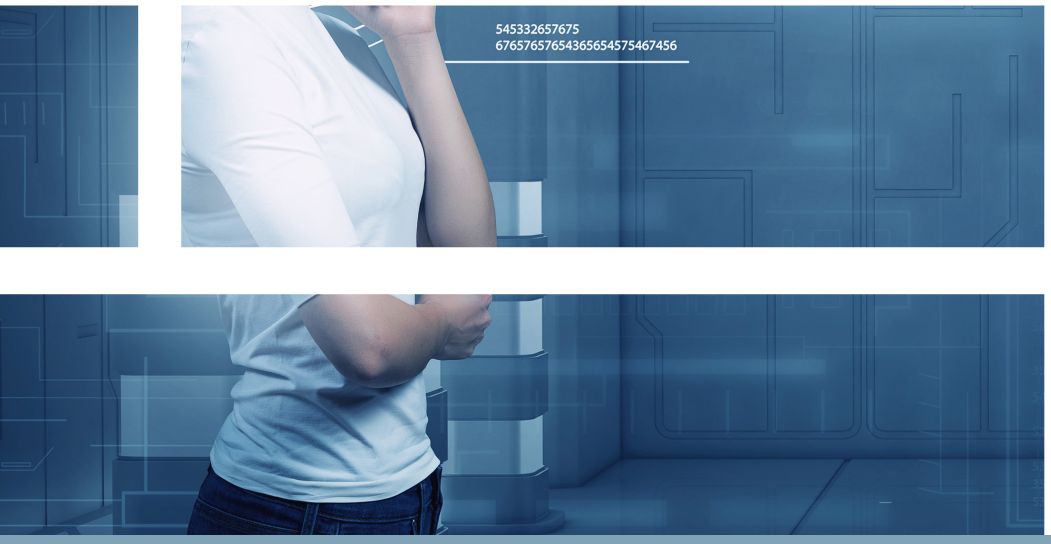

ASSESSMENT del rischio per il business legato ai sistemi informativi aziendali

La continuità di utilizzo dei sistemi informativi aziendali è condizione indispensabile per i processi di business.
Le applicazioni, le reti informatiche, le infrastrutture, i servizi in Cloud richiedono una valutazione dell'impatto che hanno sui processi e dei rischi per l'azienda che derivano da guasti o disastri.
L'industrializzazione del servizio lo rende rapido, economico ed efficace.

E' un processo di valutazione dei rischi che vengono identificati stimando le conseguenze che interruzioni dei servizi ICT potrebbero avere sul business aziendale, prevedendone la possibilità di accadimento e valutando le contromisure adottabili.
La stima dei rischi prende in considerazione l'albero delle dipendenze dei principali servizi informativi aziendali, secondo una analisi ABC. Viene concordato un livello accettabile di rischio e di conseguenza adottate soluzioni.
Il processo di gestione dei rischi consiste in una revisione periodica dell'assessment ed in una rielaborazione delle contromisure per migliorare costantemente i key indicators.
L'adozione di queste strategie produce i seguenti effetti:

- riduzione del rischio
- rimozione del rischio
- trasferimento del rischio.

Criteri di valutazione

La sicurezza delle informazioni implica la protezione di quattro aspetti:
- **Disponibilità**: l'accessibilità motivata alle informazioni
- **Integrità**: la completezza e la leggibilità delle informazioni
- **Autenticità**: la validità delle informazioni
- **Riservatezza**: la possibilità che solo chi è autorizzato possa leggere le informazioni.

La sicurezza richiede quindi, che le informazioni e l'accesso alle stesse siano rigorosamente controllate.

Standard di riferimento

Per fornire un servizio realmente aderente alle esigenze e alle caratteristiche della Piccola e Media Impresa Italiana si è deciso di creare un modello di valutazione del rischio che attingesse dai migliori sistemi esistenti, permutando il meglio da ognuno e contestualizzandone i metodi all'analisi delle Pmi.

Gli standard di riferimento:
- UNI CEI ISO/IEC 27001:2005
- Pacchetto Informativo per le Pmi
- (Enisa_07, European Network and Information Security Agency)
- (BSI, Bundesamt für Sicherheit in der ITaGrundschutz Methodology Informationstechnik)

Valutazione del rischio

La valutazione del livello di rischio è in funzione dell'entità del danno che l'asset considerato arrecherebbe all'organizzazione imprenditoriale in uno dei seguenti scenari:
- **perdita di disponibilità**: interruzione (temporanea o prolungata) del processo/servizio supportato; interruzione dell'accesso e/o di utilizzo di un determinato asset o delle informazioni ivi conservate
- **perdita di integrità**: modifica delle informazioni senza autorizzazione; perdita o distruzione dell'asset
- **perdita di riservatezza**: divulgazione delle informazioni a persone, entità o processi non autorizzati.

L'approccio utilizzato prevede la quantificazione di quattro livelli di rischio: Nullo, Basso, Medio, Alto.