ALLEGATO A – OFFERTA TECNICA DEL FORNITORE

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

Offerta Tecnica

CIG - 8884642E81

LOTTO 2

Sommario

1 Premessa

1.1 Contesto di riferimento e principi della fornitura

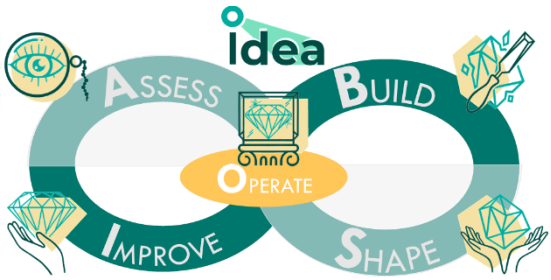
La difesa dal rischio cyber è di massima priorità in tutti i settori dell'economia, dello Stato e della società civile; lo scenario Covid poi, ha reso ancora più tangibile un'esigenza già prima impellente. La Pubblica Amministrazione è nel mirino di una minaccia sempre più sofisticata e con conseguenze sempre più gravi. Una cartella clinica può valere centinaia di euro per il cyber crime. La maggioranza delle Amministrazioni Pubbliche, per taluni analisti oltre il 60%, è vulnerabile tanto nelle tecnologie abilitanti, quanto nei processi e nelle competenze, intese nel senso più generale di capacità di orientarsi nel complesso delle conoscenze e sensibilità necessarie per operare in sicurezza nel cyber space.

La presente offerta nasce da **significative capacità ed esperienze** nel panorama professionale del settore dell'Information Technology ed in particolare nell'ambito della cybersecuity, espresse al fianco delle Pubbliche Amministrazioni Centrali e Locali.

L'intera offerta si ispira e si sostanzia per indirizzare quelli che sono - a nostro avviso - i **10 fattori critici di successo della presente fornitura** (elencati di seguito ed evidenziati ad ogni ricorrenza lungo il documento): *standardizzazione dei processi operativi* e, dove possibile, *automazione dei servizi*, finalizzata alla garanzia del risultato e alla sicurezza dell'esecuzione; *situational awareness*, attitudine nata in ambito militare, estesa negli anni a tutte le operazioni critiche (dal trasporto aereo alla gestione delle emergenze ambientali) e oggi richiamata dalle buone prassi di cyber security. Nell'offerta tale attitudine è parte dell'approccio proposto alle attività - dal presidio delle vulnerabilità alla gestione degli incidenti - e contribuisce ad un consapevole *strategy setting*; *approccio risk based*, perseguito in tutte le fasi dei servizi offerti, con l'intento di supportare l'Amministrazione nel mantenimento di un *equo rapporto tra rischio e spesa* all'interno del progetto di sicurezza, in un quadro generale di esposizione ad un crescente fabbisogno di protezione dettato dalla stretta delle normative e dalla minaccia incombente; *tailoring dei servizi*, adeguandoli alle specificità del comparto (PA centrale o locale) e della tipologia di Ente e soprattutto con la massima attenzione alla *sostenibilità degli interventi da parte dell'organizzazione*, in modo da agevolare l'applicazione della *due care* rispettando l'effettiva capacità interna; *concretezza* attraverso la proposizione di un "catalogo del riuso" (di modelli e strumenti collaudati e replicabili), che rafforzi anche l'obiettivo di standardizzazione e *velocità*; *information sharing*, pratica alla base dell'accrescimento della capacità di difesa (e velocità di risposta) contro il rischio cyber, promossa all'interno dei gruppi di lavoro, come strumento di accelerazione della knowledge base comune.

1.2 Proposta progettuale

I servizi oggetto della presente fornitura saranno erogati dal nostro raggruppamento secondo la metodologia Idea **(Intellera Digital Empowerment Accelerator)**, adottata nella Pubblica Amministrazione per il governo di progetti complessi a matrice digitale. La metodologia si compone di **4 fasi sequenziali (Assess, Shape, Build, Improve)** volte a tracciare un percorso di erogazione coerente con i servizi del Lotto 2, e di **una fase continuativa** (Operate) finalizzata al monitoraggio e al supporto operativo alle Amministrazioni. Nel dettaglio:



- **ASSESS:** declinazione degli obiettivi del servizio in priorità; analisi e valutazione del contesto operativo e del grado di maturità; individuazione delle criticità e delle aree di miglioramento;
- **SHAPE:** individuazione e macro-disegno delle soluzioni da implementare con evidenza del piano di azione, delle responsabilità, dei tempi e degli strumenti da utilizzare;
- **BUILD:** costruzione e prima adozione delle soluzioni individuate; raccolta delle evidenze circa gli output delle soluzioni ed analisi dell'efficacia delle stesse;
- **IMPROVE:** fine-tuning delle soluzioni, supporto all'adozione da parte degli utenti, valutazione dell'impatto delle soluzioni e costruzione delle lesson learned dell'iniziativa;
- **OPERATE:** durante la quale, a conclusione della fase progettuale, con un approccio di **Continuous Improvement**, vengono portate avanti attività di monitoraggio e supporto operativo.

Di seguito è riportata la leggenda dei "segna posto" utili per identificare rapidamente nel testo gli aspetti legati a metodologia, competenze tematiche, strumenti, soluzioni tecnologiche:

- Quando si menziona un obiettivo specifico per l'erogazione dei servizi
- Quando si menziona una metodologia da adottare per l'erogazione dei servizi
- Quando si menziona uno standard da adottare per l'erogazione dei servizi
- Quando si menziona uno strumento o una soluzione tecnologica da adottare per l'erogazione dei servizi
- Quando si menzionano degli aspetti di efficacia e concretezza di una soluzione specifica per l'erogazione dei servizi

2 Presentazione e descrizione dell'offerente

Le aziende che compongono il nostro Raggruppamento sono:

Intellera Consulting (*former* PwC Public Sector) è una società di consulenza nata dal management buyout della linea di business di PwC Italia **dedicata alla Pubblica Amministrazione e all'Healthcare**; dispone di **network di circa 700 professionisti**, si configura come apripista nella consulenza strategica e direzionale, e propone servizi professionali d'eccellenza

a istituzioni, amministrazioni e imprese. Intellera svolge numerosi progetti in ambito cyber security, di diversa natura e complessità, afferenti alle PA Centrali (es: Consip, Ministero dell'Economia e Finanze, Ministero della Salute, INAIL, ecc.), a PA Locali (es: Roma Capitale, Comune di Milano, Regione Lazio, Regione Toscana, Regione Campania, Comune di Venezia, ecc.) e ad altri Enti del settore pubblico (es: AgID, Sogei, Consip, ecc.).

Capgemini è leader mondiale nella Cyber Security ed opera con più di **270.000 persone**, presenti in quasi **50 paesi** in tutto il mondo, con una forte esperienza sui principali mercati internazionale e italiano. La **Cyber Security rappresenta il core business** di Capgemini e viene sviluppata attraverso **un team globale costituito da oltre 4000** risorse con competenze qualificate che offrono un approccio a 360° su piattaforme IT, OT, cloud e IoT. Includiamo un set di servizi gestiti da personale con elevati skill in ambito di **Ethical Hacking** per fare attività di analisi delle vulnerabilità di servizi e infrastrutture delle aziende clienti.

HSPI SpA è una società di consulenza direzionale nata nel 2003, leader in Italia sulle tematiche di **IT Governance, IT Service Management, Management Consulting,** che conta più di 150 professionisti dislocati sulle tre sedi di Roma, Bologna e Milano in grado di offrire una vasta gamma di servizi professionali grazie ad un modello operativo capace di integrare competenze distintive di Consulenza Direzionale e conoscenze specialistiche in ambito ICT. HSPI ha maturato una notevole esperienza nella PA attraverso l'adozione di metodologie in linea con gli standard internazionali e alla collaborazione e partnership con associazioni internazionali ed enti per lo studio e la diffusione delle migliori pratiche di **IT Governance, IT Security e IT Service Management.**

Teleconsys è una **Digital Innovation Company** il cui principale ambito di expertise è supportare le organizzazioni pubbliche e private in tutte le fasi del loro viaggio di trasformazione digitale attraverso l'adozione dei principali **digital enabler** e dell'**open innovation**. Iscritta dal 2019 nella sezione speciale del registro delle imprese in quanto investe più del 3% del VdP in RSI, ha specifiche competenze nella progettazione e realizzazione di soluzioni di Cybersecurity, Data Governance & Protection e Intelligence ed è strutturata su 3 BU (Next Generation Infrastructure & Cybersecurity, Agile Application Development & UX, Intelligent Service & Operation), intersecate da due strutture di innovazione: il **Digital Innovation Experience e l'Innovation & Contamination Lab**.

La ripartizione delle attività tra le società del RTI è particolarmente funzionale all'erogazione dei servizi perché, oltre a valorizzare gli elementi di "specializzazione" di ciascun proponente, consente di **enfatizzare la complementarità delle rispettive competenze** e assicurare una chiara individuazione delle responsabilità. Con il simbolo (✓) sono indicate gli ambiti di prevalente coinvolgimento mentre con il simbolo (✓) il coinvolgimento.

Servizi fornitura – Lotto 2	Intellera Consulting	Capgemini	HSPI	Teleconsys
Security strategy	✓	✓	✓	✓
Vulnerability assessment	✓	✓	✓	✓
Testing del codice	✓	✓	✓	✓
Supporto all'analisi e gestione degli incidenti	✓	✓	✓	✓
Penetration testing	✓	✓	✓	✓
Compliance normativa	✓	✓	✓	✓

La Presente Relazione Tecnica viene sottoscritta e firmata da:

- per **Intellera Consulting Srl**: Giancarlo Senatore, [redacted] in qualità di Amministratore Delegato e legale rappresentante, e Mario Papini [redacted] in qualità di Amministratore;
- per **Capgemini Spa**: Andrea Falleni, nato [redacted] in qualità di Amministratore Delegato e legale rappresentante;
- per **HSPI Spa**: Sebastiano Manno, nato [redacted] in qualità di Amministratore Delegato e legale rappresentante;
- per **Teleconsys Spa**: Giada Apicella, nata [redacted], in qualità di Procuratore.

3 Struttura Organizzativa

La soluzione proposta per il governo della fornitura nasce dalla nostra conoscenza del contesto Pubblico e si basa sul paradigma **dell'Agile Program Management** affinato anche grazie alle esperienze di gestione di Accordi/Contratti Quadro Consip (SPC Lotto 3 e Lotto 4, SGI Lotto 2 e Lotto 3, AQ Servizi Applicativi Lotto 1 e 2, Convenzione AT). Tali esperienze ci hanno visti impegnati nell'erogazione di numerosi contratti esecutivi/appalti specifici **(oltre 300 gestiti in parallelo)**, anche di dimensioni rilevanti, con grande eterogeneità funzionale e dimensionale (citiamo, ad es. grandi Amministrazioni Centrali quali MEF, Ministero del Lavoro, Ministero della Salute, INPS, INAIL, Consip, AgID, Agenzia per la Cybersicurezza Nazionale -ACN- e Amministrazioni Locali quali Regione Lombardia, Regione Lazio, Comune di Milano, Roma Capitale). La soluzione organizzativa è stata definita a partire dalla identificazione delle **caratteristiche di efficacia e di concretezza** necessarie alla gestione e presidio di un Accordo Quadro "multi-Amministrazione". Di seguito saranno descritti anche i ruoli e le figure organizzative aggiuntive messe a disposizione della fornitura e indicate con il simbolo .

GOVERNO DELLA COMPLESSITÀ

Capacità di governare in maniera unitaria e sinergica dagli obiettivi strategici della fornitura agli obiettivi operativi del singolo servizio/iniziativa. **Soluzione adottata:** abbiamo definito una struttura che gestisce in maniera integrata i due ambiti operativi (Accordo Quadro

e Contratti Esecutivi) e tre livelli di governo (Strategico, Programma, Progetto). ► **Livello Strategico:** presidia la definizione, il monitoraggio e la revisione della strategia complessiva di approccio all'AQ ed i suoi obiettivi. ► **Livello di Programma:** grazie all'approccio dell'**Agile Program Management** gli obiettivi strategici vengono tradotti in modo coordinato in obiettivi specifici (contratto esecutivo) e vengono gestite risorse e pianificazione a livello centralizzato. Inoltre, al fine di garantire un efficace condivisione delle informazioni tra i diversi servizi della fornitura, istituiamo un tavolo di coordinamento – il **Security Project Board (SPB)** – nel quale parteciperanno i singoli Responsabili Tecnici di tutti i servizi. Il SPB insieme al **Board dei Fornitori** (descritto di seguito) rappresentano le strutture aggiuntive che consentiranno di garantire il coordinamento unitario dei progetti di sicurezza ► **Livello di Progetto:** A livello di contratto esecutivo, i singoli interventi vengono istanziati in soluzioni operative secondo i principi Agile (**Agile Project Management)**.

Capacità di assicurare la gestione di tutte le dimensioni manageriali di un Programma (attività, tempi, risorse, competenze, qualità, rischi) e il tailoring dei servizi. **Soluzione adottata:** sono state **istituite le seguenti strutture/figure aggiuntive** ► **Quality & Risk Office (Q&R)** responsabile della qualità e del risk management nell'AQ, interfaccia unica per i RUAC-CE dei singoli Contratti Esecutivi come SME (nei casi di necessità di escalation) e come governo e diffusione delle metodologie e standard. ► **Program Manager (PM)** responsabile del coordinamento delle iniziative e delle correlazioni tra i diversi CE. È supportato operativamente da una struttura di PMO. ► **Resource Manager (RM)** responsabile della gestione delle risorse umane in tutte le fasi dell'attuazione dei contratti esecutivi, dalla loro identificazione per il "coinvolgimento nei progetti" alla formazione e scheduling, sino al rilascio al termine delle attività. Supporta il RUAC-CE dei singoli contratti esecutivi nella gestione/sostituzione delle risorse del RTI.

ASCOLTO E COMPRENSIONE

Capacità di valorizzare le singole specificità e le esigenze degli stakeholder a tutti i livelli di governo.

Soluzione adottata: abbiamo definito **strutture aggiuntive** preposte alla raccolta, analisi e comprensione delle esigenze degli stakeholder. ► **Steering Committee (SC)**, quale tavolo di coordinamento strategico permanente per condividere indirizzi, strategie, risultati ed eventuali criticità, nonché assicurare unitarietà di visione nell'erogazione dei servizi. Al tavolo partecipano oltre al RTI anche i referenti di Consip e di altri stakeholder istituzionali impattati (referenti di Consip, AgID e ACN). ►**Technical Board (TB)**, tavolo di lavoro a cui partecipano i Referenti tecnici AgID e ACN, i referenti tecnici degli Uffici di IT security e privacy delle Amministrazioni aderenti, per condividere le metodologie applicate/best practice, le scelte tecnologiche, gli strumenti di analisi. ► **Board Fornitori (BF)**, luogo di confronto con i referenti degli aggiudicatari del Lotto 1, per supportare le Amministrazioni nella individuazione dei fabbisogni e per condividere metodologie e soluzioni a eventuali criticità, favorendo l'uniformità e la standardizzazione degli interventi.

Capacità di intercettare la conoscenza e le innovazioni sia tecniche che regolamentari che si generano sul mercato e di trasferirle alle risorse dell'organizzazione. **Soluzione adottata:** sono state istituite **le seguenti strutture/figure aggiuntive** ► **Osservatorio Normativo sulla Security & Privacy (ONS&P)** rappresenta la struttura deputata all'analisi e studio della normativa in via di evoluzione sui temi di sicurezza e privacy, fornendo elementi utili per l'applicazione concreta nell'ambito dei CE. ► **Security & Privacy Enabler Solution Innovators (SPESI)** è una unità organizzativa volta a valorizzare le soluzioni innovative in tema di sicurezza prodotte dalla PMI innovativa e dai nostri centri di competenza. ► **Knowledge Manager (KM)** è la figura incaricata della gestione del know-how della Fornitura (es. presa in carico, condivisione di best practice e lesson learned, ecc.). Supporta le attività di condivisione documentale all'interno del Portale della Fornitura.

Capacità di comprendere e, dove possibile, "anticipare" in ottica di risk based le esigenze delle Amministrazioni aderenti. **Soluzione adottata:** è stata definita una **struttura ad-hoc aggiuntiva** per la raccolta delle esigenze delle Amministrazioni denominata **Account & Demand Management Office (ADMO)**. È la struttura di raccordo tra l'ambito AQ e quello CE, centralizzando il supporto alle PA nella compilazione del Piano dei Fabbisogni/Piano Operativo. Coordina le attività dei Focal Point (descritti di seguito) nelle fasi di attivazione e di esecuzione dei CE. Coordina gli Account Territoriali (AT). Gli AT hanno il compito di promuovere l'AQ presso gli Enti potenzialmente destinatari, raccogliere e razionalizzare, secondo un equo rapporto tra rischio e spesa, le esigenze delle Amministrazione aderenti e formalizzarle in un Piano dei fabbisogni/Operativo.

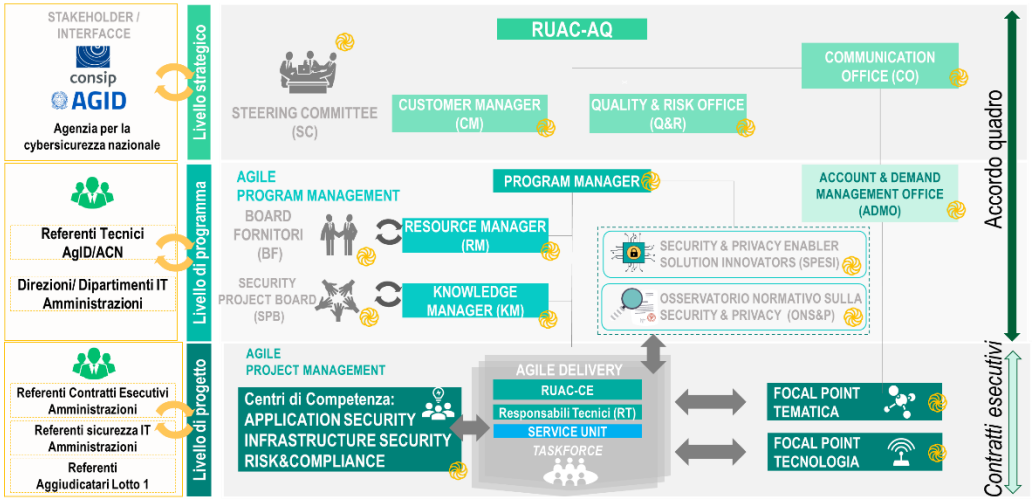
DELIVERY

Capacità di massimizzare la soddisfazione dell'Amministrazione destinataria. **Soluzione adottata:** abbiamo previsto una **figura aggiuntiva dedicata** alla cura della soddisfazione delle Amministrazioni e degli altri stakeholder (tra cui AgID e Agenzia per la cybersicurezza nazionale) denominata **Customer Manager (CM)**. Il CM raccoglie e analizza le segnalazioni delle Amministrazioni presidiando il mantenimento delle aspettative e dei livelli di qualità attesi, informando i singoli RUAC-CE su eventuali criticità da gestire. Ha la responsabilità della gestione del Portale della fornitura e dei canali di comunicazione digitali (es.: social media), e cura la creazione di contenuti di qualità dei diversi canali comunicativi.

Capacità di massimizzare la standardizzazione dei processi operativi e la flessibilità nella delivery, in relazione a cambiamenti di contesto, imprevisti o modifiche delle priorità. **Soluzione adottata:** attraverso l'approccio **Agile Project Delivery** tutte le competenze necessarie all'erogazione dei servizi sono sempre garantite nell'ambito dei Team Agile, assicurando adattabilità e flessibilità all'eterogeneità dei progetti, anche attraverso la capacità di monitoraggio e pronta risposta a picchi di attività, esigenze ad hoc e specificità territoriali.

Capacità di assicurare in termini quantitativi e qualitativi le risorse necessarie per l'esecuzione dei servizi della fornitura. **Soluzione adottata:** ogni ambito di natura tecnica e regolamentare è presidiato dai **Focal Point**, ovvero risorse con elevatissima specializzazione di tematica e tecnologia e almeno 15 anni di esperienza appartenenti alla struttura di ADMO, che assicurano il costante collegamento con i centri di Competenza e Delivery per lo staffing dei team di lavoro.

Nella figura seguente viene rappresentato **l'organigramma dell'organizzazione** nella sua interezza, dedicata per la gestione dell'Accordo Quadro e dei Contratti Esecutivi. Con il simbolo sono indicati i ruoli e le figure organizzative aggiuntive messe a disposizione della fornitura.



Nella cornice di tale struttura, **le società del nostro raggruppamento hanno delle responsabilità specifiche ma fortemente complementari rispetto a tutti gli ambiti/servizi oggetto di Fornitura.** In particolare:

Intellera Consulting Srl, in qualità di mandataria, garantirà il governo dell'AQ e sarà responsabile dell'erogazione di tutti i servizi richiesti. Grazie all'esperienza nell'ambito del public IT security & privacy, avrà un ruolo guida nell'ambito dei servizi di Security Strategy e di Compliance Normativa, nonché nel supporto alle Amministrazioni nell'analisi degli impatti e nell'implementazione concreta degli adempimenti dettati dal GDPR con un focus specifico al perimetro IT.

Capgemini Spa metterà a disposizione delle Amministrazioni destinatarie le sue competenze e professionalità tecniche maturate nella PA a tutti i livelli di governo sui temi IT e IT Security. Nell'ambito della fornitura avrà un ruolo prioritario nell'ambito dei servizi di vulnerability assessment, testing del codice, penetration testing e analisi e gestione degli incidenti.

HSPI Spa avrà un ruolo fondamentale nel supportare le PA nella strutturazione dei progetti di sicurezza, mettendo a disposizione le competenze per i servizi di Security Strategy, con un focus sull'advisory sulle soluzioni di beni e servizi in materia di IT Security.

Teleconsys Spa è una **PMI Innovativa** con specifiche competenze ed esperienze nella progettazione e realizzazione di soluzioni di Cybersecurity, Data Governance & Protection. Avrà un ruolo fondamentale nel supportare le PA nell'individuazione di soluzioni innovative e "best in class" di sicurezza e di rinnovamento tecnologico, in maniera trasversale rispetto ai servizi oggetto della fornitura.

Per garantire il **coordinamento tra le diverse strutture organizzative e le modalità di interazione con le Amministrazioni destinatarie**, proponiamo un **modello operativo basato su processi standard e azioni di condivisione strutturati**.

Promozione AQ: gli Account Territoriali (AT) promuovono in modalità proattiva l'AQ presso le Amministrazioni target del proprio ambito territoriale di riferimento, attraverso: ► **sessioni di promozione** con i Referenti di sicurezza IT e privacy delle PA, al fine di illustrare gli ambiti di applicazione dell'AQ e fornire informazioni per attivare i CE; ► **eventi tematici** o partecipazione a eventi esterni.

Definizione CE: il RUAC-CE, con il supporto del ADMO e del RKM, coordina le azioni per accompagnare le PA dal primo contatto fino alla stipula dei CE, anche attraverso la pianificazione di una serie di incontri con i diversi Referenti IT e di privacy dell'Amministrazione aderente.

Esecuzione e monitoraggio CE: le strutture aggiuntive di Technical Board e l'Osservatorio Normativo sulla Security & Privacy garantiscono il coordinamento interno in termini di aderenza agli standard e di aggiornamento rispetto alle evoluzioni che potranno verificarsi nel corso della fornitura, supportando i GdL anche attraverso pillole formative o incontri di approfondimento. Il PM è responsabile della coerenza e della sostenibilità di tutti gli interventi progettuali tramite una vista unitaria, organizzando incontri di allineamento e monitoraggio con i singoli RUAC-CE. Infine, la struttura aggiuntiva **Security & Privacy Enabler Solution Innovators (SPESI)** si interfaccia con le Amministrazioni, secondo un duplice approccio: "push", offrendo una vasta gamma di possibili interventi di potenziamento di beni e servizi di sicurezza innovativi e di frontiera, anche ricercando nuovi filoni di intervento; "pull", efficientando le tempistiche di risposta a vincoli normativi sfidanti.

Creazione e animazione della Learning & Working Security Community: proponiamo di attivare un modello di condivisione della conoscenza che consenta di regolare l'*Information Sharing* e attivare meccanismi virtuosi di trasferimento e spill-over. A tal proposito, proponiamo l'istituzione di una **Learning & Working Security Community (L&WSC)**, una community professionale costituita da tutti gli attori che intervengono nei progetti di sicurezza IT. La L&WSC è un luogo dell'apprendimento in grado di produrre innovazione e miglioramenti continui. La L&WSC opererà su tre livelli di responsabilità: ► **I livello**: è composto dai referenti delle PA (Referenti della sicurezza IT e Referenti della privacy) che svolgono la funzione di anello di congiunzione fra i decision maker, i Fornitori e eventualmente i cittadini/utenti. Hanno il compito realizzare e monitorare i progetti di sicurezza; ► **II livello**: vi fanno parte i Fornitori aggiudicatari dei due lotti ed hanno un ruolo chiave nell'analisi/ascolto dei fabbisogni e nella attuazione dei servizi. La L&WSC è attivata attraverso

modalità in presenza (focus group, riunioni, workshop) e modalità a distanza descritti al paragrafo Portale della Fornitura. ► **III livello:** è rappresentato dai cittadini/utenti dei servizi interessati dai progetti di sicurezza e ha un ruolo fondamentale nella valutazione ex-post dei risultati raggiunti.

Inoltre, ad accompagnare tale modello operativo, saranno messi a disposizione della presente fornitura un **set di strumenti di condivisione delle informazioni** già ampiamente sperimentati in Accordi/Contratti Quadro analoghi:

ATTIVITÀ	DESCRIZIONE	PERIODICITÀ	RUOLI COINVOLTI
Incontri di avanzamento AQ	Convocati dal RUAC-AQ, coinvolgendo il SC, per condividere l'andamento della fornitura, la definizione di azioni propositive nei confronti di AgID, ACN e delle PA.	Bimestrale o ad eventi significativi	RUAC-AQ, SC
SAL Programma	Convocati dal PM per coordinare e monitorare la gestione integrata delle attività, la dimensione e mix dei team sui singoli CE facilitando l'integrazione tra iniziative	Bimestrale o ad eventi significativi	RUAC-AQ, PM, PMO, RKM, ADMO
SAL di CE/Progetto di sicurezza	Convocati dal RUAC-CE, coinvolgendo il SPB e il BF, per verificare l'andamento delle attività dello specifico Contratto Esecutivo/progetto di sicurezza	Ad hoc	RUAC-CE, SPB, BT, ADMO, Referenti Amm.
SAL di Servizio	Riunioni ad hoc sull'andamento delle attività dello specifico servizio, attivati dai RT	Mensile o ad hoc	RT, GdL – Referenti Amm.
Meeting tecnici interni	Organizzati per discutere di specifici argomenti: nuove esigenze di natura normativa e tecnica, criticità, picchi di lavoro; creano sinergie informative ed operative tra i diversi team.	Mensile o ad eventi significativi	RT, FP, GdL, SPESI, ONS&P
Piano di comunicazione	Questo documento a livello di Accordo Quadro presenta l'andamento delle attività e i principali ambiti attivati anche a supporto di AgID e ACN.	Trimestrale	RUAC-AQ, PM, PMO
Documenti Operativi	Il RTI adotta standard documentali comuni a tutti i progetti/programma: Gantt, project health check, iussue log, risk log, meeting agenda, Sal, …	NA	Tutte le risorse

4 Proposta progettuale per il servizio "Security Strategy"

"E' con la scelta di strategie adatte che problemi complicati vengono ridotti a semplici fenomeni e poi risolti"
(Charles Proteus Steinmetz)

Obiettivi del servizio: supportare le PA nella definizione del Progetto di sicurezza e dei relativi fabbisogni di beni e servizi, assicurando: ► **una chiara definizione degli obiettivi di sicurezza** (Security Target Profile); ► **l'identificazione dei gap da colmare** rispetto alla situazione di partenza (Security Current Profile); ► **la definizione di una roadmap strategica** degli interventi da implementare; ► la traduzione degli interventi in un **piano dei fabbisogni** di beni e servizi; ► **una chiara identificazione dei ruoli** e delle responsabilità di governo e di gestione di tutte le fasi.

L'elaborazione del Progetto di Sicurezza è quindi il procedimento grazie al quale vengono definite le scelte strategiche di governo e gestione della sicurezza delle informazioni e delle azioni implementative da avviare per tutti i servizi. La nostra proposta ha come riferimento il Framework Nazionale per la **Cybersecurity e la Data Protection** (anche noto come Framework Nazionale 2.0), e si basa su un *approccio risk based* che si declina in attività seguendo **l'approccio metodologico** Idea (*cfr. § 1.2 Proposta progettuale*).

Metodologia: L'approccio metodologico proposto è strutturato come segue:

Analisi: di tutte le dimensioni (domini) da considerare nel Progetto di Sicurezza: **Strategia e Governo della Sicurezza delle Informazioni**, **Cyber Security Operation, Awareness, Gestione Eventi e Incident, Architetture di Sicurezza, Compliance Normativa** qualificandone i sotto domini (es. Formazione e Sensibilizzazione all'interno del dominio Awareness). Per la qualificazione di questi elementi la nostra proposta prevede un *approccio risk based* (analisi dei rischi cyber e dello stato rispetto a questi) al fine di tracciare così il ***Security Current Profile***.

Definizione del Modello: attraverso interviste e workshop con i referenti chiave della Amministrazione e benchmark con realtà analoghe, viene definito il **Modello di Gestione della Sicurezza** dell'Amministrazione e per tutti i domini e sottodomini individuati vengono declinati gli obiettivi da raggiungere, definendo il ***Security Target Profile*** dell'Amministrazione.

Pianificazione: vengono identificati i gap (es. l'assenza di un processo di Incident Management), e le aree di miglioramento (in questo caso una cultura del rischio non consolidata), elaborando la roadmap strategica e identificando le azioni da pianificare (in questo caso l'ottenimento della certificazione ISO 27001), le priorità, i risultati attesi. In questa fase viene definito il ***Modello Organizzativo di gestione della sicurezza***.

Realizzazione: grazie a tecniche tipiche del project management (es. studi di fattibilità, analisi di impatto, Portfolio Management, Business Case, PBS, WBS) la roadmap strategica viene declinata nel ***Piano dei fabbisogni di beni e servizi***, assicurandone la effettiva realizzabilità e "*sostenibilità*" economica.

Gestione e Monitoraggio: gestione e monitoraggio della implementazione del Progetto di Sicurezza, e fine tuning in un'ottica di miglioramento continuo.

Standard adottati: la metodologia si basa sugli standard nazionali ed internazionali in materia ed in particolare, come anticipato, sul Framework Nazionale 2.0; nei singoli domini (Governance, Incident, ecc), la metodologia adotta specifici standard di riferimento: es. ISO 27001; ISO 22301, Security HealthCheck dell'Information Security Forum, linee guida AgID (es. Linea Guida per la sicurezza nel procurement ICT e per lo sviluppo del software sicuro).

Strumenti a supporto: **Intellera Security Assessment Tool (ISAT)**. Repository cloud-based integrato con il Portale della Fornitura utile a guidare le attività di assessment e l'analisi dei risultati, e supportare l'elaborazione/implementazione del Progetto di Sicurezza. Lo strumento integra funzionalità di benchmarking capitalizzando, in **maniera del tutto anonima**, la knowledge maturata dal RTI in progetti di Security, consentendo la valutazione facilitata del livello di maturità dell'Amministrazione ("Security Current Profile") rispetto ad altre PA simili per caratteristiche (comparto, dimensione, modalità di gestione della tematica sicurezza, ecc). ISAT supporta anche la fase di definizione del "Security Target Profile", avvalendosi di cataloghi dei rischi e di azioni di mitigazione anch'essi costruiti in base alle esperienze maturate e fruibili come acceleratori. Affiancato a ISAT il RTI dispone dell'**Intellera Risk Knowledge Base** che si arricchisce dei report nazionali e internazionali sui trend dei rischi cyber assicurando così la disponibilità della conoscenza ai centri di competenza (Application Security, Infrastructure Security, Risk & Compliance).

4.1 Approccio proposto per l'elaborazione del "Progetto di sicurezza"

Disponiamo di un Security framework di riferimento per la rappresentazione di **Modelli di Gestione della Sicurezza** adeguati alle caratteristiche delle diverse realtà della PA. Il framework (rappresentato in figura) è da considerarsi una base di partenza, ma **può essere personalizzato** sulle base delle caratteristiche dell'Amministrazione favorendo così al tempo stesso la *velocità d'azione* e la *personalizzazione degli interventi* nei domini (es. Strategia e Governo della Sicurezza delle Informazioni) e sotto-domini (es. Policy e Procedure, Sistema di Monitoraggio, ecc.). Per ogni dominio e sotto-dominio sono predisposte checklist di valutazione a supporto delle analisi. Nel caso di PA di piccole dimensioni, il Modello viene definito in un minor numero di sotto-domini attraverso aggregazioni.

Sulla base della tipologia di Amministrazione (comparto, servizi, dimensione, ecc.) e approccio alla sicurezza, l'**ISAT** supporta i team nella realizzazione dei deliverables fondamentali quali: ① **Qualificazione e disegno del Modello di Gestione della Sicurezza** più adatto alla tipologia di PA aderente, al suo contesto operativo e alle sue capacità e competenze strutturali; ② **Definizione del Security Current Profile** e del ③ **Definizione del Security Target Profile** attraverso le analisi sul campo supportate da checklist, benchmark e analisi di impatto. Confrontando il Security Current Profile e il Security Target Profile vengono evidenziati **i gap** rispetto al Modello di Gestione della Sicurezza atteso, ④ **identificati gli interventi da effettuare** e ⑤ **articolata la Roadmap di attuazione della strategia** al fine di definire il ⑥ **Piano dei fabbisogni di beni e servizi.**

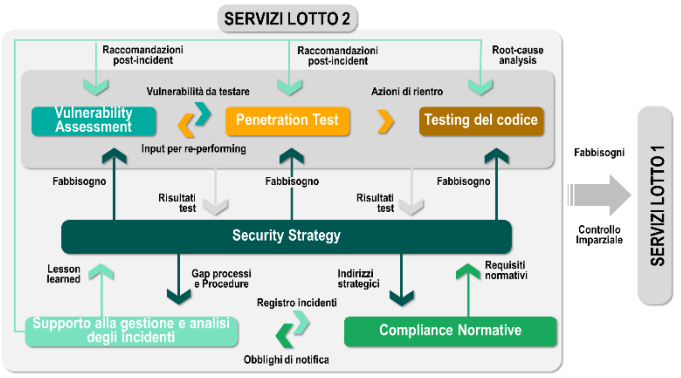
Le valutazioni vengono effettuate secondo un *approccio risk based* consentendo quindi **l'identificazione degli interventi (gap)** in base agli "obiettivi sui rischi" che si vogliono raggiungere (Security Target Profile) e la **sostenibilità** degli stessi (sia in termini di beneficio che di fattibilità) anche utilizzando la leva temporale (nel breve, medio e lungo periodo). La metodologia proposta capitalizza le tecniche tipiche del project management (es. Business Case, Product Breakdown Structure – PBS, Work Breakdown Structure-WBS) per individuare qualitativamente e quantitativamente i fattori abilitanti degli interventi, in termini di risorse necessarie e per **articolare gli interventi** della roadmap strategica in **fabbisogni di beni e servizi da approvvigionare**.

La articolazione correlata dei 6 elementi sopra illustrati, compone **il Progetto di Sicurezza della Amministrazione**. Il percorso di costruzione del Progetto di Sicurezza include, dove necessario, la redazione di studi di fattibilità, analisi di impatto, valutazione dei processi di trasformazione digitale e adeguamento al Cloud, aggiornando politiche, tassonomie e classificazioni necessarie ad indirizzare i cambiamenti nei processi di gestione.

Aspetti di correlazione con gli altri servizi

Il **Progetto di Sicurezza** indirizza dal punto di vista strategico tutti i servizi sia del Lotto 1 che del Lotto 2 e valorizza sia in input che in output tutte le informazioni prodotte nell'ambito degli altri servizi della fornitura. A livello operativo, per garantire un'efficace condivisione e coerenza delle informazioni tra i diversi servizi di gara, nella struttura organizzativa (*cfr. § 3 Struttura Organizzativa*), abbiamo inserito il **Security Project Board – SPB** (al quale

partecipano i Responsabili Tecnici dei servizi del Lotto 2) ed il **Board Fornitori - BF** (che include i referenti del Lotto 1). Tali board definiscono le modalità di *information sharing* sia in forma automatizza sia on-demand. In particolare (come evidenziato nella figura a fianco) i principali **Processi e flussi di informazioni** che il servizio di Security Strategy riceve in input dagli altri servizi del Lotto sono: ► **i risultati dei test** derivanti dalle attività di **Vulnerability Assessment, Penetration Test e Testing del codice** ► **i requisiti normativi e lesson learned** dai servizi di **Supporto all'analisi e gestione degli incidenti e Compliance normativa**. In output invece il Servizio di Security Strategy fornisce agli altri servizi: ► **gli indirizzi strategici e di coordinamento** allineati con le linee guida, le direttive e normative a livello nazionale ed europeo ► il **Piano dei fabbisogni di beni e servizi** per la realizzazione dei servizi del Lotto 1 e del Lotto 2, ed una ► **il modello di gestione della sicurezza**.



Valore aggiunto apportato dalla proposta in considerazione delle caratteristiche di contesto del Lotto

L'approccio metodologico descritto è particolarmente rilevante ed applicabile nel contesto dei servizi oggetto della gara in quanto garantisce: ► *conformità alla normativa e rispetto delle linee guida AGID*: l'utilizzo degli Standard nativamente integrato nelle metodologia (per i domini e sotto-domini di riferimento) assicura il costante aggiornamento degli interventi ai dettami normativi in essere per le diverse tipologie di PA ► *efficacia delle modalità di interazione* sia con i referenti della PA che, ove necessario, con terze parti (altre PA, imprese, organismi di governo e controllo, …), ► *omogeneità di approccio metodologico* per tutte le tipologie di PA servite, garantendo autoconsistenza del percorso seguito qualunque sia il contesto della PA aderente, stante l'applicazione del medesimo framework, opportunamente declinato a tutti i contesti ► *applicabilità a diversi contesti della PA* grazie alla disponibilità di modelli velocemente adattabili alle diverse realtà e di strumenti ampiamente sperimentati nel contesto pubblico ma provenienti da standard e best practice applicate in tutti i settori del mercato.

4.2 Proposta di elaborazione di un "Modello di analisi dei fabbisogni di beni e servizi di sicurezza"

Il piano dei fabbisogni esprime le necessità dell'Amministrazione rispetto al Modello di Gestione della Sicurezza che ha definito e che vuole implementare (insieme dei domini e sotto-domini con livello di maturità target). A supporto della identificazione dei fabbisogni il RTI dispone di **un modello di analisi** "mutuato" dalle metodologie tipiche del Project management per la definizione dei progetti tecnologici, che scompone gli interventi in beni e servizi necessari alla loro realizzazione. Gli interventi previsti nella Roadmap Strategica vengono qualificati in base a risultanze di **Business Case** specifici allo scopo di valutarne **l'effettiva "sostenibilità" costo/beneficio.** Successivamente, per ciascun intervento, si procede alla **definizione dei fabbisogni di beni e servizi** applicando tecniche di **PBS (Product Breakdown Structure)** e **WBS (Work Breakdown Structure)**. Inoltre, grazie all'utilizzo di **benchmark di comparto** eseguiti con il supporto dello strumento **ISAT,** i fabbisogni possono essere **confrontati** rispetto a contesti similari **anche in termini di Roadmap**. Questo approccio **assicura l'efficacia del piano** in quanto, collegando gli interventi e i fabbisogni agli obiettivi di sicurezza target, consente di adottare un linguaggio di comunicazione univoco (basato sul rischio) in ambito security all'interno della Amministrazione, con gli stakeholder esterni e con i fornitori.

Modelli di gestione della sicurezza e caratteristiche di comparto

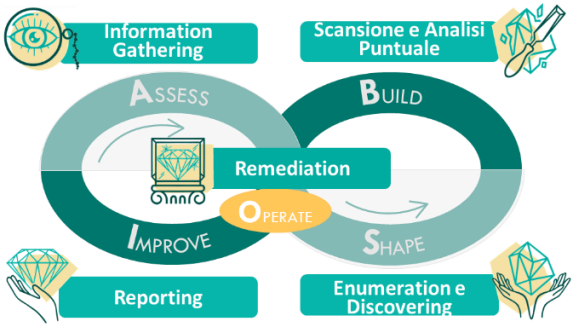
Disponiamo di **Modelli di gestione della sicurezza** già predefiniti per comparto delle PA con evidenza degli elementi rilevanti. Di seguito un esempio:

Caratteristiche comparto	Modello di Analisi dei Fabbisogni di Beni e Servizi – Driver di valutazione
Enti di grande dimensione (es. Ministeri) con estese infrastrutture IT e basi dati, Aziende in-house	► **Modello di Gestione della Sicurezza** completo ed articolato come da Security Framework. ► **Massima flessibilità** per assicurare continuità rispetto ai modelli esistenti se presenti. ► Modellazione di dettaglio dipendente del maggiore o minore grado di esternalizzazione dei servizi IT (es in Cloud – definizione di meccanismi di Cloud Security Governance) ► Ogni elemento può risultare critico. ► Non possono essere predefinite priorità di fabbisogno di acquisto in beni e servizi senza una approfondita situational awareness
Infrastrutture critiche: Operatori Servizi Essenziali (OSE), Perimetro di Sicurezza Nazionale Cibernetica (PSNC)	► **Modello di Gestione della Sicurezza** completo ed articolato come da Security Framework. ► **Disponibilità di template e modelli coerenti agli obblighi di reporting** (assessment e analisi dei rischi basati su CSF nazionale; ruoli necessari, canali di comunicazione verso le autorità preposte) ► In **caso di Operational Technology**, il modello prevede l'introduzione delle specifiche competenze necessarie, nonché l'opportuna estensione dell'anagrafica di **minacce** e vulnerabilità
Strutture sanitarie	► **Modello di Gestione della Sicurezza** commisurato alla missione della struttura: In caso di OSE - si veda modello infrastruttura OSE; In caso di strutture di ricerca - personalizzazione sotto-domini con livelli di maturità target meno stringenti (Security Target Profile) ► Focus sulla sicurezza dei sistemi nel perimetro dell'Ingegneria Clinica (nuovo sotto-dominio). ► Integrazione del Piano sicurezza con quello della struttura Sistemi Informativi
Enti di minori dimensioni e complessità	► Modello di Gestione della Sicurezza semplificato, ► Forte **focalizzazione sulla sensibilizzazione** in materia cyber e digitalizzazione e sulla crescita della cultura del rischio. ► In funzione della strategicità dei servizi e/o della criticità delle basi dati, il modello attinge dai modelli precedenti

5 Proposta progettuale per il servizio "Vulnerability Assessment"

"Se pensi che la tecnologia possa risolvere i tuoi problemi di sicurezza, non capisci i problemi e non capisci la tecnologia" (Bruce Schneier)

Obiettivi del servizio: La complessità e varietà tecnologica e applicativa, in genere riscontrabile presso le PA, determina uno scenario di rischio complessivo elevato, aggravato dalla crescente obsolescenza dei domini tecnologici rispetto al panorama delle minacce informatiche in costante evoluzione. In questo contesto i Servizi di Vulnerability Assessment forniti dal RTI hanno l'obiettivo di **valutare lo stato di esposizione alle vulnerabilità** quali ad esempio configurazioni di sicurezza errate, carenze sui livelli di protezione attivi, applicazioni web e serventi che espongano il contesto ad attacchi interni ed esterni, particolarmente utile in fase di definizione della strategia.



Metodologia: La nostra proposta progettuale valorizza la coerenza sia con i requisiti normativi del GDPR sia con le indicazioni delle Linee guida "Sviluppo software sicuro" AGID (https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro) ed è conforme all'**Open Source Security Testing Methodology Manual** (OSSTMM) di ISECOM ed a quanto definito dalla **Open Web Application Security Project** (OWASP) in tema di security assessment. Le risorse del RTI oltre a essere state parte attiva nella definizione delle suddette linee guida, si avvalgono di una consolidata metodologia, di strumenti leader di settore e acceleratori sviluppati ad-hoc (es. tool e script proprietari) per un aumento della qualità complessiva dei servizi erogati. La metodologia descritta nel corso del paragrafo prevede l'impiego di metodi operativi e strumenti specifici (automatizzati e non intrusivi) che assicurano la raccolta delle vulnerabilità adattandosi alle singole componenti presenti all'interno delle Amministrazioni: infrastrutture IT, IOT/Operational Technology/SCADA e applicative. L'utilizzo di una o più tecniche/strumenti è funzionale all'oggetto di analisi e alle diverse specificità tecnico/organizzative della PA. Le analisi del servizio, così come per i servizi di "Penetration test" e "Testing del codice", saranno contestualizzate nel perimetro e nell'ambiente di riferimento. La validità dei risultati si riferisce al momento in cui gli stessi vengono prodotti ed ai target oggetto di test.

Metodi operativi adottati: Di seguito sono riportati i principali metodi operativi che adotteremo nel corso della fornitura: Frictionless Assessment, Web App Scanning, Agent Assessment, Image Assessment, Passive Assessment, Passive Monitoring, Active Assessment, Active Query.

Strumenti a supporto: Comodo cWatch Vulnerability Scanner Nexpose Community, Tripwire IP360, OpenVAS, Nikto, Wireshark, Aircrack, Nessus Professional, Retina CS Community, Microsoft Baseline Security Analyzer (MBSA). Data la vastità del perimetro di un VA e la sua eterogeneità oltre a quelli indicati utilizzeremo ulteriori 25 strumenti che saranno selezionati in base alle specificità e senza oneri per l'Amministrazione.

5.1 Modalità di esecuzione del servizio

Per massimizzare efficacia e sostenibilità del VA, occorre **ridurre al minimo l'impatto sull'operatività** dei servizi, **utilizzare metriche standard** di valutazione, **configurare i tools** in base al contesto di analisi e **produrre deliverable** che esprimano in modo chiaro e completo tutte le informazioni utili per intraprendere eventuali azioni di mitigation o remediation. In base a quanto descritto, per tutte le attività di testing **si prevede l'utilizzo di un approccio di tipo "Safe Check"**: per ogni vulnerabilità testata gli schemi di attacco non vengono effettivamente portati a termine (tramite exploit o tentativi di ricreare direttamente l'attacco) in quanto le relative operazioni sono interrotte nell'istante che precede l'attacco vero e proprio. Questo metodo permette di evitare interruzioni dei servizi analizzati, nonché il verificarsi di situazioni che potrebbero danneggiare l'Amministrazione.

L'efficacia dell'approccio è assicurato inoltre: ► *dall'utilizzo di opportuni indicatori di rischio* calcolati secondo il framework **Common Vulnerability Scoring System - CVSS** di FIRST (Forum of Incident Response and Security Teams) le cui linee guida sono consultabili all'URL https://www.first.org/cvss e secondo il NVD del NIST (https://nvd.nist.gov/) ► *dall'utilizzo dei codici CVE nella descrizione delle vulnerabilità*. Il **Common Vulnerabilities and Exposures - CVE** rappresenta un dizionario di vulnerabilità e falle di sicurezza, note pubblicamente, le cui linee guida sono consultabili all'URL https://cve.mitre.org/, mantenuto dalla MITRE Corporation. Tale approccio di tipo *risk-based* viene affiancato da un approccio **policy-based**, che prevede la definizione di policy specifiche per il contesto tecnologico dell'Amministrazione e del relativo risk profile. Tali policy vengono utilizzate dagli strumenti citati in precedenza per **prioritizzare automaticamente le vulnerabilità** individuate e assegnarne le relative severità. L'efficacia del processo è assicurata dalla presenza di risorse professionali specializzate dedicate alla supervisione di ogni passo **integrando e perfezionando** quando necessario i risultati degli strumenti automatizzati. Di seguito la descrizione dell'approccio operativo proposto con particolare evidenza dei **risultati attesi** a fronte delle fasi di analisi, esecuzione e assegnazione automatica delle priorità/severità ai rischi di sicurezza:

Assess **Information Gathering:** Vengono raccolte le informazioni per **dettagliare la composizione dell'ecosistema IT** in essere analizzando ed indicizzando le informazioni rilevanti sia attraverso richieste ed operazioni svolte sui sistemi target che tramite interviste con i referenti IT dell'Amministrazione (es. CISO) **(Risultato A) ed il supporto dei Focal Point di Tematica e di Tecnologia** *(cfr. § 3 Struttura Organizzativa)*. In particolare, si effettuerà: ► **Condivisione ed approvazione del piano di test con l'Amministrazione**, contestuale al di kick-off avvio lavori, prevede la stesura di un piano operativo necessario a pianificare e organizzare in modo efficace l'effort delle figure coinvolte lato Amministrazione. Verrà inoltre condiviso il team di figure professionali del RTI a supporto delle attività (es. Security Principal, Penetration Tester Senior/Junior); ► **Raccolta delle**

informazioni relative alla configurazione dell'infrastruttura finalizzata, con il supporto dell'Amministrazione, a individuare i componenti infrastrutturali e/o applicativi oggetto delle attività di analisi, valutando al contempo le opportune fasce orarie di scansione al fine di tutelare l'Amministrazione da qualsiasi fermo.

Shape **Enumeration & Discovering:** Sulla base delle molteplici esperienze maturate, anche in contesti diversi dalla PA quali Financial Service, Manufacturing, Energy, Utilities, ed in coerenza con gli standard internazionali **OWASP e OSSTMM,** il team effettua le seguenti attività: → **Analisi sull'infrastruttura sistemistica o applicativa** oggetto delle attività, al fine di rilevare tutti i sistemi disponibili e i relativi servizi in esecuzione su di essi (discovering) **(Risultato B)**; ► **Creazione di un archivio di target** utile all'Amministrazione come mappa informativa aggiornata **(Risultato C)**. Su ognuno dei sistemi disponibili viene inoltre eseguita un'ulteriore scansione a al fine di rilevare i servizi in esecuzione facendo attenzione a includere i servizi "mascherati" o "nascosti", il relativo versioning e i possibili **punti di criticità (Risultato D)**.

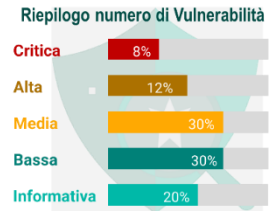
Build **Scansione:** i risultati ottenuti dalle fasi precedenti costituiscono un input per l'adeguata configurazione dei tool di scansione per la ricerca di vulnerabilità, al fine di poter reperire quante più informazioni possibili limitando al minimo il numero di **falsi positivi**. **L'attività di scansione viene condotta in due modalità** sulla base del livello di informazioni/dati inserite in input ai sistemi nel processo di scansione**:** ► **Black-box** senza ausilio di credenziali e ► **Grey/White-box** con tale ausilio. Le scansioni forniscono un primo livello di analisi poi consolidato in un report che, per ciascuna vulnerabilità rilevata, fornisce **informazioni sul target, CVE di riferimento, livello di criticità rispetto alla CVE, PoC**. **(Risultato E)**.

Build **Analisi puntuale: In base alle evidenze** emerse durante gli step precedenti, viene effettuata l'**Analisi delle sezioni critiche o di interesse** valutando l'eventuale livello di rischio **(Risultato F)**. Sulla base della nostra esperienza le vulnerabilità segnalate dalle scansioni automatiche degli strumenti comprendono spesso errori logici che possono non rappresentare un problema di sicurezza a livello di configurazione ma, se sfruttate da un'entità malevola, possono portare ad una violazione di confidenzialità, integrità o disponibilità dei dati, dei servizi o dell'intera infrastruttura.

Efficacia e concretezza delle modalità di esecuzione: Le attività descritte permettono l'acquisizione di risultati caratterizzate da: **Concretezza:** *l'approccio policy-based* descritto, frutto di anni di esperienza maturata in contesti operativi analoghi, garantisce alla PA di identificare lo stato di esposizione ai rischi cyber fornendo un quadro completo delle vulnerabilità rilevate su ogni singola componente dell'infrastruttura. **Efficacia**: *la corretta definizione dei perimetri operativi*, concordati con l'Amministrazione, assicura una gestione ottimale delle risorse a disposizione con una conseguente riduzione dell'effort. L'applicazione delle **linee guida e best practice** del settore viene effettuata tenendo in considerazione vincoli e necessità funzionali dei servizi erogati, delle applicazioni, dell'architettura e delle singole componenti tecnologiche presenti all'interno dell'Amministrazione. L'utilizzo di figure professionali altamente specializzate (*cfr § 16 Aggiornamento delle risorse professionali*), permette di affinare ulteriormente **l'analisi automatica prodotta dagli strumenti software** (assegnazione automatica delle priorità e severità ai rischi di sicurezza), validandone i risultati in funzione del contesto di rischio.

5.2 Proposta di elaborazione di un "Remediation plan" e Reportistica di sintesi

Improve **Reporting:** Durante le attività di "Reporting" vengono raccolti e classificati tutti i problemi di sicurezza rilevati al fine di fornire una visione dettagliata degli obiettivi, dei metodi e dei risultati prodotti e descritti in precedenza. In tale fase viene fatta sintesi delle evidenze emerse riclassificando le vulnerabilità in base alle severity definite all'interno dello standard **Common Vulnerability Scoring System (CVSS)** e associandogli un livello di priorità adeguato in funzione del contesto di esposizione della vulnerabilità stessa. In questo modo verrà assegnato un valore numerico ed oggettivo alla gravità delle vulnerabilità, permettendo di dare priorità alle azioni di remediation. Nella redazione dei report viene utilizzata la lista redatta dall'**OWASP 2021 Top 10** e la lista **OWASP 2016 Mobile Top 10** selezionati dal RTI per l'efficacia della assegnazione di rischio concentrata sulle vulnerabilità più rilevanti all'interno del singolo scenario tecnologico.



Il report di sintesi conclusivo è strutturato con informazioni di carattere qualitativo e quantitativo: ► **Scope:** fascia temporale in cui è stata eseguita l'attività di VA e per completezza vengono indicati i dettagli e le informazioni dei target oggetto delle analisi. L'indicazione temporale è elemento fondamentale in quanto consente di escludere, nelle successive fasi di analisi, eventuali correlazioni fra le attività degli analisti ed eventi eccezionali legati alla normale operatività dei sistemi. ► **Tools:** descrizione degli strumenti e tecniche utilizzate. ► **Executive Summary:** overview ad alto livello delle vulnerabilità, pensata per essere indirizzata ai diversi stakelholder dell'Amministrazione, con opportune raccomandazioni per l'implementazione di remediation o di fix immediate in caso di vulnerabilità di severity "high" o "critical" e a seconda che il target sia già stato rilasciato o meno in ambiente di produzione. ► **Technical Details** contenente i dettagli tecnici dell'attività con le evidenze riscontrate, corredata da una parte descrittiva delle vulnerabilità individuate e i potenziali impatti su risorse, infrastruttura, sistemi, processi, sistemi applicativi e aree di business dell'Amministrazione. Le vulnerabilità sono rappresentate in forma tabellare, fornendo per ognuna di esse le seguenti informazioni: **nome, categoria OWASP Top Ten, "Vector String"** (il modo in cui viene assegnata la severity alla vulnerabilità) e infine il **CVSS Base Score** (punteggio calcolato in base alla severity della vulnerabilità).

Operate **Remediation:** I risultati fin qui esposti consentono all'Amministrazione di acquisire piena consapevolezza sullo stato di esposizione alle vulnerabilità mediante raccolta di informazioni su servizi erogati, applicazioni, architettura e componenti tecnologiche. Il Remediation plan, documento di dettaglio personalizzato che riporta tutte le criticità individuate nelle fasi precedenti, fornisce una completa e chiara descrizione di tutte le attività legate ad uno specifico piano di rientro e necessarie per una corretta riduzione del

rischio cyber. L'approccio per la stesura di tale documento è ancora una volta di tipo *risk based*, che **considera le vulnerabilità in base alla potenziale superficie di attacco**, fornendo così una **priorità** ai singoli livelli di rischio in funzione delle necessità di business della singola Amministrazione. Nell'identificazione delle attività viene presa in considerazione la *sostenibilità dei singoli interventi* sia da un punto di vista economico che tecnologico, e la possibilità di efficientare i diversi interventi verificando ad esempio l'eventuale concorrenza di più vulnerabilità su di un singolo asset o parte di sistema. Le indicazioni operative per le singole attività di remediation prenderanno in considerazione eventuali *standard operativi* già in essere all'interno dell'Amministrazione, contribuendo all'ottimizzazione dell'intero processo.

Il remediation plan, personalizzato sulla singola Amministrazione, conterrà elementi qualitativi e quantitativi/dimensionali: ► **la descrizione della problematica rilevata**. La metodologia messa in atto dal Team descriverà e dettaglierà tutte le problematiche individuate con le relative informazioni. Oggetto della valutazione sarà l'impatto e valutazione qualitativa del rischio. La misurazione dei singoli eventi rischiosi consentirà di distribuirli secondo la loro criticità e di selezionare quelli su cui intervenire. ► **l'indicazione della root-cause.** L'obiettivo principale è fornire all'Amministrazione un chiaro livello di approfondimento sulle conseguenze che potrebbero scatenarsi in seguito ad uno specifico evento e che cosa si può/deve fare per evitare che possa accadere. La priorità degli eventi da analizzare è generalmente definita in base alla gravità dell'evento e al livello di rischio potenziale. ► **la descrizione delle attività da porre in essere per risolvere la problematica.** Consiste negli step di definizione delle azioni intraprendere affinché vengano effettuate le modifiche richieste a risolvere la problematica. Una stima qualitativa (alto, medio, basso, sulla base di criteri concordati con il referente dell'Amministrazione) dell'impatto economico, organizzativo e tecnologico dell'intervento. ► **una stima temporale dell'intervento.** Un'attenta proposta di elaborazione di remediation plan non può assolutamente precludere un attento studio temporale dell'intervento. Il nostro team di analisti si affiancherà all'Amministrazione nel comprendere eventuali esigenze operative, con l'obiettivo disegnare al meglio tutte le singole fasi in orari sostenibili per le attività di business al fine di ridurre gli impatti. ► **la priorità di implementazione dell'intervento**. permetterà al cliente di prendere contezza di come andranno pianificate e distribuite le modifiche sui target impattati (infrastrutturali o applicativi), corretta pianificazione e riavvio dei servizi e sistemi, eventuale valutazione nell'applicabilità di script o GPO policy per l'automazione del deploy, ed infine pianificazione della correzione di codice non sicuro (bugfix).

Le fasi di reporting e remediation fin qui descritte si distinguono per concretezza ed efficacia in quanto viene *prodotto un documento esaustivo* contenente il dettaglio delle singole vulnerabilità, le relative root-cause, il grado di severity e di priority, ed un remediation plan in grado *di indicare all'Amministrazione tutte quelle azioni che devono essere impiegate*, in termini di risorse economiche e/o tecniche funzionali, per una corretta risoluzione.

6 Proposta progettuale per il servizio "Testing Del Codice"

"Il test di un programma può essere usato per mostrare la presenza di bug, ma mai per mostrare la sua assenza"
(Edsger Wybe Dijkstra)

Obiettivi del servizio: indirizzare la produzione di applicazioni sicure ed efficienti minimizzando gli impatti operativi e l'effort dell'Amministrazione, grazie al supporto di professionisti altamente specializzati e all'adozione di strumenti in grado di automatizzare sia il testing del codice (statico e dinamico) che la produzione delle schede tecniche di dettaglio utili alla produzione dei report (technical e executive) elaborate dai Security Analyst.

Metodologia: L'approccio metodologico adottato dal RTI per il servizio di Testing del Codice si basa **sul framework DevSecOps curato dal Centro di Competenza di Application Security** ed è integrabile nel **Software Development Life Cycle (SDLC) d**ell'Amministrazione.

Standard adottati: Gli standard indicati sono stati individuati dal RTI sulla base di conoscenze approfondite dell'Information Security di riferimento quali ad esempio **AgID** (Linee guida per lo sviluppo sicuro del codice), **OWASP** (OWASP Software Assurance Maturity Model, OWASP Development Guide, OWASP Testing Guide, OWASP Cheat Sheets, OWASP Secure Coding Practices), **SAFECode** (Software Assurance Forum for Excellence in Code)**, WASC** (Web Application Security Consortium)**, CAPEC** (CERT Secure Coding e Common Attack Pattern Enumeration and Classification)**, OSSTMM** (Open Source Security Testing Methodology Manual).

In coerenza con l'approccio Idea, di seguito la metodologia adottata:

Assess **Definizione:** definizione della **mappa applicativa**, comprensione della **matrice di valutazione dei rischi** e della superficie d'attacco, indispensabile per definire la lista degli interventi dell'Amministrazione contraente (anche rispetto al SLDC adottato);

Shape **Prioritizzazione:** in relazione alla mappa applicativa e alla matrice dei rischi, definizione delle **priorità di intervento** (per aree, sistemi e applicativi) con valutazione specifica rispetto alle caratteristiche dell'Amministrazione contraente almeno rispetto a: processi, risorse e strumenti adottati per la gestione del SLDC;

Build **Configurazione:** in relazione alle priorità di intervento identificate nella fase precedente sono eseguite le attività di: **ridisegno del processo di SDLC** adottato dall'Amministrazione, la **configurazioni degli strumenti** messi a disposizione dal RTI (utili al testing del codice e al reporting ed integrati con il processo formalizzato) e l'**affiancamento delle risorse** dell'Amministrazione identificate al fine di garantire la corretta adozione di processi/strumenti e supportare l'Amministrazione nella corretta interpretazione

dell'executive report (vista di sintesi) e del techincal report (elenco delle vulnerabilità indentificate con relativa sezioni di codice) redatto dai Security Analyst sulla base delle evidenze prodotte dai vari tool configurati;

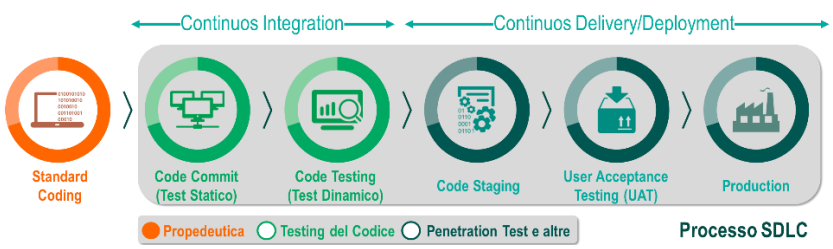
Remediation Plan: in relazione alle evidenze emerse viene formalizzato un **piano di miglioramento continuo** indispensabile per identificare e prioritizzare eventuali interventi su: processo SDLC (miglioramento del processo adottato), strumenti (attività di fine tuning sulle configurazioni eseguite) e risorse (attività di formazione e training-on-the-job). Verrà inoltre formalizzato un **remediation plan** sugli applicativi esaminati rispetto alle evidenze emerse dal technical report secondo un *approccio risk-based*.

Continuos Improvement: supporto continuativo all'Amministrazione contraente al fine di garantire il **miglioramento continuo** del processo di SDLC definito, degli strumenti adottati (configurati e integrati all'interno delle piattaforme di release e build management) oltre che del training-on-the-job offerto alle risorse dell'Amministrazione.

Strumenti a supporto: gli strumenti messi a disposizione dal RTI (Jenkins, Junit, SonarQube, Coverty, Fortify, Burp, Ghidra, JD-GUI, Frida, iNalyzer) permettono l'integrazione del framework DevSecOps all'interno del SDLC (*crf. § 6.3 Strumenti adottati e Integrazione per il Testing del Codice*)

6.1 Modalità di esecuzione del servizio

Descriviamo nel dettaglio le attività di testing del codice (statico, dinamico e mobile) rispetto alla catena di Continuous Integration e Continuous Delivery (CI/CD) schematizzata, coerente con lo standard DevSecOps proposto dal RTI



Attività/Servizio	Analisi Statica	Analisi Dinamica	Analisi Mobile
Standard & Plan	✓	✓	✓
Code Commit	✓	✗	✓
Code Testing	✗	✓	✓

Come riportato in figura i servizi di Testing del Codice si posizionano all'interno delle attività di "Standard&Plan", "Code Commit" e "Code Testing" della fase di Continuous Integration, garantendo la *completa efficacia e concretezza* rispetto alle modalità di esecuzione del servizio di seguito descritto.

6.1.1 Analisi Statica

Il servizio di Testing del Codice che intendiamo implementare per l'Analisi Statica è orientato **all'identificazione di vulnerabilità software presenti all'interno del codice, comprensivo della valutazione di librerie terze utilizzate, a *"commit-time"*,** ovvero ogni volta che viene eseguita l'archiviazione del codice sorgente sul repository software centrale dell'Amministrazione, grazie all'integrazione degli **strumenti di CI/CD**. Queste le fasi operative previste:

Standard & Plan: l'attività ha come obiettivo quello di **formalizzare gli standard di riferimento** (sia in termini di sicurezza che coding) da adottare per lo sviluppo e definire le logiche/regole di integrazione con i repository dell'Amministrazione indispensabili per lo scambio del codice sorgente (es. File Transfer Service proprietario del RTI oppure tramite integrazione con strumenti di code management dell'Amministrazione come SVN, CVS, Git o TFVC qualora non si decida di intervenire direttamente sugli ambienti di Build&Release Management dell'Amministrazione). In particolare, i test di sicurezza minimi che verranno eseguiti agiranno su aspetti semantici e sintattici rispetto a: service exposure, data validation, third-party library, control flow e buffer validation e faranno riferimento al documento di Best Practice e Linee Guida messo a disposizione dell'Amministrazione da parte del RTI.

Code Commit: ogni qual volta che verrà archiviato il codice sorgente all'interno del repository dell'Amministrazione (o all'interno dell'area di interscambio del codice sorgente tra Amministrazione e RTI), verranno avviati i test di sicurezza definiti durante l'attività precedente che andranno ad analizzare oltre che il codice sorgente prodotto tutte le librerie e servizi di terze parti utilizzate. Tale attività oltre a poter essere configurata attraverso gli strumenti di **Continuous Integration Server** messi a disposizione dal RTI *(crf § 6.3 Strumenti adottati e Integrazione per il Testing del Codice*) potrà essere schedulata manualmente ogni qual volta lo si riterrà opportuno. Per ogni vulnerabilità identificata verrà prodotta una **scheda tecnica** di dettaglio con le seguenti informazioni: ► **ID** (identificativo progressivo della issue rilevata costruita secondo la seguente sintassi <APPLIVATIVO><DATA><BUILDVERSION><PROGESSIVO>), ► **Tipologia** (riferimento specifico alla best-practice/linea guida violata) , ► **Descrizione** (descrizione sintetica dell'issue rilevata come da standard e linee guida), ► **Evidenza** (identificazione della sezione esatta di codice sorgente compresi eventuali file di configurazione) e ► **Severità** (valutazione della severità della violazione in termini di sicurezza come da standard adottati). Tali schede di dettaglio sono gestite direttamente dal Continuous Integration Server, messe in relazione ad una specifica build dell'applicativo in esame, e rese disponibili nel Portale di Fornitura per la consultazione on/off-line del team di lavoro che le utilizzerà per produrre sia il **Technical** che **l'Executive Report**.

Reporting (Technical & Executive): a partire dalle evidenze prodotte nella fase precedente i Security Analyst analizzeranno le informazioni riportate all'interno delle schede tecniche al fine di elaborare un report di dettaglio che oltre a considerare il livello di severità identificato valuta gli elementi di contesto riportati all'interno dei documenti di Mappa Applicativa e di Matrice dei Rischi prodotti entrambi nella fase di Assess. Più nello specifico il **Technical Report** arricchirà ogni scheda tecnica con le informazioni di: ► **Priorità di Risoluzione** (assegnazione di una priorità secondo la scala alta/media/bassa in relazione al rischio correlato valutato rispetto ad elementi come: sicurezza perimetrale, esposizione dei servizi su rete interna o esterna, tipologia accessi e frequenza, tipologia di informazioni conservate, livello di integrazione/isolamento, ecc.), ► **Difficoltà di Risoluzione** (valutazione dell'effort necessario per eseguire la patch di sicurezza secondo la scala alta/media/rapida) ► **Mitigazione** (azione correttiva su codice sorgente e/o file di configurazione da

apportare al fine di garantire il rientro l'issue di sicurezza). Per quanto concerne l'**Executive Report** i Security Analyst (a partire dal Technical Report) elaboreranno una vista di sintesi sia di tipo tabellare che grafica (in riferimento a quanto già riportato nella mappa applicativa) al fine di verificare e valutare opportunatamente eventuali rischi correlati. Tutte le informazioni elaborate sia a livello di Technical Report che Executive Report potranno essere consultate sia in modalità off-line (es. PDF/DOCS File) che on-line direttamente all'interno del Portale della Fornitura.

6.1.2 Analisi Dinamica

Il servizio di Testing del Codice che intendiamo implementare per l'Analisi Dinamica è orientato all'**identificazione delle vulnerabilità software presenti all'interno del codice binario/compilato degli applicativi**. L'analisi verrà condotta a *"compile-time"* (ossia ogni volta che viene eseguita la compilazione e il packaging del codice sorgente conservato all'interno del repository software centrale) grazie all'integrazione degli strumenti di CI/CD. Il servizio di analisi dinamica del codice sorgente sarà condotto attraverso le attività riportate nel seguito del paragrafo.

Standard & Plan: l'attività oltre a fare riferimento a quanto già descritto nel paragrafo relativo all'analisi statica del codice definisce la modalità di esecuzione dei test dinamici. In particolare, sarà possibile adottare un approccio di tipo **Stage&Gate** (test dinamici eseguiti a valle dei test statici e solo nel caso in cui siano garantiti i requisiti minimi di sicurezza) o **Passthrough** (test dinamici eseguiti direttamente a partire dal codice binario/compilato). In entrambi i casi i test di sicurezza dinamici minimi che verranno eseguiti verificheranno aspetti di: autenticazione, gestione della sessione, controllo degli accessi, validazione (e cifratura dei) dati, configurazione, audit, logging e error handling e faranno riferimento ad un documento di Best Practice e Linee Guida messo a disposizione dell'Amministrazione da parte dell'RTI e sulla base del quale verranno eseguiti i test del codice. A titolo esemplificativo e non esaustivo subito sotto sono riportati alcune pagine del documento.

ID Requisito	AUT-001
Descrizione	Le credenziali o in generale le informazioni sensibili che vengono scambiate tra client e server (quali cookie di autenticazione), oppure tra i vari livelli di un'applicazione web, dovrebbero sempre transitare su canale criptato. Assicurarsi che per le informazioni sensibili o riservate (come ad esempio username o password) sia implementato un canale cifrato (HTTPS) per l'invio delle informazioni. Utilizzare solo il metodo POST HTTP per l'invio delle credenziali.
Java/J2ee/Tomcat	Aggiungere nel file di configurazione web.xml il seguente codice: <security-constraint> <web-resource-collection> <web-resource-name>Security page </web-resource-name> <url-pattern>/web/login/signup.jsp</url-pattern> </web-resource-collection> <user-data-constraint> <transport-guarantee>CONFIDENTIAL</transport-guarantee> </user-data-constraint> </security-constraint>
Riferimento per verifica	OWASP-AT-001 http://www.owasp.org/index.php/Testing_for_credentials_transport_(OWASP-AT-001)

ID Requisito	CM-001
Descrizione	È necessario non esporre le console di management dell'applicazione, o in generale di permetterne l'accesso solo ad utenti locali (Intranet). L'accesso può quindi essere effettuato internamente attraverso un tunnel SSH o tramite VPN dall'esterno. Assicurarsi che non vi siano credenziali di default e che siano implementate password policy robuste. Tale requisito va applicato anche a tutte le console di management di Jboss ove utilizzato.
Java/J2ee/Tomcat	Modificare il file web.xml principale dell'applicazione di amministrazione con i seguenti valori: <security-constraint> <web-resource-collection> <url-pattern>/*</url-pattern> </web-resource-collection> <auth-constraint> <role-name>admin</role-name> </auth-constraint> </security-constraint> Si raccomanda, inoltre di non inserire nessuno specifico http-method nella restrizione di accesso, dal momento che apre potenzialmente l'accesso attraverso alcune modalità di attacco.
Riferimento per verifica	OWASP-CM-007 http://www.owasp.org/index.php/Testing_for_Admin_Interfaces_(OWASP-CM-007)

ID Requisito	SM-005
Descrizione	Per le applicazioni critiche, implementare un controllo che verifichi che un utente già autenticato non possa aprire una nuova sessione fino allo scadere della sessione attiva. Nel caso in cui si verifichi tale situazione, segnalare e tenere traccia dell'evento. Assicurarsi inoltre che l'IP dell'utente sia legato alla sua sessione quando l'utente accede alle risorse dell'applicazione.

Java/J2ee/struts	Aggiungere l'IP di provenienza in sessione all'atto del login.
	request.getSession().setAttribute("IP",request.getRemoteAddr());
	successivamente inserire in un filtro di controllo il check dell'IP da cui è generata la richiesta con quello in sessione.
	public void doFilter(ServletRequest req, ServletResponse res,
	FilterChain chain).{
	If(req.getSession()!=null &&
	!req.getSession().getAttribute("IP").equals(req.getRemoteAddr()))
	// potential session hijacking, throw loginException
	else
	// go on with filtering
	}

Riferimento per verifica	OWASP-SM-001 http://www.owasp.org/index.php/Testing_for_Session_Management_Schema_(OWASP-SM-001)

Code Testing: in relazione al tipo di approccio adottato (Stage&Gate Vs Passthrough) e ogni qual volta che verrà eseguito il packaging dell'applicativo a partire dal repository dell'Amministrazione (o depositato il file binario/compilato dell'area di interscambio tra Amministrazione e RTI) verranno avviati i test di sicurezza dinamici. Tale attività oltre a poter essere configurata attraverso lo strumento di **Continuous Integration Server messo a disposizione dal RTI** (*cfr. § 6.3 Strumenti adottati e Integrazione per il Testing del Codice*) potrà essere schedulata manualmente ogni qual volta lo si riterrà opportuno. I test guidati dal team mirano a verificare comportamenti del sistema anomali o potenziali vulnerabilità e si concentreranno sulla **superficie esposta di una applicazione up-&-running** testandone il comportamento dinamico rispetto ad una sollecitazione esterna malevola. Ciò richiede la predisposizione di **staging areas** (gestite anche direttamente dagli strumenti di Continuous Integration) all'interno delle quali predisporre un ambiente sicuro e controllato ove eseguire i test preventivati attraverso degli strumenti descritti nel seguito del documento. Analogamente a quanto già descritto nel caso di analisi statica del codice per ogni vulnerabilità identificata verrà prodotta una **scheda tecnica** di dettaglio secondo le modalità ed il tracciato già descritte in precedenza con l'aggiunta dell'informazione relativa al **Digest** (identificativo del codice/package binario analizzato).

Reporting (Technical & Executive): a partire dalle evidenze prodotte a "compile-time" il Team analizzerà le informazioni riportate all'interno delle schede tecniche al fine di elaborare un report di dettaglio che oltre a considerare il livello di severità identificato valuti gli elementi di contesto sintetizzati all'interno del documenti di Mappa Applicativa e di Matrice dei Rischi prodotti entrambi nella fase di Assess analogamente a quanto già descritto nell'ambito dell'ambito dell'analisi statice del codice.

6.1.3 Mobile

Il servizio di Testing del Codice che intendiamo implementare per l'Analisi delle Applicazioni Mobile è orientato all'identificazione delle vulnerabilità del software sia a livello di codice sorgente che a livello di codice binario/compilato. L'analisi verrà **condotta seguendo quanto già presentato per l'analisi Statica e Dinamica del codice** seguendo la logica di servizio a canone annuo (rispetto le fasce 1,2 e 3 del Capitolato Tecnico).

Standard & Plan: La modalità di esecuzione per le Applicazioni Mobile (iOS, Android e Windows Phone) sarà solo di tipo **Stage&Gate** (test dinamici eseguiti a valle dei test statici e solo nel caso in cui siano garantiti i requisiti minimi di sicurezza) e punterà a rilevare le vulnerabilità già presentate in precedenza con particolare enfasi alla verifica delle policy adottate per gestire gli accessi ai dati e alle funzioni del dispositivo.

Code Commit: ogni qual volta che verrà eseguito un commit all'interno del repository dell'Amministrazione (o all'interno dell'area di interscambio del codice sorgente tra Amministrazione e RTI), verranno avviati i test di sicurezza definiti durante l'attività precedente che andranno ad analizzare oltre che il

codice sorgente prodotto tutte le librerie e servizi di terze parti utilizzate (modalità scansioni periodiche). L'analisi statica del codice sorgente Java/Swift avverà usando software di settore quali XCode (Ghidra) nativo per iOS o Lint nativo di Android (JD-Gui) con gli obiettivi e tecniche di analisi citati all'inizio del paragrafo per l'analisi statica del codice ma usando una base di conoscenza di regex uniche per l'ambiente Mobile, in compliance alla OWASP Top 10 Mobile, OSSTMM ed altri standard di settore.

Code Testing: ogni qual volta che verrà eseguito il packaging dell'applicativo a partire dal repository dell'Amministrazione (o depositato all'interno di APP market place "interni") verranno avviati i test di sicurezza dinamici (modalità scansioni periodiche). L'analisi dinamica dell'APP avverrà in sandbox ovvero in ambiente chiuso e controllato facendo leva su strumenti di settore quali Frida, iNalyzer, Charles, al fine di evidenziare eventuali problemi di sicurezza di natura Web, cercando di determinare se l'applicazione in questione comunica con interfacce di altri sistemi e/o applicazioni così come con altre risorse collegate che potrebbero avere un impatto sulla sicurezza globale del sistema, evidenziando eventuali errori logici che potrebbero portare ad una grave violazione di confidenzialità, integrità o disponibilità dei dati, dei servizi o dell'intera infrastruttura.

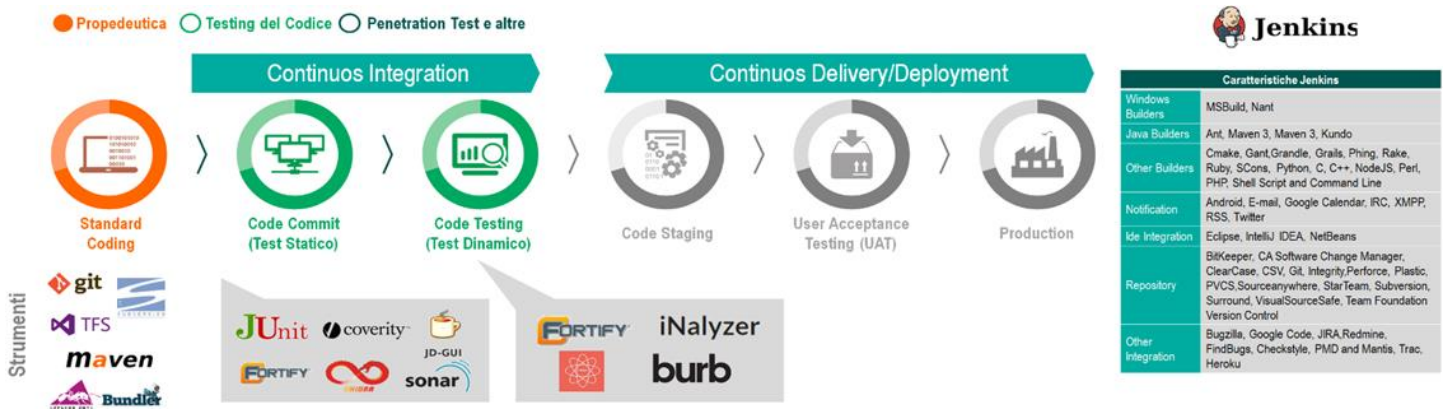
Reporting (Technical & Executive): a partire dalle evidenze prodotte il Team specializzato analizzerà le informazioni riportate all'interno delle schede tecniche al fine di elaborare un report di dettaglio che oltre a considerare il livello di severità identificato valuti gli elementi di contesto sintetizzati all'interno del documenti di Mappa Applicativa e di Matrice dei Rischi prodotti entrambi nella fase di Assess analogamente a quanto già descritto nell'ambito dell'ambito dell'analisi statica del codice.

6.2 Remediation Plan

In relazione ai test sul codice eseguiti (statici, dinamici e mobile) i Security Analyst, elaboreranno il **remediation plan** indispensabile per identificare le attività di bonifica da implementare su ciascuna componente impattata comprensivo della road-map di interventi. L'approccio alla base della stesura di tale documento è di tipo *risk based*, e vengono considerate le vulnerabilità in base alla potenziale superficie di attacco, fornendo così una priorità ai singoli livelli di rischio in funzione delle necessità di business della singola Amministrazione. Nell'identificazione delle attività verrà presa in considerazione la *sostenibilità dei singoli interventi* sia da un punto di vista economico che tecnologico, e la possibilità di efficientare i diversi interventi verificando, ad esempio, l'eventuale concorrenza di più vulnerabilità su di un singolo asset o parte di sistema. Le indicazioni operative per le singole attività di remediation prenderanno in considerazione eventuali standard operativi già in essere all'interno dell'Amministrazione, *contribuendo all'ottimizzazione dell'intero processo*. Il documento in particolare conterrà almeno le sezioni ► **Vulnerability Technical Analysis** dove si classificherà, mediante criteri di violazione agli standard sopra citati, ciascuna vulnerabilità confermata e si darà evidenza della relativa prioritizzazione formulata sulla base della sua intrinseca gravità, della raggiungibilità dell'asset coinvolto, della difficoltà di sfruttamento, della vulnerabilità stessa e di quanto questa sia nota, e dell'impatto in caso di sfruttamento; ► **Vulnerability Remediation** dove creare e condividere con l'Amministrazione criteri di analisi per suggerire in maniera costruttiva, per ciascuna vulnerabilità comunicata nei technical ed executive reports, un piano di bonifica della stessa inclusivo di pre-requisiti necessari all'espletamento dell'attività (es. uso di libreria open-source non presente in perimetro, upgrade della versione del linguaggio di programmazione, ecc.), offrendo continuativo supporto agli stakeholders per la corretta ed esaustiva implementazione di ogni azione di bonifica.

6.3 Strumenti adottati e Integrazione per il Testing del Codice

Come già descritto in precedenza la metodologia adottata dal RTI si basa sul framework DevSecOps che ha come obiettivo quello di semplificare, standardizzare e automatizzare il processo di sviluppo software sia in termini di operations che di developing garantendo un approccio security-by-design e security-by-default attraverso l'adozione di una serie di strumenti di automazione integrati nel SDLC e orchestrati dal Continuous Integration Server. Il RTI nell'ambito della fornitura dei servizi in oggetto, metterà a disposizione dell'Amministrazione il tool Continuous Integration Server (Jenkins) senza alcun onere aggiuntivo per l'Amministrazione che consente piena integrabilità con gli strumenti identificati a capitolato tecnico (SVN - Subversion, CVS - Concurrent Versions System, Git, TFVC - Team Foundation Version Control). Inoltre, oltre ad essere riportate le caratteristiche principali del server di integrazione è rappresentato il SDLC standard proposto dall'RTI (con relativi strumenti messi a disposizione dell'Amministrazione da parte dell'RTI per ogni fase del processo) nel caso in cui si preveda un'integrazione sui sistemi di Code Repository.



7 Proposta progettuale per il servizio "Supporto all'analisi e gestione degli incidenti"

Ci sono solo due tipologie di organizzazione: quelle che sono state hackerate e quelle che lo saranno
(Robert Muller, direttore del FBI)

Obiettivi del servizio: supportare le Amministrazioni nelle fasi di analisi, progettazione e verifica post-mortem dei processi di gestione degli incidenti di sicurezza, nonché nella opportuna condivisione delle informazioni ottenute e delle diagnosi effettuate al fine di minimizzare l'insorgenza di ulteriori incidenti e l'impatto avverso.

Metodologia: il RTI possiede un bagaglio di profonda esperienza di Security Incident Management maturata nel corso di centinaia di progetti, svolti avvalendosi di profonda competenza su best practice e standard nazionali, (es. CERT-Agid) e internazionali, quali la "Computer Security Incident Handling Guide" del NIST. in base alla quale ha potuto sviluppare un **approccio metodologico** ad hoc, illustrato in figura:

Assess **Preparazione:** vengono svolte le attività necessarie a supportare le Amministrazioni nella **definizione, implementazione e miglioramento continuo di un processo** di gestione degli incidenti di sicurezza finalizzato a prevenire, rispondere, limitare gli impatti e apprendere dagli incidenti di sicurezza. Tali attività includono, ad esempio, la creazione e gestione di un piano di risposta agli incidenti (IRP), la definizione delle modalità di classificazione della remediation dell'incidente, delle modalità di analisi dei log e degli eventi, dei processi di analisi post-mortem, dei processi di escalation verso le entità interne ed esterne (inclusi CSIRT-Italia, organi di polizia giudiziaria), delle modalità di gestione delle comunicazioni interne/esterne e degli aggiornamenti, ecc.

Rilevazione e analisi e Contenimento, erogazione e recovery sono attività incluse nell'ambito della fornitura del servizio SOC del Lotto 1 e pertanto qui non trattate.

Improve **Post-incident activities**: vengono svolte le attività finalizzate a **identificare le root-cause dell'incidente e adottare le necessarie azioni a livello tecnologico e / o organizzativo** per prevenire la sua reiterazione in futuro. Tali attività includono tipicamente l'acquisizione, in loco o da remoto, delle evidenze digitali afferenti all'incidente mediante tecniche di informatica forense, nonché la successiva analisi delle stesse mediante strumenti e tecniche specifiche per il caso di specie (es. log analysis, network forensics, malware forensics, system forensics, ecc.).

Metodi: Di seguito l'elenco dei principali metodi adottati nel corso della fornitura: ► **organizzazione e facilitazione di workshop dedicati** con i referenti chiave dell'Amministrazione al fine di rilevare le *capability* già in essere per la gestione degli incidenti in termini di procedure, prassi operative, competenze, strumenti tecnologici, ecc., nonché a comprendere le necessità e le aspettative per l'intervento in corso; ► **utilizzo di checklist e template per l'Incident Forensics**, realizzate tramite strumenti di office automation, finalizzate a delimitare, tramite compilazione guidata con i referenti tecnici dell'Amministrazione, il perimetro dell'incidente e identificare quindi gli asset oggetto di acquisizione e analisi forense.

Standard adottati: Di seguito l'elenco dei principali standard adottati nel corso della fornitura: ► **ISO/IEC 27035-1:2016 - "Part 1**: Principles of incident management". ► **ISO/IEC 27035-2:2016 - "Part 2**: Guidelines to plan and prepare for incident response". ► **ISO/IEC 27035-3:2020** - "Part 3: Guidelines for ICT incident response operations". ► **ISO/IEC 27037:2012** - "Guidelines for identification, collection, acquisition, and preservation of digital evidence". ► **ISO/IEC 27042:2015** - "Guidelines for the analysis and interpretation of digital evidence". ► **NIST SP 800-61 Rev. 2** - "Computer Security Incident Handling Guide". ► **NIST SP 800-83 Rev. 1** - "Guide to Malware Incident Prevention and Handling for Desktops and Laptops". ► **Linee guida per lo sviluppo e la definizione del modello nazionale di riferimento per i CERT regionali dell'AGID**. ► **Pubblicazioni e guide di fonti istituzionali** quali CSIRT Italia e CERT-AgID con particolare riferimento alle "linee guida per lo sviluppo e la definizione del modello nazionale di riferimento per i CERT regionali" dell'AgID, che forniscono numerosi strumenti utili quali matrici di classificazione e prioritizzazione degli incidenti, tassonomie e workflow dei processi di gestione e comunicazione.

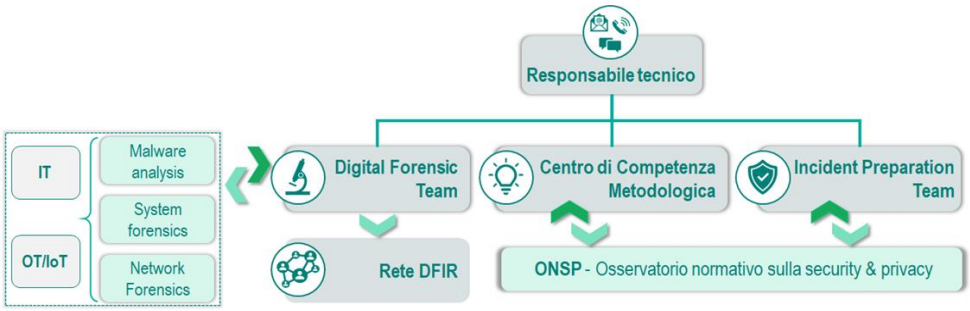
Strumenti a supporto: A supporto delle attività di gestione degli incidenti il Security Principal/Analyst e i Forensic Experts utilizzano i migliori strumenti disponibili sul mercato, siano essi open source o proprietari già acquistati dal RTI, che può quindi metterli a disposizione senza alcun onere per l'Amministrazione. Il RTI dispone inoltre di **acceleratori sviluppati ad-hoc** per un aumento della qualità complessiva dei servizi erogati e il contenimento dei tempi di esecuzione. **Strumenti proposti per le attività di analisi forense:** ► **EnCase, Axiom, X-Ways, Autopsy Digital Forensics**: piattaforme di Digital Forensics, utilizzate sia per l'acquisizione dei dispositivi con tecniche forensi, sia per la loro analisi; ► **UFED**: strumento per eseguire attività di Mobile Forensics, dall'acquisizione del dispositivo sul campo all'analisi dei suoi contenuti sul campo o in laboratorio; ► **CAINE Linux, Ttsurugi Linux, SIFT Workstation**: distribuzioni Linux che possono essere utilizzate sia in modalità "live" per acquisire in modo forense dei sistemi da analizzare, sia come workstation per l'analisi vera e propria degli artefatti acquisiti; ► **Plaso**: strumento utilizzato per generare la cosiddetta super timeline, utile a dettagliare quanti più eventi possibili durante l'analisi di un dispositivo digitale, come il suo traffico Internet, le e-mail ricevute e inviate, le operazioni eseguite dall'utente, ecc.; ► **Timesketch**: piattaforma web per l'analisi collaborativa della super timeline, generata per esempio tramite Plaso; ► **Volatility**: framework utilizzato per l'analisi forense della memoria volatile (es. RAM) dei dispositivi analizzati, tramite il quale si possono ottenere utili informazioni per arricchire la super timeline, o per analizzare un malware che si nasconde in memoria; ► **Velociraptor**: strumento open source utile per il monitoraggio

degli endpoint durante o a seguito di un incidente, ivi inclusa la raccolta degli artefatti dagli stessi per una loro analisi forense. ► gli **strumenti messi a disposizione da fonti istituzionali** quali il CERT-AgID e il CSIRT (es. https://cert-agid.gov.it/strumenti/).

Strumenti proposti a supporto delle attività dell'Incident Preparation Team: ► **Incident Best Practice Repository** documentale, centralizzato a livello di fornitura, utilizzato per la continua alimentazione e condivisione di una knowledge-base sulle *migliori pratiche, casi d'uso reali e success story* relative all'implementazione di processi di gestione degli incidenti di sicurezza in ambito PA, preventivamente anonimizzate con la messa a disposizione delle sole informazioni utili a fornire valore aggiunto in termini di uniformità ed efficacia alle attività progettuali. ► **CSIRT Maturity assessment**, toolkit ENISA - European Union Agency for Cybersecurity, che consente di misurare in maniera efficace, ripetibile e comparabile il livello di maturità di un Computer Security Incident Response Team secondo il modello SIM3 definito dall'Open CSIRT Foundation, nonché ulteriori strumenti messi a disposizione da ENISA come la *good practice guide* "How to setup up CSIRT and SOC"

7.1 Modello organizzativo adottato e strumenti proposti per le attività di analisi forense

Il modello organizzativo prevede i seguenti **organismi e strutture**: ► Un **Responsabile Tecnico**, corrispondente alla figura professionale di *Senior Security Analyst* prevista dalla documentazione di gara, raggiungibile in modalità multicanale (telefono, e-mail, messaggistica istantanea, ecc.), la cui responsabilità principale sarà raccogliere gli elementi preliminari per comprendere la natura e le caratteristiche di urgenza delle richieste pervenute e instradarle affinché possano essere prese in carico coerentemente. ► Un **Digital Forensic Team**, composto da professionisti con competenze verticali ed esperienze specifiche in tutte le attività di Digital Forensic quali analisi dei log e degli eventi, malware forensic, network e system forensic, ecc., che coordina a sua volta ► una **Rete DFIR – Digital Forensic Incident Responder** capillare a livello nazionale, costituita dai *Forensic Experts* previsti dalla documentazione di gara che operano in qualità di professionisti qualificati e specializzati nell'acquisizione di evidenze digitali mediante strumenti e metodologie proprie dell'informatica forense. Tale rete è opportunamente dimensionata per poter rispondere tempestivamente anche in caso di incidenti sistemici che dovessero coinvolgere multiple Amministrazioni. ► Un **Incident Preparation Team**, composto da professionisti con esperienza pluriennale sul campo ed esperti di best practice, standard, metodologie e procedure di Security Incident Management, responsabile del supporto di carattere metodologico previsto nella fase di Incident Preparation e della quality assurance delle attività di Digital Forensics. L'Incident Preparation Team lavora inoltre a stretto contatto con l'**ONSP - Osservatorio normativo sulla security & privacy** (*cfr. § 3 Struttura Organizzativa*), al fine di intercettare e gestire eventuali evoluzioni normative che potrebbero avere impatti sulla gestione degli incidenti per le Amministrazioni, come ad esempio la pubblicazione di nuovi regolamenti / linee guida / modelli per la notifica degli stessi. ► Dei **centri di competenza**, organizzati secondo una struttura matriciale. Tale struttura prevede la collaborazione tra personale specializzato nelle infrastrutture tecnologiche IT e OT/IoT (*horizontal*) in termini, ad esempio, di sistemi operativi e applicazioni più comunemente attaccati, e di personale altamente qualificato in attività (*vertical*) di network forensics, system forensics e malware analysis Tale struttura a matrice consentirà al team operativo di poter combinare e usufruire in ogni momento delle conoscenze necessarie sia in termini di sistemi impattati, sia di strumenti e best practice per le attività di analisi.

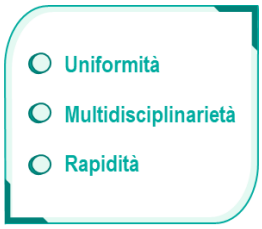


Il ***meccanismo di funzionamento*** del modello prevede che il Responsabile Tecnico (RT) agisca da interfaccia unica nei confronti del cliente, recependone le esigenze e indirizzandole verso i team operativi secondo i rispettivi ambiti di competenza e compatibilmente con il carattere di urgenza della richiesta. Il RT indirizza pertanto la richiesta verso l'*Incident Preparation Team* in caso di necessità di supporto metodologico e attiva il *Digital Forensic Team* in caso di attività di analisi post-mortem, avvalendosi eventualmente della *Rete DFIR* per l'acquisizione forense di dispositivi IT / OT / IoT localizzati sul territorio.

In relazione ai ***collegamenti con altre strutture*** il Responsabile Tecnico agisce da interfaccia nei confronti dei responsabili degli altri servizi previsti sia nel Lotto 1 sia nel Lotto 2. In particolare, il servizio di *Incident Management* è strettamente collegato al servizio di *Security Operation Center (SOC)* del Lotto 1 che gestisce operativamente gli incidenti di sicurezza a valle dei quali vengono effettuate le attività di analisi i cui risultati possono pertanto essere utilizzati sia come elemento di verifica indipendente circa l'efficace funzionamento del SOC, sia come "*lesson learned*" per promuovere il suo miglioramento continuo. Ulteriori elementi di collegamento con gli altri servizi possono essere identificati nell'ambito della compliance normativa, per quanto riguarda la gestione e notifica di *data breach* al Garante della Privacy, piuttosto che nell'ambito della Security Strategy, ove le "*lesson learned*" apprese possono essere utilizzate per indirizzare le scelte strategiche e i fabbisogni dell'organizzazione.

Efficacia e funzionalità del modello organizzativo adottato per le attività di analisi forense: Il modello organizzativo descritto ci consente di **indirizzare al meglio i fattori critici di successo** individuati dal RTI per il presente servizio, massimizzandone pertanto **l'efficacia**. ► *Multidisciplinarietà delle competenze a disposizione dell'analisi Forense*: la **presenza di team dedicati con competenze verticali**, che caratterizza il modello organizzativo illustrato, garantisce la copertura di tutte le competenze previste dal servizio in tutti i possibili contesti tecnologici che caratterizzano le diverse Amministrazioni. Ogni incidente rappresenta un *unicum* e può richiedere l'utilizzo di professionalità diverse, ad esempio in ambito

analisi dei log, analisi forense di malware, reti o sistemi, piuttosto che **acquisizione forense di una vasta gamma di dispositivi in ambito IT (Information Technology), OT (Operational Technology) o IoT (Internet of Things)**. L'accesso a **centri di competenza tematici** messi a disposizione dal RTI (*cfr. § 3 Struttura Organizzativa e § 14 Innovazione*) consente l'accesso a **professionalità diverse** da parte del RTI per affrontare problematiche complesse che necessitano analisi multidisciplinari eseguite da figure di competenza diversa. I nostri professionisti, infatti, possono vantare esperienza in tale settore a livello nazionale e internazionale, sia per l'**ambito Information Technology** (es. postazioni di lavoro, portatili, tablet, smartphone, server, NAS) con sistemi operativi Windows, macOS e Unix-like, sia per l'**ambito Operational Technology / IoT** (es. engineering workstation, field DB, SCADA, industrial PC) con sistemi operativi basati su Windows e Linux. Riteniamo tali competenze multidisciplinari fondamentali per Amministrazioni che, ad esempio, fanno largo uso di dispositivi IoT, come quelle che operano nel settore sanitario. Oltre a ciò, risulta fondamentale il **confronto con un network internazionale**, che fornirà ai professionisti impegnati sulle attività oggetto del contratto un canale privilegiato per fruire di informazioni sulle modalità di contrasto rispetto alle ultime minacce locali e internazionali, per analizzare minacce precedentemente sconosciute (es. malware reverse engineering, 0-day analysis, ecc.), nonché per confrontarsi su strumenti, tecnologie e best practice rispetto a casi d'uso. ► *Rapidità di esecuzione*: è elemento chiave per ► **acquisire il contenuto nelle memorie volatili** dei dispositivi impattati, fondamentale per la completezza dell'analisi forensica post-mortem ► **l'identificazione delle azioni di miglioramento utili a prevenire la reiterazione** dell'incidente o la sua diffusione a livello sistemico con impatto su altre PA ► **i processi di notifica previsti a livello normativo**, tra cui ad esempio ► **l'obbligo di notifica per i data breach** previsto dall'Art. 33 del GDPR entro le 72 ore dalla relativa scoperta, > l'obbligo di notifica "senza ingiustificato ritardo" previsto dalla Direttiva NIS per gli incidenti di sicurezza informatica, ► **i necessari processi di escalation verso le entità interne ed esterne** (inclusi CSIRT-Italia, organi di polizia giudiziaria, ecc.). **Il modello** da noi proposto **garantisce rapidità** di esecuzione sulla base di ① presenza della figura di Responsabile di Servizio **su base continuativa**, raggiungibile attraverso molteplici canali di comunicazione ② presenza di un **Digital Forensic Team dedicato**, che si avvale della presenza di una rete capillare sul territorio di DFIR, resa possibile dalla forte e ramificata presenza geografica del RTI sul territorio italiano; ③ predisposizione di **Go-Bag distribuite geograficamente sul territorio**, contenenti strumenti tecnologici essenziali per espletare le necessarie attività di acquisizione forense ad opera dei **DFIR** (es. write-blocker, chiavette USB *bootable* con sistemi operativi dedicati all'acquisizione forense, dischi con cifratura hardware su cui riversare i dati acquisiti, set di connettori/adattatori USB/SATA/ecc., set di cacciaviti, moduli di chain of custody prestampati, ecc.). Il modello garantisce inoltre la flessibilità organizzativa per gestire eventuali picchi di lavoro (*cfr. § 15 Flessibilità delle risorse*), e abilita la condivisione di conoscenze tra professionisti che supportano Amministrazioni diverse. ► *Uniformità dei processi di gestione degli incidenti di sicurezza tra PA*: in ambito sicurezza **è importante considerare le diverse PA come parte di un sistema integrato a livello Paese**, dialoganti tra loro attraverso una rete di CERT territoriali al fine di scambiarsi rapidamente informazioni e scongiurare incidenti a rilevanza sistemica, in coerenza con le linee guida AgID per lo sviluppo e la definizione del modello nazionale di riferimento. A tale scopo **il RTI persegue una diffusa uniformità di linguaggi, modelli e tassonomie** garantita tramite l'utilizzo di un modello organizzativo che **coniughi presenza locale con meccanismi di condivisione territoriale e coordinamento centrale**. L'utilizzo sistematico da parte del RTI **degli standard internazionali** in ambito Forense elencati in precedenza e di procedure rigorose e ispirate a queste best practice di settore, è elemento chiave per garantire sia l'uniformità dei processi tra PA sia la rigorosità del processo di indagine forense in se stesso. Il modello consente inoltre la gestione efficace dei **flussi di comunicazione interni e nei confronti dell'Amministrazione**, garantendo la presenza nel gruppo di lavoro di tutte le competenze necessarie per rispondere efficacemente a richieste specifiche e dialogare con tutte le parti coinvolte (vedi anche punto successivo)



7.2 Proposta di elaborazione di documento di "catena di custodia"

Per quanto riguarda la **catena di custodia**, abbiamo sviluppato un **modello realizzato ad hoc** ispirato alle best practice e affinato nel corso di centinaia di acquisizioni forensi effettuate sul campo. Riteniamo tale modello particolarmente efficace in quanto coniuga ► La **completezza di informazioni** necessaria a garantire la rigorosità del processo che recepisce, in particolare, i requisiti minimi in materia di Chain of Custody definiti all'interno dello standard ISO/IEC 27037:2012. ► La **facilità di utilizzo** che rappresenta un elemento fondamentale per non ingessare le attività di acquisizione forense svolte sul campo, spesso caratterizzate da tempistiche stringenti e condizioni logistiche precarie.

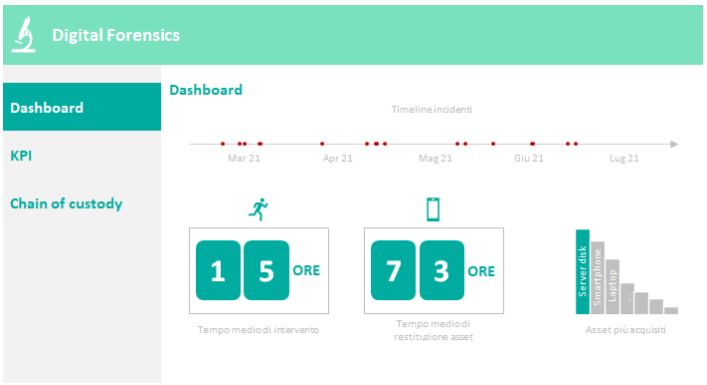
Rappresentazione delle informazioni qualitative e dimensionali oggetto di tracciamento. Il modello proposto di Catena di Custodia prevede **due sezioni**: ① una sezione di **Descrizione evidenze** dedicata all'inventariazione di tutti gli asset oggetto di acquisizione (es. dischi, smartphone, ecc.), attraverso l'assegnazione di un numero identificativo univoco (ID) e la raccolta di tutte le informazioni dimensionali e qualitative (es. modello, numero seriale, condizioni estetiche e funzionali, ecc.) necessarie a identificare in maniera puntuale ciascun asset e il suo stato al momento dell'acquisizione

Descrizione evidenze						
ID evidenza	**Quantità**	**Dimensioni**	**Descrizione (modello, # seriale, condizioni, danneggiamenti)**			
001	1	-	T480s	001	1	-

② una sezione **Catena di Custodia**, finalizzata a tracciare tutti i passaggi di consegna degli asset acquisiti attraverso l'annotazione del relativo ID, delle parti coinvolte (consegnatario e ricevente), delle motivazioni del passaggio di consegna e delle eventuali modifiche subite dall'asset nel periodo di custodia.

Catena di Custodia						
ID evidenza	**Data / ora**	**Consegnato da (firma e # documento di identità)**	**Preso in carico da (firma e # documento di identità)**	**Motivo del passaggio di custodia**	**Eventuali modifiche intercorse nel periodo**	**Note**
001	10/09/2021 ore 15:00	Mario Rossi	Giuseppe Verdi	Il passaggio di custodia è avvenuto in quanto …	Nessuna	-

Metteremo inoltre a disposizione delle Amministrazioni un applicativo web dedicato sul Portale della Fornitura per consentire un rapido accesso da parte delle PA aderenti. Sarà nostra premura caricare e mantenere aggiornati su tale applicativo tutti i documenti di Catena di Custodia, sia sotto forma di scansione, sia sotto forma di dati strutturati. In tale modo, **le Amministrazioni potranno in qualsiasi momento eseguire ricerche per conoscere lo stato di tutti e soli gli asset di cui sono proprietarie** che sono stati oggetto di acquisizione forense, nonché lo stato di completamento delle attività. Su una sezione dedicata del medesimo applicativo forniremo inoltre **statistiche, in forma aggregata e anonima, accessibili da tutte le amministrazioni**, che illustrano il tempo medio di intervento, il tempo medio di restituzione dell'asset, la quantità media di asset oggetto di acquisizione per indagine e le tipologie di asset maggiormente oggetto di acquisizione.

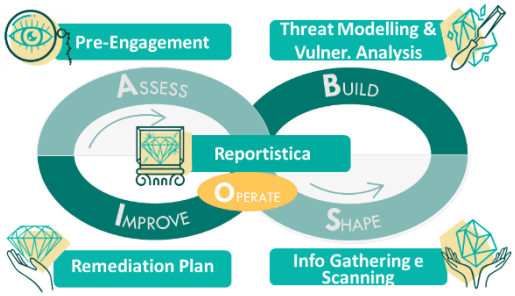


8 Proposta progettuale per il servizio "Penetration Testing"

"La sicurezza nell'Information Technology è come chiudere a chiave la casa o l'auto: non ferma i cattivi, ma li indirizza verso un obiettivo più facile" (Paul Herbka, Presidente dell'ISSA Advisory Board)

Obiettivi del servizio: obiettivo del servizio è fornire una soluzione in grado di garantire l'analisi e valutazione dei punti di vulnerabilità in termini di sicurezza rispetto ai sistemi IT dell'Amministrazione (Infrastrutture, Applicativi e IoT). In particolare, verranno condotti degli attacchi informatici simulati (preservando in ogni caso la disponibilità del servizio) al fine di evidenziare e classificare le diverse vulnerabilità. Il RTI nel corso degli anni grazie ad importati progetti di Information Security, in diversi settori di mercato, ha consolidato e maturato un approccio metodologico standard utile a presidiare: ► **gli ambiti infrastrutturali** (vulnerabilità interne/esterne al sistema, vulnerabilità delle reti wireless); ► **gli ambiti applicativi** (vulnerabilità delle applicazioni web e mobile, vulnerabilità delle API, phishing); ► **gli ambiti IoT** (vulnerabilità dell'infrastruttura di trasmissione e dei device connessi). Tale approccio è basato sulle *best practices* nazionali ed internazionali di settore come (a titolo esemplificativo e non esaustivo): **PTES** (Penetration Testing Execution Standard), **OWASP** (Open Source Web Application Security Project) e **OSSTMM** (Open Source Security Testing Methodology Manual), **MITRE ATT&CK** (Adversaries Tactics, Techniques and Common Knowledge), Unified Cyber Kill Chain, European Framework for Threat Intelligence-Based Ethical Red Teaming, G-7 Fundamental Elements of Threat-Led Penetration Testing e GFMA Framework for the Regulatory Use of penetration Testing and Red Teaming in the Finance Industry.

Metodologia: l'approccio metodologico IDEA, illustrato nel dettaglio nel paragrafo seguente, risulta caratterizzato, ove necessario, rispetto agli ambiti prima identificati (infrastrutturali, applicativi e IoT) e rispetto alle **cautele adottate nell'esecuzione dei penetration test** al fine di evitare il sovraccarico e/o l'indisponibilità dell'ambiente oggetto di valutazione e dei dati in coerenza con quanto previsto dalla normativa GDPR. Le evidenze raccolte saranno poi elaborate dagli specialisti messi a disposizione dal RTI all'Amministrazione all'interno di opportuni report (*cfr. § 8.2* Proposta di deliverable documentali con evidenza della rappresentazione delle informazioni qualitative e dimensionali oggetto di analisi).



Strumenti a supporto: gli strumenti messi a disposizione nell'**ambito infrastrutturale** sono nmap, Metasploit, netcat, wireshark, aircrack-ng, nell'**ambito applicativo** Burp Suite e Fortify e nell'**ambito IoT** Baudrate.py, Esptool, Flashrom, Minicom, Binwalk, Strings, IDAPro, Radare2, Qumu, Gatttool, hcitool, GNURadio e Killerbee.

8.1 Modalità di esecuzione del servizio: Penetration Testing e Cautele Adottate

Descriviamo nel dettaglio le modalità di esecuzione del servizio strutturate appositamente per *assicurarne concretezza ed efficacia*:

Assess **Assess cross-ambito**: in questa fase verrà svolta l'attività di **pre-engagement** necessaria alla definizione del **perimetro di scansione** in relazione all'oggetto di analisi.

Cross-ambito	Cautele adottate
Attività e Oggetti	**Metodi e Benefici**
Pre engagement sul perimetro di scansione: ambito di analisi, tempistiche, modalità di esecuzione dei test (white-box, grey-box o black-box), ambiente su cui svolgere le attività (produzione, UAT, integration, dev, ecc.) ed eventuali vincoli tecnici/operativi da considerare.	**Pen Ten Agreement – PTA** da concordare con i Key Stakeholders (es. CISO, Responsabile SOC, Responsabile NOC, ecc.): regole di ingaggio, aspetti operativi per lo svolgimento dell'attività, tempistiche, range temporali, perimetro tecnologico, ambienti target (sviluppo, pre-produzione ecc.) segmenti di rete da cui verranno effettuate le scansioni

Catena di erogazione end-to-end (es. Catena IoT: Device Connesso, Trasporto, APIs, Applicativo e Infrastruttura) incluse componenti applicative e infrastrutturali utili all'erogazione del servizio oggetto di valutazione.	e/o simulati gli attacchi a seconda modalità concordate (White/Grey Box Test). Il PTA ci consente di evitare disservizi dovuti a blocchi di segmenti di rete dovuti ad azioni di difesa dei firewall durante le attività di scansione, di concordare procedure di gestione di eventuali allarmi generati da sistemi SIEM, IDS o IPS e di attivare procedure automatiche/manuali causanti disservizi in risposta all'attacco simulato.

Shape specifica per ambito: in questa fase verrà svolta l'attività di **Info Gathering e Scanning** che ha l'obiettivo di raccogliere quante più informazioni possibili circa la *"superficie di attacco"* attraverso l'utilizzo di tecniche e strumenti tipici dell'ambito oggetto di analisi.

Ambito infrastrutturale	Cautele adottate
Attività e Oggetto	**Metodi e Benefici**
Approccio passivo tramite tecniche di OSINT e attivo tramite scansione di porte/servizi grazie all'utilizzo dei tool messi a disposizione del RTI (es. nmap, Metasploit, netcat, wireshark, aircrack-ng, ecc.). L'insieme delle informazioni raccolte, oltre a guidare le fasi successive della metodologia, permetterà tra le altre cose di individuare eventuali componenti non conformi alle policy aziendali (es. presenza servizi SMTP, NFS, FTP, SMB, ecc.).	Al fine di ridurre i possibili impatti derivanti dai Penetration Test le attività vengono concordare nel minimo dettaglio con i team di NOC e SOC e in ogni caso in fasce orario di scarso utilizzo/carico delle risorse. Le attività di scansione sono generalmente eseguite sugli ambienti di produzione, a meno di infrastrutture di tipo Virtuali e/o Software Defined per le quali si può operare su repliche fedeli dell'infrastruttura di esercizio.
Ambito Applicativo	**Cautele adottate**
Attività e Oggetto	**Metodi e Benefici**
Approccio passivo tramite l'integrazione e validazione delle informazioni esposte a livello applicativo da eventuali "registri" (es. SOA Registry, RESTful Service Registry, ecc.). **Approccio attivo** tramite la scansione di risorse esposte mediante tecniche di Crowling con l'utilizzo di strumenti specifici messi a disposizione dall'RTI (es. Burp Suite, Fortify, ecc.).	Attività condotte secondo quanto condiviso nel Pen Test Agreeement, garantendo il coordinamento delle attività tra NOC/SOC dell'Amministrazione (ove presenti) e il team di esperti messi a disposizione dal RTI. Qualora possibile tutte le attività vengono condotte su ambienti di collaudo/pre-produzione gestiti direttamente nell'ambito del SDLC e secondo i dettami del framework DevSecOps già presentato nell'ambito del servizio di Testing del Codice.
Ambito IoT	**Cautele adottate**
Attività e Oggetto	**Metodi e Benefici**
Approccio di **verifica dell'intera catena di erogazione del servizio** utilizzando le medesime tecniche già presentate per gli ambiti infrastrutturali e applicativi, valutando utleriori aspetti di Info Gathering e Scanning tipiche delle soluzioni protocollari di comunicazione adottate dai device connessi (es. Zigbee, zWave, 6LoWPAN, LPWAN, ecc.), attraverso l'adozione da parte del RTI di strumenti specifici (es. GNURadio). Vengono inoltre eseguite verifiche hardware del dispositivo come ad esempio: porte UART, tampering e JTAG Debbuing al fine di verificare eventuali superfici di attacco aggiuntive.	**Relativamente ai device connessi** è strettamente necessario valutare, grazie all'analisi della documentazione tecnica messa a disposizione dai vendor, i meccanismi di protezione automatica dei singoli dispositivi che se attivati potrebbero determinare il blocco del servizio. Inoltre, ove tecnicamente possibile, si effettuano delle scansioni passive sfruttando tecniche di analisi del traffico di tipo Port Mirroring e/o Tapping (replica fisica del dato) oltre che l'installazione e configurazione di device "gemelli" al fine di isolare quanto più possibile le attività di testing.

Build specifica per ambito: vengono svolte le attività di **Threat Modelling/Vulnerability Analysis al fine di identificare i differenti vettori di attacco e le superfici vulnerabili che verranno utilizzati per il PenTest, necessarie per condurre l'attività di Exploitation (e successivamente di Post-Exploitation) che sfrutta** tecniche e strumenti tipici dell'ambito oggetto di analisi indispensabili per confermare l'effettiva presenza di vulnerabilità oltre che il livello di criticità calcolata in base all'impatto che quest'ultime generano sul core-business dell'Amministrazione e su possibili dati di natura riservata

Ambito infrastrutturale	Cautele adottate
Attività e Oggetti	**Metodi e Benefici**

Utilizzo di exploit customizzati dai penetration tester di RTI anche attraverso l'utilizzo di strumenti a supporto quali: Metasploit, Exploit DB, ecc. Gli exploit customizzati sono stati sviluppati del team di penetration test di RTI che gode di un'esperienza pluriennale nel settore del penetration testing, e vengono utilizzati per attaccare anche i sistemi più aggiornati, bypassando i moderni meccanismi di protezione attivi e presenti sui sistemi quali Antivirus, EDR (Endpoint Detection and Response) ed EPP (Endpoint Protection Platform).	A seconda delle caratteristiche riconducibili agli ambienti infrastrutturali, le attività in questa fase verranno condotte adottando un approccio di tipo "Safe Check" (cfr. § 5), per cui per ogni vulnerabilità testata i relativi schemi di attacco non vengono effettivamente portati a termine salvo espresse indicazioni dell'Amministrazione. Nel caso vengano identificate vulnerabilità il cui sfruttamento porti all'indisponibilità dall'ambiente o dei dati, verrà verificata con l'Amministrazione la possibilità di condurre il test in un ambiente speculare. Nei penetration test di tipo black-box il comportamento in caso di potenziale sfruttamento di una vulnerabilità dovrà essere necessariamente condiviso a monte nel Pen test Agreement descritto sopra.
Ambito Applicativo	**Cautele adottate**
Attività e Oggetti	**Metodi e Benefici**
Attività condotta da un team di esperti messi a disposizione dell'Amministrazione che agiranno in relazione alle evidenze emerse in fase di shape e che, attraverso adozione di strumenti a supporto (Whireshark, Burp, ecc.) eseguiranno gli exploit applicativi. I test, eseguiti con il supporto dei centri di competenza del RTI, si baseranno su una base di conoscenza consolidata maturata tramite lo svolgimento di progettualità/attività di penetration test e agiranno sugli ambiti: Configuration e Deployment Management, Authentication, Authorization, Identity Management, Session Handling, Service Exposure, Input Validation, Error/Exception Handling, Weak Cryptography, Business Logic	Sfruttando la catena e gli strumenti di CI/CD, ed in linea con il processo di SDLC descritto nell'ambito del servizio di Testing del Codice, le attività di penetration test verranno svolte su aree dedicate. Tali ambienti saranno gestiti, ove possibile, virtualmente attraverso l'adozione di strumenti "infrastructure-as-a-code" (es. open-stack) e con l'utilizzo del Continuous Integration Server Jenkins *(cfr. § 6Proposta progettuale per il servizio "Testing Del Codice")* per la parte di deploy automation al fine di garantire il completo isolamento con gli ambienti di esercizio e evitare eventi di Data Corruption.
Ambito IoT	**Cautele adottate**
Attività e Oggetti	**Metodi e Benefici**
Data la peculiarità d'ambito, l'attività viene condotta a livello hardware (agendo fisicamente su eventuali porte UART aperte JTAG exploitation e Dumping Flash Memory), a livello firmware (agendo attraverso tecniche di reverse engineering, forced upgrade, Binary Analysis) e a livello radio (agendo a livello protocollare attraverso tecniche di sniffing-modifying-replaying di pacchetti o tecniche di jamming) attraverso l'utilizzo di alcuni strumenti specifici (livello hardware: Baudrate.py, Esptool, Flashrom, Minicom e Screen; livello firmware: Binwalk, Strings, IDAPro, Radare2 e Qumu; livello radio: Gatttool, hcitool, GNURadio e Killerbee).	Analogamente a quanto già descritto nell'ambito delle attività della fase di Shape, al fine di ridurre al minimo gli impatti sull'infrastruttura di esercizio (intera catena), il RTI metterà a disposizione i propri centri di competenza e laboratori di testing per simulare in ambiente controllato le condizioni di esercizio del singolo servizio utilizzando device IoT di test.

Improve & Operate cross-ambito: in questa fase verranno raccordate tutte le informazioni raccolte nelle precedenti fasi e generati dei **deliverables inerenti alle attività svolte con informazioni qualitative e dimensionali fruibili sia da personale tecnico sia non tecnico**. In questa fase verrà inoltre redatto un **Remediation plan** che permetterà all'Amministrazione di risolvere le falle di sicurezza riscontrate e fornirà delle raccomandazioni di sicurezza per ottenere un improvement della security posture dell'intera organizzazione. In particolare, **l'attività di Reportistica sarà finalizzata alla raccolta delle evidenze relative alle vulnerabilità confermat**e. Queste verranno riportate step-by-step in maniera da poter essere riprodotte e verificabili in caso di eventuali audit. La classificazione delle vulnerabilità prenderà in considerazione almeno le seguenti dimensioni: Impegno richiesto ad un attaccante per sfruttare con successo la vulnerabilità, impatto che si avrebbe sul business aziendale qualora la vulnerabilità venisse effettivamente confermata (rischio legale, di business, di immagine, di compliance, operativo) e Impatto in termini di Riservatezza, Integrità e Disponibilità del dato (coerentemente anche a quanto previsto dalla normativa GDPR). Le evidenze raccolte lungo lo svolgimento dell'iter metodologico saranno poi elaborate dagli specialisti messi a disposizione dal RTI all'Amministrazione all'interno di opportuni report illustrati di seguito.

8.2 Proposta di deliverable documentali con evidenza della rappresentazione delle informazioni qualitative e dimensionali oggetto di analisi

L'obiettivo della seguente proposta legata alla fase di Reporting è quello di **fornire una visione dettagliata ed esaustiva dei contenuti che verranno forniti all'interno dei deliverable documentali (o reportistica)**. Tali deliverable conterranno le evidenze delle azioni intraprese all'interno delle fasi operative precedenti, l'effetto di tali azioni ed i relativi risultati. Verranno inoltre specificati i singoli passi necessari intrapresi per sfruttare le vulnerabilità rilevate. La classificazione e la presentazione delle singole vulnerabilità identificate seguiranno le seguenti classificazioni di Severity Levels, in accordo ai framework internazionale adottati e citati in precedenza.

Severity score	Description
Critical (9.0 – 10.0)	Vulnerabilità che permette ad un attaccante di ottenere il controllo completo di una risorsa informatica (es. un server web) o permette di ottenere dati business-critical o legalmente rilevanti (es. dati protetti da leggi sulla privacy).
High (7.0 – 8.9)	Vulnerabilità che permette ad un attaccante di compromettere la riservatezza/integrità/disponibilità dei dati dell'utente o delle risorse.
Medium (4.0 – 6.9)	Vulnerabilità o esposizione di dati che non portano ad compromissione diretta dall'applicazione, ma possono essere utili all'attaccante per compromettere il target.
Low (0.1 – 3.9)	Vulnerabilità o esposizione di dati non rilevanti, ma che rappresentano una non conformità delle best practice di sicurezza seppur non introducono un rischio rilevante immediato.

I seguenti deliverable documentali descriveranno in modo efficace il dettaglio delle attività di Penetration Test eseguite sui target oggetto di analisi: ►**Executive Report: overview ad alto livello delle vulnerabilità riscontrate**, con informazioni dimensionali quali il numero totale delle vulnerabilità riscontrate e la percentuale delle vulnerabilità trovate suddivisa per severity critica, alta, media e bassa. Sarà inoltre presente un codice che permetterà di identificare univocamente ognuna delle diverse vulnerabilità nel caso di necessità da parte dell'Amministrazione. Il documento sarà fruibile anche da personale non tecnico. ►**Technical Report: dettagli tecnici dell'attività di PT svolta.** Per ognuna delle vulnerabilità riscontrate durante l'attività, si forniscono contenuti dimensionali relativi al **numero di risorse impattate da ogni vulnerabilità, numero di parametri vulnerabili, numero di servizi esposti vulnerabili e numero di componenti affette da vulnerabilità**. Viene mostrato il dettaglio sulla vulnerabilità rilevata e i contenuti qualitativi come immagini di tool e opportuna configurazione per sfruttare una vulnerabilità, porzioni di codice utilizzate per attaccare i sistemi, tecniche utilizzate per bypassare AV, EDR o EPP, azioni e comandi eseguiti sui sistemi oggetto di analisi. Il report consente la comprensione di ogni step dell'attacco eseguito in maniera puntuale e precisa, rendendo il processo chiaro ed eventualmente ripetibile. ►**Remediation Plan: misure da mettere in atto** per ogni vulnerabilità individuata, customizzate per lo specifico target oggetto di analisi e necessarie per sanare il problema di sicurezza rilevato e renderlo non più sfruttabile. Arricchito da una tabella riassuntiva che contiene l'elenco delle vulnerabilità ordinate secondo la gravità in modo da consentire la prioritizzazione delle bonifiche da applicare.

Inoltre, all'interno di ognuno dei deliverable saranno presenti sezioni con informazioni necessarie per contestualizzare quanto svolto: ►**Scope**: informazioni dimensionali relative al numero di target oggetto di analisi, finestre temporali concordate per lo svolgimento dei test, numero di utenze fornite, indirizzi sorgente e destinazione specifici dell'attività. Permette di consultare le informazioni relative a quanto concordato in fase di **Assess** in maniera concisa, efficace e schematica, permettendo ad eventuali auditor esterni di verificare in maniera semplice e concreta quanto svolto durante le attività di Penetration test. ►**Tools**: informazioni qualitative su tools e tecniche utilizzate durante le attività di Penetration Test, che consentono l'installazione e la configurazione dei tool necessari per replicare gli esatti step che hanno portato allo sfruttamento delle vulnerabilità identificate, rendendo il processo completamente trasparente e riproducibile sia per necessità in fase di audit sia per necessità durante la fase di applicazione delle bonifiche suggerite dal team RTI.

9 Proposta progettuale per il servizio "Compliance Normativa"

"Noi pensiamo di discutere soltanto di protezione dei dati, ma in realtà ci occupiamo del destino della nostra società"
(S. Rodotà)

Il contesto straordinario in cui opera l'intero sistema Paese e, di riflesso, la Pubblica Amministrazione, richiede rapidità ed efficacia senza precedenti nell'erogazione di servizi alla cittadinanza, anche alla luce degli importanti pacchetti di misure stanziate a livello comunitario per fronteggiare l'emergenza sanitaria e socioeconomica. In tale scenario, il servizio di **"Compliance Normativa"** supportato dal Centro di competenza Risk & Compliance consente alle Amministrazioni di sopperire alle criticità e ai limiti che quotidianamente si trovano a fronteggiare con riferimento alla protezione dei dati personali. Sulla base della nostra esperienza, infatti: ► la privacy è concepita spesso come un **mero adempimento normativo**, e non ne sono valorizzati **gli aspetti etici e tecnologici** che consentirebbero all'Amministrazione di perseguire in maniera strutturata il percorso verso la trasformazione e innovazione digitale; ► **è spesso carente l'approccio "federativo"** nella gestione di servizi e banche dati pubbliche, ovvero le Amministrazioni che erogano servizi affini o che interrogano vicendevolmente le proprie banche dati, dovrebbero cooperare per indirizzare fin dal principio i requisiti di privacy; ► **non sempre è prevista l'adeguata interoperabilità** e messa a fattor comune delle banche dati pubbliche; tali elementi consentirebbero di ottenere risultati significativi in termini di fiducia, efficacia e trasparenza che la cittadinanza richiede al Sistema Paese.

Obiettivi del servizio: la nostra **profonda conoscenza dei processi in ambito privacy**, declinati in funzione delle specificità dei singoli Comparti della PA, ci consente di offrire un servizio finalizzato non solo a garantire il raggiungimento della piena "compliance normativa" ma, in aggiunta, **l'adozione efficace di prassi e strumenti di governo e gestione dei trattamenti dei dati personali**, con un approccio scalabile in funzione degli scenari di rischio applicabili alle finalità di trattamento.

Metodologia: con riferimento all'approccio metodologico, riteniamo fondamentale **distinguere**, nella complice normativa, **tra attività puntuali (o se necessario ricorsive) e continuative**. L'approccio puntuale (di cui alle prime 4 fasi di seguito declinate) consente un **supporto end-to-end all'Amministrazione**, a partire dall'analisi del contesto fino ad arrivare al supporto nell'implementazione delle azioni correttive. L'approccio continuativo (di cui alla fase Operate sotto declinata), invece, **garantisce la sistematicità delle attività day-by-day, in linea con quanto prescritto** dalla normativa

privacy in relazione al continuo miglioramento dei presidi di sicurezza. Le attività seguono il framework Idea consolidato già in numerose esperienze presso primarie Amministrazioni Pubbliche:

Assess **Comprensione contesto:** la fase di Assess è finalizzata alla comprensione del contesto, in relazione ai processi di trattamento dei dati personali con un focus sul perimetro IT, nonché alla valutazione del livello di maturità attuale dell'Amministrazione in ambito privacy;

Shape **Gap Analysis:** la fase di Shape è finalizzata alla definizione e stima in termini di criticità degli scostamenti (Gap Analysis) tra il livello di maturità attuale e il livello di maturità atteso dell'Amministrazione, dove quest'ultimo rappresenta il livello di maturità che si intende raggiungere, in relazione ai requisiti per i quali non è stata raggiunta la piena conformità, nonché degli obiettivi strategici da perseguire;

Build **Piano di interventi:** la fase di Build consente di identificare le azioni di intervento, formalizzate all'interno di un apposito Piano di Interventi oggetto di continuo monitoraggio e miglioramento, da implementare per perseguire il livello di maturità atteso;

Improve **Azioni correttive:** la fase di Improve è finalizzata al supporto nell'implementazione delle azioni correttive incluse nel Piano di Intervento;

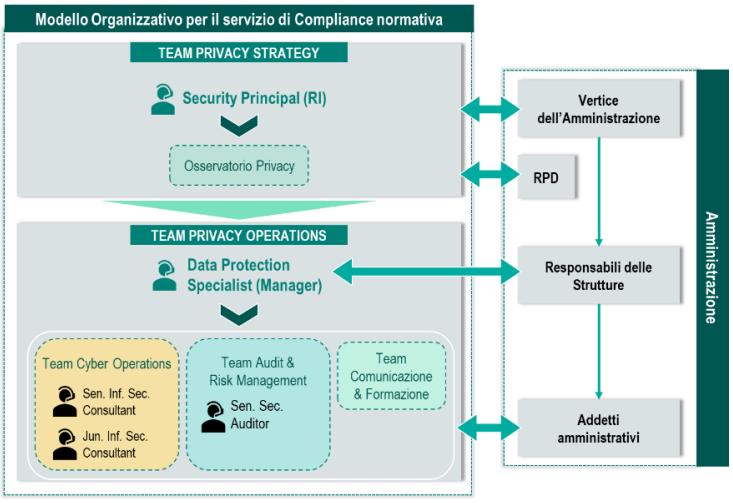
Operate **Supporto e gestione:** la fase di Operate è finalizzata a garantire un supporto specialistico nella gestione day-by-day non solo degli adempimenti privacy, ma anche nel perseguimento degli obiettivi e indirizzi strategici dell'Amministrazione.

Strumenti di automazione e governo: al fine di garantire il governo dei processi di trattamento dei dati personali, nonché assicurare il rispetto degli adempimenti normativi, mettiamo a disposizione una **suite di strumenti di Privacy Management** che integra soluzioni custom per la singola Amministrazione con strumenti di Office Automation; si tratta di un insieme di moduli per l'automazione, governo e monitoraggio di tutti gli adempimenti privacy, quali: **gestione del Registro delle attività di trattamento; gestione dei data breach, integrazione dei principi di Privacy by Design & by Default, esecuzione della Data Protection Impact Assessment.**

Standard adottati: per l'esecuzione delle attività, ricorriamo a metodologie e strumenti definiti in linea con best practice e standard internazionali. Nello specifico, il nostro approccio risulta essere basato sull'analisi del rischio, ovvero, le misure di sicurezza sono commisurate ai rischi per i diritti e le libertà degli interessati. A tale scopo, **mutuiamo nei nostri strumenti i principi degli standard più recenti e all'avanguardia in ambito privacy e cybersecurity, quali, a titolo esemplificativo, ISO/IEC 27701:2019, ISO/IEC 29134:2017, ISO/IEC 31000:2018, Enisa Threat Landscape Report, ecc.**

9.1 Modello organizzativo, elementi di efficacia e funzionalità

Intendiamo adottare il seguente modello organizzativo:



Team Privacy Strategy (Service Unit): il Team di Privacy Strategy fornisce supporto nel definire, indirizzare e migliorare la strategia dell'Amministrazione con riferimento a obiettivi e linee di indirizzo da perseguire in ambito privacy. Esso è costituito da: ► **Security Principal**: esso costituisce il punto di contatto unico con il vertice Amministrativo e con il Responsabile Protezione Dati ("RPD" o "DPO") dell'Amministrazione. Supporta l'Amministrazione in occasione di tavoli tecnici e/o incontri istituzionali con l'Autorità di Controllo e con i RPD di altre Amministrazioni. Garantisce il rispetto, in ciascuna attività del Servizio eseguita dal Team Privacy Operations, degli indirizzi strategici che l'Amministrazione persegue in ambito privacy; ► **Osservatorio Privacy**: esegue continua sorveglianza normativa, analisi e adozione delle nuove prassi e strumenti in ambito privacy in linea con nuovi standard e framework internazionali. La tempestiva rilevazione di trend ed elementi innovativi nelle prassi internazionali è funzionale alla definizione di indirizzi strategici all'avanguardia. In caso di evoluzioni normative, le comunica al Team Privacy Operations cui fornisce supporto nella valutazione degli impatti per l'Amministrazione in termini di adempimenti privacy. **Team Privacy Operations (Service Unit)** verifica periodicamente il livello di maturità attuale dell'Amministrazione, anche alla luce delle evoluzioni normative comunicate dall'Osservatorio Privacy e supporta l'implementazione delle azioni correttive. Esso è composto da:

DATA PROTECTION SPECIALIST

Manager responsabile del coordinamento del **Team Privacy Operations**; si interfaccia quotidianamente con la struttura del Titolare per il tramite dei Responsabili delle Funzioni/Direzioni dell'Amministrazione e attiva prontamente i sotto-team Cyber, Audit & Risk Management e Comunicazione & Formazione in relazione alle attività di privacy by design, DPIA, Privacy Culture e aggiornamento del registro dei trattamenti, laddove necessario

TEAM CYBER OPERATIONS

Costituito da **Senior Information Security Consultant** e **Junior Information Security Consultant**, mette a disposizione competenze specialistiche in ambito Cyber security sia dal punto di vista della security governance, sia di conoscenza di prassi e soluzioni tecnologiche per la tutela dei dati (e.g. cifratura, data retention, strong authentication, Identity and Access Management). Gli scostamenti rilevati in termini di misure di sicurezza ICT sono prontamente comunicati al Team Privacy Strategy che li declina in nuovi indirizzi strategici per l'innalzamento del livello di maturità dell'Amministrazione dal punto di vista tecnologico

TEAM AUDIT & RISK MANAGEMENT

Costituito dal **Senior Security Auditor**, mette a disposizione dell'Amministrazione comprovata esperienza nell'applicazione delle metodologie di audit e privacy risk management, che consentono di verificare periodicamente l'osservanza della normativa da parte dell'Amministrazione e contribuire alla definizione di azioni correttive secondo un approccio risk-based. Gli scostamenti rilevati in termini di mitigazione dei rischi sono prontamente comunicati al Team Privacy Strategy che li declina in nuovi indirizzi strategici per l'innalzamento del livello di maturità con riferimento alle metodologie di audit

TEAM COMUNICAZIONE E FORMAZIONE

Composto da **professionisti con comprovata esperienza nei rapporti istituzionali tra differenti PA**, mediante la partecipazione a tavoli tecnici, comitati, etc. Inoltre, i nostri professionisti applicano metodologie di **culture & awareness** avanzate per aumentare la sensibilità privacy dei funzionari amministrativi. Il dialogo costante tra Team Comunicazione & Formazione e Team Privacy Strategy consente di integrare la "privacy culture" negli indirizzi strategici dell'Amministrazione.

Efficacia e funzionalità del modello organizzativo: alla luce del disposto normativo privacy nazionale e comunitario, delle prassi più evolute sul panorama internazionale e, da ultimo, delle difficoltà che le Amministrazioni si trovano a fronteggiare nell'operatività quotidiana –in precedenza rilevate – riteniamo che i **fattori critici di successo** per l'adozione di un modello di gestione della privacy maturo siano: ▶ *adottare modalità e canali di comunicazione efficace e tempestiva* tra il Titolare (i.e. l'Amministrazione) e il RPD al fine di innescare prontamente gli adempimenti privacy; ▶ *concepire procedure e misure per la protezione dei dati* non solo come mezzo per il raggiungimento della compliance normativa e, conseguentemente, per evitare le sanzioni, ma come strumento atto a perseguire gli indirizzi strategici che l'Amministrazione si è posta in termini di digitalizzazione e innovazione; ▶ *essere in grado di rilevare tempestivamente evoluzioni normative*, valutarne applicabilità e impatti sui processi dell'Amministrazione; ▶ disporre di un *centro di controllo che indirizzi gli aspetti privacy* in maniera complessiva; ▶ integrare nei processi dell'Amministrazione la *"cultura del dato" a tutti i livelli e ambiti di intervento*. In tale contesto, il **modello organizzativo** da noi proposto si rileva particolarmente **efficace e funzionale** nell'indirizzare e abilitare i sopramenzionati fattori critici di successo:

Comunicazione efficace

Prevediamo risorse e team dedicati: il Data Protection Specialist e, nella sua interezza, il Competence Center Risk & Compliance supporta day-by-day nelle operatività quotidiana le singole Direzioni/Funzioni che costituiscono la struttura del Titolare; in tal modo, siamo in grado di rilevare near real-time variazioni ai processi esistenti o la definizione di nuovi servizi/processi di trattamento che richiedono l'avvio di attività di privacy by design & by default e di valutazione dei rischi ex artt. 25, 32 e 35 del GDPR. Non appena rilevata un'esigenza in tal senso, avviene la comunicazione verso il Team Privacy Strategy, che coopera a stretto contatto con il RPD al fine di attivare i relativi adempimenti *privacy*

Visione evoluta delle procedure e misure di privacy

Il modello organizzativo dimostra **efficacia e flessibilità**, garantite dalla presenza del Team di Privacy Strategy, in grado di tenere in considerazione non solo i requisiti normativi, ma anche gli **obiettivi** che si intende perseguire nel breve, medio e lungo termine, tra cui: ① **semplificazione dei processi di raccolta di dati personali** (es. laddove opportuno, incrementare il ricorso all'autodichiarazione e rafforzare i controlli ex post circa la veridicità delle informazioni dei cittadini); ② **potenziamento dell'interoperabilità tecnica** tra banche dati pubbliche; ③ **efficienza nelle procedure di aggiornamento ed esattezza** dei dati personali al fine di ridurre i rischi legati a erroneo rigetto di domande/istanze; ④ **principi di Privacy by Design & by Default** su perimetro IT; integrazione nei processi aziendali della "cultura del dato" di cui al successivo punto ⑤, ovvero del rispetto della riservatezza dei dati personali al fine di mitigarne i rischi per gli interessati

Capacità di rilevare e valutare gli impatti delle evoluzioni normative

Il nostro modello si rivela particolarmente **efficace in quanto prevede l'Osservatorio Privacy**, che valuta applicabilità e impatti per ciascuna evoluzione normativa e/o nuovo standard, emettendo un bollettino verso tutti i soggetti interni e attivando il Competence Center Risk & Compliance per il raggiungimento della compliance

Centro di controllo degli aspetti di privacy

Riteniamo doveroso convergere significativamente sull'interoperabilità tecnica dei sistemi/banche dati di diverse Amministrazioni; a tal fine, supportiamo l'Amministrazione nel costituire un centro di controllo con tavoli tecnici con altre PA al fine di stabilire protocolli di comunicazione e scambio di dati in conformità a: ① **Provvedimento del Garante per la Protezione dei Dati personali** del 2 luglio 2015 – Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche; ② **Linea di indirizzo sull'interoperabilità tecnica delle Pubbliche Amministrazioni di AgID**; ③ **Codice dell'Amministrazione digitale** di cui al Decreto Legislativo 7 marzo 2005, n. 82. L'esperienza di applicazione dei principi inclusi nei suddetti riferimenti normativi ci consente di supportare l'Amministrazione nell'identificazione di adeguate soluzioni in termini di **architetture API** (Application programming interface), **servizi REST** (Representational State Transfer), **accessi selettivi ai dati** e, in generale, misure di sicurezza tecniche (backup, cifratura, log management, network security, ecc.)

Cultura del dato

Il nostro modello organizzativo prevede un t**eam dedicato di Comunicazione & Formazione**, che eroga un servizio di **Privacy Culture & Awareness** che include l'erogazione di sessioni formative rivolte a tutti i livelli del personale amministrativo con un approccio di experiential learning cycle, ovvero mediante lo strumento del workshop in cui i referenti simulano l'applicazione delle procedure privacy interne (es. privacy by design e DPIA) a casi d'uso attinenti alla tipologia di Comparto della PA

9.2 Rapporto di compliance

Nel corso dell'erogazione del Servizio, predisponiamo e aggiorniamo sistematicamente il Rapporto di Compliance, da intendersi non come un semplice documento, ma come un **tool che fornisce una vista real-time dello stato di maturità dell'Amministrazione in ambito privacy e dello stato di avanzamento delle azioni correttive.** Al fine di garantire immediatezza ed efficacia in termini di fruibilità e accessibilità**, il Rapporto di Compliance costituisce una sezione del Portale della Fornitura**, che consente **il download in formati open delle singole sezioni sottostanti**. A ciascuna funzionalità del tool corrisponde un'area all'interno del Portale, quali, ad esempio: ► **criteri di verifica** laddove è possibile visionare la metodologia adottata per la selezione dei trattamenti da sottoporre ad Assessment, quali, ad esempio, criticità dei dati trattati (es. categorie particolari ex art. 9 GDPR) e di interessati coinvolti (es. soggetti vulnerabili o minori) o delle modalità di trattamento (es. trattamento su larga scala, correlazione di banche dati oltre le aspettative degli interessati, ecc.); inoltre, sono previsti collegamenti via web link al corpo normativo applicabile, quali il Regolamento UE 2016/679, la normativa nazionale in materia di privacy (es. D.lgs. 196 del 2003 e ss.mm.ii, Provvedimenti del Garante per la Protezione dei Dati Personali) e agli standard internazionali di riferimento (es., ISO/IEC 27017:2019, ISO/IEC 27001:2013, ISO/IEC 27701:2019). Il tool mette a disposizione funzionalità di "filtraggio" che consentono di personalizzare la ricerca in funzione degli ambiti di interesse, ovvero standard e fonti normative; ► **risultanze delle attività** che illustra gli esiti delle attività di valutazione della maturità e della fase di Shape. Sono resi disponibili i documenti ed evidenze raccolte e analizzate in fase di Assess, nonché prodotte schede di dettaglio per ciascun gap rilevato. Il tool consente di eseguire attività di benchmarking rispetto ad altre PA (naturalmente in forma anonima) per verificare il posizionamento dell'Amministrazione rispetto al panorama pubblico italiano nella sua interezza e/o a singoli Comparti; inoltre, è possibile testare il livello di maturità rispetto a una singola fonte normativa e generare report personalizzati in termini di arco temporale preso in considerazione, ambiti di controllo di interesse e per singoli processi/sistemi dell'Amministrazione; ► **conclusioni delle attività di verifica**: consente la navigazione del Piano di interventi definiti per perseguire il livello di maturità atteso. Sono messe a disposizione funzionalità che consentono di monitorare lo stato di effettiva implementazione delle azioni, nonché eseguire il download di report executive summary o di dettaglio per attività di relazione periodica del RPD e di altri referenti amministrativi interessati verso il vertice amministrativo o materiale di supporto in caso di visita ispettiva da parte dell'Autorità di Controllo. Da ultimo, il tool consente di generare analisi storiche circa l'evoluzione nel tempo del livello di maturità privacy dell'Amministrazione fornendo highlight sulle principali variazioni in termini di processi, procedure, prassi e soluzioni tecniche adottate per sanare i gap identificati in passato.

10 Portale della Fornitura

"L'utilizzo di canali di comunicazione rapidi e diretti fra amministrazioni e fornitori, o fra questi e gli organismi di coordinamento e controllo, rappresenta un fattore determinante per garantire il rispetto dei principi di economicità, efficacia ed efficienza dell'azione amministrativa."
(Corollario del buon andamento dell'azione amministrativa (Legge 241/1990, art. 97 della Costituzione Italiana)

Il **Portale della fornitura (PDF)** che il RTI propone è stato concepito per diventare a tutti gli effetti il "luogo di incontro" di tutti gli attori coinvolti a diverso titolo nella fornitura. È stato progettato in ottica **multicanale** (siti, portali, blog, social network, mobile, ecc.), raggiungibile tramite Internet, per consentire alle singole Amministrazioni ed agli Organismi di coordinamento e controllo di attivare e governare agevolmente i servizi e di **promuovere la condivisione** e l'esperienza maturata nelle singole iniziative. Strutturato sulla base delle aree previste da Capitolato, il Portale è stato arricchito di numerosi elementi migliorativi, grazie ad una **progettazione user centered** basata sui principi di facilità di utilizzo e rilevanza rispetto alle esigenze dell'utente. I principali obiettivi del PDF sono: ► **Informare e coinvolgere le Amministrazioni**, perché aderiscano all'Accordo Quadro; ► **migliorare il processo di interazione e collaborazione tra gli stakeholder** per la condivisione di documenti e contenuti; ► indirizzare un **confronto su esperienze e iniziative di interesse comune** per favorire il riuso delle soluzioni; ► gestire l'intero **ciclo di vita degli affidamenti** e controllare e monitorare la **conduzione**

dei contratti esecutivi; ► **garantire la condivisione della documentazione** e la messa a disposizione di cruscotti grafici riassuntivi in merito all'andamento di tutti i Contratti Esecutivi; ► consentire a Consip ed AgID di svolgere le proprie **funzioni di monitoraggio** sulla qualità dei servizi erogati in AQ. Il Portale sarà implementato con certificato per la navigazione esclusiva in HTTPS e configurato con certificati non self-signed; sarà cura del RTI assicurare i servizi di gestione dei contenuti, delle utenze, la messa a disposizione del manuale d'uso e il servizio di assistenza all'utente.

10.1 Soluzioni tecnologiche e funzionalità del Portale della fornitura e strumenti di analisi dei dati e reporting

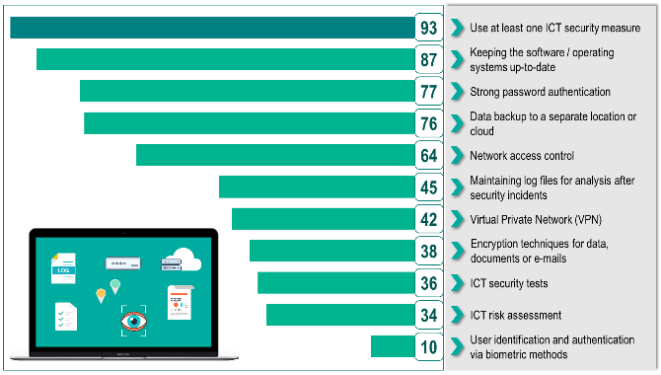
Il RTI vuole offrire attraverso il PDF un vero e proprio **kit di strumenti, funzionalità e soluzioni tecnologiche a supporto delle diverse Amministrazioni**, di Consip, degli Organismi di Coordinamento e Controllo e più in generale di tutti gli stakeholder interessati. Di seguito un quadro sinottico per ogni area del portale in cui sono rappresentati gli strumenti, le funzionalità a disposizione e le soluzioni tecnologiche adottate.

Area	Funzionalità	Strumenti	Soluzione tecnologica
Comunicazione Area ad accesso pubblico del portale per informazione e promozione dei servizi sull'AQ e sui progetti in esecuzione	Funzionalità di ricerca tra gli obiettivi dell'Accordo Quadro Funzionalità di ricerca e consultazione di Faq Funzionalità di ricerca e consultazione di best practice, linee guida, contenuti normativi, news e aggiornamenti in ambito cyber security Funzionalità di ricerca e consultazione di best practice, linee guida, contenuti normativi, news e aggiornamenti in ambito cyber security Funzionalità di ricerca e consultazione Library di case studies in termini di evoluzione delle minacce "cyber" e dei relativi impatti, sia dal punto di vista quantitativo che da quello qualitativo	Knowledge Base	WordPress
	Funzionalità di ricerca e consultazione di dati di libero accesso attraverso cruscotti	Analytics Dashboard e Reporting	KNOWAGE, OpenDataSoft, wpDataTables
	Funzionalità di supporto utente attraverso Chatbot Funzionalità di gestione delle anagrafiche Funzionalità di gestione delle richieste di supporto degli utenti	Customer Relationship Management	odoo
Informativa Area ad accesso pubblico del portale per supportare le PA nel processo di adesione all'accordo. Contiene inoltre un'area privata per la profilazione delle Amministrazioni che hanno aderito all'accordo	Funzionalità di registrazione Funzionalità di configurazione profilo Funzionalità di ricerca e fruizione di contenuti informativi	Self Assessment	Alfresco, WordPress, Formidable Forms, OpenAM
	Funzionalità "wizard" che semplificano le procedure di adesione ai servizi guidando l'utente nella compilazione del Piano dei Fabbisogni attraverso l'utilizzo di modulistica	Editor modulistica, wizard	<form.io>
	Funzionalità di consultazione e profilazione per le amministrazioni che hanno aderito ai servizi Funzionalità di consultazione dei servizi consigliati segmentati sulla base delle caratteristiche del self-assessment	Profilazione PA	Alfresco, OpenAM
Osservatorio Area che consente alle Amministrazioni, ad AgID ed a Consip di svolgere le funzioni di monitoraggio della qualità	Funzionalità di analisi e monitoraggio con un cono di visibilità specifico su singoli Piani dei Fabbisogni, sull'andamento dei loro indicatori di performance e percentuale di aderenza degli interventi al Piano Triennale per l'Informatica della PA, aggiornato al triennio 2020-2022 Funzionalità di alert e strumenti di segnalazione nel caso di mancato rispetto degli SLA Funzionalità di conversazione diretta con la PA interessata e con il Fornitore al fine di chiarire il rilievo effettivo e qualitativo	Analytics Dashboard e Reporting	OpenDataSoft, wpDataTables, KNOWAGE

Project Management Area ad accesso riservato e profilato per le singole Amministrazioni tramite la quale è possibile disporre degli strumenti di attivazione, pianificazione e gestione delle singole iniziative progettuali	Funzionalità di pianificazione e monitoraggio delle attività amministrative, gestionali e operativo delle proprie iniziative Funzioni di governo e monitoraggio di tutti gli adempimenti privacy	Planner utente	Upstream
	Funzionalità di classificazione, gestione e l'archiviazione di tutti i documenti prodotti nell'ambito dello specifico progetto e nei singoli contratti esecutivi	Document management	Upstream
	Funzionalità di gestione delle singole iniziative progettuali attraverso l'elaborazione di cruscotti di avanzamento per ciascuna iniziativa progettuale	Project management	Upstream
Collaborazione e monitoraggio Area che contiene gli strumenti di promozione, collaborazione e condivisione tra le PA e gli strumenti di monitoraggio e governo della fornitura	Funzionalità di social blogging; Funzionalità di forum di discussione; Funzionalità di chat; Funzionalità di mailing list; Funzionalità di talk & training; Funzionalità di wiki	Collaboration	Open2.0
	Funzionalità di analisi e monitoraggio di dati qualitativi e quantitativi (es. controlli ABSC "Agid Basic Security Control" sarà calcolato il valore del relativo Indicatore di Progresso (Ip) dell'intervento ottenuto attraverso la realizzazione dei servizi di gara	Analytics Dashboard e Reporting	OpenDataSoft; wpDataTables; KNOWAGE
	Funzionalità di predisposizione, compilazione e analisi di survey di customer satisfaction Funzionalità di reporting su soddisfazione utente; Funzionalità di analisi della soddisfazione utente rilevata	Analytics Dashboard e Reporting	SurveyMonkey

Il Portale si configura come strumento di contatto e di lavoro in grado di assicurare il costante monitoraggio e la valutazione dell'andamento delle attività; ogni informazione gestita nell'ambito dei servizi sarà quindi classificata, organizzata, storicizzata e resa accessibile.

Il RTI dispone di un'ampia gamma di soluzioni tecnologiche per facilitare la raccolta, la strutturazione, la visualizzazione e la condivisione delle informazioni rilevanti; si propone l'utilizzo di strumenti **di analisi dati e reporting leader di mercato**: ► **OpenDataSoft® e Knowage®**: strumenti innovativi per la gestione e l'analisi di Basi Dati (anche di grandi dimensioni), attraverso l'utilizzo di workflow ripetibili; tipicamente sono utilizzati per aspetti di integrabilità, facilità nell'interrogazione, capacità di rappresentazione delle informazioni. ► **WpDataTables ®**: rappresenta un componente di Data Visualization, per l'analisi e la rappresentazione di Basi Dati (anche di grandi dimensioni); garantisce semplicità di utilizzo (grazie al sistema "drag & drop") e la possibilità di esplorare "in profondità" i dati, rappresentarli in modo efficace attraverso il supporto grafico e condividerli in modo interattivo.



Il sistema di reporting configurato è stato selezionato dal RTI perché caratterizzato dai seguenti punti di forza: ► **facilità d'uso**: per utilizzare gli strumenti di analisi e monitoraggio proposti non occorre essere dei programmatori, grazie all'intuitivo sistema "drag & drop" caratterizzato da interfacce "user friendly"; ► **analisi di qualunque tipo di dato**: è possibile analizzare dai semplici fogli di calcolo (xlsx, csv, txt, ecc.) ai Database e strutture dati più complesse tipiche dei Big Data; ► **cruscotti interattivi**: le infinite combinazioni di "viste" interattive confermano gli strumenti proposti leader nella Data Preparation, Data Visualization e Data Story Telling; ► **dati sempre aggiornati**: è possibile "connettersi" a diversi sistemi e fonti dati, scegliendo la modalità di aggiornamento (automatica, pianificata, manuale); ► **condivisione interattiva**: in pochi click è possibile pubblicare e condividere le proprie analisi sul web, mantenendo sempre l'interattività dei dati.

10.2 Soluzioni, processi, strumenti di comunicazione e di collaborazione in chiave "social" con le PA contraenti

In coerenza con l'approccio proposto dal RTI che si rifà all'adozione di tecnologie digitali per stimolare la comunicazione in chiave "social" e innescare nuove modalità di lavoro collaborative (anche attraverso la creazione di spazi di co-working), il Portale prevederà alcuni moduli di collaboration. La soluzione

tecnologica identificata a supporto è la piattaforma **Open2.0®**,è un software open source la creazione di piattaforme software complesse e strumenti collaborativi che ha ottenuto tra l'altro la qualificazione di AgID come software a riuso per la Pubblica Amministrazione.

L'utente PA "accreditato", una volta effettuato il log-in, visualizzerà una Home Page personalizzata che lo abiliterà ad interagire con i "colleghi" delle altre Amministrazioni. Il Portale prevede tre soluzioni di collaboration che coprono rispettivamente: **l'anima social con una bacheca pubblica per la PA, l'anima di collaboration con una community in costante aggiornamento, gli spazi di co-working.**

La Bacheca di discussione pubblica delle PA

Uno "spazio virtuale" aperto dove poter pubblicare notizie, richiedere informazioni e/o abilitare gli altri utenti a commentare e caricare allegati a beneficio esteso di tutta la community della PA. La Bacheca riprende il concept oramai largamente diffuso dei principali strumenti social di maggior successo commerciale (i.e. Linkedin, Facebook, ecc.). In quest'area i contenuti saranno più "statici"; saranno infatti le rispettive Amministrazioni a valutare e decidere quali articoli, dati, informazioni, risultati dovranno essere esposti. L'interazione sarà "mediata" da un processo di moderazione dei post e dei commenti; tramite questo "spazio", le Amministrazioni possono "fare rete" e creare una base di conoscenza condivisa, soprattutto per quelle PA che collaborano in territori con caratteristiche simili e/o con la stessa tipologia di utenza, così da ridurre la complessità ed aumentare l'efficacia dell'azione amministrativa.

La Community di divulgazione delle esperienze

Uno spazio che ha l'obiettivo di condividere con gli utenti interessati i dettagli delle singole esperienze/iniziative progettuali maturate. Questo modulo si configura come un "catalogo delle esperienze", etichettate per tipologia di servizio e per stato (appena avviata, in corso di svolgimento, terminata), allo scopo di abilitare una rapida ricerca in base alle specifiche preferenze dell'utenza. Gli utenti avranno la possibilità di manifestare la propria preferenza per la singola esperienza: questa funzionalità permetterà al sistema di portare automaticamente "in primo piano" le iniziative più "quotate". Le esperienze sono valorizzate con la pubblicazione di una pagina di dettaglio, nella quale si possono reperire i contatti dei referenti di progetto, inserire commenti e/o allegare documentazione rilevante.

Gli spazi riservati di co-working

Il terzo modulo si configura come lo spazio di collaborazione che risponde all'esigenza di maggior privacy nella condivisione delle informazioni e del know-how acquisito nell'ambito delle progettualità avviate all'interno dell'Accordo Quadro. Gli spazi riservati di co-working potranno essere creati o a partire dalla "Community di divulgazione delle esperienze" (attraverso un'apposita funzionalità di richiesta di collaborazione all'interno della pagina di dettaglio) oppure "ex novo" (slegati quindi da specifiche esperienze maturate dalle PA). Il RTI, a fronte di analisi di benchmark effettuate per Enti Pubblici in ambito di tool di collaboration, prevede anche l'inserimento di un modulo di "team matching", strumento indispensabile per la ricerca di collaborazioni.

Il RTI si assume la responsabilità di garantire tutti gli obblighi contenuti a pag. 41 del punto 9.1 del Capitolato Tecnico Generale.

11 Miglioramento soglie indicatori di qualità: RLFN – Rilievi sulla fornitura

Con riferimento a quanto indicato nell'Appendice 1 al Capitolato Tecnico Speciale "Indicatori di qualità", il RTI si impegna a garantire una riduzione della soglia dell'indicatore **RLFN - Rilievi sulla fornitura** ad un valore pari a 1.

12 Miglioramento soglie indicatori di qualità: SLSC – Rispetto di una scadenza contrattuale

Con riferimento a quanto indicato nell'Appendice 1 al Capitolato Tecnico Speciale "Indicatori di qualità", il RTI si impegna a garantire una riduzione della soglia dell'indicatore **SLSC - Rispetto di una scadenza contrattuale** ad un valore pari a 1.

13 Miglioramento soglie indicatori di qualità: NAPP – Non approvazione di documenti

Con riferimento a quanto indicato nell'Appendice 1 al Capitolato Tecnico Speciale "Indicatori di qualità", il RTI si impegna a garantire una riduzione della soglia dell'indicatore **NAPP - Non approvazione di documenti** ad un valore pari a 0.

14 Innovazione

"L'innovazione consiste nel vedere ciò che tutti hanno visto e nel pensare ciò che nessuno ha pensato"
(Albert Szent-Gyorgyi)

Il coinvolgimento delle PMI e dei Centri di ricerca **avviene a livello di RTI** al fine di garantire la massima rapidità nell'attivazione e nel coinvolgimento di tali operatori specializzati; il ruolo di questi soggetti è duplice: **a) operare da centri di competenza per il supporto orizzontale alla erogazione dei servizi del Lotto**, fornendo spunti metodologici, best practices, strumenti e professionalità disponibili per tutti gli stakeholders; **b) operare direttamente nella erogazione di servizi** a favore di specifiche PA a causa di specificità geografiche favorevoli e/o opportunità di impiego di competenze specialistiche della PMI. Come evidenziato nella tabella **disponiamo di strutture in grado di favorire innovazione per ognuno dei servizi della presente fornitura.**

14.1 Soggetti coinvolti, principali caratteristiche e valore aggiunto

PMI/Start up innovativa	Caratteristiche	Ambito di intervento	Valore aggiunto per l'esecuzione delle prestazioni
Teleconsys Sharing Innovation	Teleconsys ha specifiche competenze nella progettazione e realizzazione di soluzioni di Cybersecurity, Data Governance & Protection e Intelligence. Inoltre, è fondatore e socio Gold del Digital Innovation Hub del Lazio; fa parte del board della Sezione IT di Unindustria ed è membro del Tavolo Tecnico Università, Ricerca e Trasferimento Tecnologico che lavora con le sette università del Lazio per il trasferimento tecnologico e la promozione dell'Open Innovation.	- Vulnerability Assessment - Security Strategy - Testing codice - Penetration Test.	- Fornisce una piattaforma innovativa che, abbracciando il paradigma della API Economy, è finalizzata a dare maggior valore alla compliance normativa e fornire uno strumento a servizio dell'analisi e gestione degli incidenti in ambito cybersecurity sfruttando strumenti innovativi di AI e Deep Learning. - Offre, grazie ad uno specialistico network, un ampliamento delle competenze funzionali, metodologiche e tecnologiche, nonché un supporto specializzato su trend e soluzioni emergenti in ambito cybersecurity.

Centri di ricerca	Società/Istituto	Caratteristiche	Ambito di intervento	Valore aggiunto per l'esecuzione delle prestazioni
Cyber Security Vulnerability Research Center	intellera consulting	Centro di ricerca specializzato nell'individuazione di vulnerabilità non note su sistemi e prodotti.	- Vulnerability Assessment - Penetration test	- Consente l'individuazione di vulnerabilità di tipo zero-day, fornendo dei workaround per la gestione delle stesse prima ancora che vengano rilasciate patch ufficiali dai vendor
Cyber Security Threat Intelligence Research Center	intellera consulting	Centro di ricerca specializzato nella definizione di strategie innovative per la risposta agli incidenti attraverso analisi degli strumenti di mercato e di malware analysis.	- Supporto all'analisi e gestione degli incidenti	- Definisce modalità di risposta verso delle minacce non ancora note o diffuse nel panorama mondiale e di preparare i clienti ad affrontarle. - Guida il cliente all'identificazione delle migliori soluzioni software per le loro esigenze.
Cybersecurity Experience Center	Capgemini	Centro di ricerca che nasce con l'obiettivo di supportare i clienti a prevenire gli incidenti informatici e a ridurre l'impatto di attacchi significativi.	- Supporto all'analisi e gestione degli incidenti - Vulnerability Assessment - Testing Del Codice	- Offre una simulazione immersiva per un supporto nella comprensione delle dinamiche di un incidente di sicurezza informatica e la tecnologia, le persone e i processi necessari per proteggere il core business.
Information Security Governance	TXT HSPI	Centro di ricerca specializzato nell'analisi di processi e assetti organizzativi per identificare obiettivi e strategie in ambito cybersecurity coerenti con i contesti di mercato ed aderenti alle normative vigenti.	- Security strategy - Compliance normativa	Il centro di competenza assicura il continuo approfondimento e contestualizzazione di standard e linee guida internazionali in materia di Governance della sicurezza delle informazioni.

14.2 Modalità organizzative del coinvolgimento, in termini sia di tempistiche di ingaggio, che di modalità di relazione internamente e verso le Amministrazioni

Per assicurare un continuo e qualificato supporto di innovazione alla realizzazione dei servizi di fornitura abbiamo definito una **modalità di coinvolgimento ed interazione con le Amministrazioni** basato su tre pilastri: ► *Azzeramento delle tempistiche di attivazione*, grazie alla disponibilità di tutte le competenze necessarie già all'interno del Raggruppamento. ► *Presidio continuo delle esigenze delle Amministrazioni*, attraverso figure chiavi quali l'Account Manager e il Knowledge Manager, coordinati centralmente dallo SPESI al fine di facilitare la distribuzione della conoscenza e permettere il riutilizzo di soluzioni tra differenti Amministrazioni che risultino simili per contesto ed esigenze. ► *Analisi continua e specializzata dei principali trend di innovazione* da parte dei centri di ricerca e dei relativi network che garantisca proattività e rapidità nel cogliere le evoluzioni del mercato e trasformale in soluzioni per le Amministrazioni grazie all'esperienza e al modello organizzativo flessibile del **Security & Privacy Enabler Solution Innovators (SPESI).**

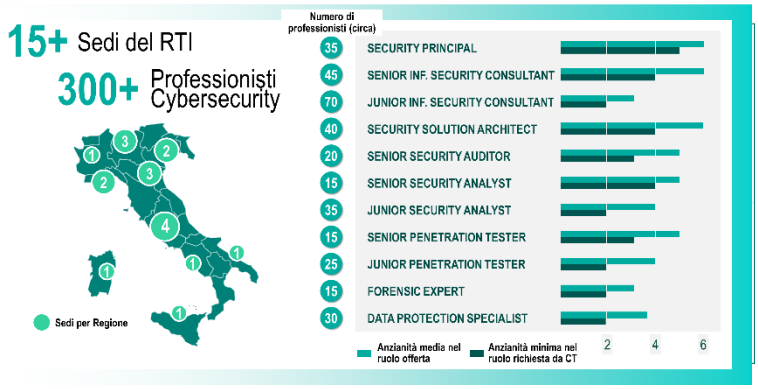
15 Flessibilità delle risorse

Sii saldo nelle tue decisioni ma rimani flessibile nel tuo approccio (Tony Robbins)

In uno scenario caratterizzato dalla necessità di staffing continuo di risorse specialistiche su numerosi Contratti Esecutivi attivabili in parallelo, è fondamentale dotarsi di un efficace processo di **workforce management** che assicuri, da un lato, la gestione integrata e multilivello del miglior mix quali-quantitativo delle risorse specialistiche, e dall'altro, tempi di disponibilità brevi o a volte brevissimi, come ad esempio la gestione di incidenti potenzialmente ad alto impatto dirompente sui sistemi delle Amministrazioni.

15.1 Disponibilità e tempestività di allocazione delle risorse in relazione all'ambito di riferimento del Lotto

Grazie alla consolidata esperienza delle nostre aziende sui temi della presente fornitura, disponiamo di **oltre 300** risorse in ambito Cyber Security (con **anzianità media nel ruolo superiore e certificazioni aggiuntive** rispetto ai requisiti minimi richiesti nell'*Appendice 2 al CTS Lotto 2_Profili Professionali)*, utilmente impiegabili ed **opportunamente distribuite territorialmente.** Le nostre aziende dispongono di forti legami di partnership con i più diffusi e importanti vendor tecnologici che garantiscono il massimo presidio verticale di competenza anche sui prodotti e soluzioni di mercato. **La rete di partnership del RTI permette di coprire tutti i servizi richiesti nel Capitolato.**



Vista la strategicità della presente fornitura, intendiamo adottare ogni soluzione a nostra disposizione per garantire **piena e immediata impiegabilità di tutta la capacità produttiva disponibile**. In particolare, faremo ricorso a: ► **Processi** di pre-booking delle risorse dei nostri centri di competenze e delivery sui diversi contratti esecutivi potenzialmente attivabili, in base ad analisi di tendenza, confronti tecnico-commerciali con le Amministrazioni interessate, demand management, ecc.; ► **Team di twin resources**: per le risorse chiave identificate nell'ambito dell'AQ sarà identificato un pool di risorse aggiuntive, con competenze interscambiabili, da allocare sulle attività critiche ad integrazione delle risorse dei team. Tale soluzione consentirà di assicurare l'immediato allineamento della forza lavoro e delle competenze alle variazioni sia in incremento dell'effort, sia in caso di indisponibilità temporanea, senza alcun onere aggiuntivo e/o disservizio per la Committenza. Per garantire risorse immediatamente attivabili, i professionisti del pool di risorse aggiuntive saranno continuamente allineati sul contratto e sulle attività attraverso workshop tematici. I workshop riguardano, in primis: ① **aggiornamenti su forniture tra le più complesse e ritenute "a più alto grado di variabilità",** ② aggiornamenti sull'evoluzione dei contratti nell'ambito dell'AQ. Ai workshop si aggiunge il processo di formazione continua (cfr. *§ 16 Aggiornamento delle risorse professionali*); ► **Team di continuità**: per i servizi che nel corso della fornitura dovessero subire sospensioni temporanee e/o riduzioni di effort, in caso di ripresa/incremento delle relative attività, assicureremo la riallocazione delle medesime risorse che precedentemente operavano nell'ambito degli stessi, a garanzia di abbattimento dei tempi di ingaggio sul singolo intervento e salvaguardia del know-how; ► **Orario flessibile**: fermo restando il pieno rispetto degli orari di lavoro previsti dai contratti, le risorse impegnate sui singoli task progettuali potranno essere allocate secondo una logica di turnazione per coprire una fascia oraria giornaliera di lavoro più ampia (es. dalle 8.00 alle 20.00) rispetto a quella indicata nel Capitolato (cfr. § 5.9 Orario di erogazione dei servizi). Tale misura consentirà un presidio continuativo più ampio rispetto alle normali otto ore di lavoro e garantirà una più efficace operatività in relazione ad attività critiche. In casi di particolare emergenza in cui si renda necessario concentrare in tempo reale forza lavoro (es. per far fronte a improvvise/coincidenti scadenze) potrà, inoltre, essere fatto ricorso al lavoro straordinario.

La presente fornitura contiene linee di servizio nelle quali la **tempestività** è, nei fatti, uno dei fattori critici di successo (es. nel caso della gestione degli incidenti informatici). Per ottimizzare i tempi di risposta al riguardo, il RTI attiva tutte le leve di disponibilità sopra illustrate in tempi estremamente rapidi grazie a: ► **la presenza di presidi organizzativi** deputati ad **intercettare in tempi ridotti** (e dove possibile anticipare) le esigenze dei clienti o potenziali clienti (processo di demand management opportunamente presidiato da Demand Manager specifici per ogni Contratto); a **valutare in anticipo esigenze di modifiche di staffing** dovute ad emergenze o criticità particolari (Project Risk Management) o a modifiche nella pianificazione (PMO); a **presidiare con piena e diretta responsabilità i processi di staffing** (Resource Manager); ► **l'utilizzo di strumenti integrati di workforce management e di skill inventory** (es. Talent Link) di supporto alla pianificazione e rimodulazione delle risorse specialistiche.

Grazie a queste soluzioni il RTI è in grado di mettere a disposizione delle Amministrazioni un team di risorse specialistiche, per ciascuno dei servizi previsti, **al di fuori della pianificazione prevista nel Piano di Lavoro Generale**, con le seguenti tempistiche: ► **entro 3 giorni dall'esigenza** per i servizi di "Security Strategy", "Vulnerability Assessment", "Testing del codice (Statico, Dinamico o Mobile)", "Penetration Testing" e "Compliance Normativa"; ► **entro 3 ore dalla esigenza,** per il servizio di "Supporto analisi e gestione incidenti".

15.2 Metodologie e strumenti proposti per la flessibilità nella gestione di più contratti in contemporanea

Per garantire flessibilità nella gestione di progetti in contemporanea adottiamo un **framework di Agile Program Management** (*cfr. § 3* Struttura Organizzativa), strutturato in metodologie di dettaglio e strumenti che rappresentano best *practice* di Scaled Agile applicate allo specifico contesto della fornitura. Questa metodologia agile garantisce un **coordinamento e controllo complessivo di tutte le iniziative progettuali** che verranno attivate e, allo stesso modo la necessaria flessibilità e tempestività d'azione necessarie alla gestione contemporanea di più progetti (sia presso la stessa Amministrazione che in più Amministrazioni). A livello di Accordo Quadro, in particolare, grazie alle metodologie di **Portfolio, Program e Team backlog management** siamo in grado di aggregare e disaggregare le iniziative legandole ad attività sempre più granulari che consentono un **controllo più efficace ed una maggiore adattabilità e flessibilità in caso di cambiamenti,** indipendentemente dal livello (inter-Amministrazioni o intra-Amministrazione). A livello esecutivo progettuale, invece, grazie all'**approccio incrementale** basato su **metodologie agile** anticipiamo il risultato finale e garantiamo flessibilità e tempestività soprattutto nel raccogliere i feedback delle Amministrazioni mitigando i rischi e massimizzando così l'efficacia del risultato finale della delivery. Nel dettaglio grazie a metodologie operative e strumenti di **Continuous delivery** e **Sprint planning,** siamo in grado di gestire flessibilmente e tempestivamente eventuali cambiamenti e modifiche con minimizzazione degli impatti di pianificazione.

Il framework metodologico appena presentato è supportato inoltre da **strumenti** ad hoc che garantiscono: ► *Efficacia*: **Redmine** è uno strumento di Agile PPM che fornisce in modo efficiente e collaborativo, in tempo reale, analisi ed approfondimenti sulla delivery. La piattaforma digitale viene utilizzata come "fonte di verità" centralizzata per tutte le informazioni su Portafogli e Programmi, eliminando la necessità di fare affidamento su documenti e strumenti stand-alone. ► *Tempestività e Flessibilità*: **Talent Link** e **Smart Planner**: strumenti che consentono di avere una visione di insieme ed in tempo reale di tutte le skill e le competenze messe a disposizione della fornitura da parte del RTI con informazioni sempre aggiornate della percentuale di impegno

sui diversi progetti presso le diverse o le stesse Amministrazioni. Sulla base delle percentuali di ingaggio e della criticità della singola risorsa è possibile adattare in modo flessibili le composizioni dei team a picchi di lavoro, esigenze particolari ed estemporanee.

Redmine fornisce un ambiente altamente configurabile per stabilire una visione personalizzata del proprio portafoglio, consentendo a tutti gli stakeholder del progetto, del programma e del portafoglio di ottenere informazioni dettagliate sugli avanzamenti progettuali, attraverso un'interfaccia moderna e *user-friendly* che **consente un efficace gestione dei team di programma** attraverso le funzionalità mostrate nella figura seguente.

Talent Link® è la piattaforma di gestione del personale, già in uso presso le aziende del RTI, per consentire l'allocazione di risorse e competenze in risposta a una o più richieste di adesione all'AQ. L'utilizzo della piattaforma consente di identificare e selezionare le risorse ottimali sulla base delle competenze possedute e della loro disponibilità secondo una struttura a matrice che incrocia i settori di mercato a livello "verticale", (PAC, PAL, Sanità) e le aree/dominii di competenza del personale a livello "orizzontale" (Strategy, Management, Technology e Risk Consulting, ecc.). La presenza di ulteriori dati strutturati (e. le esperienze avute, i clienti per i quali hanno lavorato, le Industry conosciute, ecc.) consente di valutarne l'utilizzabilità per la fornitura con **ricerche mirate e su più criteri**. Talent link è integrato con lo strumento **Smart Planner®**, utilizzato dal RTI per la **gestione della pianificazione** delle persone. Permette di visualizzare l'impegno di una risorsa mappandone il progetto e il cliente per cui sta lavorando. Tali strumenti consentono la simulazione, il planning giornaliero, la valutazione delle competenze e delle performance del personale impiegato, la **gap analysis** di competenze e risorse nei team e le necessarie azioni correttive.

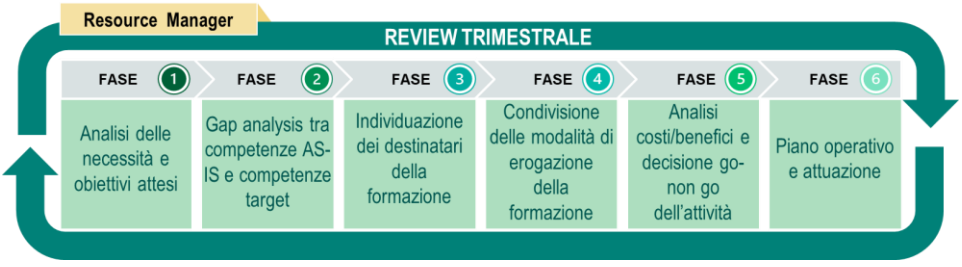
16 Aggiornamento delle risorse professionali

La peculiarità dei servizi di gara richiede il presidio di frontiere di conoscenza tematiche (normative, studi di settore, best practice) e tecnologiche (prodotti, tecniche, strumenti specifici) da preservare nel tempo con **metodi e programmi di formazione diversificati per figura professionale**. I numeri di seguito testimoniano l'impegno che il RTI dedica alle attività formative: ① **Oltre 7 giorni medi per risorsa dedicati ogni anno ad attività formative**, di cui **4 riservati all'IT Security**; ② **Oltre 1.500 certificazioni** tecnologiche e metodologiche, di cui **oltre 250 in ambito IT Security**; ③ Disponibilità di **oltre 10 docenti accreditati** ad erogare formazione certificata di cui **2 in ambito IT Security**.

16.1 Soluzioni progettuali e strumenti tecnologici per garantire la formazione e l'aggiornamento continuo

La formazione e l'aggiornamento continuo delle risorse impiegate nella fornitura sono garantite - senza alcun onere aggiuntivo per le Amministrazioni - da un **framework formativo** che ha le seguenti caratteristiche: una soluzione organizzativa snella ed efficace, un processo specifico a supporto, contenuti e modalità di erogazione differenziate e soggette a review periodiche, uno strumento in grado di gestire e tracciare tutte le attività di formazione.

La **soluzione organizzativa** prevede: ① un **Resource Manager** a livello di intero Accordo Quadro, che supervisiona l'intero processo di framework formativo, fornisce supporto metodologico per la standardizzazione delle modalità formative, mantenendo uno skill inventory centralizzato ed aggiornato; ② **professionisti con esperienza certificata sui temi della formazione** nei team di progetto a livello di contratto esecutivo, per individuare e pianificare le esigenze formative specifiche legate ai servizi offerti nel contratto.



Un **processo formativo**, basato su sei fasi e schematizzato in figura, per garantire concretezza ed efficacia rispetto alle continue evoluzioni del mercato. Un **mix di metodologie elementari** che assicurano il raggiungimento degli obiettivi di efficacia del piano formativo:

- **Lezione frontale**, consente di acquisire nozioni teoriche e di attivare confronti tra discenti
- **Laboratori/esercitazioni**, le esercitazioni pratiche assicurano un adeguato bilanciamento tra teoria e pratica
- **Simulazioni/Role-Playing**: basata sulla immaginazione e capacità di immedesimazione in una determinata situazione
- **Risorse online**: corsi e-learning per la fruizione asincrona sulla piattaforma **Moodle**
- **Gamification**: metodologia asincrona nella quale i discenti sono coinvolti in una serie di processi e pratiche proprie del gioco.
- **Sessioni di Studio/Eventi**: workshop organizzati da organizzazioni nazionali/internazionali per promuovere specifici eventi tematici

Uno **strumento tecnologico** denominato ILMS (*Intellera Learning Management System)* che integra sulla piattaforma Moodle tutte le features di un Learning Management System consentendo la gestione completamente digitalizzata del processo sopra-descritto a partire dalla analisi del fabbisogno, fino alla erogazione del corso e alla certificazione di avvenuta acquisizione delle competenze correlate. Lo strumento è nativamente integrato con Talent

Link - lo strumento di tracciatura delle competenze del personale (cfr. 15.2 Metodologie e strumenti proposti per la flessibilità nella gestione di più contratti in contemporanea) - ed è reso accessibile sia in modalità web che mobile a tutto il personale coinvolto nella presente fornitura.

16.2 Completezza ed efficacia della proposta di piano formativo

Il tailoring specifico del framework sui contenuti del piano formativo si basa su tre direttrici: ① **Mantenimento ed integrazione delle certificazioni** previste dai profili e migliorate in fase di Offerta Tecnica; ② **Sensibilizzazione rispetto alla sicurezza nell'erogazione dei servizi**; ③ **Aggiornamento su standard e normative**. I corsi **in ambito IT Security** identificati sono i seguenti:

Ambito	Cluster Formativi	Figura Professionale / Ore anno										
		SP	SISC	JISC	SSAR	SSAU	SSA	JSA	SPT	JPT	FE	DPS
Sensibiliz-zazione	Uso dotazioni informatiche in tutte le modalità operative (meccanismi e regole definite per la protezione dei dati che verranno acquisiti nel corso delle operazioni). Formazione su regole, procedure, SLA previsti dall'AQ. Formazione sugli standard definiti per i deliverable di progetto	8	8	8	8	8	8	8	8	8	8	8
Governance, Risk and Control	CISM (Certified Information Security Manager), CISA (Certified Information Systems Auditor), CRISC (Certified in Risk & Information Systems Control), CISSP (Certified Information Systems Security Professional), ISO/IEC 27001, COBIT, CMMI.	32				32						16
Normative	CDPSE (Certified Data Privacy Solution Engineer). ISO/IEC 27701/27017/27018. Gestione data breach, GDPR e misure di sicurezza, Analisi rischi e valutazioni di impatto, Registro dei trattamenti. Aggiornamento normative privacy, ecc.	8	24	24	8	16	8	16				32
Technical Skills 1	EC-Council CSA (Certified Ethical Hacker), EC-Council CSA (Certified SOC Analyst), CompTIA CySA+ (Cyber Security Analyst), OSSTMM Professional Security Tester, GIAC CFA/CFE/DFIP/CIH/ENCE						32		32	16	32	
Technical Skills 2	Prodotti di sicurezza (FW, Antimalware, IDS/IPS, WAF, SIEM, I&AM, ecc.) Architetture, protocolli e servizi infrastrutturali. Processi di hardening di sistemi s middleware. Sviluppo sicuro del codice. Sicurezza architetture di Cloud Computing		24	24	40		8	24	24	32	24	
P&S Mgmt	ITIL, Prince2, PMI	8					8	8				
Framework di Controllo	Eventi CSA (Cloud Security Alliance), Aggiornamento principali framework di controlli: NIST cybersecurity framework e framework nazionale, CSA-CCM, CIS-CSC (ex SANS20), Linee guida AGID (e nuova Agenzia), Linee guida ENISA	8	8	8	8	8		8		8		8

Al fine di evitare impatti della formazione sull'erogazione dei servizi si agirà sui seguenti aspetti: ► privilegio della modalità e-learning da fruire di norma al di fuori del normale orario di lavoro (utilizzo del regime dello straordinario); ► pianificazione organizzata per non impegnare nella stessa sessione un numero sostenuto di risorse del medesimo profilo e/o che operano nel medesimo team operativo; ► in caso di sessione formativa che richiede la "presenza fisica" dei discenti in aula, le risorse allocate stabilmente sui servizi potranno essere sostituite, qualora necessario, da risorse del pool di risorse ausiliarie. Per consentire una **gestione integrata e un monitoraggio qualitativo e quantitativo sull'andamento delle iniziative formative** declinate nel Piano di Formazione, sarà messa a disposizione una dashboard ad uso del livello Governo, all'interno del Portale di Governo della Fornitura, con appositi **report e viste informative multidimensionali** al fine di dare evidenza alle Amministrazioni, ed a Consip, delle iniziative formative effettuate e previste.

17 Assunzione delle risorse professionali

Rispetto al complesso delle assunzioni necessarie per ogni contratto esecutivo finanziato, in tutto o in parte, con le risorse previste dal Regolamento (UE) 2021/240 del Parlamento europeo e del Consiglio del 10 febbraio 2021 e dal Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021, nonché dal PNC, e fermo restando il rispetto del requisito necessario di cui al Capitolato tecnico generale al par. 7.1, il RTI si impegna ad assumere persone disabili, giovani di qualsiasi genere, con età inferiore a trentasei anni, e donne per l'esecuzione di ciascun contratto esecutivo o per la realizzazione di attività ad essi connessi o strumentali, almeno nella misura del 36%.

18 Documentazione coperta da riservatezza

L'opposizione all'ostensione è motivata in ragione del presupposto che l'Offerta Tecnica contiene informazioni di carattere estremamente riservato, riguardanti il *know-how* e, in particolare, le metodologie e gli strumenti che caratterizzano il servizio offerto dallo Scrivente RTI, nonché le strategie tecniche e commerciali seguite dalle Società. Informazioni che, ove rese note alle società concorrenti, nuocerebbero gravemente agli interessi commerciali e imprenditoriali dello Scrivente RTI, con conseguente inevitabile pregiudizio di ogni futuro leale confronto concorrenziale. Per i motivi sopra esposti, pertanto, si chiede a codesta Amministrazione di non consentire l'accesso, sia con riferimento alla visione sia all'estrazione di copia, degli atti e parti di atti di cui sopra, per ragioni inerenti alla tutela dei diritti di privativa commerciale di titolarità dello Scrivente RTI.

intellera consulting — **Giancarlo Senatore – Mario Papini**

Capgemini — **Andrea Falleni**

TXT HSPI — **Sebastiano Manno**

Teleconsys Sharing Innovation — **Giada Apicella**