

Ministero della Giustizia

Dipartimento per l’innovazione tecnologica della giustizia

Direzione Generale per i Sistemi Informativi Automatizzati

**Rapporto Avanzamento Contrattuale (RAC)**

*Adesione Accordo Quadro per l’affidamento di Servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni - lotto 1 - CIG: 99026071D0*

**Sommario**

[1. Scheda di sintesi dei dati identificativi 3](#_Toc177383665)

[2. Executive Summary 5](#_Toc177383666)

[**2.1** **Descrizione Sommaria dell’iniziativa contrattuale** 5](#_Toc177383667)

[3. Obiettivi Contrattuali 5](#_Toc177383668)

[4. Esecuzione del contratto 6](#_Toc177383669)

[**4.1** **Stato di avanzamento - SAL e SAC** 6](#_Toc177383670)

[**4.2** **Indicatori di monitoraggio e livelli di servizio** 6](#_Toc177383671)

[**4.3** **Eventuali innovazioni tecnologiche** 8](#_Toc177383672)

[**4.4** **Aspetti della eventuale non conformità** 8](#_Toc177383673)

[**4.5** **Indicazioni per la Governance** 9](#_Toc177383674)

# Scheda di sintesi dei dati identificativi

|  |  |
| --- | --- |
| Denominazione dell’Amministrazione | Ministero della Giustizia – Dipartimento per l’innovazione tecnologica della giustizia - Direzione Generale per i Sistemi Informativi Automatizzati (DGSIA) |
| Denominazione del contratto | Adesione Accordo Quadro per l’affidamento di Servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni - lotto 1 |
| CIG - Codice Identificativo di Gara | 99026071D0 |
| Codice e oggetto e data del parere di riferimento AGID (se presente) | - |
| Importo netto (previsto originariamente ed eventuali variazioni successive) | Importo Originario: 19.428.754,76 € (esclusa IVA)  (Parte dell’importo economico per il triennio 2023 -2026 è stato disimpegnato. Nello specifico, il disimpegno è pari a 3.869.137,37 €)  Importo complessivo: 15.559.617,39 € (esclusa IVA)  Variante in aumento pari a 445.000,00 € in data 07/11/2024 (esclusa IVA) |
| Importo lordo (previsto originariamente ed eventuali variazioni successive) | 19.525.633,10 € |
| Denominazione del Fornitore | Telecom Italia S.p.A. |
| Eventuali altri contratti collegati (quinto  d’obbligo, atti aggiuntivi) | - |
| RUP – Responsabile Unico del  Procedimento | Enrico Maresca |
| DEC – Direttore dell’Esecuzione | Fulvio Nicolò Giannone |
| Numero progressivo del rapporto | 1 |
| Numero progressivo della versione con evidenza delle variazioni intervenute (eventuale, in caso di riemissione) | 1 |
| Periodo di riferimento esaminato | 05/03/2024 – 15/09/2025 |
| Il Responsabile del monitoraggio dell’Amministrazione | Ing. Ettore Sala |
| Referente di monitoraggio dell’Amministrazione (nome e cognome, recapito telefonico e di posta elettronica) | Dott. Luigi Pagnotta |
| Data di emissione del rapporto | 15/09/2025 |
| Lista di distribuzione (organizzazione e nominativo) | - |
| Breve descrizione del contratto | Servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni |
| Data stipula | 29/06/2023 |
| Data inizio - Data fine attività | 26/11/2023 - 26/11/2026 |

# Executive Summary

### **Descrizione Sommaria dell’iniziativa contrattuale**

*Con l’adesione all’Accordo Quadro, l’Amministrazione intende usufruire dei seguenti servizi:*

* *L1.S1 - Security Operation Center - SOC*
* *L1.S4 - Gestione continua delle vulnerabilità di sicurezza*
* *L1.S7 - Protezione degli end-point – EPP – portali e siti web*
* *L1.S7 - Protezione degli end-point – EPP – postazioni di lavoro*
* *L1.S9 - Servizio di Formazione e Security awareness*
* *L1.S15 - Servizi specialistici*

*Il valore complessivo massimo del contratto è 16.004.617,30 € IVA esclusa.*

*Al 05 Marzo 2025 risultano liquidati dal precedente monitoraggio ulteriori 440.340,19 € IVA inclusa.*

# Obiettivi Contrattuali

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Servizio | Descrizione | Valore economico  (Iva Esclusa) | Incidenza (%) | Stato |
| Sicurezza informatica | Security Operation Center (SOC) | 6.000.539,76 € | 30,88% | In linea |
| Sicurezza informatica | Gestione continua delle vulnerabilità di sicurezza | 79.920,00 € | 0,41% | Chiuso |
| Sicurezza informatica | Protezione degli end-point – postazioni lavoro | 5.015.843,28 € | 25,82% | In linea |
| Sicurezza informatica | Protezione degli end-point (Portali) | 324.918,72 € | 1,67% | Chiuso |
| Sicurezza informatica | Servizio di Formazione e Security awareness | 982.443,00 € | 5,06% | In linea |
| Sicurezza informatica | Servizi specialistici | 138.650,00 € | 0,71% | Chiuso |
| Sicurezza informatica | Servizi specialistici | 411.250,00 € | 2,12% | chiuso |
| Sicurezza informatica | Servizi specialistici | 89.535,00 € | 0,46% | chiuso |
| Sicurezza informatica | Servizi specialistici (Portal) | 2.602.124,63 € | 28,20% | In linea\* |
| Sicurezza informatica | Servizi specialistici | 906.160,00 € | 4,66% | In linea |

* Parte dell’importo economico è stato disimpegnato

# Esecuzione del contratto

### **Stato di avanzamento - SAL e SAC**

*Avanzamento intervento:*

* *Realizzazione di un’architettura DHCP-IPAM con gestone centralizzata :30%*
* *Componente funzionale PAM: 40%*
* *Componente funzionale EDR: 100%*
* *Gestione Servizi di Sicurezza per i Portali in Cloud: 80%*
* *Sensibilizzazione, in tema di cybersicurezza, dei Magistrati e del personale amministrativo: 45%*

*Facendo riferimento al periodo di monitoraggio, l’Amministrazione ha emesso certificati di pagamento per un importo complessivo di 10.184.564,30 € IVA inclusa così ripartita:*



### **Indicatori di monitoraggio e livelli di servizio**

*L’attività di monitoraggio svolta durante l’esecuzione del contratto nel 2024-2025 si è basata sul calcolo del rispetto dei valori attesi per ciascun indicatore (riportati nella tabella che segue). Pertanto, si osserva il rispetto totale dei valori attesi per ciascun indicatore contrattuale.*

*Di seguito vengono riportati i principali KPI che sono stati monitorati durante il corso del 2024 e del 2025:*

|  |  |
| --- | --- |
| **Servizio Monitorato** | **Descrizione Indicatore** |
| *Realizzazione di un’architettura DHCP-IPAM con gestone centralizzata* | * *Raccolta dati AS-IS* * *Installazione e configurazione dell’infrastruttura Configurazione e caricamento dei dati nei server DHCP* * *On boarding delle configurazioni di rete delle varie articolazioni ministeriali nella nuova soluzione* |
| *Componente funzionale PAM* | * *Verifica dello stato attuale della gestione delle utenze privilegia-te e del monitoraggio degli accessi alle risor-se informatiche* * *Disegno ed implementazione dell’architettura che permetta la gestione accessi per utenti con elevati privilegi e integrazione con elementi infrastrutturali* * *On boarding del parco applicativo di Giustizia nella nuova soluzione PAM* |
| *Componente funzionale EDR* | * *Raccolta di tutte le informazioni necessarie al fine di definire il perimetro di intervento* * *Integrazione massiva dell’agent EDR nelle risorse informatiche di tipo Postazioni di Lavoro e delle risorse informatiche di tipo server* |
| *Gestione Servizi di Sicurezza per i Portali in Cloud* | * *Migrazione dei portali Giustizia verso il tenant AWS* * *Attivazione dei presidi di sicurezza del cloud* * *Abilitazione servizio di VPN client to site* * *Abilitazione della Multi factor authentication* * *Installazione e Configurazione Server FW Inspection* * *Supporto alla gestione degli incidenti* |
| *Sensibilizzazione, in tema di cybersicurezza, dei Magistrati e del personale amministrativo* | * *Identificazione dei Re-quisiti utente in termini di esigenze di forma-zione ed awareness* * *Acquisizione e predi-sposizione della piat-taforma formazione ed awareness selezionata* * *Definizione del processo e della procedura di gestione delle attività di formazione* |

*Per ulteriori informazioni è possibile consultare l’excel in allegato:*



### **Eventuali innovazioni tecnologiche**

*Codesta Amministrazione ha provveduto a installare presso le quattro sale server nazionali le seguenti soluzioni software:*

* *DHCP-IPAM: consente la configurazione, aggiunta, modifica di un indirizzo ip a una specifica risorsa, il monitoraggio dello stato operativo, di patching, di troubleshooting e di profilatura utenti;*
* *PAM: consente di controllare, monitorare e rendere sicure tutte le identità digitali privilegiate (umane e non) e le loro attività nell’ambiente IT dell’organizzazione, garantendo l’evoluzione della gestione degli account privilegiati mediante la conservazione e gestione delle credenziali da loro usate in casseforti digitali;*
* *EDR: L’Endpoint Detection and Response è una categoria di soluzioni di sicurezza informatica progettate per individuare, indagare e rispondere a minacce avanzate che possono eludere le tradizionali misure di sicurezza di rete. Codesta Amministrazione ha adottato come soluzione EDR quella proposta da TrendMicro e sta provvedendo a installarla su tutte le postazioni di lavoro e sui server a disposizione del personale Giustizia*

*Per completezza di rappresentazione, si fa presente che Codesta Amministrazione ha provveduto ad attivare su tutti i portali Giustizia in esecuzione sul tenant AWS il servizio di protezione del traffico HTTP/HTTPS fornita dal vendor Fortinet..*

### **Aspetti della eventuale non conformità**

*Non si sono riscontrate al momento eventuali non conformità legate alle attività del progetto in oggetto*

### **Indicazioni per la Governance**

N/A