CONSIGLIO NAZIONALE INGEGNERI

C3i COMITATO ITALIANO INGEGNERIA DELL'INFORMAZIONE

Necessità di nuovi paradigmi per gli appalti pubblici in ambito ICT

Problematiche, attuazione e proposte
28 gennaio 2021

a cura del Gruppo di lavoro del C3i - Appalti pubblici in ambito ICT, monitoraggio bandi e concorsi

Stefano Bossi – Presidente Filiera Digital Confindustria Emilia, Membro Consiglio Generale Confindustria Nazionale

Digit PA (NG-EU) : UN'OCCASIONE SENZA PRECEDENTI

Complessivamente il capitolo digitalizzazione, innovazione e sicurezza della Pa beneficia di fondi per 11,45 miliardi. Le tre voci principali riguardano:

- 7,95 miliardi per la digitalizzazione, suddivisi in 5,57 miliardi per la Cittadinanza Digitale, Servizi e Piattaforme Abilitanti, 1,25 miliardi per le Infrastrutture digitali e cyber security, 1,13 miliardi per i Dati e l'interoperabilità
- 1,5 miliardi per la Modernizzazione della Pa
- 2 miliardi per l'innovazione organizzativa della Giustizia.

(fonte: Ministero per la PA)

- Dati Assinform 2020 sulla domanda digitale per il settore PA: Difesa (0,5Mld); Enti Locali (0,7Mld); Sanità (1 Mld)

- Indice DESI Italia sui Servizi Pubblici Digitali: 19° Posto (su 28 …) , punteggio 67,5 (72 dato medio Europeo)

Il contesto attuale in ambito Gare ICT

- Gare Pubbliche ambito ICT: evidenti differenze di skills tra Centrali Appaltanti di tipo PAC e tipo PAL (Enti Locali Sanità)
- Convenzioni Centrali : MEPA (commodity)
- CONSIP (appannaggio dei grandissimi player ICT)
- Convenzioni Regionali (i.e. Intercenter)

Estrarre Valore nella assegnazione degli «Appalti di Lavori» (1)

- Nuovi Paradigmi … forse più correttamente nuovi criteri valutativi per le Valutazioni Tecniche dei Capitolati ICT
- Per i Capitolati a rilevante valore Tecnico-Economico è giusto determinare griglie di valutazione tecnica più oggettive e corrispondenti ai reali skills reperibili sul mercato.
- La norma sembra essere un livellamento verso il basso delle qualifiche tecnico professionali e di mercato (oggi esistono «standard de facto» in termini di certificazioni tecniche rilasciate dai primari Technology Leader a livello WW che troppo spesso vengono ignorati …)
- Nei Medi/Grandi progetti in ambito ICT, le tecnologie «compliant» ai requisiti sono spesso inferiori a 5 oppure vi è già un «lock-in tecnologico» predeterminato.
- La differenza dovrebbe giocarsi nel campo del valore oggettivo dei Partner ICT, ma raramente vengono indicati requisiti distintivi sul personale qualificato e sulle certificazioni aziendali. PROGETTI DI SOLUZIONI ICT SIGNIFICA «APPALTARE LAVORI E NON FORNITURE»!

Estrarre Valore nella assegnazione degli «Appalti di Lavori» (2)

- Va riconosciuto che le griglie valutative sulle «Referenze» Tecniche sono più adeguate, ma pur sempre livellate verso il basso …

- Ispirarsi maggiormente alle Gare del Mercato Privato (Grandi Clienti) DOVE VI E' MAGGIORE CONSAPEVOLEZZA CHE PER «ESTRARRE VALORE DAGLI APPALTI DI LAVORI» E' NECESSARIO UN APPROCCIO PIU' QUANTITATIVO E DETERMINISTICO DELLE PROFESSIONALITA' IN CAMPO

- Le Gare con complessità ed importi rilevanti sui nuovi «Digital Enabler» necessitano e necessiteranno forzatamente di criteri di selezione più «coraggiosi» cioè più restrittivi ed aderenti alle effettive e dimostrabili capacità dei fornitori ICT (Cloud, Cybersecurity, AI, Big Data, Blockchain, IoT …)
- QUALCOSA STA CAMBIANDO … MISE CENTRO DI VALUTAZIONE E CERTIFICAZIONE NAZIONALE – Sole 24 Ore 28 Gennaio

CONSIGLIO NAZIONALE INGEGNERI

C3i COMITATO ITALIANO INGEGNERIA DELL'INFORMAZIONE

Estrarre Valore nella assegnazione degli «Appalti di Lavori» (3)

Il Sole 24 ORE

Data 28-01-2021
Pagina 1
Foglio 2 / 3

Cybersecurity, stretta del Mise sulle forniture Ict

Il regolamento. Pronto il Dpr attuativo della legge sul perimetro di sicurezza nazionale cibernetica, ma serve l'ok definitivo del cdm. Controlli in tre mosse

Spese. A carico delle imprese gli oneri per la valutazione di beni e servizi Previste attività di ispezione a valle della procedura. Altri decreti in arrivo

Marco Ludovico
ROMA

Verifiche in tre mosse contro il rischio cyber nelle forniture agli enti pubblici e sensibili. Si stringe la morsa contro gli attacchi informatici delineata dalla legge sul cosiddetto «perimetro di sicurezza nazionale cibernetica» (l. 18 novembre 2019, n. 133).

Un'architettura di norme complesse con una serie di provvedimenti di attuazione in arrivo. Ora vede il traguardo il Dpr (decreto del presidente della Repubblica) con le regole sulla selezione e i controlli dovuti da chi rientra nel «perimetro» quando sono in ballo «forniture di beni, sistemi e servizi (information and communication tecnology)».

La minaccia di un attacco informatico è dietro l'angolo, sempre più insidiosa. Le barriere da innalzare più urgenti ed estese. Le procedure di difesa, di conseguenza, dettagliate e articolate. Non senza conseguenze, è inevitabile, per le imprese fornitrici: dai costi aggiuntivi ai mancati profitti.

Soggetto strategico di valutazione è il Cvcn, il centro di valutazione e certificazione nazionale insediato presso il Mise. Proprio i tecnici del dicastero dello Sviluppo economico hanno curato il Dpr in arrivo. Un regolamento in 20 articoli, tassello essenziale per la costruzione dei processi di difesa e prevenzione dagli attacchi cyber. Il Dpr è stato calendarizzato per il prossimo preconsiglio dei ministri, una riunione in sede tecnica tra gli uffici legislativi dei dicasteri. Il percorso del regolamento, del resto, è ormai quasi ultimato. Il testo ha recepito le osservazioni del Consiglio di Stato dopo la prima lettura a palazzo Chigi il 7 agosto 2020.

Adesso potrebbe ottenere il sì definito in Cdm. A condizione, però, del riconoscimento nella riunione di governo di far parte degli atti relativi «agli affari correnti» come ha disposto la direttiva emanata dal presidente del Consiglio dimissionario, Giuseppe Conte. Se, dunque, durante le consultazioni per la crisi di governo ci sarà il tempo di fare un altro consiglio dei ministri presieduto da Conte, in assenza di ostacoli politici il Dpr avrà il via libera. I provvedimenti attuativi del perimetro di sicurezza nazionale cibernetica sono ancora diversi, la regia di coordinamento è in capo al Dis, il dipartimento informazioni e sicurezza presso la presidenza del Consiglio.

Il Dpr messo a punto dal Mise, dunque, per garantire la sicurezza informatica delle forniture ai soggetti dentro il «perimetro nazionale di sicurezza cibernetica» definisce le procedure di valutazione svolte dal Cvcn e dai centri di valutazione dei ministeri dell'Interno e della Difesa, dicasteri con una struttura di valutazione propria a parte.

Le fasi di verifica sono tre. Con la prima, il Centro di valutazione analizza «la comunicazione trasmessa dal soggetto incluso nel perimetro e si conclude con l'individuazione di test e condizioni da includere nei bandi di gara o nei contratti» come si legge nella relazione illustrativa. Poi «una volta noto il fornitore e l'oggetto» l'iter prevede «la seconda fase» con «l'attività di preparazione all'esecuzione dei test» e infine la terza fase con «l'esecuzione dei test» vera e propria.

Secondo l'articolo 9 del regolamento gli oneri per la valutazione sono in capo alle imprese: «Le spese a carico del fornitore per le attività di valutazione svolte dal Cvcn e dai Cv sono calcolate sulla base delle disposizioni contenute nel decreto 15 febbraio 2006 del Ministro delle comunicazioni».

L'ultimo blocco normativo disciplina nel dettaglio in sette articoli le attività di verifica e ispezione: è indispensabile, infatti, in caso di forniture di beni e servizi informatici, il controllo della sicurezza delle procedure anche dopo la loro iniziale validazione. In ballo ci sono anche procedimenti specifici se è necessario accedere a strutture e documentazioni con classificazioni di riservatezza: lì il rischio di attacco cyber va scongiurato cento volte di più. La sfida è enorme. Altri provvedimenti sono in arrivo. E per le imprese coinvolte le dinamiche di mercato sono sempre più complicate.

IN CIFRE

13,3 milioni
Le risorse per la realizzazione del Cvcn (Centro di valutazione e certificazione nazionale) istituito presso il Mise e il potenziamento delle tecnologie dell'informazione

77 le assunzioni
Quelle aggiuntive presso il Cvcn spesa massima annua di tre milioni a partire dal 2020. Altre 10 le assunzioni aggiuntive alla presidenza del Consiglio

CONSIGLIO NAZIONALE INGEGNERI

C3i COMITATO ITALIANO INGEGNERIA DELL'INFORMAZIONE

Una Sfida di Sistema

- **Obiettivo: sensibilizzare la PA nella introduzione di criteri più moderni dove si possa estrarre valore da un mix ponderato di certificazioni in svariati ambiti dell'ecosistema ICT. Cosa prevedere?**
  - ordini professionali, SOA/OS dedicate all' ICT, ISO/ITIL, certificazioni professionali e aziendali dei technology leader, referenze richieste in linea con le dimensioni e complessità tecniche dell'appalto da assegnare)
- **Da un modello di Filtro «passa basso» ad un modello di filtro «passa alto»: per continuità di metafora oggi la «frequenza di taglio» deve essere oggettivamente innalzata per poter «Estrarre il Valore dagli Appalti di Lavori»:**
  - i Progetti della PA con questi nuovi criteri garantirebbero alla comunità di dotarsi effettivamente di **INFRASTRUTTURE MODERNE, INTEROPERABILI e soprattutto SICURE …**
- **Come Raccogliere la sfida?**
  - **Fare Sistema! Anzi Ecosistema ed individuare «ambasciatori» che possano sensibilizzare il mondo PAC/PAL. Senza un «game changing» difficilmente avremo un PA i cui servizi al cittadino potranno passare nella «TOP 10» Europea.**