Testata: **Venezie Post - Monitor**
Periodicità: **settimanale**
Pagina: **web**
Data: **5 marzo 2016**

ADACTA RISPONDE

Adacta Risponde

Gestione dei rischi informatici: nuovi obblighi ed opportunità

Sono amministratore di una Spa che detiene importanti asset immateriali (know-how) e che è dotata di sistemi informatici discretamente complessi. Come deve essere gestito correttamente l'obbligo di adottare e mantenere un generale standard di "adeguatezza organizzativa" aziendale in relazione ai rischi in ambito informatico? Come ...

Strada Marosticana, 6/8 – 36100 Vicenza
Tel. 0444.228000 Fax 0444.228600 E-mail: info@adacta.it

Testata: **Venezie Post - Monitor**
Periodicità: **settimanale**
Pagina: **web**
Data: **5 marzo 2016**

Gestione dei rischi informatici: nuovi obblighi ed opportunità

DI LUCA DE MURI

Sono amministratore di una Spa che detiene importanti asset immateriali (know-how) e che è dotata di sistemi informatici discretamente complessi. Come deve essere gestito correttamente l'obbligo di adottare e mantenere un generale standard di "adeguatezza organizzativa" aziendale in relazione ai rischi in ambito informatico? Come si può evitare il rischio di sovrapposizioni tra presidii e controlli, ma al tempo stesso rispettare le diverse normative che regolano i relativi processi operativi e gestionali ed evitare sanzioni? Come si può dimostrare ai soci, agli organi di controllo, al personale e in genere all'utenza, che l'azienda è stata diligente?

La gestione del rischio informatico, e più in generale del rischio aziendale in materia di tutela dei sistemi di protezione delle informazioni, è oggi un fronte caldissimo, per varie ragioni. In primis: l'applicazione necessaria di una pletora di norme non coordinate: D. Lgs. 196/2003 sulla privacy a breve sostituito dal nuovo Regolamento UE 2016; Provvedimenti del Garante; D.Lgs. 231/2001 su modelli organizzativi per prevenire i reati informatici; D.Lgs. 30/2005 sulla tutela del know-how; artt. 621-623 codice penale sulla violazione dei segreti; pareri dei Garanti Europei; disciplina sul cd. "Patent box"; Jobs Act, ecc.

In secondo luogo, l'incessante sviluppo della tecnologia, che espone l'azienda a nuovi pericoli connessi per esempio ai servizi "cloud" (SaaS, Iaas, Paas, portali e siti), all'uso di device mobili come tablet e smartphone e ai sistemi GPS. Ancora: il ricorso all'outsourcing di importanti attività infrastrutturali e di sicurezza IT verso big player (Google, Amazon, ecc.) o terzi fornitori critici, con esigenze di adeguata contrattualizzazione dei rapporti; l'internazionalizzazione, che causa un inevitabile aumento degli scambi di dati transfrontalieri; la diffusioni di beni e servizi basati su sistemi intelligenti IoT (Internet of Things) e sul trattamento dei big data.

Tali scenari operativi richiedono l'adozione di soluzioni coerenti ed efficienti di Governance IT a sostegno del business.

Le soluzioni possono essere diversificate: dalla certificazione di qualità (norme es. ISO/EN 27001), a standard ripetibili quali COBIT e ITIL, o metodi più "lean", modulari e meno impattanti (DPS, DPIA), ma talora molto efficaci in rapporto al costo/beneficio.

Strada Marosticana, 6/8 – 36100 Vicenza
Tel. 0444.228000 Fax 0444.228600 E-mail: info@adacta.it

Un adeguato assetto della Governance IT, pur nella varietà dei contesti aziendali, presuppone alcune azioni che sono oramai qualificabili come "minimo sindacale". Per evitare potenziali censure o sanzioni l'amministratore dovrà adottare un metodo di risk approach che contemperi la necessità di ridurre i rischi ad un livello accettabile e l'efficacia-efficienza dei controlli. Occorre perciò un progetto strategico da trasformare in step tattici ed operativi. E' ineludibile "fotografare" l'infrastruttura, operare l'individuazione dei rischi (IT, normativi, operativi, ecc.) tramite apposite griglie valutative, attuare una gap analysis rispetto ai medesimi e agli obiettivi aziendali (valutando tramite eventuale BIA -Business Impact Analysis- l'impatto dei rischi sui diversi processi). Bisogna ridefinire gli obiettivi IT ed allineare ad essi la programmazione delle risorse (umane, di budget, tecniche, organizzative). Serve una chiara distribuzione di responsabilità tra tutti i soggetti coinvolti (Responsabili IT, incaricati interni, outsourcers, consulenti, ecc.) e la puntuale ricognizione, ed eventuale re-engineering, della contrattualistica informatica, in modo da tutelare l'azienda rispetto a comportamenti inadeguati dei fornitori e verso i clienti. Assume grande importanza anche l'adozione di policies "trasversali" che regolino l'utilizzo degli strumenti informatici e garantiscano la compliance dei relativi controlli. È opportuno stabilire flussi monitorabili di informazioni periodiche per avvicinare gli IT Manager al management e ai terzi controllori (collegio sindacale, membri dell'organismo di vigilanza 231). Aiuta infine la capacità di gestire centralmente i processi di Risk Compliance Management, anche via software, per evitare ridondanze, formalizzare e monitorare costantemente i presidii e i controlli, personalizzare l'approccio ed evitare quindi il ricorso quanto mai inopportuno a soluzioni cheap o "generaliste".

l.demuri@adacta.it

Sabato 5 Marzo 2016

Strada Marosticana, 6/8 – 36100 Vicenza
Tel. 0444.228000 Fax 0444.228600 E-mail: info@adacta.it