Una metodologia di valutazione dei rischi per la sicurezza delle informazioni

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

Gli approcci possibili alla valutazione dei rischi possono essere diversi ed i metodi per effettuare il cosiddetto ***Risk Assessment*** possono variare di caso in caso, in funzione della dimensione, della complessità e del tipo di organizzazione che si sta esaminando.

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

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

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

1) Identificazione dei rischi

2) Analisi e ponderazione dei rischi

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

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

5) Accettazione dei rischi residui.

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

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

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

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

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

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

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

Impatto = Valore Asset x Gravità Minaccia x Gravità Vulnerabilità.

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

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

una scala qualitativa avviene secondo il seguente schema:

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

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

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

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

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

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

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

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

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

Il piano di trattamento dei rischi riporta le seguenti informazioni:

1) Elenco dei rischi da trattare;

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

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

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

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

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

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

Gli asset possono essere delle seguenti tipologie:

1. *Information asset*: dati digitali e non digitali, sistemi operativi, software

applicativo, beni intangibili (conoscenza, marchi, brevetti, …).
2. *Asset fisici*: infrastruttura IT, Hardware, Sistemi di controllo, Servizi IT.
3. *Risorse Umane*: dipendenti, collaboratori esterni e consulenti.

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

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

Ad ogni *asset* di supporto o *asset* non informativo (risorse fisiche e risorse umane) viene associato un valore in termini di criticità dell'asset, dato dalla somma dei valori di importanza dei requisiti *dell'asset* in termini di Riservatezza, Integrità, Disponibilità in funzione delle informazioni che esso gestisce. Dunque l'importanza di una risorsa per la sicurezza dipende dai requisiti di Riservatezza, Integrità e Disponibilità, espressi in livelli (Basso/Medio/Alto) a cui corrisponde il valore 1/2/3.

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

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

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

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