

Cybersecurity per la Pa, Consip attiva il nuovo contratto da 468 milioni di euro

Consip ha attivato un nuovo contratto da 468 milioni di euro per i Servizi di sicurezza da remoto, che amplia l'offerta nel settore ICT e in particolare nei servizi di cybersecurity.

L'offerta Consip dei servizi di cybersecurity alla Pubblica amministrazione italiana si arricchisce con un nuovo "contratto pronto all'uso" per servizi di sicurezza, in coerenza con le indicazioni del **Piano Triennale dell'informatica nella Pa**, anche per la realizzazione dei progetti PNRR, che afferiscono principalmente ma non solo alla Missione 1 (Digitalizzazione, Innovazione, Competitività, Cultura) – Componente 1 (Digitalizzazione, innovazione e sicurezza nella Pa).

Dopo il Lotto 2 *"Servizi di compliance e controllo"*, è stato attivato il Lotto 1 dell'Accordo quadro *"Servizi di sicurezza da remoto"* – con un valore totale di 468 milioni di euro – che mette a disposizione un insieme articolato di servizi di sicurezza erogati "da remoto" (presso il fornitore) per la protezione di infrastrutture, applicazioni e dati.

L'Accordo quadro è della modalità "multifornitore" a condizioni tutte fissate dai seguenti aggiudicatari:

- **Rti Accenture S.p.A**
- **Fincantieri Nextech S.p.A**
- **Fastweb S.p.A**

- **Deas Difesa e Analisi Sistemi S.p.A.** (Amministrazioni locali)
- **Rti Telecom Italia S.p.A**
- **Net Group S.p.A., Reevo S.p.A., Kpmg Advisory S.p.A., Al maviva -The Italian Innovation Company S.p.A.** (Amministrazioni centrali)

Questi i servizi messi a disposizione:

- **Security Operation Center:** centro di erogazione di servizi mirati a garantire la corretta operatività dei sistemi attraverso la prevenzione, gestione, risoluzione di criticità di sicurezza
- **Next Generation Firewall:** filtraggio del traffico di rete interno ed esterno, limitando o bloccando eventi quali accessi non autorizzati, malware o servizi non consentiti
- **Web Application Firewall:** monitoraggio e blocco del traffico da e verso un servizio Web, proteggendo le PA dagli attacchi incorporati nei dati trasmessi dalle applicazioni web
- **Gestione continua delle vulnerabilità di sicurezza:** quadro del livello e gravità del rischio a cui sono esposti i sistemi informatici tramite un processo automatico di assessment delle vulnerabilità
- **Threat Intelligence & Vulnerability Data Feed:** flusso continuo di dati relativi a minacce e vulnerabilità di sicurezza del Sistema informativo
- **Protezione navigazione Internet e Posta elettronica:** sistema di filtraggio in tempo reale del traffico internet, compreso e-mail, con contenuti dannoso
- **Protezione degli end-point:** protezione dei dispositivi collegati alla rete aziendale (ad es. pc desktop, laptop, smartphone, tablet) da accessi non autorizzati o dall'esecuzione di software dannoso
- **Certificati SSL:** certificati (Secure Sockets Layer e Transport Layer Security) per garantire affidabilità e

sicurezza della comunicazione tra le componenti client e server di un'applicazione internet

- **Servizio di Formazione e Security Awareness del personale:** sviluppo di competenze essenziali, tecniche e metodi fondamentali per la prevenzione degli incidenti di sicurezza
- **Gestione dell'identità e l'accesso utente:** gestione delle attività di identificazione, autenticazione e autorizzazione propedeutiche all'accesso a servizi erogati in rete
- **Firma digitale remota e Sigillo elettronico:** garanzia di efficacia probatoria dei documenti informatici firmati digitalmente, favorendo la dematerializzazione e l'ottimizzazione dei processi aziendali
- **Timbro elettronico:** creazione di documenti informatici che possano conservare la medesima validità legale anche dopo essere stati stampati su supporto cartaceo
- **Validazione temporale elettronica qualificata:** associazione di data e ora, certe e legalmente valide, a un documento informatico, per una validazione temporale del documento opponibile a terzi.
- **Servizi specialistici:** supporto tecnico connesso all'attivazione dei servizi da remoto oggetto di fornitura.

Cristiano Cannarsa, ad Consip: “La cybersecurity tema centrale per la PA”

Il nuovo contratto va ad affiancarsi al Lotto 2 “Servizi di compliance e controllo” e a quello già attivo da marzo inerente i servizi di sicurezza “on premise” (cioè presso il cliente), per la protezione dei dati e delle applicazioni in uso alle PA, attraverso i quali le amministrazioni possono acquisire prodotti per la gestione degli eventi di sicurezza e

degli accessi, per la protezione dei canali email, web e dati.

Cristiano Cannarsa, ad Consip, aveva commentato: *“La gara per prodotti e servizi nell’ambito della cybersecurity, un tema molto importante sul quale il governo con la creazione dell’**Agenzia per la cybersicurezza nazionale** guidata da **Roberto Baldoni**, ha voluto dare particolare risalto alla sicurezza in ambito digitale in quanto aumentando il numero di servizi messi a disposizione di cittadini e imprese aumenta l’esposizione al rischio che servizi e infrastrutture possano essere oggetto di attacchi hacker. Abbiamo notevolmente aumentato il gradimento degli strumenti e dei contratti di Consip da parte delle Pubblica amministrazione”* spiega Cannarsa *“tanto che abbiamo focalizzato quattro elementi nel riposizionare Consip nell’ambito della Pa: è più utilizzata, è più efficiente perché abbiamo più che raddoppiato il valore delle gare aggiudicate (nel 2021 un valore di 11 mld euro mentre nel 2016 il valore è stato di 5,5 mld) aumentando tutti i parametri di efficienza produttiva ovvero di gare e volumi aggiudicati pro capite per i nostri dipendenti: oggi abbiamo meno dipendenti, nel 2016 erano 439 e oggi siamo 422”*.

<https://www.key4biz.it/cybersecurity-per-la-pa-consip-attiva-il-nuovo-contratto-da-468-milioni-di-euro/417498/>