LE NOVITÀ

La cyber security entra nel Codice Appalti: perché è un cambio di passo fondamentale

Dar vita ad una norma in grado di tutelare i soggetti, pubblici e privati, sempre più esposti a minacce cibernetiche: è questa la ratio dietro all'attenzione posta alla cyber security nel nuovo Codice Appalti. Le novità e perché si tratta di un importante "cambio di mentalità", anche per le aziende

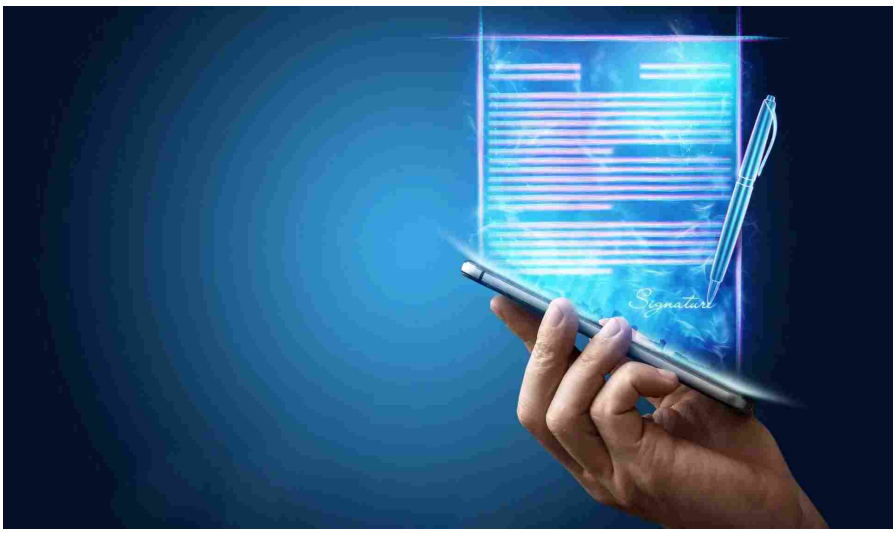
Pubblicato il 28 Apr 2023

Luisa Franchina

Presidente Associazione Italiana esperti in Infrastrutture Critiche

Tommaso Ruocco

Junior Analyst Hermes Bay



Tra le principali formulazioni presenti all'interno del "Codice degli Appalti" (D.lgs. 36/2023 pubblicato in Gazzetta Ufficiale in data 31 marzo 2023) figura anche la cybersicurezza, inserita per la prima volta nel testo del Codice degli Appalti. La disposizione concernente le misure di sicurezza informatica è stata introdotta all'articolo 108, *Criteri di aggiudicazione degli appalti di lavori, servizi e forniture*, comma 4. Questa prevede che le stazioni appaltanti tengano sempre in considerazione gli elementi di cybersicurezza nell'approvvigionamento di beni e servizi informatici, in particolare quando l'impiego dei suddetti beni e servizi risulti essere connesso alla tutela degli interessi nazionali strategici.

Nuovo Codice appalti, niente paura: subappalto, RUP e semplificazioni, tutto ciò che bisogna sapere

28 Marzo 2023

di Francesco Porzio

La riforma non riguarda solamente la Pubblica Amministrazione, come riportato inizialmente nel testo approvato dal Consiglio dei ministri, bensì risulterebbe vigente per tutti quei soggetti che sono tenuti al rispetto del nuovo codice. La *ratio* è perciò stata quella di dar vita ad una norma che fosse in grado di tutelare i soggetti, pubblici e privati, sempre più esposti a minacce cibernetiche.

Indice degli argomenti

Gli investimenti in digitale e la cybersecurity nel nuovo codice appalti

Gli investimenti nel digitale, che risultano essere un elemento cardine all'interno del nuovo testo del Codice degli appalti, richiedono infatti un'elevata attenzione sul piano cibernetico, maggiormente esposto a vulnerabilità di vario genere. In conseguenza di ciò, si è rivelato necessario agire per rafforzare le componenti cyber degli strumenti acquistati e impiegati da Pubbliche Amministrazioni, concessionari di opere pubbliche, società partecipate e centrali di committenza.

Il nuovo testo del Codice degli Appalti rappresenta quindi un importante elemento per far fronte alle più recenti esigenze di sicurezza cibernetica nazionale. Sul tema si è già espresso il Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale, Bruno Frattasi, in un'intervista al Corriere della Sera tenuta lo scorso 5 aprile. Il nuovo Direttore di ACN ha sottolineato l'importanza di tale riforma, in relazione agli sforzi posti in essere per raggiungere gli obiettivi perseguiti dalla Strategia nazionale di cybersecurity entro il 2026 e, come detto in precedenza, in ottemperanza alle misure di attuazione del Piano nazionale di ripresa e resilienza. Secondo quanto dichiarato da Frattasi, in questo scenario "serve un ecosistema con standard condivisi, aumentando la capacità di innovazione tecnologica del Paese con programmi di investimento che l'Agenzia sta portando avanti con risorse nazionali e con i fondi del PNRR".

Articoli correlati

REGIONE PUGLIA
PROGRAMMAZIONE E INVESTIMENTI
Agenda PugliaDigitale2030: così territorio e imprese partecipano alla trasformazione digitale
08 Mar 2023
di Vito Bavaro


L'INTERVENTO
Assocontact: "Vicini alla svolta contro il telemarketing selvaggio. Ecco cosa serve ora"
11 Apr 2023
di Lelio Borgherese

LE PROPOSTE
Assintel: "Innovare la PA con l'aiuto delle piccole imprese digitali: ecco un approccio win-win"
28 Apr 2023
di Danilo Cattaneo

Cosa cambia per le stazioni appaltanti

Da quanto riportato all'articolo 108 comma 4 è possibile, quindi, evincere la volontà del Governo in carica di attribuire un peso maggiore agli aspetti concernenti la cybersicurezza di prodotti e servizi acquistati, prediligendo una valutazione tecnico-qualitativa degli stessi, basata su aspetti "qualitativi, ambientali o sociali, connessi all'oggetto dell'appalto". La stazione appaltante è, infatti, tenuta alla valorizzazione di tali aspetti, per individuare il miglior rapporto qualità/prezzo e garantire "un confronto concorrenziale effettivo sui profili tecnici", compresi gli "elementi di cybersicurezza", ponendo sempre particolare attenzione nei casi in cui l'impiego dei beni o degli strumenti sia connesso alla tutela degli interessi nazionali strategici. In questi casi, il legislatore ha stabilito che la stazione appaltante debba decretare un tetto massimo per il punteggio economico entro il limite del 10 per cento. Per i contratti ad alta intensità di manodopera, invece, questa dovrà stabilire un tetto massimo per il punteggio economico entro il limite del 30 per cento. Tale discrezionalità, concessa alle stazioni appaltanti, si ritiene possa rappresentare un vantaggio, in quanto il prezzo risulterebbe meno determinante a fronte di altri fattori correlati alla sicurezza cibernetica e digitale.
Oltre al commento positivo del nuovo direttore dell'Agenzia, la quale aveva a più riprese sottolineato l'importanza di tale riforma relativamente al panorama della cybersecurity, diversi enti e istituzioni hanno espresso soddisfazione per l'inserimento di un preciso riferimento alla cybersicurezza all'interno del Codice. Anche il Consiglio Nazionale Ingegneri (CNI), dopo aver evidenziato alcune perplessità sul Decreto in questione, ha espresso soddisfazione per lo spazio riservato al tema della sicurezza informatica.

Conclusioni

Per concludere, le novità introdotte dal Decreto Legislativo 36/2023 costituiscono quindi un "cambio di mentalità", fondamentale anche per le aziende che, ad oggi, risultano essere quotidianamente sottoposte a minacce cyber. I numerosi fenomeni cibernetici, che colpiscono su ampia scala le aziende e i loro clienti, rendono la strategia di protezione informatica di un'azienda un fattore sempre più rilevante e in grando di qualificare positivamente la stessa nel mercato.
Nonostante i risultati concreti già raggiunti nel nostro Paese in tema di cybersecurity, soprattutto a fronte di un panorama geopolitico sempre più caratterizzato da interconnessioni digitali, l'attenzione in materia dovrà rimanere massima, in quanto esigenza fondamentale dell'intero Sistema-Paese.

Valuta la qualità di questo articolo

☹ ☹ ☺ ☺