Identificativo: Piano Operativo V1

Data: 21/02/2023

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

Piano Operativo

Comune di Napoli

Costituito

Raggruppamento Temporaneo di Imprese

composto da:

Deloitte Risk Advisory S.r.l.

EY Advisory S.p.A.

Teleco S.r.l.

Deloitte. EY teleco

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 21 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" nel quale l'RTI intende formulare la proposta tecnico/economica secondo le modalità tecniche ed i listini previsti nell'Accordo Quadro, in risposta al "Piano dei Fabbisogni" redatto dall'istituzione pubblica del Comune di Napoli.

1.2 Richieste dell'Amministrazione contraente

Il Comune di Napoli è l'istituzione pubblica che gestisce l'omonima città. Gli obiettivi strategici che il Comune di Napoli si pone mirano a rafforzare il sistema metropolitano in modo tale che accresca la propria intelligenza ed efficienza; lo scopo principale è infatti quello di migliorare la qualità della vita dei cittadini.

La Città di Napoli, come ogni Ente di medio-grandi dimensioni, si trova a fronteggiare ogni giorno decine di migliaia di attacchi informatici, per lo più automatici, ma talora anche mirati e preparati con competenza e risorse dedicate. Per questo motivo, nell'ambito di una transizione digitale volta a monitorare ed evolvere la postura cyber dell'ente, si è ritenuta necessaria un'attività di definizione del piano di lavoro con l'obiettivo di verificare lo stato di maturità corrente e sulla base del quale verrà poi definito un piano strategico in ambito Cyber indirizzato ad identificare le iniziative di breve-medio e lungo periodo per rafforzare la Cybersecurity Posture. L'intervento mira, infatti, a rafforzare la relazione tra il Comune di Napoli e i propri cittadini aumentando la sicurezza e la resilienza del Sistema Informativo della Città.

In attuazione di quanto, la procedura di gara ID 2296 bandita da Consip S.p.A. ai sensi dell'art. 54, comma 3, del D. lgs. n. 50/2016, suddivisa in 2 lotti, avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni, consente tramite l'adesione al **Lotto n.2**, aggiudicato al **RTI** è Deloitte Risk Advisory S.r.l. - EY Advisory S.p.A. - Teleco S.r.l, di fruire degli specifici servizi di:

- Servizio di Security Strategy - L2.S16
- Vulnerability Assessment - L2.S17
- Testing del codice Statico - L2.S18
- Supporto all'analisi e gestione degli incidenti - L2.S21
- Penetration Testing - L2.S22
- Servizio di Compliance normativa - L2.S23

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
PA	Pubblica Amministrazione

PAC	Pubblica Amministrazione Centrale
S.I.	Sistema Informativo
AGID	Agenzia per l'Italia Digitale
ICT	Information and Communications Technology
DLT R.A.	Deloitte Risk Advisory Srl
EY	EY Advisory SpA
Teleco	Teleco Srl

2 Anagrafica dell'amministrazione

DATI ANAGRAFICI DELL'AMMINISTRAZIONE	
Ragione sociale Amministrazione	Comune di Napoli
Indirizzo	Piazza Municipio - Palazzo San Giacomo
CAP	80133
Comune	Napoli
Provincia	Napoli
Regione	Campania
Codice Fiscale	80014890638
Indirizzo mail	
PEC	protocollo@pec.comune.napoli.it
Codice PA	c_f839
Comparto di Appartenenza (PAL/PAC)	PAL

DATI ANAGRAFICI REFERENTE DELL'AMMINISTRAZIONE	
Nome	Vincenzo
Cognome	Ferrara
Telefono	0817958800
Indirizzo mail	vincenzo.ferrara@comune.napoli.it
PEC	reti.tecnologiche@pec.napoli.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

4 Servizi richiesti e ambito di intervento

4.1 Ambiti di intervento

L'ambito funzionale di intervento per tale fornitura è da intendersi prevalentemente finalizzato a rafforzare il governo e la maturità di Sicurezza e Privacy di tutto l'ecosistema Comunale, ossia è volto a garantire la Riservatezza, l'Integrità e la Disponibilità del patrimonio informativo, con particolare riferimento ai dati personali, nel contesto della digitalizzazione dei servizi dell'ecosistema Comunale.

Nello specifico, gli ambiti di intervento oggetto di tale fornitura prevedono:

- di individuare le linee strategiche in materia di sicurezza ICT, di definire e monitorare le relative azioni strategiche adottate, al fine di realizzare un "progetto di sicurezza" unitario e coerente all'interno dell'ecosistema Comunale (L2.S16)
- di identificare 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)
- di identificare le vulnerabilità software (code review) all'interno del codice (sorgente o binario) delle applicazioni, delle applicazioni Web e mobile (L2.S18)
- di migliorare la gestione degli incidenti per incrementare efficacia ed efficienza dei processi di Incident Management (L2.S21)
- di eseguire attacchi simulati (penetration test) per verificare concretamente la possibilità di sfruttare vulnerabilità identificate su sistemi/reti/applicazioni/dispositivi (L2.S22)
- di garantire la corretta attuazione degli adempimenti del GDPR (General Data Protection Regulation - Regolamento UE 2016) applicato all'ambito del perimetro IT (L2.S23)

4.2 Servizi richiesti

SERVIZI RICHIESTI				
ID	**NOME SERVIZIO**	**VOCE DI COSTO**	**QUANTITA'**	**IMPORTO**
L2.S16	Security Strategy	L2.S16 - gg/p Team ottimale	1440	**360.000 €**
L2.S17	Vulnerability Assessment	L2.S17 – gg/p Team ottimale	224	**36.960 €**
L2.S18	Testing del codice Statico	L2.S18 - Singola esecuzione	20	**26.180 €**
L2.S21	Supporto all'analisi e gestione incidenti	L2.S21 - gg/p Team ottimale	100	**17.000 €**
L2.S22	Penetration Testing	L2.S22 - gg/p Team ottimale	140	**23.100 €**
L2.S23	Compliance normativa	L2.S23 - gg/p Team ottimale	285	**48.450 €**
			TOTALE	**511.690 €**

4.3 Dettaglio dei servizi richiesti

4.3.1 L2.S16 - Security Strategy

Descrizione e caratteristiche del servizio

Si riporta di seguito, a titolo esemplificativo e non esaustivo, una descrizione delle attività e dei deliverable richiesti all'interno del servizio. Il dettaglio degli interventi verrà di volta in volta definito con il Fornitore, in funzione del supporto richiesto dall'Amministrazione in considerazione delle azioni da attuare per la realizzazione del Progetto di Sicurezza, con conseguente revisione e/o integrazione dei deliverable.

Macro-attività	Attività	Deliverable
Analisi maturità e Piano strategico	Cyber Maturity volto all'attività di analisi di dettaglio delle procedure, processi, organizzazione ed alla consapevolezza delle capacità cyber Consolidamento del piano strategico delle iniziative tattiche	Piano di Sicurezza
Miglioramento della Security Governance	Miglioramento del modello di governo Cyber a livello organizzativo, procedurale, documentale e tecnologico con particolare riferimento agli ambiti gestione identità e degli accessi, analisi del rischio, audit, gestione delle terze parti, continuità operativa, gestione asset, hardening e patch management, data protection e loss prevention, sicurezza perimetrale, gestione dei log	Modello di Security Governance

Articolazione Dettagliata del Servizio di Security Strategy

Il servizio ha l'obiettivo di fornire al Comune il Piano Strategico in ambito Cybersecurity, che, a partire dagli obiettivi definiti nella propria strategia digitale, descriva le linee evolutive previste per la Sicurezza Informatica dell'Ente. L'acquisizione del servizio prevede l'esecuzione delle attività di seguito elencate:

Si riportano di seguito le attività principali:

- Assessment del livello di Maturità in ambito sicurezza dell'Ente ed identificazione dei principali punti di miglioramento e delle aree di intervento;
- Disegno/revisione del piano Strategico della sicurezza delle informazioni con indicazione dei servizi da attivare;
- Supporto al miglioramento del modello di governo Cyber a livello organizzativo, procedurale, documentale e tecnologico con particolare riferimento agli ambiti gestione identità e degli accessi, analisi del rischio, audit, gestione delle terze parti, continuità operativa, gestione asset, hardening e patch management, data protection e loss prevention, sicurezza perimetrale, gestione dei log.

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 di tipologia "progettuale (a corpo)" e che la metrica di misurazione è "*giorni/persona del team ottimale*".

Saranno definiti di concerto con l'Amministrazione i task progettuali e i deliverable delle attività, dimensionati e valorizzati economicamente. La avverrà sulla base dello stato dell'avanzamento lavori mensile, determinato coerentemente con il piano di lavoro definito, 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 e da remoto (es: presso le sedi del RTI).

Attivazione e durata

Si prevede l'avvio del servizio entro Marzo 2023 per una durata di 21 mesi.

Modalità di configurazione

N.A.

Specifiche di collaudo

N.A.

4.3.2 L2.S17 - Vulnerability assessment

Descrizione e caratteristiche del servizio

Si riporta di seguito, a titolo esemplificativo e non esaustivo, una descrizione delle attività e dei deliverable richiesti all'interno del servizio. Il dettaglio degli interventi verrà di volta in volta definito con il Fornitore, in funzione del supporto richiesto dall'Amministrazione in considerazione delle azioni da attuare per la realizzazione del Progetto di Sicurezza, con conseguente revisione e/o integrazione dei deliverable.

Macro-attività	Attività	Deliverable
Vulnerability Assessment	Pianificazione delle attività, Cyber Threat Intelligence, Esecuzione dei Vulnerability Assessment, Prioritizzazione delle vulnerabilità e verifica dei risultati, Re-test delle vulnerabilità a seguito del remediation plan	Executive Summary Technical Report Remediation Plan

Articolazione dettagliata del Servizio di Vulnerability Assessment

Il servizio di Vulnerability Assessment ha l'obiettivo di identificare in maniera proattiva, mediante una verifica dinamica della sicurezza, le vulnerabilità presenti su dispositivi di rete, software e applicazioni dell'Ente e la

mitigazione dei rischi cyber connessi. L'acquisizione del servizio prevede l'esecuzione delle attività di seguito elencate:

- Pianificazione: tale fase è fondamentale per la pianificazione delle attività di VA (tempistiche e orari di test) e per la raccolta delle informazioni necessarie all'esecuzione di verifiche di sicurezza efficaci;
- Esecuzione: in tale fase sono rilevate le vulnerabilità presenti per i target oggetto di analisi mediante tool automatizzati e tecniche manuali. I relativi risultati saranno analizzati e correlati dal Team operativo;
- Prioritizzazione delle vulnerabilità e verifica dei risultati: le vulnerabilità identificate dagli strumenti di analisi saranno classificate (grazie alle opportune configurazioni preliminari) inizialmente dagli stessi in maniera automatica in base al sistema di scoring CVSS. Successivamente saranno riviste in maniera critica dagli analisti per escludere i falsi positivi e fornire una migliore contestualizzazione per l'Ente. Per ogni vulnerabilità identificata saranno fornite raccomandazioni sulle azioni da intraprendere per la loro risoluzione o mitigazione, con anche indicazione delle priorità da attribuire sempre in coerenza con le policy dell'Ente e del livello di criticità/rischio precedentemente determinato. Queste saranno riportate all'interno di un piano di rientro concreto e applicabile al contesto (con indicazione anche delle tempistiche di risoluzione condivise con l'Ente) in grado di supportare le linee tecniche dell'Ente nella risoluzione. I risultati delle attività di VA e le raccomandazioni fornite saranno riportate in specifici report: Executive Summary, Technical Report e Remediation Plan;
- Re-test delle vulnerabilità: successivamente all'esecuzione delle azioni di rimedio delle vulnerabilità identificate, riportate all'interno del piano di rientro, potranno essere pianificate e svolte attività di re-test per verificare in maniera efficace la risoluzione delle vulnerabilità sui target analizzati e la mitigazione dei rischi connessi.

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 di tipologia "progettuale (a corpo)" e che la metrica di misurazione è "*giorni/persona del team ottimale*".

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

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 saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

Attivazione e durata

Si prevede l'avvio del servizio entro Marzo 2023 per una durata di 21 mesi.

Modalità di configurazione

N.A

Specifiche di collaudo

N.A.

4.3.3 L2.S18 – Testing del codice statico

Descrizione e caratteristiche del servizio

Si riporta di seguito, a titolo esemplificativo e non esaustivo, una descrizione delle attività e dei deliverable richiesti all'interno del servizio. Il dettaglio degli interventi verrà di volta in volta definito con il Fornitore, in funzione del supporto richiesto dall'Amministrazione in considerazione delle azioni da attuare per la realizzazione del Progetto di Sicurezza, con conseguente revisione e/o integrazione dei deliverable.

Macro-attività	Attività	Deliverable
Analisi statistica del codice (SAST)	Analisi del contest (es. Analisi funzionale, workflow dell'applicazione, lista funzionalità, librerie terze parti utilizzate, architettura tecnica, acquisizione del codice sorgente), Secure Code Review, Reporting	Executive Summary Technical Report Remediation Plan

Articolazione dettagliata del Servizio di Testing del Codice Statico

Il servizio di Testing del Codice prevede la rilevazione in maniera proattiva delle vulnerabilità presenti nel codice degli applicativi oggetto di analisi.

Si riportano di seguito le attività principali:

- Analisi del contesto: in tale fase si procede con la richiesta, raccolta e analisi della documentazione tecnica dell'applicazione (analisi funzionale, workflow dell'applicazione, lista funzionalità, librerie terze parti utilizzate, architettura tecnica, ecc.) e con l'acquisizione del codice sorgente;
- Secure Code Review: esecuzione dell'analisi statica del codice sorgente dell'applicazione. Nello specifico verranno eseguite le seguenti attività:
  - Configurazione dei tool di analisi necessari per l'esecuzione delle attività sulla base delle caratteristiche del codice sorgente in ambito (es. linguaggio di programmazione)
  - Code Scanning;
  - Verifica manuale delle evidenze fornite dai tool di scansione (manual code review) per la rilevazione ed eliminazione efficace dei falsi positivi ed identificazione di vulnerabilità di sicurezza per le funzionalità critiche;
  - Assegnazione del livello di criticità alle vulnerabilità rilevate in base alla probabilità di sfruttamento e del relativo impatto;
  - Correlazione delle informazioni, identificazione azioni di rimedio, prioritizzazione e definizione del remediation plan;

- Reporting: predisposizione di report e dashboard con l'obiettivo di fornire una chiara visione sui risultati e focalizzare l'attenzione sulla prioritizzazione delle vulnerabilità tecniche rilevate.

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

- "singola esecuzione", nel caso in cui il servizio sia erogato per unica scansione (one time);
- "numero di applicazioni/anno", nel caso della Fascia 1, Fascia 2 e Fascia 3;
- "canone annuale", nel caso in cui il servizio sia erogato in modalità continua (scansioni periodiche);

e che la metrica di misurazione è "*Numero di applicazioni*".

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.

Le attività saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

Attivazione e durata

Si prevede l'avvio del servizio entro Marzo 2023 per una durata di 21 mesi.

Modalità di configurazione

N.A

Specifiche di collaudo

N.A

4.3.4 L2.S21 - Supporto all'analisi e gestione degli incidenti

Descrizione e caratteristiche del servizio

Si riporta di seguito, a titolo esemplificativo e non esaustivo, una descrizione delle attività e dei deliverable richiesti all'interno del servizio. Il dettaglio degli interventi verrà di volta in volta definito con il Fornitore, in funzione del supporto richiesto dall'Amministrazione in considerazione delle azioni da attuare per la realizzazione del Progetto di Sicurezza, con conseguente revisione e/o integrazione dei deliverable.

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

Articolazione dettagliata del Supporto all'analisi e gestione degli incidenti

Il servizio ha l'obiettivo di fornire al Comune il piano di risposta agli incidenti e il modello per la ripartenza dei servizi. L'acquisizione del servizio prevede l'esecuzione delle attività di seguito elencate:

- Assessment finalizzato all'identificazione degli asset e dei servizi critici dell'organizzazione;
- Definizione dei playbook di risposta agli incidenti;
- Definizione del processo di Crisis Management.

A supporto dell'esecuzione delle attività, si renderanno disponibili le competenze necessarie al fine di valutare le informazioni utili e necessarie per l'erogazione dei servizi, ad esempio i repository documentali, le azioni di formazione e sensibilizzazione, la gestione dei requisiti normativi, organizzativi, procedurali e tecnologici.

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 di tipologia "progettuale (a corpo)" e che la metrica di misurazione è "*giorni/persona del team ottimale*".

Saranno definiti di concerto con l'Amministrazione i task progettuali e i deliverable delle attività, dimensionati e valorizzati economicamente. La fatturazione avverrà sulla base dello stato dell'avanzamento lavori mensile, determinato coerentemente con il piano di lavoro definito, e sarà riconosciuta bimestralmente.

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 saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

Attivazione e durata

Si prevede l'avvio del servizio entro Luglio 2023 per una durata di 3 mesi.

Modalità di configurazione

N.A

Specifiche di collaudo

N.A.

4.3.4 L2.S22 – Penetration Testing

Descrizione e caratteristiche del servizio

Si riporta di seguito, a titolo esemplificativo e non esaustivo, una descrizione delle attività e dei deliverable richiesti all'interno del servizio. Il dettaglio degli interventi verrà di volta in volta definito con il Fornitore, in funzione del supporto richiesto dall'Amministrazione in considerazione delle azioni da attuare per la realizzazione del Progetto di Sicurezza, con conseguente revisione e/o integrazione dei deliverable.

Macro-attività	Attività	Deliverable
Penetration test su infrastrutture e applicazioni	Planning and Preparation, Information Gathering, Service scanning, Post-exploitation, Reporting	Executive Summary Technical Report Remediation Plan

Articolazione dettagliata del Servizio di Penetration Testing

Il servizio di Penetration Testing ha l'obiettivo di verificare concretamente la possibilità di sfruttare le eventuali vulnerabilità identificate su sistemi/reti/applicazioni/dispositivi dell'Amministrazione. L'acquisizione del servizio prevede l'esecuzione delle attività di seguito elencate:

- Planning and Preparation: a seguito della richiesta dell'Amministrazione per esecuzione di PT, sarà pianificato ed eseguito un Kick Off meeting dove verranno discussi gli aspetti preliminari per l'esecuzione delle attività, con particolare focus sul perimetro dell'attività (target in scope e criticità degli stessi), sui vincoli operativi e sulle regole d'ingaggio. La presente fase infine prevede l'installazione e/o la configurazione degli strumenti hardware e software necessari per l'esecuzione delle analisi;
- Information Gathering: sarà effettuata l'acquisizione delle informazioni esposte dagli applicativi e dai sistemi che li ospitano al fine di contestualizzare gli attacchi da portare a termine;
- Service scanning: in questa fase sarà effettuata una scansione automatica delle vulnerabilità. I risultati saranno revisionati manualmente per individuare i servizi su cui effettuare attacchi mirati e contestualmente si procederà all'eventuale personalizzazione degli exploit necessari allo sfruttamento delle vulnerabilità;
- Exploitation: in base alla tipologia di PT, saranno eseguiti una serie di attacchi finalizzati allo sfruttamento delle possibili vulnerabilità identificate.

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 di tipologia "progettuale (a corpo)" e che la metrica di misurazione è "*giorni/persona*".

Saranno definiti di concerto con l'Amministrazione i task progettuali e i deliverable delle attività, dimensionati e valorizzati economicamente. La fatturazione avverrà sulla base dello stato dell'avanzamento lavori mensile determinato coerentemente con il piano di lavoro definito e sarà riconosciuta bimestralmente.

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 saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

Attivazione e durata

Si prevede l'avvio del servizio entro Marzo 2023 per una durata di 21 mesi.

Modalità di configurazione

N.A.

Specifiche di collaudo

N.A.

4.3.4 L2.S23 – Compliance normativa

Descrizione e caratteristiche del servizio

Si riporta di seguito, a titolo esemplificativo e non esaustivo, una descrizione delle attività e dei deliverable richieste all'interno del servizio. Il dettaglio degli interventi verrà di volta in volta definito con il Fornitore, in funzione del supporto richiesto dall'Amministrazione in considerazione delle azioni da attuare per la realizzazione del Progetto di Sicurezza, con conseguente revisione e/o integrazione dei deliverable.

Macro-attività	Attività	Deliverable
Governo della Conformità Privacy	Consolidamento del livello di compliance normativa in ambito Privacy mediante revisione dei processi e delle procedure in ambito Data Breach, Gestione interessati, Privacy By Design, DPIA, Privacy Policy, revisione del registro dei trattamenti, esecuzione di DPIA per i trattamenti ritenuti critici	Set documentale in ambito privacy Scheda censimento e registri dei trattamenti Report DPIA

Articolazione dettagliata del Servizio di Compliance normativa

Il servizio di Compliance normativa prevede il supporto dell'Ente nell'esecuzione delle attività di seguito elencate:

- Revisione dei processi e del corpo documentale nei seguenti ambiti:
  - gestione delle richieste dei soggetti interessati nonché dei modelli di risposta alle richieste con i relativi strumenti/pratiche IT/Sicurezza (es. individuazione dei dati, portabilità, cancellazione) a supporto;
  - processo di Privacy by Design, incluse le misure tecniche IT/Sicurezza ed organizzative necessarie per assicurare che siano trattati, fin dalla progettazione e per impostazione predefinita, solo i dati necessari per ogni specifica finalità di trattamento nel rispetto del principio di minimizzazione, e processo di DPIA, per assicurare una valutazione corretta delle attività di trattamento al fine di identificare eventuali criticità che necessitino sottoposizione a Data Protection Impact Assessment;
  - Data Breach, al fine di definire processi, modelli standard e strumenti (Notification Criteria workflow) per la valutazione dell'impatto di un eventuale Data Breach e per la gestione dell'eventuale notifica all'Autorità Garante o la comunicazione ai soggetti interessati;
  - Relazione di un documento di privacy policy mediante cui definire ad alto livello i criteri di compliance normativa di cui l'ente deve dotarsi.
- Supporto alla revisione e all' aggiornamento del registro dei trattamenti in uso presso l'ente;
- Supporto per l'esecuzione di Data Protection Impact Assessment (DPIA) sui trattamenti ritenuti critici.

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 di tipologia "progettuale (a corpo)" e che la metrica di misurazione è "*giorni/persona*".

Saranno definiti di concerto con l'Amministrazione i task progettuali e i deliverable delle attività, dimensionati e valorizzati economicamente. La fatturazione avverrà sulla base dello stato dell'avanzamento lavori mensile determinato coerentemente con il piano di lavoro definito e sarà riconosciuta bimestralmente.

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 saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

Attivazione e durata

Si prevede l'avvio del servizio entro Marzo 2023 per una durata di 6 mesi.

Modalità di configurazione

N.A.

Specifiche di collaudo

N.A.

5 Organizzazione e modalità di erogazione del contratto esecutivo

5.1 Attività in carico alle aziende del RTI

Nell'ambito della specifica fornitura le attività saranno svolte dalle aziende secondo la ripartizione seguente:

SERVIZIO	Deloitte Risk Advisory (39,38 %)	EY Advisory (60,62 %)	Teleco (0%)
L2.S16	27,29%	72,71%	0 %
L2.S17	100,00 %	0,00 %	0 %
L2.S18	100,00 %	0,00 %	0 %
L2.S21	100,00 %	0,00 %	0 %
L2.S22	100,00 %	0,00 %	0 %
L2.S23	0,00 %	100,00 %	0 %
TOTALE	39,38 %	60,62 %	0 %

5.2 Modalità di ricorso al subappalto da parte del fornitore

SERVIZIO	AZIENDA RTI	QUOTA SUBAPPALTABILE	SUBAPPALTATORE
L2.S16, L2.S17, L2.S18, L2.S21, L2.S22, L2.S23	**DLT R.A.- EY-TELECO**	**50%**	**DA DEFINIRE**

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	Rodolfo Mecozzi
Referente Tecnico CE (RT)	Marco Ceccon
Responsabile Attività L2.S16	Federico Di Vivo
Responsabile Attività L2.S17	Marco Ceccon
Responsabile Attività L2.S18	Marco Ceccon
Responsabile Attività L2.S21	Marco Ceccon
Responsabile Attività L2.S22	Marco Ceccon
Responsabile Attività L2.S23	Federico Di Vivo

5.4 Modalità di esecuzione dei servizi

Le attività relative all'esecuzione dei servizi saranno svolte presso gli uffici del Fornitore e, ove necessario e/o richiesto per l'espletamento delle attività contrattuali, presso l'Amministrazione, nel rispetto della normativa sanitaria.

6 Piano di lavoro

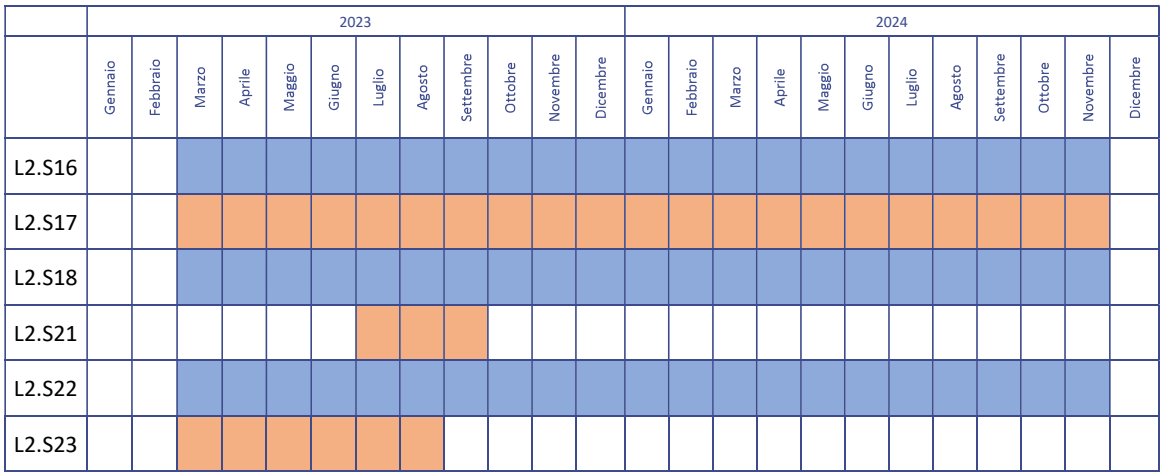
6.1 Piano di Presa in carico

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
Pianificazione	Pianificazione delle attività					
Predisposizione Strumenti	Predisposizione e aggiornamento strumenti					
Assessment documentale	Analisi AS IS dei progetti in corso					
Acquisizione competenze	Incontri con il personale dell'Amministrazione e del fornitore uscente, training on the job, self training, workshop					
Ottimizzazione	Individuazione delle possibili aree di miglioramento					
Fine presa in carico	Ricognizione e verifica delle attività svolte					
Governance	Verifica dello stato delle attività					

6.2 Cronoprogramma, copia pianificazione

Di seguito si riporta la pianificazione di massima dei servizi previsti:



Le milestone e i deliverable specifici relativi a ciascuna delle attività verranno preventivamente concordate con l'amministrazione.

6.3 Data di attivazione e durata del servizio

Il contratto esecutivo avrà i suoi effetti dalla data di stipula, avrà una durata di **21 mesi** dalla data di attivazione dei servizi, compatibilmente con il vincolo definito dall'Accordo quadro, ovvero che i Contratti Esecutivi abbiano una durata massima pari alla durata residua, al momento della sua stipula, dell'Accordo Quadro, e terminerà entro e non oltre il **24 Novembre 2024**.

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 di ciascun servizio.

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.
Security Solution Architect	Figura professionale dedicata al mantenimento della sicurezza del sistema informatico di un'organizzazione. Sarà responsabile dell'analisi dell'infrastruttura IT e delle relazioni tra i differenti sistemi e componenti infrastrutturali volta all'individuazione di problematiche architetturali che ne potrebbero compromettere la sicurezza.

	Si occuperà, inoltre, dell'analisi delle configurazioni e delle regole tecniche delle principali soluzioni di sicurezza utilizzate per proteggere l'infrastruttura e i servizi (Firewall, IPS/IDS, SIEM, soluzioni anti-malware, Web Application Firewall, Database Monitoring, servizi Anti-DDoS, servizi cloud oriented per la sicurezza).
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.

Vulnerability Assessment (L2.S17)

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 Penetration tester	Definito anche ethical hacker, tenta di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza rispettando opportune regole concordate in fase di ingaggio. Responsabile del coordinamento delle figure più Junior.
Junior Penetration tester	Definito anche ethical hacker, tenta di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza rispettando opportune regole concordate in fase di ingaggio

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.

Testing del codice - statico (L2.S18)

Il dimensionamento a canone di tale servizio non prevede un team ottimale, come invece previsto per i rimanenti servizi a dimensionamento progettuale oggetto del presente Piano.
Con riferimento ai profili professionali che prevediamo di coinvolgere nell'erogazione delle attività, il team sarà composto dalle seguenti figure con le relative responsabilità assegnate:

Profilo	Responsabilità
Senior Penetration tester	Effettua le attività di analisi statica del codice sorgente o delle configurazioni di sistema. Responsabile del coordinamento delle figure più Junior.
Junior Penetration tester	Partecipa all'analisi statica del codice sorgente o delle configurazioni di sistema.

Supporto all'analisi e gestione degli incidenti (L2.S21)

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 Security Analyst	Gestisce l'esame periodico della sicurezza di sistemi, reti e applicazioni evidenziando le vulnerabilità tecniche nonché gli eventuali scostamenti rilevati rispetto e regole interne, normative esterne e best practices internazionali in materia Responsabile del coordinamento delle figure più Junior.
Junior Security Analyst	Gestisce l'esame periodico della sicurezza di sistemi, reti e applicazioni evidenziando le vulnerabilità tecniche nonché gli eventuali scostamenti rilevati rispetto e regole interne, normative esterne e best practices internazionali in materia.
Forensic Expert	E' chiamato a gestire la raccolta di evidenze e l'analisi delle stesse in concomitanza di un incidente relativo alla sicurezza delle informazioni documentando il tutto in modo che sia correttamente presentabile in sede processuale.

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.

Penetration Testing (L2.S22)

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 Penetration tester	Definito anche ethical hacker, tenta di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza rispettando opportune regole concordate in fase di ingaggio. Responsabile del coordinamento delle figure più Junior.
Junior Penetration tester	Definito anche ethical hacker, tenta di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza rispettando opportune regole concordate in fase di ingaggio
Forensic Expert	E' chiamato a gestire la raccolta di evidenze e l'analisi delle stesse in concomitanza di un incidente relativo alla sicurezza delle informazioni documentando il tutto in modo che sia correttamente presentabile in sede processuale.

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.

Compliance normativa (L2.S23)

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.
Junior Information Security Consultant	Contribuisce nell'attuazione della strategia definita all'interno del suo ambito di responsabilità (sia questo un progetto, un processo, una location) partecipando al ruolo di 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.

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 (a livello nazionale ed europeo) e gli input esogeni ed endogeni, per definire - attraverso l'ausilio di metodologie, approcci operativi e strumenti - il PdS. Il PdS, 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 (i.e. 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:

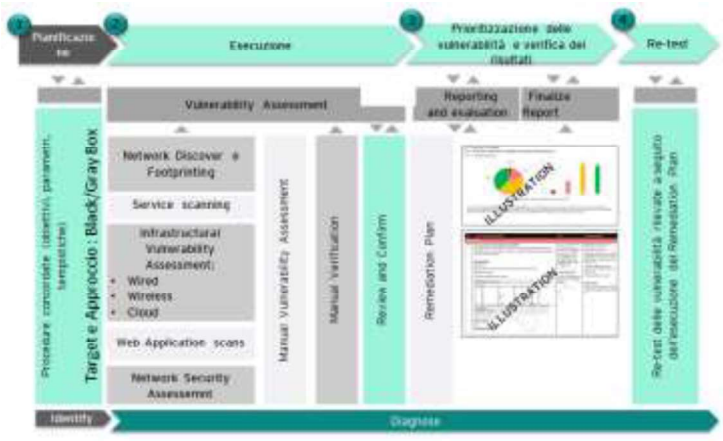
- Identify: strategia e pianificazione, Governance Asset e Processi, gestione del rischio cyber, security assurance (VA, PT, Testing del Codice), sicurezza terze parti e contratti di servizio, Compliance normativa;
- Protect (Management): Information & Data Security, Identity & Access Management, Security 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.

Vulnerability Assessment (L2.S17)

Il servizio di Vulnerability Assessment prevede l'identificazione in maniera proattiva, mediante una verifica dinamica della sicurezza, delle vulnerabilità presenti su dispositivi di rete, software e applicazioni delle Amministrazioni e la mitigazione dei rischi cyber connessi. Il RTI eroga le attività in ambito al presente servizio facendo affidamento sugli elementi distintivi sotto riportati.

1. Standardizzazione del reporting e dei piani di prioritizzazione/remediation attraverso l'utilizzo di una piattaforma centralizzata (denominata Bug Blast) ed indipendente dai motori di scansione (vulnerability scanner), garantendo ripetibilità ed uniformità dei risultati;
2. Metodologia per la definizione dei "remediation plan" con approccio risk-based e reportistica in grado di rappresentare le vulnerabilità identificate sia ad interlocutori executive che tecnici, fornendo pratici strumenti operativi per agevolare la risoluzione delle stesse;
3. Centri di eccellenza nazionali ed internazionali in ambito Cybersecurity (Roma, Milano, Bari, ed oltre 10 in EU), con la presenza di laboratori specialistici e con professionalità verticali su attività di Offensive Security. Tali centri supportano i team nella raccolta di informazioni relative a nuove vulnerabilità (es. mediante tecniche di Cyber Threat Intelligence) e tecniche innovative per lo sfruttamento delle stesse;
4. Eterogeneità nella copertura degli ambienti target (IT/OT/IoT/Cloud) attraverso strumenti e tecniche idonee e specifiche a garantire il discovery per ciascuna tipologia di target;
5. Ampio supporto nel discovery di misconfiguration e vulnerability specifiche per gli ambienti di cloud computing (IaaS, PaaS, SaaS), anche in presenza di CSP differenti (AWS, Azure, Google, ecc.).

Le attività di Vulnerability Assessment (VA) forniranno evidenze di dettaglio sulle vulnerabilità riconducibili all'infrastruttura ICT e IoT/OT (, funzionali anche ad elaborare una baseline iniziale del livello di vulnerabilità e di esposizione del sistema informativo dell'Amministrazione. L'attività sarà svolta sia con strumenti automatici sia con strumenti definiti ad-hoc sulla base della tipologia del target oggetto di analisi. Il RTI, sulla base della propria esperienza e del contesto di riferimento in cui saranno svolte le analisi di sicurezza, proporrà gli strumenti di analisi più adatti per l'esecuzione dei VA. Le attività di VA eseguite sono basate sulle metodologie OSSTMM, OWASP, PTES, NIST 800-52/53 e ISA 62443, riconosciute globalmente come standard de-facto.



L'applicazione di tali metodologie garantirà risultati coerenti, ripetibili e misurabili. Nell'ambito delle attività di VA terremo in considerazione il sempre più diffuso utilizzo delle tecnologie Cloud da parte delle Amministrazione, in coerenza con quanto definito dalla Strategia Cloud Italia. A tal fine, su specifica richiesta dell'Amministrazione, il RTI è in grado di integrare all'interno dei servizi offerti anche l'esecuzione di attività di Assessment del livello di sicurezza dei servizi Cloud IaaS e SaaS, verificandone la compliance rispetto a standard, requisiti normativi e best practice di settore, e ricercando vulnerabilità celate negli errori di configurazione dei diversi ambienti cloud. Il RTI potrà eseguire le attività di VA in maniera periodica ove richiesto e ritenuto opportuno.
Per l'esecuzione dei servizi richiesti dall'Amministrazione, la metodologia prevede l'esecuzione di 4 fasi progettuali:

- Pianificazione delle attività,
- Esecuzione dei Vulnerability Assessment,
- Proritizzazione delle vulnerabilità e verifica dei risultati,
- Re-test delle vulnerabilità a seguito del remediation plan.

Il RTI propone l'adozione di una piattaforma specifica per l'esecuzione di attività di Vulnerability Assessment. La Piattaforma Bug Blast ha l'obiettivo di fornire report personalizzati e di tracciare le vulnerabilità dalla fase di discovery e per tutte le fasi di remediation. Le informazioni che afferiscono alle attività di VA richieste saranno disponibili nel portale tramite un sistema di autorizzazione granulare e le Amministrazioni potrà accedere a tali informazioni sulla base del periodo di retention che sarà concordato di volta in volta con le stesse e comunque, salvo diversa indicazione da parte dell'Amministrazione e nel rispetto delle normative vigenti, per un periodo garantito non inferiore a 1 mese dalla fine delle attività. Tale modalità di erogazione è consigliata dal RTI, che tuttavia è disponibile ad adattare la stessa sulla base di eventuali esigenze delle Amministrazioni, concordandole di volta in volta con le stesse. Approccio operativo. L'approccio operativo proposto dal RTI prevede l'esecuzione di tutte le attività tecniche previste dal CTS. I relativi risultati saranno analizzati e correlati dal Team operativo. Ove possibile, per le vulnerabilità rilevate sarà effettuata una verifica manuale al fine di identificare ed eliminare i falsi positivi; tale attività è svolta mediante processi innovativi di controllo, sviluppati nel corso delle esperienze in ambito Offensive Security e tramite il supporto dei Centri di eccellenza del RTI, che consentono di ridurre al minimo la presenza di errori.

Di seguito sono riportati i principali strumenti/soluzioni tecnologiche che saranno utilizzati per l'erogazione del servizio:

Ambito di utilizzo	Principali strumenti
Vulnerability Assessment	● **Open Source**: Kali Linux, nmap, netdiscovery, dnsrecon, dig, metasploit, netcat, masscan, Shodan, Zoomeye, Censys, Air-Ng tools, Wifite, Airgeddon, Wireshark. ● **Di Mercato**: Nessus, Hak5 WiFi, Burp Proxy Professional. ● **Proprietario**: Bug Blast
Cloud Security Assessment	● **Di Mercato**: Cloud Security Posture Management (CSPM), SaaS Security Posture Management (SSPM)
Vulnerability Assessment IoT	● **Open Source**: Blue Scanner, Blue Sniff, BlueBugger, BTBrowser, BTCrawler, BlueSnarfing, HackRF (HW), ZigDiggity, Proxmark (HW), TLSAssistant. ● **Di Mercato**: Burp Proxy Professional

Testing del codice statico (L2.S18)

Il servizio di Testing del Codice prevede la rilevazione in maniera proattiva delle vulnerabilità presenti nel codice degli applicativi oggetto di analisi. Il RTI si impegna ad erogare le attività nel rispetto dei requisiti tecnico-funzionali specificati nel CTS, facendo affidamento sugli elementi distintivi sotto riportati:

1. Adozione di una piattaforma SAST proprietaria, specifica per l'acquisizione del codice e l'interazione con gli utenti finali, assicurando la generazione di report standardizzati, confrontabili e soprattutto agnostici rispetto ai software di scansione adottati (motori di scansione)
2. Metodologia per la definizione dei "remediation plan" con approccio risk-based e reportistica in grado di rappresentare le vulnerabilità identificate sia ad interlocutori executive che tecnici, fornendo pratici strumenti operativi per agevolare la risoluzione delle stesse
3. Molteplici Centri di eccellenza sulla Sicurezza Applicativa e DevSecOps, con la presenza di laboratori specialistici sulle attività di analisi statica (SAST) e dinamica (DAST) che analizzano costantemente le nuove tecniche di sfruttamento delle vulnerabilità con accesso ai più aggiornati dati di riferimento sulle stesse (es. Cyber Threat Intelligence e database con TTP utilizzate negli attacchi, segnalazione di API/librerie di terze parti vulnerabili)
4. Alleanze strategiche con i principali produttori mondiali di tecnologia per l'analisi statica/dinamica del codice assicurando l'accesso privilegiato alle risorse tecniche degli stessi.

L'analisi statica del codice (SAST) mira ad identificare le vulnerabilità presenti nel codice sorgente. Tale attività è svolta in modalità white-box, richiedendo all'Amministrazione sia il codice sorgente dell'applicazione che la documentazione tecnica della stessa. Le attività sono eseguite principalmente sulla base dello standard OWASP Top 10 e tramite le seguenti tre fasi progettuali:

FASE 1 - ANALISI DEL CONTESTO: in tale fase si procede con la richiesta, raccolta e analisi della documentazione tecnica dell'applicazione (*analisi funzionale, workflow dell'applicazione, lista funzionalità, librerie terze parti utilizzate, architettura tecnica, ecc.)* e con l'acquisizione del codice sorgente

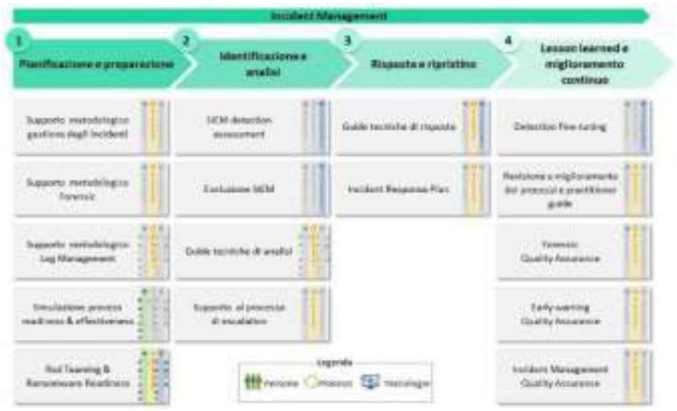
FASE 2 – SECURE CODE REVIEW: esecuzione dell'analisi statica del codice sorgente dell'applicazione, ovvero:

- Configurazione dei tool di analisi necessari per l'esecuzione delle attività sulla base delle caratteristiche del codice sorgente in ambito (es. linguaggio di programmazione)
- Code Scanning mediante l'utilizzo di tool messi a disposizione dal RTI e selezionati sulla base delle caratteristiche dell'applicazione (es: linguaggio) ed in considerazione della complessità/criticità degli asset in oggetto. Gli strumenti che saranno messi a disposizione garantiranno la copertura di più di 20 linguaggi di programmazione e copriranno le vulnerabilità attualmente conosciute;
- Verifica manuale delle evidenze fornite dai tool di scansione (manual code review) per la rilevazione ed eliminazione efficace dei falsi positivi ed identificazione di vulnerabilità di sicurezza per le funzionalità critiche;
- Assegnazione del livello di criticità alle vulnerabilità rilevate in base alla probabilità di sfruttamento e del relativo impatto. L'assegnazione del livello di severità è fornita in primo luogo in maniera automatica dagli strumenti di analisi e rivisto dagli analisti di sicurezza. Il livello di severità è assegnato sulla base delle leading practice, delle policy di sicurezza dell'Amministrazione e di ulteriori fattori rilevanti (es. criticità dell'asset, rilevanza asset in ambito GDPR, facilità di sfruttamento della vulnerabilità, impatto della vulnerabilità, informazioni di CTI provenienti dai centri di eccellenza);
- Correlazione delle informazioni, identificazione azioni di rimedio, prioritizzazione e definizione del remediation plan. Le attività SAST di scansione periodica seguiranno un piano di verifica concordato con l'Amministrazione secondo modalità e tempistiche definite, come ad esempio a seguito di major-change e/o mediante integrazione con i repository dell'Amministrazione (integrazione con pipeline CI/CD). L'esecuzione periodica delle attività consente il monitoraggio efficace dello stato di risoluzione delle vulnerabilità

FASE 3 – REPORTING: predisposizione di report e dashboard con l'obiettivo di fornire una chiara visione sui risultati SAST e focalizzare l'attenzione sulla prioritizzazione delle vulnerabilità tecniche rilevate. Nello specifico sarà predisposto un Executive Summary e un Technical Report per singola esecuzione, evidenziando in maniera puntuale anche le aree di miglioramento.

Supporto all'analisi e gestione degli incidenti (L2.S21)

Il servizio di supporto all'analisi e gestione degli incidenti prevede lo svolgimento da parte del RTI di attività consulenziali volte a incrementare efficacia ed efficienza dei processi di Forensic e Incident Management, nelle fasi di analisi, progettazione e verifica (post-mortem) di tali processi, nonché di supporto alla divulgazione delle informazioni. Il RTI si impegna ad erogare le attività in ambito nel rispetto dei requisiti tecnico-funzionali specificati nel CTS, facendo affidamento sugli elementi distintivi elencati di seguito:



1. Coinvolgimento di risorse con ampia e riconosciuta esperienza nella realizzazione di CERT e SOC in Italia e nel mondo per organizzazioni pubbliche e private di primaria importanza. Il RTI ha inoltre supportato 7 delle 11 organizzazioni italiane che hanno accreditato i loro CERT alla community internazionale FIRST
2. Coinvolgimento di risorse che hanno contribuito direttamente allo sviluppo delle pratiche di Incident Readiness come dimostrato dalla pubblicazione di numerosi studi nazionali e internazionali.
3. Disponibilità di una libreria proprietaria composta da oltre 350 Use Case di monitoraggio costantemente aggiornata sulla base delle esperienze acquisite presso i clienti del network a livello globale, evoluzioni tecnologiche, trasformazioni nelle tattiche, tecniche e procedure (TTP) utilizzate dagli attori di minaccia in diverse tipologie di ambienti (es. cloud SaaS, PaaS e IaaS, Mobile, IoT, ecc.)
4. Disponibilità di framework proprietari, sviluppati internamente dal RTI e aggiornati in maniera continuativa sulla base delle esperienze acquisite e di report specialistici di settore, per la valutazione del livello di maturità di CERT e SOC e l'identificazione delle tecnologie di sicurezza a supporto delle attività di gestione degli incidenti
5. Team di lavoro multidisciplinare altamente qualificato e certificato in ambito Forensic, Security Defense e Offense.

Il servizio di supporto all'analisi e gestione degli incidenti proposto affronta la tematica in modo olistico e multidisciplinare. Al fine di raggiungere tali obiettivi, il RTI supporta l'Amministrazione al fine di abilitare il corretto svolgimento di ciascuna delle fasi di gestione degli incidenti attraverso attività consulenziali da svolgersi in maniera preventiva come supporto all'intero processo (analisi e progettazione) e definire un processo strutturato di Forensic e verificarne l'efficacia (verifica).

A) Incident Management

Il RTI propone un approccio strutturato al supporto in ambito gestione incidenti, che prevede l'esecuzione di attività di natura consulenziale da svolgersi preventivamente per guidare il corretto svolgimento del servizio di Incident Management da parte dell'Amministrazione. Ciascuna delle attività proposte consentirà di abilitare lo svolgimento e incrementare l'efficacia di una diversa fase del processo di Incident Management, come di seguito riportato:

- A.1 Pianificazione e preparazione: una fase di preparazione correttamente eseguita e personalizzata sulla base del contesto permette di minimizzare gli impatti degli incidenti, facendo leva su un'adeguata infrastruttura tecnologica di sicurezza e personale specializzato.

- A.2 Identificazione e analisi: la fase di identificazione e analisi di un incidente ha l'obiettivo di monitorare in modo centralizzato gli eventi di sicurezza provenienti da fonti strutturate (es. SIEM) e non strutturate (es. e-mail da utenti) per rilevare minacce miranti agli asset e ai servizi della PA, analizzarli per comprendere se si tratti di un falso positivo che necessita di azioni correttive o di un incidente con potenziale impatto sul perimetro e classificare e prioritizzarne la gestione sulla base di criteri definiti.
- A.3 Risposta e ripristino: tale fase prevede l'identificazione e l'implementazione delle azioni di contenimento a breve termine dell'incidente, con l'obiettivo di limitare le conseguenze dell'incidente e ripristinare la normale operatività in maniera tempestiva ed efficace.
- A.4 Lesson learned e miglioramento continuo: tale fase prevede, immediatamente a valle della gestione di un incidente, una valutazione ex-post della stessa per verificare che le attività siano state condotte in conformità con quanto previsto dal processo, e un'attività periodica volta a identificare eventuali punti di miglioramento nelle attività svolte attraverso l'elaborazione di reportistica, lo svolgimento di meeting ricorrenti per condividere eventuali gap e relative azioni di rimedio.

B) Forensic

Le attività di supporto all'Amministrazione nella gestione di incidenti di sicurezza prevedono un approccio sinergico, finalizzato a incrementare l'efficienza delle modalità di intervento e dei tempi di reazione da parte dell'Amministrazione, in particolare nell'analisi forense post-mortem degli incidenti.

Le attività di supporto erogate nei confronti dell'Amministrazione prevedranno una costante verifica di quality assurance da parte di profili esperti, al fine di garantire un elevato livello qualitativo dell'esecuzione del processo di Forensic.

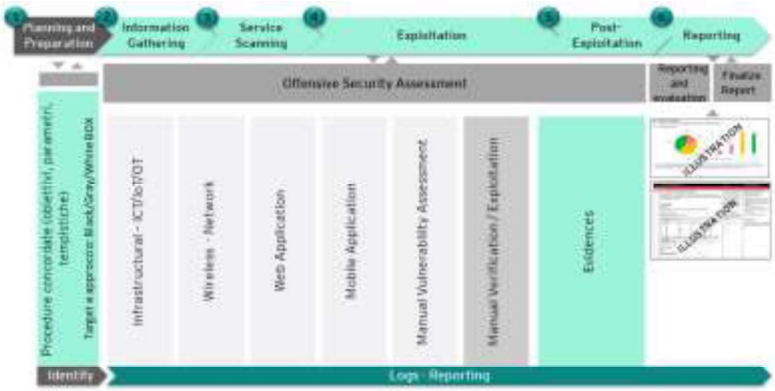
- Definizione di un template di catena di custodia per supportare i team di Forensic nel tracciamento delle attività eseguite sulle evidenze acquisite;
- Definizione di un processo di Forensic secondo best practice volto a definire ruoli, responsabilità, principi e attività operative che regolano il processo stesso;
- Governo (organizzazione, pianificazione, coordinamento, controllo) delle attività di verifica tecnica (quality assurance) del processo di Forensic.

Penetration Testing (L2.S22)

Il servizio di Penetration Test prevede l'esecuzione di attacchi simulati per verificare concretamente la possibilità di sfruttare vulnerabilità identificate su sistemi/reti/applicazioni/dispositivi delle Amministrazioni. L'approccio offensivo consente di ottenere una chiara percezione degli effettivi livelli di esposizione/compromissione dei target analizzati, determinando la capacità di difesa e resilienza rispetto agli attacchi Cyber e fornendo conseguentemente elementi concreti per adeguare le misure di contrasto e protezione. Il servizio proposto è fondato sugli elementi distintivi sotto riportati:

1. Eccellenza del team di Ethical Hacking dimostrata dalla pubblicazione regolare di Common Vulnerabilities and Exposures (CVE) elenco di vulnerabilità divulgate pubblicamente e Zero Day, condivise attraverso i metodi di "Responsible Disclosure";

2. Copertura completa dei principali vettori di attacco per ogni singola sessione e tipologia di target, acquisita mediante l'aggiornamento continuo di un archivio centralizzato contenente il Threat Modelling e relative Tactics, Techniques and Procedures (TTP), alimentato dal team di Pen Tester coinvolti a livello globale nell'erogazione di tali servizi;



3. Utilizzo estensivo di fonti Cyber Threat Intelligence (OSINT e CLOSINT) con copertura geografica mondiale, derivante dai servizi di sicurezza gestista (SOC) del RTI, che consentono al Pen Tester di ottenere un quadro più ampio dell'effettivo livello di esposizione dei target in analisi, come ad esempio compromissioni/vulnerabilità/tecniche pubblicate nel dark web o in community specifiche, potenzialmente accessibili anche agli attaccanti e sfruttabili per realizzare una reale compromissione,;
4. Molteplicità di laboratori a livello nazionale ed internazionale con personale, strumenti ed infrastrutture dedicate alle attività di offensive security, con possibilità di verificare costantemente i vettori e le tecniche di attacco in ambienti simulati e su dispositivi di test; tali laboratori sono impiegati anche per addestramento, formazione ed aggiornamento continuo dei Pen Tester.

Di seguito sono riportati i principali strumenti/soluzioni tecnologiche che saranno utilizzati per l'erogazione del servizio.

Ambito di utilizzo	Principali strumenti
PT Infrastrutturale	● **Open Source**: nmap, netdiscovery, dnsrecon, dig, metasploit, netcat, masscan,scapy,hping, CrackMapExec, Air-Ng tools, Wifite, Airgeddon, Wireshark; ● **Di Mercato:** Acrylic WIFI **,** Hak5 Wifi (HW e SW), Nessus
PT Applicativo	● **Open Source**: Objection, Frida ,Apktool, Dex2jar, Hopper, Drozer, MobSF, Clang Static Analyzer, Andrubis, Flawfinder, ApkAnalyser, Androwarn, Ghidra, Radare; ● **Di Mercato:** Nessus, Burp Proxy Professional
PT Device IOT	● **Open Source**: Burp Proxy Professional, Blue Scanner, Blue Sniff, BlueBugger, BTBrowser, BTCrawler, BlueSnarfing, ZigDiggity; ● **Di Mercato:** HackRF, Proxmark
Red Team	● **Open Source**: Social Engineering Toolkit (SET) , Gophish , Invoke-Obfuscation, Veil Framework, Empire Project, DNSExfiltrator, Cloakify Factory; ● **Di Mercato:** Cobalt Strike, Metasploit Pro

Compliance normativa (L2.S23)

Il servizio di Compliance normativa prevede la definizione di un Sistema di gestione della Privacy in grado di governare in un'ottica di lungo periodo tutti gli adempimenti GDPR impattanti sui sistemi IT. Il RTI si impegna ad erogare le attività in ambito nel rispetto dei requisiti tecnico-funzionali specificati nel CTS, facendo affidamento sugli elementi distintivi elencati di seguito:

- Multidisciplinarietà delle competenze (IT, legali, operative e organizzative) integrate in team strutturati.

- Utilizzo del GDPR Compliance Framework (GDPR CF), che include la metodologia per lo svolgimento delle attività, modelli, processi, questionari, baseline di requisiti, strumenti automatizzati, in grado efficientare le attività progettuali
- Costante aggiornamento normativo realizzato attraverso l'Osservatorio Privacy del RTI
- DRA ed EYA si possono avvalere della collaborazione dei propri Studi Legali Associati.

Il Sistema di gestione della Privacy ha necessità di essere disegnato, analizzato, implementato, monitorato e continuamente migliorato in un'ottica anche di lungo periodo, al fine di trasformare la privacy in un fattore abilitante per il trattamento dei dati da parte dell'Amministrazione e garantire agli interessati la protezione dei dati personali. A tale scopo, il RTI utilizzerà, per guidare lo svolgimento delle attività, il GDPR Compliance Framework (GDPR CF). Tale strumento propone una metodologia per la definizione e mantenimento del sistema privacy ed è caratterizzato da un ciclo di 4 fasi: a) Analisi; b) Implementazione; c) Verifica; d) Continuous Improvement. Quest'ultima fase è abilitata dal Privacy Maturity Model (PMM), ovvero uno strumento in grado di intercettare nel continuo, i punti di forza e di miglioramento del Sistema di gestione della privacy esprimendo lo stato di maturità e identificando in modo dinamico le aree di intervento. L'utilizzo del GDPR CF, oltre a mettere a disposizione un set esaustivo di strumenti automatici, potrà, essere supportato da un prodotto software integrato che consente di gestire il Sistema Privacy in modalità condivisa e collaborativa tra tutti i soggetti interessati (es. DPO, Privacy Officer, IT, Sicurezza, Risorse Umane, Acquisti).
Analisi: la fase di analisi prevede lo svolgimento di un assessment per verificare lo stato di conformità alla normativa applicabile da parte delle Amministrazioni al fine di comprendere le aree maggiormente a rischio e identificare gli eventuali interventi di rimedio necessari per garantire conformità e allo stesso tempo automatizzare i processi privacy.
Implementazione. tale fase consentirà di indirizzare le azioni di rimedio emerse a seguito dell'Assessment ed incluse nel Piano degli interventi o già previste dai piani di conformità dell'Amministrazione. Allo scopo di massimizzare l'efficacia degli interventi e la logica del riuso, le attività di implementazione sono eseguite secondo un modello operativo che prevede la messa a disposizione di template consolidati per le componenti del framework documentale (es. politiche, procedure, metodologie, nomine a responsabile, informative, data processing agreement, materiale formativo) che saranno condivisi con l'Amministrazione e personalizzati sulla base delle specifiche necessità
Verifica: tale fase consente di misurare l'effettiva implementazione dei requisiti normativi a cui è soggetta l'Amministrazione, valutare il rischio derivante dai gap ed il livello di maturità raggiunto, proponendo eventuali punti di miglioramento, attraverso piani di azione costantemente monitorati.
Continuous Improvement: al fine di trasformare la privacy da adempimento di legge ad abilitatore "mandatorio" e cogliere tempestivamente i rischi normativi/sanzionatori/IT, si prevede l'adozione del PMM (o in alternativa il Data Protection Maturity Self-Assessment Model rilasciato dal CNIL).