Associazione Italiana Cultura Qualità
via Cornalia 19, 20124 Milano
Direzione: aicqna.direzione@aicq.it
Segreteria: aicqna.segreteria@aicq.it

All'attenzione del
Direttore Generale
dell'Agenzia per l'Italia Digitale,
Dott.ssa Alessandra Poggiani

Oggetto: Sulla "Strategia per la Crescita Digitale 2014-2020"

Con riferimento al documento "Strategia per la Crescita Digitale 2014-2020" del 6 novembre 2014, disponibile per la pubblica consultazione sul sito dell'Agenzia per l'Italia Digitale, la scrivente Associazione Italiana Cultura Qualità (AICQ) ritiene opportuno sottolineare diversi aspetti che debbano essere compiutamente affrontati al fine di dare un contributo in linea con l'esigenza di digitalizzazione del nostro Paese, nel rispetto di normative di riferimento diffusamente adottate, anche a livello europeo.
L'AICQ ritiene che la Crescita Digitale debba avvenire attraverso un'evoluzione, anche culturale, che sottolinei l'importanza del rispetto delle normative e al tempo stesso porti alla semplificazione nella loro applicazione. Un'evoluzione che deve produrre un insieme di best practices che siano modello di riferimento per il mondo delle imprese e, più in generale, per la società civile e soprattutto siano percepite in quanto tali.
L'elaborazione del nostro contributo è fondata sull'idea che le novità normative e tecnologiche debbano essere il lievito di una trasformazione culturale capace di generare ***nuove*** *strumentazioni e competenze del "****management delle organizzazioni digitali****" nelle Amministrazioni PAC/PAL e nel mondo delle imprese.*
Il contributo è articolato in diverse proposte sotto elencate, che si ritiene possano costituire oggetto di approfondimento, in sede di sviluppo della Strategia per la Crescita Digitale 2014-2020, a cui l'AICQ fin d'ora dà la propria disponibilità.

1. Adozione standard internazionali

La proposta è quella di adottare per le amministrazioni PAC/PAL gli standard internazionali sottoelencati anche attraverso linee guida concepite specificatamente per esse.
La stesura delle linee guida potrebbe giovarsi di una propedeutica attività di valutazione delle esperienze in corso. Gli standard sono:

- ISO 22301 – Business Continuity Management System
- ISO/IEC 27001 – Information Security Management System
- ISO 9001 – Sistemi di Gestione della Qualità applicati al settore del SW e servizi IT
- ISO/IEC 20000-1 – IT service management

2. Protection Profile

Si propone per le stazioni appaltanti e per i processi di acquisizione l'adozione dei profili di protezione certificati. A partire dagli standard e dalle linee guida di sicurezza (Cybersecurity) definite per tutta la pubblica amministrazione da AGid, potrebbero essere definiti uno o più Profili di Protezione (Protection Profile) certificati da OCSI (Organismo di certificazione della Sicurezza Informatica le cui certificazioni CC sono riconosciute a livello internazionale) secondo i Common Criteria sulla base dei quali possano essere realizzate soluzioni ICT certificabili per gli aspetti di sicurezza informatica, rispondenti ad un set di requisiti di ICT security condiviso e in grado di offrire livelli di garanzia di sicurezza confrontabili. La norma di riferimento è la ISO/IEC 15408 (Common Criteria - CC)

3. Sviluppo di linee guida per l'implementazione di sistemi integrati e auditing

Un radicale cambiamento potrebbe derivare dalla coniugazione di un approccio multistandard con tutte le necessarie declinazioni del concetto d'integrazione verso un unico sistema di gestione: si propone l'adozione di un modello integrato di organizzazione, gestione e controllo. Al tema dello sviluppo integrato dei sistemi di gestione si connette il tema della rendicontazione e della trasparenza. Si propone l'adozione del bilancio sociale per l'organizzazione digitale.

4. Sviluppo di linee guida finalizzate alla prevenzione e al contrasto della criminalità informatica

La proposta è quella di suggerire alle amministrazioni e agli enti di adottare le BEST-PRACTICES che di fatto introducano nella PAC/PAL il sistema di controllo DUALE rispetto a quello previsto nelle aziende dalle norme di cui sotto finalizzate alla prevenzione e al contrasto della criminalità informatica. Si tratta di promuovere l'adozione di un adeguato Modello di Organizzazione e Gestione idoneo ad individuare e prevenire reati, vigilando sul suo funzionamento e osservanza. Devono ovviamente essere previste idonee verifiche, iniziali e periodiche, nonché le eventuali modifiche che, nel tempo, fossero ritenute necessarie.
Nel Modello dovranno trovare opportuno risalto i temi della GOVERNANCE dell'innovazione in generale e della digitalizzazione. Le norme sono:

- Legge sulla Privacy
- CAD – Codice Amministrazione Digitale
- Legge 231/2001 e modelli di organizzazione-gestione-controllo.
- Legge 190/2012

Tutto ciò finalizzato a definire modalità per costruire, attuare e monitorare i Piani Anticorruzione nella PA in ottica innovativa e di servizio al cittadino, nonché a promuovere un approccio sistemico anti corruzione che consideri anche le norme in materia di tracciabilità dei flussi finanziari, antiriciclaggio, antimafia, trasparenza e valutazione performance.

In particolare l'adozione nella PAC/PAL di un Modello di Organizzazione e Gestione (corrispondente al modello aziendale 231) costituirebbe un efficace contrasto alla corruzione e come tale un vantaggio competitivo per il Paese in questo difficile congiuntura economica.

Fra le best practices sarebbe opportuno valutare l'introduzione di strumenti per standardizzare ed informatizzare le segnalazioni del dipendente che evidenzia gli illeciti (wisthleblowing).

5. Sui ruoli e le competenze della gestione

Al cuore del cambiamento ci sono le competenze e le persone che sosterranno i nuovi ruoli del management nella nuova organizzazione digitale.
Si propone di partire dalle definizioni europee (e-CF 3.0) e di applicarle alle amministrazioni PAC/PAL, se necessario, anche attraverso rielaborazioni specificatamente concepite per esse. I livelli di management (tecnico-operativo, intermedio, apicale) dovranno essere opportunamente rielaborati per le esigenze delle amministrazioni PAC/PAL.
A carico dei livelli apicali di management rimane la responsabilità di gestire i ruoli chiave del cambiamento e dell'innovazione tecnologica.
I profili interessati possono essere:

- Livello tecnico-operativo
  - Capo progetto
  - Capo servizio
  - Quality manager
- Livello intermedio
  - Capo programma
  - Responsabile di divisione (BUSINESS UNIT)
  - Direttore dei sistemi informativi – CIO
- Livello apicale
  - I ruoli preposti al cambiamento e all'innovazione tecnologica

6. Formazione e certificazione delle competenze

Con riferimento ai profili indicati al punto precedente, ma anche ad altri (quali gli auditor e i progettisti di sistemi) si propone un sistema di qualificazione, certificazione e mantenimento delle competenze digitali in coerenza con i modelli organizzativi, integrato con un programma di formazione continua indispensabile per affrontare l'evoluzione e l'innovazione continua sempre più determinante.

7. Gestione degli approvvigionamenti IT

Per le stazioni appaltanti PAC/PAL si propone di elaborare delle linea guida relative alla gestione degli approvvigionamenti di attrezzature/infrastrutture/servizi/prodotti IT mirate al raggiungimento efficace ed efficiente degli obiettivi previsti, avendo come riferimento le norme citate al punto n. 1 ed in particolare la norma ISO-IEC 20000-1. L'intento è quello di coordinare in modo strutturato, semplificandolo, tutto il processo di approvvigionamento in ambito IT, a partire dalle definizioni tecniche delle specifiche dei beni/servizi da approvvigionare, fino alle fasi finali di validazione operativa dei risultati ottenuti, mediante test, verifiche e valutazione di SLA (Service Level Agreement) in ottica utenti/utilizzatori finali dei beni/servizi IT.
Si propone inoltre di introdurre nei contratti opportuni SLA anche a carico dell'ente appaltante, con relative di metriche di rilevazione ed eventuali penali, in caso di mancato rispetto delle tempistiche che devono essere osservate dall'Amministrazione per portare a completamento le fasi, i controlli, le approvazioni di propria competenza. Infine, potrà essere utile approfondire i rischi di comportamenti illeciti nella gestione degli appalti, nei casi in cui lo sblocco di fasi di avanzamento di progetto è demandato ai singoli che non devono sottostare a nessuno SLA, e come questi possano essere ridotti costruendo dei protocolli di controllo efficienti.

AICQ ringrazia l'Agenzia per l'Italia Digitale per l'opportunità offerta e il gruppo di lavoro che ha elaborato questa nota, così costituito (i cui componenti sono sotto elencati in ordine alfabetico):

1. **Roberto Baracco** – AICQ Piemontese
2. **Giulio Cantù** – Comitato AICQ *Qualità del software e dei Servizi IT*
3. **Mario Cislaghi** – Comitato AICQ *Qualità del software e dei Servizi IT*
4. **Almerico Fedele** – Comitato AICQ *Qualità del software e dei Servizi IT*
5. **Ettore La Volpe** - AICQ Tosco Ligure
6. **Claudio Provetti** - Direttore Funzione Sistemi di Gestione Sicurezza ICT, Ispezioni e Formazione & Direttore CSQ e membro del Consiglio di AICQ Centronord
7. **Antonio Rassu** - Comitato AICQ *Qualità del software e dei Servizi IT*
8. **Attilio Rampazzo –** AICQ triveneta
9. **Silvano Ronchi** - Responsabile SICEV per l'area informatica
10. **Claudio Rosso –** Area Associazioni professionali e Commissioni UNI
11. **Valerio Teta** – Comitato AICQ *Qualità del software e dei Servizi IT*
12. **Claudio Zottola** – Comitato AICQ *Qualità del software e dei Servizi IT*

Per ogni comunicazione il referente è Antonio Rassu, mail: consultazione-agid@rassu.org