

Ministero della Giustizia

Dipartimento per l’innovazione tecnologica della giustizia

Direzione Generale per i Sistemi Informativi Automatizzati

**PIANO DI MONITORAGGIO  
CONTRATTO**

*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 DATI IDENTIFICATIVI DEL CONTRATTO 3](#_Toc177383675)

[2 INTRODUZIONE 4](#_Toc177383676)

[2.1 BREVE DESCRIZIONE DEL CONTRATTO E DEGLI EVENTUALI ATTI COLLEGATI 4](#_Toc177383677)

[2.2 BREVE DESCRIZIONE DEI SERVIZI CONTRATTUALI 4](#_Toc177383678)

[**2.2.1** **Servizi di Sicurezza Informatica** 4](#_Toc177383679)

[2.3 BREVE DESCRIZIONE DEI PRODOTTI/SERVIZI REALIZZATI E COLLAUDATI 5](#_Toc177383680)

[2.4 BREVE DESCRIZIONE ATTIVITÀ DI MONITORAGGIO SVOLTE 5](#_Toc177383681)

[3 SINTESI PER L’ALTA DIREZIONE 6](#_Toc177383682)

[4 METODOLOGIA DI ANALISI 6](#_Toc177383683)

[5 STORIA DEL CONTRATTO 7](#_Toc177383684)

[6 RISULTATI OTTENUTI 7](#_Toc177383685)

[7 LEZIONI APPRESE ED INIZIATIVE FUTURE 7](#_Toc177383686)

# DATI IDENTIFICATIVI DEL CONTRATTO

|  |  |
| --- | --- |
| Denominazione dell’Amministrazione | Ministero della Giustizia - Dipartimento per l’innovazione tecnologica della giustizia - Direzione Generale per i Sistemi Informativi Automatizzati (DGSIA) |
| Codice parere |  |
| 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 |
| Codice contratto (CIG, REP, ovvero  codice interno) | 99026071D0 |
| RUP – Responsabile Unico del  Procedimento | Enzo Maresca |
| DEC – Direttore dell’Esecuzione | Fulvio Nicolò Giannone |
| Denominazione del Fornitore | Telecom Italia S.p.A. |
| Data stipula | 29/06/2023 |
| Data inizio – data fine attività | 26/11/2023 - 26/11/2026 |
| Importo complessivo | 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) |
| Eventuali altri contratti collegati (quinto  d’obbligo, atti aggiuntivi) | - |
| Importo complessivo contratti collegati | - |
| Importo complessivo contratto base più  contratti collegati | 15.559.617,39 € (esclusa IVA) |
| Eventuali proroghe collegate | - |
| Data stipula proroghe | - |
| Data inizio – data fine proroghe | - |
| Importo complessivo proroghe | - |
| Importo totale contratti e proroghe | 15.559.617,39 € (esclusa IVA) |

# INTRODUZIONE

## BREVE DESCRIZIONE DEL CONTRATTO E DEGLI EVENTUALI ATTI COLLEGATI

*Con l’adesione all’Accordo Quadro, l’amministrazione intende dotarsi di servizi mirati a garantire la corretta operatività dei sistemi.*

*Le finalità principali dell’adesione all’accordo quadro sono:*

* *La gestione e monitoraggio dei servizi di sicurezza oggetto di fornitura e, in aggiunta, ricevere ed analizzare la reportistica e i log dando giusta priorità ai processi di risoluzione e/o mitigazione delle minacce.*
* *La gestione continua delle vulnerabilità di sicurezza tramite un processo automatico di assessment delle vulnerabilità*
* *La protezione degli endpoint e di conseguenza la protezione dei dispositivi collegati alla rete aziendale (es. Pc desktop, Laptop, Smartphone, Tablet)*
* *La sensibilizzazione del personale amministrativo, su svariati aspetti riguardanti la sicurezza delle informazioni, attraverso sessioni di formazione.*
* *Il supporto tecnico specialistico connesso all’attivazione di svariati servizi da remoto previsti dall’accordo (es. migrazione servizi di sicurezza dell’amministrazione, definizione/ configurazione/ erogazione del servizio di monitoraggio continuo delle vulnerabilità)*

## BREVE DESCRIZIONE DEI SERVIZI CONTRATTUALI

*Di seguito si riporta una descrizione sintetica dei servizi sopraelencati, previsti contrattualmente, ed il loro rispettivo valore economico.*

### **Servizi di Sicurezza Informatica**

*I servizi di sicurezza informatica si articolano in:*

* *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 economico contrattuale associato a questa attività/servizio è* 15.559.617,39 *euro IVA esclusa.*

## BREVE DESCRIZIONE DEI PRODOTTI/SERVIZI REALIZZATI E COLLAUDATI

*l’Amministrazione ha provveduto a definire procedure e processi per il governo della Sicurezza delle informazioni e a fornire una modellazione dell’Amministrazione in classi di contesto, quali Ufficio Centrale, Ufficio Giudiziario e Sala Server, in cui le principali entità e unità organizzative del Ministero di Giustizia e dell’Autorità Giudiziaria sono state classificate. Per ogni classe sono stati individuati i livelli di sicurezza informatica definiti critico, basso, medio e alto. Un livello di sicurezza corrisponde a un elenco di misure di sicurezza informatica che un’entità o un’unità deve attuare per ridurre il rischio di esposizione a determinate minacce cyber.*

*Nello specifico, si è 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*
* *FortiWeb: servizio di protezione del traffico HTTP/HTTPS fornita dal vendor fortinet e attivata su tutti i portali Giustizia in esecuzione sul tenant AWS.*

## BREVE DESCRIZIONE ATTIVITÀ DI MONITORAGGIO SVOLTE

*L’amministrazione svolge attività di monitoraggio dell’intero servizio di fornitura, oltre ad occuparsi della gestione operativa, delle anomalie e problematiche che possono sorgere ponendosi come obiettivo la verifica della completezza e della qualità della documentazione fornita.*

*Le attività di monitoraggio svolte sono di seguito riportate:*

* *Verifica con i fornitori, tramite SAL settimanali, dello stato di avanzamento delle attività svolte.*
* *Revisione dei Piani di Lavoro prodotti dall’RTI.*
* *Richiesta di documenti a supporto delle verifiche rispetto alle attività che sono oggetto di monitoraggio al fine di prevenire criticità dovute a date di consegna non rispettate. Tutta la documentazione rilasciata dai fornitori è stata protocollato e memorizzato nel sistema di archiviazione informatico usato da codesta Amministrazione*
* *Richiesta documentazione per fasi di collaudo con indicazioni sul numero di test effettuati e il numero di test positivi e/o negativi.*
* *Verifica dello stato delle risorse allocate tramite richiesta periodica di documentazione atta a fornire lo staffing rispetto ai requisiti richiesti sulle attività progettuali.*
* *Richiesta di documentazione atta a fornire indicazioni sul turnover del personale da parte del fornitore.*

# SINTESI PER L’ALTA DIREZIONE

*Questa informazione sarà condivisa nella prima nota utile dopo la conclusione del contratto.*

# METODOLOGIA DI ANALISI

*I principali indicatori utilizzati per il monitoraggio e l’analisi dell’andamento del contratto sono riportati seguito.*

|  |  |
| --- | --- |
| ***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 dettagli fare riferimento alla tabella allegata.*

****

# STORIA DEL CONTRATTO

*Questa informazione sarà condivisa nella prima nota utile dopo la conclusione del contratto.*

# RISULTATI OTTENUTI

*Queste informazioni saranno condivise nella prima nota utile dopo la conclusione contratto.*

# LEZIONI APPRESE ED INIZIATIVE FUTURE

*Le evidenze saranno inviate nella prima nota utile dopo la conclusione contratto.*