

Identificativo: AOOMTO_Piano Operativo v01

Data: 29/01/2024

**ACCORDO QUADRO PER L’AFFIDAMENTO DI SERVIZI DI
SICUREZZA DA REMOTO, DI COMPLIANCE E
CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI**

**LOTTO 2 – SERVIZI DI COMPLIANCE E CONTROLLO
PUBBLICHE AMMINISTRAZIONI LOCALI**

Piano Operativo



**A.O. Ordine
Mauriziano
di Torino**

Costituito

Raggruppamento Temporaneo di Imprese

composto da:

Deloitte Risk Advisory S.r.l.

EY Advisory S.p.A.

Teleco S.r.l.

ASOOM_TO_Azienda Ospedaliera Ordine Mauriziano di Torino - Rep. DG 01/02/2024.0000092.I



Deloitte.

EY

teleco

CONTENUTI

1	Introduzione	3
1.1	Ambito.....	3
1.2	Richieste dell'Amministrazione contraente	3
1.3	Riferimenti.....	3
1.4	Acronimi e glossario.....	4
2	Anagrafica dell'amministrazione	5
3	Categorizzazione dell'intervento	6
3.1	Categorizzazione di I livello	6
3.2	Categorizzazione di II livello	7
4	Servizi richiesti e ambito di intervento.....	8
4.1	Ambiti di intervento	8
4.2	Servizi richiesti	8
4.3	Dettaglio dei servizi richiesti.....	9
4.3.1	L2.S16 - Security Strategy.....	9
4.4	Indici di digitalizzazione.....	10
4.4.1	Indicatori di digitalizzazione	10
4.4.2	Indicatori generali di digitalizzazione.....	10
4.4.3	Indicatori di progresso	11
5	Organizzazione e modalità di erogazione del contratto esecutivo.....	12
5.1	Attività in carico alle aziende del RTI	12
5.2	Modalità di ricorso al subappalto da parte del fornitore	12
5.3	Organizzazione e figure di riferimento del fornitore	12
5.4	Modalità di esecuzione dei servizi	12
6	Piano di lavoro	13
6.1	Piano di Presa in carico	13
6.2	Cronoprogramma.....	13
6.3	Data di attivazione e durata del servizio	13
7	Piano della qualità specifico	14
7.1	Organizzazione dei Servizi	14
	<i>Security Strategy (L2.S16)</i>	14
7.2	Metodologie e Tecniche	15
	<i>Security Strategy (L2.S16)</i>	15



1 INTRODUZIONE

1.1 Ambito

Nel Settembre 2021 CONSIP ha bandito una procedura aperta, suddivisa in due lotti, per “l’affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni – ID 2296”. Il Lotto 2, inerente ai servizi di compliance e controllo, è stato assegnato come primo aggiudicatario al Raggruppamento Temporaneo di Imprese (RTI), la cui mandataria è Deloitte Risk Advisory S.r.l. e le società mandanti sono EY Advisory S.p.A. e Teleco S.r.l., per la stipula di contratti esecutivi con le Pubbliche Amministrazioni Locali (PAL).

La durata dell’Accordo Quadro è di 24 mesi, decorrenti dalla data di attivazione. Per durata dell’Accordo Quadro si intende il periodo entro il quale le Amministrazioni potranno affidare, a seguito della approvazione del Piano Operativo, contratti esecutivi agli operatori economici aggiudicatari parti dell’Accordo Quadro per l’approvvigionamento dei servizi oggetto dell’Accordo Quadro. Ciascun Contratto esecutivo avrà una durata massima di 48 mesi decorrenti dalla relativa data di conclusione delle attività di presa in carico.

Il presente documento costituisce il “Piano Operativo” (o “Ordinativo di fornitura”), nel quale l’RTI intende formulare la proposta tecnico/economica secondo le modalità tecniche ed i listini previsti nell’Accordo Quadro.

1.2 Richieste dell’Amministrazione contraente

Nell’ambito dell’Accordo Quadro per l’affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni (Sigef 2296, Lotto2), A.O. Ordine Mauriziano di Torino intende acquisire la fornitura di alcuni servizi da Deloitte per attuare interventi volti ad innalzare il livello di maturità dell’Amministrazione in ambito cyber. L’ambito di riferimento dei servizi sarà:

- **L2.S16 – Servizio di Security Strategy**, composto dalle seguenti attività:
 - Supporto nella valutazione e attuazione della compliance alla normativa NIS1/2
 - Supporto nell’implementazione di attività di rimedio volte al potenziamento del livello di sicurezza

1.3 Riferimenti

IDENTIFICATIVO	TITOLO/DESCRIZIONE
ID 2296 - Gara Sicurezza da remoto - Allegato 1 - Capitolato Tecnico Generale	Capitolato Tecnico Generale della GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L’AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI
ID 2296 - Gara Sicurezza da remoto - Allegato 2B - Capitolato Tecnico Speciale Lotto 2	Capitolato Tecnico Speciale della GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L’AFFIDAMENTO DI SERVIZI DI SICUREZZA DA

	REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI
ID 2296 - Gara Sicurezza da remoto - Capitolato Oneri	Capitolato d'Oneri della GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L’AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI
ID 2296 - Gara Sicurezza da remoto - Bando GURI	Bando GURI della GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L’AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI

1.4 Acronimi e glossario

DEFINIZIONE/ACRONNIMO	DESCRIZIONE
RTI	Raggruppamento Temporaneo di Impresa
AQ	Accordo Quadro
CE	Contratto Esecutivo
PAL	Pubblica Amministrazione Locale



2 Anagrafica dell'amministrazione



DATI ANAGRAFICI DELL'AMMINISTRAZIONE

Ragione sociale Amministrazione	Azienda Ospedaliera Ordine Mauriziano di Torino
Indirizzo	Via Magellano, 1
CAP	10128
Comune	Torino
Provincia	TO
Regione	Piemonte
Codice Fiscale	09059340019
Indirizzo mail	ssi@mauriziano.it
PEC	ssi.mauriziano@pcert.postecert.it
Codice PA	asoom_to
Comparto di Appartenenza (PAL/PAC)	PAL



DATI ANAGRAFICI REFERENTE DELL'AMMINISTRAZIONE

Nome	Stefano
Cognome	Geninatti Togli
Telefono	011 5082792
Indirizzo mail	senginatti@mauriziano.it
PEC	ssi.mauriziano@pcert.postecert.it



3 CATEGORIZZAZIONE DELL'INTERVENTO

3.1 Categorizzazione di I livello

AMBITO I LIVELLO (LAYER)	OBIETTIVI PIANO TRIENNALE
SERVIZI	Servizi al cittadino
	Servizi a imprese e professionisti
	Servizi interni alla propria PA
	Servizi verso altre PA
DATI	Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese
	Aumentare la qualità dei dati e dei metadati
	Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati
PIATTAFORME	Favorire l'evoluzione delle piattaforme esistenti per migliorare i servizi offerti a cittadini ed imprese semplificando l'azione amministrativa
	Aumentare il grado di adozione ed utilizzo delle piattaforme abilitanti esistenti da parte delle PA
	Incrementare e razionalizzare il numero di piattaforme per le amministrazioni al fine di semplificare i servizi ai cittadini
	Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni locali favorendone l'aggregazione e la migrazione sul territorio (Riduzione Data Center sul territorio)
	Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni centrali favorendone l'aggregazione e la migrazione su infrastrutture sicure ed affidabili (Migrazione infrastrutture interne verso il paradigma cloud)
	Migliorare la fruizione dei servizi digitali per cittadini ed imprese tramite il potenziamento della connettività per le PA
INTEROPERABILITÀ	Favorire l'applicazione della Linea guida sul Modello di Interoperabilità da parte degli erogatori di API
	Adottare API conformi al Modello di Interoperabilità
x SICUREZZA INFORMATICA	Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA
	Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione



3.2 Categorizzazione di II livello

I LIVELLO (LAYER)		II LIVELLO
SERVIZI		Servizi al cittadino
		Servizi a imprese e professionisti
		Servizi interni alla propria PA
		Servizi verso altre PA
PIATTAFORME		Sanità digitale (FSE e CUP)
		Identità Digitale
		Pagamenti digitali
		App IO
		ANPR
		NoiPA
		INAD
		Musei Siope+
DATI		Agricoltura, pesca, silvicoltura e prodotti alimentari
		Economia e finanze
		Istruzione, cultura e sport
		Energia
		Ambiente
		Governo e Settore pubblico
		Salute
		Tematiche internazionali
		Giustizia e sicurezza pubblica
		Regioni e città
		Popolazione e società
		Scienza e tecnologia Trasporti
INTEROPERABILITA		Agricoltura, pesca, silvicoltura e prodotti alimentari
		Economia e finanze
		Istruzione, cultura e sport
		Energia
		Ambiente
		Governo e Settore pubblico
		Salute
		Tematiche internazionali
		Giustizia e sicurezza pubblica
		Regioni e città
		Popolazione e società
		Scienza e tecnologia Trasporti
INFRASTRUTTURE		Data center e Cloud
		Connettività
SICUREZZA INFORMATICA	x	Portali istituzionali e CMS
	x	Sensibilizzazione del rischio cyber

ASOOM_TO_Azienda Ospedaliera Ordine Mauriziano di Torino - Rep. DG 01/02/2024.0000092.I



4 Servizi richiesti e ambito di intervento

4.1 Ambiti di intervento


La crescente e profonda evoluzione delle minacce informatiche nel contesto della pubblica amministrazione ha reso imperativo adottare una serie di misure di sicurezza cibernetica mirate al contrasto e alla mitigazione dei rischi derivanti.

Una maggiore attenzione sui temi della sicurezza cibernetica è, inoltre, richiesta anche alla luce dei nuovi sviluppi normativi che a livello europeo stanno modellando il framework di riferimento. In un primo momento con la Direttiva sulla sicurezza delle reti e dei sistemi informativi dell'Unione (Direttiva NISUE 2016/1148), attuata a livello nazionale grazie al D. Lgs.n. 65 del 2018 e recentemente con la Direttiva (UE) 2022/2555 (Direttiva NIS2), relativa a misure per un livello comune elevato di cibersecurity nell'Unione che, nonostante attenda ancora di un di un atto interno di recepimento, estende la platea dei destinatari e impone ulteriori obblighi in termini di sicurezza delle informazioni e delle infrastrutture cibernetiche. In questo contesto, diventa essenziale porre una maggiore attenzione sulle tematiche relative alla sicurezza delle informazioni e alla protezione dei dati sensibili in un'ottica strategica e proattiva rispetto al quadro normativo di riferimento in continuo aggiornamento. In tale quadro, A.O. Ordine Mauriziano di Torino intende irrobustire/potenziare i propri processi, sistemi e servizi.

In linea con questo scopo, sono stati individuati, nell'ambito del Lotto 2 – Servizi di Compliance e controllo dell'AQ, avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni, i seguenti obiettivi di sintesi:

- **Obiettivo 1: Valutare** il livello di compliance dell'Ente in vista del recepimento della **Direttiva NIS2** attraverso l'esecuzione di un assessment che permetta di definire una fotografia dello stato attuale dell'Ente, e la revisione e/o eventuale definizione ex novo della documentazione relativa ai temi NIS1/2;
- **Obiettivo 2: Implementare** opportune azioni di rimedio a seguito dell'individuazione di eventuali aree di scoperta dell'Ente in relazione ai nuovi obblighi introdotti dalla Direttiva.

4.2 Servizi richiesti

 SERVIZI RICHIESTI				
SERVIZIO	NOME SERVIZIO	VOCE DI COSTO	QUANTITA'	IMPORTO (al netto di IVA)
L2.S16 - Security Strategy	1.Supporto nella valutazione della compliance alla normativa NIS1/2	gg/p Team ottimale	500	125.000 €
	2. Supporto nell'implementazione di attività di rimedio volte al potenziamento del livello di sicurezza	gg/p Team ottimale	500	125.000€
TOTALE			1000	250.000 €

4.3 Dettaglio dei servizi richiesti

4.3.1 L2.S16 - Security Strategy

4.3.1.1 Descrizione e caratteristiche del servizio

Macro-attività	Attività	Deliverable
<p>Supporto nella valutazione e attuazione della compliance alla normativa NIS1/2</p>	<ul style="list-style-type: none"> • Valutazione del livello di compliance dell’Ente in vista del recepimento della Direttiva NIS2 – L’attività dovrà prevedere un’analisi del contesto attuale di A.O. Ordine Mauriziano di Torino al fine di valutarne il livello di maturità cyber in vista del recepimento della Direttiva NIS2. • Stesura e/o revisione delle procedure interne all’Ente al fine di innalzare il livello di conformità agli obblighi normativi – L’attività dovrà prevedere la stesura e/o la revisione di procedure in ambito cyber relative alla Direttiva NIS1/2. 	<ul style="list-style-type: none"> • Presentazione di avvio lavori • Documento di SAL periodico • Checklist diagnostica per la valutazione della maturità dell’Ente rispetto alla direttiva NIS2 • Documento contenente risultati dell’Assessment e di analisi delle aree di scoperta • Predisposizione / revisione di n.6 procedure
<p>Supporto nell’implementazione di attività di rimedio volte al potenziamento del livello sicurezza</p>	<ul style="list-style-type: none"> • Supporto specialistico all’Amministrazione nella valutazione e attuazione delle attività di rimedio da implementare, che saranno definite sulla base dei risultati dell’assessment e un’attenta valutazione delle esigenze di A.O. Ordine Mauriziano, sulla base delle loro priorità in ambito cybersecurity. 	<ul style="list-style-type: none"> • <i>Es., Policy e/o Procedure in ambito NIS1/2 (deliverable da definire a valle dei risultati dell’Assessment)</i>

4.3.1.2 Modalità di erogazione e consuntivazione

Coerentemente a quanto previsto nel “CAPITOLATO TECNICO SPECIALE SERVIZI DI COMPLIANCE E CONTROLLO” si precisa che la modalità di remunerazione di tali servizi è “progettuale (a corpo)” e che la metrica di misurazione è “giorni/persona del team ottimale”.

Saranno definiti di concerto con l’Amministrazione dei task e dei deliverable, dimensionati e valorizzati economicamente. La fatturazione avverrà sulla base dello stato dell’avanzamento lavori determinato coerentemente con il piano di lavoro definito alla consegna dei deliverable concordati, anche in versione parziale, previo benestare/e sarà riconosciuta bimestralmente.

Il team di lavoro per la realizzazione delle attività sopraccitate prevede il coinvolgimento delle seguenti figure professionali:

- Security Principal
- Security Solution Architect
- Senior Information Security Consultant
- Senior Security Auditor
- Data Protection Specialist



Le attività saranno erogate presso le sedi dell'Amministrazione Contraente oppure da remoto (presso le sedi del RTI, o presso altra sede da concordare con l'Amministrazione Stessa).

4.3.1.3 Attivazione e durata

Si prevede una durata massima di **24 mesi**.

4.4 Indici di digitalizzazione

4.4.1 Indicatori di digitalizzazione

Nell'ambito delle attività di governance ed in particolare della valutazione del livello di efficacia degli interventi operati dalle Amministrazioni attraverso l'utilizzo di contratti esecutivi afferenti alle Gare Strategiche in ambito Sicurezza ICT, si intendono definite due tipologie di indicatori:

- **Indicatori Generali**, che mappano il macro-obiettivo dell'intervento rispetto ai principali obiettivi strategici del Piano Triennale;
- **Indicatori Specifici**, che definiscono, sulla base delle specificità della Gara Strategica, le misure di digitalizzazione applicabili allo specifico contratto esecutivo, in funzione dei prodotti/servizi acquisiti. In tale contesto, è definito un indicatore (cd. "indicatore di progresso" in seguito descritto) che indica il livello di maturità della infrastruttura di sicurezza ICT delle Amministrazioni, sulla base del grado di mappatura degli interventi effettuati con le misure minime di sicurezza AGID (Circolare 18 aprile 2017, n. 2/2017, Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)»).

Gli indicatori saranno utilizzati per il monitoraggio dei contratti e del raggiungimento dei relativi obiettivi.

Nel contesto ACME, per la tipologia di interventi previsti, si considerano gli indicatori presentati nei prossimi due paragrafi e che saranno oggetto di monitoraggio nell'intero arco temporale dell'incarico presentato in questo Piano Operativo.

4.4.2 Indicatori generali di digitalizzazione

Di seguito si riportano gli indicatori Generali di digitalizzazione previsti per la presente fornitura:

INDICATORI DI COLLABORAZIONE E RIUSO		VALORE EX ANTE	VALORE EX POST
1	Riuso di processi per erogazione servizi digitali	Nessuna	<i>Gestione Uniforme della Sicurezza delle informazioni per A.O. Ordine Mauriziano di Torino</i> <i>Dato da valorizzare ogni 12 mesi</i>

Per ciascuno dei sopra riportati indicatori, verrà effettuata una valutazione in fase di avvio degli interventi progettuali e a valle (ogni 12 mesi), così da misurare il livello di digitalizzazione raggiunto per ciascuno di essi.



4.4.3 Indicatori di progresso

Per ogni classe di controlli ABSC (Agid Basic Security Control) previsti dalle misure minime di sicurezza AGID, ove successivamente modificate ed integrate, sarà calcolato il valore del relativo Indicatore di Progresso (Ip) dell'intervento ottenuto attraverso la realizzazione dell'Ordinativo di Fornitura (acquisto di servizi previsti nell'Ordinativo), che sarà determinato come da schema seguente:

Denominazione	Indicatore di progresso		
Aspetto da valutare	Grado di mappatura di ciascuna classe di controlli ABSC delle misure minime di sicurezza AGID		
Unità di misura	Numero di Controlli	Fonte dati	Piano dei Fabbisogni o Piano di lavoro Generale
Periodo di riferimento	Momento di Pianificazione dell'intervento	Frequenza di misurazione	Per ogni intervento pianificato
Dati da rilevare	<i>N1: numero di controlli relativi alla specifica classe ABSC soddisfatti attraverso l'intervento</i> <i>NT: numero totale di controlli relativi alla specifica classe previsti dalle misure minime di sicurezza AGID</i>		
Regole di campionamento	Nessuna		
Formula	$Ip = (N_1 - N_0) / N_T$		
Regole di arrotondamento	Nessuna		
Valore di soglia	<i>N0: numero di controlli relativi alla specifica classe soddisfatti prima dell'intervento;</i>		
Applicazione	Amministrazione Contraente		

Lo studio dell'effettiva applicabilità e la conseguente scelta e valorizzazione ex-ante ed ex-post degli indicatori di progresso è una delle attività che prevediamo all'interno del servizio **L2.S16 Security Strategy**.



5 Organizzazione e modalità di erogazione del contratto esecutivo

5.1 Attività in carico alle aziende del RTI

SERVIZIO	Deloitte Risk Advisory (100%)	EY Advisory (0%)	Teleco (0%)
L2.S16 - Security Strategy	100 %	0 %	0 %
TOTALE	100 %	0 %	0 %

5.2 Modalità di ricorso al subappalto da parte del fornitore

SERVIZIO	AZIENDA	QUOTA SUBAPPALTATA
L2.S16 – Security Strategy	Deloitte Risk Advisory Srl S.B.	0%

Si precisa che la quota di subappalto della singola Società non potrà mai essere superiore alla quota massima subappaltabile fatta salva espressa deroga concessa dal Committente.

5.3 Organizzazione e figure di riferimento del fornitore

In relazione all'organizzazione e alle figure di riferimento del Fornitore per la conduzione del progetto, si prevede la presenza di un RUAC con una struttura di Governance a supporto per le attività di PMO. In particolare, il **RUAC del CE** collabora con il RUAC di AQ ed è responsabile dei servizi del singolo CE.

Per l'erogazione dei servizi è prevista la presenza del referente tecnico per ciascun CE e comunque per ciascuna Amministrazione per tutti i servizi del Lotto 2 - Referente Tecnico CE (RT) - che assicura il corretto svolgimento dei servizi ed il relativo livello di qualità di erogazione, nel pieno rispetto degli indicatori condivisi. Per ciascun servizio oggetto del presente Piano Operativo, l'organizzazione prevede la composizione di un gruppo dedicato composto da un **Responsabile Attività** e da un gruppo di lavoro di supporto.

RUOLO	NOMINATIVI
RUAC CE	Fabio Battelli
Referente Tecnico CE (RT)	Andrea Abate
Responsabile Attività L2.S16	Silvia Rescigno

5.4 Modalità di esecuzione dei servizi

Le attività saranno erogate presso le sedi dell'Amministrazione Contraente oppure da remoto (presso le sedi del RTI, o presso altra sede da concordare con l'Amministrazione Stessa).



6 Piano di lavoro

6.1 Piano di Presa in carico

Il piano di presa in carico si basa sul coinvolgimento del personale che verrà poi impegnato a regime nella fornitura, sia a livello di governo che di erogazione dei servizi e trasparenza sull'andamento del processo di subentro nei confronti di tutti gli attori interessati attraverso una governance operativa e focalizzata.

FASE	ATTIVITÀ	W1	W2	W3	W4	W5
Incontri con l'Amministrazione	Incontri con il personale dell'Amministrazione volti a validare gli obiettivi di progetto e le relative modalità di esecuzione					
Predisposizione documentazione di gestione del progetto	Predisposizione degli strumenti e documentazione a supporto della gestione del progetto (presentazione di avvio attività, SAL ecc.)					
Avvio attività di PMO	Avvio delle attività di coordinamento del progetto per consentire il corretto svolgimento delle attività progettuali nelle tempistiche di progetto previste					

6.2 Cronoprogramma

	2024												2025												2026
	Febbraio	Marzo	Aprile	Maggio	Giugno	Luglio	Agosto	Settembre	Ottobre	Novembre	Dicembre	Gennaio	Febbraio	Marzo	Aprile	Maggio	Giugno	Luglio	Agosto	Settembre	Ottobre	Novembre	Dicembre	Gennaio	
L2.S16 Supporto nella valutazione e attuazione della compliance alla normativa NIS1/2																									
L2.S16 Supporto nell'implementazione di attività di rimedio volte al potenziamento del livello sicurezza																									

6.3 Data di attivazione e durata del servizio

Si prevede una durata massima di **24 mesi**.



7 Piano della qualità specifico

7.1 Organizzazione dei Servizi

A Livello di gestione del contratto esecutivo sono state identificate le seguenti figure con le relative responsabilità:

- Responsabili dei Servizi (RdS): per ciascun servizio è individuato un responsabile che supporta i Referenti Tecnici dei CE assicurando omogeneità di approccio trasversalmente alle diverse Amministrazioni e abilitando il riuso delle soluzioni già applicate con successo su altri CE.
- RUAC CE: figura responsabile dell'attuazione del CE, rappresenta il RTI nei confronti della singola Amministrazione.
- Referente Tecnico CE (RT) per l'erogazione dei servizi, assicura il corretto svolgimento dei servizi ed il relativo livello di qualità di erogazione, nel pieno rispetto degli indicatori condivisi. Ha la responsabilità delle attività di Presa in carico e trasferimento di Know How durante le quali è il riferimento per il fornitore uscente/entrante e coordina le attività dei team di lavoro.
- Responsabile Attività è referente tecnico per ciascuna attività all'interno del CE, coordina e assicura il corretto svolgimento delle attività operative eseguite dal team di lavoro.
- Team di Lavoro (TL), team operativi di intervento impegnati nell'erogazione dei servizi, composti da professionisti con profili previsti.

Nei successivi paragrafi sono declinate le figure previste all'interno del Team di Lavoro.

Security Strategy (L2.S16)

Il team ottimale sarà composto dalle seguenti figure con le relative responsabilità assegnate:

Profilo	Responsabilità
Security Principal	Project Manager, ha lo scopo di definire e gestire il progetto dal concepimento iniziale alla consegna finale. Responsabile dell'ottenimento di risultati ottimali, conformi agli standard di qualità, sicurezza e sostenibilità nonché coerenti con gli obiettivi, le performance, i costi ed i tempi definiti.
Senior Information Security Consultant	Presidia l'attuazione della strategia definita all'interno del suo ambito di responsabilità (sia questo un progetto, un processo, una location) coordinando attivamente le eventuali figure operative a lui assegnate per tale scopo, rappresentando il naturale raccordo tra la struttura di governance della cyber security e il resto del personale operativo. Controlla il rispetto alle regole definite e del cogente in materia di sicurezza delle informazioni. Pianifica ed attua misure di sicurezza per proteggere le reti e i sistemi informatici di un'organizzazione.
Senior Security Auditor	Garantisce la conformità con le procedure di controllo interno stabilite esaminando i registri, i rapporti, le pratiche operative e la documentazione. Completa i giornali di audit documentando test e risultati dell'audit. Individua i possibili punti vulnerabili di un sistema informativo.
Data Protection Specialist	Esperto nella protezione dei dati personali e dotato di competenze giuridiche e informatiche specifiche, verifica il rispetto di quanto previsto nelle normative italiane ed europee in termini di protezione



dei dati nonché delle politiche applicate dal titolare del trattamento o dal responsabile del trattamento in materia di protezione dei dati personali

Il RTI si impegna a modificare o ampliare la composizione del team di progetto in funzione dell'operatività e dei deliverable richiesti, garantendo la disponibilità dei profili professionali e delle competenze previste.

7.2 Metodologie e Tecniche

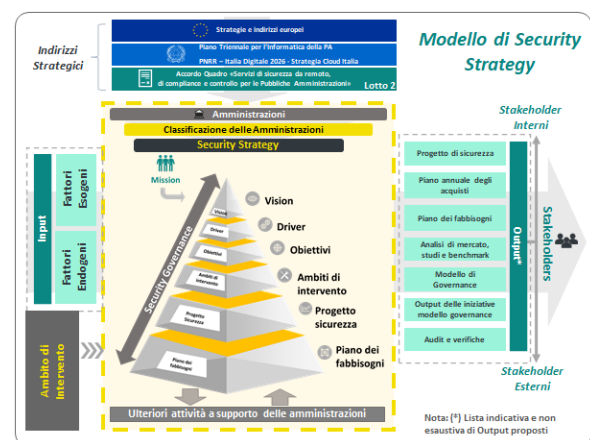
Security Strategy (L2.S16)

La strategia di sicurezza è l'abilitatore fondamentale che consente di individuare le azioni più appropriate per gestire i rischi di sicurezza in coerenza con le specificità delle Amministrazioni individuando le modalità con cui raggiungere i livelli di sicurezza richiesti e al contempo assicurare la conformità alle normative vigenti ed alle direttive di settore.

L'approccio concreto di elaborazione del Progetto di Sicurezza (di seguito PdS) avviene tramite modelli di PdS differenziati sulla base della classificazione e della complessità delle Amministrazioni (MappaPA). Allo scopo di supportare le Amministrazioni nella pianificazione strategica della Sicurezza ICT, il RTI prevede l'utilizzo di uno specifico Modello di Security Strategy, sviluppato sulla base di standard e leading practices riconosciute in ambito Security ICT (es. ISO27001-2, ISO27017-8, ISO27701 ISO31000, ISA62443, NIST800.53 v5, Framework Nazionale, Linee guida ENISA).

Tramite tale modello l'Amministrazione sarà in grado di recepire gli indirizzi strategici sia a livello nazionale che europeo, con un particolare focus verso gli ulteriori obblighi che saranno imposti a valle del recepimento della Direttiva NIS 2, e gli input esogeni ed endogeni, per definire - attraverso l'ausilio di metodologie, approcci operativi e strumenti - il PdS. Quest'ultimo, coerentemente con il contesto di riferimento e con le esigenze di stakeholder interni ed esterni, avrà lo scopo di attuare la Missione e la derivata Visione dell'Amministrazione (es. la trasposizione della Missione in una strategia a lungo termine di evoluzione tecnologica e/o organizzativa mirata al suo soddisfacimento). Con riferimento agli ambiti del PdS, allo scopo di articolare una risposta completa rispetto a tutte le fasi del ciclo di vita della sicurezza delle informazioni e dei sistemi ICT, il RTI propone di considerare, a titolo indicativo e non esaustivo, i seguenti Ambiti di intervento:

- Identify: strategia e pianificazione, Governance Asset e Processi, gestione del rischio cyber, security assurance (VA, PT, Testing del Codice), sicurezza terze parti e contratti di servizio, Compliance normativa
- Protect (Management): Information & Data Security, Identity & Access Management, Security by Design e Secure SDLC, Application & System Protection, Network Protection, Data Center Security, Secure Cloud Computing, Cyber Awareness & Training, Security Operations
- Detect: Monitoraggio continuo di sicurezza, Incident Detection, Threat intelligence, Threat Hunting
- Response: Cyber Incident Response, Investigation and Forensics
- Recovery: Continuità Operativa and Crisis Management, Disaster Recovery.



Identificativo: AOOMTO_Piano Fabbisogni | Rev 11.01.2024

Data: 11/01/2024

**ACCORDO QUADRO PER L’AFFIDAMENTO DI SERVIZI DI
SICUREZZA DA REMOTO, DI COMPLIANCE E
CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI**

**LOTTO 2 – SERVIZI DI COMPLIANCE E CONTROLLO
PUBBLICHE AMMINISTRAZIONI LOCALI**

A.O. Ordine Mauriziano di Torino



ASOOM_TO_Azienda Ospedaliera Ordine Mauriziano di Torino - Rep. DG 01/02/2024.0000092.I



CONTENUTI

1	Introduzione.....	
1.1	Ambito.....	
1.2	Richieste dell'Amministrazione contraente.....	
1.3	Riferimenti.....	
1.4	Acronimi e glossario.....	
2	Anagrafica dell'amministrazione.....	
3	Contesto di riferimento.....	
3.1	Contesto dei servizi.....	
3.2	Contesto tecnico ed operativo.....	
3.3	Contesto Economico – Finanziario.....	Firm
4	Ambiti funzionali oggetto di intervento.....	a
4.1	Obiettivi e benefici da perseguire.....	
4.2	Categorizzazione dell'intervento.....	
4.2.1	Categorizzazione di I livello.....	
4.2.2	Categorizzazione di II livello.....	
5	Servizi richiesti.....	
5.1	Dettaglio dei servizi richiesti.....	
5.1.1	L2.S16 - Security Strategy.....	
6	Elementi quantitativi e qualitativi per il dimensionamento servizi.....	
6.1	Elementi quantitativi dei servizi.....	
6.2	Elementi qualitativi dei servizi.....	
6.3	Pianificazione dei servizi.....	



1 INTRODUZIONE

1.1 Ambito

Nel Settembre 2021 CONSIP ha bandito una procedura aperta, suddivisa in due lotti, per “l’affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni – ID 2296”. Il Lotto 2, inerente ai servizi di compliance e controllo, è stato assegnato come primo aggiudicatario al Raggruppamento Temporaneo di Imprese (RTI), la cui mandataria è Deloitte Risk Advisory S.r.l. e le società mandanti sono EY Advisory S.p.A. e Teleco S.r.l., per la stipula di contratti esecutivi con le Pubbliche Amministrazioni Locali (PAL).

La durata dell’Accordo Quadro è di 24 mesi, decorrenti dalla data di attivazione. Per durata dell’Accordo Quadro si intende il periodo entro il quale le Amministrazioni potranno affidare, a seguito della approvazione del Piano Operativo, contratti esecutivi agli operatori economici aggiudicatari parti dell’Accordo Quadro per l’approvvigionamento dei servizi oggetto dell’Accordo Quadro. Ciascun Contratto esecutivo avrà una durata massima di 48 mesi decorrenti dalla relativa data di conclusione delle attività di presa in carico.

Il presente documento costituisce il “Piano dei fabbisogni” (o “Ordinativo di fornitura”), contenente i) i requisiti, i servizi, le caratteristiche qualitative, i dimensionamenti; ii) la descrizione del contesto tecnologico ed applicativo e la descrizione delle attività dimensionate, al fine di permettere la identificazione e contestualizzazione dei servizi nonché la eventuale declinazione delle figure professionali e degli strumenti a supporto.

1.2 Richieste dell’Amministrazione contraente

Nell’ambito dell’Accordo Quadro per l’affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni (Sigef 2296, Lotto2), A.O. Ordine Mauriziano di Torino intende acquisire la fornitura di alcuni servizi da Deloitte per attuare interventi volti ad innalzare il livello di maturità dell’Amministrazione in ambito cyber. L’ambito di riferimento dei servizi sarà:

- **L2.S16 – Servizio di Security Strategy**, composto dalle seguenti attività:
 - Supporto nella valutazione e attuazione della compliance alla normativa NIS1/2
 - Supporto nell’implementazione di attività di rimedio volte al potenziamento del livello di compliance dell’Ente rispetto alla normativa NIS1/2

1.3 Riferimenti

IDENTIFICATIVO	TITOLO/DESCRIZIONE
ID 2296 - Gara Sicurezza da remoto - Allegato 1 - Capitolato Tecnico Generale	Capitolato Tecnico Generale della GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L’AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E



CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI	
ID 2296 - Gara Sicurezza da remoto - Allegato 2B - Capitolato Tecnico Speciale Lotto 2	Capitolato Tecnico Speciale della GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L’AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI
ID 2296 - Gara Sicurezza da remoto - Capitolato Oneri	Capitolato d'Oneri della GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L’AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI
ID 2296 - Gara Sicurezza da remoto - Bando GURI	Bando GURI della GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L’AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI

1.4 Acronimi e glossario

DEFINIZIONE/ACRONIMO	DESCRIZIONE
RTI	Raggruppamento Temporaneo di Impresa
AQ	Accordo Quadro
CE	Contratto Esecutivo
PAL	Pubblica Amministrazione Locale



2 Anagrafica dell'amministrazione



DATI ANAGRAFICI DELL'AMMINISTRAZIONE

Ragione sociale Amministrazione	Azienda Ospedaliera Ordine Mauriziano di Torino
Indirizzo	Via Magellano, 1
CAP	10128
Comune	Torino
Provincia	TO
Regione	Piemonte
Codice Fiscale	09059340019
Indirizzo mail	ssi@mauriziano.it
PEC	ssi.mauriziano@pcert.postecert.it
Codice PA	asoom_to
Comparto di Appartenenza (PAL/PAC)	PAL



DATI ANAGRAFICI REFERENTE DELL'AMMINISTRAZIONE

Nome	Stefano
Cognome	Geninatti Togli
Telefono	011 5082792
Indirizzo mail	senginatti@mauriziano.it
PEC	ssi.mauriziano@pcert.postecert.it



3 Contesto di riferimento

3.1 Contesto dei servizi

L'Azienda Ospedaliera Ordine Mauriziano di Torino si distingue nel panorama della sanità piemontese come un'azienda dotata di aree di alta specializzazione, supportate da un'area di assistenza di base di grande professionalità e di aree di assistenza ben rappresentate e sviluppate, dedicate alla tutela delle fragilità. L'Azienda è costituita dal Presidio Umberto I di Torino (che deriva dall'Ordine Mauriziano) costruito nel 1881 e arricchito di numerosi padiglioni. All'interno dei principi e delle scelte organizzative per lo sviluppo della qualità dei servizi erogati, l'Azienda pone ai primi posti:

- La valorizzazione delle eccellenze professionali presenti nell'ospedale e della sperimentata collaborazione dei gruppi multidisciplinari e multiprofessionali, valore aggiunto di questa realtà ospedaliera, in un'ottica di effettivo governo clinico;
- La sicurezza e lo sviluppo della competenza di operatori e pazienti, mediante un modello organizzativo per intensità di cura e orientato al potenziamento dei meccanismi culturali e comportamentali di promozione ed educazione alla salute.

In tale contesto, per A.O. Ordine Mauriziano di Torino risulta importante aumentare la conoscenza e la consapevolezza sui rischi inerenti la propria organizzazione in ambito sicurezza informatica, al fine di aumentare il proprio livello di maturità e adottare delle azioni volte alla mitigazione dei rischi individuati.

In aggiunta, i recenti sviluppi in ambito normativo europeo, in particolare la Direttiva Europea NIS1/2, hanno rafforzato la necessità di attivare un processo di adeguamento ai nuovi obblighi e requisiti con particolare focus sugli enti del settore sanitario.

3.2 Contesto tecnico ed operativo

Per tale fornitura non sono individuati specifici vincoli di tipo tecnico ed operativo.

In termini di requisiti specifici per l'esecuzione delle attività oggetto dei servizi richiesti si rimanda ai requisiti trasversali previsti per l'AQ.

Le attività relative al presente Piano di Fabbisogni verranno condotte all'interno di eventuali gruppi di lavoro costituiti dagli interlocutori dell'Ente e/o di eventuali fornitori che hanno il compito di gestire il Sistema informativo dell'Ente.

3.3 Contesto Economico – Finanziario

La presente iniziativa dell'Aso 908 Mauriziano - Umberto I di Torino è volta all'ammodernamento e potenziamento del livello di digitalizzazione delle strutture sanitarie come previsto dall'investimento 1.1.1 nell'ambito della missione 6 "Salute" componente 2 (M6C2) del Piano Nazionale di Ripresa e Resilienza (PNRR).

Il progetto approvato con Deliberazione del Direttore Generale n. 176 del 7.3.2022 è inserito nei finanziamenti PNRR, CUP G16G22000070005.



4 Ambiti funzionali oggetto di intervento

La profonda evoluzione delle minacce informatiche verso la pubblica amministrazione detta la necessità di dotarsi di elevate misure di sicurezza cibernetica di contrasto e mitigazione. Vi è la necessità di una maggior attenzione alle tematiche che riguardano la sicurezza delle informazioni e la protezione dei dati; in tale quadro, A.O. Ordine Mauriziano di Torino intende irrobustire/potenziare i propri processi, sistemi e servizi.

4.1 Obiettivi e benefici da perseguire

In linea con quanto descritto in precedenza, è stato individuato, nell'ambito del Lotto 2 – Servizi di Compliance e controllo dell'AQ, avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni, i seguenti obiettivi di sintesi:

- **Obiettivo 1: Valutare** il livello di compliance dell'Ente in vista del recepimento della **Direttiva NIS2** attraverso l'esecuzione di un assessment che permetta di definire una fotografia dello stato attuale dell'Ente, e la revisione e/o eventuale definizione ex novo della documentazione relativa ai temi NIS1/2;
- **Obiettivo 2: Implementare** opportune azioni di rimedio a seguito dell'individuazione di eventuali aree di scopertura dell'Ente in relazione ai nuovi obblighi introdotti dalla Direttiva;

4.2 Categorizzazione dell'intervento

4.2.1 Categorizzazione di I livello

AMBITO	
I LIVELLO (LAYER)	OBIETTIVI PIANO TRIENNALE
SERVIZI	Servizi al cittadino
	Servizi a imprese e professionisti
	Servizi interni alla propria PA
	Servizi verso altre PA
DATI	Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese
	Aumentare la qualità dei dati e dei metadati
	Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati
PIATTAFORME	Favorire l'evoluzione delle piattaforme esistenti per migliorare i servizi offerti a cittadini ed imprese semplificando l'azione amministrativa
	Aumentare il grado di adozione ed utilizzo delle piattaforme abilitanti esistenti da parte delle PA
	Incrementare e razionalizzare il numero di piattaforme per le amministrazioni al fine di semplificare i servizi ai cittadini
	Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni locali favorendone l'aggregazione e la migrazione sul territorio (Riduzione Data Center sul territorio)
	Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni centrali favorendone l'aggregazione e la migrazione su infrastrutture sicure ed affidabili (Migrazione infrastrutture interne)



		verso il paradigma cloud)
		Migliorare la fruizione dei servizi digitali per cittadini ed imprese tramite il potenziamento della connettività per le PA
	INTEROPERABILITÀ	Favorire l'applicazione della Linea guida sul Modello di Interoperabilità da parte degli erogatori di API
		Adottare API conformi al Modello di Interoperabilità
x	SICUREZZA INFORMATICA	Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA
		Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione

4.2.2 Categorizzazione di II livello

I LIVELLO (LAYER)	II LIVELLO
SERVIZI	Servizi al cittadino
	Servizi a imprese e professionisti
	Servizi interni alla propria PA
	Servizi verso altre PA
PIATTAFORME	Sanità digitale (FSE e CUP)
	Identità Digitale
	Pagamenti digitali
	App IO
	ANPR
	NoiPA
	INAD
	Musei
DATI	Siope+
	Agricoltura, pesca, silvicoltura e prodotti alimentari
	Economia e finanze
	Istruzione, cultura e sport
	Energia
	Ambiente
	Governo e Settore pubblico
	Salute
	Tematiche internazionali
	Giustizia e sicurezza pubblica
	Regioni e città
	Popolazione e società
Scienza e tecnologia	
Trasporti	
INTEROPERABILITÀ	Agricoltura, pesca, silvicoltura e prodotti




		alimentari
		Economia e finanze
		Istruzione, cultura e sport
		Energia
		Ambiente
		Governo e Settore pubblico
		Salute
		Tematiche internazionali
		Giustizia e sicurezza pubblica
		Regioni e città
		Popolazione e società
		Scienza e tecnologia
		Trasporti
INFRASTRUTTURE		Data center e Cloud
		Connettività
SICUREZZA INFORMATICA	X	Portali istituzionali e CMS
	X	Sensibilizzazione del rischio cyber

ASOOM_TO.Azienda Ospedaliera Ordine Mauriziano di Torino - Rep. DG 01/02/2024.0000092.I



5 Servizi richiesti

 SERVIZI RICHIESTI				
SERVIZIO	NOME SERVIZIO	VOCE DI COSTO	QUANTITA'	IMPORTO (al netto di IVA)
L2.S16 - Security Strategy	1. Supporto nella valutazione e attuazione della compliance alla normativa NIS1/2	gg/p Team ottimale	500	125.000 €
	2. Supporto nell'implementazione di attività di rimedio volte al potenziamento del livello di sicurezza	gg/p Team ottimale	500	125.000€
TOTALE			1000	250.000 €

5.1 Dettaglio dei servizi richiesti

5.1.1 L2.S16 - Security Strategy

5.1.1.1 Descrizione e caratteristiche del servizio

Il servizio prevede gli ambiti di intervento descritti al paragrafo 3.1 e 4.1 del presente documento e di seguito ulteriormente descritti in termini di attività e deliverable.

Macro-attività	Attività	Deliverable
1. Supporto nella valutazione e attuazione della compliance alla normativa NIS1/2	<ul style="list-style-type: none"> Valutazione del livello di compliance dell'Ente in vista del recepimento della Direttiva NIS2 – L'attività dovrà prevedere un'analisi del contesto attuale di A.O. Ordine Mauriziano di Torino al fine di valutarne il livello di maturità cyber in vista del recepimento della Direttiva NIS2. Stesura e/o revisione delle procedure interne all'Ente al fine di innalzare il livello di conformità agli obblighi normativi – L'attività dovrà prevedere la stesura e/o la revisione di procedure in ambito cyber relative alla Direttiva NIS1/2. 	<ul style="list-style-type: none"> Documento contenente risultati dell'Assessment e di analisi delle aree di scoperta Predisposizione / revisione di n.6 procedure



Macro-attività	Attività	Deliverable
<p>2. Supporto nell'implementazione di attività di rimedio volte al potenziamento del livello di sicurezza</p>	<ul style="list-style-type: none"> Attuazione di attività di rimedio definite in base alle esigenze emerse a seguito dell'attività di assessment 	<ul style="list-style-type: none"> Documentazione in ambito security

5.1.1.2 Modalità di erogazione e consuntivazione

Coerentemente a quanto previsto nel "CAPITOLATO TECNICO SPECIALE SERVIZI DI COMPLIANCE E CONTROLLO" si precisa che la modalità di remunerazione di tali servizi è "progettuale (a corpo)" e che la metrica di misurazione è "giorni/persona del team ottimale".

Saranno definiti di concerto con l'Amministrazione dei task e dei deliverable, dimensionati e valorizzati economicamente. La fatturazione avverrà sulla base dello stato dell'avanzamento lavori determinato coerentemente con il piano di lavoro definito alla consegna dei deliverable concordati previo benessere/e sarà riconosciuta bimestralmente.

Il team di lavoro per la realizzazione delle attività sopracitate prevede il coinvolgimento delle seguenti figure professionali:

- Security Principal
- Security Solution Architect
- Senior Information Security Consultant
- Senior Security Auditor
- Data Protection Specialist

Le attività saranno erogate presso le sedi dell'Amministrazione Contraente oppure da remoto (presso le sedi del RTI, o presso altra sede da concordare con l'Amministrazione Stessa).

5.1.1.3 Attivazione e durata

Si prevede una durata massima di **24 mesi**



6 Elementi quantitativi e qualitativi per il dimensionamento servizi

6.1 Elementi quantitativi dei servizi

Si riporta di seguito una caratterizzazione quantitativa di riferimento data dalla complessità dei processi individuati:

ID	NOME SERVIZIO	Gg/p Team ottimale	Uffici interessati	Enti Coinvolti	Numero di utenti principali coinvolti	Numero Volumi
L2.S16	Security Strategy	1000	N.D.	1	c.a 10	N.A.

6.2 Elementi qualitativi dei servizi

I servizi dovranno essere svolti tenendo conto delle linee guida tecniche del Dipartimento e in ottemperanza alla normativa vigente così come in considerazione delle successive modifiche che verranno individuate.

6.3 Pianificazione dei servizi

La durata ipotizzata per la fornitura è di massimo **24 mesi** dalla data di attivazione, compatibilmente con il vincolo definito dall'AQ, ovvero che i Contratti Esecutivi hanno una durata massima pari alla durata residua, al momento della sua stipula, dell'AQ.

Di seguito si riporta la pianificazione di massima del programma con indicazione degli obiettivi in ambito del presente piano dei fabbisogni.

	Mese 1	Mese 2	Mese 3	Mese 4	Mese 5	Mese 6	Mese 7	Mese 8	Mese 9	Mese 10	Mese 11	Mese 12	Mese 13	Mese 14	Mese 15	Mese 16	Mese 17	Mese 18	Mese 19	Mese 20	Mese 21	Mese 22	Mese 23	Mese 24
L2.S16 Security Strategy																								

