Identificativo: Piano Operativo Sicurezza Da Remoto Lotto 2

Data: 19 Dicembre 2024

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

LOTTO 2 – SERVIZI DI COMPLIANCE E CONTROLLO

PUBBLICHE AMMINISTRAZIONI LOCALI

Piano Operativo

ARES - Azienda regionale della salute

Costituito

Raggruppamento Temporaneo di Imprese

composto da:

Deloitte Consulting Srl S.B.

EY Advisory S.p.A.

Teleco S.r.l.

Deloitte. EY teleco

1 INTRODUZIONE

1.1 Ambito

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

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

Il presente documento costituisce il "Piano Operativo" (o "Ordinativo di fornitura"), nel quale l'RTI intende formulare la proposta tecnico/economica secondo le modalità tecniche ed i listini previsti nell'Accordo Quadro, in risposta al "Piano dei Fabbisogni" redatto dall'istituzione pubblica Azienda Regionale della Salute (ARES).

1.2 Richieste dell'Amministrazione contraente

Con la Deliberazione della Giunta Regionale della Regione Autonoma della Sardegna n. 46/27 del 25/11/2021 la Giunta stabilisce di costituire l'ARES a partire dalla data del 1° gennaio 2022.

L'ARES è una azienda sanitaria parte integrante del sistema del Servizio Sanitario della Regione Autonoma della Sardegna e del sistema del Servizio Sanitario Nazionale, è stata istituita per offrire supporto alla produzione di servizi sanitari e socio-sanitari e svolge la propria attività nel rispetto del principio di efficienza, efficacia, razionalità ed economicità.

La mission di ARES, dotata di personalità giuridica di diritto pubblico, di autonomia amministrativa, patrimoniale, organizzativa, tecnica, gestionale e contabile, è quella di supportare le Aziende sanitarie regionali nella produzione di servizi sanitari e sociosanitari. ARES affianca l'Assessorato Regionale alla Sanità e dei Servizi Sociali nella funzione di governance complessiva del Servizio Sanitario Regionale e nel perseguire un'azione omogenea e coordinata tra le Aziende Sanitarie.

All'interno della L.R. 24/2020, la Regione assegna ad ARES importanti compiti di programmazione, monitoraggio e trasformazione digitale, in particolare vengono assegnate ad ARES le seguenti funzioni:

- centrale di committenza per conto delle aziende sanitarie e ospedaliere della Sardegna ai sensi degli articoli 38 e 39 del decreto legislativo 18 aprile 2016, n. 50 (Codice dei contratti pubblici) e successive modifiche e integrazioni, con il coordinamento dell'Assessorato regionale competente in materia di sanità. Nell'esercizio di tale funzione può avvalersi della centrale regionale di committenza di cui all'articolo 9 della legge regionale 29 maggio 2007, n. 2 (legge finanziaria 2007), e successive modifiche e integrazioni. Resta salva la facoltà di tutte le aziende di procedere direttamente all'acquisizione di beni e servizi nei limiti di quanto previsto dall'articolo 37 del decreto legislativo n. 50 del 2016;
- gestione delle procedure di selezione e concorso del personale del Servizio sanitario regionale, sulla base delle esigenze rappresentate dalle singole aziende; può delegare alle aziende sanitarie, sole o aggregate, le procedure concorsuali per l'assunzione di personale dotato di elevata specificità;
- gestione delle competenze economiche e della gestione della situazione contributiva e previdenziale del personale delle aziende sanitarie regionali;
- gestione degli aspetti legati al governo delle presenze nel servizio del personale;

- omogeneizzazione della gestione dei bilanci e della contabilità delle singole aziende;
- omogeneizzazione della gestione del patrimonio;
- supporto tecnico all'attività di formazione del personale del servizio sanitario regionale;
- procedure di accreditamento ECM;
- servizi tecnici per la valutazione delle tecnologie sanitarie (Health Technology Assessment - **HTA**), servizi tecnici per la fisica sanitaria e l'ingegneria clinica;
- gestione delle infrastrutture di tecnologia informatica, connettività, sistemi informativi e flussi dati in un'ottica di omogeneizzazione e sviluppo del sistema ICT;
- progressiva razionalizzazione del sistema logistico;
- gestione della committenza inerente all'acquisto di prestazioni sanitarie e socio-sanitarie da privati sulla base dei piani elaborati dalle aziende sanitarie;
- gestione degli aspetti economici e giuridici del personale convenzionato;
- tutte le competenze in materia di controlli di appropriatezza e di congruità dei ricoveri ospedalieri di qualunque tipologia, utilizzando metodiche identiche per tutte le strutture pubbliche e private. Il valore dei ricoveri giudicati inappropriati è scontato dalle spettanze alla struttura interessata al pagamento immediatamente successivo alla notifica del giudizio definitivo di appropriatezza.

Nell'ambito del contratto quadro per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni, l'Amministrazione ha richiesto un'attività di analisi dello status quo e di supporto al disegno del piano strategico in ambito Cybersecurity dell'Ente e alle iniziative per rafforzare il livello di maturità della Cybersecurity tenendo in considerazione anche i temi di compliance (es. GDPR, Direttiva NIS2, Legge 90/2024, ecc.) e l'evoluzione tecnologica sempre più spostata verso paradigmi di cloud ibrido, attraverso le seguenti linee di servizio:

- Security Strategy (L2.S16);
- Vulnerability Assessment (L2.S17);
- Testing Dinamico del Codice (L2.S19);
- Supporto all'analisi e alla gestione incidenti (L2.S21);
- Penetration Testing (L2.S22);
- Compliance Normativa (L2.S23).

1.3 Riferimenti

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

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

1.4 Acronimi e glossario

DEFINIZIONE/ACRONNIMO	DESCRIZIONE
RTI	Raggruppamento Temporaneo di Impresa
AQ	Accordo Quadro
CE	Contratto Esecutivo
PAL	Pubblica Amministrazione Locale
PA	Pubblica Amministrazione
PAC	Pubblica Amministrazione Centrale
S.I.	Sistema Informativo
DLT	Deloitte Consulting Srl S.B.
EY	EY Advisory SpA
Teleco	Teleco Srl

2 Anagrafica dell'amministrazione

DATI ANAGRAFICI DELL'AMMINISTRAZIONE	
Ragione sociale Amministrazione	Azienda Regionale della Salute (ARES)
Indirizzo	Via Piero della Francesca 1
CAP	09047
Comune	Selargius
Provincia	Cagliari
Regione	Sardegna
Codice Fiscale	03990570925
Indirizzo mail	segreteria.direzionegenerale@aressardegna.it
PEC	protocollo@pec.aressardegna.it
Codice PA	P65P3X9X
Comparto di Appartenenza (PAL/PAC)	PAL

DATI ANAGRAFICI REFERENTE DELL'AMMINISTRAZIONE	
Nome	Marco
Cognome	Galisai
Telefono	+39 3386570799
Indirizzo mail	marco.galisai@aressardegna.it
PEC	ict.infrastrutture@pec.aressardegna.it

3 CATEGORIZZAZIONE DELL'INTERVENTO

3.1 Categorizzazione di I livello

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

3.2 Categorizzazione di II livello

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

4 Servizi richiesti e ambito di intervento

4.1 Ambiti di intervento

L'ambito funzionale di intervento per tale fornitura è da intendersi prevalentemente finalizzato ad aumentare la consapevolezza dell'Ente e del personale sugli attacchi informatici, sui rischi cyber inerenti alla propria organizzazione e servizi, e poter supportare l'Amministrazione nel programmare le azioni da porre in essere per mitigarli attraverso attività di pianificazione, coordinamento e monitoraggio della sicurezza informatica, nonché aumentare di conseguenza il livello di resilienza alle minacce. Si è costruito quindi un piano di **security/data protection enforcement e compliance** attinente alle infrastrutture e servizi "digitali" ricadenti nel perimetro di seguito riportato:

- ARES
- AREUS
- il sistema della sanità regionale
  - ✓ N.8 ASL regione Sardegna
  - ✓ Azienda Ospedaliera Universitaria di Cagliari
  - ✓ Azienda Ospedaliera Universitaria di Sassari
  - ✓ ARNAS Brotzu

Nello specifico, i principali ambiti di intervento oggetto di tale fornitura prevedono:

- Definizione delle strategie di Governo in relazione ai principali processi in ambito Sicurezza ed in relazione alle principali normative / standard di settore, ad esempio NIS2/D.Lgs. 138/2024, PSNC, ISO27001, FNSC (L2.S16 – Security Strategy)
- Gestione sicura delle terze parti attive sugli Enti, compresa la gestione degli accessi ai sistemi dell'ente (L2.S16 – Security Strategy)
- Classificazione, protezione e gestione degli asset informativi (L2.S16 – Security Strategy)
- Adeguamento del processo di gestione degli incidenti (L2.S21 - Supporto all'analisi e alla gestione incidenti)
- Verifiche tecniche di sicurezza sui principali sistemi dell'ente (L2.S17 - Vulnerability assessment, L2.S19 – Testing Dinamico del Codice e L2.S22 - Penetration testing)
- Irrobustimento del processo di gestione della privacy in ottica di una corretta attuazione degli adempimenti del GDPR (L2. S23 – Compliance Normativa)

L'erogazione di tali servizi sarà definita in coordinamento con le ulteriori attività previste per il perimetro sanità nel progetto regionale "Attivazione CERT- CSIRT" finanziato con fondi PNRR Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" – e proposto dalla Regione Autonoma della Sardegna con il supporto di ARES Sardegna.

4.2 Servizi richiesti

Di seguito si riporta la quantificazione dei servizi richiesti nell'arco temporale previsto di 48 mesi:

ID SERVIZIO	NOME SERVIZIO	METRICA	MODALITA' DI EROGAZIONE	MODALITA' CONSUNTIVAZIONE	PERIODICITA' CONSUNTIVAZIONE	PREZZO UNITARIO OFFERTO	QUANTITA'	VALORE ECONOMICO
L2.S16	Security Strategy	gg/p Team ottimale	progettuale (a corpo)	A deliverable	Mensile	**250 €**	**7.350 gg/p**	**1.837.500,00 €**

L2.S17	Vulnerability assessment	gg/p Team ottimale	progettuale (a corpo)	A deliverable	Mensile	**165 €**	**2.048 gg/p**	**337.920,00 €**
L2.S19	Dynamic Application Security Testing	N° applicazioni per profilo	progettuale (a corpo)	A deliverable	Mensile	**482 € bronze** **1.113 € silver** **2.067 € gold**	**7 bronze** **4 silver** **3 gold**	**56.108,00 €**
L2.S21	Supporto all'analisi e alla gestione incidenti	gg/p Team ottimale	progettuale (a corpo)	A deliverable	Mensile	**170 €**	**936 gg/p**	**159.120,00 €**
L2.S22	Penetration testing	gg/p Team ottimale	progettuale (a corpo)	A deliverable	Mensile	**165 €**	**696 gg/p**	**114.840,00 €**
L2.S23	Compliance normativa	gg/p Team ottimale	progettuale (a corpo)	A deliverable	Mensile	**170 €**	**4.927 gg/p**	**837.590,00 €**
TOTALE								**3.343.078,00 €**

Nella tabella sottostante si riporta la ripartizione negli anni degli importi sopra indicati, anche con riferimento all'utilizzo di fondi derivanti da finanziamenti:

Lotto	Servizio	2025				2026				2027				2028				TOTALE
		Bilancio ARES	Avviso 8 AREUS	Misura 55 ACN Capex	Misura 55 ACN Opex	Bilancio ARES	Avviso 8 AREUS	Misura 55 ACN Capex	Misura 55 ACN Opex	Bilancio ARES	Avviso 8 AREUS	Misura 55 ACN Capex	Misura 55 ACN Opex	Bilancio ARES	Avviso 8 AREUS	Misura 55 ACN Capex	Misura 55 ACN Opex	
Lotto 2	Security Strategy	574.000,00	69.000,00			551.250,00				367.500,00				275.750,00				1.837.500,00
Lotto 2	Vulnerability assessment	35.145,00	49.335,00			84.480,00				84.480,00				84.480,00				337.920,00
Lotto 2	Dynamic Application Security Testing	14.027,00				14.027,00				14.027,00				14.027,00				56.108,00
Lotto 2	Supporto all'analisi e gestione degli incidenti	87.720,00				23.800,00				23.800,00				23.800,00				159.120,00
Lotto 2	Penetration testing	28.710,00				28.710,00				28.710,00				28.710,00				114.840,00
Lotto 2	Compliance normativa	156.400,00	136.850,00			209.440,00				209.440,00				125.460,00				837.590,00
		896.002,00	255.185,00			911.707,00				727.957,00				552.227,00				3.343.078,00

4.3 Dettaglio dei servizi richiesti

4.3.1 L2.S16 - Security Strategy

Descrizione e caratteristiche del servizio

Per le attività di durata superiore ad un anno è stata introdotta una macro descrizione delle stesse sui diversi anni.

L2.S16 - Security Strategy			**Macro Descrizione per Anno (ove applicabile)**	**Organizzazioni TARGET**
SS.1	Classificazione degli asset	Definizione di un modello per la mappatura e classificazione degli asset e di una procedura per l'identificazione di ruoli e responsabilità, sulla base della classificazione degli asset prodotta dalla piattaforma di asset intelligence e sicurezza selezionata. Definizione del campo di applicazione, contesto e criteri di rischio (rif. ISO 31000).	1 ANNO: attività di definizione di un modello per la classificazione degli asset e relativa procedura 2-3-4 ANNO: attività di mantenimento del modello di classificazione degli asset	ARES AREUS 8 ASL AOU Cagliari AOU Sassari ARNAS Brotzu
SS.2	Maturity Model	Definizione di un "maturity model", a partire dal risk assessment prodotto dalla piattaforma di asset intelligence e sicurezza selezionata, finalizzato alla valutazione del	1 ANNO: definizione del maturity model e del risk scoring degli asset critici	

		rischio, al supporto per la definizione delle misure di trattamento del rischio e al monitoraggio e riesame (rif. ISO 31000)	2-3-4 ANNO: attività di mantenimento del modello di maturity e del risk scoring	
SS.3	Assessment sulla Cybersecurity Posture – CIS v8	Esecuzione di un security assessment su ambiti/perimetri concordati finalizzato all'analisi del livello di maturità delle capacità cyber in termini di organizzazione, processi e tecnologie. L'assessment sarà eseguito sulla base dei controlli del framework CIS - Center for Internet Security - Critical Security Controls V8. Ponderazione del rischio cyber sulla base del livello di maturità dei controlli di sicurezza analizzati. Identificazione dei gap rispetto al framework CIS - Center for Internet Security - Critical Security Controls V8.		
SS.4	Azioni di contenimento di emergenza del rischio cibernetico	Dalle prime risultanze del security assessment emerse, qualora risultassero evidenze esplicite con carattere di urgenza e indifferibilità si individuano nell'immediato le azioni di contenimento del rischio implementabili rapidamente da eseguire in parallelo allo sviluppo del piano definitivo e completo.		
SS.5	Assessment sulla Cybersecurity Posture - FNCS e Misure AGID e Linee Guida Legge 90	Estensione e correlazione dei controlli del Maturity Model rispetto alle Misure Minime per la Sicurezza ICT nelle Pubbliche Amministrazioni predisposte da AgID (circolare AgID 2/2027) e al FNCS v2 di cui agli Allegati A e A2 (livelli minimi delle infrastrutture) della Determina AgID 628/2021, alle Linee Guida di resilienza della Legge 90. Identificazione dei gap rispetto alle norme citate e delle relative azioni di rimedio.	1 ANNO: estensione dell'esecuzione del security assessment alle misure minime AgID, al FNCS v2 e alle Linee Guida di resilienza della Legge 90 2-3-4 ANNO: attività di mantenimento del framework e ricalcolo del livello di security maturity in considerazione delle azioni via via implementate	
SS.6	Gestione dei fornitori e dei rischi associati	Definizione di un modello e di una procedura per la gestione dei rischi di cybersecurity e data protection (nell'ambito della gestione del dato digitale) dei fornitori. Supporto per il censimento dei fornitori rispetto ai servizi di sicurezza esternalizzati e prioritizzazione dei fornitori in termini di cyber risk rating. Definizione del modello e delle checklist per la conduzione di verifiche, in modalità self-assessment, sulle misure di sicurezza adottate dai fornitori critici.	1 ANNO: Definizione di un modello per la gestione dei rischi di cybersecurity e data protection dei fornitori e della checklist per la conduzione di audit/verifiche sulle misure di sicurezza adottate dai fornitori; Assessment dell'attuale modello di controllo degli accessi logici, rispetto agli asset e servizi IT critici, con focus sull'accesso da parte delle terze parti e delle utenze con accessi privilegiati, al fine di individuarne punti di miglioramento 1-2-3-4 ANNO: Supporto per il censimento dei fornitori di servizi esternalizzati e prioritizzazione rispetto al rischio cyber; Supporto alla conduzione	

			delle verifiche sulle misure di sicurezza adottate dai fornitori per un numero di fornitori critici, nell'ordine di massimo 5 fornitori per anno	
SS.7	Definizione del modello di gestione e controllo accessi	Esecuzione di un assessment sull'attuale modello di controllo degli accessi logici, rispetto agli asset e servizi IT critici, con focus sull'accesso da parte delle terze parti e delle utenze con accessi privilegiati, al fine di individuarne punti di miglioramento e disegnare il modello to-be da adottare.		
SS.8	Compliance Direttiva NIS2/D.Lgs. 138/2024	Aggiornamento del risk assessment e del maturity assessment rispetto alle misure di gestione del rischio previste dalla Direttiva NIS2 e dal decreto italiano di recepimento D.Lgs. 138/2024 e del relativo remediation plan. Redazione dei compliance documents NIS2/D.Lgs. 138/2024. Aggiornamento periodico, annuale, della documentazione predisposta.	1 ANNO: valutazione dello stato di compliance as-is alla normativa NIS2/D.Lgs. 138/2024 e definizione del piano di adeguamento 2-3-4 ANNO: attività di mantenimento del framework NIS2/D.Lgs. 138/2024 e relativa compliance	ARES AREUS 8 ASL AOU Cagliari AOU Sassari ARNAS Brotzu
SS.9	Compliance PSNC	Svolgimento di un assessment, basato su Framework Nazionale Cyber Security, comprensivo delle disposizioni di cui ai regolamenti vigenti per i soggetti inclusi nel Perimetro di Sicurezza Nazionale in modo da: • Indicare il grado di adeguamento dell'Amministrazione ai livelli standard di sicurezza previsti per il Perimetro di Sicurezza; • Individuare le possibili azioni correttive e soluzioni rispetto agli standard vigenti nell'organizzazione; • Predisporre la documentazione obbligatoria per la compliance e l'accountability delle misure adottate ai sensi del DPCM 81/2021.	1 ANNO: valutazione dello stato di compliance as-is ai requisiti del PSNC e aggiornamento della documentazione obbligatoria per la compliance 2-3-4 ANNO: attività di mantenimento della compliance al PSNC	AREUS
SS.10	Supporto coordinamento alle iniziative di Secure Design in ambito PSN	Supporto e coordinamento per la verifica delle iniziative di Security By Design avviate nel corso delle attività di migrazione verso il PSN (erogate a cura dei professionisti PSN), al fine di garantire la corretta implementazione delle misure by default e by design necessarie.		ARES AREUS 8 ASL AOU Cagliari AOU Sassari ARNAS Brotzu
SS.11	Definizione dei piani di sicurezza e compliance	Individuazione delle azioni di remediation e definizione dei piani di sicurezza e compliance delle organizzazioni nel perimetro di intervento, derivanti dall'applicazione del Maturity Model completo. Sviluppo del piano strategico di cybersecurity di ARES.		
SS.12	Coordinamento dei piani di sicurezza e compliance	Supporto e coordinamento dell'implementazione dei piani di sicurezza e compliance delle organizzazioni nel perimetro di intervento.		

SS.13	Analisi della conformità ISO 27001 e sue estensioni - ARES	Individuazione dell'ambito di attuazione e verifica della conformità rispetto allo standard ISO27001:2022 e sue estensioni (ISO27017, ISO27018). Identificazione di eventuali gap e definizione delle azioni di rientro, implementazione dei controlli finalizzati a conseguire la certificazione ISO di ARES.		ARES
SS.14	Implementazione del SGSI - ARES	Predisposizione della documentazione specifica in ambito ISO/IEC 27001:2022 e sue estensioni (ISO27017, ISO27018) e raccolta delle evidenze dell'implementazione del Sistema di Gestione della Sicurezza delle Informazioni. Erogazione formazione in ambito ISO, supporto nell'esecuzione di audit interni e nel Riesame di Direzione.	2 ANNO: implementazione delle misure organizzative e documentali necessarie per l'implementazione del SGSI 3-4 ANNO: attività di mantenimento del framework ISO27001 e sue estensioni	ARES
SS.15	Qualificazione ACN servizi cloud ARES	Individuazione dei servizi e predisposizione della documentazione e delle azioni indicate nel Decreto direttoriale prot. N. 29 del 02/01/2023 richieste per la qualifica dei servizi.		ARES
SS.16	Miglioramento continuo	Manutenzione periodica del Maturity Model e degli indici di rischio al fine di valutare i miglioramenti della posture di cybersecurity e di aggiornare la prioritizzazione degli interventi residui. Analisi e miglioramento del modello di governo a livello organizzativo e documentale in merito ai principali processi di gestione della cybersecurity e della data protection.		ARES AREUS 8 ASL AOU Cagliari AOU Sassari ARNAS Brotzu
SS.17	Cyber Strategic Risk Management	Valutazione ed analisi del rischio strategico, valutazione dell'intelligence sulle minacce più verticali al contesto in modo strutturato per valutare e mitigare i rischi specifici del contesto di azione con un approccio Data driven.		ARES AREUS 8 ASL AOU Cagliari AOU Sassari ARNAS Brotzu

Articolazione Dettagliata del Servizio di Security Strategy

Il servizio di Security Strategy prevede l'esecuzione di una serie di macro-attività di seguito riportate, con riferimento a quanto riportato in tabella.

- **Classificazione asset (rif. SS1):**
  - Definizione di un modello per la mappatura e classificazione degli asset
  - Redazione di una procedura per l'identificazione di ruoli e responsabilità, sulla base della classificazione degli asset prodotta dalla piattaforma di asset intelligence e sicurezza selezionata dall'Ente
  - Condivisione di un documento formativo/informativo internamente ad ARES

- **Maturity Model (rif. SS2-SS4):**
  - Definizione di un "maturity model" finalizzato alla valutazione del rischio cyber, comprensiva delle misure di trattamento del rischio e al monitoraggio e riesame (rif. ISO 31000), sulla base

delle valutazioni di risk assessment prodotte dalla piattaforma di asset intelligence e sicurezza selezionata dall'Ente
  - Individuazione delle azioni prioritarie di contenimento del rischio, implementabili rapidamente, da eseguire in parallelo allo sviluppo del piano definitivo e completo
  - Manutenzione periodica del maturity model e degli indici di rischio, tramite la piattaforma di asset intelligence e sicurezza selezionata dall'Ente, al fine di valutare i miglioramenti dei livelli di maturità e di aggiornare la prioritizzazione degli interventi

- **Cybersecurity Posture Framework (rif. SS3-SS5):**
  - Esecuzione di un maturity security assessment su organizzazione, processi e tecnologie, basato sui controlli del framework CIS - Center for Internet Security - Critical Security Controls V8
  - Estensione e correlazione dei controlli del Maturity Model rispetto alle Misure Minime per la Sicurezza ICT nelle Pubbliche Amministrazioni predisposte da AgID (circolare AgID 2/2027)
  - Estensione e correlazione dei controlli del Maturity Model rispetto al FNCS v2 di cui agli Allegati A e A2 (livelli minimi delle infrastrutture) della Determina AgID 628/2021
  - Estensione e correlazione dei controlli del Maturity Model rispetto alle Linee Guida di resilienza della Legge 90/2024

- **Gestione Terze Parti e Modello Accessi (rif. SS6-SS7):**
  - Definizione di un modello per la gestione dei rischi di cybersecurity e data protection dei fornitori
  - Supporto per il censimento dei fornitori di servizi esternalizzati e prioritizzazione rispetto al rischio cyber
  - Definizione della checklist per la conduzione di audit/verifiche sulle misure di sicurezza adottate dai fornitori
  - Supporto alla conduzione delle verifiche sulle misure di sicurezza adottate dai fornitori per un numero di fornitori critici, nell'ordine di massimo 5 fornitori per anno
  - Assessment dell'attuale modello di controllo degli accessi logici, rispetto agli asset e servizi IT critici, con focus sull'accesso da parte delle terze parti e delle utenze con accessi privilegiati, al fine di individuarne punti di miglioramento
  - Disegno del modello to-be di gestione degli accessi logici da adottare
- **Sviluppo, coordinamento e monitoraggio continuo dei piani di sicurezza e di compliance (rif. SS11-SS12-SS16):**
  - Definizione dei piani di sicurezza e di compliance specifici per le organizzazioni in ambito sulla base delle azioni emerse dalle attività precedenti
  - Supporto e coordinamento all'implementazione degli stessi anche tramite le attività previste da ulteriori stream progettuali che l'Ente attiva o attiverà (es. attività comprese in Lotto 1, PSN)
  - Identificazione delle aree di rischio e definizione delle strategie di gestione dello stesso
  - Analisi e miglioramento del modello di governo organizzativo e documentale, in merito ai principali processi di gestione della cybersecurity e della data protection
  - Sviluppo del piano strategico di cybersecurity di ARES
  - Verifica continua dell'allineamento del programma definito rispetto agli obiettivi previsti
  - Aggiornamento del piano delle attività, del registro delle criticità, del registro dei cambiamenti richiesti
  - Elaborazione del materiale per gli stati di avanzamento lavoro (SAL) periodici
- **Compliance Direttiva NIS2/D.Lgs. 138/2024 (rif. SS8):**
  - Aggiornamento del risk assessment e del maturity assessment rispetto alle misure di gestione del rischio previste dalla Direttiva NIS2 e dal decreto italiano di recepimento D.Lgs. 138/2024
  - Redazione del remediation plan e del compendio documentale richiesto in ambito NIS2/D.Lgs. 138/2024
  - Aggiornamento periodico della documentazione predisposta

- **Compliance PSNC (rif. SS9):**
  - Svolgimento di un assessment, basato su Framework Nazionale Cyber Security, e secondo le disposizioni previste dal Perimetro di Sicurezza Nazionale Cibernetica per la verifica dello stato as-is di AREUS
  - Definizione del livello di adeguamento di AREUS ai livelli standard di sicurezza previsti per il Perimetro di Sicurezza Nazionale Cibernetica
  - Individuazione delle azioni di rimedio e proposta di possibili soluzioni in considerazione anche degli standard vigenti nell'organizzazione
  - Predisposizione della documentazione obbligatoria per la compliance e l'accountability delle misure adottate ai sensi del DPCM 81/2021 (PSNC)
- **Supporto coordinamento alle iniziative di Secure Design in ambito PSN (rif. SS10):** Supporto e coordinamento per la verifica delle iniziative di Security By Design avviate nel corso delle attività di migrazione verso il PSN ed erogate da terze parti, al fine di assicurare che sia garantita la corretta implementazione delle misure by default e by design necessarie
- **Cyber Strategic Risk Management (rif. SS17):** Valutazione ed analisi del rischio strategico, valutazione dell'intelligence sulle minacce più verticali al contesto in modo strutturato per valutare e mitigare i rischi specifici del contesto di azione con un approccio data driven
- **ISO Compliance (rif. SS13-SS14):**
  - Individuazione dell'ambito di attuazione e verifica della conformità rispetto allo standard ISO27001:2022 e sue estensioni (ISO27017, ISO27018)
  - Individuazione di gap puntuali e definizione delle azioni di rientro
  - Implementazione dei controlli finalizzati a conseguire la certificazione ISO27001:2022 di ARES e predisposizione della documentazione specifica in ambito ISO/IEC 27001:2022 e sue estensioni (ISO27017, ISO27018)
  - Erogazione di sessioni di formazione in ambito ISO, supporto nell'esecuzione di audit interni e nella predisposizione della documentazione per il Riesame di Direzione
- **Qualificazione ACN servizi cloud ARES (rif. SS15):** Individuazione dei servizi e predisposizione della documentazione e delle azioni indicate nel Decreto direttoriale prot. N. 29 del 02/01/2023 richieste per la qualifica dei servizi cloud

Modalità di erogazione e consuntivazione

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

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

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

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

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

Attivazione e durata

Si prevede l'avvio del servizio entro Gennaio 2025 per una durata di 48 mesi.

Modalità di configurazione

N.A.

Specifiche di collaudo

N.A.

4.3.2 L2.S17 - Vulnerability assessment

Descrizione e caratteristiche del servizio

L2.S17 Vulnerability Assessment			**Organizzazioni TARGET**
VA.1	Vulnerability Assessment periodici	Verifiche annuali di sicurezza sul perimetro di sistemi, applicazioni e medical device concordato (infrastruttura di base), nell'ordine di 20 applicazioni per anno.	ARES AREUS 8 ASL AOU Cagliari AOU Sassari ARNAS Brotzu
VA.2	Esecuzione delle attività in modalità black-box	Esecuzione delle attività in modalità black-box dall'esterno della rete aziendale e dall'interno sui sistemi locati nei data center on-premise, secondo gli standard della metodologia OWASP, al fine di rilevare vulnerabilità presenti per i target oggetto di analisi mediante tool automatizzati e tecniche manuali.	
VA.3	Prioritizzazione delle vulnerabilità e Remediation Plan.	Prioritizzazione delle vulnerabilità, verifica dei risultati e predisposizione Remediation Plan.	
VA.4	Re-test delle vulnerabilità	Re-test delle vulnerabilità concordando con l'Ente tempistiche e vulnerabilità da analizzare, a seguito del processo di mitigazione delle vulnerabilità effettuato.	

Articolazione dettagliata del Servizio di Vulnerability Assessment

Il servizio di Vulnerability Assessment ha l'obiettivo di identificare in maniera proattiva, mediante una verifica dinamica della sicurezza, le vulnerabilità presenti su dispositivi di rete, software e applicazioni delle organizzazioni in perimetro e la mitigazione dei rischi cyber connessi. L'acquisizione del servizio prevede l'esecuzione delle attività di seguito elencate:

- Pianificazione: tale fase è fondamentale per la pianificazione delle attività di VA (tempistiche e orari di test) e per la raccolta delle informazioni necessarie all'esecuzione di verifiche di sicurezza efficaci e per la definizione esatta del perimetro di intervento (nell'ordine di 20 applicazioni per anno);
- Esecuzione: Esecuzione delle attività in modalità black-box dall'esterno della rete aziendale e dall'interno sui sistemi locati nei data center on-premise, secondo gli standard della metodologia

OWASP, al fine di rilevare vulnerabilità presenti per i target oggetto di analisi mediante tool automatizzati e tecniche manuali. I relativi risultati saranno analizzati e correlati dal Team operativo;

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

Modalità di erogazione e consuntivazione

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

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

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

- Security Principal
- Senior Penetration tester
- Junior Penetration tester

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

Attivazione e durata

Si prevede l'avvio del servizio entro Gennaio 2025 per una durata di 48 mesi.

Modalità di configurazione

N.A

Specifiche di collaudo

N.A.

4.3.3 L2.S19 – Testing Dinamico del Codice

Descrizione e caratteristiche del servizio

L2.S19 Testing Dinamico del Codice			Organizzazioni TARGET
TD.1	Identificazione del perimetro di applicazioni	Identificazione del perimetro di applicazioni da verificare annualmente, in base alle evoluzioni tecnologiche e nuove implementazioni critiche. Si ipotizza per ogni anno l'esecuzione di testing dinamico del codice su 7 applicazioni con profilo "bronze", 4 con profilo "silver" e 3 con profilo "gold"	ARES AREUS 8 ASL AOU Cagliari AOU Sassari ARNAS Brotzu
TD.2	Definizione delle modalità operative	Definizione delle modalità operative di esecuzione delle analisi.	
TD.3	Esecuzione del Testing	Esecuzione del Testing del codice sulle applicazioni dell'Ente target, secondo il perimetro concordato.	
TD.4	Analisi risultati e predisposizione reportistica	Analisi risultati e predisposizione reportistica a livello executive e tecnica.	
TD.5	Definizione del remediation plan	Definizione del piano di rimedio da attuare per eliminare le vulnerabilità riscontrate.	
TD.6	Re-test delle applicazioni	Re-test delle applicazioni concordando con l'Ente tempistiche e vulnerabilità da analizzare, a seguito del processo di mitigazione delle vulnerabilità effettuato.	

Articolazione dettagliata del Servizio di Testing Dinamico del Codice

FASE 1: Al fine di definire la corretta ed efficiente pianificazione e monitoraggio delle attività di test dinamici di sicurezza, si provvederà alla individuazione della lista di applicazioni da sottoporre a testing di sicurezza in base a specifici driver di business quali:

- Esistenza di portali esposti su Internet.
- Distribuzione degli asset su Cloud oltre che on-premises.
- Tipologia di dati trattati (sensibili, sanitari, giudiziari, ecc.).
- Funzione di business esposta (es. B2B come il portale per le gare telematiche, B2C come il fascicolo sanitario).
- Complessità intrinseca dell'applicazione e suo livello di rischio cyber.

Le modalità operative saranno dunque concordate preventivamente rispetto a ciascun test di sicurezza in linea con gli standard internazionali di settore quali Open Web Application Security Project (OWASP) ed Open Source Security Testing Methodology Manual (OSSTMM), dunque seguendo alcuni fattori chiave:

- Valutazione delle criticità del singolo sistema rispetto all'architettura IT generale, sue interdipendenze e flussi dati.
- Predisposizione di ambienti segregati ed appositamente predisposti per l'esecuzione dei test di sicurezza, con eventuale apertura network e whitelisting firewall.
- Scelta degli strumenti software, tecniche di attacco e fasce temporali entro le quali eseguire i test di sicurezza al fine di non causare danni o rallentamenti ai sistemi aziendali.
- Condivisione e sottoscrizione di un documento di manleva che riepiloghi ogni informazione sopra riportata vincolandola unicamente al test di sicurezza da eseguire.

Le vulnerabilità di sicurezza saranno censite secondo gli standard Common Vulnerabilities Exposure (CVE) e Common Weakness Enumeration (CWE), e saranno associate ad un livello di severità o gravità secondo lo standard Common Vulnerability Scoring System (CVSS) v3.0.

FASE 2: Al fine di identificare potenziali vulnerabilità di sicurezza note secondo gli standard CVE e CWE afferenti alle applicazioni in-scope, si provvederà ad eseguire una scansione semi-automatica ovvero dinamica delle stesse avvalendosi di strumenti automatici in una prima fase ed effettuando un secondo livello di scansione manuale per filtrare i falsi positivi.
Le attività di dettaglio che saranno eseguite in questa fase progettuale sono qui elencate:

- Configurazione dello strumento per eseguire DAST con le informazioni dell'applicazione da scansionare o del servizio da testare.
- Esecuzione dei test di sicurezza rispettando il toolset preaccordato rispetto ai target presenti in manleva.
- Analisi e filtraggio dei risultati parziali con l'obiettivo di individuare e rimuovere gli eventuali falsi positivi qualora presenti, mediante attenta revisione manuale di ogni risultanza rispetto al contesto di riferimento.

In caso di riscontro di vulnerabilità di sicurezza aventi gravità altissima (CVSS con score > 8.0), si allerteranno tempestivamente le strutture preposte al fine di adottare un approccio collaborativo e proattivo mirato alla gestione di problemi in modo congruo rispetto al contesto di riferimento.

FASE 3: Una volta consolidate le risultanze confermando l'effettiva presenza di sole vulnerabilità realmente sfruttabili, si provvederà alla stesura di due deliverables di progetto quali:

- Un documento di Technical Report (di taglio tecnico) il quale contiene tutte le vulnerabilità di sicurezza individuate durante il processo e fornisce informazioni dettagliate sulle lacune di sicurezza identificate.
- Un documento di Executive Report (di taglio dirigenziale) il quale riassume le risultanze identificate aggregandole per severità, suggerendo l'adozione di misure di sicurezza correttive.

FASE 4: sarà redatto il cosiddetto piano di rimedio che ha l'obiettivo di prioritizzare nel tempo specifiche azioni di bonifica delle vulnerabilità di sicurezza precedentemente censite.

FASE 5: Per ogni applicazione già sottoposta a test di sicurezza, è possibile definire azioni di re-test delle stesse a valle del processo di mitigazione delle vulnerabilità, effettuato mediante il remediation plan: tale fase di re-test dovrà necessariamente ripercorrere ovvero rivalutare l'esecuzione di ogni fase citata sin d'ora, poiché alcuni dettagli operativi relativi al perimetro di re-test possono essere cambiati a seguito dell'effettiva implementazione di azioni correttive di bonifica. La fase di re-test delle applicazioni prevedrà dunque un nuovo confronto con i referenti applicativi al fine di confermare le modalità operative di esecuzione dei test, vincoli ad esse collegati e pianificazione delle attività.

Modalità di erogazione e consuntivazione

Coerentemente a quanto previsto nel "CAPITOLATO TECNICO SPECIALE SERVIZI DI COMPLIANCE E CONTROLLO" si precisa che la modalità di remunerazione di tali servizi è "canone (annuale)" e che la metrica di misurazione è "*numero di applicazioni per profilo (Bronze/Silver/Gold)/anno"*.

La fatturazione avverrà sulla base dello stato dell'avanzamento dell'esecuzione delle attività di testing dinamico del codice sulle singole applicazioni per tipo di profilo (Bronze, Silver e Gold) e sarà riconosciuta bimestralmente.

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

Attivazione e durata

Si prevede l'avvio del servizio entro Gennaio 2025 per una durata di 48 mesi.

Modalità di configurazione

N.A

Specifiche di collaudo

N.A.

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

Descrizione e caratteristiche del servizio

Per le attività di durata superiore ad un anno è stata introdotta una macro descrizione delle stesse sui diversi anni.

L2.S21 Supporto all'analisi e gestione degli incidenti			**Macro Descrizione per Anno**	**Organizzazioni TARGET**
GI.1	Analisi processi e strumenti per la gestione degli incidenti	Analisi degli attuali processi e strumenti per la gestione degli incidenti nelle organizzazioni in scope, anche con riferimento alle normative applicabili in materia (es. GDPR, Legge 90, Direttiva NIS2, PSNC).	1 ANNO: Analisi processi e strumenti per la gestione degli incidenti; Definizione del modello di	ARES AREUS 8 ASL AOU Cagliari AOU Sassari ARNAS Brotzu

GI.2	Definizione del modello di gestione degli incidenti	Definizione del modello di gestione degli incidenti in termini di: - People: ruoli e responsabilità per la rilevazione e gestione degli incidenti di sicurezza e per la gestione delle crisi da incidenti informatici; - Process: processi, policy, procedure operative e playbook per la risposta agli incidenti di sicurezza; - Technology: strumenti e soluzioni tecnologiche funzionali alla gestione degli incidenti. Individuazione ed applicazioni delle eventuali azioni da implementare a valle di un incidente grave occorso	gestione degli incidenti to-be; 1-2-3-4 ANNO: Simulazione annuale di un incidente; miglioramento continuo del processo di gestione incidenti anche tramite l'analisi ex-post degli incidenti di tipo grave occorsi.	
GI.3	Simulazione annuale di un incidente	Simulazione annuale di un incidente cyber tramite table top exercise, su un perimetro concordato di organizzazioni, e aggiornamento periodico del modello definito.		

Articolazione dettagliata del servizio di Supporto all'analisi e gestione degli incidenti

Il servizio di Supporto all'analisi e gestione degli incidenti prevede l'esecuzione di una serie di macro-attività di seguito riportate:

- Analisi del processo di gestione degli incidenti as- is nelle organizzazioni in scope, al fine di verificarne il corretto adeguamento alle normative applicabili in materia e/o le scoperture in essere (es. GDPR, Legge 90, Direttiva NIS2, PSNC)
- Definizione del modello di gestione degli incidenti to-be da adottare in termini di: ruoli e responsabilità per la rilevazione e gestione degli incidenti di sicurezza e per la gestione delle crisi da incidenti informatici; processi, policy, procedure operative e playbook per la risposta agli incidenti di sicurezza; individuazione di possibili strumenti e soluzioni tecnologiche funzionali alla gestione degli incidenti
- Lesson learned e miglioramento continuo: analisi ex-post degli incidenti di tipo grave gestiti dalle strutture preposte dell'Ente, occorsi nel corso del periodo di supporto, al fine di individuare le eventuali azioni tecniche e/o organizzative migliorative da implementare a valle dello stesso
- Simulazione di tipo table-top di un incidente al fine di testare il modello di gestione dell'incidente definito
- Definizione ed implementazione delle azioni di miglioramento da introdurre nel processo di gestione incidenti a seguito della simulazione

Modalità di erogazione e consuntivazione

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

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

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

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

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

Attivazione e durata

Si prevede l'avvio del servizio entro Gennaio 2025 per una durata di 48 mesi.

Modalità di configurazione

N.A

Specifiche di collaudo

N.A.

4.3.5 L2.S22 – Penetration Testing

Descrizione e caratteristiche del servizio

L2.S22 Penetration testing			**Organizzazioni TARGET**
PT.1	Identificazione del perimetro di sistemi	Identificazione del perimetro di sistemi, con rilevazione dei servizi e delle applicazioni critiche da verificare annualmente, in base alle evoluzioni tecnologiche e nuove implementazioni critiche, nell'ordine di 7 applicazioni a bassa complessità (classificazione "light") per il primo anno e 6 applicazioni a bassa complessità (classificazione "light") per anno per gli anni successivi al primo.	ARES AREUS 8 ASL AOU Cagliari AOU Sassari ARNAS Brotzu
PT.2	Definizione delle modalità operative	Definizione delle modalità operative di esecuzione delle analisi.	

PT.3	Esecuzione del Penetration test	Esecuzione del Penetration test sull'infrastruttura e sulle applicazioni dell'Ente target, secondo il perimetro concordato, dall'esterno della rete aziendale e dall'interno sui sistemi locati nei data center on-premise, secondo gli standard della metodologia OWASP.	
PT.4	Analisi risultati e predisposizione reportistica	Analisi risultati e predisposizione reportistica a livello executive e tecnica.	
PT.5	Definizione del remediation plan.	Definizione del piano di rimedio da attuare per eliminare le vulnerabilità riscontrate.	
PT.6	Re-test delle applicazioni	Re-test delle applicazioni concordando con l'Ente tempistiche e vulnerabilità da analizzare, a seguito del processo di mitigazione delle vulnerabilità effettuato.	

Articolazione dettagliata del Servizio di Penetration Testing

Il servizio di Penetration Testing ha l'obiettivo di verificare concretamente la possibilità di sfruttare le eventuali vulnerabilità identificate su sistemi/reti/applicazioni/dispositivi dell'Amministrazione. L'acquisizione del servizio prevede, su un set di applicazioni di bassa complessità e con un approccio timebox, l'esecuzione delle attività operative di seguito elencate:

- Planning and Preparation: discussione di un Kick Off meeting dove verranno discussi gli aspetti preliminari per l'esecuzione delle attività, con particolare focus sul perimetro dell'attività (target in scope e criticità degli stessi), sui vincoli operativi e sulle regole d'ingaggio. La presente fase infine prevede l'installazione e/o la configurazione degli strumenti hardware e software necessari per l'esecuzione delle analisi;
- Acquisizione delle informazioni esposte dagli applicativi e dai sistemi che li ospitano al fine di contestualizzare gli attacchi da portare a termine;
- Esecuzione di una scansione automatica delle vulnerabilità. I risultati saranno revisionati manualmente per individuare i servizi su cui effettuare attacchi mirati e contestualmente si procederà all'eventuale personalizzazione degli exploit necessari allo sfruttamento delle vulnerabilità;
- Exploitation: in base alla tipologia di PT, saranno eseguiti una serie di attacchi finalizzati allo sfruttamento delle possibili vulnerabilità identificate.
- Per ogni vulnerabilità identificata saranno fornite raccomandazioni sulle azioni da intraprendere per la loro risoluzione o mitigazione, con anche indicazione delle priorità da attribuire sempre in coerenza con le policy dell'Ente e del livello di criticità/rischio precedentemente determinato. Queste saranno riportate all'interno di un piano di rientro concreto e applicabile al contesto (con indicazione anche delle tempistiche di risoluzione condivise con l'Ente) in grado di supportare le linee tecniche dell'Ente nella risoluzione. I risultati delle attività di VA e le raccomandazioni fornite saranno riportate in specifici report: Executive Summary, Technical Report e Remediation Plan;
- Re-test delle vulnerabilità: successivamente all'esecuzione delle azioni di rimedio delle vulnerabilità identificate, riportate all'interno del piano di rientro, potranno essere pianificate e svolte attività di re-test per verificare in maniera efficace la risoluzione delle vulnerabilità sui target analizzati e la mitigazione dei rischi connessi.

Modalità di erogazione e consuntivazione

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

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

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

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

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

Attivazione e durata

Si prevede l'avvio del servizio entro Gennaio 2025 per una durata di 48 mesi.

Modalità di configurazione

N.A.

Specifiche di collaudo

N.A.

4.3.6 L2.S23 - Compliance normativa

Descrizione e caratteristiche del servizio

Per le attività di durata superiore ad un anno è stata introdotta una macro descrizione delle stesse sui diversi anni.

L2.S23 Compliance Normativa			**Macro Descrizione per Anno**	**Organizzazioni TARGET**
GDPR.1	Assessment della conformità Privacy	Assessment preliminare per la verifica dello stato di compliance as is delle organizzazioni in perimetro, in ambito Privacy, mediante predisposizione di un framework di controllo ed esecuzione di interviste per l'analisi dei processi e delle procedure in ambito e relativa gap analysis rispetto ai requisiti normativi.	1 ANNO: Assessment della conformità Privacy 1-2-3-4 ANNO: Aggiornamento del registro dei	ARES AREUS 8 ASL AOU Cagliari AOU Sassari ARNAS Brotzu

GDPR.2	Aggiornamento del registro dei trattamenti	Tramite il supporto dello strumento opportunamente selezionato, aggiornamento del registro dei trattamenti di ARES e dalle altre AS a partire dalle attuali versioni dei registri dei trattamenti, tramite interviste di approfondimento ed analisi della documentazione rilevante rispetto a nuove progettualità ed esigenze che prevedono trattamenti di dati personali. Manutenzione periodica del registro dei trattamenti in funzione delle iniziative sviluppate da ARES e dalle altre AS che prevedono trattamenti di dati personali.	trattamenti; Esecuzione di analisi dei rischi privacy e DPIA sui trattamenti rilevanti; Consolidamento e governo della Conformità Privacy	
GDPR.3	Esecuzione di analisi dei rischi privacy e DPIA sui trattamenti rilevanti	Tramite il supporto dello strumento opportunamente selezionato, ricognizione dei trattamenti di dati personali svolti da ARES e dalle altre AS che necessitano di specifica analisi dei rischi di impatti privacy. Svolgimento di attività di analisi dei rischi e DPIA, consultazione con i DPO di ARES e delle altre AS e redazione di un documento per ogni trattamento analizzato riportante i risultati emersi, i rischi connessi e le decisioni intraprese.		
GDPR.4	Consolidamento e governo della Conformità Privacy	Consolidamento del livello di compliance normativa in ambito Privacy mediante revisione ed ottimizzazione dei processi e delle procedure in ambito e piano di rafforzamento delle misure tecniche da adottare per un adeguato livello di sicurezza al trattamento dei dati sui sistemi ICT, tramite una esecuzione periodica dell'assessment basato sul framework predisposto.		

Articolazione Dettagliata del Servizio di Compliance Normativa

Il Sistema di gestione della Privacy ha necessità di essere disegnato, analizzato, implementato, monitorato e continuamente migliorato in un'ottica anche di lungo periodo, al fine di trasformare la privacy in un fattore abilitante per il trattamento dei dati da parte di ARES e degli altri Enti e garantire agli interessati la protezione dei dati personali. A tale scopo il servizio prevede l'esecuzione di tali attività:

- Svolgimento di un assessment, tramite interviste ed analisi della documentazione presente, basato su uno specifico framework di controllo basato sugli standard vigenti, per verificare lo stato di conformità alla normativa applicabile da parte degli Enti

- Definizione delle aree maggiormente a rischio e identificazione degli eventuali interventi di rimedio necessari per garantire conformità e allo stesso tempo automatizzare i processi privacy
- Ricognizione dei registri di trattamento ad oggi presenti per le organizzazioni in scope
- Aggiornamento del registro dei trattamenti, tramite l'utilizzo di uno strumento di supporto e tramite interviste di approfondimento ed analisi della documentazione rilevante
- Manutenzione periodica del registro dei trattamenti
- Predisposizione di una nuova metodologia per l'individuazione dei trattamenti ad alto rischio e per l'esecuzione della Data Protection Impact Assessment (DPIA)
- Esecuzione di DPIA per i trattamenti ritenuti critici, su un numero massimo di 5 DPIA per Ente
- Redazione di un documento per ogni trattamento analizzato riportante i risultati emersi, i rischi connessi e le decisioni intraprese.
- Aggiornamento del compendio documentale Privacy, a seguito di una nuova esecuzione dell'assessment tramite il framework predisposto per il mantenimento della compliance (es. politiche, procedure, metodologie, nomine a responsabile, informative, data processing agreement, materiale formativo)

Modalità di erogazione e consuntivazione

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

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

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

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

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

Attivazione e durata

Si prevede l'avvio del servizio entro Gennaio 2025 per una durata di 48 mesi.

Modalità di configurazione

N.A.

Specifiche di collaudo

N.A.

5 Organizzazione e modalità di erogazione del contratto esecutivo

5.1 Attività in carico alle aziende del RTI

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

SERVIZIO	Deloitte Consulting	EY Advisory	Teleco
TOTALE	**36,43 %**	**38,56 %**	**25,01 %**

5.2 Modalità di ricorso al subappalto da parte del fornitore

SERVIZIO	AZIENDA RTI	QUOTA SUBAPPALTABILE	SUBAPPALTATORE
L2.S16, L2.S17, L2.S19, L2.S21, L2.S22, L2.S23	**Deloitte Consulting Srl S.B.** **EY Advisory SpA** **Teleco S.r.l.**	**50%**	**DA DEFINIRE**

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

5.3 Organizzazione e figure di riferimento del fornitore

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

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

RUOLO	NOMINATIVI
RUAC CE	Fabio Cappelli
Referente Tecnico CE (RT)	Andrea Mariotti
Responsabile Attività L2.S16	Lorenzo Pietrini
Responsabile Attività L2.S17	Michele Dell'Uomo
Responsabile Attività L2.S19	Michele Dell'Uomo
Responsabile Attività L2.S21	Marco Ceccon

Responsabile Attività L2.S22	Michele Dell'Uomo
Responsabile Attività L2.S23	Giacomo Fatigati

5.4 Modalità di esecuzione dei servizi

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

6 Piano di lavoro

6.1 Piano di Presa in carico

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

FASE	ATTIVITÀ	W1	W2	W3	W4	W5
Pianificazione	Pianificazione delle attività					
Predisposizione Strumenti	Predisposizione e aggiornamento strumenti					
Assessment documentale	Analisi AS IS dei progetti in corso					
Acquisizione competenze	Incontri con il personale dell'Amministrazione, training on the job, self training, workshop					
Ottimizzazione	Individuazione delle possibili aree di miglioramento					
Fine presa in carico	Ricognizione e verifica delle attività svolte					
Governance	Verifica dello stato delle attività					

6.2 Cronoprogramma

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

		Anno 1						Anno 2						Anno 3						Anno 4					
		B1	B2	B3	B4	B5	B6	B1	B2	B3	B4	B5	B6	B1	B2	B3	B4	B5	B6	B1	B2	B3	B4	B5	B6
	L2.S16 - Security Strategy																								
SS.1	*Classificazione degli asset*																								
SS.2	*Maturity Model*																								
SS.3	*Assessment sulla Cybersecurity Posture – CIS v8*																								
SS.4	*Azioni di contenimento di emergenza del rischio cibernetico*																								
SS.5	*Assessment sulla Cybersecurity Posture - FNCS e Misure AGID e Linee Guida Legge 90*																								
SS.6	*Gestione dei fornitori e dei rischi associati*																								
SS.7	*Definizione del modello di gestione e controllo accessi*																								
SS.8	*Compliance Direttiva NIS2 / D.Lgs. 138/2024*																								
SS.9	*Compliance PSNC*																								
SS.10	*Supporto coordinamento alle iniziative di Secure Design in ambito PSN*																								
SS.11	*Definizione dei piani di sicurezza e compliance*																								
SS.12	*Coordinamento dei piani di sicurezza e compliance*																								
SS.13	*Analisi della conformita ISO 27001 e sue estensioni - ARES*																								
SS.14	*Implementazione del SGSI - ARES*																								
SS.15	*Qualificazione ACN servizi cloud ARES*																								
SS.16	*Miglioramento continuo*																								
SS.17	*Cyber Strategic Risk Management*																								
	L2.S17 Vulnerability Assessment																								
VA.1	Vulnerability Assessment periodici																								
VA.2	Esecuzione delle attività in modalità black-box																								
VA.3	Prioritizzazione delle vulnerabilità e Remediation Plan																								
VA.4	Re-test delle vulnerabilità																								
	L2.S19 Testing Dinamico del Codice																								
TD.1	*Identificazione del perimetro di applicazioni*																								
TD.2	*Definizione delle modalità operative*																								
TD.3	*Esecuzione del Penetration test*																								
TD.4	*Analisi risultati e predisposizione reportistica*																								
TD.5	*Definizione del remediation plan*																								
TD.6	*Re-test delle applicazioni*																								
	L2.S21 Supporto all'analisi e gestione degli incidenti																								
GI.1	Analisi processi e strumenti per la gestione degli incidenti																								
GI.2	Definizione del modello di gestione degli incidenti																								
GI.3	Simulazione annuale di un incidente																								
	L2.S22 Penetration testing																								
PT.1	*Identificazione del perimetro di sistemi*																								
PT.2	*Definizione delle modalità operative*																								
PT.3	*Esecuzione del Testing*																								
PT.4	*Analisi risultati e predisposizione reportistica*																								
PT.5	*Definizione del remediation plan*																								
PT.6	*Re-test delle applicazioni*																								
	L2.S23 Compliance Normativa																								
GDPR.1	*Assessment della conformità Privacy*																								
GDPR.2	*Aggiornamento del registro dei trattamenti*																								
GDPR.3	*Esecuzione di analisi dei rischi privacy e DPIA sui trattamenti rilevanti*																								
GDPR.4	*Consolidamento e governo della Conformità Privacy*																								

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

6.3 Data di attivazione e durata del servizio

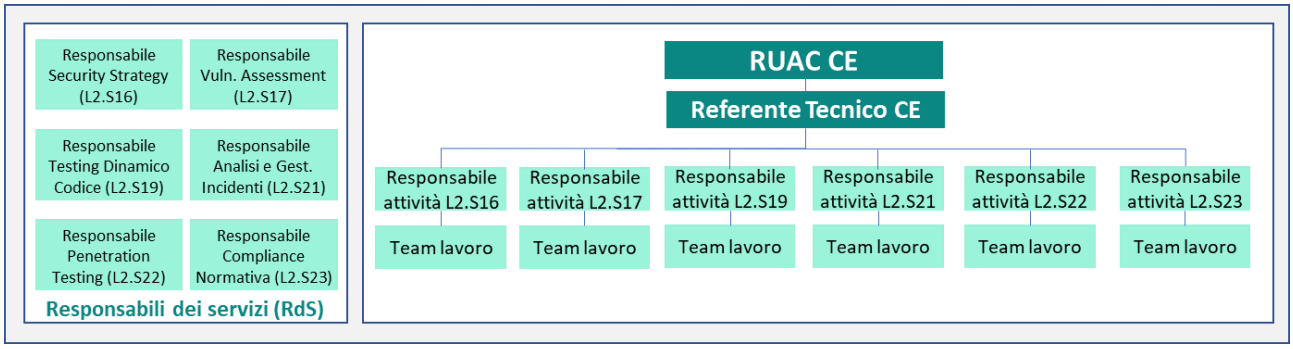
Il contratto esecutivo avrà i suoi effetti dalla data di stipula e avrà una durata di **48 mesi** dalla data di attivazione dei servizi, compatibilmente con il vincolo definito dall'Accordo quadro, ovvero che i Contratti Esecutivi abbiano una durata massima pari alla durata residua, al momento della sua stipula, dell'Accordo Quadro.

7 Piano della qualità specifico

7.1 Organizzazione dei Servizi

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

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



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

7.1.1 Security Strategy (L2.S16)

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

Profilo	Responsabilità
Security Principal	Project Manager, ha lo scopo di definire e gestire il progetto dal concepimento iniziale alla consegna finale. Responsabile dell'ottenimento di risultati ottimali, conformi agli standard di qualità, sicurezza e sostenibilità nonché coerenti con gli obiettivi, le performance, i costi ed i tempi definiti.
Security Solution Architect	Figura professionale dedicata al mantenimento della sicurezza del sistema informatico di un'organizzazione. Sarà responsabile dell'analisi dell'infrastruttura IT e delle relazioni tra i differenti sistemi e componenti infrastrutturali volta all'individuazione di problematiche architetturali che ne potrebbero compromettere la sicurezza.

	Si occuperà, inoltre, dell'analisi delle configurazioni e delle regole tecniche delle principali soluzioni di sicurezza utilizzate per proteggere l'infrastruttura e i servizi (Firewall, IPS/IDS, SIEM, soluzioni anti-malware, Web Application Firewall, Database Monitoring, servizi Anti-DDoS, servizi cloud oriented per la sicurezza).
Senior Information Security Consultant	Presidia l'attuazione della strategia definita all'interno del suo ambito di responsabilità (sia questo un progetto, un processo, una location) coordinando attivamente le eventuali figure operative a lui assegnate per tale scopo, rappresentando il naturale raccordo tra la struttura di governance della cyber security e il resto del personale operativo. Controlla il rispetto alle regole definite e del cogente in materia di sicurezza delle informazioni. Pianifica ed attua misure di sicurezza per proteggere le reti e i sistemi informatici di un'organizzazione.
Senior Security Auditor	Garantisce la conformità con le procedure di controllo interno stabilite esaminando i registri, i rapporti, le pratiche operative e la documentazione. Completa i giornali di audit documentando test e risultati dell'audit. Individua i possibili punti vulnerabili di un sistema informativo.
Data Protection Specialist	Esperto nella protezione dei dati personali e dotato di competenze giuridiche e informatiche specifiche, verifica il rispetto di quanto previsto nelle normative italiane ed europee in termini di protezione dei dati nonché delle politiche applicate dal titolare del trattamento o dal responsabile del trattamento in materia di protezione dei dati personali

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

7.1.2 Vulnerability Assessment (L2.S17)

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

Profilo	Responsabilità
Security Principal	Project Manager, ha lo scopo di definire e gestire il progetto dal concepimento iniziale alla consegna finale. Responsabile dell'ottenimento di risultati ottimali, conformi agli standard di qualità, sicurezza e sostenibilità nonché coerenti con gli obiettivi, le performance, i costi ed i tempi definiti.
Senior Penetration tester	Definito anche ethical hacker, tenta di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza rispettando opportune regole concordate in fase di ingaggio. Responsabile del coordinamento delle figure più Junior.
Junior Penetration tester	Definito anche ethical hacker, tenta di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza rispettando opportune regole concordate in fase di ingaggio

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

7.1.3 Testing Dinamico del Codice (L2.S19)

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

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

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

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

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

Profilo	Responsabilità
Security Principal	Project Manager, ha lo scopo di definire e gestire il progetto dal concepimento iniziale alla consegna finale. Responsabile dell'ottenimento di risultati ottimali, conformi agli standard di qualità, sicurezza e sostenibilità nonché coerenti con gli obiettivi, le performance, i costi ed i tempi definiti.
Senior Security Analyst	Gestisce l'esame periodico della sicurezza di sistemi, reti e applicazioni evidenziando le vulnerabilità tecniche nonché gli eventuali scostamenti rilevati rispetto e regole interne, normative esterne e best practices internazionali in materia Responsabile del coordinamento delle figure più Junior.
Junior Security Analyst	Gestisce l'esame periodico della sicurezza di sistemi, reti e applicazioni evidenziando le vulnerabilità tecniche nonché gli eventuali scostamenti rilevati rispetto e regole interne, normative esterne e best practices internazionali in materia.
Forensic Expert	E' chiamato a gestire la raccolta di evidenze e l'analisi delle stesse in concomitanza di un incidente relativo alla sicurezza delle informazioni documentando il tutto in modo che sia correttamente presentabile in sede processuale.

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

7.1.5 Penetration Testing (L2.S22)

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

Profilo	Responsabilità
Security Principal	Project Manager, ha lo scopo di definire e gestire il progetto dal concepimento iniziale alla consegna finale. Responsabile dell'ottenimento di risultati ottimali, conformi agli standard di qualità, sicurezza e sostenibilità nonché coerenti con gli obiettivi, le performance, i costi ed i tempi definiti.

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

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

7.1.6 Compliance Normativa (L2.S23)

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

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

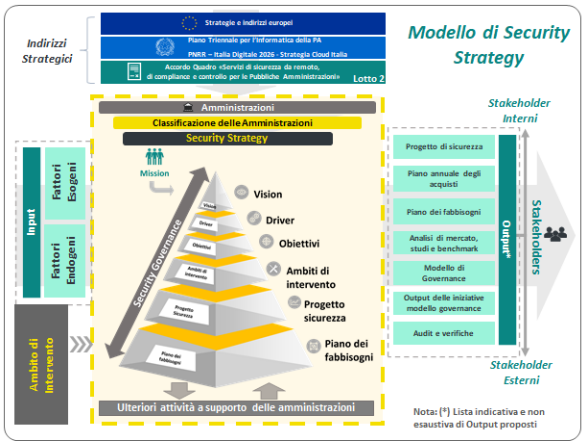
	previsto nelle normative italiane ed europee in termini di protezione dei dati nonché delle politiche applicate dal titolare del trattamento o dal responsabile del trattamento in materia di protezione dei dati personali

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

7.2 Metodologie e Tecniche

7.2.1 Security Strategy (L2.S16)

La strategia di sicurezza è l'abilitatore fondamentale che consente di individuare le azioni più appropriate per gestire i rischi di sicurezza in coerenza con le specificità delle Amministrazioni individuando le modalità con cui raggiungere i livelli di sicurezza richiesti e al contempo assicurare la conformità alle normative vigenti ed alle direttive di settore.
L'approccio concreto di elaborazione del Progetto di Sicurezza (di seguito PdS) avviene tramite modelli di PdS differenziati sulla base della classificazione e della complessità delle Amministrazioni (MappaPA).
Allo scopo di supportare le Amministrazioni nella pianificazione strategica della Sicurezza ICT, il RTI prevede l'utilizzo di uno specifico Modello di Security Strategy, sviluppato sulla base di standard e leading practices riconosciute in ambito Security ICT (es. ISO27001-2, ISO27017-8, ISO27701 ISO31000, ISA62443, NIST800.53 v5, Framework Nazionale, Linee guida ENISA).
Tramite tale modello l'Amministrazione sarà in grado di recepire gli indirizzi strategici (a livello nazionale ed europeo) e gli input esogeni ed endogeni, per definire - attraverso l'ausilio di metodologie, approcci operativi e strumenti - il PdS. Il PdS, coerentemente con il contesto di riferimento e con le esigenze di stakeholder interni ed esterni, avrà lo scopo di attuare la Missione e la derivata Visione dell'Amministrazione (i.e. la trasposizione della Missione in una strategia a lungo termine di evoluzione tecnologica e/o organizzativa mirata al suo soddisfacimento). Con riferimento agli ambiti del PdS, allo scopo di articolare una risposta completa rispetto a tutte le fasi del ciclo di vita della sicurezza delle informazioni e dei sistemi ICT, il RTI propone di considerare, a titolo indicativo e non esaustivo, i seguenti Ambiti di intervento:



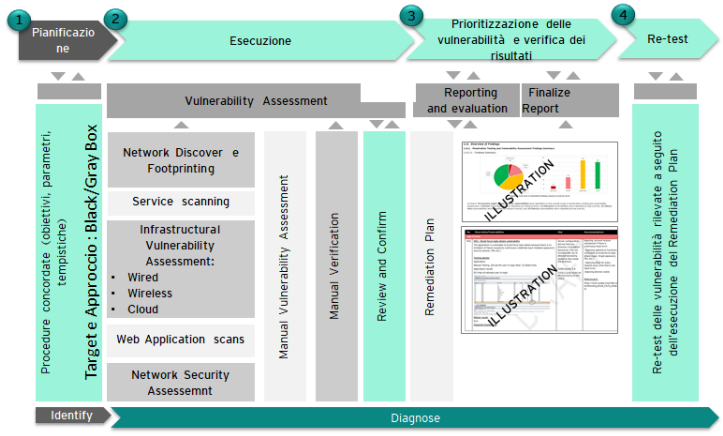
- Identify: strategia e pianificazione, Governance Asset e Processi, gestione del rischio cyber, security assurance (VA, PT, Testing del Codice), sicurezza terze parti e contratti di servizio, Compliance normativa;
- Protect (Management): Information & Data Security, Identity & Access Management, Security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

7.2.2 Vulnerability Assessment (L2.S17)

Il servizio di Vulnerability Assessment prevede l'identificazione in maniera proattiva, mediante una verifica dinamica della sicurezza, delle vulnerabilità presenti su dispositivi di rete, software e applicazioni delle Amministrazioni e la mitigazione dei rischi cyber connessi. Il RTI si impegna ad erogare le attività in ambito al presente servizio nel rispetto dei requisiti tecnico-funzionali specificati nel CTS, facendo affidamento sugli elementi distintivi sotto riportati.

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

Le attività di Vulnerability Assessment (VA) forniranno evidenze di dettaglio sulle vulnerabilità riconducibili all'infrastruttura ICT e IoT/OT (, funzionali anche ad elaborare una baseline iniziale del livello di vulnerabilità e di esposizione del sistema informativo dell'Amministrazione. L'attività sarà svolta sia con strumenti automatici sia con strumenti definiti ad-hoc sulla base della tipologia del target oggetto di analisi. Il RTI, sulla base della propria esperienza e del contesto di riferimento in cui saranno svolte le analisi di sicurezza, proporrà gli strumenti di analisi più adatti per l'esecuzione dei VA. Le attività di VA eseguite sono basate sulle metodologie OSSTMM, OWASP, PTES, NIST 800-52/53 e ISA 62443, riconosciute globalmente come standard de-facto. L'applicazione di tali metodologie garantirà risultati coerenti, ripetibili e misurabili. Nell'ambito delle attività di VA terremo in considerazione il sempre più diffuso utilizzo delle tecnologie Cloud da parte delle Amministrazione, in coerenza con quanto definito dalla Strategia Cloud Italia. A tal fine, su specifica richiesta dell'Amministrazione, il RTI è in grado di integrare all'interno dei servizi offerti anche l'esecuzione di attività di Assessment del livello di sicurezza dei servizi Cloud IaaS e SaaS, verificandone la compliance rispetto a standard, requisiti normativi e best practice di settore, e ricercando vulnerabilità celate negli errori di configurazione dei diversi ambienti cloud. Il RTI potrà eseguire le attività di VA in maniera periodica ove richiesto e ritenuto opportuno.



Per l'esecuzione dei servizi richiesti dall'Amministrazione, la metodologia prevede l'esecuzione di 4 fasi progettuali:

- Pianificazione delle attività,
- Esecuzione dei Vulnerability Assessment,

- Proritizzazione delle vulnerabilità e verifica dei risultati,
- Re-test delle vulnerabilità a seguito del remediation plan.

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

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

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

7.2.3 Testing Dinamico del Codice (L2.S19)

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

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

La metodologia utilizzata per l'esecuzione delle attività richieste prevede la combinazione di strumenti automatici e verifiche manuali ed ha come obiettivo l'identificazione di vulnerabilità nel codice sorgente delle applicazioni analizzate. La modalità di esecuzione è concepita per garantire risultati consistenti rispetto ad

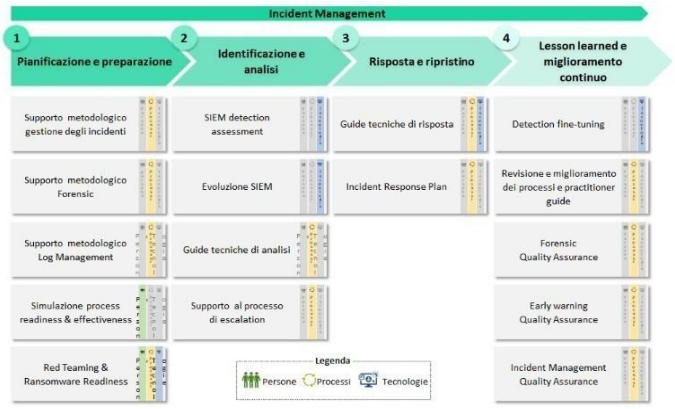
esecuzioni multiple successive sullo stesso applicativo, fornendo dettagli specifici sulle vulnerabilità fino alla specifica sezione/linea di codice. Tale modalità rende il servizio efficace anche su analisi incrementali, adattandosi anche a contesti di sviluppo agile in cui si intende reiterare le analisi. Coerentemente, il servizio di testing del codice prevede sempre una fase iniziale di ispezione ed una seconda fase che ha l'obiettivo di verificare che le azioni di rimedio siano state implementate e risolutive. Le attività di Testing del Codice saranno eseguite mediante strumenti software open source, proprietari e/o di mercato, messi a disposizione dal RTI.

L'analisi dinamica del codice (DAST) mira ad identificare le vulnerabilità delle applicazioni in runtime. Le attività sono eseguite sulla base dei principali standard OWASP Top 10 e OSSTMM, in modalità black-box e secondo tre macro-fasi tenendo conto del profilo dell'applicazione concordato (Bronze, Silver, Gold):

- FASE 1 - Analisi del contesto: raccolta delle informazioni necessarie all'esecuzione dell'attività (e.g. nome applicazione, URLs)
- FASE 2 – Dynamic Security Testing: esecuzione dell'analisi dinamica del codice sorgente dell'applicazione, ovvero:
  - Configurazione dei tool di analisi necessari per l'esecuzione delle attività sulla base delle caratteristiche dell'applicazione in scope
  - Vulnerability Scan dell'applicazione tramite strumenti open-source, proprietari e di mercato (ove necessario e su base periodica). Gli strumenti, opportunamente configurati sulla base delle leading practice e delle policy di sicurezza dell'Amministrazione, forniranno una valutazione automatica, in termini di severità/priorità, della vulnerabilità. Gli strumenti messi a disposizione garantiranno la copertura di più di 20 linguaggi e copriranno le vulnerabilità attualmente conosciute;
  - Esecuzione di un'analisi di dettaglio delle evidenze fornite dai tool di scansione per la rilevazione ed eliminazione dei falsi positivi ed esecuzione di un'analisi tecnica manuale per le funzionalità critiche; saranno eseguite verifiche di sicurezza specifiche sulla base del profilo assegnato all'applicazione in scope (Bronze, Silver, Gold). Nello specifico, a titolo non esaustivo, saranno eseguiti test di autenticazione (inclusi multilivello), autorizzazione, gestione della sessione, validazione degli input e manipolazione della logica applicativa, verifica dei messaggi di errore, protocolli utilizzati per le comunicazioni, meccanismi di logging e verifiche di compliance PCI-DSS;
  - PoC Development (profilo Gold): se richiesto e necessario, verranno dimostrate le limitazioni di sicurezza e le vulnerabilità identificate attraverso lo sviluppo di "Proof of Concept" in grado di far comprendere le modalità di realizzazione di uno scenario d'attacco da parte di un agente di minaccia specifico;
  - Correlazione delle informazioni, identificazione azioni di rimedio, prioritizzazione e definizione del remediation plan
- FASE 3 – Reporting: predisposizione di report e dashboard con l'obiettivo di fornire una chiara visione sui risultati DAST e focalizzare l'attenzione sulla prioritizzazione delle vulnerabilità tecniche rilevate. Nello specifico sarà predisposto un Executive Summary e un Technical Report per singola esecuzione, evidenziando in maniera puntuale anche le aree di miglioramento.

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

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



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

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

A) Incident Management

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

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

- Supporto metodologico gestione degli incidenti: sviluppo e/o revisione di modelli operativi e processi strutturati di Incident Management;
- Supporto metodologico Forensic: sviluppo e/o revisione di processi strutturati di analisi forense volti a guidare gli specialisti nelle relative attività;
- Supporto metodologico Log Management: sviluppo e/o revisione di una policy strutturata di Log Management al fine di standardizzare la raccolta e centralizzazione dei log da parte dell'amministrazione, definendo un livello standard di logging per ciascuna fonte, al fine di supportare le attività di analisi degli eventi;

● Simulazione Process readiness & effectiveness: svolgimento di simulazioni interattive di attacchi cyber realistici basati sugli scenari di minaccia più frequenti al fine di verificare la conoscenza del processo in ambito e la capacità degli attori coinvolti di gestire tali eventi.

● Red Teaming & Ransomware Readiness: svolgimento, in sinergia con il servizio di "Penetration Testing", di attività di Red Teaming e Ransomware Readiness al fine di testare, rispettivamente, l'efficacia dei processi di rilevazione e risposta alle minacce cyber e il livello di resilienza dell'Amministrazione nei confronti delle minacce di tipo ransomware identificando eventuali gap di sicurezza, incrementando la postura di sicurezza complessiva e le capacità di risposta a tali incidenti.

A.2 Identificazione e analisi: la fase di identificazione e analisi di un incidente ha l'obiettivo di monitorare in modo centralizzato gli eventi di sicurezza provenienti da fonti strutturate (es. SIEM) e non strutturate (es. e-mail da utenti) per rilevare minacce miranti agli asset e ai servizi della PA, analizzarli per comprendere se si tratti di un falso positivo che necessita di azioni correttive o di un incidente con potenziale impatto sul perimetro e classificare e prioritizzarne la gestione sulla base di criteri definiti.

● SIEM detection assessment: valutazione delle capacità di rilevazione delle minacce sulla base della visibilità offerta da regole e Use Case di monitoraggio implementati e relative sorgenti, sulla base di framework di settore (es. MITRE ATT&CK), in presenza di una piattaforma SIEM già esistente o nel caso di attivazione di un servizio SOC esterno;

● Evoluzione SIEM: definizione di Use Case di monitoraggio volti a incrementare la capacità di rilevazione di potenziali incidenti, sulla base dei risultati dell'assessment di cui al punto precedente e di una vasta libreria di Use Case;

● Guide tecniche di analisi: sviluppo e/o revisione di guide step-by-step (practitioner guide) che orientino le attività di analisi dei log e degli eventi a valle dell'identificazione di un potenziale incidente di sicurezza e di ricerca proattiva delle minacce (Threat Hunting).

● Supporto al processo di escalation: supporto all'Amministrazione nel coordinamento della comunicazione e dell'invio di notifiche/aggiornamenti circa incidenti verso le autorità competenti (es. Organi di Polizia) laddove necessario, ivi incluse la segnalazione di potenziali data breach, in ottemperanza a quanto previsto dalla normativa GDPR, e la notifica degli incidenti aventi un impatto rilevante sui servizi essenziali e digitali verso il CSIRT-Italia, nelle modalità previste dal D.lgs 65/2018 (attuazione Direttiva NIS) e dal decreto n. 81/2021.

A.3 Risposta e ripristino: tale fase prevede l'identificazione e l'implementazione delle azioni di contenimento a breve termine dell'incidente, con l'obiettivo di limitare le conseguenze dell'incidente e ripristinare la normale operatività in maniera tempestiva ed efficace.

● Supporto specialistico nell'elaborazione e nel coordinamento dell'implementazione di una strategia di risposta e ripristino per la corretta gestione degli incidenti.

A.4 Lesson learned e miglioramento continuo: tale fase prevede, immediatamente a valle della gestione di un incidente, una valutazione ex-post della stessa per verificare che le attività siano state condotte in conformità con quanto previsto dal processo, e un'attività periodica volta a identificare eventuali punti di miglioramento nelle attività svolte attraverso l'elaborazione di reportistica, lo svolgimento di meeting ricorrenti per condividere eventuali gap e relative azioni di rimedio.

B) Forensic

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

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

● Definizione di un template di catena di custodia per supportare i team di Forensic nel tracciamento delle attività eseguite sulle evidenze acquisite;

● Definizione di un processo di Forensic secondo best practice volto a definire ruoli, responsabilità, principi e attività operative che regolano il processo stesso;

● Governo (organizzazione, pianificazione, coordinamento, controllo) delle attività di verifica tecnica (quality assurance) del processo di Forensic.

Il processo di Forensic, in via generale, può astrattamente essere declinato nei seguenti step, per ciascuno dei quali sono riportate le attività principali il cui corretto svolgimento verrà verificato e valutato dal RTI, sulla base del processo definito:

▪ Assessment iniziale, rilevazione preliminare del contesto specifico, necessaria a identificare la strategia di intervento più idonea ed efficiente in base alla tipologia di incidente rilevato.;

▪ Data collection acquisizioni di evidenze informatiche ("ESI"), svolte preservando l'integrità delle fonti dati originali e garantendo allo stesso tempo la validità probatoria dei dati acquisiti (copie forensi) attraverso l'uso di procedure e strumenti certificati secondo le best practice internazionali di Forensic.

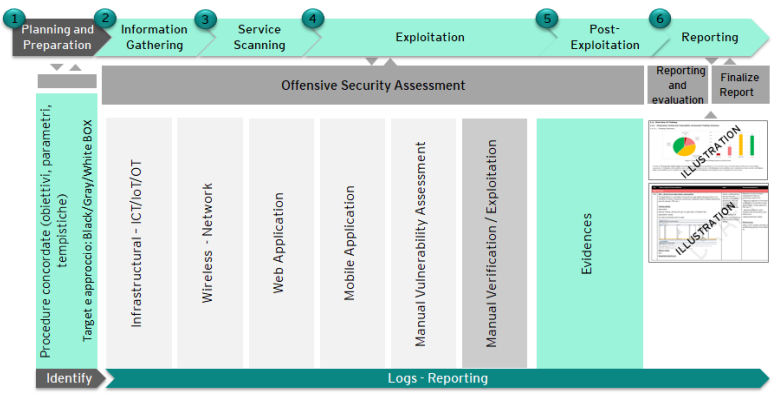
▪ Investigazione, svolgimento di analisi tecniche sulle evidenze informatiche acquisite, diversificate in base alla peculiarità del caso di specie. Diverse in considerazione della varietà delle tipologie di incidenti di sicurezza, oltre che della specificità dei sistemi coinvolti.

7.2.5 Penetration Testing (L2.S22)

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

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

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



3. Utilizzo estensivo di fonti Cyber Threat Intelligence (OSINT e CLOSINT) con copertura geografica mondiale, derivante dai servizi di sicurezza gestista (SOC) del RTI, che consentono al Pen Tester di ottenere un quadro più ampio dell'effettivo livello di esposizione dei target in analisi, come ad esempio compromissioni/vulnerabilità/tecniche pubblicate nel dark web o in community specifiche, potenzialmente accessibili anche agli attaccanti e sfruttabili per realizzare una reale compromissione,;

4. Molteplicità di laboratori a livello nazionale ed internazionale con personale, strumenti ed infrastrutture dedicate alle attività di offensive security, con possibilità di verificare costantemente i vettori e le tecniche di attacco in ambienti simulati e su dispositivi di test; tali laboratori sono impiegati anche per addestramento, formazione ed aggiornamento continuo dei Pen Tester.

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

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

7.2.6 Compliance Normativa (L2.S23)

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

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

Il Sistema di gestione della Privacy ha necessità di essere disegnato, analizzato, implementato, monitorato e continuamente migliorato in un'ottica anche di lungo periodo, al fine di trasformare la privacy in un fattore abilitante per il trattamento dei dati da parte dell'Amministrazione e garantire agli interessati la protezione dei dati personali. A tale scopo, il RTI utilizzerà, per guidare lo svolgimento delle attività, il GDPR Compliance Framework (GDPR CF). Tale strumento propone una metodologia per la definizione e mantenimento del sistema privacy ed è caratterizzato da un ciclo di 4 fasi: a) Analisi; b) Implementazione; c) Verifica; d) Continuous Improvement. Quest'ultima fase è abilitata dal Privacy Maturity Model (PMM), ovvero uno strumento in grado di intercettare nel continuo, i punti di forza e di miglioramento del Sistema di gestione della privacy esprimendo lo stato di maturità e identificando in modo dinamico le aree di intervento. L'utilizzo del GDPR CF, oltre a mettere a disposizione un set esaustivo di strumenti automatici, potrà, essere supportato da un prodotto software integrato che consente di gestire il Sistema Privacy in modalità condivisa e collaborativa tra tutti i soggetti interessati (es. DPO, Privacy Officer, IT, Sicurezza, Risorse Umane, Acquisti).
Analisi: la fase di analisi prevede lo svolgimento di un assessment per verificare lo stato di conformità alla normativa applicabile da parte delle Amministrazioni al fine di comprendere le aree maggiormente a rischio e identificare gli eventuali interventi di rimedio necessari per garantire conformità e allo stesso tempo automatizzare i processi privacy.
Implementazione: tale fase consentirà di indirizzare le azioni di rimedio emerse a seguito dell'Assessment ed incluse nel Piano degli interventi o già previste dai piani di conformità dell'Amministrazione. Allo scopo di

massimizzare l'efficacia degli interventi e la logica del riuso, le attività di implementazione sono eseguite secondo un modello operativo che prevede la messa a disposizione di template consolidati per le componenti del framework documentale (es. politiche, procedure, metodologie, nomine a responsabile, informative, data processing agreement, materiale formativo) che saranno condivisi con l'Amministrazione e personalizzati sulla base delle specifiche necessità

Verifica: tale fase consente di misurare l'effettiva implementazione dei requisiti normativi a cui è soggetta l'Amministrazione, valutare il rischio derivante dai gap ed il livello di maturità raggiunto, proponendo eventuali punti di miglioramento, attraverso piani di azione costantemente monitorati.

Continuous Improvement: al fine di trasformare la privacy da adempimento di legge ad abilitatore "mandatorio" e cogliere tempestivamente i rischi normativi/sanzionatori/IT, si prevede l'adozione del PMM (o in alternativa il Data Protection Maturity Self-Assessment Model rilasciato dal CNIL).