SAN GIUSEPPE MOSCATI - AVELLINO
AZIENDA OSPEDALIERA DI RILIEVO NAZIONALE E DI ALTA SPECIALITÀ

C.da Amoretta 83100 Avellino – P.IVA 01948180649

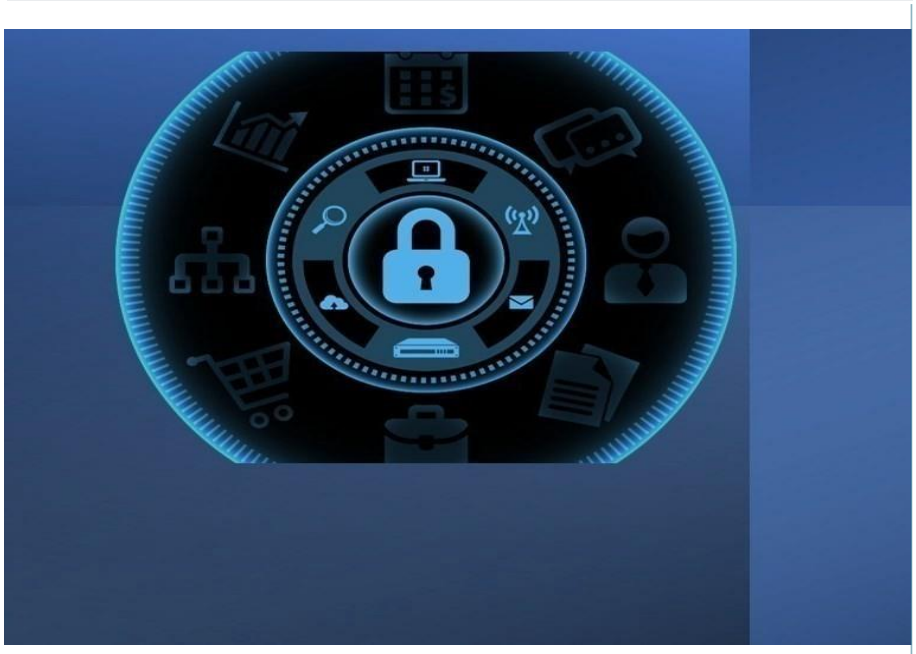
Identificativo: Piano dei Fabbisogni V1

Data: 07/06/2023

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



Azienda Ospedaliera di Rilievo Nazionale e di Alta Specialità San Giuseppe Moscati

Costituito

Raggruppamento Temporaneo di Imprese

composto da:

Deloitte Risk Advisory S.r.l.

EY Advisory S.p.A.

Teleco S.r.l.

Firma

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 24 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

Negli ultimi mesi gli attacchi informatici ad aziende sanitarie si sono moltiplicati, mettendo in serio pericolo i dati (e la salute) dei pazienti. Il settore sanitario, infatti, è molto appetibile per i cybercriminali, perché considerato uno dei più vulnerabili al pagamento dei riscatti (ransomware), per evitare la diffusione dei dati e proteggere le infrastrutture critiche. Negli ultimi anni, diverse strutture sanitarie sono state colpite da attacchi informatici che hanno causato la perdita di dati sensibili e il blocco dei sistemi informatici, impedendo ai medici di accedere ai dati dei pazienti e di erogare i servizi sanitari previsti.

In particolare, nelle strutture tecnologicamente più avanzate un crescente numero di apparecchiature elettromedicali e diagnostiche vengono interconnesse alle reti, accrescendo la possibilità di subire attacchi informatici. Questo è evidenziato dai molti episodi di ospedali colpiti da ransomware riportati dai media.

Le aziende ospedaliere devono fare i conti non solo con i rischi esterni, ma anche con quelli interni derivanti da personale non sufficientemente sensibilizzato ed una cultura aziendale non matura rispetto agli scenari di rischio emergenti.

Per questo motivo **A.O.R.N. San Giuseppe Moscati** ha deciso di ricevere un supporto qualificato per mantenere ed irrobustire la propria IT Security Posture, strutturando il proprio Sistema di Gestione della Sicurezza delle Informazioni (SGSI o ISMS in inglese) in conformità allo standard ISO/IEC 27001, intraprendendo il percorso verso la Certificazione formale del Sistema e gestendo un programma di test periodici sulla sicurezza applicativa dei propri sistemi simulandone la compromissione da parte di un attaccante esterno, identificando le vulnerabilità e sanandole in ottica di aumento dei livelli di sicurezza.

In tal senso è fondamentale attuare un continuo e programmato miglioramento della postura di sicurezza, con la formalizzazione dei processi virtuosi esistenti e nella cornice – più organizzata – di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

L'obiettivo è quello di rafforzare il governo e la maturità Cyber dell'**A.O.R.N. San Giuseppe Moscati,** ossia garantire Riservatezza, Integrità e Disponibilità del patrimonio informativo, con particolare riferimento ai dati personali, nel contesto della digitalizzazione dei servizi dell'intero ecosistema. La progettualità include le seguenti attività:

- Assessment iniziale finalizzato una valutazione dettagliata delle attuali misure di sicurezza e dei rischi

specifici insistenti sull'Azienda Ospedaliera, al fine di individuare eventuali aree di miglioramento;

Attività ciclica di processi continui nel tempo

- **Implementazione tecnica:** attraverso il supporto specialistico costante nelle azioni di rimedio e adozione degli strumenti tecnici necessari per affrontare le vulnerabilità individuate nelle attività di assessment, secondo il Programma di miglioramento continuo.
- **Formalizzazione, monitoraggio ed evoluzione dei processi organizzativi:** attraverso l'identificazione delle pratiche e processi virtuosi esistenti nell'ambito del U.O.C. Sistemi Informativi, formalizzazione degli stessi, per ottenere la maturità organizzativa necessaria ai fini della certificazione ISO27001:2022. Questo standard internazionale, ben noto e riconosciuto, fornisce un insieme di regole chiare e strutturate per organizzare le attività di sicurezza ed agevolare la conformità agli obblighi di legge in materia di privacy e protezione dei dati personali (GDPR).
- **Valutazione tecnica periodica e monitoraggio continuo:** per supportare il monitoraggio costante dello stato delle misure di sicurezza ed individuare eventuali nuove vulnerabilità ottenendo i dati necessari per le iniziative di rimedio. Questo processo consiste in due attività cicliche:
    - **Vulnerability Assessment (VA):** valuta periodicamente le vulnerabilità esistenti in ragione delle minacce;
    - **Penetration Test (PT):** verifica l'effettiva efficacia delle misure di sicurezza adottate a contrasto delle minacce.

Nell'ambito del contratto quadro per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni, l'A.O.R.N. San Giuseppe Moscati ha richiesto, ai fini dello sviluppo del **Progetto di Sicurezza,** l'esecuzione dei servizi afferenti al **Lotto 2- Servizi di Compliance e controllo:**

- **Servizio di Security Strategy;**
- **Servizio di Vulnerability Assessment;**
- **Supporto all'Analisi e alla Gestione degli Incidenti;**
- **Servizio di Penetration Testing;**
- **Compliance Normativa.**

1.3 Riferimenti

IDENTIFICATIVO	TITOLO/DESCRIZIONE
ID 2296 - Gara Sicurezza da remoto - Allegato 1 - Capitolato Tecnico Generale	Capitolato Tecnico Generale della GARA 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 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 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 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
AGID	Agenzia per l'Italia Digitale
ICT	Information and Communications Technology
PA	Pubblica Amministrazione

2. Anagrafica dell'amministrazione

DATI ANAGRAFICI DELL'AMMINISTRAZIONE	
Ragione sociale Amministrazione	Azienda Ospedaliera di Rilievo Nazionale
Indirizzo	C.da Amoretta
CAP	83100
Comune	Avellino
Provincia	AV
Regione	Campania
Codice Fiscale	01948180649
Indirizzo mail	info@aornmoscati.it
PEC	protocollo.generale@pec.aornmoscati.it
Codice PA	ao_sgma
Comparto di Appartenenza (PAL/PAC)	PAL

DATI ANAGRAFICI REFERENTE DELL'AMMINISTRAZIONE	
Nome	Giuseppe
Cognome	Versace
Telefono	
Indirizzo mail	giuseppe.versace@aornmoscati.it
PEC	

3. Contesto di riferimento

3.1 Contesto dei servizi

Il **Progetto di Sicurezza** dell'A.O.R.N. San Giuseppe Moscati, si pone l'obiettivo di rafforzare il governo e la maturità di Sicurezza dell'Azienda Ospedaliera, ossia garantire Riservatezza, Integrità e Disponibilità del patrimonio informativo nel contesto della digitalizzazione dei servizi erogati.

Nel corso degli ultimi anni U.O.C. Sistemi Informativi ha intrapreso e finalizzato importanti interventi volti al miglioramento della stabilità dei sistemi informativi mediante il consolidamento dell'infrastruttura fisica e logica (a titolo esemplificativo e non esaustivo: Data center, server, rete, programmi di realizzazione di ambienti virtuali, backup e continuità operativa, antivirus e piattaforme per la sicurezza preventiva). In tale contesto ed al fine di continuare nel processo di consolidamento dei Sistemi Informativi, la Direzione del Dipartimento suggerisce un approccio progettuale che implica l'adozione di una strategia focalizzata sull'analisi e sullo sviluppo costante della postura di sicurezza, adatta al contesto attuale.

L'obiettivo è assicurare un aggiornamento continuo in relazione all'evolversi del panorama dei rischi ed in aggiunta e coerentemente a quanto già implementato nel corso degli ultimi anni mediante la pianificazione e l'esecuzione di specifiche attività caratterizzate da una valenza temporale una tantum, altre caratterizzate da una ciclicità di processi continui nel tempo, secondo la metodologia Plan-Do-Check-Act.

Tale strategia può portare numerosi benefici all'azienda, fra cui principalmente:

- la realizzazione di un Programma di miglioramento, unitario e coerente, idoneo a prevenire e contrastare le minacce informatiche dirette ai pazienti e all'Azienda Ospedaliera;
- la conformità alle principali normative e standard di settore, quali le "Misure Minime di Sicurezza" indicate dall' Agenzia Italia Digitale (AgID), le indicazioni dell'Agenzia Nazionale per la cybersicurezza Nazionale (ACN) la normativa nazionale in materia di cybersecurity, Regolamento Europeo Protezione dei Dati (GDPR) e lo standard ISO 27001:2022, che rappresenta una cornice unitaria e agevolatrice per la gestione della sicurezza informatica;

permettendo, così, di affrontare le crescenti sfide date dall'evoluzione tecnologica, attraverso il monitoraggio, la prevenzione e la risposta continua.

Il programma altresì consentirà all'Azienda, ed in particolare al perimetro di azione del U.O.C. Sistemi Informativi, l'ottenimento della certificazione ISO27001:2022.

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'Accordo Quadro.

Le attività verranno condotte all'interno di eventuali gruppi di lavoro costituiti dagli interlocutori istituzionali nell'ambito dell'A.O.R.N. San Giuseppe Moscati

3.3 Contesto Economico – Finanziario

L'Amministrazione ricorre alle forme di finanziamento con le risorse previste dal PNRR

4. Ambiti funzionali oggetto di intervento

4.1 Obiettivi e benefici da perseguire

Il **Progetto di Sicurezza** mira a rafforzare il governo e la maturità di Sicurezza l'ecosistema aziendale nel contesto della digitalizzazione dei servizi.

In linea con quanto descritto in precedenza, sono stati individuati, nell'ambito del **Lotto 2- Servizi di**

Compliance e controllo dell'Accordo Quadro, avente ad oggetto per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni, i seguenti obiettivi di sintesi, che ricadono nel più ampio programma di attuazione delle iniziative in ambito Progetto di Sicurezza anzi riepilogate:

- **Obiettivo 1:** individuare le linee strategiche in materia di sicurezza ICT, definire e monitorare le relative azioni strategiche adottate, al fine di realizzare un "progetto di sicurezza" unitario e coerente all'interno dell'ecosistema aziendale (L2.S16)
- **Obiettivo 2:** identificare con ciclicità lo stato di esposizione alle vulnerabilità (vulnerability assessment) mediante la raccolta di informazioni concernente i servizi erogati, le applicazioni, l'architettura e le componenti tecnologiche (L2.S17)
- **Obiettivo 3:** migliorare la gestione degli incidenti per incrementare efficacia ed efficienza dei processi di Incident Management (L2.S21)
- **Obiettivo 4:** eseguire attacchi simulati (penetration test) per verificare concretamente la possibilità di sfruttare vulnerabilità identificate su sistemi/reti/applicazioni/dispositivi (L2.S22)
- **Obiettivo 5:** garantire la corretta attuazione degli adempimenti del GDPR (General Data Protection Regulation - Regolamento UE 2016) con riferimento al perimetro del SGSI (U.O.C. Sistemi Informativi) (L2.S23)

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
		NAD
		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

4.3 Indicatori di digitalizzazione

4.3.1 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
	Riuso di processi per erogazione dei servizi digitali	*Nessuna*	*Gestione uniforme della Sicurezza delle informazioni*

Per ciascuno dei soprariportati indicatori, verrà effettuata una valutazione in fase di avvio dei singoli interventi progettuali e a valle, così da misurare il livello di digitalizzazione raggiunto per ciascuno di essi.

5. Servizi richiesti

Di seguito si riporta una sintesi dei servizi e relativa quantificazione:

SERVIZI				
ID	**NOME SERVIZIO**	**VOCE DI COSTO**	**QUANTITA'**	**IMPORTO**
L2.S16	Security Strategy	L2.S16 - gg/p Team ottimale	1.798	**449.500,00 €**
L2.S17	Vulnerability Assessment	L2.S17 - gg/p Team ottimale	873	**144.000,00 €**
L2.S21	Supporto all'Analisi e alla Gestione degli Incidenti	L2.S21 - gg/p Team ottimale	147	**25.000,00 €**
L2.S22	Penetration Testing	L2.S22 - gg/p Team ottimale	461	**76.000,00 €**
L2.S23	Compliance Normativa	L2.S23 - gg/p Team ottimale	70	**12.000,00 €**
			TOTALE	**706.500,00 €**

5.1 Dettaglio dei servizi richiesti

5.1.1 L2.S16 - Security Strategy

5.1.1.1 Descrizione e caratteristiche del servizio

Macro-Attività	Attività	Deliverable
Percorso ISO27001 – Primo anno - Attività propedeutiche e preparatorie	Definizione degli aspetti operativi e metodologici per la realizzazione del lavoro. In particolare: ➢ Obiettivi e il campo di applicazione del SGSI (U.O.C. Sistemi Informativi) ➢ Perimetro di dettaglio in termini di servizi, asset e dipartimenti coinvolti ➢ Elenco preliminare della documentazione che verrà visionata e sviluppata (es. politica per la sicurezza delle informazioni, organigramma, processi e procedure relative all'analisi del rischio) ➢ Modalità di condivisione dei risultati delle diverse fasi di lavoro.	Piano di lavoro di dettaglio Presentazione per il primo workshop informativo
Percorso ISO27001 – Primo anno – Assessment e Pianificazione	Realizzazione di interviste e verifiche orientate a comprendere lo stato dell'arte e gli interventi documentali ed operativi da realizzare all'interno dell'U.O.C.	Output interviste referenti Assessment Report e roadmap di pianificazione degli interventi
Percorso ISO27001 – Primo anno – Disegno del SGSI	Progettazione del SGSI e delle sue componenti, in termini di: ➢ Redazione del modello di servizi e processi adottato,	ISO 27001 Policies ISO 27001 Specific

	con riferimento al perimetro di certificazione ➢ Disegno della struttura organizzativa e operativa del SGSI (es. ruoli e responsabilità, asset coinvolti); ➢ Redazione del corpo documentale di Policy allineate ai domini ISO27001 e del «ISO27001 specific kit»	Kit Modello servizi e processi
Percorso ISO27001 – Primo anno – Analisi dei rischi di sicurezza	Esecuzione di Security Risk Assessment sulla base della metodologia definita	Risk Assesment
Percorso ISO27001 – Primo anno – Formazione	Erogazione di sessioni di formazione in aula fisica e/o virtuale: ➢ N.1 Corso rivolto alla Direzione con finalità formative sugli elementi strategici dell'ISMS (es. Direzione Amministrativa). ➢ N.1 Corso per gli addetti operativi del SGSI (come il personale IT) sui principali temi di IT Security al fine di approfondire conoscenza sulle minacce e le tecniche di risposta agli attacchi. ➢ N.1 Corso rivolto a tutto il personale aziendale (o sotto-insieme maggiormente coinvolto nel Sistema). Il corso verterà sugli elementi fondamentali del Sistema, sulle procedure implementate, ponendo particolare attenzione agli aspetti più operativi.	Materiale didattico e Test di apprendimento per ciascuna delle sessioni di formazione Erogazione di n° 3 sessioni di formazione
Percorso ISO27001 – Primo anno – Audit del Sistema di Gestione	In questa fase verrà pianificato e svolto un audit interno del Sistema di gestione con l'obiettivo di: ➢ Verificare il grado di funzionamento del Sistema di Gestione e di applicazione delle relative procedure. ➢ Individuare eventuali aree critiche di funzionamento del sistema. ➢ Riportare alla Direzione i risultati.	Piano di Audit interno Verbale di Audit Interno
Percorso ISO27001 – Primo anno – Riesame del Sistema	L'attività di riesame prevede un supporto nelle seguenti azioni: ➢ Calcolare gli indicatori precedentemente definiti allo scopo di misurare l'efficacia del Sistema di Gestione (indicatori sia tecnici come, ad esempio, numero incidenti/breach e rilevazioni emerse dall'analisi dei rischi/audit); ➢ Esaminare i dati e le informazioni raccolte all'interno del SGSI (es. esiti del Risk Assessment e degli Audit, feedback Formazione); ➢ Revisionare il Sistema ai fini del suo miglioramento.	Relazione di Input per la Management Review Management Review
Percorso ISO27001 – Primo anno – Assistenza alla Certificazione	Questa attività è orientata ad assistere il personale, durante le giornate di visite ispettive esterne condotte dall'Ente di Certificazione* e saranno finalizzate al riscontro dell'effettiva aderenza del SGSI alla Norma ISO 27001: ➢ Sia per quanto riguarda la documentazione predisposta ➢ Sia per le attività effettivamente messe in atto. Verrà inoltre fornita assistenza nell'interlocuzione con l'Ente di certificazione e supporto nella gestione delle	Sintesi dei risultati riscontrati durante le verifiche Piano per la chiusura di eventuali osservazioni rilasciate dal certificatore

	richieste dell'Ente e delle eventuali osservazioni, che verranno formalizzate in un "Piano di adeguamento", nel quale saranno suggeriti tempi, risorse e responsabilità per la loro risoluzione.	
Percorso ISO27001 – Primo anno – Supporto Specialistico per la valutazione dei controlli tecnologici	Durante il percorso di certificazione emergerà la necessità di svolgere attività di supporto al fine di indirizzare azioni tecniche. A titolo esemplificativo e non esaustivo: ➢ Controlli applicativi. Supporto all'identificazione e alle configurazioni sui sistemi di autenticazione applicativa. Interazioni con i sistemi di certificazione a chiave pubblica e privata. Supporto all'identificazione delle vulnerabilità e alle mitigazioni da applicare su sistemi applicativi ➢ Controlli infrastrutturali.	Report periodici di stato avanzamento
Percorso ISO27001 – Secondo anno – Supporto Specialistico al mantenimento della certificazione	➢ Revisione del SGSI; ➢ Aggiornamento del Risk Assessment e rielaborazione dei risultati; ➢ Sessione formativa di aggiornamento e refresh; ➢ Esecuzione audit su 1 ambito/processo e 1 fornitore critico; ➢ Riesame del sistema; ➢ supporto al team durante la visita del certificatore; ➢ controlli applicativi ed infrastrutturali.	Come per attività previste per il primo anno, esclusi output relativi ad "attività propedeutiche e preparatorie" e "Assesment e pianificazione"
Attività di supporto System Hardening	Supporto alla revisione delle configurazioni dei sistemi a seguito degli esiti delle attività di VA-PT	Eventuale revisione delle configurazioni dei sistemi

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 consuntivazione avverrà sulla base dello stato dell'avanzamento lavori mensile determinato coerentemente con il piano di lavoro definito.

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, per il primo anno e per l'anno successivo, saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

5.1.1.3 Attivazione e durata

Si prevede l'avvio del servizio entro Luglio 2023 per una durata di 24 mesi.

5.1.2 L2.S17 - Vulnerability assessment

5.1.2.1 Descrizione e caratteristiche del servizio

Macro-attività	Attività	Deliverable
Vulnerability Assessment	Cyber Testing volto all'identificazione delle capacità dei sistemi e degli strumenti di sicurezza mediante ➢ Attività Vulnerability Assessment su un sottoinsieme dei sistemi IT rilevante dell'Ente ➢ Definizione del piano di azione e supporto all'identificazione delle modalità di implementazione ➢ Re-check delle vulnerabilità a seguito del remediation plan	Executive Summary Technical Report Remediation Plan

5.1.2.2 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 consuntivazione avverrà sulla base dello stato dell'avanzamento lavori mensile determinato coerentemente con il piano di lavoro definito.

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

- Security Principal
- Senior Penetration tester
- Junior Penetration tester

Le attività, per il primo anno e per l'anno successivi, saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

5.1.2.3 Attivazione e durata

Si prevede l'avvio del servizio entro Luglio 2023 per una durata di 24 mesi.

5.1.3 L2.S21 – Supporto all'Analisi e alla Gestione degli Incidenti

5.1.3.1 Descrizione e caratteristiche del servizio

Macro-attività	Attività	Deliverable
Miglioramento del processo di Incident Management	Analisi e miglioramento del processo di incident management (rilevazione, risposta agli incidenti, playbook e processi di gestione della crisi)	Processo di Incident Management

5.1.3.2 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"*.

Saranno definiti di concerto con l'Amministrazione dei task e dei deliverable, dimensionati e valorizzati economicamente. La consuntivazione avverrà sulla base dello stato dell'avanzamento lavori mensile determinato coerentemente con il piano di lavoro definito.

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

professionali:

- Security Principal
- Senior Security Analyst
- Junior Security Analyst
- Forensic Expert

Le attività, per il primo anno e per l'anno successivo, saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

5.1.3.3 Attivazione e durata

Si prevede l'avvio del servizio entro Luglio 2023 per una durata di 24 mesi.

5.1.4 L2.S22 – Penetration testing

5.1.4.1 Descrizione e caratteristiche del servizio

Macro-attività	Attività	Deliverable
Penetration Testing	Cyber Testing volto all'identificazione delle capacità dei sistemi e degli strumenti di sicurezza mediante ➢ Attività Penetration Test su un sottoinsieme dei sistemi IT rilevante dell'Ente ➢ Definizione del piano di azione e supporto all'identificazione delle modalità di implementazione ➢ Re-check delle vulnerabilità a seguito del remediation plan	Executive Summary Technical Report Remediation Plan

5.1.4.2 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*".

Saranno definiti di concerto con l'Amministrazione dei task e dei deliverable, dimensionati e valorizzati economicamente. La consuntivazione avverrà sulla base dello stato dell'avanzamento lavori mensile determinato coerentemente con il piano di lavoro definito.

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

- Security Principal
- Senior Penetration tester
- Junior Penetration tester
- Forensic Expert

Le attività, per il primo anno e per il secondo anno, saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

5.1.4.3 Attivazione e durata

Si prevede l'avvio del servizio entro Luglio 2023 per una durata di 24 mesi.

5.1.5 L2.S23 – Compliance Normativa

5.1.5.1 Descrizione e caratteristiche del servizio

Macro-attività	Attività	Deliverable
Governo della Conformità Privacy	Supporto operative nelle attività di consolidamento del livello di Compliance Normativa in ambito Privacy con riferimento al perimetro del SGSI (U.O.C. Sistemi Informativi).	Set documentale in ambito Privacy

5.1.4.2 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*".

Saranno definiti di concerto con l'Amministrazione dei task e dei deliverable, dimensionati e valorizzati economicamente. La consuntivazione avverrà sulla base dello stato dell'avanzamento lavori mensile determinato coerentemente con il piano di lavoro definito.

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

- Security Principal
- Senior Information Security Consultant
- Junior Information Security Consultant
- Senior Security Auditor
- Data Protection Specialist

Le attività, per il primo anno e per il secondo anno, saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

5.1.4.3 Attivazione e durata

Si prevede l'avvio del servizio entro Luglio 2023 per una durata di 24 mesi.

5.2 Organizzazione e figure di riferimento dell'amministrazione

Si riportano di seguito il personale incaricato dall'Amministrazione con i relativi ruoli/responsabilità.

STRUTTURA	FIGURE DI RIFERIMENTO
U.O.C. Sistemi Informativi - **AREA SISTEMI INFORMATIVI E AGENDA DIGITALE** ***Servizio Sviluppo Software, Agenda Digitale e Gestione Banche Dati***	Direttore U.O.C.
U.O.C. Sistemi Informativi - **AREA SISTEMI INFORMATIVI E AGENDA DIGITALE** ***Servizio Gestione Sistemi e Reti Tecnologiche***	Direttore U.O.C.

5.3 Organizzazione e figure di riferimento del fornitore

Si richiede di indicare nel Piano Operativo le persone incaricate dal Fornitore per la conduzione del progetto e i relativi ruoli/responsabilità.

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	Ambiti di servizio	Numero Key user coinvolti	Numero Volumi
L2.S16	Security Strategy	1.798	**>2**	**>5**	**>15**	**N/A**
L2.S17	Vulnerability Assessment	873	**>2**	**>5**	**>15**	**N/A**
L2.S21	Supporto all'Analisi e alla Gestione degli Incidenti	147	**>2**	**>5**	**>15**	**N/A**
L2.S22	Penetration Testing	461	**>2**	**>5**	**>15**	**N/A**
L2.S23	Compliance Normativa	70	**>2**	**>5**	**>15**	**N/A**

6.2 Elementi qualitativi dei servizi

I servizi dovranno essere svolti tenendo conto delle linee guida tecniche e la normativa vigente o le successive modificazioni che verranno individuate.

Si riportano di seguito i principali riferimenti alla normativa regionale, nazionale ed internazionale in ambito Sicurezza e Privacy con riferimento al perimetro del presente Piano dei fabbisogni:

- Regolamento Europeo in materia di protezione dei dati personali ("GDPR") e Decreto Legislativo 10 agosto 2018, n. 101, che hanno completamente cambiato il paradigma di conformità alla normativa privacy e che pertanto richiedono un grosso lavoro di analisi e di adeguamento;
- Misure di Sicurezza AgID che prevedono l'esecuzione di un'analisi dell'infrastruttura informatica al fine di garantire la conformità ai livelli previsti dall'AgID;
- Strategia Cloud Italia che prevede nuovi livelli di adeguamento per le infrastrutture digitali e per i servizi Cloud per la pubblica amministrazione, fino al completamento della migrazione dei servizi presso il PSN (Polo Strategico Nazionale) o altro Cloud Provider qualificato entro il 30 giugno 2026

6.3 Pianificazione dei servizi

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

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																								
L2.S17																								
L2.S21																								
L2.S22																								
L2.S23																								

Il Direttore U.O.C. Sistemi Informativi
Dott. Giuseppe Versace