da trasferimento di know-how al personale interno della PMI.

Il presente documento fornisce alle PMI quanto è necessario per prendere la decisione di "fare o comprare". Vengono fornite inoltre tutte le informazioni necessarie per aiutare le PMI ad effettuare l'autovalutazione. Questo modello di valutazione del rischio può fungere, nelle decisioni di valutazione con personale interno o di esternalizzazione parziale, da linea guida per la valutazione del rischio, iniziale e futura (cfr. capitolo 4. Un modello semplificato: panoramica e capitolo 5. Linee guida per l'autovalutazione, corredate da due esempi).

Nella comparazione, ogni modello di valutazione del rischio presenta vantaggi e svantaggi. La Tabella 1 fornisce una prima idea dei fatti relativi alla decisione di "fare o comprare" rispetto alla valutazione del rischio. I paragrafi seguenti affrontano nello specifico i parametri ed i fattori di cui si deve tener conto quando si seleziona un determinato approccio alla gestione del rischio per una PMI.

Opzioni per l'implementazione della valutazione del rischio	Parametri e fattori per l'implementazione				
	Competenze interne necessarie	Dipendenza da terzi	Risorse interne necessarie	Oggettività della valutazione	Impegno di terzi[1]
Con personale interno	Si	Basso	1-5 persone	Bassa	-
Esternalizzazione totale	No	Alto	1 persona (per la gestione del progetto)	Alta	10-40 giorni
Esternalizzazione parziale	Si	Basso	1-2 persone	Media	5-10 giorni

Tabella 1. Opzioni per l'implementazione della valutazione del rischio

Nelle sezioni seguenti descriviamo ciascuna possibile opzione per la valutazione e la gestione del rischio. Un questionario aiuterà i responsabili decisionali a determinare quale sia l'opzione percorribile rispetto ad una determinata tipologia di PMI.

3.3.1 Personale interno

La scelta interna può offrire molti **vantaggi, quali lo sviluppo e la competenza delle strutture interne dell'organizzazione nella valutazione del rischio e nella gestione del rischio. Inoltre, tenuto conto dei prezzi delle consulenze sul mercato specifico della sicurezza, questo approccio può comportare una spesa più ridotta.** Si tratta di un'opzione particolarmente attraente per le organizzazioni aventi una struttura semplice, una buona reperibilità dei dati per aver già svolto all'interno attività similari (ad esempio, ISO 9001), adeguate capacità e conoscenze tecniche.

Per stabilire se la valutazione del rischio con personale interno sia la decisione giusta per l'organizzazione, si può utilizzare il questionario seguente.

[1] Per calcolare l'impegno ipotizziamo una PMI che abbia un massimo di 100 dipendenti.

Domande per prendere una decisione	Risposta	
	☺ SI	☹ NO
L'organizzazione è piccola? Ha una struttura gerarchica piatta o semplice?		
Disponete di **know-how interno nel campo dei sistemi e delle reti IT?**		
L'organizzazione dispone di risorse umane qualificate e disponibili?		
Le vostre attività hanno un basso livello di dipendenza dai sistemi IT e non prevedono di salvare o elaborare dati della clientela di natura sensibile? L'organizzazione è stata coinvolta in attività analoghe, vale a dire processi di miglioramento della qualità?		
Riuscite a trovare un gruppo di tre-cinque persone che abbiano un'ampia ed approfondita conoscenza dell'organizzazione e possiedano inoltre la maggior parte delle caratteristiche seguenti? ▫ Capacità di risoluzione dei problemi ▫ Capacità di analisi ▫ Capacità di lavorare in gruppo ▫ Doti di leadership ▫ **Capacità di comprendere i processi aziendali e l'infrastruttura dell'organizzazione** ▫ Capacità di dedicare alcune giornate di lavoro all'apprendimento del metodo		
Avete un'infrastruttura IT relativamente semplice, che sia ben compresa da almeno una persona della vostra organizzazione?		

Quanto maggiore è il numero delle risposte "SI" che sono state date a queste domande, tanto maggiore è la probabilità che l'autovalutazione del rischio sia la scelta giusta per una PMI.

Utilizzando modello di valutazione del rischio qui proposto e le prassi migliori (cfr. capitolo 4. Un modello semplificato: panoramica e capitolo 5. Linee guida per l'autovalutazione, corredate da due esempi) i responsabili decisionali saranno in grado di valutare il rischio con un approccio efficiente per quanto riguarda l'identificazione e la gestione dei rischi per la sicurezza delle informazioni: saranno così in grado di migliorare continuamente la propria posizione in materia di sicurezza.

3.3.2 Esternalizzazione totale

Prendendo la strada dell'esternalizzazione totale, una PMI trasferisce in toto la valutazione e la gestione del rischio ad un contraente esterno. Ciò può comprendere sia la valutazione iniziale, sia le valutazioni successive e le attività facenti parte dell'intero ciclo di vita della gestione del rischio (ad esempio, implementazione e manutenzione delle misure). Il contraente applica il proprio approccio alla valutazione ed alla gestione del rischio. In tal modo, il contraente non realizza alcun trasferimento di know-how al cliente. A questo punto occorre rilevare che l'esternalizzazione delle attività di valutazione e gestione del rischio non libera la direzione della PMI dalle proprie responsabilità in tema di sicurezza (delle informazioni).

A seconda della struttura, della strategia, delle risorse disponibili e della situazione di mercato, l'esternalizzazione **può offrire vantaggi specifici**. La decisione di esternalizzare la valutazione del

rischio consente alla PMI di concentrarsi sull'attività caratteristica, demandando l'esecuzione delle attività periferiche ad un esperto esterno specializzato in sicurezza delle informazioni.

Per stabilire se la valutazione del rischio mediante esternalizzazione totale sia la decisione giusta per l'organizzazione, si può utilizzare il questionario seguente.

Domande per prendere una decisione	**Risposta**	
	☺ **SI**	☹ **NO**
Ritenete necessario **concentrarvi sempre di più** sulle competenze caratteristiche e sui processi aziendali strategici?		
Avete **difficoltà a mettere a disposizione due - cinque persone** che abbiano un'ampia ed approfondita conoscenza dell'organizzazione e possiedano inoltre la maggior parte delle caratteristiche seguenti? o **Capacità di comprendere i processi aziendali e l'infrastruttura dell'organizzazione** o Capacità di risoluzione dei problemi o Capacità di analisi o Capacità di lavorare in gruppo o Doti di leadership o Capacità di dedicare alcune giornate di lavoro all'apprendimento del metodo		
Avete **un'infrastruttura IT sofisticata e relativamente ampia**?		
Tra i prodotti o servizi che offrite figurano **operazioni finanziarie**?		
Gestite un'azienda che è notevolmente esposta a rigidi vincoli legali e regolamentari, comunitari o nazionali, e/o mandati specifici?		
Avete un'infrastruttura IT relativamente semplice, che sia ben compresa da almeno una persona della vostra organizzazione?		

Ancora una volta, quanto maggiore è il numero delle risposte "SI", tanto maggiore è la probabilità che l'esternalizzazione si adatti alle esigenze dell'organizzazione.

L'esternalizzazione delle attività di valutazione del rischio richiede **un processo di selezione del fornitore, fra cui una "*due diligence*" ed una valutazione complessiva del fornitore, nonché la valutazione della competenza del fornitore nel campo specifico della sicurezza delle informazioni** (cfr. anche Allegato E. Alcuni semplici consigli**,** Soggetti terzi**,**

Provider di servizi**).**

Alla base della collaborazione dovrebbe esserci un accordo sul livello dei servizi, il quale dovrebbe definire alcuni elementi chiave, quali la certificazione professionale degli ingegneri esperti in sicurezza di cui il fornitore dispone, clausole di riservatezza e non divulgazione, durata dell'incarico, assegnazione delle risorse, costi e metodologia da applicare.

Quando si deve sottoscrivere un accordo sul livello dei servizi, dovrebbero essere prese in considerazione le seguenti domande (una sorta di checklist dei contenuti dell'accordo).

- **Le questioni della responsabilità sono affrontate?** Cosa accade, ad esempio, se nel corso della valutazione importanti attività aziendali vengono bloccate o rallentate a causa dell'incompetenza del fornitore ad eseguire la valutazione dell'infrastruttura IT e della rete?
- L'accordo **identifica con chiarezza le responsabilità**? Chi sarà responsabile per fare che cosa? Qual è il coinvolgimento dell'organizzazione in termini di risorse?
- **Il campo di applicazione dell'attività è chiaramente documentato**? Che cosa includerà il fornitore nel campo di applicazione dell'attività? Si raccomanda caldamente che il campo di applicazione comprenda l'intera gamma delle attività aziendali e l'infrastruttura sottostante. Altrimenti, è possibile che il risultato sia inadeguato o perfino fuorviante.
- **Come si prevede avvenga il rispetto delle norme di legge,** ad esempio, nel settore della tutela dei dati?
- Quali soluzioni sono previste per far sì che tutte le parti coinvolte nell'esternalizzazione, subappaltatori compresi, siano consapevoli delle proprie responsabilità in termini di sicurezza?
- Come si prevede **di mantenere e verificare l'integrità e la riservatezza del patrimonio aziendale?**
- **Quali controlli fisici ed elettronici saranno utilizzati per restringere e delimitare agli utenti autorizzati l'accesso ai dati sensibili dell'organizzazione?**
- **In caso di disastro qual è il livello di disponibilità dei servizi da mantenere?**
- **Le condizioni generali prevedono il diritto di sottoporre a verifica le misure di sicurezza e di tutela delle informazioni adottate dal fornitore?**
- **Le risorse minime, la competenza e la certificazione professionale** del fornitore sono espressi con chiarezza?
- Il contenuto, la frequenza e la struttura della rendicontazione sono definiti con chiarezza?

Chiaramente, le organizzazioni possono ordinare ai fornitori di eseguire la valutazione sulla base del modello di gestione del rischio qui proposto (cfr. il capitolo 5. Linee guida per l'autovalutazione, corredate da due esempi). Nella misura in cui la PMI comprende i contenuti del modello qui proposto, essa è in grado di controllare meglio le attività del contraente.

3.3.3 Esternalizzazione parziale

Una soluzione mista **può riunire i vantaggi della scelta interna e dell'esternalizzazione**. In tal caso, l'organizzazione partecipa attivamente al processo di autovalutazione, fruendo però dell'intervento di un soggetto terzo. Il modello di valutazione del rischio, inoltre, è ben compreso dal cliente: può trattarsi, ad esempio, del modello qui presentato (cfr. capitolo 4. Un modello semplificato: panoramica). Si tratta di una **condizione sine qua non affinché vi sia un trasferimento di know-how** tra contraente e cliente.

In questa ipotesi, la PMI sviluppa la capacità interna di eseguire alcuni compiti importanti in tema di sicurezza quando ciò sia necessario. Un chiaro vantaggio può derivare dal fatto che l'organizzazione può regolare e gestire i costi futuri del contraente e può fornire un contributo significativo alle competenze fornite da un soggetto terzo specializzato.

Per stabilire se la valutazione del rischio mediante esternalizzazione parziale sia la decisione giusta per l'organizzazione, si può utilizzare il questionario seguente.

Domande per prendere una decisione	Risposta ☺ SI	Risposta ☹ NO
Ritenete necessario concentrarvi sempre di più sulle competenze caratteristiche e sui processi aziendali strategici, ma intendete anche migliorare la consapevolezza e le competenze interne nel campo della sicurezza delle informazioni?		
Riuscite a mettere a disposizione una - due persone che abbiano un'ampia ed approfondita conoscenza dell'organizzazione e possiedano inoltre la maggior parte delle caratteristiche seguenti? ▫ **Capacità di comprendere i processi aziendali e l'infrastruttura dell'organizzazione** ▫ Capacità di risoluzione dei problemi ▫ Capacità di analisi ▫ Capacità di lavorare in gruppo ▫ Doti di leadership ▫ Capacità di dedicare alcune giornate di lavoro all'apprendimento del metodo ▫ Rapporto di lavoro a lungo termine		
Avete un'infrastruttura IT sofisticata e relativamente ampia, ma un modello aziendale sufficientemente semplice?		
Tra i prodotti o servizi che offrite figurano operazioni finanziarie?		
Gestite un'azienda che è notevolmente esposta a rigidi vincoli legali e regolamentari, comunitari o nazionali, e/o mandati specifici?		

Come in precedenza, quanto maggiore è il numero delle domande a cui è stata data la risposta "SI" tanto maggiore è la probabilità che questo approccio alla valutazione del rischio si adatti all'azienda.

Come base per la collaborazione con il contraente, la decisione di esternalizzare in parte la valutazione del rischio richiede un accordo sul livello dei servizi. Gli elementi chiave di un accordo comprendono la certificazione professionale degli ingegneri esperti in sicurezza di cui il fornitore dispone, clausole di riservatezza, durata dell'incarico, assegnazione delle risorse, costi e metodologia da applicare. Anche in questo caso, le organizzazioni possono ordinare ai fornitori di eseguire la valutazione sulla base della metodologia ENISA qui proposta (cfr. capitolo 4. Un modello semplificato: panoramica).

Per l'esternalizzazione parziale della valutazione del rischio relativo alla sicurezza delle informazioni, l'accordo sul livello dei servizi dovrebbe fornire una risposta almeno alle seguenti domande.

- Il contraente accetta di seguire un modello predefinito di valutazione del rischio, che sia noto anche al cliente (ad esempio, il modello qui proposto)?
- Le questioni della **responsabilità** sono affrontate? Cosa accade, ad esempio, se nel corso della valutazione importanti attività aziendali vengono bloccate o rallentate a causa dell'incompetenza del fornitore ad eseguire la valutazione dell'infrastruttura IT e della rete?

- L'accordo identifica con chiarezza le **responsabilità**? Chi sarà responsabile per fare che cosa? Qual è il coinvolgimento dell'organizzazione in termini di risorse?
- **Il campo di applicazione** dell'attività è chiaramente documentato? Che cosa includerà il fornitore nel campo di applicazione dell'attività? Si raccomanda caldamente che il campo di applicazione comprenda l'intera gamma delle attività aziendali e l'infrastruttura sottostante. Altrimenti, è possibile che il risultato sia inadeguato o perfino fuorviante.
- Come si prevede avvenga il rispetto delle **norme di legge,** ad esempio, nel settore della tutela dei dati?
- Quali soluzioni sono previste per far sì che tutte le parti coinvolte nell'esternalizzazione, subappaltatori compresi, siano consapevoli delle proprie responsabilità in termini di sicurezza?
- Come si prevede di mantenere e verificare **l'integrità e la riservatezza del patrimonio aziendale**?
- Quali **controlli fisici ed elettronici** saranno utilizzati per restringere e delimitare agli utenti autorizzati l'accesso ai dati sensibili dell'organizzazione?
- **In caso di disastro** qual è **il livello di disponibilità dei servizi da mantenere?**
- Le condizioni generali prevedono **il diritto di sottoporre a verifica** le misure di sicurezza e di tutela delle informazioni adottate dal **fornitore**?
- **Le risorse minime, la competenza e la certificazione professionale del fornitore** sono espressi con chiarezza?
- Il contenuto, la frequenza e la struttura della rendicontazione sono definiti con chiarezza?

4. Un modello semplificato: panoramica

Questo capitolo presenta un modello semplificato di valutazione e gestione del rischio, utilizzabile dalle PMI per l'autovalutazione anche nel quadro di progetti di esternalizzazione, come indicato nel capitolo 3.

Generalmente i modelli esistenti di valutazione e gestione dei rischi per la sicurezza sono in gran parte incentrati sulle esigenze delle grandi organizzazioni. Oggi non esiste un modello semplice, concepito ad hoc per le piccole organizzazioni, almeno non sotto forma di linee guida pubblicamente disponibili. Alcune società di consulenza hanno sviluppato a tal fine delle buone prassi, che utilizzano però nel quadro dei progetti con la propria clientela. Altri modelli, pur affermando di essere adeguati alle PMI, restano troppo complessi per l'autovalutazione (per esempio, OCTAVE). D'altro canto, come è già stato affermato, la maggior parte delle PMI non può permettersi il costo dell'esternalizzazione totale a soggetti esterni.

Il nostro intento è quello di fornire alle PMI un modello semplice, efficiente ed economico per identificare e gestire i propri rischi per la sicurezza delle informazioni. **Questo modello semplificato fornisce alle piccole organizzazioni uno strumento per eseguire l'autovalutazione. Si basa sui principi, gli attributi ed i risultati di OCTAVE[2] ed è rapportato all'ambiente ed alle esigenze tipiche delle PMI. Infatti questo modello è compatibile anche con altri standard esistenti, come per esempio ISO 13335-2.**

Per un'azienda che cerchi di capire quali siano le sue esigenze in termini di sicurezza delle informazioni, questo modello racchiude sia una tecnica di autovalutazione basata sulla nozione di profilo di rischio, sia una tecnica di pianificazione della sicurezza. Diversamente da altre valutazioni imperniate sulla tecnologia, che si rivolgono unicamente ai rischi tecnologici, questo metodo si occupa dei rischi intrinseci e collegati al contesto, oltre ad essere imperniato sugli aspetti strategici e correlati alla prassi.

Il principale vantaggio del presente modello è dato dal fatto che esso può fornire un livello accettabile di sicurezza con un minimo sforzo in termini di valutazione e gestione. Ciò è dovuto ai seguenti aspetti che ne potenziano la praticabilità:

- il profilo di rischio dell'organizzazione può essere facilmente identificato;
- nelle piccole organizzazioni gli asset tipici sono dei dati di fatto;
- la protezione degli asset mediante misure (controlli) è predefinita tramite schede di controllo.

Questi vantaggi possono portare ad un'autovalutazione a basso costo, realizzata da gruppi con una modesta competenza in materia di sicurezza. Se l'autovalutazione viene eseguita attentamente, si consegue un livello accettabile di sicurezza.

Il modello di valutazione che qui si propone può essere applicato anche da non esperti. Nel corso della valutazione, il gruppo a ciò dedicato non deve fare i conti con una miriade di minacce ad asset vulnerabili. Si suggerisce piuttosto un livello predefinito di protezione, determinato in rapporto alla tipologia degli asset ed al livello di sicurezza necessario.

L'attività svolta per lo sviluppo del modello di rischio sottostante a questo approccio si basa sui seguenti assunti/elementi:

- **la valutazione dei rischi intrinseci.** Spesso l'ambiente può definire il contesto di rischio (rischio intrinseco) entro il quale un'azienda opera. Ad esempio, una piccola organizzazione di panificazione presenta un contesto di rischio significativamente inferiore rispetto ad una piccola organizzazione che fornisca assistenza sanitaria o servizi di intelligence ad altre imprese. A prescindere dalle misure di sicurezza, dalle infrastrutture e dalle relative entrate, le due tipologie di impresa operano in un ambiente di rischio totalmente diverso, che deve essere

[2] *Operationally Critical Threat, Asset, and Vulnerability Evaluation* e OCTAVE sono marchi di servizio della Carnegie Mellon University. OCTAVE è stato sviluppato dal Centro di coordinamento del CERT (*Computer Emergency Response Team*). Formatosi nel 1988 e tuttora esistente, si tratta del primo gruppo nato per rilevare gli incidenti di sicurezza informatica.

attentamente preso in considerazione prima di definire una strategia di sicurezza delle informazioni e di selezionare i controlli di sicurezza;

- **la variazione degli scenari di rischio (profili) riscontrabili nelle PMI**. Come d'altronde ci si poteva aspettare, abbiamo notato che, in termini di rischi intrinseci, tra le PMI i rischi sono piuttosto tipici nonostante la dispersione e per lo più, se raggruppati, essi tendono a formare profili generali di rischio applicabili ad un buon numero di PMI. A questo proposito, la nostra attività si è incentrata sull'elaborazione di modelli di minacce attraverso profili generali di rischio. I profili generali di rischio così sviluppati servono a riflettere il livello di rischio proprio dell'organizzazione. Successivamente, le misure sono state identificate e raggruppate a fronte dei rispettivi profili di rischio.

L'**approccio proposto è autodiretto**, nel senso che le persone dell'organizzazione si assumono la responsabilità di valutare i rischi, selezionare i controlli e pertanto stabilire la strategia dell'organizzazione in termini di sicurezza. Questa tecnica fa leva sulla conoscenza che le persone hanno delle prassi e dei processi relativi alla sicurezza della propria organizzazione per **a) comprendere quale sia la situazione attuale della prassi inerente la sicurezza all'interno dell'organizzazione**, **b) identificare i rischi cui sono esposti gli asset a maggiore criticità, c) stabilire un ordine di priorità delle aree in cui apportare miglioramenti e definire la strategia di sicurezza dell'organizzazione nel suo insieme.** Nel fare questo, si viene a coprire l'intero ciclo di vita della valutazione e della gestione del rischio.

Per l'applicazione del modello qui proposto deve operare un piccolo gruppo di persone provenienti dalle unità operative (o aziendali) e dal dipartimento IT, per affrontare insieme le esigenze di sicurezza dell'organizzazione bilanciando così due aspetti chiave della sicurezza, vale a dire le misure organizzative e le misure tecniche.

Le organizzazioni sono vivamente incoraggiate ad applicare le linee guida e le prassi migliori facenti parte di questo modello soltanto a titolo di piano a breve termine, per raggiungere l'obiettivo rapidamente ed efficacemente proteggendo le componenti cruciali e critiche della propria attività. Questo modello copre rischi significativi ai quali le PMI sono solitamente esposte. Tuttavia il modello qui proposto non intende sostituire in permanenza una valutazione completa ed esaustiva degli asset critici. Raccomandiamo vivamente questi "approfondimenti" per una migliore valutazione del rischio, specialmente se si utilizzano componenti complesse per asset di valore elevato.

L'introduzione di questo modello di valutazione e gestione del rischio intende perseguire i seguenti obiettivi:

- **migliorare le soglie europee esistenti in termini di sicurezza delle informazioni**. Il modello può servire per catalizzare ed accelerare l'impegno delle PMI verso la gestione del rischio relativo alla sicurezza delle informazioni, affrontando almeno i rischi elevati. Inoltre, il fatto di mirare agli scenari tipici di rischio può servire a migliorare, in ultima analisi, le soglie europee esistenti in termini di sicurezza delle informazioni;
- rispettare le esigenze delle imprese, il contesto ed i vincoli che si ritrovano tipicamente nell'ambiente delle PMI **evitando una terminologia specializzata ed eliminando i compiti molto impegnativi** previsti da quasi tutte le metodologie professionali esistenti e dagli standard di settore (vale a dire, valutazione del patrimonio informativo, analisi dell'impatto sull'azienda, identificazione dei requisiti di sicurezza, ecc.);
- **utilizzare un approccio autodiretto,** rapportato agli strumenti, alle risorse ed alle competenze che si possono tipicamente riscontrare nell'ambiente di una PMI;
- **concentrarsi sugli elementi critici e sui rischi più elevati**. Questo metodo vuole essere una guida semplice e facile per identificare e proteggere gli elementi ritenuti a maggior criticità per l'organizzazione;
- sviluppare un metodo di valutazione e gestione del rischio **indipendente dalle misure**. Per produrre un primo risultato pratico e realistico sono stati utilizzati i controlli OCTAVE. Tuttavia,

il metodo può utilizzare virtualmente tutti gli standard di controllo oggi disponibili (ISO, BS7799, NIST, BSI).

4.2 Ipotesi di lavoro

Oltre agli obiettivi precedentemente menzionati, per l'elaborazione di questa guida e del modello di valutazione del rischio che essa presenta sono state fatte alcune considerazioni/ipotesi:

- in molti casi la PMI può non essere consapevole della sicurezza informatica e, di conseguenza, può trarre vantaggio dall'accesso a materiali di sensibilizzazione, formazione ed orientamento;
- la creazione di un quadro di orientamento alla sicurezza tramite le associazioni di categoria delle PMI aiuterà a promuovere la comprensione delle questioni relative alla sicurezza tra coloro che sono meno preparati sul tema della sicurezza delle informazioni;
- le PMI rappresentano un'area prioritaria per la politica economica dell'UE e sono considerate di importanza chiave per la crescita socioeconomica dell'Unione europea;
- le PMI hanno solitamente un retroterra di passione imprenditoriale e risorse finanziarie limitate, con sistemi aziendali che sono spesso "assemblati" e pertanto eterogenei ed indipendenti;
- le politiche e gli schemi per la pianificazione della sicurezza delle informazioni e per il disaster recovery sono solitamente inesistenti. Inoltre, la comprensione del rischio relativo alla sicurezza delle informazioni nelle PMI non va molto al di là dei virus e dei software antivirus;
- la maggior parte dei dirigenti delle PMI comprende a fatica la terminologia scientifica complessa ed altamente tecnica riguardante la sicurezza delle informazioni;
- le piccole società operano solitamente all'interno di un contesto in cui l'ambiente di elaborazione dei dati, pur nella sua importanza per l'azienda, è standardizzato. Esse utilizzano pacchetti di software, prodotti da scaffale che consistono, in tutto o in parte, in "congegni" (con tutti i rischi potenziali a ciò associati). Esse sono inoltre collegate ad Internet, dove sono in agguato tante minacce per la sicurezza IT;
- le minacce di natura involontaria rappresentano alcuni dei massimi rischi di sicurezza per le PMI, eppure la formazione del personale ed i programmi di sensibilizzazione sono spesso trascurati. Anche quando il personale della PMI ha una conoscenza specifica dei sistemi informativi, può non possedere un know-how specifico in materia di sicurezza IT. Un fattore aggravante è dato dal fatto che in genere le società non possono permettersi di investire risorse sufficienti per la valutazione e la gestione del rischio.

4.3 Un approccio in quattro fasi

Il modello di valutazione del rischio qui proposto prevede **quattro fasi** per esaminare le questioni inerenti la sicurezza (dell'organizzazione e delle tecnologie), raccogliendo così in un ampio quadro olistico le esigenze in materia di sicurezza delle informazioni. Le quattro fasi del metodo sono delineate nella figura 2.

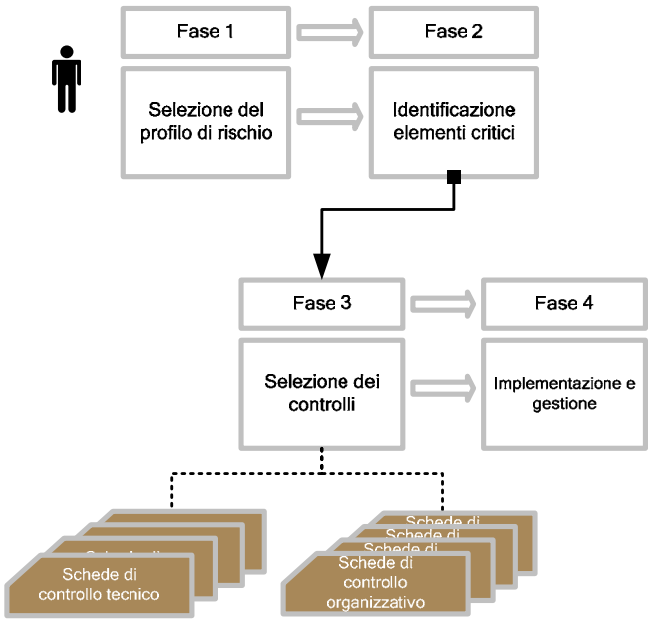

Figura 2. Le quattro fasi del modello di valutazione del rischio qui proposto

Il modello di valutazione del rischio è guidato da due elementi chiave: **1) il profilo di rischio dell'azienda e 2) l'identificazione degli asset critici**.

La valutazione del rischio è guidata da un gruppo di valutazione piccolo e interdisciplinare (da tre a cinque persone, personale interno, esterno o misto, a seconda della tipologia di implementazione, cfr. il capitolo 3.3 Come mettere in sicurezza le informazioni) il quale raccoglie ed analizza le informazioni e produce piani di riduzione del rischio basati sui rischi per la sicurezza dell'organizzazione. Per poter effettuare un'efficace valutazione del rischio, il gruppo deve possedere un'ampia conoscenza dell'attività dell'organizzazione (in altri termini, dei processi aziendali) e relativa infrastruttura IT.

Come punto di partenza, il gruppo di analisi **utilizza la tabella di valutazione del profilo di rischio per identificare il profilo di rischio dell'impresa.** Il passo successivo consiste nella **identificazione degli elementi critici dell'organizzazione** e dei relativi **requisiti di sicurezza** in termini di riservatezza, integrità e disponibilità.

Si procede successivamente con la selezione dei controlli (schede di controllo). Il processo di selezione è radicalmente semplificato grazie all'uso di schede standard di controllo. Il gruppo conclude il processo di selezione dei controlli **semplicemente "estraendo" le schede di controllo associate al rischio**, per l'organizzazione e per gli asset critici identificati, create per ogni livello di profilo di rischio, per ogni categoria di asset e per ogni requisito di sicurezza (riservatezza, integrità, disponibilità).

Le schede di controllo contengono controlli derivanti dalla metodologia OCTAVE. È stata adottata questa decisione perché questi controlli sono relativamente semplici e di facile comprensione da parte di persone non esperte in sicurezza. In alternativa, si possono utilizzare altri controlli di sicurezza. Ciò può rivelarsi necessario nel caso in cui la PMI disponga già di una politica di sicurezza basata su un altro standard (ad esempio, ISO 17799).

In ultimo, il gruppo di analisi stabilisce un ordine di priorità degli asset rispetto alla loro criticità, agli effetti sull'azienda ed al piano di protezione.

I paragrafi seguenti descrivono nel dettaglio le fasi di valutazione del rischio.

4.3.1 Fase 1: selezione del profilo di rischio

Durante questa fase il gruppo di valutazione valuta il profilo di rischio dell'impresa utilizzando un insieme predefinito di **criteri qualitativi**. Utilizzando la tabella di valutazione del profilo di rischio (Tabella 2) il gruppo è in grado di identificare il proprio contesto di rischio. Il contesto di rischio deriva dall'impresa e dall'ambiente esterno ad essa. Può essere suddiviso in **quattro aree di rischio: legale e regolamentare, reputazione e fiducia della clientela, produttività e stabilità finanziaria**.

Area di rischio	Alto	Medio	Basso
Legale e regolamentare	L'organizzazione gestisce informazioni sulla clientela di natura sensibile e personale, fra cui aspetti sanitari e dati personali critici, come definiti dalla normativa comunitaria sulla tutela dei dati personali	L'organizzazione gestisce informazioni sulla clientela di natura personale, ma non sensibile così come definite dalla normativa comunitaria sulla tutela dei dati personali	L'organizzazione non gestisce dati personali diversi da quelli del personale dipendente dell'organizzazione stessa
Produttività	L'organizzazione occupa più di 100 lavoratori, che hanno la necessità quotidiana di accedere alle applicazioni ed ai servizi dell'impresa	L'organizzazione occupa più di 50 lavoratori, che hanno la necessità quotidiana di accedere alle applicazioni ed ai servizi dell'impresa	L'organizzazione occupa meno di 10 lavoratori, che hanno la necessità quotidiana di accedere alle applicazioni ed ai servizi dell'impresa
Stabilità finanziaria	Le entrate annue dell'organizzazione sono superiori a 25 milioni di euro e/o le operazioni finanziarie con terzi o clienti avvengono nel quadro dell'attività imprenditoriale, come processo usuale	Le entrate annue dell'organizzazione sono inferiori a 25 milioni di euro	Le entrate annue dell'organizzazione sono inferiori a 5 milioni di euro
Reputazione e fiducia della clientela	L'indisponibilità o la qualità del servizio hanno un impatto diretto sull'attività dell'organizzazione e/o più del 70% della clientela ha l'accesso on line ai prodotti ed ai servizi dell'impresa	L'indisponibilità o la qualità del servizio possono avere un impatto indiretto sull'attività dell'organizzazione e/o meno del 5% della clientela ha l'accesso on line ai prodotti ed ai servizi dell'impresa	L'indisponibilità o la qualità del servizio non possono incidere, né direttamente, né indirettamente, sull'attività dell'organizzazione, né determinare una perdita di entrate

Tabella 2. Valutazione del profilo di rischio

Ogni area è classificata secondo tre classi di rischio: alto, medio e basso. Queste classi esprimono criteri quantitativi per l'organizzazione in questione rispetto all'area di rischio ed aiutano a identificare il livello di rischio. Il gruppo valuta i rischi identificati rispetto a ciascuna area allo scopo di elaborare il **profilo di rischio dell'organizzazione**.

Come regola generale, il rischio più elevato identificato in una determinata classe di rischio definisce il profilo di rischio complessivo dell'impresa. Un rischio alto nella classe dei rischi finanziari rappresenta un profilo di rischio alto. Analogamente, un rischio medio porta ad un profilo di rischio medio ed un rischio basso ad un profilo di rischio basso. Ad esempio, se nell'area "reputazione e fiducia della clientela", nell'area "legale e regolamentare" e nell'area "produttività" il rischio è basso, ma nell'area "stabilità finanziaria" il rischio è alto, il profilo di rischio complessivo dell'organizzazione è alto.

La definizione del profilo di rischio va considerata come una decisione importantissima, da cui scaturisce la selezione degli elementi critici e la loro protezione tramite le schede di controllo.

4.3.2 Fase 2: identificazione degli elementi critici

In questa fase, il gruppo di valutazione seleziona gli elementi critici sulla base della loro importanza relativa per l'organizzazione e definisce i requisiti di sicurezza per ogni elemento critico.

È normale che la direzione sappia quali siano gli **asset chiave** e utilizzi le proprie limitate risorse per concentrarsi sulla loro protezione. Il gruppo di valutazione stabilisce ciò che è importante per l'organizzazione (ad esempio, le informazioni) e seleziona gli asset che sono più importanti per l'organizzazione: gli **asset critici**.

La tabella seguente definisce le categorie degli asset e le tipologie prese in considerazione nel corso della selezione degli elementi critici. Si presta attenzione agli asset che vengono utilizzati per permettere all'organizzazione di svolgere la propria attività. Va rilevato che alcune tipologie di asset possono racchiudere ulteriori tipologie di asset: ad esempio, un'applicazione può comprendere server, postazioni di lavoro, router, porzioni di rete, ecc.

Va rilevato che l'elenco seguente è rappresentativo della maggior parte delle piccole imprese e non è esaustivo. Su richiesta (ad esempio, nelle versioni future di questo documento) si possono introdurre ulteriori asset. È possibile inoltre che alcune categorie di asset utilizzino altri asset per il proprio funzionamento: ad esempio, un'applicazione potrebbe comprendere un server, alcune postazioni di lavoro, un dispositivo per il salvataggio dei dati ed un segmento di rete. Va rilevato che, oltre alla protezione del singolo asset, anche ciascuna delle sue componenti deve essere adeguatamente protetta.

Asset (categoria)	Descrizione	Asset (tipologie)
Sistemi	I sistemi informativi che elaborano ed immagazzinano le informazioni. I sistemi sono una combinazione di informazioni, software ed hardware. Un host, un client, un server, o una rete possono essere considerati un sistema. I sistemi critici sono quelli identificati come essenziali per poter fornire senza soluzione di continuità i servizi dell'impresa o l'offerta dei prodotti, quelli che immagazzinano le informazioni critiche per l'impresa (dati proprietari o della clientela) oppure quelli che sono esposti al mondo esterno per le funzioni o i servizi dell'impresa	Server Computer portatile Postazione di lavoro Archiviazione e backup Dispositivo di memorizzazione di massa (storage)
Rete	Si tratta di dispositivi importanti per le reti dell'organizzazione: router, switch e modem sono tutti esempi di questa classe di componenti. Idem dicasi per i componenti/dispositivi wireless, come telefoni cellulari ed access point wireless che il personale utilizza per accedere alle informazioni (ad esempio, alla posta elettronica). Tipicamente, le reti critiche sono quelle che vengono utilizzate a supporto di applicazioni o sistemi critici essenziali, oppure quelle che sono condivise con terzi e solitamente con reti non affidabili	Router Cablaggio Gateway Access point wireless Segmento di rete (ad esempio, cablaggio e attrezzature tra due computer) Altro (satellitare, laser)
Persone	Le persone che operano nell'organizzazione, comprese le loro capacità tecniche, la formazione, le conoscenze e l'esperienza. Le persone critiche sono quelle che ricoprono un ruolo chiave nei processi produttivi o operativi. Va attribuita importanza alle risorse (persone) critiche che sono considerate insostituibili o rappresentano un possibile anello debole	Gestione dell'impresa e delle risorse umane Funzionamento e tecnologia Ricerca e sviluppo Commerciale e marketing Contraenti e terzi
Applicazioni	Applicazioni critiche: le applicazioni che rappresentano una componente chiave o fanno parte dell'offerta di prodotti e servizi. Tipicamente l'interruzione di applicazioni critiche può provocare gravi ripercussioni o la congestione dei processi successivi	Controllo finanziario Assistenza alla clientela Logistica Commercio elettronico Pianificazione delle risorse aziendali (Enterprise Resource Planning - ERP)

Tabella 3. Elenco degli asset

Durante la fase di identificazione, è essenziale tener conto delle opinioni dell'alta dirigenza (o della proprietà). La partecipazione dei vertici all'analisi garantisce che il valore delle informazioni per l'impresa sia adeguatamente identificato.

Successivamente, occorre procedere alla valutazione dei requisiti di sicurezza degli asset più importanti, i quali esprimono le qualità di un asset che è importante proteggere. Nel corso del processo di valutazione, sono stati esaminati i seguenti requisiti di sicurezza:

- riservatezza – la necessità di far sì che i dati proprietari, sensibili o personali restino privati e non accessibili a tutti coloro il cui accesso non sia stato preventivamente autorizzato,
- integrità – l'autenticità, l'accuratezza e la completezza di un asset,
- disponibilità – la qualità dell'asset di essere disponibile al momento dell'uso.

Per identificare i requisiti di sicurezza più importanti rispetto alle varie categorie di asset, il gruppo di valutazione può utilizzare i criteri di selezione dei requisiti di cui alla tabella 4. I requisiti di sicurezza servono successivamente per la selezione delle schede di controllo tecnico. La selezione dei requisiti di sicurezza è stata sviluppata come una guida semplice e pratica all'identificazione delle qualità, in termini di sicurezza, degli asset critici precedentemente selezionati. I requisiti segnalano l'importanza dell'asset e rappresentano un indicatore del livello di protezione occorrente (utilizzando, ad esempio, controlli appropriati).

La tabella seguente può aiutare il gruppo di valutazione a identificare i requisiti di sicurezza per le varie categorie di asset precedentemente menzionate.

Asset (categoria)	Riservatezza	Integrità	Disponibilità
Sistemi	Un sistema che ha requisiti di riservatezza gestisce spesso informazioni societarie proprietarie (ricerca e sviluppo), informazioni sulla clientela, dati sensibili sulla clientela, di natura sanitaria o personale	I sistemi che hanno requisiti di integrità gestiscono tipicamente transazioni di natura finanziaria, acquisto di beni o commercio elettronico	I requisiti di disponibilità si incontrano nei sistemi sensibili all'attività quotidiana, dove un guasto comporta solitamente costi e spese generali in termini di assegnazione delle risorse
Rete	Una rete con requisiti di riservatezza copre tipicamente lo scambio di comunicazioni ed informazioni attraverso ambienti poco sicuri e poco affidabili	I requisiti di integrità della rete sono necessari tipicamente quando le transazioni avvengono attraverso reti pubbliche o reti metropolitane condivise o provider di telecomunicazioni	I requisiti di disponibilità sono necessari, in particolare, quando la rete viene utilizzata per l'assistenza alla clientela o l'offerta di servizi o prodotti
Persone	I requisiti di riservatezza si incontrano tipicamente quando le persone gestiscono informazioni proprietarie e riservate relative all'organizzazione che, se divulgate, potrebbero danneggiare il buon nome dell'organizzazione e la clientela	I requisiti di integrità si incontrano quando le persone interessate condividono alcuni elementi riservati, quali chiavi crittografiche o password. Il possesso di conoscenze di questo tipo introduce un rischio legato al fattore umano che va affrontato con controlli ispettivi	I requisiti di disponibilità riguardano le persone particolarmente importanti, le persone che sono risorse critiche affinché l'azienda possa continuare ad offrire prodotti e servizi senza soluzione di continuità
Applicazioni	Le applicazioni che hanno requisiti di riservatezza gestiscono spesso informazioni societarie proprietarie (ricerca e sviluppo), informazioni sulla clientela, dati sensibili sulla clientela, di natura sanitaria o personale	Le applicazioni che hanno requisiti di integrità gestiscono tipicamente transazioni di natura finanziaria, acquisto di beni o commercio elettronico	I requisiti di disponibilità si incontrano nelle applicazioni sensibili all'attività quotidiana, dove un guasto comporta solitamente costi e spese generali in termini di assegnazione delle risorse

Tabella 4. Selezione dei requisiti di sicurezza

Al termine del processo, il gruppo di valutazione dovrebbe disporre di una tabella degli asset critici classificati per categoria ed un elenco dei requisiti di sicurezza corrispondenti, insieme con elementi giustificativi o informazioni a supporto, presi in esame nel corso della valutazione.

Il risultato sarà poi utilizzato come bagaglio iniziale nella fase 3 – selezione delle schede di controllo, come indicato nel capitolo successivo.

4.3.3 Fase 3: selezione delle schede di controllo

Durante la fase 3 il gruppo di valutazione seleziona i controlli più appropriati sulla base del profilo di rischio selezionato per ogni categoria di rischio e degli asset identificati come critici (requisiti compresi). I controlli sono suddivisi in due categorie: controlli organizzativi e controlli tecnici.

L'organizzazione è considerata come un tutt'uno da proteggere nel suo insieme. I controlli di sicurezza di tipo organizzativo sono generalmente di ampio respiro e si applicano all'organizzazione in maniera orizzontale. Al contrario, i controlli tecnici sono mirati a realizzare la protezione specifica richiesta dagli asset stessi (ad esempio, consentendo la disponibilità di una componente critica della rete).

I controlli sono ulteriormente raggruppati in schede di controllo. Il gruppo che effettua la valutazione di una PMI ha a disposizione due tipologie di schede di controllo:

- le schede di controllo che contengono controlli applicabili orizzontalmente a tutta l'organizzazione e riguardano le prassi e le procedure gestionali;
- le schede di controllo che si riferiscono ad asset critici e sono specifiche per le singole categorie di asset. Le schede di controllo sono essenzialmente predefinite: i controlli sono raggruppati a seconda dei profili di rischio e dei requisiti di sicurezza degli asset.

La tabella 5 elenca le categorie dei controlli, la loro articolazione e la loro denominazione, così come esse sono prese in considerazione nell'ambito di questo modello. Come già indicato, questi controlli sono stati ripresi da OCTAVE in ragione della loro semplicità. Al loro posto, si possono utilizzare altri controlli (ad esempio, ISO 17799, IT-Grundschutz, ecc.). Una descrizione più dettagliata si può trovare in ....

Categoria dei controlli	Controllo n.	Denominazione del controllo
Organizzativi	**SP1**	Sensibilizzazione alla sicurezza e formazione
	SP2	Strategia in materia di sicurezza
	SP3	Gestione della sicurezza
	SP4	Politiche e norme di sicurezza
	SP5	Gestione collaborativa della sicurezza
	SP6	Piani alternativi/disaster recovery
Tecnici	**OP1.1**	Piani e procedure per la sicurezza fisica
	OP1.2	Controllo fisico degli accessi
	OP1.3	Monitoraggio e verifica della sicurezza fisica
	OP2.1	Gestione dei sistemi e della rete
	OP2.2	Strumenti di amministrazione del sistema
	OP2.3	Monitoraggio e verifica sicurezza IT
	OP2.4	Autenticazione ed autorizzazione
	OP2.5	Gestione delle vulnerabilità
	OP2.6	Crittografia
	OP2.7	Architettura e concezione della sicurezza
	OP3.1	Gestione degli incidenti
	OP3.2	Prassi generali del personale

Tabella 5. Controlli utilizzati nel modello qui presentato

Conseguentemente, la fase 3 del modello di valutazione qui proposto consiste in due passaggi separati ma egualmente importanti:

- passaggio A: selezione dei controlli organizzativi;
- passaggio B: selezione dei controlli tecnici.

Durante questi passaggi i controlli riguardano l'organizzazione (in quanto singolo bene importante) e gli asset identificati come critici.

Selezione delle schede di controllo organizzativo

La selezione delle schede di controllo organizzativo avviene in maniera relativamente diretta: i controlli organizzativi sono disponibili per ogni profilo di rischio (definito nella matrice relativa ai vari profili di rischio). La tabella seguente assegna i controlli organizzativi ai profili di rischio di cui al capitolo

4.3.1 Fase 1: selezione del profilo di rischio. Si raccomanda di effettuare i controlli elencati qui di seguito per attenuare i rispettivi rischi organizzativi. Per una descrizione dettagliata dei controlli, cfr. Allegato C. Controlli organizzativi.

Aree di rischio	Alto	Medio	Basso
Legale e regolamentare	(SP1) (SP4)	(SP1) (SP4)	SP1.1
Produttività	(SP3) (SP4) (SP6) (SP5)	(SP4) (SP6)	SP4.1
Stabilità finanziaria	(SP2) (SP1) (SP4)	(SP4)	SP4.1
Reputazione e fiducia della clientela	(SP1) (SP5)	(SP4) (SP1)	SP4.1

Tabella 6. Schede di controllo organizzativo

Selezione delle schede di controllo tecnico

Sulla base del profilo di rischio e dei requisiti di sicurezza, per la protezione degli asset critici il gruppo di valutazione può utilizzare le schede di controllo basate sugli asset (nel prosieguo "schede di controllo tecnico" - cfr. tabella 7), identificando così i controlli più appropriati.

Schede di controllo tecnico			
Asset	**Rischio alto**	**Rischio medio**	**Rischio basso**
Applicazione	**CC-1A**	**CC-2°**	**CC-3A**
Sistema	**CC-1S**	**CC-2S**	**CC-3S**
Rete	**CC-1N**	**CC-2N**	**CC-3N**

Persone	CC-1P	CC-2P	CC-3P

Tabella 7. Schede di controllo tecnico

Le schede di controllo tecnico sono raggruppate essenzialmente in tre categorie, corrispondenti al profilo di rischio dell'organizzazione, alla categoria di asset ed ai requisiti di sicurezza. Ad esempio, un gruppo di valutazione che si trovi ad affrontare un profilo di rischio alto per l'organizzazione individuerà requisiti di sicurezza diversi rispetto ad un profilo di rischio medio o basso. Ogni scheda di controllo prevede un certo numero di controlli (cfr. Allegato B. Schede di controllo tecnico) onde affrontare l'intera gamma dei rischi e dei requisiti di sicurezza necessari per quel particolare profilo e derivanti dai requisiti di sicurezza precedentemente selezionati. Una descrizione più dettagliata dei controlli previsti dalle schede di controllo figura all'allegato D, Controlli tecnici.

Ai fini della presentazione, aggiungiamo a questo punto la scheda di controllo CC-1A. Come indicato in tabella, la scheda si adatta alla protezione di un'applicazione in uno scenario ad alto rischio (profilo di rischio alto).

Scheda di controllo tecnico	**CC-1A**									
Profilo di rischio	**Alto**									
Categoria di asset	**Applicazione**									
Requisiti di sicurezza	**Sicurezza fisica**	**Gestione dei sistemi e della rete**	**Strumenti di amministrazione del sistema**	**Monitoraggio e verifica sicurezza IT**	**Autenticazione ed autorizzazione**	**Gestione delle vulnerabilità**	**Crittografia**	**Architettura e concezione della sicurezza**	**Gestione degli incidenti**	**Prassi generali del personale**
Riservatezza		2.1.3			2.4.2	2.5.1	2.6.1			
Integrità		2.1.4			2.4.2	2.5.1	2.6.1			
Disponibilità		2.1.6								

Tabella 8. Esempio di scheda di controllo per un'applicazione con profilo di rischio alto

Il gruppo di valutazione, utilizzando i requisiti di sicurezza precedentemente identificati e la scheda di controllo può successivamente identificare controlli più specifici (ad esempio, controlli relativi alla disponibilità, alla riservatezza o all'integrità). Va rilevato che nei casi in cui sia stato selezionato più di un requisito, i controlli applicabili a quel determinato asset sono dati dalla somma dei controlli relativi a ciascun requisito.

4.3.4 Fase 4: implementazione e gestione

Nel corso della fase 4, sulla scorta degli elementi già valutati, il gruppo di valutazione elabora piani di riduzione del rischio per affrontare i rischi a cui sono esposti gli asset critici.

Dopo aver individuato 1) il profilo di rischio dell'organizzazione, 2) gli asset critici e 3) le schede di controllo, il gruppo di valutazione pianifica l'implementazione dei controlli selezionati. Si prevede che, a causa delle risorse limitate disponibili, le PMI non saranno in grado di implementare in un colpo solo tutti i controlli identificati per tutti gli asset critici. A questo proposito, un elemento chiave di successo per la riduzione del rischio è dato dalla definizione di un ordine di priorità.

Il piano di implementazione definisce come l'organizzazione intenda innalzare o conservare il livello esistente di sicurezza. L'obiettivo consiste nel fornire un orientamento per i futuri sforzi in tema di sicurezza delle informazioni, piuttosto che nel trovare una soluzione immediata per ogni elemento di vulnerabilità e preoccupazione.

Qui di seguito sono riportati alcuni criteri per stabilire un ordine di priorità delle azioni volte ad implementare le schede di controllo già identificate. Anche se non tutti questi criteri sono applicabili in tutte le imprese, essi possono servire come guida generale.

- **Allineamento strategico con gli obiettivi dell'organizzazione.** L'asset in questione va direttamente a supporto degli obiettivi documentati dell'organizzazione e/o dei piani di lavoro divisionali? Quali sono gli obiettivi generali e/o specifici dei piani di lavoro che saranno così supportati? E come?
- **Impegno verso un miglioramento continuo.** L'asset in questione serve per il miglioramento continuo di una determinata divisione? Qual è l'asset interessato dal miglioramento continuo? Come fa, questo asset, a supportare obiettivi di miglioramento continuo?
- **Vincoli legali o regolamentari.** Se un asset è necessario per far fronte agli obblighi di legge, ciò si rifletterà nell'ordine di priorità da stabilire.
- **Vantaggi sistemici.** I vantaggi sistemici comprendono un miglior servizio alla clientela per svariati gruppi di clienti. Un ordine di priorità più elevato sarà attribuito ai gruppi di clienti considerati critici. Tuttavia, quanto più grande è il gruppo interessato, maggiori sono i vantaggi.
- **Risparmio di costi/tempo.** La stima del risparmio in termini di costi e/o tempo comprende il tempo del personale e della clientela, la creazione di reddito e le riduzioni dirette di budget/costi.
- **Riduzione del rischio.** A seguito del progetto, le informazioni e/o i servizi impediranno la perdita di reddito e/o il mancato rispetto delle politiche o degli obblighi legali e di audit.

Il passo successivo è dato dal processo di pianificazione, il quale indica il calendario preciso dell'implementazione degli strumenti e delle procedure di sicurezza, con il relativo monitoraggio.

In quasi tutti i casi, una domanda chiave da porsi riguarda l'adeguatezza o meno, la competenza o meno, delle risorse interne di cui si dispone per il piano di implementazione. In altre parole, può darsi che sia necessario prendere una decisione sull'opportunità di svolgere all'interno, o di esternalizzare, l'attività correlata di implementazione e gestione.

5. Linee guida per l'autovalutazione, corredate da due esempi

In questo capitolo si presenta una più dettagliata suddivisione, in passaggi logici, delle quattro fasi. Ciò serve ad aiutare le PMI 1) ad identificare il proprio profilo di rischio, 2) ad identificare gli asset critici che devono essere messi in sicurezza, 3) a selezionare i controlli e le soluzioni per migliorare la sicurezza ed in ultimo 4) ad elaborare piani di miglioramento. Tuttavia, le azioni e le soluzioni che si possono applicare alle PMI non si limitano assolutamente a quelle qui indicate.

Ancora una volta, le organizzazioni sono vivamente incoraggiate a seguire le linee guida e le prassi migliori incluse in questo metodo soltanto a titolo di piano a breve termine e per un obiettivo di protezione rapida ed efficace delle componenti cruciali e critiche della propria azienda. Tuttavia, questo processo non sostituisce un approccio alla valutazione del rischio completo ed esaustivo, che si raccomanda vivamente come base per una strategia di gestione del rischio a lungo termine.

Prima di cercare di utilizzare questo metodo, le PMI devono comprendere i suoi tre elementi specifici, qui riassunti:

- un piccolo gruppo di analisi interdisciplinare, composto da tre-cinque persone, guida il processo di valutazione del rischio. Il gruppo di analisi, per poter svolgere tutte le attività di valutazione del rischio, deve disporre collettivamente di una visione piuttosto ampia dell'attività e dei processi di sicurezza dell'organizzazione. Per questo motivo, il metodo non prevede seminari formali di raccolta dei dati come momento di avvio della valutazione;
- il metodo comprende una limitata esplorazione dell'infrastruttura informatica. Poiché le piccole organizzazioni spesso esternalizzano i propri servizi e le proprie funzioni IT, esse tipicamente non sviluppano al proprio interno le capacità organizzative atte a gestire ed interpretare i risultati degli strumenti di valutazione delle vulnerabilità. Tuttavia, il fatto che l'organizzazione non disponga della capacità di gestire questi strumenti, non significa che essa non possa darsi una propria strategia di protezione;
- anziché limitarsi ad utilizzare i dati relativi alle vulnerabilità per affinare la propria visione delle prassi correnti in materia di sicurezza, l'organizzazione che compia una valutazione deve esaminare i processi impiegati nell'ottica di configurare e conservare in sicurezza la propria infrastruttura informatica.

Il documento è strutturato in fasi e passaggi, come i blocchi di una costruzione. Per ogni fase vengono forniti due esempi. Gli esempi utilizzano i seguenti scenari aziendali:

- **nell'esempio A**, prendiamo in esame il caso particolare di una società di medie dimensioni che offre servizi di assistenza sanitaria on line, fornendo un supporto medico on line ai medici che chiedono servizi di consulenza per i propri pazienti ed un aggiornamento farmacologico. La banca dati a supporto dell'applicazione ovviamente contiene dati critici e riservati di natura personale. La società occupa 100 lavoratori ed ha tre dipartimenti: il dipartimento di supporto medico e farmacologico, il dipartimento di scienze mediche ed il dipartimento gestionale, che comprende le attività relative alle risorse umane ed al controllo finanziario;
- **la società dell'esempio B** è una società legale di piccole dimensioni. In questo caso, i sistemi IT sono utilizzati principalmente per raccogliere le informazioni sui procedimenti, per lo scambio di messaggi di posta elettronica e per preparare ed elaborare i documenti occorrenti. La società occupa cinque avvocati ed una segretaria.

Ogni fase è illustrata da una figura (diagramma del flusso di lavoro); a fianco delle descrizioni, nei riquadri tratteggiati sono forniti cenni relativi ai singoli passaggi.

Fase 1: selezione del profilo di rischio

Il gruppo di analisi prende in considerazione gli aspetti di rischio di cui è portatrice l'azienda in termini di protezione delle informazioni che possano a) incidere direttamente o indirettamente sulla reputazione e sulla fiducia della clientela, b) determinare il mancato rispetto degli obblighi di legge e regolamentari, c) provocare perdite finanziarie e d) diminuire la produttività. Successivamente, utilizzando la tabella di valutazione del profilo di rischio, il gruppo seleziona il livello di rischio corrispondente ad ogni area di rischio. Le aree specificate sono le seguenti: legale e regolamentare, produttività, stabilità finanziaria, reputazione e fiducia della clientela. Come illustrato dalla figura 3, questa fase prevede due passaggi.

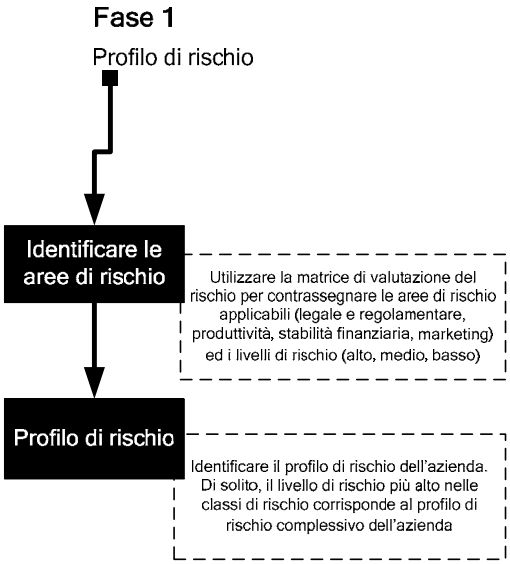

Figura 3. Fase 1: flusso di lavoro per la selezione del profilo di rischio

Per individuare il livello di rischio, attuale o potenziale, il gruppo di analisi dovrebbe evidenziare le aree di rischio e leggere la descrizione corrispondente in ciascuna colonna. Si scelgono le aree di rischio che sono più vicine al proprio profilo aziendale. Si deve seguire questo processo per ogni area di rischio. Al termine, dovrebbe risultare una MATRICE da cui emerga il livello di rischio corrispondente a ciascuna area di rischio.

Esempio A (profilo di rischio alto)

Nell'esempio A il gruppo di analisi utilizza la **tabella di valutazione del profilo di rischio** per identificare il contesto di rischio dell'impresa. Il gruppo identifica un livello di rischio alto (contrassegnato in rosso) nell'area legale e regolamentare, poiché l'azienda gestisce informazioni sulla clientela di natura sensibile e personale. Nel contempo, il gruppo individua un livello di rischio alto (contrassegnato in rosso) nell'area della produttività, visto che l'azienda occupa 100 lavoratori, un livello di rischio medio (contrassegnato in arancione) nell'area della stabilità finanziaria ed un livello di rischio basso (contrassegnato in blu) nell'area della reputazione e fiducia della clientela, come risulta dalla tabella seguente.

Area di rischio	Alto	Medio	Basso
Legale e regolamentare	**L'azienda gestisce informazioni sulla clientela di natura sensibile e personale, fra cui aspetti sanitari e dati personali critici, come definiti dalla normativa comunitaria sulla tutela dei dati personali**	L'azienda gestisce le informazioni sulla clientela di natura personale, ma non sensibile così come definite dalla normativa comunitaria sulla tutela dei dati personali	L'azienda non gestisce dati personali diversi da quelli del personale dipendente dell'organizzazione stessa
Produttività	**L'azienda occupa più di 100 lavoratori, che hanno la necessità quotidiana di accedere alle applicazioni ed ai servizi dell'impresa**	L'azienda occupa più di 50 lavoratori, che hanno la necessità quotidiana di accedere alle applicazioni ed ai servizi dell'impresa	L'azienda occupa meno di 10 lavoratori, che hanno la necessità quotidiana di accedere alle applicazioni ed ai servizi dell'impresa
Stabilità finanziaria	Le entrate annue sono superiori a 25 milioni di euro e/o le operazioni finanziarie con terzi o clienti avvengono nel quadro dell'attività imprenditoriale, come processo usuale	**Le entrate annue sono inferiori a 25 milioni di euro**	Le entrate annue sono inferiori a 5 milioni di euro
Reputazione e fiducia della clientela	L'indisponibilità o la qualità del servizio hanno un impatto diretto sul profilo dell'azienda e/o più del 70% della clientela ha l'accesso on line ai prodotti ed ai servizi dell'impresa	L'indisponibilità o la qualità del servizio possono avere un impatto indiretto sul profilo dell'azienda e/o meno del 5% della clientela ha l'accesso on line ai prodotti ed ai servizi dell'impresa	**L'indisponibilità o la qualità del servizio non possono incidere, né direttamente, né indirettamente, sul profilo dell'azienda, né determinare una perdita di entrate**

Tabella 9. Valutazione del profilo di rischio: esempio A

Successivamente, si provvede a determinare il profilo di rischio dell'azienda. Le aree di rischio connotano il contesto complessivo di rischio. **Si raccomanda che il profilo di rischio corrisponda al livello più elevato identificato nelle sottostanti aree di rischio della matrice del rischio.**

La tabella seguente illustra i livelli di rischio identificati nelle aree di rischio predefinite ed indica dove l'organizzazione dovrebbe concentrare i propri sforzi per applicare controlli di sicurezza adeguati. La tabella può essere utilizzata anche per stabilire delle priorità. Se il livello di rischio è alto vi è la necessità urgente di apportare miglioramenti, mentre se il livello di rischio è basso le azioni individuate possono essere prese in considerazione in un momento successivo.

Aree di rischio	Livello di rischio	Profilo di rischio
Legale e regolamentare	**Alto**	**Alto**
Produttività	**Alto**	
Stabilità finanziaria	**Medio**	
Reputazione e fiducia della clientela	**Basso**	

Tabella 10. Profilo di rischio dell'organizzazione: esempio A

Esempio B (profilo di rischio medio)

Nell'esempio B, il gruppo utilizza la **tabella di valutazione del profilo di rischio** per individuare il contesto di rischio dell'impresa. Il gruppo di analisi identifica un livello di rischio basso (contrassegnato in blu) nell'area legale e regolamentare, poiché l'azienda non gestisce dati personali diversi da quelli del personale dipendente dell'organizzazione stessa, un livello di rischio basso

nell'area della produttività (contrassegnato in blu), un livello di rischio basso (contrassegnato in blu) nell'area della stabilità finanziaria ed un livello di rischio medio (contrassegnato in arancione) nell'area della reputazione e fiducia della clientela, come risulta dalla tabella seguente.

Area di rischio	Alto	Medio	Basso
Legale e regolamentare	L'azienda gestisce informazioni sulla clientela di natura sensibile e personale, fra cui aspetti sanitari e dati personali critici, come definiti dalla normativa comunitaria sulla tutela dei dati personali	L'azienda gestisce le informazioni sulla clientela di natura personale, ma non sensibile così come definite dalla normativa comunitaria sulla tutela dei dati personali	**L'azienda non gestisce dati personali diversi da quelli del personale dipendente dell'organizzazione stessa**
Produttività	L'azienda occupa più di 100 lavoratori, che hanno la necessità quotidiana di accedere alle applicazioni ed ai servizi dell'impresa	L'azienda occupa più di 50 lavoratori, che hanno la necessità quotidiana di accedere alle applicazioni ed ai servizi dell'impresa	**L'azienda occupa meno di 10 lavoratori, che hanno la necessità quotidiana di accedere alle applicazioni ed ai servizi dell'impresa**
Stabilità finanziaria	Le entrate annue sono superiori a 25 milioni di euro e/o le operazioni finanziarie con terzi o clienti avvengono nel quadro dell'attività imprenditoriale, come processo usuale	Le entrate annue sono inferiori a 25 milioni di euro	**Le entrate annue sono inferiori a 5 milioni di euro**
Reputazione e fiducia della clientela	L'indisponibilità o la qualità del servizio hanno un impatto diretto sul profilo dell'azienda e/o più del 70% della clientela ha l'accesso on line ai prodotti ed ai servizi dell'impresa	**L'indisponibilità o la qualità del servizio possono avere un impatto indiretto sul profilo dell'azienda e/o meno del 5% della clientela ha l'accesso on line ai prodotti ed ai servizi dell'impresa**	L'indisponibilità o la qualità del servizio non possono incidere, né direttamente, né indirettamente, sul profilo dell'azienda, né determinare una perdita di entrate

Tabella 11. Valutazione del profilo di rischio: esempio B

Successivamente, si provvede a determinare il profilo di rischio dell'azienda. Le aree di rischio connotano il contesto complessivo di rischio. **Si raccomanda che il profilo di rischio complessivo corrisponda al livello più elevato identificato nelle singole aree di rischio della matrice del rischio.**

La tabella seguente illustra i livelli di rischio identificati nelle aree di rischio predefinite ed indica dove l'organizzazione dovrebbe concentrare i propri sforzi per applicare controlli di sicurezza adeguati. La tabella può essere utilizzata anche per stabilire delle priorità. Se il livello di rischio è alto vi è la necessità urgente di apportare miglioramenti, mentre se il livello di rischio è basso le azioni individuate possono essere prese in considerazione in un momento successivo.

Aree di rischio	Livello di rischio	Profilo di rischio
Legale e regolamentare	**Basso**	**Medio**
Produttività	**Basso**	
Stabilità finanziaria	**Basso**	
Reputazione e fiducia della clientela	**Medio**	

Tabella 12. Profilo di rischio dell'organizzazione: esempio B

Fase 2: identificazione degli asset critici

La fase 2, che riguarda la selezione degli asset critici dell'organizzazione, richiede decisioni che si ripercuotono sulla parte restante della valutazione. A seconda delle dimensioni dell'organizzazione, il patrimonio informativo censito durante questa fase potrebbe essere facilmente superiore ad un centinaio di unità. Per rendere gestibile l'analisi le PMI devono restringere il campo della valutazione selezionando gli asset a maggiore criticità rispetto al conseguimento della missione e degli obiettivi dell'organizzazione. Questi sono gli unici asset che saranno analizzati nel corso delle attività successive. Come delineato nella figura 4, questa fase comprende tre passaggi.

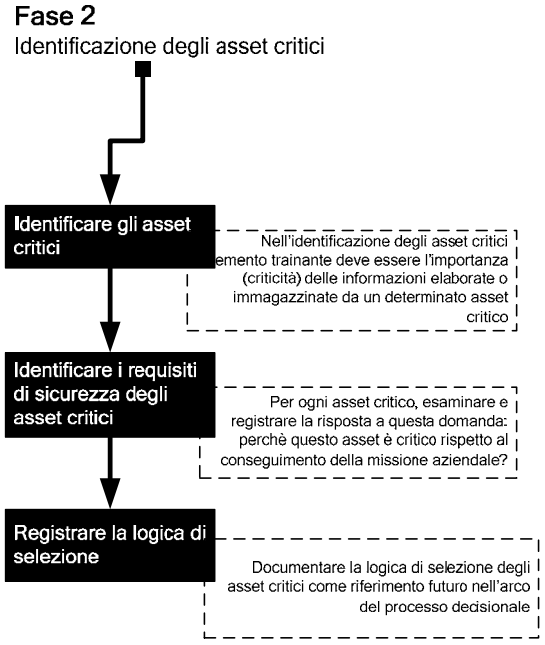

Figura 4. Fase 2: flusso di lavoro per l'identificazione degli asset critici

Passaggio 1. Selezionare i cinque asset critici più importanti dell'organizzazione

In fase di selezione degli asset critici, il gruppo di analisi non si limita a sceglierne soltanto cinque. Di solito, però, cinque asset sono sufficienti per consentire all'organizzazione di sviluppare, nel corso della fase 4, un buon insieme di piani di riduzione del rischio. Tuttavia, i componenti del gruppo di analisi devono valutare l'opportunità di utilizzare più o meno di cinque asset critici. Durante il relativo processo di selezione, i componenti del gruppo devono valutare quali asset potrebbero avere un significativo impatto negativo sull'organizzazione in uno dei seguenti scenari:

- **divulgazione** delle informazioni a persone non autorizzate,
- **modifica** delle informazioni senza autorizzazione,
- **perdita o distruzione** degli asset,
- **interruzione dell'accesso** ad un determinato asset o alle informazioni ivi immagazzinate.

Nei casi in cui gli asset critici siano di difficile identificazione, il gruppo deve tener conto delle funzioni/aree interne all'organizzazione: può trattarsi di progetti diversi, di gruppi di lavoro (gruppi di persone con un diverso mansionario) o anche di dipartimenti separati (risorse umane, amministrazione, marketing, commerciale, ecc.). Gli asset vanno poi elencati in ordine di importanza rispetto al processo aziendale. Dopo aver definito le aree che devono essere messe in sicurezza, o dopo aver riorganizzato gli asset aziendali, il passaggio successivo consiste nell'elencare tutti gli asset

rispetto al loro impatto sul processo aziendale. Un modo più fattibile per farlo consiste nel raggruppare gli asset rispetto al dipartimento o alla funzione interna all'organizzazione.

Nell'identificazione degli asset critici l'elemento trainante deve essere l'importanza (criticità) delle informazioni elaborate o immagazzinate da un determinato asset critico. Effettuando l'analisi per scomposizione, i componenti del gruppo possono individuare facilmente dove e come le informazioni siano immagazzinate o utilizzate.

Passaggio 2. Registrare la logica di selezione di ciascun asset critico

Quando, nel passaggio 1, si effettua la selezione degli asset critici, si procede anche a discutere di alcune questioni ad essi attinenti. Nel passaggio 2 bisogna documentare la logica di selezione degli asset critici a scopo di futuro riferimento nell'arco del processo decisionale. Inoltre, la comprensione del perchè un determinato asset sia di importanza critica può consentire meglio la definizione dei requisiti di sicurezza nel corso del passaggio successivo. Per ogni asset critico, occorre porsi le seguenti domande e dare ad esse una risposta.

- Perchè questo asset è critico rispetto al conseguimento della missione dell'organizzazione?
- Chi lo controlla?
- Chi ne è responsabile?
- Chi lo utilizza?
- Come è utilizzato?

Queste domande sono incentrate sul come gli asset siano utilizzati e sul perchè essi siano importanti. Se non si riesce a dare una risposta a tutte queste domande, occorre individuare le persone interne all'organizzazione che siano in grado di fornire le risposte, inserendole nel gruppo di analisi. Le informazioni raccolte rispondendo a queste domande saranno utili in un momento successivo del processo. A questo proposito, le informazioni qui raccolte devono essere registrate attentamente.

Passaggio 3. Identificare i requisiti di sicurezza degli asset critici

In generale, quando si descrive il requisito di sicurezza di un asset, occorre capire quale ne sia l'aspetto veramente importante. Per il patrimonio informativo, i requisiti di sicurezza riguardano in particolare la riservatezza, l'integrità e la disponibilità delle informazioni.

I requisiti di sicurezza possono variare in rapporto alle diverse categorie degli asset, ma per la successiva selezione delle modalità di controllo è essenziale una loro attenta selezione. In altre parole, se il requisito della disponibilità è elevato, i relativi controlli devono essere altrettanto elevati.

Il gruppo di analisi utilizza i **criteri per la selezione dei requisiti** qui forniti per identificare i requisiti di sicurezza più importanti. **I requisiti di sicurezza degli asset sono utilizzati successivamente per la selezione delle schede di controllo.** Tali criteri sono stati sviluppati a mo' di guida semplice e pratica per valutare i requisiti di sicurezza (in termini di riservatezza, integrità e disponibilità) degli asset critici selezionati. È la valutazione a sottolineare l'importanza degli attributi in termini di sicurezza di un determinato asset e a indicarne i controlli più adeguati per la relativa protezione.

Come risultato finale, il gruppo di analisi dovrebbe disporre di **una tabella in cui sono elencati gli asset critici, insieme con una breve descrizione della loro importanza per il conseguimento della missione aziendale, gli elementi di base ed i requisiti di sicurezza.**

Per tutti e tre i passaggi precedentemente esposti possono essere utilizzate le tabelle della sezione 4.3.2 per identificare gli asset ed i relativi requisiti (cfr. Tabella 3 e Tabella 4).

Esempio A (profilo di rischio: alto, asset critico: applicazione, fase 2)

[Passaggio 1] Nell'esempio A, l'asset a maggiore criticità è individuato nell'applicazione web, che fornisce un sostegno on line ai clienti – i medici. Questa applicazione è essenziale per l'azienda, in quanto essa rappresenta l'elemento più importante dell'offerta di servizi e pertanto è selezionata come l'asset più critico.

[Passaggio 2] Nel passaggio successivo, i componenti del gruppo documentano gli elementi che compongono l'asset e la logica della selezione. Essi identificano così la banca dati che raccoglie le informazioni riguardanti i clienti, il segmento di rete che supporta la connessione con le reti interne ed esterne, il server web ed il firewall in quanto componenti essenziali dell'asset in questione.

[Passaggio 3] Successivamente, si identificano i requisiti di sicurezza. Utilizzando la tabella seguente (Tabella 13), il gruppo individua i riquadri che si prestano ai propri requisiti. Nell'esempio A, il gruppo seleziona il requisito della riservatezza rispetto alla banca dati, visto che i dati ivi raccolti riguardano i clienti della società; il gruppo seleziona inoltre i requisiti della disponibilità e della riservatezza rispetto alla rete, in quanto la rete trasmette informazioni che devono rimanere intatte e riservate per poter completare le transazioni o le richieste.

Asset	Riservatezza	Integrità	Disponibilità
Sistemi	Un sistema che ha requisiti di riservatezza gestisce spesso informazioni societarie proprietarie (ricerca e sviluppo), informazioni sulla clientela, dati sensibili sulla clientela, di natura sanitaria o personale	I sistemi che hanno requisiti di integrità gestiscono tipicamente transazioni di natura finanziaria, acquisto di beni o commercio elettronico	I requisiti di disponibilità si incontrano nei sistemi sensibili all'attività quotidiana, dove un guasto comporta solitamente costi e spese generali in termini di assegnazione delle risorse
Rete	Una rete con requisiti di riservatezza copre tipicamente lo scambio di comunicazioni e informazioni attraverso ambienti poco sicuri e poco affidabili	I requisiti di integrità della rete sono necessari tipicamente quando le transazioni avvengono attraverso reti pubbliche o reti metropolitane condivise o provider di telecomunicazioni	I requisiti di disponibilità sono necessari, in particolare, quando la rete viene utilizzata per l'assistenza alla clientela o l'offerta di servizi o prodotti
Persone	I requisiti di riservatezza si incontrano tipicamente quando le persone gestiscono informazioni proprietarie e riservate relative all'organizzazione che, se divulgate, potrebbero danneggiare il buon nome dell'organizzazione e la clientela	I requisiti di integrità si incontrano quando le persone interessate condividono alcuni elementi segreti riservati, quali chiavi crittografiche o password. Il possesso di conoscenze di questo tipo introduce un rischio legato al fattore umano che va affrontato con controlli ispettivi	I requisiti di disponibilità riguardano le persone particolarmente importanti, le persone che sono risorse critiche affinché l'azienda possa continuare ad offrire prodotti e servizi senza soluzione di continuità
Applicazioni	**Le applicazioni che hanno requisiti di riservatezza gestiscono spesso informazioni societarie proprietarie (ricerca e sviluppo), informazioni sulla clientela, dati sensibili sulla clientela, di natura sanitaria o personale**	**Le applicazioni che hanno requisiti di integrità gestiscono tipicamente transazioni di natura finanziaria, acquisto di beni o commercio elettronico**	**I requisiti di disponibilità si incontrano nelle applicazioni sensibili all'attività quotidiana, dove un guasto comporta solitamente costi e spese generali in termini di assegnazione delle risorse**

Tabella 13. Selezione dei requisiti di sicurezza: esempio A

Come risultato finale, il gruppo di analisi dispone di una tabella in cui sono elencati gli asset critici, insieme con la logica di selezione, gli elementi di base ed i requisiti di sicurezza rispetto ai servizi forniti. La tabella sottostante corrisponde al risultato della fase 1 per l'esempio A (cfr. Tabella 14).

Asset critico	Categoria di asset	Componenti	Requisiti di sicurezza	Logica di selezione
Applicazione per il commercio elettronico	Applicazione	Banca dati Firewall Segmento di rete Server	**Riservatezza** **Integrità** **Disponibilità**	L'applicazione è essenziale per l'azienda, in quanto essa rappresenta l'elemento più importante dell'offerta di servizi

Tabella 14. Logica dei requisiti di sicurezza

Esempio B (profilo di rischio: medio, asset critico: sistema, fase 2)

[Passaggio 1] Nell'esempio B, l'asset più critico è individuato nelle postazioni di lavoro utilizzate per lo svolgimento delle attività quotidiane, fra cui corrispondenza con i clienti, informazioni sui clienti in merito ai procedimenti ed informazioni contabili di base riguardanti le fatture ed i crediti.

[Passaggio 2] Nel passaggio successivo, i componenti del gruppo documentano gli elementi che compongono l'asset selezionato e la logica di selezione. Essi identificano quattro postazioni di lavoro, la rete interna ed il server.

[Passaggio 3] Successivamente, si identificano i requisiti di sicurezza. Utilizzando la tabella seguente il gruppo individua i riquadri che si prestano ai propri requisiti. Nell'esempio B, il gruppo seleziona il requisito della disponibilità rispetto alle postazioni di lavoro, nel senso che esse sono utilizzate per le attività quotidiane e pertanto devono rimanere operative.

Asset critici	Riservatezza	Integrità	Disponibilità
Sistemi	Un sistema che ha requisiti di riservatezza gestisce spesso informazioni societarie proprietarie (ricerca e sviluppo), informazioni sulla clientela, dati sensibili sulla clientela, di natura sanitaria o personale	I sistemi che hanno requisiti di integrità gestiscono tipicamente transazioni di natura finanziaria, acquisto di beni o commercio elettronico	**I requisiti di disponibilità si incontrano nei sistemi sensibili all'attività quotidiana, dove un guasto comporta solitamente costi e spese generali in termini di assegnazione delle risorse**
Rete	Una rete con requisiti di riservatezza copre tipicamente lo scambio di comunicazioni e informazioni attraverso ambienti poco sicuri e poco affidabili	I requisiti di integrità della rete sono necessari tipicamente quando le transazioni avvengono attraverso reti pubbliche o reti metropolitane condivise o provider di telecomunicazioni	I requisiti di disponibilità sono necessari, in particolare quando la rete viene utilizzata per l'assistenza alla clientela o l'offerta di servizi o prodotti
Persone	I requisiti di riservatezza si incontrano tipicamente quando le persone gestiscono informazioni proprietarie e riservate relative all'organizzazione che, se divulgate, potrebbero danneggiare il buon nome dell'organizzazione e la clientela	I requisiti di 'integrità si incontrano quando le persone interessate condividono alcuni elementi segreti, quali chiavi crittografiche o password. Il possesso di conoscenze di questo tipo introduce un rischio legato al fattore umano che va affrontato con controlli ispettivi	I requisiti di disponibilità riguardano le persone particolarmente importanti, le persone che sono risorse critiche affinché l'azienda possa continuare ad offrire prodotti e servizi senza soluzione di continuità
Applicazioni	Le applicazioni che hanno requisiti di riservatezza gestiscono spesso informazioni societarie proprietarie (ricerca e sviluppo), informazioni sulla clientela, dati sensibili sulla clientela, di natura sanitaria o personale	Le applicazioni che hanno requisiti di integrità gestiscono tipicamente transazioni di natura finanziaria, acquisto di beni o commercio elettronico	I requisiti di disponibilità si incontrano nelle applicazioni sensibili all'attività quotidiana, dove un guasto comporta solitamente costi e spese generali in termini di assegnazione delle risorse

Tabella 15. Selezione dei requisiti di sicurezza: esempio B

Come risultato finale, il gruppo di analisi dispone di una tabella in cui sono elencati gli asset critici, insieme con la logica di selezione, gli elementi di base ed i requisiti di sicurezza rispetto ai servizi forniti. La tabella sottostante corrisponde al risultato del passaggio 3 per l'esempio B (cfrTabella 16).

Asset critico	Categoria di asset	Componenti	Requisiti di sicurezza	Logica di selezione
Postazioni di lavoro	**Sistema**	**4 postazioni di lavoro** **Segmento di rete** **Server**	**Disponibilità**	**Le postazioni di lavoro sono importanti per lo svolgimento delle attività quotidiane, fra cui corrispondenza con i clienti, informazioni sui clienti in merito ai procedimenti ed informazioni contabili di base riguardanti le fatture ed i crediti**

Tabella 16. Logica dei requisiti di sicurezza

Fase 3: selezione delle schede di controllo

Nel corso della fase 3 i componenti del gruppo di analisi sono in grado di "estrarre" le schede di controllo correlate alle aree di rischio precedentemente identificate (nella fase 1) e all'elenco degli asset critici individuati (nella fase 2). Come illustrato nella figura 5, la fase comprende tre passaggi.

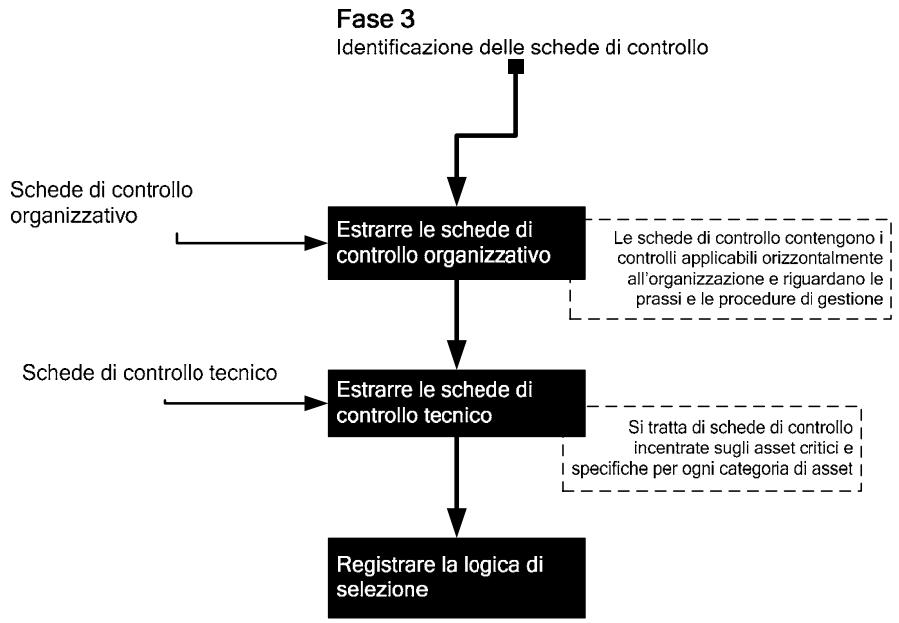

Figura 5. Fase 3: flusso di lavoro per la selezione delle schede di controllo

Le schede di controllo contengono i controlli tratti dal catalogo delle prassi utilizzate nell'ambito della metodologia OCTAVE. Tale catalogo comprende una raccolta di buone prassi di sicurezza strategiche ed operative. Un'organizzazione che stia effettuando una valutazione del proprio rischio di sicurezza delle informazioni fa un confronto tra se stessa e il suddetto catalogo. Il catalogo è utilizzato come parametro di riferimento rispetto a quanto l'organizzazione sta facendo correttamente rispetto alla sicurezza (le sue prassi attuali in materia di sicurezza) e quello che non sta facendo correttamente (le sue vulnerabilità organizzative).

Il catalogo è deliberatamente suddiviso in **due tipologie di controlli, i controlli di tipo organizzativo ed i controlli tecnici**:

- **i controlli organizzativi** sono incentrati sulle questioni organizzative (a livello di politiche aziendali) e forniscono buone prassi generali di gestione. I controlli organizzativi comprendono questioni che sono correlate all'attività dell'azienda, nonché alle tematiche che richiedono una pianificazione ed una partecipazione di tipo globale;
- le prassi relative ai **controlli tecnici** riguardano gli aspetti di carattere tecnologico: come le persone utilizzano le tecnologie, come interagiscono con esse e come le proteggono.

Il catalogo è di tipo generale, non è dedicato specificatamente a nessun settore, a nessuna organizzazione e a nessun insieme di norme. Può essere modificato per adattarlo agli standard di un particolare settore o ad un determinato insieme di norme, ad esempio, la comunità medica e le norme di sicurezza in materia di scambio elettronico di dati sanitari (HIPPA – *Health Insurance Portability and Accountability Act*). Può anche comprendere gli standard di una specifica organizzazione, oppure può essere modificato in modo da riflettere la terminologia di un determinato settore. **Inoltre, può essere sostituito con qualsiasi elenco compatibile di controlli standard.**

I controlli, a loro volta, sono raggruppati in schede di controllo suddivise in due categorie/aree di controllo: le aree di controllo organizzativo e le aree di controllo tecnico. Il gruppo che effettua l'analisi di una PMI ha a propria disposizione due tipologie di schede di controllo:

- **le schede di controllo organizzativo,** che contengono i controlli applicabili orizzontalmente all'organizzazione e riguardano le prassi e le procedure di gestione. Le schede di controllo della sicurezza dell'organizzazione sono tipicamente ampie ed intendono ridurre i tipici rischi informativi correlati al profilo di rischio dell'organizzazione;
- **le schede di controllo tecnico,** che sono incentrate sugli asset critici e che sono specifiche per ogni categoria di asset. Le schede di controllo tecnico consistono essenzialmente in gruppi di controlli predefiniti in rapporto al profilo di rischio ed ai requisiti di sicurezza di un determinato asset. Come indicato in precedenza, in un'organizzazione i principali gruppi di asset sono i seguenti: informazioni, sistema/rete, persone ed applicazioni. Le schede di controllo tecnico sono impostate in maniera tale da concentrarsi sulle attività quotidiane e riguardano rischi specifici.

Una descrizione dettagliata dei controlli organizzativi figura all'Allegato C. Controlli organizzativi.

Passaggio 1. Selezionare le schede di controllo organizzativo

In questo passaggio, il gruppo di analisi seleziona le schede di controllo dell'organizzazione rispetto alle aree di rischio identificate nella fase 1 (selezione del profilo di rischio) e definisce così l'orientamento dell'organizzazione rispetto alla sicurezza delle informazioni. Tuttavia, considerazioni pratiche possono impedire ad una PMI di adottare tutte le iniziative immediatamente dopo la valutazione. Le organizzazioni hanno probabilmente a disposizione risorse limitate, finanziarie ed umane, per poter mettere in pratica la strategia di protezione. Una volta effettuata la valutazione, il gruppo di analisi stabilisce un ordine di priorità tra le attività della strategia di protezione e poi si concentra sulla realizzazione delle attività la cui priorità è massima.

Queste schede di controllo sono disponibili per ciascun profilo di rischio, come risulta dalla matrice del profilo di rischio.

Passaggio 2. Selezionare le schede di controllo tecnico

Sulla base del profilo di rischio e delle esigenze di sicurezza degli asset, il gruppo di analisi può utilizzare la tabella relativa alle schede di controllo tecnico (cfr. Allegato B. Schede di controllo tecnico) per individuare i controlli più appropriati. Queste schede di controllo consistono in controlli essenziali raggruppati in tre categorie, a seconda del profilo di rischio dell'organizzazione, della categoria degli asset e dei requisiti di sicurezza. Ad esempio, se il profilo di rischio dell'organizzazione è alto, il gruppo di analisi riscontrerà requisiti diversi, in termini di rischi e sicurezza, rispetto ad un profilo medio o basso. Parimenti, le schede di controllo comprendono più controlli per affrontare una gamma più vasta di rischi e di requisiti di sicurezza.

Passaggio 3. Elenco documentato dei controlli selezionati e delle relative logiche

Quando si estraggono le schede di controllo degli asset critici nel corso del passaggio 2 occorre affrontare un gran numero di questioni relative ai controlli. Occorre documentare la logica seguita per selezionare le schede di controllo e le azioni necessarie per la loro attuazione. Inoltre, se si comprendono le schede di controllo, si è maggiormente in grado di definire i piani d'azione nel corso della fase successiva. Per ogni scheda di controllo, occorre prendere in esame e registrare la risposta a questa domanda: cosa è richiesto, in termini di risorse e modifiche, per implementare i controlli selezionati? Occorre esaminare gli aspetti operativi di ciascun controllo e, per ciascuno, prendere in esame le seguenti domande:

- Chi dovrebbe effettuarli?
- Chi dovrebbe esserne responsabile?

- Chi dovrebbe trarne beneficio?
- Come dovrebbero essere realizzati?

Le domande precedenti sono incentrate sulle modalità di effettuazione dei controlli e sulla motivazione della loro importanza. Se non si è in grado di rispondere a tutte le domande, bisogna rivolgersi ad altre persone, all'interno dell'organizzazione, che siano in grado di darle. Le informazioni reperite rispondendo a queste domande saranno utili nella fase 4, quando verranno elaborati i piani di riduzione del rischio. Occorre accertarsi di aver registrato queste informazioni.

Esempio A (profilo di rischio: alto; asset critico: applicazione)

[Passaggio 1] Il gruppo di analisi che utilizza la **tabella di valutazione del profilo di rischio e la tabella di selezione dei controlli organizzativi (Tabella 17)** seleziona le schede di controllo organizzativo per le aree di rischio identificate nel corso della fase 1 (profilo di rischio), definendo così l'orientamento dell'organizzazione rispetto alla sicurezza delle informazioni.

Nell'esempio A, i controlli organizzativi per un livello di rischio alto nell'area "legale e regolamentare" introducono prassi di sicurezza (controlli) dettate dai controlli organizzativi **SP1 e SP4**. Analogamente, una classe di rischio elevata nell'area "produttività" impone l'esigenza delle contromisure e delle prassi previste dai controlli **SP3, SP4, SP5** e **SP6**. Se nell'area "stabilità finanziaria" il livello di rischio è medio, il controllo è SP4, mentre se nell'area "reputazione e fiducia della clientela" il livello di rischio è basso si applicano i controlli SP4.1 (sezione inclusa nei controlli SP4).

Area di rischio	Alto	Medio	Basso
Legale e regolamentare	**(SP1)** **(SP4)**	(SP1) (SP4)	SP1.1
Produttività	**(SP3)** **(SP4)** **(SP6)** **(SP5)**	(SP4) (SP6)	SP4.1
Stabilità finanziaria	(SP2) (SP1) (SP4)	**(SP4)**	SP4.1
Reputazione e fiducia della clientela	(SP1) (SP5)	(SP4) (SP1)	**SP4.1**

Tabella 17. Selezione dei controlli organizzativi: esempio A

[Passaggio 2] Il gruppo di analisi seleziona le schede di controllo tecnico utilizzando l'apposita tabella. Nell'esempio A, in considerazione del profilo di rischio alto dell'organizzazione (identificato nella fase 1) e della tipologia degli asset critici individuati nel passaggio 2, il gruppo seleziona la scheda 1 per le applicazioni a profilo di rischio alto, vale a dire la scheda CC-1A.

Tabella delle schede di controllo			
Asset critici	**Schede per rischio alto**	**Schede per rischio medio**	**Schede per rischio basso**
Applicazione	**CC-1A**	CC-2A	CC-3A
Sistema	CC-1S	CC-2S	CC-3S
Rete	CC-1N	CC-2N	CC-3N
Persone	CC-1P	CC-2P	CC-3P

Tabella 18. Selezione delle schede di controllo tecnico: esempio A

La scheda selezionata nell'esempio A (cfr. Allegato B. Schede di controllo tecnico) indica i controlli che devono essere effettuati se l'applicazione riguarda un'organizzazione a profilo di rischio alto. Il gruppo identifica i controlli e si occupa dei requisiti di sicurezza individuati nella fase 3. In questo esempio, si tiene conto dei requisiti relativi alla riservatezza ed alla disponibilità. Vengono selezionati i seguenti controlli degli asset: **2.1.3, 2.1.6, 2.4.2, 2.5.1** e **2.6.1**.

Scheda di controllo tecnico		**CC-1A**								
Profilo di rischio		**Alto**								
Categoria di asset		**Applicazione**								
Requisiti di sicurezza	**Sicurezza fisica**	**Gestione dei sistemi e della rete**	**Strumenti di amministrazione del sistema**	**Monitoraggio e verifica sicurezza IT**	**Autenticazione ed autorizzazione**	**Gestione delle vulnerabilità**	**Crittografia**	**Architettura e concezione della sicurezza**	**Gestione degli incidenti**	**Prassi generali del personale**
Riservatezza		**2.1.3**			**2.4.2**	**2.5.1**	**2.6.1**			
Integrità		**2.1.4**			**2.4.2**	**2.5.1**	**2.6.1**			
Disponibilità		**2.1.6**								

Tabella 19. Scheda di controllo tecnico: esempio A (CC-1A)

[Passaggio 3] Il gruppo di analisi si occupa della raccolta dei dati e dell'analisi dei risultati prodotti nei passaggi 1 e 2. I controlli tecnici ed i controlli organizzativi sono ricapitolati nella tabella sottostante.

Asset	Controllo	Logica di selezione
Controlli tecnici	**2.1.3**	I controlli relativi al sistema ed alla gestione della rete sono essenziali per mantenere la disponibilità e la riservatezza dell'asset in questione
	2.1.6	
	2.1.4	L'integrità dell'applicazione è importante, perchè le informazioni mediche devono essere accurate
	2.4.2	L'autenticazione e l'autorizzazione per gli utenti interni ed esterni o per i terzi possono garantire un accesso controllato all'asset in questione
	2.5.1	La gestione delle vulnerabilità, fra cui la valutazione regolare delle vulnerabilità e le iniziative da effettuare per porvi rimedio sono essenziali per poter valutare le misure ed i sistemi di sicurezza

	2.6.1	Le informazioni riservate devono essere protette in fase di trasmissione e memorizzazione
Controlli organizzativi	**SP1**	Sensibilizzazione alla sicurezza e formazione
	SP3	Gestione della sicurezza
	SP4	Politica di sicurezza
	SP5	Gestione collaborativa
	SP6	Disaster recovery

Tabella 20. Logica di selezione dei controlli: esempio A

Esempio B (profilo di rischio: medio; asset critico: sistema)

[Passaggio 1] Il gruppo di analisi, utilizzando la **tabella dei controlli organizzativi** (Tabella 21) seleziona le schede di controllo organizzativo per le aree di rischio identificate nel corso della fase 1 (passaggio 1 **– Tabella di valutazione del profilo di rischio**), definendo così l'orientamento dell'organizzazione rispetto alla sicurezza delle informazioni.

Nel caso dell'**esempio B**, il controllo organizzativo per un livello di rischio basso nell'area "legale e regolamentare" è SP1.1, mentre per un livello di rischio basso nelle aree "produttività" e "stabilità finanziaria" è SP4.1. Un livello di rischio medio nell'area "reputazione e fiducia della clientela" prevede il ricorso ai controlli organizzativi SP1 e SP4.

La Tabella 21 ricapitola i controlli per l'esempio B precedentemente illustrato.

Area di rischio	**Alto**	**Medio**	**Basso**
Legale e regolamentare	(SP1)	(SP1)	**SP1.1**
	(SP4)	(SP4)	
Produttività	(SP3)	(SP4)	**SP4.1**
	(SP4)		
	(SP6)	(SP6)	
	(SP5)		
Stabilità finanziaria	(SP2)	(SP4)	**SP4.1**
	(SP1)		
	(SP4)		
Reputazione e fiducia della clientela	(SP1)	**(SP4)**	SP4.1
	(SP5)	**(SP1)**	

Tabella 21. Selezione dei controlli organizzativi: esempio B

[Passaggio 2] Il gruppo di analisi seleziona le schede di controllo basate sugli asset utilizzando l'apposita tabella. Nel caso dell'esempio B in considerazione del profilo di rischio medio dell'organizzazione, identificato nella fase 1 (passaggio 1) e della tipologia degli asset critici identificata nel passaggio 2, il gruppo seleziona la scheda 2 per i sistemi a profilo di rischio medio, vale a dire la scheda CC-2S.

Tabella delle schede di controllo			
Asset critici	**Schede per rischio alto**	**Schede per rischio medio**	**Schede per rischio basso**
Applicazione	CC-1A	CC-2A	CC-3A
Sistema	CC-1S	**CC-2S**	CC-3S
Rete	CC-1N	CC-2N	CC-3N
Persone	CC-1P	CC-2P	CC-3P

Tabella 22. Selezione delle schede di controllo tecnico: esempio B

La scheda selezionata nell'esempio B (cfr. Allegato B. Schede di controllo tecnico) indica i controlli necessari per il sistema di un'organizzazione avente un profilo di rischio medio. Il gruppo individua i controlli che si riferiscono ai requisiti di sicurezza individuati nella fase 3. Nell'esempio B, sulla base del risultato della fase 2 (passaggio 3) si utilizzano i requisiti della disponibilità per identificare i controlli più appropriati mediante la **scheda di controllo CC-2S**. Vengono pertanto selezionati i controlli **2.1.7, 2.1.6**.

Scheda di controllo tecnico		**CC-2S**								
Profilo di rischio		**Medio**								
Categoria di asset		**Sistema**								
Requisiti di sicurezza	**Sicurezza fisica**	**Gestione dei sistemi e della rete**	**Strumenti di amministrazione del sistema**	**Monitoraggio e verifica sicurezza IT**	**Autenticazione ed autorizzazione**	**Gestione delle vulnerabilità**	**Crittografia**	**Architettura e concezione della sicurezza**	**Gestione degli incidenti**	**Prassi generali del personale**
Riservatezza		**2.1.6** **2.1.7**			**2.4.1**					
Integrità		**2.1.9**			**2.4.1**					
Disponibilità		**2.1.6** **2.1.7**								

Tabella 23. Scheda di controllo tecnico: esempio B (CC-2S)

[Passaggio 3] Il gruppo di analisi si occupa della raccolta dei dati e dell'analisi dei risultati prodotti nei passaggi 1 e 2. I controlli tecnici ed i controlli organizzativi sono ricapitolati nella tabella sottostante.

Asset	**Controllo**	**Logica di selezione**
Controlli tecnici	**2.1.6** **2.1.7**	I controlli relativi al sistema ed alla gestione della rete sono essenziali per mantenere la disponibilità e la riservatezza dell'asset in questione
Controlli organizzativi	**SP1**	Sensibilizzazione alla sicurezza e formazione
	SP4	Politica di sicurezza
	SP1.1	Compreso in SP1
	SP4.1	Compreso in SP4

Tabella 24. Logica di selezione dei controlli: esempio B

Fase 4: implementazione e gestione

Nel corso della fase 4, il gruppo di analisi identifica le azioni e raccomanda un elenco di azioni, indicando la strada per migliorare la sicurezza. Affinché l'implementazione dia esito positivo, è essenziale che l'alta direzione (i responsabili decisionali) sia determinata nel sostenere il miglioramento della sicurezza.

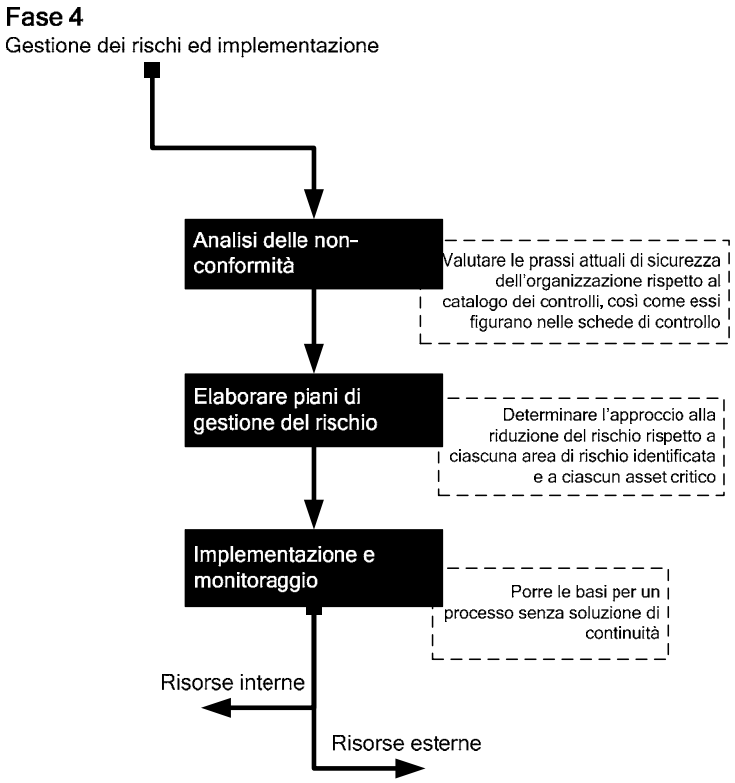

Figura 6. Fase 4: flusso di lavoro per l'implementazione e la gestione

Passaggio 1. Analisi delle non-conformità

L'analisi delle non-conformità è essenziale per migliorare le modalità di gestione della sicurezza delle informazioni da parte dell'organizzazione e per individuare la situazione attuale della sicurezza, vale a dire quanto viene fatto bene e quali siano i miglioramenti necessari.

In questo passaggio, il gruppo di analisi si occupa della valutazione delle prassi attuali dell'organizzazione in materia di sicurezza, confrontandole con quanto risulta dalle schede di controllo. Il gruppo di analisi deve leggere le schede di controllo attentamente selezionate e ricavare informazioni dettagliate sulle politiche, le procedure e le prassi correnti dell'organizzazione, fornendo così un punto di partenza per il miglioramento.

Durante questo processo, il gruppo di analisi utilizza le schede di controllo come se fossero i "requisiti" e valuta lo scostamento tra questi ultimi e le prassi correnti di sicurezza, sia a livello di organizzazione, sia a livello di asset critici. Il gruppo di analisi dovrebbe documentare attentamente i risultati su due piani distinti: **1) rispetto ai miglioramenti organizzativi** e **2) rispetto alla protezione dei singoli asset**.

L'esito di questo processo può fungere da base per l'attività di pianificazione immediatamente successiva, la quale può essere suddivisa in due categorie: **a) i controlli organizzativi**, nel qual

caso il gruppo di analisi dovrebbe identificare ciò che si fa e ciò che non si fa, definendo le azioni per i miglioramenti a livello organizzativo; **b) i controlli tecnici,** nel qual caso il gruppo di analisi valuta le misure di protezione esistenti rispetto agli asset critici identificati.

Passaggio 2. Elaborare piani di riduzione del rischio

Il gruppo di analisi ha già identificato gli asset critici, il profilo di rischio dell'organizzazione ed i requisiti di sicurezza. Inoltre ha selezionato altri controlli appropriati ed è pronto a stabilire l'approccio alla riduzione del rischio per ogni area di rischio identificata e per ogni asset critico.

Nel compiere questi primi passi verso un miglioramento, l'organizzazione può cominciare a costruire quanto è necessario per realizzare la propria strategia di protezione.

L'esito di questa attività è il piano di riduzione del rischio, il quale **comporta una serie di passaggi** che l'organizzazione può fare per innalzare o conservare il livello esistente di sicurezza. L'obiettivo consiste nel fornire un orientamento pro futuro rispetto alla sicurezza delle informazioni, piuttosto che una soluzione immediata ad ogni elemento di vulnerabilità o preoccupazione in termini di sicurezza. Poiché un piano di riduzione del rischio fornisce all'organizzazione un orientamento rispetto alle attività volte a mettere in sicurezza le informazioni, suggeriamo di strutturarlo attorno alle schede di controllo selezionate (fase 3 – schede di controllo organizzativo e schede di controllo tecnico).

Passaggio 3. Implementazione, monitoraggio e controllo

Uno dei principi del metodo di valutazione del rischio consiste nel gettare le fondamenta per un processo senza soluzione di continuità. Questo principio si rivolge alla necessità di mettere in pratica i risultati derivanti dalla valutazione del rischio, fornendo così la base per migliorare la sicurezza delle informazioni. **Se l'organizzazione non riesce a mettere in pratica i risultati della valutazione, essa non riuscirà neanche a migliorare la propria posizione in materia di sicurezza**.

In qualsiasi attività tendente al miglioramento, uno dei compiti più difficili consiste nel mantenere i risultati derivanti dalla valutazione. Tuttavia, considerazioni pratiche possono impedire alla maggior parte delle organizzazioni di realizzare immediatamente le iniziative risultanti dalla valutazione. È probabile che le PMI abbiano a disposizione risorse limitate, finanziarie ed umane, per mettere in pratica la strategia di protezione.

Il gruppo di analisi attribuisce alle attività un ordine di priorità e poi si concentra sull'attuazione delle attività la cui priorità è massima.

Sono possibili tre distinte opzioni:

- **accettazione del rischio**: in questo caso, non si interviene per ridurre il rischio e le conseguenze di una sua eventuale manifestazione sono anch'esse accettate;
- **riduzione del rischio**: in questo caso**,** le azioni volte a contrastare la minaccia e a ridurre il rischio sono identificate ed applicate.

Dopo aver identificato gli interventi specifici da realizzare, il gruppo di analisi deve non solo assegnare le responsabilità, ma anche definire la data per il completamento degli interventi. Occorre registrare, per ciascuna iniziativa, le risposte alle seguenti domande:

- Chi sarà **responsabile** di ogni iniziativa?
- Che cosa può fare la direzione per **agevolare** il completamento dell'iniziativa?
- Quanto **costerà**?
- **Quanto tempo** occorrerà?
- **Possiamo farcela da soli?**
- **Abbiamo bisogno di assistenza esterna?**

NOTA

Le ultime due domande sono di importanza critica rispetto al fatto **che un'organizzazione possa realizzare i necessari controlli con risorse interne**. Entrambe le risposte sono egualmente importanti e molto difficili da dare, in quanto sia l'una sia l'altra soluzione (esternalizzazione o risorse interne) presentano vantaggi e svantaggi.

L'esternalizzazione corrisponde alla **decisione di "fare o comprare" rispetto alla risorsa in questione**. Se la decisione è ben motivata, l'esternalizzazione può offrire senz'altro dei vantaggi. I principali obiettivi dell'esternalizzazione, oltre alle funzioni di supporto, sono il taglio dei costi, il dimensionamento e la volontà di concentrarsi sull'attività caratteristica (competenza caratteristica). La mancanza di competenze nel campo delle IT all'interno dell'organizzazione può anche essere una delle motivazioni per l'esternalizzazione. Data la crescente importanza delle IT, spesso le società riscontrano un'ampia disparità tra le capacità e le competenze tecniche necessarie per sfruttare il potenziale tecnologico e la realtà delle proprie conoscenze tecnologiche interne.

Vi sono comunque parecchie opzioni che dovrebbero essere prese in considerazione e che uniscono le competenze caratteristiche dell'organizzazione con il supporto esterno o di soggetti terzi (esternalizzazione parziale o totale). Come si può rilevare dalla figura 7, sia la gestione sia l'implementazione possono essere esternalizzate. **L'offerta di servizi tipicamente riscontrabile tra i fornitori è così riassumibile**:

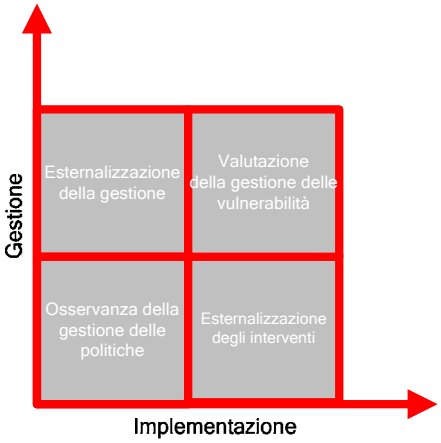

Figura 7. Opzioni relative all'esternalizzazione della gestione o dell'implementazione

- **Esternalizzazione della gestione**. In questo caso, i fornitori erogano servizi di gestione nel campo della sicurezza dell'informazione. In altre parole, **un addetto alla sicurezza è assegnato dal fornitore** a gestire il programma di sicurezza. Generalmente, gli oneri sono calcolati su base trimestrale, in rapporto sia alle dimensioni ed alla complessità dell'organizzazione, sia alle capacità ed alle conoscenze necessarie.
- **Osservanza della gestione delle politiche**. In questo caso, i consulenti esperti in sicurezza **eseguono periodicamente verifiche programmate** per garantire la continuità dell'osservanza delle politiche e dei controlli di sicurezza precedentemente stabiliti, nonché per individuare gli eventuali scostamenti. A seguito di questo processo periodico, l'azienda riceve una relazione dettagliata sulla situazione complessiva dei sistemi, sulle aree di mancata osservanza delle politiche e dei controlli di sicurezza ed un orientamento su come rientrare nella norma. Questo tipo di accordi comprende generalmente la segnalazione e l'analisi dell'andamento, che aiuta a stabilire se la propria situazione in materia di sicurezza stia o meno migliorando e per quale motivo.

- **Valutazione della gestione delle vulnerabilità**. Con queste formule contrattuali, **i fornitori forniscono un insieme unitario di servizi di valutazione delle vulnerabilità,** che possono essere tagliati su misura per affrontare tutti i possibili punti di ingresso delle informazioni per l'organizzazione: Internet, le reti interne, le applicazioni, l'accesso remoto e le soluzioni wireless. Sulla base degli elementi trainanti dell'azienda, degli asset tecnici e dei fattori di rischio, i fornitori possono aiutare i clienti a stabilire quale sia l'intervallo più adeguato per le valutazioni ricorrenti ed il grado ottimale di verifica, in profondità ed ampiezza.
- **Supporto per gli interventi di gestione**. Il supporto costante per gli **interventi interni di messa in sicurezza,** su base quotidiana, rappresenta una risorsa per il cliente. Generalmente i fornitori offrono livelli di supporto diversi e modulari, che vanno dalla semplice consulenza/assistenza per l'attuazione delle soluzioni e delle politiche di sicurezza all'ingegnerizzazione ed alla realizzazione tecnica delle infrastrutture per la sicurezza. Gli interventi costanti in materia di sicurezza comprendono tipicamente il potenziamento dei server, le modifiche alla configurazione di sicurezza, la creazione di patch per la sicurezza delle applicazioni.
- **Risposta in caso di emergenza o incidente**. I servizi di risposta in caso di emergenza o incidente garantiscono un'assistenza con ingegneri esperti in loco nelle situazioni di emergenza o di crisi. I servizi di gestione e risposta in caso di incidente consentono ai clienti di **rispondere rapidamente e positivamente agli incidenti di sicurezza correlati ai computer** fra cui compromissioni del sistema, attacchi di virus ed accesso negato ai servizi, aiutando a minimizzare il dispendio di tempo e denaro.

I requisiti di sicurezza delle organizzazioni che esternalizzano la gestione ed il controllo di tutti i propri sistemi informativi, o di una parte di essi, delle reti e/o dell'ambiente del desk top dovrebbero essere affrontati in un accordo a livello di servizi tra le parti. Come minimo, un accordo di questo tipo per l'esternalizzazione della gestione e degli interventi di messa in sicurezza delle informazioni dovrebbe comprendere i seguenti aspetti (controlli):

A. Livello di esternalizzazione e questioni inerenti la responsabilità
B. Monitoraggio degli adempimenti
C. Responsabilità di gestione
D. Campo di applicazione dell'attività
E. Modalità di osservanza degli obblighi di legge, ad esempio della legislazione sulla tutela dei dati
F. Soluzioni adottate per garantire che tutte le parti coinvolte nell'esternalizzazione, fra cui i subappaltatori, siano consapevoli delle proprie responsabilità in tema di sicurezza
G. Come l'integrità e la riservatezza degli asset aziendali saranno conservate e verificate
H. Quali controlli fisici ed informatici saranno effettuati per restringere e delimitare agli utenti autorizzati l'accesso ai dati sensibili dell'organizzazione
I. Come deve essere mantenuta la disponibilità dei servizi in caso di disastro
J. Diritto di ispezione
K. Competenza delle risorse e certificazione professionale
L. Rendicontazione (contenuto, frequenza e struttura).

Esempio A (profilo di rischio: alto; asset critico: applicazione)

[Passaggio 1] Il gruppo di analisi si occupa della valutazione delle prassi correnti di sicurezza dell'organizzazione rispetto ai controlli descritti nelle schede di controllo. Il gruppo di analisi legge attentamente i controlli che si applicano al profilo (come delineato dalle schede di controllo

selezionate – fase 3, passaggio 3) e chiede informazioni dettagliate sulle politiche, sulle procedure e sulle prassi correnti dell'organizzazione, fornendo così il punto di partenza per un miglioramento.

La tabella seguente si riferisce all'esempio A.

Asset	Controllo	Stiamo eseguendo i controlli che figurano nelle schede di controllo?
Controlli tecnici	**2.1.3**	No
	2.1.4	In parte
	2.1.6	No
	2.4.2	In parte
	2.5.1	No
	2.6.1	No
Controlli organizzativi	**SP1**	No
	SP3	No
	SP4	Si
	SP5	No
	SP6	In parte

Tabella 25. Elenco derivante dall'analisi delle non-conformità: esempio A

[Passaggio 2] Il gruppo di analisi legge i controlli (allegati A, B, C, D) e decide quali siano gli interventi necessari.

Asset	Controllo	Azione
Controlli tecnici	**2.1.3**	Il gruppo decide di proteggere i dati sensibili memorizzandoli in sicurezza, ad esempio con catene di custodia precise, l'archiviazione dei backup in luogo diverso dalla sede, dispositivi rimovibili per la raccolta dei dati, processi di disabilitazione ai dati sensibili o ai mezzi su cui sono memorizzati
	2.1.4	Il gruppo decide di proteggere i dati sensibili verificando periodicamente l'integrità del software di base installato per l'applicazione
	2.1.6	Il gruppo decide di sviluppare un piano documentato per il backup dei dati che sia aggiornato di routine, testato periodicamente, richieda backup periodici programmati del software e dei dati, test periodici e verifica della capacità di recuperare i dati salvati in backup
	2.4.2	Il gruppo decide di fissare politiche e procedure documentate relative all'uso delle informazioni rispetto all'accesso dei singoli e dei gruppi per: A) definire le regole per la concessione di un livello appropriato di accesso, B) stabilire il diritto iniziale di accesso, C) modificare il diritto di accesso, D) togliere il diritto di accesso, F) rivedere e verificare periodicamente i diritti di accesso

	2.5.1	Il gruppo decide di selezionare gli strumenti per la valutazione delle vulnerabilità, le checklist e gli script, mantenendosi al passo delle tipologie note di vulnerabilità e dei metodi di attacco, rivedendo le fonti di informazione su annunci di vulnerabilità, allarmi sicurezza ed avvisi analoghi, individuando le componenti infrastrutturali da valutare, programmando la valutazione delle vulnerabilità, fornendo un'interpretazione dei risultati ed una risposta ad essi, conservando/eliminando in sicurezza i dati vulnerabili
	2.6.1	Il gruppo decide di NON attuare la crittografia dei dati da trasmettere. Rispetto alla riservatezza, i dati immagazzinati sono protetti, da un sistema di controllo degli accessi
Controlli organizzativi	**SP1**	Il gruppo decide di lanciare una campagna di sensibilizzazione di base, insegnando a tutti gli avvocati i rischi derivanti dall'uso di e-mail, internet, ecc.
	SP3	Deve essere istituita la funzione di gestione della sicurezza, cui sarà assegnato un incaricato della sicurezza
	SP4	Il gruppo decide inoltre di elaborare una politica generale della sicurezza, definendo la titolarità delle informazioni e le relative responsabilità
	SP5	Occorre stabilire le procedure di gestione collaborativa che riguardano il terzo responsabile della manutenzione dell'applicazione
	SP6	Il piano di disaster recovery deve essere implementato e testato periodicamente

Tabella 26. Elenco delle azioni: esempio A

[Passaggio 3] Il gruppo di analisi stabilisce un ordine di priorità degli interventi e si concentra sulla realizzazione degli interventi la cui priorità è massima. Il gruppo decide di realizzare gli interventi ad alta priorità entro il trimestre successivo, gli interventi a media priorità nei successivi sei mesi e gli interventi a bassa priorità prima del termine dell'anno successivo.

Ora che sono state identificate le iniziative specifiche rispetto al piano d'azione, occorre stabilire le responsabilità ed una data per il loro completamento. Occorre rispondere alle domande seguenti per ciascuna iniziativa in elenco, registrando i risultati.

- Chi sarà responsabile di ogni iniziativa?
- Entro quale data l'iniziativa deve essere realizzata?
- Che cosa può fare la direzione per agevolare il completamento dell'iniziativa?
- Quanto costerà?
- Quanto tempo occorrerà?
- Possiamo farcela da soli?
- Abbiamo bisogno di assistenza esterna?

Il risultato del piano è riassunto nella tabella seguente:

Asset	Controllo	Responsabile	Assistenza esterna necessaria	Momenti di verifica	Priorità
Controlli tecnici	**2.1.3**	Dipendente A	No	gg/mm	Elevata
	2.1.4	Dipendente A	Si		Media
	2.1.6	Dipendente A	Si		Elevata
	2.4.2	Dipendente A	Si		Media
	2.5.1	Dipendente A	No		Bassa
	2.6.1	Dipendente A	No		Media

Controlli organizzativi	**SP1**	Dipendente B	No		Bassa
	SP3	Dipendente B	No		Media
	SP4	Dipendente B	Si		Media
	SP5,	Dipendente B	No		Elevata
	SP6	Dipendente B	No		Elevata

Tabella 27. Piano di implementazione: esempio A

Esempio B (profilo di rischio: medio; asset critico: sistema)

[Passaggio 1] Il gruppo di analisi si occupa della valutazione delle prassi correnti di sicurezza dell'organizzazione rispetto ai controlli descritti nelle schede di controllo. Il gruppo di analisi legge attentamente i controlli che si applicano al profilo (come delineato dalle schede di controllo selezionate – fase 3, passaggio 3) e chiede informazioni dettagliate sulle politiche, sulle procedure e sulle prassi correnti dell'organizzazione, ponendo così le basi per un miglioramento.

La tabella seguente si riferisce all'esempio B.

Asset	Controllo	Stiamo eseguendo i controlli che figurano nelle schede di controllo?
Controlli tecnici	**2.1.6**	No
	2.1.7	Si
Controlli organizzativi	**SP1**	In parte
	SP4	Si
	SP1.1	No
	SP4.1	Si

Tabella 28. Elenco derivante dall'analisi delle non-conformità: esempio B

[Passaggio 2] Il gruppo di analisi legge i controlli (allegati A, B, C, D) e decide quali siano gli interventi necessari.

Asset	Controllo	Azione
Controlli tecnici	**2.1.6**	Il gruppo decide di sviluppare un piano documentato per il backup dei dati che sia aggiornato di routine, testato periodicamente, richieda backup periodici programmati del software e dei dati, test periodici e verifica della capacità di recuperare i dati salvati in backup
	2.1.7	Il gruppo decide di informare ed istruire tutto il personale affinché sia consapevole e sia in grado di far fronte alle proprie responsabilità nel quadro dei piani di backup
Controlli organizzativi	**SP1**	Il gruppo decide di lanciare una campagna di sensibilizzazione di base, insegnando a tutti gli avvocati i rischi derivanti dall'uso di e-mail, internet, ecc.
	SP4	Il gruppo decide inoltre di elaborare una politica generale della sicurezza, definendo la titolarità delle informazioni e le relative responsabilità
	SP1.1	Compreso in SP1.
	SP4.1	Compreso in SP4.

Tabella 29. Elenco delle azioni: esempio B

[Passaggio 3] Il gruppo di analisi stabilisce un ordine di priorità degli interventi e si concentra sulla realizzazione degli interventi la cui priorità è massima. Il gruppo decide di realizzare gli interventi ad alta priorità entro il trimestre successivo, gli interventi a media priorità nei successivi sei mesi e gli interventi a bassa priorità prima del termine dell'anno successivo.

Ora che sono state identificate le iniziative specifiche rispetto al piano d'azione, occorre stabilire le responsabilità ed una data per il loro completamento. Occorre rispondere alle domande seguenti per ciascuna iniziativa in elenco, registrando i risultati.

- Chi sarà responsabile di ogni iniziativa?
- Entro quale data l'iniziativa deve essere realizzata?
- Che cosa può fare la direzione per agevolare il completamento dell'iniziativa?
- Quanto costerà?
- Quanto tempo occorrerà?
- Possiamo farcela da soli?
- Abbiamo bisogno di assistenza esterna?

Il risultato del piano è riassunto nella tabella seguente:

Asset	Controllo	Responsabile	Assistenza esterna necessaria	Momenti di verifica	Priorità
Controlli tecnici	**2.1.6**	Dipendente A	No	gg/mm	Elevata
	2.1.7	Dipendente A	No		Elevata
Controlli organizzativi	**SP1**	Dipendente A	No		Media
	SP4	Dipendente A	No		Bassa
	SP1.1	Dipendente A	No		Bassa
	SP4.1	Dipendente A	No		Elevata

Tabella 30. Piano di implementazione: esempio B

Allegato A. Schede di controllo organizzativo

Sensibilizzazione alla sicurezza e formazione (SP1)	
SP1	La scheda di controllo “Sensibilizzazione alla sicurezza e formazione” comprende i controlli che devono rendere il personale consapevole del proprio ruolo e delle proprie responsabilità in materia di sicurezza. A tutto il personale occorre fornire strumenti di sensibilizzazione alla sicurezza, di formazione e di richiamo periodico. Il livello di consapevolezza del personale in materia di sicurezza in rapporto ai rispettivi ruoli dovrebbe essere documentato con chiarezza. L’adeguamento al ruolo dovrebbe essere verificato periodicamente.
Strategia di sicurezza (SP2)	
SP2	La scheda di controllo “Strategia di sicurezza” comprende i controlli relativi all’inserimento di routine, nelle strategie dell’organizzazione, di elementi relativi alla sicurezza. Analogamente, le strategie e le politiche in materia di sicurezza devono tener conto delle strategie e degli obiettivi generali dell’organizzazione. Le strategie e gli obiettivi in materia di sicurezza devono essere documentati ed oggetto di revisione periodica, aggiornamento e comunicazione all’organizzazione.
Gestione della sicurezza (SP3)	
SP3	La scheda di controllo “Gestione della sicurezza” comprende i controlli relativi all’attuazione ed all’applicazione del processo di gestione della sicurezza. Il processo deve valutare senza soluzione di continuità i livelli richiesti di sicurezza delle informazioni, definendo controlli appropriati ed equilibrati in termini di costo/rischio, da applicare e documentare.
Politiche e norme di sicurezza (SP4)	
SP4	La scheda di controllo “Politiche e norme di sicurezza” prevede che l’organizzazione disponga di un insieme esauriente e documentato di politiche inerenti la sicurezza delle informazioni, da riesaminare ed aggiornare periodicamente.
Gestione collaborativa della sicurezza (SP5)	
SP5	La scheda di controllo “Gestione collaborativa della sicurezza” comprende i controlli di sicurezza che prevedono l’applicazione documentata e monitorata delle procedure volte a proteggere le informazioni dell’organizzazione quando si opera con organizzazioni esterne (ad esempio, soggetti terzi, collaboratori, subappaltatori o partner).
Piani alternativi/ piani di *disaster recovery* (SP6)	
SP6	La scheda di controllo “Piani alternativi/piani di disaster recovery” comprende i controlli di sicurezza volti a garantire la continuità dell’operatività aziendale in caso di disastro o di indisponibilità delle informazioni. Gli elementi chiave di questa scheda di controllo sono i seguenti: ▫ piani di continuità aziendale o di operatività in caso di emergenza, ▫ piani di disaster recovery, ▫ piani alternativi in risposta ad eventuali situazioni di emergenza (*contingency planning*).

Allegato B. Schede di controllo tecnico[3]

Scheda di controllo tecnico										CC-1A
Profilo di rischio										Alto
Categoria di asset										Applicazione
Requisiti di sicurezza	Sicurezza fisica	Gestione dei sistemi e della rete	Strumenti di amministrazione del sistema	Monitoraggio e verifica sicurezza IT	Autenticazione ed autorizzazione	Gestione delle vulnerabilità	Crittografia	Architettura e concezione della sicurezza	Gestione degli incidenti	Prassi generali del personale
Riservatezza		2.1.3			2.4.2	2.5.1	2.6.1			
Integrità		2.1.4			2.4.2	2.5.1	2.6.1			
Disponibilità		2.1.6								

I controlli relativi alla riservatezza di un'applicazione, nel caso in cui il profilo di rischio sia alto, riguardano tipicamente i requisiti di sicurezza a livello di quell'applicazione, allo scopo di salvaguardare il ciclo di vita delle informazioni critiche. I controlli sono selezionati principalmente nell'ottica di contrastare il fenomeno della divulgazione di informazioni a soggetti non autorizzati, esterni o interni all'ambiente.

I controlli essenziali per la protezione della riservatezza degli asset critici sono i seguenti:

OP2.4.2 Occorre predisporre politiche e procedure documentate relative all'uso delle informazioni rispetto all'accesso di individui o di gruppi per: A) definire le regole per la concessione di un livello appropriato di accesso, B) stabilire il diritto iniziale di accesso, C) modificare il diritto di accesso, D) togliere il diritto di accesso, F) rivedere e verificare periodicamente i diritti di accesso;

OP2.5.1 Occorre prevedere un insieme documentato di procedure per la gestione delle vulnerabilità, fra cui la selezione di strumenti per la loro valutazione, checklist e script, mantenendosi aggiornati rispetto alle tipologie note di vulnerabilità e ai metodi di attacco, rivedendo le fonti di informazione su annunci di vulnerabilità, allarmi sicurezza ed avvisi analoghi, individuando le componenti infrastrutturali da valutare, programmando la valutazione delle vulnerabilità, interpretando i risultati e fornendo una risposta ad essi, mettendo in sicurezza i dati vulnerabili memorizzati o eliminati;

OP2.1.3 I dati sensibili devono essere archiviati in sicurezza, ad esempio con precise catene di custodia, archiviazione dei backup in luogo diverso dalla sede, dispositivi rimovibili per la raccolta dei dati, processi di disabilitazione ai dati sensibili o ai mezzi su cui essi sono memorizzati;

OP2.1.4 L'integrità del software installato deve essere verificata periodicamente;

OP2.1.6 Occorre predisporre un piano documentato per il backup dei dati che sia aggiornato di routine e verificato periodicamente, prevedendo backup periodici programmati del software e dei dati, test periodici e verifica della capacità di recuperare i dati salvati in backup;

OP2.6.1 Occorre effettuare controlli appropriati di sicurezza per proteggere i dati sensibili memorizzati e nel corso della trasmissione dei dati, fra cui crittografia in fase di trasmissione dei dati o di scrittura su disco, uso di un'infrastruttura a chiave pubblica, di tecnologia VPN (*virtual private network*) e della crittografia per tutti i dati trasmessi tramite Internet.

[3] In questo allegato, l'attribuzione dei controlli alle singole schede di controllo tecnico è stata effettuata in modo tale da garantire un buon livello di protezione. Se gli asset presentano requisiti di sicurezza molto elevati, si possono prendere in considerazione controlli ulteriori. Ciononostante, utilizzando queste schede di controllo tecnico si può conseguire un buon livello medio di protezione, che sembra adattarsi alla maggioranza delle PMI. A medio termine, l'ENISA ha in progetto di convalidare le ipotesi avanzate in questo documento mediante progetti pilota.

Scheda di controllo tecnico					CC-1S					
Profilo di rischio					Alto					
Categoria di asset					Sistema					
Requisiti di sicurezza	Sicurezza fisica	Gestione dei sistemi e della rete	Strumenti di amministrazione del sistema	Monitoraggio e verifica sicurezza IT	Autenticazione ed autorizzazione	Gestione delle vulnerabilità	Crittografia	Architettura e concezione della sicurezza	Gestione degli incidenti	Prassi generali del personale
Riservatezza		2.1.3 2.1.4 2.1.5 2.1.9			2.4.1 2.4.6		2.6.1			
Integrità		2.1.4 2.1.5 2.1.8 2.1.9 2.1.10			2.4.1 2.4.3 2.4.6			2.7.1 2.7.2		
Disponibilità		2.1.6 2.1.7 2.1.9			2.4.6					

Un profilo di rischio alto implica la minaccia di un'indisponibilità del sistema tale da portare ad un'indisponibilità del servizio. I sistemi possono non essere in grado di ospitare determinate applicazioni oppure possono determinare la perdita di informazioni critiche. Le fonti della minaccia possono essere l'instabilità del sistema a causa di malfunzionamenti meccanici oppure di un'istallazione o di un uso inadeguati.

I controlli sul sistema relativi alla riservatezza, quando il profilo di rischio dell'organizzazione è alto, comprendono metodi che garantiscono un'adeguata configurazione e funzionalità del sistema. I controlli sul sistema relativi all'integrità, quando il profilo di rischio dell'organizzazione è alto, riguardano tipicamente i requisiti di sicurezza del sistema, per garantire la stabilità del sistema e l'integrità delle informazioni critiche. La costante disponibilità del sistema è un requisito indispensabile per la continuità dell'azienda. I controlli sono selezionati principalmente nell'ottica di contrastare il fenomeno della divulgazione di informazioni a soggetti non autorizzati, esterni o interni all'ambiente.

I controlli essenziali per la protezione dell'integrità degli asset critici sono i seguenti:

OP2.1.3 I dati sensibili devono essere archiviati in sicurezza, ad esempio con precise catene di custodia, archiviazione dei backup in luogo diverso dalla sede, dispositivi rimovibili per la raccolta dei dati, processi di disabilitazione ai dati sensibili o ai mezzi su cui essi sono memorizzati;
OP2.1.4 L'integrità del software installato deve essere verificata periodicamente;
OP2.1.5 Tutti i sistemi devono essere aggiornati rispetto a revisioni, patch e raccomandazioni (nei consigli per la sicurezza);

OP2.1.6 Occorre predisporre un piano documentato per il backup dei dati che sia aggiornato di routine e verificato periodicamente, prevedendo backup periodici programmati del software e dei dati, test periodici e verifica della capacità di recuperare i dati salvati in backup;
OP2.1.7 Tutto il personale deve essere consapevole ed essere in grado di farsi carico delle proprie responsabilità derivanti dai piani di backup;

OP2.1.8 Le modifiche all'hardware ed al software IT devono essere pianificate, controllate e documentate;

OP2.1.9 Il personale IT deve seguire determinate procedure quando rilascia, modifica e interrompe le password, gli account ed i privilegi degli utenti. Per tutti gli utenti del sistema, compresi i soggetti terzi, si richiede un'unica identificazione dell'utente. Gli account e le password di default vanno eliminati dal sistema;

OP2.1.10 Sul sistema devono essere disponibili soltanto i servizi necessari: tutti i servizi non necessari vanno eliminati;

OP2.2.1 L'applicabilità di nuovi strumenti, nuove procedure e nuovi meccanismi di sicurezza deve essere oggetto di revisione periodica rispetto alle strategie di sicurezza dell'organizzazione;

OP2.2.2 Occorre utilizzare strumenti e meccanismi per un'amministrazione in sicurezza del sistema e della rete, da riesaminare, aggiornare o sostituire periodicamente. Ecco alcuni esempi: controllo dell'integrità dei dati, strumenti per la crittografia, per la scansione delle vulnerabilità, per verificare la qualità delle password o per la scansione dei virus, strumenti di gestione dei processi, sistemi di individuazione delle intrusioni, amministrazione remota in sicurezza, strumenti per la manutenzione della rete, analizzatori del traffico, strumenti di risposta agli incidenti, strumenti di analisi forense dei dati;

OP2.3.1 L'organizzazione deve utilizzare di routine alcuni strumenti di monitoraggio e verifica del sistema e della rete. L'attività è monitorata dal personale IT, il funzionamento del sistema e della rete è registrato, i log sono rivisti periodicamente, l'attività insolita è gestita come previsto dalle politiche o dalle procedure in materia, gli strumenti sono oggetto di revisione ed aggiornamento periodico;

OP2.4.1 Occorre utilizzare controlli adeguati degli accessi e strumenti di autenticazione degli utenti (ad esempio, accesso ai file, configurazione della rete) in coerenza con politiche predefinite, allo scopo di delimitare l'accesso degli utenti alle informazioni, alle utility di sistema, al codice sorgente dei programmi, ai sistemi sensibili, ad applicazioni e servizi specifici, alla connessione in rete all'interno dell'organizzazione, alla connessione in rete dall'esterno dell'organizzazione;

OP2.4.3 I metodi/i meccanismi di controllo degli accessi devono delimitare l'accesso alle risorse in rapporto ai diritti di accesso previsti da politiche e procedure;

OP2.4.6 Occorre utilizzare meccanismi di autenticazione per proteggere la disponibilità, l'integrità e la riservatezza dei dati sensibili (ad esempio, firme digitali e dati biometrici);

OP2.6.1 Occorre effettuare controlli appropriati di sicurezza per proteggere i dati sensibili memorizzati e nel corso della trasmissione dei dati, fra cui crittografia in fase di trasmissione dei dati o di scrittura su disco, uso di un'infrastruttura a chiave pubblica, di tecnologia VPN (*virtual private network*) e della crittografia per tutti i dati trasmessi tramite Internet;

OP2.7.1 I sistemi nuovi e modificati devono tener conto, nell'architettura e nella concezione, delle strategie, delle politiche e delle procedure aziendali in materia di sicurezza, della cronologia dei compromessi in materia di sicurezza e del risultato delle valutazioni del rischio sicurezza;

OP2.7.2 L'organizzazione deve disporre di diagrammi aggiornati che mostrino l'architettura di sicurezza a livello di impresa e la topologia di rete.

Scheda di controllo tecnico					CC-1N					
Profilo di rischio					**Alto**					
Categoria di asset					**Rete**					
Requisiti di sicurezza	**Sicurezza fisica**	**Gestione dei sistemi e della rete**	**Strumenti di amministrazione del sistema**	**Monitoraggio e verifica sicurezza IT**	**Autenticazione ed autorizzazione**	**Gestione delle vulnerabilità**	**Crittografia**	**Architettura e concezione della sicurezza**	**Gestione degli incidenti**	**Prassi generali del personale**
Riservatezza					**2.4.6**	**2.5.3**	**2.6.1**			
Integrità	**1.1.4**	**2.1.1** **2.1.10**			**2.4.1** **2.4.3** **2.4.4** **2.4.6**	**2.5.3**		**2.7.2**		
Disponibilità	**1.1.4**				**2.4.6**					

Un profilo di rischio alto implica minacce in aree di vulnerabilità della rete che possono portare ad attacchi dall'esterno, oppure all'accesso non autorizzato a determinati punti della rete di interesse elevato o di rischio elevato.

La mancanza di sicurezza della rete comporta effetti immediati e diretti sul funzionamento delle applicazioni e sul flusso delle informazioni.

I controlli relativi alla riservatezza della rete, nel caso in cui il profilo di rischio dell'organizzazione sia alto, dovrebbero proteggere le informazioni critiche ed interne dalla perdita potenziale o da un uso improprio. Le informazioni salvate in rete, inoltre, devono essere disponibili e facilmente accessibili, ma anche tenute separate in rapporto al livello di criticità.

I controlli essenziali per la protezione della riservatezza, dell'integrità e della disponibilità all'interno della rete sono i seguenti:

OP2.6.1 Occorre effettuare controlli appropriati di sicurezza per proteggere i dati sensibili memorizzati e nel corso della trasmissione dei dati, fra cui crittografia in fase di trasmissione dei dati o di scrittura su disco, uso di un'infrastruttura a chiave pubblica, tecnologia VPN (*virtual private network*) e della crittografia per tutti i dati trasmessi tramite Internet;

OP2.4.6 Occorre utilizzare meccanismi di autenticazione per proteggere la disponibilità, l'integrità e la riservatezza dei dati sensibili (ad esempio, firme digitali e dati biometrici);

OP2.7.2 L'organizzazione deve disporre di diagrammi aggiornati che mostrino l'architettura di sicurezza a livello di impresa e la topologia di rete;

OP2.1.1 Occorre predisporre piani di sicurezza documentati per la protezione del sistema e della rete;

OP2.4.1 Occorre utilizzare controlli adeguati degli accessi e strumenti di autenticazione degli utenti (ad esempio, accesso ai file, configurazione della rete) in coerenza con politiche predefinite, allo scopo di delimitare l'accesso degli utenti alle informazioni, alle utility di sistema, al codice sorgente dei programmi, ai sistemi sensibili, ad applicazioni e servizi specifici, alla connessione in rete all'interno dell'organizzazione, alla connessione in rete dall'esterno dell'organizzazione;

OP2.4.3 I metodi/i meccanismi di controllo degli accessi devono delimitare l'accesso alle risorse in rapporto ai diritti di accesso previsti da politiche e procedure;

OP2.1.10 Sul sistema devono essere disponibili soltanto i servizi necessari: tutti i servizi non necessari vanno eliminati;

OP2.5.3 Occorre esaminare periodicamente i punti di vulnerabilità delle tecnologie, che devono essere affrontati non appena individuati;

OP1.1.4 Devono esserci politiche e procedure documentate per la gestione dei visitatori, tra cui firma, accompagnamento, log degli accessi, ricevimento ed ospitalità;

OP2.4.6 Occorre utilizzare meccanismi di autenticazione per proteggere la disponibilità, l'integrità e la riservatezza dei dati sensibili (ad esempio, firme digitali e dati biometrici).

Scheda di controllo tecnico										CC-1P
Profilo di rischio										Alto
Categoria di asset										Persone
Requisiti di sicurezza	Sicurezza fisica	Gestione dei sistemi e della rete	Strumenti di amministrazione del sistema	Monitoraggio e verifica sicurezza IT	Autenticazione ed autorizzazione	Gestione delle vulnerabilità	Crittografia	Architettura e concezione della sicurezza	Gestione degli incidenti	Prassi generali del personale
Riservatezza										3.2.1 3.2.2 3.2.3
Integrità	1.1.4 1.3.2									3.2.1 3.2.2 3.2.3
Disponibilità										

Un profilo di rischio alto implica minacce relative alla gestione delle persone e, più in generale, delle risorse umane. Il livello dell'impegno del personale nell'utilizzare controlli di sicurezza appropriati sulle risorse di rete determina il livello di protezione che può essere conseguito.

Un aspetto critico è dato dalla manipolazione delle informazioni e dal riutilizzo di dati non recenti aventi un alto valore per l'organizzazione. Le informazioni interne o riservate del personale devono essere trattate con rispetto. Il monitoraggio delle politiche del personale riguardanti tali procedure garantisce la riservatezza, l'integrità e la disponibilità delle informazioni.

I controlli essenziali per garantire la riservatezza, l'integrità e la disponibilità delle informazioni laddove l'elemento critico siano le persone sono i seguenti:

OP3.2.1 I membri del personale devono seguire una buona prassi in materia di sicurezza, mettendo in sicurezza le informazioni di cui sono responsabili, non divulgando dati sensibili ad altri (resistenza alla cosiddetta "ingegneria sociale"), avendo un'adeguata capacità di utilizzo di hardware e software, utilizzando una buona prassi in materia di password, comprendendo e rispettando le politiche e le norme di sicurezza, riconoscendo e segnalando gli eventuali incidenti;

OP3.2.2 Tutto il personale, a tutti i livelli di responsabilità, deve attenersi ai ruoli e alle responsabilità assegnati per la sicurezza delle informazioni;

OP3.2.3 Devono esserci procedure documentate per l'autorizzazione ed il controllo delle persone che dispongono di dati sensibili o che operano nei luoghi in cui tali informazioni sono archiviate. Fra queste: i dipendenti, gli appaltatori, i partner, i collaboratori ed il personale di organizzazioni terze, il personale che si occupa della manutenzione dei sistemi, nonché il personale addetto alla manutenzione dei locali;

OP1.1.4 Devono esserci politiche e procedure documentate per la gestione dei visitatori, tra cui firma, accompagnamento, log degli accessi, ricevimento ed ospitalità;

OP1.3.2 Gli individui o i gruppi – rispetto a tutti i mezzi fisicamente controllati – devono poter essere considerati responsabili delle proprie azioni.

Scheda di controllo tecnico					CC-2A					
Profilo di rischio					**Medio**					
Categoria di asset					**Applicazione**					
Requisiti di sicurezza	**Sicurezza fisica**	**Gestione dei sistemi e della rete**	**Strumenti di amministrazione del sistema**	**Monitoraggio e verifica sicurezza IT**	**Autenticazione ed autorizzazione**	**Gestione delle vulnerabilità**	**Crittografia**	**Architettura e concezione della sicurezza**	**Gestione degli incidenti**	**Prassi generali del personale**
Riservatezza					2.4.2		2.6.1			
Integrità					2.4.2					
Disponibilità		2.1.6 2.1.7								

Un profilo di rischio medio implica il salvataggio e l'elaborazione di informazioni proprietarie di valore interno o moderato, tipicamente soggette ad una minaccia generica proveniente da soggetti esterni che tendono abusivamente a violare o compromettere la riservatezza di informazioni di valore specifico o moderato. Nel caso di un profilo di rischio medio, i controlli su un'applicazione relativi alla riservatezza riguardano tipicamente i requisiti di sicurezza volti a salvaguardare il ciclo di vita delle informazioni critiche, i controlli relativi all'integrità definiscono il livello di accuratezza delle informazioni, mentre i controlli relativi alla disponibilità si riferiscono al livello di accessibilità.

I controlli essenziali per garantire la riservatezza, l'integrità e la disponibilità di un'applicazione sono i seguenti:

OP2.4.2 Occorre predisporre politiche e procedure documentate relative all'uso delle informazioni rispetto all'accesso di individui o di gruppi, allo scopo di definire le regole per la concessione di un livello appropriato di accesso, stabilire il diritto iniziale di accesso, modificare il diritto di accesso, togliere il diritto di accesso, rivedere e verificare periodicamente i diritti di accesso;

OP2.6.1 Occorre effettuare controlli appropriati di sicurezza per proteggere i dati sensibili memorizzati e nel corso della trasmissione dei dati, fra cui crittografia in fase di trasmissione dei dati o di scrittura su disco, uso di un'infrastruttura a chiave pubblica, di tecnologia VPN (*virtual private network*) e della crittografia per tutti i dati trasmessi tramite Internet.

OP2.1.6 Occorre predisporre un piano documentato per il backup dei dati che sia aggiornato di routine e verificato periodicamente, preveda backup periodici programmati del software e dei dati, test periodici e verifica della capacità di recuperare i dati salvati in backup;

OP2.1.7 Tutto il personale deve essere consapevole ed essere in grado di farsi carico delle proprie responsabilità derivanti dai piani di backup.

Scheda di controllo tecnico										CC-2S
Profilo di rischio										Medio
Categoria di asset										Sistema
Requisiti di sicurezza	Sicurezza fisica	Gestione dei sistemi e della rete	Strumenti di amministrazione del sistema	Monitoraggio e verifica sicurezza IT	Autenticazione ed autorizzazione	Gestione delle vulnerabilità	Crittografia	Architettura e concezione della sicurezza	Gestione degli incidenti	Prassi generali del personale
Riservatezza		2.1.6 2.1.7			2.4.1					
Integrità		2.1.9			2.4.1					
Disponibilità		2.1.6 2.1.7								

Un profilo di rischio medio implica minacce di livello moderato provenienti da instabilità del sistema, che possono portare all'indisponibilità del servizio per un breve periodo di tempo. Il sistema non è in grado di sostenere adeguatamente le applicazioni o le funzioni.

I controlli sul sistema, quando il profilo di rischio è medio, comprendono metodi che garantiscono un'adeguata configurazione e funzionalità del sistema per un accesso appropriato.

I controlli essenziali per garantire la riservatezza, l'integrità e la disponibilità del sistema sono i seguenti:

OP2.4.1 Occorre utilizzare controlli adeguati degli accessi e strumenti di autenticazione degli utenti (ad esempio, accesso ai file, configurazione della rete) in coerenza con politiche predefinite, allo scopo di delimitare l'accesso degli utenti alle informazioni, alle utility di sistema, al codice sorgente dei programmi, ai sistemi sensibili, ad applicazioni e servizi specifici, alla connessione in rete all'interno dell'organizzazione, alla connessione in rete dall'esterno dell'organizzazione;

OP2.1.6 Occorre predisporre un piano documentato per il backup dei dati che sia aggiornato di routine e verificato periodicamente, prevedendo backup periodici programmati del software e dei dati, test periodici e verifica della capacità di recuperare i dati salvati in backup;

OP2.1.7 Tutto il personale deve essere consapevole ed essere in grado di farsi carico delle proprie responsabilità derivanti dai piani di backup;

OP2.1.9 Il personale IT deve seguire determinate procedure quando rilascia, modifica e interrompe le password, gli account ed i privilegi degli utenti. Per tutti gli utenti del sistema, compresi i soggetti terzi, si richiede un'unica identificazione dell'utente. Gli account e le password di default vanno eliminati dal sistema.

Scheda di controllo tecnico							CC-2N			
Profilo di rischio							**Medio**			
Categoria di asset							**Rete**			
Requisiti di sicurezza	**Sicurezza fisica**	**Gestione dei sistemi e della rete**	**Strumenti di amministrazione del sistema**	**Monitoraggio e verifica sicurezza IT**	**Autenticazione ed autorizzazione**	**Gestione delle vulnerabilità**	**Crittografia**	**Architettura e concezione della sicurezza**	**Gestione degli incidenti**	**Prassi generali del personale**
Riservatezza							**2.6.1**			
Integrità					**2.4.3**					
Disponibilità		**2.1.5**								

Un profilo di rischio medio implica minacce provenienti da vulnerabilità della rete a causa di un'architettura della rete errata o mal realizzata, che possono portare ad attacchi esterni o all'accesso non autorizzato a determinate aree della rete di interesse moderato e di valore medio per l'organizzazione.

La mancanza di sicurezza della rete comporta effetti immediati e diretti sul funzionamento delle applicazioni e sul flusso delle informazioni. Il rischio è considerato medio quando il sistema non consente l'accesso a componenti critiche che potrebbero incidere direttamente sulla reputazione o sulla situazione finanziaria dell'organizzazione.

I controlli essenziali per garantire la riservatezza, l'integrità e la disponibilità di una rete sono i seguenti:

OP2.6.1 Occorre effettuare controlli appropriati di sicurezza per proteggere i dati sensibili memorizzati e nel corso della trasmissione dei dati, fra cui crittografia dei dati in fase di trasmissione dei dati o di scrittura su disco, uso di un'infrastruttura a chiave pubblica, di tecnologia VPN (*virtual private network*) e della crittografia per tutti i dati trasmessi tramite Internet;

OP2.4.3 I metodi/i meccanismi di controllo degli accessi devono delimitare l'accesso alle risorse in rapporto ai diritti di accesso previsti da politiche e procedure;

OP2.1.5 Tutti i sistemi devono essere aggiornati rispetto a revisioni, patch e raccomandazioni (nei consigli per la sicurezza).

Scheda di controllo tecnico										CC-2P
Profilo di rischio										Medio
Categoria di asset										Persone
Requisiti di sicurezza	Sicurezza fisica	Gestione dei sistemi e della rete	Strumenti di amministrazione del sistema	Monitoraggio e verifica sicurezza IT	Autenticazione ed autorizzazione	Gestione delle vulnerabilità	Crittografia	Architettura e concezione della sicurezza	Gestione degli incidenti	Prassi generali del personale
Riservatezza										3.2.1 3.2.2
Integrità										3.2.1 3.2.2
Disponibilità	1.1.4									

Un profilo di rischio medio implica minacce provenienti dalla gestione delle risorse umane di imprese di medie dimensioni, quando le prassi correnti di sicurezza potrebbero portare a problemi di impatto moderato.

Incidenti derivanti da un uso improprio delle password o dei diritti di accesso possono far uscire inavvertitamente delle informazioni. Il livello di riservatezza delle informazioni (medio) determina il livello di rischio o l'eventuale danno economico per l'organizzazione.

Il monitoraggio delle politiche del personale riguardanti tali procedure garantisce la riservatezza, l'integrità e la disponibilità delle informazioni.

I controlli essenziali per garantire la riservatezza, l'integrità e la disponibilità delle informazioni laddove l'elemento critico siano le persone sono i seguenti:

OP3.2.1 I membri del personale devono seguire una buona prassi in materia di sicurezza, mettendo in sicurezza le informazioni di cui sono responsabili, non divulgando dati sensibili ad altri (resistenza alla cosiddetta "ingegneria sociale"), avendo un'adeguata capacità di utilizzo di hardware e software, utilizzando una buona prassi in materia di password, comprendendo e rispettando le politiche e le norme di sicurezza, riconoscendo e segnalando gli eventuali incidenti;

OP3.2.2 Tutto il personale, a tutti i livelli di responsabilità, deve attenersi ai ruoli e alle responsabilità assegnati per la sicurezza delle informazioni;

OP1.1.4 Devono esserci politiche e procedure documentate per la gestione dei visitatori, tra cui firma, accompagnamento, log degli accessi, ricevimento ed ospitalità.

Scheda di controllo tecnico					CC-3A					
Profilo di rischio					**Basso**					
Categoria di asset					**Applicazione**					
Requisiti di sicurezza	**Sicurezza fisica**	**Gestione dei sistemi e della rete**	**Strumenti di amministrazione del sistema**	**Monitoraggio e verifica sicurezza IT**	**Autenticazione ed autorizzazione**	**Gestione delle vulnerabilità**	**Crittografia**	**Architettura e concezione della sicurezza**	**Gestione degli incidenti**	**Prassi generali del personale**
Riservatezza					2.4.2					
Integrità										
Disponibilità										

Un profilo di rischio basso implica il salvataggio e l'elaborazione di informazioni pubbliche o interne, prive però di un livello critico di importanza, per cui il danno economico sarebbe soltanto di lieve entità. La reputazione dell'organizzazione non è in gioco. Tuttavia, vanno introdotti controlli atti a prevenire la fuga di informazioni anche di questo tipo e ad assicurare il ciclo di vita delle informazioni.

Inoltre, anche se non vi è nessun impatto sulla riservatezza, occorre garantire l'integrità e la disponibilità delle informazioni rispetto a tutti gli utenti autorizzati.

Un controllo essenziale relativo alla riservatezza in un'applicazione è il seguente:

OP2.4.2 Occorre predisporre politiche e procedure documentate relative all'uso delle informazioni rispetto all'accesso di individui o di gruppi, allo scopo di definire le regole per la concessione di un livello appropriato di accesso, stabilire il diritto iniziale di accesso, modificare il diritto di accesso, togliere il diritto di accesso, rivedere e verificare periodicamente i diritti di accesso.

Scheda di controllo tecnico										CC-3S
Profilo di rischio										Basso
Categoria di asset										Sistema
Requisiti di sicurezza	Sicurezza fisica	Gestione dei sistemi e della rete	Strumenti di amministrazione del sistema	Monitoraggio e verifica sicurezza IT	Autenticazione ed autorizzazione	Gestione delle vulnerabilità	Crittografia	Architettura e concezione della sicurezza	Gestione degli incidenti	Prassi generali del personale
Riservatezza		2.1.9			2.4.1					
Integrità					2.4.1					
Disponibilità		2.1.6								

Un profilo di rischio basso implica minacce di livello minimo che comportano potenziali instabilità del sistema, tali da determinare l'indisponibilità del servizio per un breve periodo di tempo.

I controlli sul sistema, quando il profilo di rischio è basso, comprendono metodi che garantiscono un'adeguata configurazione e funzionalità del sistema per un accesso appropriato.

L'impatto dell'indisponibilità del sistema non incide sulla reputazione dell'organizzazione, in quanto le informazioni non sono private, né di importanza critica per l'organizzazione.

L'indisponibilità del sistema non incide sulla qualità del servizio o del prodotto.

I controlli essenziali per garantire la riservatezza e la disponibilità del sistema sono i seguenti:

OP2.4.1 Occorre utilizzare controlli adeguati degli accessi e strumenti di autenticazione degli utenti (ad esempio, accesso ai file, configurazione della rete) in coerenza con politiche predefinite, allo scopo di delimitare l'accesso degli utenti alle informazioni, alle utility di sistema, al codice sorgente dei programmi, ai sistemi sensibili, ad applicazioni e servizi specifici, alla connessione in rete all'interno dell'organizzazione, alla connessione in rete dall'esterno dell'organizzazione;

OP2.1.6 Occorre predisporre un piano documentato per il backup dei dati che sia aggiornato di routine e verificato periodicamente, prevedendo backup periodici programmati del software e dei dati, test periodici e verifica della capacità di recuperare i dati salvati in backup;

OP2.1.9 Il personale IT deve seguire determinate procedure quando rilascia, modifica e interrompe le password, gli account ed i privilegi degli utenti. Per tutti gli utenti del sistema, compresi i soggetti terzi, si richiede un'unica identificazione dell'utente. Gli account e le password di default vanno eliminati dal sistema.

Scheda di controllo tecnico							CC-3N			
Profilo di rischio							**Basso**			
Categoria di asset							**Rete**			
Requisiti di sicurezza	**Sicurezza fisica**	**Gestione dei sistemi e della rete**	**Strumenti di amministrazione del sistema**	**Monitoraggio e verifica sicurezza IT**	**Autenticazione ed autorizzazione**	**Gestione delle vulnerabilità**	**Crittografia**	**Architettura e concezione della sicurezza**	**Gestione degli incidenti**	**Prassi generali del personale**
Riservatezza							**2.6.1**			
Integrità										
Disponibilità										

Un profilo di rischio basso implica minacce derivanti da vulnerabilità minori della rete o dall'indisponibilità di informazioni a causa di un'architettura della rete errata o mal realizzata. L'impatto, tuttavia, può essere considerato insignificante, poiché le informazioni non sono di grande interesse né di elevata riservatezza per l'organizzazione. Conseguentemente, il danno economico potenziale per l'organizzazione è di modesta entità.

Si raccomandano comunque controlli di sicurezza relativi al trasferimento di informazioni crittografate.

Il controllo essenziale per garantire la riservatezza della rete è il seguente:

OP2.6.1 Occorre effettuare controlli appropriati di sicurezza per proteggere i dati sensibili memorizzati e nel corso della trasmissione dei dati, fra cui crittografia in fase di trasmissione dei dati o di scrittura su disco, uso di un'infrastruttura a chiave pubblica, di tecnologia VPN (*virtual private network*) e della crittografia per tutti i dati trasmessi tramite Internet.

Scheda di controllo tecnico										CC-3P
Profilo di rischio										**Basso**
Categoria di asset										**Persone**
Requisiti di sicurezza	**Sicurezza fisica**	**Gestione dei sistemi e della rete**	**Strumenti di amministrazione del sistema**	**Monitoraggio e verifica sicurezza IT**	**Autenticazione ed autorizzazione**	**Gestione delle vulnerabilità**	**Crittografia**	**Architettura e concezione della sicurezza**	**Gestione degli incidenti**	**Prassi generali del personale**
Riservatezza										
Integrità										
Disponibilità	1.1.4									

Un profilo di rischio basso implica minacce potenziali con un impatto basso sulla gestione delle risorse umane. Le prassi correnti in materia di sicurezza potrebbero comportare problemi, ma con un rischio minimo per l'organizzazione.

La criticità delle informazioni non è di livello elevato. Pertanto, l'impatto in termini finanziari è modesto e il danno economico può essere considerato insignificante.

Tuttavia, il monitoraggio delle politiche del personale, anche rispetto a tali procedure, garantisce ulteriormente la riservatezza, l'integrità e la disponibilità delle informazioni.

Il controllo essenziale per garantire la riservatezza, l'integrità e la disponibilità delle informazioni, laddove l'elemento critico siano le persone, è il seguente:

OP1.1.4 Devono esserci politiche e procedure documentate per la gestione dei visitatori, tra cui firma, accompagnamento, log degli accessi, ricevimento ed ospitalità.

Allegato C. Controlli organizzativi

Sensibilizzazione alla sicurezza e formazione (SP1)	
SP1.1	I membri del personale sono consapevoli del proprio ruolo e delle proprie responsabilità in tema di sicurezza. Ciò è documentato e verificato.
SP1.2	All'interno dell'azienda vi sono competenze adeguate per i servizi, i meccanismi e le tecnologie (ad esempio, logging, monitoraggio o crittografia), comprese le operazioni in sicurezza. Ciò è documentato e verificato.
SP1.3	La sensibilizzazione alla sicurezza, la formazione ed i richiami periodici interessano tutto il personale. Le conoscenze del personale sono documentate e la relativa conformità è verificata periodicamente. La formazione comprende i seguenti argomenti:
	· strategie ed obiettivi di sicurezza
	· norme, politiche e procedure di sicurezza
	· politiche e procedure per lavorare con soggetti terzi
	· piani alternativi e di disaster recovery
	· requisiti di sicurezza fisica
	· prospettiva degli utenti su:
	- gestione dei sistemi e della rete
	- strumenti di amministrazione del sistema
	- monitoraggio e verifica sicurezza IT, fisica e delle informazioni
	- autenticazione ed autorizzazione
	- gestione delle vulnerabilità
	- crittografia
	- architettura e concezione della sicurezza
	· gestione degli incidenti
	· prassi generali del personale
	· applicazione, sanzioni ed azioni disciplinari per violazioni della sicurezza
	· modalità adeguate di accesso a dati sensibili o operatività in aree in cui è possibile accedere a dati sensibili
	· politiche e procedure di interruzione dell'accesso per motivi di sicurezza

Strategia di sicurezza (SP2)	
SP2.1	Le strategie dell'organizzazione comprendono di routine riflessioni sulla sicurezza.
SP2.2	Le strategie e le politiche in materia di sicurezza tengono conto delle strategie e degli obiettivi dell'organizzazione.
SP2.3	Le strategie e gli obiettivi in materia di sicurezza sono documentati e sono oggetto di revisione periodica, aggiornamento e comunicazione all'organizzazione.

Gestione della sicurezza (SP3)	
SP3.1	La direzione assegna risorse sufficienti, umane e finanziarie, per le attività relative alla sicurezza delle informazioni.
SP3.2	I ruoli e le responsabilità in materia di sicurezza sono definiti per tutto il personale.
SP3.3	Le prassi di assunzione e cessazione del rapporto di lavoro, per tutto il personale, tengono conto delle questioni inerenti la sicurezza delle informazioni.
SP3.4	I livelli richiesti di sicurezza delle informazioni rispetto agli individui ed ai gruppi sono documentati ed applicati.
SP3.5	L'organizzazione gestisce i rischi per la sicurezza delle informazioni, fra cui:
	· valuta il rischio di sicurezza delle informazioni, sia periodicamente, sia in risposta a cambiamenti rilevanti delle tecnologie, nelle minacce interne/esterne o nei sistemi e nelle operazioni dell'organizzazione
	· adotta misure atte a ridurre i rischi ad un livello accettabile
	· mantiene un livello di rischio accettabile
	· utilizza la valutazione del rischio relativo alla sicurezza delle informazioni per selezionare le misure ed i controlli aventi il miglior rapporto costi/benefici, realizzando un equilibrio tra costi di attuazione e perdite potenziali.
SP3.6	La direzione riceve rendiconti periodici che sintetizzano i risultati delle operazioni seguenti, agendo di conseguenza:
	· revisione dei log di sistema
	· revisione del tracciato di verifica
	· valutazione delle vulnerabilità tecnologiche
	· incidenti riguardanti la sicurezza e relative risposte
	· valutazione del rischio
	· revisione della sicurezza fisica
	· piani e raccomandazioni per il miglioramento della sicurezza

Politiche e norme di sicurezza (SP4)	
SP4.1	L'organizzazione dispone di un insieme esauriente di politiche correnti documentate, che sono oggetto di revisione periodica ed aggiornamento. Tali politiche riguardano aree tematiche chiave in materia di sicurezza, fra cui:
	· strategia e gestione della sicurezza
	· gestione del rischio sicurezza
	· sicurezza fisica
	· gestione dei sistemi e della rete
	· strumenti di amministrazione del sistema
	· monitoraggio e verifica della sicurezza IT
	· autenticazione ed autorizzazione
	· gestione delle vulnerabilità
	· crittografia
	· architettura e concezione della sicurezza
	· gestione degli incidenti
	· prassi generali del personale
	· leggi e norme applicabili
	· sensibilizzazione e formazione
	· gestione collaborativa della sicurezza delle informazioni
	· piani alternativi e di disaster recovery
SP4.2	L'organizzazione dispone di un processo documentato per la gestione delle politiche di sicurezza, fra cui:
	· creazione
	· amministrazione (compreso riesame ed aggiornamento periodico)
	· comunicazione
SP4.3	L'organizzazione dispone di un processo documentato per la valutazione periodica (tecnica e non tecnica) dell'osservanza delle politiche di sicurezza delle informazioni, delle leggi e delle norme applicabili, nonché degli obblighi assicurativi.
SP4.4	L'organizzazione dispone di un processo documentato per garantire l'osservanza delle politiche di sicurezza delle informazioni, delle leggi e delle norme applicabili, nonché degli obblighi assicurativi.
SP4.5	L'organizzazione applica in maniera uniforme le proprie politiche in materia di sicurezza.
SP4.6	Soltanto il personale autorizzato può disporre la verifica e la revisione delle politiche e delle procedure in materia di sicurezza.

Gestione collaborativa della sicurezza (SP5)	
SP5.1	L'organizzazione dispone di procedure documentate, monitorate ed applicate per la tutela delle informazioni quando opera con organizzazioni esterne (ad esempio, soggetti terzi, collaboratori, subappaltatori o partner).
SP5.2	L'organizzazione ha accertato che i servizi di sicurezza, i meccanismi e le tecnologie esternalizzati rispondono alle proprie necessità ed esigenze.
SP5.3	L'organizzazione documenta, tiene sotto osservazione ed applica strategie di tutela delle informazioni appartenenti ad organizzazioni esterne alle quali proprie componenti infrastrutturali abbiano accesso, o che siano utilizzate da personale proprio.
SP5.4	L'organizzazione si occupa, verificandole, della sensibilizzazione e della formazione del personale che opera con organizzazioni esterne rispetto alle politiche ed alle procedure di sicurezza delle suddette organizzazioni esterne.
SP5.5	L'organizzazione dispone di procedure documentate per togliere l'accesso a personale esterno, le quali specificano le misure di sicurezza più appropriate a tal fine. Tali procedure sono comunicate all'organizzazione esterna e con essa coordinate.

Piani alternativi/piani di disaster recovery (SP6)	
SP6.1	É stata effettuata un'analisi delle operazioni, delle applicazioni e delle criticità dei dati.
SP6.2	L'organizzazione dispone di:
	· piani di continuità aziendale o di operatività in caso di emergenza
	· piani di disaster recovery
	· piani alternativi in risposta ad eventuali situazioni di emergenza.
SP6.3	I piani di continuità aziendale, i piani alternativi e di disaster recovery, tengono conto dei requisiti di accesso fisico ed elettronico e dei relativi controlli.
SP6.4	I piani di continuità aziendale, i piani alternativi e di disaster recovery, sono oggetto di revisione periodica e verifica.
SP6.5	Tutto il personale:
	· è consapevole dei piani di continuità aziendale, dei piani alternativi e di disaster recovery
	· è consapevole delle proprie responsabilità ed è in grado di farvi fronte.

Allegato D. Controlli tecnici

Sicurezza fisica (OP1)	
Piani e procedure per la sicurezza fisica (OP1.1)	
OP1.1.1	L'organizzazione dispone di piani documentati di sicurezza per proteggere i locali, gli edifici e le eventuali aree ad accesso limitato.
OP1.1.2	I piani di sicurezza sono oggetto di revisione periodica, verifica ed aggiornamento.
OP1.1.3	Le procedure ed i dispositivi per la sicurezza fisica sono oggetto di verifiche e revisioni di routine.
OP1.1.4	L'organizzazione dispone di politiche e procedure documentate per la gestione dei visitatori, tra cui:
	· firma
	· accompagnamento
	· log degli accessi
	· ricevimento ed ospitalità
OP1.1.5	L'organizzazione dispone di politiche e procedure documentate per il controllo fisico di hardware e software, tra cui:
	· postazioni di lavoro, portatili, modem, componenti wireless e tutte le altre componenti utilizzate per accedere alle informazioni
	· accesso, archiviazione e recupero dei dati salvati in backup
	· archiviazione di dati sensibili su dispositivi fisici ed elettronici
	· eliminazione di dati sensibili, oppure dei dispositivi sui quali essi sono memorizzati
	· riutilizzo e riciclaggio di carta e dispositivi elettronici
Controllo degli accessi fisici (OP1.2)	
OP1.2.1	L'organizzazione dispone di politiche e procedure documentate per l'accesso di individui e gruppi, tra cui:
	· le regole per la concessione di un livello appropriato di accesso fisico
	· le regole per stabilire il diritto iniziale di accesso
	· le regole per modificare il diritto di accesso
	· le regole per togliere il diritto di accesso
	· la revisione e la verifica periodica dei diritti di accesso
OP1.2.2	L'organizzazione dispone di politiche, procedure e meccanismi documentati per controllare l'accesso fisico a determinate entità. Ciò comprende:
	· aree di lavoro
	· hardware (computer, dispositivi per la comunicazione, ecc.) e software
OP1.2.3	L'organizzazione dispone di procedure documentate per la verifica delle autorizzazioni all'accesso prima di concedere l'accesso fisico.
OP1.2.4	Le postazioni di lavoro e le altre componenti che permettono l'accesso a dati sensibili sono fisicamente protette per prevenire eventuali accessi non autorizzati.
Monitoraggio e verifica della sicurezza fisica (OP1.3)	
OP1.3.1	L'organizzazione conserva la registrazione delle manutenzioni effettuate per documentare le riparazioni e le modifiche apportate alle parti fisiche di una determinata struttura.
OP1.3.2	Gli individui e i gruppi, rispetto a tutti i mezzi fisicamente controllati, devono poter essere considerati responsabili delle proprie azioni.

OP1.3.3	L'organizzazione conserva la registrazione degli interventi di verifica e monitoraggio, i quali sono periodicamente esaminati per individuare le anomalie; sono intraprese le azioni correttive eventualmente necessarie.

Sicurezza IT (OP2)	
Gestione dei sistemi e della rete (OP2.1)	
OP2.1.1	L'organizzazione dispone di piani documentati di sicurezza per proteggere i sistemi e le reti.
OP2.1.2	I piani di sicurezza sono oggetto di revisione periodica, verifica ed aggiornamento.
OP2.1.3	I dati sensibili sono protetti mediante una loro memorizzazione in sicurezza, ad esempio:
	· precise catene di custodia
	· archiviazione dei backup in luogo diverso dalla sede
	· dispositivi rimovibili per la raccolta dei dati
	· processi di disabilitazione ai dati sensibili o ai dispositivi su cui sono memorizzati.
OP2.1.4	L'integrità del software installato è oggetto di verifica periodica.
OP2.1.5	Tutti i sistemi sono aggiornati rispetto a revisioni, patch e raccomandazioni (nei consigli per la sicurezza)
OP2.1.6	L'organizzazione dispone di un piano documentato per il backup dei dati, che:
	· è aggiornato di routine
	· è verificato periodicamente
	· richiede il backup periodico e programmato di software e dati
	· richiede verifiche periodiche della capacità di recuperare i dati salvati in backup.
OP2.1.7	Tutto il personale è consapevole ed è in grado di farsi carico delle responsabilità derivanti dai piani di backup.
OP2.1.8	Le modifiche all'hardware ed al software sono pianificate, controllate e documentate.
OP2.1.9	I membri del personale IT seguono le procedure quando rilasciano, modificano o interrompono le password degli utenti, i loro account e privilegi.
	· è prevista un'identificazione unica per ciascun utente dei sistemi informativi, soggetti terzi compresi
	· gli account e le password di default vanno eliminati dal sistema.
OP2.1.10	Sul sistema figurano soltanto i servizi necessari – tutti i servizi non necessari vanno eliminati.
Strumenti di amministrazione del sistema (OP2.2)	
OP2.2.1	L'applicabilità di nuovi strumenti, nuove procedure e nuovi meccanismi di sicurezza è oggetto di revisione periodica rispetto alle strategie dell'organizzazione in materia di sicurezza
OP2.2.2	L'organizzazione fa uso di strumenti e dispositivi per l'amministrazione in sicurezza del sistema e della rete, che sono oggetto di revisione periodica, aggiornamento o sostituzione. Ad esempio:
	· controllo dell'integrità dei dati
	· strumenti per la crittografia
	· scansione delle vulnerabilità
	· strumenti per verificare la qualità delle password
	· scansione antivirus
	· strumenti di gestione dei processi
	· sistemi di individuazione delle intrusioni
	· amministrazione remota in sicurezza

	· strumenti per la manutenzione della rete
	· analizzatori del traffico
	· strumenti di risposta agli incidenti
	· strumenti di analisi forense dei dati
Monitoraggio e verifica sicurezza IT (OP2.3)	
OP2.3.1	L'organizzazione utilizza di routine strumenti di monitoraggio e verifica del sistema e della rete:
	· l'attività è monitorata dal personale IT
	· l'attività del sistema e della rete è registrata
	· i log sono oggetto di revisione periodica
	· l'attività insolita è affrontata con riferimento alla politica o alla procedura più appropriata
	· gli strumenti sono oggetto di revisione periodica ed aggiornamento.
OP2.3.2	I firewall e le altre componenti di sicurezza sono oggetto di verifica periodica per accertare l'osservanza delle politiche in materia di sicurezza.
Autenticazione ed autorizzazione (OP2.4)	
OP2.4.1	L'organizzazione fa uso di controlli adeguati degli accessi e di strumenti di autenticazione degli utenti (ad esempio, accesso ai file, configurazione della rete) in coerenza con le politiche aziendali relative alla delimitazione dell'accesso degli utenti a:
	· informazioni
	· utility di sistema
	· codice sorgente dei programmi
	· sistemi sensibili
	· applicazioni e servizi specifici
	· connessione in rete all'interno dell'organizzazione
	· connessione in rete dall'esterno dell'organizzazione.
OP2.4.2	L'organizzazione predispone politiche e procedure documentate relative all'uso delle informazioni ed all'accesso di individui e di gruppi:
	· per stabilire le regole per la concessione di un livello appropriato di accesso
	· per stabilire il diritto iniziale di accesso
	· per modificare il diritto di accesso
	· per togliere il diritto di accesso
	· per la revisione e la verifica periodica dei diritti di accesso.
OP2.4.3	I metodi/i meccanismi di controllo degli accessi delimitano l'accesso alle risorse, in rapporto ai diritti di accesso previsti da politiche e procedure.
OP2.4.4	I metodi/i meccanismi di controllo degli accessi sono oggetto di revisione periodica e verifica.
OP2.4.5	L'organizzazione fornisce metodi o meccanismi atti a garantire che non si verifichi l'accesso a dati sensibili, o che essi non siano alterati o distrutti in maniera non autorizzata.
OP2.4.6	L'organizzazione fa uso di meccanismi di autenticazione per proteggere la disponibilità, l'integrità e la riservatezza dei dati sensibili, ad esempio:
	· firme digitali
	· dati biometrici
Gestione delle vulnerabilità (OP2.5)	
OP2.5.1	L'organizzazione dispone di un insieme documentato di procedure per la gestione delle vulnerabilità, tra cui:

	· selezione degli strumenti di valutazione delle vulnerabilità, checklist e script
	· aggiornamento rispetto alle tipologie note di vulnerabilità ed ai metodi di attacco
	· revisione delle fonti di informazione su annunci di vulnerabilità, allarmi di sicurezza ed avvisi analoghi
	· individuazione delle componenti infrastrutturali da valutare
	· programmazione della valutazione delle vulnerabilità
	· interpretazione dei risultati e risposta ad essi
	· conservazione in sicurezza dei dati memorizzati ed eliminazione di dati vulnerabili
OP2.5.2	L'organizzazione adotta le procedure per la gestione delle vulnerabilità, che sono periodicamente oggetto di revisione ed aggiornamento.
OP2.5.3	L'organizzazione effettua periodiche valutazioni della vulnerabilità delle tecnologie; le vulnerabilità sono affrontate a mano a mano che esse vengono individuate.
Crittografia (OP2.6)	
OP2.6.1	L'organizzazione fa uso di appropriati controlli di sicurezza per proteggere i dati sensibili una volta archiviati e durante la loro trasmissione, fra cui:
	· crittografia dei dati in fase di trasmissione
	· crittografia dei dati in fase di scrittura su disco
	· uso di un'infrastruttura a chiave pubblica
	· tecnologia VPN (*virtual private network*)
	· crittografia per tutte le trasmissioni di dati che avvengono tramite Internet
OP2.6.2	Si utilizzano protocolli criptati quando si gestiscono in remoto sistemi, router e firewall.
OP2.6.3	I controlli ed i protocolli relativi alla crittografia sono oggetto di revisione periodica e verifica.
Architettura e concezione della sicurezza (OP2.7)	
OP2.7.1	I sistemi nuovi o modificati devono tener conto, nell'architettura e nella concezione, di:
	· strategie, politiche e procedure aziendali in materia di sicurezza
	· cronologia dei compromessi in materia di sicurezza
	· risultato delle valutazioni del rischio sicurezza
OP2.7.2	L'organizzazione dispone di diagrammi aggiornati che mostrano l'architettura di sicurezza a livello di impresa e la topologia di rete.

Sicurezza del personale (OP3)	
Gestione degli incidenti (OP3.1)	
OP3.1.1	Esistono procedure documentate per identificare, segnalare e dare risposta a sospetti, incidenti e violazioni della sicurezza, fra cui:
	· incidenti riguardanti la rete
	· incidenti relativi all'accesso fisico
	· incidenti dovuti a forme di "ingegneria sociale"
OP3.1.2	Le procedure di gestione degli incidenti sono oggetto di verifica periodica ed aggiornamento.
OP3.1.3	L'organizzazione dispone di politiche e procedure documentate per rapportarsi con i soggetti preposti all'applicazione della legge.
Prassi generali del personale (OP3.2)	
OP3.2.1	I membri del personale seguono una buona prassi in materia di sicurezza, vale a dire:

	· mettono in sicurezza le informazioni di cui sono responsabili
	· non divulgano i dati sensibili ad altri (resistenza alla cosiddetta “ingegneria sociale”)
	· hanno una capacità adeguata di utilizzo di hardware e software IT
	· utilizzano buone prassi in materia di password
	· conoscono ed applicano le politiche e le norme in materia di sicurezza
	· riconoscono e segnalano gli incidenti.
OP3.2.2	Tutto il personale, a tutti i livelli di responsabilità, mette in pratica i ruoli e le responsabilità assegnati per la sicurezza delle informazioni.
OP3.2.3	L’organizzazione dispone di procedure documentate per l’autorizzazione ed il controllo delle persone che dispongono di dati sensibili o che operano nei luoghi in cui tali informazioni sono memorizzate. Ciò comprende:
	· dipendenti
	· appaltatori, partner, collaboratori e personale di organizzazioni terze
	· personale addetto alla manutenzione dei sistemi
	· personale addetto alla manutenzione delle strutture

Allegato E. Alcuni semplici consigli[4]

CENNI IMPORTANTI IN TEMA DI SICUREZZA PER LE PICCOLE E MEDIE IMPRESE

Questi sono gli elementi essenziali di difesa per l'azienda

- ☐ Effettuazione di uno screening di base di tutti i dipendenti e degli appaltatori (ad esempio, sulla base di referenze o raccomandazioni)
- ☐ Conoscenza e documentazione del patrimonio informativo dell'organizzazione
- ☐ Predisposizione di politiche e procedure in materia di sicurezza brevi, efficienti e chiaramente documentate
- ☐ Effettuazione di corsi di formazione di base per sensibilizzare i dipendenti al tema della sicurezza
- ☐ Applicazione di patch per le vulnerabilità del software, in automatico o non appena possibile, previa verifica della loro funzionalità
- ☐ Conoscenza delle persone che possono aver accesso al sistema, con relative motivazioni
- ☐ Utilizzo di password forti da cambiare periodicamente
- ☐ Accertarsi della presenza di sistemi antivirus per i computer e i dispositivi mobili, con aggiornamento automatico
- ☐ Utilizzo di prodotti antivirus diversi per il server e per i client
- ☐ Utilizzo di un sistema di filtraggio dei contenuti per mettere in guardia contro spamming, phishing, contenuti illeciti e proibiti
- ☐ Utilizzo di firewall, specialmente se l'accesso ad Internet è a banda larga
- ☐ Utilizzo di un sistema difensivo multifunzione ("tutto-in-uno") a servizio di una piccola rete

Password

Si tratta della chiave che consente di aprire la porta delle informazioni elettroniche. Chiunque può leggere le informazioni che non sono protette da una password. Se si scelgono password semplici, è possibile che qualcun altro le indovini o le decifri. Presentiamo qui alcuni suggerimenti per creare una password complessa ("forte").

- Aprire il dizionario in maniera casuale e selezionare una parola lunga (di quattro sillabe, ad esempio). Utilizzare questa parola, inserendo però all'interno il numero della pagina. Ad esempio, se il termine <multifarious> si trova alla pagina 345 del dizionario, la password diventa <multi345farious> (se si dimentica la password, bisogna essere in grado di ricordare la pagina selezionata).
- Scegliere una frase che abbia un significato personale. Ad esempio, "my zebra is called Spot and is 9 years old" (la mia zebra si chiama Spot ed ha

[4] Questo allegato intende fornire agli utenti una guida semplice sugli elementi di sicurezza di base. Il materiale è tratto dalle fonti [1], [6] e [10] indicate tra i riferimenti bibliografici.

9 anni). Questa frase, utilizzando le iniziali delle parole, si può trasformare nella password <mzicS&i9yo>. Si tratta di una password molto forte perchè utilizza lettere, numeri e caratteri speciali. Sarà estremamente difficile forzarla.

I must della password sono i seguenti:

- la password deve avere almeno otto caratteri,
- occorre accertarsi di cambiare periodicamente la password, ad esempio, tutti i mesi,
- se un dipendente lascia l'azienda, occorre cambiare immediatamente la sua vecchia password,
- utilizzare una password per ogni applicazione – non utilizzare mai la medesima password per ogni cosa.

Viceversa, vi sono alcune cose che non bisogna mai fare con le password.
Fra queste:

- non mettere mai la password per iscritto,
- non utilizzare mai il proprio nome, il nome del partner o dei propri figli, il numero di targa della macchina, la data di compleanno o qualsiasi altra informazione riguardante se stessi o la propria famiglia, che sia risaputa o possa essere facilmente elaborata con un minino di "ingegneria sociale",
- non usare mai codici speciali che si applichino alla propria persona, ad esempio, numero di telefono, codice fiscale, numero di licenza del software: tutti elementi a cui qualcun altro potrebbe risalire,
- non utilizzare mai gli stessi numeri o le stesse lettere, ad esempio <11111111>, in una password e non utilizzare mai il termine <password> perchè è il primo termine che un hacker proverà,
- non condividere mai la password con altri,
- non utilizzare mai una password di default fornita insieme con un elemento del software – cambiarla subito,
- non utilizzare mai le funzioni di "ricorda la password" sul computer perchè le password archiviate in questo modo sono facilmente recuperabili, con minimo sforzo.

In breve, occorre trattare la password con attenzione, scegliendone una "forte", cambiandola periodicamente ed avendone buona cura.

Virus, worm e trojan

I puristi potranno dire che si tratta di cose diverse, ma dal punto di vista aziendale si possono mettere sul medesimo piano. Il punto critico è dato dal fatto che tutti e tre (virus, worm e trojan) possono danneggiare i computer e le informazioni in essi archiviate. Tuttavia, è veramente semplice evitarli: si può utilizzare un software antivirus. Qualsiasi software antivirus può andar bene, in quanto tutti operano più o meno allo stesso modo e fanno lo stesso tipo di lavoro. La cosa più importante è, semplicemente, utilizzarne uno.

Ciò di cui le persone non si rendono conto è che il software antivirus deve essere tenuto aggiornato. Il che significa aggiornamenti quotidiani – sì, proprio quotidiani – perché ogni giorno vengono rilasciate nuove versioni del software.

Se non si installa un programma antivirus e non lo si mantiene aggiornato, si può essere certi al 100% di prendere un virus prima o poi.

Qualunque sia il software antivirus che si utilizza, occorre installarlo in maniera tale da verificare automaticamente tutti i nuovi dati. In questo modo, se si ricevono nuovi dati tramite un floppy disk, un CD oppure tramite Internet, il software cercherà i virus prima che essi possano provocare qualche danno.

Una regola d'oro è che i file o i dati infettati da virus dovrebbero essere distrutti. Alcuni software antivirus sostengono di disinfettare i file, ma ciò non è mai garantito. La strada più sicura è sempre quella di eliminare i file insieme con il virus. Se si tratta di messaggi di posta elettronica, è meglio distruggerli senza aprirli.

Spamming

Si può pensare che lo spamming sia soltanto fastidioso, ma sfortunatamente comporta anche dei pericoli. Lo spamming:

- può nascondere una frode,
- può innescare una catena perversa di messaggi di posta elettronica,
- può contenere un codice nascosto che altera il settaggio del computer (ad esempio, indirizza ad un sito porno),
- può contenere un codice nascosto che trasforma il proprio computer in un centro di smistamento di spam (vale a dire, una gran quantità di spam viene inviata dal proprio computer in tutto il mondo), spedendo così a tutto il mondo gli indirizzi dei propri clienti e allegando ad essi una nuova copia di spam, worm o trojan.

Nel caso del codice nascosto è altamente probabile che ciò rientri nella categoria dei "trojan" e che sia individuato dal software antivirus. Tuttavia, vi sono alcune regole che occorre seguire con la posta elettronica "spam": se lo si fa, i rischi possono essere ridotti al minimo.

- Se il messaggio è palesemente privo di valore, non ha nessuna importanza personale o per l'azienda, è sgrammaticato, ecc. cancellarlo senza aprirlo.
- Non rispondere mai a messaggi di posta elettronica "spam". L'indirizzo e-mail è stato recuperato in qualche modo e gli "spammer" non sanno neppure se si esiste veramente.
- In caso di risposta, non si fa altro che confermare la propria esistenza e si riceverà una quantità ancora maggiore di spamming.
- All'interno del messaggio di posta elettronica, non cliccare sulla voce "clicca qui per cancellare il tuo nome dalla mailing list". Di solito è un trucco. Lungi dall'essere cancellati, non si fa altro che confermare la propria esistenza.
- Non fornire il proprio indirizzo di posta elettronica a nessuno, se non a persone di fiducia.
- Ciò è molto difficile quando si gestisce un'azienda, perchè si può voler mettere ampiamente a disposizione il proprio indirizzo di posta elettronica. Si può ipotizzare di avere due indirizzi di posta elettronica: uno di uso pubblico ed uno di uso personale, attentamente controllato.
- Se un sito Internet chiede l'indirizzo di posta elettronica, occorre fare una rapida valutazione del rischio. Si tratta di un'organizzazione legittima che gode di una reputazione consolidata? Si tratta di qualcuno di cui non si è

mai sentito parlare e che non indica un indirizzo fisico sul sito web? Va ricordato che gli imbroglioni fingono di essere aziende del tutto legittime.

- I siti Internet che promettono di cancellare il nominativo da una mailing list "spam" in genere non lo fanno. Non utilizzarli mai.

È possibile bloccare lo spamming. Esistono dei software specializzati in questo senso, che però possono essere troppo costosi per le piccole imprese. Probabilmente vale la pena chiedere al proprio provider Internet (ISP) se – per un piccolo canone supplementare – è in grado di bloccare lo spamming utilizzando i propri mezzi. Tuttavia, occorre un poco di cautela: il blocco dello spamming è non solo una scienza, ma anche un'arte. Se i criteri fissati sono troppo rigidi, è facile bloccare anche i messaggi legittimi di posta elettronica.

N.B. Se si riceve un messaggio di posta elettronica che, in qualche modo, minaccia direttamente la propria azienda (ad esempio, contiene minacce di ricatto), occorre mettersi immediatamente in contatto con le forze locali di polizia. Si viene rapidamente indirizzati ad un gruppo di persone specializzate nel gestire le minacce elettroniche. È molto probabile che ciò non vi riguardi direttamente, ma se per caso accadesse .....

Spyware

Si tratta di piccoli programmi spia che si inseriscono nel sistema operativo del computer per raccogliere surrettiziamente informazioni sull'utente/sull'azienda senza che gli interessati se ne accorgano. In gran parte ciò avviene a fini pubblicitari, ma il programma può servire anche a raccogliere informazioni sugli indirizzi di posta elettronica, le password ed i riferimenti delle carte di credito.

Recentemente sono stati diffusi avvertimenti ufficiali riguardanti alcuni programmi spia utilizzati per raccogliere informazioni commercialmente sensibili, ad esempio dettagli relativi ai contratti.
I programmi spia non sono una buona cosa e l'utente attento cerca di delimitarli o rimuoverli completamente. Su Internet sono disponibili due buoni programmi in grado di rimuoverli. Essi sono gratuiti per le persone fisiche, ma a pagamento per le aziende:

- Lavasoft (Ad-aware)
- Spybot

Si raccomanda di scaricare entrambi questi programmi e di farli girare almeno una volta alla settimana. Si rimarrà sorpresi da quello che essi riusciranno a trovare (e non va dimenticato che anch'essi devono essere tenuti costantemente aggiornati!)

Firewall

I firewall traggono il loro nome dalle barriere fisiche (antincendio) costruite negli edifici per impedire il propagarsi delle fiamme. In termini informatici, un firewall è qualcosa che funge da barriera per prevenire l'accesso non autorizzato a/da un sistema informatico privato. Si tratta di una sorta di porta di sicurezza e di allarme contro i ladri, ma applicata ai computer. I firewall servono a ridurre tutte le minacce intenzionali precedentemente indicate. Se si dispone di uno o più computer collegati ad Internet, oggi un firewall è considerato essenziale.

Il firewall può essere sotto forma di software o sotto forma di hardware. Per proteggere i sistemi di grandi dimensioni, può essere un mix di software ed hardware.

Il punto principale è che il firewall controlla tutti i dati in entrata ed anche in uscita, per accertare che essi siano legittimi. Per dirla in due parole: il firewall rappresenta la difesa migliore contro gli hacker. Per citare un caso reale, il firewall può impedire che il proprio computer sia fagocitato da un soggetto terzo e diventi un punto di smistamento di

messaggi di posta elettronica "spam". Vale la pena ricordare che, quando si collega il computer ad Internet, si aprono 65 536 "porte", attraverso le quali i dati possono entrare nel computer. Quello che si vuole realmente è che le porte (quelle necessarie) si aprano soltanto quando le si vuole aprire, per inviare o ricevere dati, e rimangano invece chiuse per la restante parte del tempo.

Si tratta di un'area molto complessa e non è questa la sede per sviscerarne i principi e le prassi, che sono oggetto di tesi di dottorato. Per fortuna i firewall sotto forma di software sono oggi economici, semplici da gestire e facilmente disponibili.
Se si ha un computer, si consiglia di comprare un firewall sotto forma di software, la cui installazione è semplice. Basta accettare il settaggio di default. Se si hanno due o più computer collegati ad Internet, un firewall sotto forma di hardware potrebbe essere un investimento migliore, da installare tra tutti i computer ed il cavo che si collega ad Internet. I firewall sotto forma di hardware sono più complessi ed è preferibile rivolgersi ad un esperto per loro installazione e configurazione. Un professionista potrà garantire che il firewall non sia così tanto sicuro da impedire di fatto il collegamento ad Internet.

(Le aziende che hanno uno o due computer possono comprare un unico pacchetto di software contenente il firewall e l'antivirus. Per le piccole imprese, questa soluzione offre vantaggi economici e tecnici).

Patch

Le patch sono poco conosciute, ma sono molto importanti e si ricollegano alle problematiche dei virus e degli attacchi sferrati dagli hacker. Tutti i software presentano malfunzionamenti e difetti. Nella maggior parte dei casi, i difetti sono minimali, per cui possono essere ignorati e probabilmente non avranno alcun impatto sull'attività aziendale. Alcuni difetti però sono troppo importanti e non possono essere ignorati.

Tutti i produttori di software forniscono delle patch – vale a dire, aggiornamenti del software intesi ad eliminare i problemi del software stesso. Se si dispone di un unico computer che funziona bene e non è collegato a nient'altro (né ad un altro computer, né ad Internet, ecc.), probabilmente non si ha bisogno di preoccuparsi tanto delle patch.

Le problematiche riguardano essenzialmente il sistema operativo del computer, vale a dire il programma di base che fa girare il computer. Si utilizzano magari alcune versioni di Microsoft Windows, o Apple OSX oppure Unix/Linux. Tutti questi sistemi operativi hanno bisogno, ogni tanto, di patch. Ma anche molte applicazioni hanno bisogno occasionalmente di patch. Spesso i browser di navigazione ed i software di posta elettronica hanno bisogno di patch e non è raro che i più comuni software di contabilità abbiano bisogno di patch.

Se non si mantiene aggiornato il software con le patch, si rischia che il software manifesti delle lacune oppure (è il caso del browser o del software di posta elettronica) subisca l'intrusione illecita di un software che può danneggiare il computer o di utenti che possono impossessarsi abusivamente del proprio computer.

La maggior parte dei produttori di software fornisce un servizio di notifica via e-mail con cui essi comunicano ai clienti il rilascio di nuove patch. Di solito essi classificano questi avvisi secondo una scala che va da un massimo di "critico" a "normale" (l'intervento può essere fatto anche in un momento successivo). Se si riceve l'avviso di una patch critica, che riguarda un elemento del software su cui si basa l'attività aziendale, si consiglia di farlo installare il più presto possibile. La continuità aziendale può dipendere da questo intervento. Si può anche consultare il sito web del fornitore di software per eventuali novità sugli aggiornamenti.

Attualmente la maggior parte dei fornitori di software offre aggiornamenti automatici tramite Internet.

Backup

Il backup consiste nel processo di fare una copia dei dati elettronici, ad esempio una copia dei file relativi alla contabilità. Perchè bisogna preoccuparsene? Perchè i dati elettronici si possono perdere facilmente, archiviare in posizioni sbagliate, o distruggere. Se si perde oggi l'unica copia dei file elettronici relativi alla contabilità, come si farà domani a gestire l'azienda?

Un regime formale ed efficiente di backup eviterà molte delle minacce naturali o involontarie precedentemente indicate. I dati essenziali possono essere copiati nel modo seguente:

- su nastro (un metodo vecchio, che però vale ancora la pena di considerare, perchè i nastri possono essere riutilizzati),
- su un secondo hard disk (preferibilmente rimovibile),
- su un CD (circa 700 Mb) oppure su un DVD (circa 4,3 Gb).

Occorre considerare l'ipotesi di fare più di un backup dei dati critici utilizzando tre generazioni di strumenti. Ad esempio, si possono conservare progressivamente i dati "di fine settimana" delle ultime tre settimane, in modo tale da disporre sempre del backup di tre settimane (o generazioni) nel caso in cui si debba ricreare il sistema. Un regime adeguato di backup per un'azienda (ma ciò vale anche per un commerciante singolo) sarebbe il seguente:

- alla fine di ogni giornata: backup di tutti i file che sono stati modificati in quella giornata,
- alla fine di ogni settimana: backup di tutte le applicazioni (contabilità, corrispondenza, ecc.),
- alla fine di ogni mese: backup anche del sistema operativo.

Qualora si debba ricostruire il computer dopo un evento catastrofico, si può utilizzare il backup dell'ultimo "fine mese" per recuperare il sistema operativo e poi si riprende il backup relativo alle applicazioni dell'ultimo "fine settimana".
Per finire, si riprende il backup effettuato a "fine giornata" per ciascuno dei giorni successivi all'ultimo "fine settimana". In questo modo, si riesce a ricostruire il sistema completo. Se uno dei backup è illeggibile (un evento sorprendentemente frequente, a prescindere dal mezzo utilizzato per il backup), si può passare alla copia immediatamente precedente e ricominciare da lì. Se ciò accade, è improbabile che si riesca a recuperare tutto fino all'ultimo file di dati. È inevitabile che qualcosa si perda. Ciò è tuttavia preferibile alla perdita di tutti i propri preziosi dati.

Questo tipo di metodologia di backup è in uso da quando sono stati inventati i computer e, con il passare del tempo, ha dimostrato la propria affidabilità. Si possono utilizzare metodologie più complesse quando i dati cambiano rapidamente o hanno un valore molto elevato. Bisogna essere pronti al cambiamento qualora il rischio aziendale si modifichi.

I dati salvati in backup vanno conservati al sicuro. Il loro valore è pari a quello dei dati originali. Essi sono soggetti anche ai medesimi principi dell'*Information Architecture Institute* (IA). Non bisogna lasciarli in luoghi dove essi possano essere trafugati o danneggiati. Non bisogna neanche lasciarli appoggiati sul computer. Se il computer

esplode o brucia che cosa accadrà al backup di sicurezza? Idealmente, i dati salvati in backup devono essere conservati in un edificio completamente diverso da quello dove si trova il computer. Se l'ufficio viene distrutto da un incendio, occorre fare in modo che il medesimo destino non riguardi anche i dati salvati in backup.

Un problema non trascurabile può verificarsi quando si ha fretta di trovare il backup di alcuni dati, ma il titolare del backup ha dimenticato di apporre sui dischi di backup l'etichetta contenente data ed argomento.....

Un'opzione percorribile, se si dispone di un gran numero di backup su mezzi diversi, consiste nell'acquistare una "cassaforte ignifuga". Tale cassaforte può essere conservata in loco, ma bisogna essere consapevoli del fatto che, dopo un grosso incendio, possono occorrere anche 2/3 giorni prima che la cassaforte si raffreddi tanto da poterla aprire.

Furto di informazioni e identità

Si tratta di uno dei reati in più rapida crescita, sia nel Regno Unito, sia in altri paesi sviluppati. È stata fatta molta pubblicità sul tema, ma un punto importante non viene menzionato: il furto di informazioni e identità può riguardare sia le imprese, sia gli individui.

Per un'impresa è essenziale che le informazioni superate siano eliminate in sicurezza. Ciò comprende le copie su carta e su mezzi elettronici. Non è raro che il sito Internet di piccole imprese sia "dirottato" da qualcuno che ha rubato vecchi esemplari di carta intestata e ha recuperato la firma degli amministratori. Ciò viene utilizzato per falsificare lettere da inviare alle agenzie che registrano i domini Internet facendo registrare nuovamente il sito web con un nuovo indirizzo fisico. A quel punto si instaura un'impresa fraudolenta, che può perfino ricorrere al credito.

Anche gli individui possono essere oggetto di furto dell'identità per intenti fraudolenti. Nei casi di chiara frode perpetrata da altri, non si è considerati responsabili, ma il problema – quando avviene un furto di identità – consiste nel recuperare la credibilità presso le banche e gli istituti finanziari, in particolare presso le agenzie che attribuiscono il rating del credito.
Ecco alcune cose da non fare:

- non fornire mai, a nessuno, informazioni personali tramite Internet, posta elettronica, telefono o lettera, a meno che non si sia certi di potersi fidare;
- ricordare che le banche non chiedono mai ai propri clienti di confermare la password o il codice di accesso tramite posta elettronica, per cui queste informazioni non devono essere fornite;
- non gettare documenti personali o aziendali riservati senza prima averli strappati; sarebbe meglio utilizzare un distruttore di documenti che li taglia due volte (trasversalmente e diagonalmente);
- il materiale elettronico o magnetico non più necessario deve essere danneggiato fisicamente, in maniera tale da non poter essere riutilizzato;
- se si hanno conti correnti bancari aziendali inutilizzati o linee di credito con vecchi fornitori, è opportuno chiuderli perchè potrebbero essere sfruttati per intenti fraudolenti.

In ogni caso, occorre verificare attentamente gli estratti conto bancari e gli altri documenti finanziari non appena si ricevono. Pagamenti o addebiti strani devono essere oggetto di accertamento immediato. La banca non si preoccupa se i clienti le pongono dei quesiti: la

banca è interessata quanto i clienti a limitare le frodi. Un altro punto da considerare consiste nel verificare periodicamente la propria posizione di credito, personale o aziendale, nel caso in cui si verifichi uno dei seguenti fatti inattesi:

- ditte di cui non si è mai sentito parlare fanno domande sul proprio rating del credito,
- commenti negativi sul proprio rating,
- notifica di una variazione di indirizzo,
- riferimenti a sentenze di un tribunale, ecc.

Reti wireless

Le reti wireless (WiFi in breve) sono molto attraenti per le piccole imprese. La loro installazione è economica, la configurazione è facile; esse consentono flessibilità e diminuiscono il problema del cablaggio, difficile ed oneroso. Sfortunatamente, è anche molto facile costruire una rete WiFi che consenta a chiunque di leggere i propri dati aziendali riservati.

Il grande rischio è che chiunque, nel raggio d'azione wireless, possa utilizzare la propria rete WiFi: altre persone potrebbero utilizzare gratuitamente la connessione ad Internet, captare il traffico di dati, ad esempio messaggi di posta elettronica, password, file di dati di accesso presenti sul computer o perfino captare i propri riferimenti bancari via Internet. Una rete WiFi non sicura presenta un grande rischio di spionaggio industriale.

L'installazione di una rete WiFi all'interno della propria azienda deve essere attentamente pianificata e probabilmente richiede l'aiuto di esperti. Questo documento non può rappresentare una guida completa all'installazione di una rete. Qui il punto importante da considerare è che la rete WiFi può e deve essere creata in sicurezza, in modo tale che soltanto se stessi e i propri dipendenti possano utilizzarla e attraverso di essa accedere ai dati o condividerli. Forniamo qui alcuni suggerimenti essenziali.

In primo luogo, sfortunatamente, alcune importanti note tecniche. Tutto il WiFi deve conformarsi allo standard IEEE 802.11, il quale comprende svariati sottoinsiemi. Quelli importanti sono 802.11 G e 802.11 N. La versione "G" è già operativa, mentre la versione "N" non lo è ancora. A fini aziendali, si può cercare la versione "G" anche se sono già in vendita alcuni kit denominati "pre N", i quali però potrebbero non risultare pienamente compatibili con lo standard "N" definitivo. La versione "N" consente una velocità di trasmissione molto superiore ed una sicurezza potenzialmente migliore. Non bisogna farsi tentare dalle varianti "A" o "B", oggi superate, in quanto esse sono più lente e meno sicure.

Non bisogna fidarsi delle dichiarazioni dei fornitori. In genere, la velocità di trasmissione è la metà di quella dichiarata per metà della distanza, a meno che non si operi in condizioni di laboratorio. Le caratteristiche costruttive dell'edificio possono incidere notevolmente sulle prestazioni WiFi; sono gli edifici in pietra a manifestare la maggior parte dei problemi.

Che cosa occorre:

- un router wireless che trasmetta e riceva i segnali dei dati diffusi all'interno dell'ufficio; i router più elaborati possono essere configurati in modo tale che il raggio d'azione del segnale non vada oltre il confine del proprio edificio;

- una connessione a banda larga, se non se ne dispone;
- un adattatore wireless per ogni computer; nella maggior parte dei portatili moderni l'adattatore è già fornito, ma i desk top devono essere dotati di un apposito adattatore; si raccomanda un adattatore wireless che si inserisca direttamente in una porta USB.

Quando l'azienda ha un server centrale già installato, con una connessione Internet già esistente, al server sarà collegato direttamente un router. Gli uffici di piccole dimensioni possono comprare il router con un modem incorporato a banda larga. Possono essere acquistati dispositivi più elaborati, che uniscono al router un firewall per maggior protezione. Un buon suggerimento è quello di comprare tutto il kit WiFi da un solo produttore. È meglio non mescolare i fornitori perchè se, una volta fatto l'abbinamento, qualcosa non funziona ciascuno darà la colpa all'altro. Inoltre, naturalmente, è meglio non comprare una marca sconosciuta.

Per la sicurezza sono essenziali le seguenti note tecniche:

- tutte le trasmissioni dei dati devono essere criptate; anziché utilizzare la crittografia WEP (*Wired Equivalent Privacy*), sarebbe preferibile la crittografia WPA (*Wi-Fi Protected Access*) o WPA2;
- utilizzare chiavi precondivise (PSK) per creare una sorta di password tra i computer ed il router; si raccomanda di utilizzare una password forte;
- attribuire un nome unico alla rete WiFi (attraverso il *Service Set IDentifier* o SSID);
- creare un nome sicuro che sia di fantasia;
- configurare il router WiFi in maniera tale che l'identificativo (SSID) non venga trasmesso;
- non utilizzare mai la chiave SSID di default del produttore;
- registrare nel router gli indirizzi MAC dei computer dell'ufficio e creare una regola che preveda che soltanto gli indirizzi MAC registrati possano dialogare con il router;
- accertarsi che il server e i sistemi operativi dei computer supportino il WiFi prima di comprare il kit.

Se tutto ciò suona un po' difficile, non tentare il "fai-da-te". Bisogna chiedere ad un esperto di installare la rete WiFi. E non bisogna dimenticare che i dati sono probabilmente il cespite più importante che si ha, da proteggere con un WiFi sicuro. Dopo tutto, non si vuole che la propria rete diventi un "access point" pubblico.

Soggetti terzi

Abbastanza spesso, nelle varie attività di una PMI, sono coinvolti soggetti terzi. Si tratta, in generale, di servizi di consulenza per la gestione ed il marketing, nonché di supporto IT per i sistemi critici. Il più delle volte a questi soggetti viene consentito l'accesso ad informazioni societarie riservate o a sistemi e infrastrutture di rete a fini di manutenzione. È essenziale che le aziende assicurino la riservatezza di queste informazioni, sia sul piano contrattuale, sia attraverso un adeguato processo di controllo degli accessi. Come minimo, quando vengono a contatto con soggetti terzi, le PMI dovrebbero prendere in considerazione i controlli seguenti:

- far firmare un impegno di non divulgazione e riservatezza;
- consentire l'accesso alle informazioni in rapporto alle esigenze, il che significa che i soggetti terzi dovrebbero poter accedere soltanto alle

informazioni di cui hanno assolutamente bisogno per lo svolgimento delle proprie attività;

- l'accesso a soggetti terzi che si occupano di supporto IT NON dovrebbe essere consentito in permanenza, a meno che ciò non sia esplicitamente richiesto e necessario; una volta terminate le necessarie attività, l'accesso va interrotto immediatamente; il tracciato di verifica va stampato e esaminato per verificare che le attività svolte si siano limitate ad operazioni legittime di manutenzione;
- chiedere ai soggetti terzi interessati di poter verificare le loro misure di protezione della sicurezza, nei casi in cui le informazioni riservate e societarie siano elaborate nei locali dei suddetti soggetti terzi.

Provider di servizi

I provider di servizi sono tipicamente *Internet Service Provider* (ISP), *Application Service Provider* (ASP) e provider di telecomunicazioni. Prima di selezionare un determinato provider, i responsabili dell'azienda dovrebbero informarsi circa le regole stabilite dal potenziale provider, per sapere ad esempio se sono stati stabiliti limiti superiori per l'ampiezza di banda, se i messaggi di posta elettronica sono filtrati e, in caso affermativo, sulla base di quali regole.

Tipicamente i provider archiviano i dati degli utenti per la fatturazione (nome, indirizzo, identificativo utente, conto corrente bancario), nonché i dati relativi alle connessioni ed i contenuti trasmessi (per un periodo di tempo variabile da un provider ad un altro).

Gli utenti dovrebbero chiedere ai propri provider quali dati resteranno archiviati presso di loro e per quanto tempo. Quando si seleziona un provider, occorre tener conto del fatto che i provider dell'UE devono rispettare le norme riguardanti la tutela dei dati che si applicano all'elaborazione di informazioni di questo tipo.

Ricorrendo alla crittografia, gli utenti possono impedire ai provider di leggere i contenuti dei dati trasferiti.

Per ulteriori controlli, è sufficiente rispondere alle domande seguenti:

- Quali sono i criteri di selezione del provider?
- Quali sono le misure di sicurezza adottate dal provider?
- Secondo quali criteri i messaggi di posta elettronica sono filtrati dal provider di posta? Il provider è disponibile H24 per risolvere gli eventuali problemi tecnici? Qual è il suo livello di competenza?
- Fino a che punto il provider è preparato in caso di malfunzionamento di uno o più dei suoi sistemi IT (piani alternativi, backup dei dati)?
- Qual è il livello di disponibilità che il provider può garantire (tempo massimo di guasto)? Il provider verifica periodicamente che le connessioni ai clienti restino stabili e, in caso negativo, adotta misure appropriate?
- Cosa fa il provider per garantire la sicurezza dei propri sistemi IT e quella dei propri clienti?

Politiche e linee guida in materia di sicurezza delle informazioni dovrebbero essere un fatto scontato per tutti i provider. Gli utenti esterni dovrebbero poter visionare le linee guida in materia di sicurezza del provider. Il personale del provider deve essere messo a conoscenza degli aspetti relativi alla sicurezza IT e deve essere obbligato ad osservare le linee guida in materia di sicurezza. Il personale dovrebbe anche seguire periodicamente corsi di formazione (non soltanto in materia di sicurezza).

Protezione dei dati e privacy

Dipendenti a parte, occorre chiedersi quale sia il cespite chiave dell'organizzazione che è invisibile, per lo più sottovalutato, di cui mani sbagliate possono fare un uso improprio e che si può perdere in un istante.

La risposta più probabile è: le informazioni. Una buona prassi in materia di sicurezza delle informazioni consente alle persone giuste, nel momento in cui esse ne hanno bisogno, di visualizzare ed elaborare informazioni corrette. La legislazione oggi impone che i dati di carattere personale siano protetti in maniera adeguata.

La legge del 1998 in materia di tutela dei dati personali è entrata in vigore il 1° marzo 2000. Essa riguarda i dati di carattere personale, vale a dire le informazioni su individui viventi e identificabili - le "persone interessate".

Gli obblighi previsti dalla legge sono così riassumibili:

- valutazione del rischio relativo ad informazioni di natura personale e sensibile;
- identificazione dei controlli necessari per proteggere i dati e la privacy;
- sviluppo ed attuazione di politiche di sicurezza delle informazioni.

Riferimenti

1. Panel consultivo sulle frodi, I reati cibernetici: tutto quello che le PMI dovrebbero sapere.
2. Jack A. Jones, CISSP, CISM, CIS, *An Introduction to Factor Analysis of Information Risk (FAIR)*, un quadro d'insieme per comprendere, analizzare e misurare il rischio relativo alle informazioni
3. ENISA, *Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises (SMEs)*
4. ENISA, *Risk Management: Implementation Principles and Inventories for Risk Management/Risk Assessment Methods and Tools*
5. ISO 27001
6. *Directors Guide for Information Security,* Department of Trade and Industry
7. *Security in an Uncertain World: SME's and a Level Playing Field,* Oxford Integrated Systems
8. Commissione delle Comunità europee, Direzione generale, unità B6, Sicurezza delle telecomunicazioni e dei sistemi informativi, *Information Technology Security Evaluation Manual* (manuale ITSEM), versione 1.0
9. *Information Technology Security Evaluation Criteria* (ITSEC), Department of Trade and Industry, Regno Unito
10. *Information Assurance Guide and Questionnaire for Small & Medium Sized Businesses (SMEs),* Leeds City Council
11. Russell Morgan, *Information Security for Small Businesses*
12. *Network and Information Security Report*, ICTSB / NISSG
13. Raccomandazione della Commissione, del 3 aprile 1996, relativa alla definizione delle piccole e medie imprese
14. *The OCTAVE (SM) Method Implementation Guide*, versione 2.0
15. Charles A. Shoniregun, *Impacts and Risk Assessment of Technology for Internet Security - Enabled Information Small-Medium Enterprises*
16. Gazzetta ufficiale dell'Unione europea (20.5.2003)
17. Alpa A. Virdi, *Risk Management among SMEs - Executive report of discovery research*, Institute of Chartered Accountants in England and Wales, novembre 2005
18. *Reputation: Risk of risks*, An Economist Intelligence Unit White Paper, dicembre 2005
19. «Risk management service for SMEs» (Newsletter), International Accounting Bulletin n. 3, 24 maggio 2006, ISSN: 0265-0223, Lafferty Publications Ltd
20. *Information Security Guide for Small Businesses,* Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), INFOSEC of the office of Government Chief Information Officer (OGCIO) and the Technology Crime Division HK Police force of the HKSAR Government [Guida alla sicurezza informatica per le piccole imprese, predisposta da strutture governative e di polizia di Hong Kong, regione amministrativa speciale della Repubblica Popolare Cinese]
21. http://sme.cordis.lu/home/index.cfm (SME TechWeb)
22. http://europa.eu.int/information_society/policy/ecomm/info_centre/documentation/legislation/index_en.htm#top (La società dell'informazione in Europa – Portale tematico)