## Aspetti di sicurezza delle infrastrutture informatiche della P.A.

**A B S T R A C T**

Nell’attuale contesto di rapidissima evoluzione tecnologica, i sistemi informatici e di comunicazione rappresentano un fattore sempre più cruciale per la crescita del Paese. Le grandi opportunità offerte da questa evoluzione si accompagnano, però, a sempre maggiori rischi di vulnerabilità dei sistemi informatici, per i quali, spesso, si sottovalutano gli aspetti di protezione necessari.

Anche la Pubblica Amministrazione sta operando su vari fronti per l’adeguamento tecnologico delle proprie infrastrutture informatiche, attraverso un percorso di razionalizzazione delle risorse e reingegnerizzazione dei processi, soprattutto in un’ottica di maggiore sicurezza e resilienza dei sistemi.

La crescita dell’informatica nella Pubblica Amministrazione è avvenuta, negli anni, in maniera disorganica. E’ stata spesso frutto delle politiche di *marketing* delle aziende, piuttosto che delle reali esigenze degli enti pubblici, ed ha determinato un’elevata frammentarietà a scapito dei necessari elementi di robustezza e stabilità. E così, mentre si è riusciti, tutto sommato, a dare delle risposte in termini di fornitura di servizi ai cittadini sempre più automatizzati, al contrario non si è attuato quel processo di necessaria pianificazione e razionalizzazione delle risorse *hardware* che avrebbe determinato maggiore efficienza operativa, standardizzazione delle procedure e riduzione dei costi.

L’inefficienza e la stratificazione tecnologica prodotta da uno scenario del genere sono evidenti. Si pensi alle tante funzioni duplicate, alla ridondanza dei servizi di gestione, al sotto-utilizzo delle risorse informatiche, alla dispersione di spazi fisici, ai consumi energetici necessari per alimentare gli apparati, in particolar modo quelli relativi al condizionamento, alla frammentazione dei contratti con i fornitori che riduce fortemente il potere negoziale e le economie di scala.

Anche un recente studio del Centro di Ricerca in Cyber Intelligence e Information Security dell’Università “La Sapienza”, in collaborazione con L’Agenzia per l’Italia Digitale (AgID), volto a capire il livello di consapevolezza della minaccia cibernetica e l’attuale capacità difensiva della PA Italiana, ha evidenziato una situazione di estrema frammentazione e di sostanziale impreparazione in termini di sicurezza cibernetica.

La soluzione individuata per migliorare la sicurezza del contesto infrastrutturale informatico pubblico è, senza dubbio, il suo “consolidamento” in pochi *data center* nazionali (espandibili), in possesso di elevati livelli tecnologici, rigidi criteri di sicurezza logica e fisica, e con caratteristiche energetiche innovative ed ambientalmente sostenibili. I benefici che ne deriverebbero, valutabili in termini di riduzione dei costi, maggiore utilizzazione delle risorse, bilanciamento automatico del loro impiego, alta affidabilità, minori consumi energetici, semplificazione di gestione, sono evidenti. Inoltre si ridurrebbe la superficie di possibili attacchi cibernetici, con conseguenti vantaggi in termini di sicurezza e resilienza.

Riguardo quest’ultima, al fine di realizzare un disegno architetturale solido ed efficiente, è indispensabile l’implementazione di un sistema per la gestione della continuità operativa dei servizi e per il loro ripristino in caso di disastro (così come anche previsto normativamente dall’art 50 bis del C.A.D.).

In tal modo si potrebbe dare vita ad un “ecosistema” digitale all’avanguardia, integrato e condiviso da più amministrazioni pubbliche, magari basato su un’architettura di tipo “*cloud*” privato, nel quale ciascuna Amministrazione, pur mantenendo la propria autonomia gestionale, possa fornire servizi in totale sicurezza. Verrebbe così agevolata la creazione di un importante “polo tecnologico nazionale”, nonché la possibilità di implementare una *cloud community* della Pubblica Amministrazione, per l’erogazione di servizi digitali sempre più innovativi.