



A.S.L. V.C.O.

Azienda Sanitaria Locale
del Verbano Cusio Ossola

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

DELIBERAZIONE DEL DIRETTORE GENERALE

N. 650 del 09/08/2023

**Oggetto: REVOCA DELIBERAZIONE N. 638 DEL 2 AGOSTO 2023 ED APPROVAZIONE DEL PROGETTO DEI FABBISOGNI DELL'AIC N. 3 – ASL VCO E ADESIONE AL CONTRATTO DI UTENZA CON LA SOCIETÀ POLO STRATEGICO NAZIONALE S.P.A. (PSN), NELL'AMBITO DELLA CONVENZIONE SOTTOSCRITTA TRA IL DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE DELLA PRESIDENZA DEL CONSIGLIO DEI MINISTRI (DTD) E LA SOCIETÀ POLO STRATEGICO NAZIONALE S.P.A. (PSN), PER LA REALIZZAZIONE E GESTIONE DI UNA NUOVA INFRASTRUTTURA INFORMATICA AL SERVIZIO DELLA PUBBLICA AMMINISTRAZIONE - SISTEMA GESTIONALE DI LABORATORIO ANALISI E MICROBIOLOGIA OCCORRENTE ALLE AZIENDE AFFERENTI ALL'AIC N. 3
CUP J51B21005710007
CIG 9066973ECE**

DIRETTORE GENERALE - DOTT.SSA CHIARA SERPIERI
(NOMINATO CON DGR N.11-3293 DEL 28/05/2021)

DIRETTORE AMMINISTRATIVO - AVV. CINZIA MELODA



A.S.L. V.C.O.

*Azienda Sanitaria Locale
del Verbano Cusio Ossola*

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

DELIBERAZIONE DEL DIRETTORE GENERALE

L'estensore dell'atto: Coster Comi Silvia

Il Responsabile del procedimento: Femia Benedetto

Il Responsabile Servizio Economico Finanziario: Succi Manuela

Il funzionario incaricato alla pubblicazione.



A.S.L. V.C.O.

Azienda Sanitaria Locale
del Verbano Cusio Ossola

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

IL DIRETTORE GENERALE

Nella data sopraindicata, su proposta istruttoria del Responsabile SOS Tecnologia dell'Informazione e della Comunicazione (ICT) di seguito riportata, in conformità al Regolamento approvato con delibera n. 290 del 12/05/2017 e modificato con delibera n. 65 del 28/01/2020,

PREMESSO CHE:

la deliberazione n. 638 del 2 agosto 2023, di pari oggetto e contenuto rispetto alla presente, deve essere revocata in autotutela in quanto, in due degli allegati parte integrante della medesima, comparivano informazioni delicate dal punto di vista della sicurezza informatica e che, pertanto, si è provveduto a bloccare l'iter di pubblicazione di tale atto all'albo ufficiale online;

con deliberazione della Giunta Regionale n. 43-6861 del 09/12/2013, sono state individuate, in attuazione dell'art. 1, comma 3, della Legge Regionale n. 20 del 13/11/2013, le Aree Interaziendali di Coordinamento, tra le quali l'AIC 3, alla quale afferiscono l'A.S.L. BI, l'A.S.L. NO, l'A.S.L. VC, l'A.S.L. VCO e l'A.O.U. Maggiore della Carità di Novara;

con deliberazione della Giunta Regionale n. 34-189 del 28/07/2014, considerata l'esigenza di aggregare la programmazione degli acquisti nell'ambito dell'area interaziendale, ai sensi dell'art. 1, comma 2, della citata L.R. n. 20/2013, sono state individuate le Aziende Sanitarie capofila del coordinamento degli acquisti per ognuna delle AIC e, in particolare, per l'AIC 3, l'A.O.U. Maggiore della Carità di Novara;

con D.G.R. n. 50 del 23/11/2015 e n. 20 del 20/04/2018, la Giunta Regionale Piemontese ha approvato la riorganizzazione della rete dei laboratori che prevede il consolidamento delle analisi dei laboratori di analisi e microbiologia;

al fine di raggiungere gli obiettivi indicati e dall'esperienza maturata durante l'attività di concentrazione delle analisi specialistiche di laboratorio tra gli ospedali dell'AIC3, si rende necessaria la realizzazione di una piattaforma informatica unitaria per risolvere in maniera completa e mirata tutte le problematiche emerse;

la citata piattaforma informatica unitaria dovrà essere ospitata in una infrastruttura server qualificata, conforme ai requisiti di sicurezza, garantire capacità elaborativa, affidabilità necessarie e sufficienti all'erogazione del servizio di laboratorio;

RICHIAMATI:

- Le circolari AgID n.2 e n. 3 del 9 aprile 2018;
- Il Piano Triennale per l'informatica nella Pubblica Amministrazione di AgID (Aggiornamento 2022-2024);
- La Delibera 307/2022 dell'Agenzia per la Cybersicurezza Nazionale (ACN);
- La classificazione dei dati e dei servizi digitali registrata sulla Piattaforma PA Digitale



Il presente documento informatico è sottoscritto con firma digitale, creato e conservato digitalmente secondo la normativa vigente



A.S.L. V.C.O.

Azienda Sanitaria Locale
del Verbano Cusio Ossola

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

nella quale sono identificati nello specifico come "CRITICI" i servizi di Assistenza Ospedaliera Ricoveri, Assistenza Ospedaliera Day-Hospital, Assistenza Ospedaliera/Territoriale Specialistica Ambulatoriale, Assistenza Ospedaliera Riabilitativa, Assistenza Farmaceutica, Assistenza Ospedaliera Day-Surgery, Attività Trasfusionale, Attività Diagnostica Ospedaliera e Territoriale;

PRESO ATTO del Piano nazionale di ripresa e resilienza (PNRR), ufficialmente presentato alla Commissione Europea in data 30 aprile 2021 ai sensi dell'art. 18 del Regolamento (UE) n. 2021/241 e della decisione di esecuzione del Consiglio (UE) del 13 luglio 2021 relativa all'approvazione della valutazione del Piano di ripresa e resilienza per l'Italia;

CONSIDERATO che l'Investimento 1.1 "Infrastrutture digitali" della Missione 1 – Componente 1 del PNRR prevede espressamente che "La trasformazione digitale della PA segue un approccio "cloud first", orientato alla migrazione dei dati e degli applicativi informatici delle singole amministrazioni verso un ambiente cloud. ...";

PRESO ATTO della determinazione del Direttore Generale dell'Agenzia per l'Italia digitale (AgID) n. 628/2021 del 15 dicembre 2021, con la quale è stato adottato il regolamento di cui all'art. 33-septies, comma 4, del decreto-legge n. 179/2012, recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione, nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione, il quale ha il fine di:

- stabilire i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la pubblica amministrazione;
- definire le caratteristiche di qualità, di sicurezza, di performance e scalabilità, interoperabilità, portabilità dei servizi cloud per la pubblica amministrazione;
- individuare i termini e le modalità con cui le amministrazioni devono effettuare le migrazioni, anche stabilendo il processo e le modalità per la classificazione dei dati e dei servizi digitali delle pubbliche amministrazioni;
- individuare le modalità del procedimento di qualificazione dei servizi cloud per la pubblica amministrazione;

PRESA VISIONE dell'art. 10 del Regolamento, rubricato "Termini e modalità per la migrazione dei dati e dei servizi della pubblica amministrazione" e, in particolare, il comma 1, secondo cui "Le amministrazioni, all'esito del processo di conferimento dell'elenco e della classificazione dei dati e dei servizi digitali di cui all'articolo 5, predispongono il piano di migrazione dei loro dati e servizi digitali secondo il modello adottato dal DTD, d'intesa con l'ACN";

PRESO ATTO della determinazione del 7 ottobre 2022 della Presidenza del Consiglio dei Ministri, Dipartimento per la trasformazione digitale che, in conformità alle previsioni di cui all'articolo 10 comma 1 del Regolamento, ha definito il Modello di piano di migrazione, le



A.S.L. V.C.O.

Azienda Sanitaria Locale
del Verbano Cusio Ossola

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

regole per la corretta predisposizione del piano di migrazione da parte delle amministrazioni e la relativa modalità di trasmissione al DTD, ai fini della verifica di conformità di cui all'articolo 10 comma 5 del Regolamento;

PRESA VISIONE della Convenzione Nazionale tra il Dipartimento per la Trasformazione Digitale e il Polo Strategico Nazionale sottoscritta il 24 agosto 2022, nell'ambito del PNRR

(Missione 1, componente1, investimenti 1.1 Cloud PA/Polo Strategico Nazionale e 1.2 "Abilitazione e facilitazione migrazione al cloud"), che prevede a partire dal 22 dicembre 2022 la possibilità per le PP.AA. di sottoscrivere i contratti di adesione alla convenzione;

RICHIAMATA le deliberazioni n. 654 del 12/09/2022 "ADESIONE ACCORDO QUADRO CONSIP "SERVIZI APPLICATIVI IT2 – LOTTO 1" PER L'ACQUISIZIONE DI SERVIZI PER LA GESTIONE E LO SVILUPPO DEL SISTEMA GESTIONALE DI LABORATORIO ANALISI E MICROBIOLOGIA (LIS) OCCORRENTI ALLE AZIENDE AFFERENTI AD AIC 3 PER UN ARCO TEMPORALE DI MESI SESSANTA-CIG DERIVATO 93750632BB" e n. 870 del 09/12/2022 di rettifica e integrazione della precedente;

DATO ATTO che l'affidamento dei servizi per la gestione e lo sviluppo del sistema gestionale di laboratorio analisi e microbiologia rientra nell'ambito del "PNRR – MISSIONE 6 – COMPONENTE 2 – INVESTIMENTO 1.1.1 "AMMODERNAMENTO DEL PARCO TECNOLOGICO E DIGITALE OSPEDALIERO (DIGITALIZZAZIONE DELLE STRUTTURE OSPEDALIERE - DEA I E II)" di cui al CUP F96G22000400006;

CONSIDERATO che risulta necessario individuare l'infrastruttura *cloud* secondo le indicazioni normative per installare l'ambiente operativo del sistema GESTIONALE DI LABORATORIO ANALISI E MICROBIOLOGIA OCCORRENTE ALLE AZIENDE AFFERENTI ALL'AREA INTERAZIENDALE DI COORDINAMENTO N.3 di cui alle delibere n. 654 del 12/09/2022 e 870 del 09/12/2022, stante che il sistema di LABORATORIO ANALISI E MICROBIOLOGIA rientra tra i servizi individuati come Critici;

RICHIAMATA la DGR 15-6172 del 07/12/2023 che indirizza ad Azienda Zero il ruolo di coordinamento ai fini dell'aggiornamento e attuazione del Piano Triennale per l'Informatica nelle Aziende Sanitarie Regionali 2021-2023 e s.m.i. e per gli interventi di abilitazione e facilitazione migrazione al *cloud* per le PA locali;

CONSIDERATO che la Regione ha attribuito con la citata D.G.R. ad Azienda Zero funzioni di supporto alle ASR, nello specifico un "...ruolo di coordinamento verso le ASR, supportando le stesse nell'ambito degli eventuali adempimenti necessari per l'identificazione della soluzione, abilitazione e facilitazione migrazione al cloud";

DATO ATTO che, sulla base della disposizioni regionali sopra citate, le ASR dell'AIC3, al fine di identificare la soluzione più idonea ad ospitare l'infrastruttura *cloud* del progetto LIS (Laboratorio Analisi) per il quadrante nord-est, hanno avviato una serie di interlocuzioni e



A.S.L. V.C.O.

Azienda Sanitaria Locale
del Verbano Cusio Ossola

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

richieste di documentazione tecnica ed economica condivise con Azienda zero, coinvolgendo i *Cloud Service Provider* individuati dalla Regione come potenziali erogatori di servizi *cloud*, nello specifico PSN (Polo Strategico Nazionale) e CSI Piemonte;

PRESA VISIONE della nota 2023/1135 del 09/05/2023, Prot. AOU Novara 15432/2023, pervenuta da Azienda Zero Piemonte, quale risultanza di tale confronto tecnico comparativo a seguito degli incontri sopra citati, ad oggetto "Relazione comparativa servizi

PSN e CSI Piemonte – caso LIS - quadrante nord-est", dove si evidenzia che "A fronte di un costo maggiore PSN offre però livelli di servizio e di disponibilità, dichiarati, migliorativi rispetto a CSI unitamente ad una gestione del DR e tempi di RPO e RTO inferiori. Pertanto consigliamo di valutare questo fornitore";

RICHIAMATA la nota "Infrastruttura cloud per i progetto LIS – quadrante Nord est" prot. 16905/23 AOU Maggiore Novara del 19/05/2023, allegata parte integrante alla presente deliberazione, nella quale il gruppo di lavoro interaziendale comunicava alle Direzioni Generali dell'ASR dell'AIC3 gli esiti della valutazione comparata e la soluzione di *cloud* individuata;

CONSIDERATO che in relazione a quanto sopra indicato, le ASR dell'AIC3, AOU Maggiore della Carità di Novara, ASL Novara, ASL Biella, ASL VCO, ASL Vercelli hanno predisposto il "Piano dei Fabbisogni per il progetto GESTIONE E SVILUPPO DEL SISTEMA GESTIONALE DI LABORATORIO ANALISI E MICROBIOLOGIA", allegato parte integrante alla presente deliberazione e che per ragioni di sicurezza informatica viene pubblicato con ommissis, descrivendo le esigenze e i servizi che l'AIC n. 3 intende richiedere, e inviandolo al Polo Strategico Nazionale con PEC del 23/03/2023 (2023-0000001521330033-PdF-P1R1);

DATO ATTO che il Polo Strategico Nazionale ha predisposto il "Progetto dei Fabbisogni", anch'esso allegato parte integrante alla presente deliberazione e che per ragioni di sicurezza informatica viene pubblicato con ommissis, e che detto "Progetto dei Fabbisogni" contiene la proposta tecnico-economica relativa all'esigenza espressa dalle ASR dell'AIC3, sviluppata secondo le modalità tecniche e i listini previsti dalla Convenzione e dai relativi allegati, inviandolo tramite PEC all'ASL VCO in data 03/07/2023 prot. 42297;

PRESO ATTO della congruità del predetto Progetto dei Fabbisogni e ritenuto di approvarlo, nonché della necessità di procedere di conseguenza alla stipula del Contratto d'Utenza con il Polo Strategico Nazionale, di cui alla citata determinazione 7 ottobre 2022 della Presidenza del Consiglio dei Ministri, Dipartimento per la trasformazione digitale;

CONSIDERATO che, in considerazione della natura dei servizi oggetto della presente procedura, non sussiste, ai sensi dell'art. 26 del D. Lgs. 81/2008, l'obbligo di procedere alla predisposizione dei documenti di cui all'art. 26, comma 3 e 3 ter del predetto decreto;

DATO ATTO che l'aggiudicatario Polo Strategico Nazionale della citata procedura



A.S.L. V.C.O.

Azienda Sanitaria Locale
del Verbano Cusio Ossola

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

stipulerà, con ogni singola Azienda, il contratto relativo ai servizi di fornitura e gestione dell'infrastruttura *datacenter* in *cloud* a supporto della gestione e lo sviluppo del sistema gestionale di Laboratorio Analisi e Microbiologia delle Aziende facenti parte dell'AIC3;

Condivisa la proposta come sopra formulata e ritenendo sussistere le condizioni per l'assunzione della presente delibera;

Acquisiti i pareri favorevoli espressi ai sensi dell'art. 3 del d.Lgs. 502/1992 e smi, come formulati nel frontespizio del presente atto;

DELIBERA

1. Di revocare, per le motivazioni indicate in premessa e che qui si intendono integralmente richiamate, la deliberazione n. 638 del 2 agosto 2023.
2. Di approvare i richiami, le premesse e l'intera narrativa quali parti integranti e sostanziali del presente dispositivo, ivi inclusi i documenti allegati parte integrante, per due dei quali (il "Piano dei Fabbisogni" e il "Progetto del piano dei fabbisogni") si provvede alla pubblicazione con omissis per ragioni di sicurezza informatica.
3. Di approvare il Progetto dei Fabbisogni prot. 42297 del 03/07/2023, contenente la proposta tecnico-economica relativa all'esigenza espressa dall'AIC3 per il progetto "Sistema gestionale di laboratorio e microbiologia delle Aziende all'Area Interaziendale di Coordinamento N. 3, di cui l'ASL VCO è un componente.
4. Di stipulare contestualmente il Contratto di Utenza con la Società Polo Strategico Nazionale S.P.A. (PSN), nell'ambito della Convenzione sottoscritta tra il Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei Ministri (DTD) e la Società Polo Strategico Nazionale S.P.A. (PSN), per la realizzazione e gestione di una nuova infrastruttura informatica al servizio della pubblica amministrazione.
5. Di prendere atto che la data di decorrenza del contratto decorrerà presumibilmente dal 01/09/2023 e avrà durata di anni 10 (dieci), dunque fino al 31/08/2033.
6. Di dare atto, altresì, che la spesa complessiva prevista per lo svolgimento dell'attività sopra descritta è suddivisa tra le ASR dell'AIC3 secondo il seguente schema, che riporta la stessa ripartizione dei costi del progetto "Sistema gestionale di laboratorio e microbiologia delle Aziende all'Area Interaziendale di Coordinamento N. 3":

ASR	AOU NOVARA 24,5%	ASL NOVARA 19,5%	ASL BIELLA 19,25%	ASL VCO 18,00%	ASL VC 18,75%
SERVIZIO	Importo	Importo	Importo	Importo	Importo
UT Predisposizione	29.464,59 €	23.451,41 €	23.150,75 €	21.647,46 €	22.549,43 €

**A.S.L. V.C.O.**Azienda Sanitaria Locale
del Verbano Cusio OssolaSede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

Canone Sett/Dic 2023	71.878,67 €	57.209,55 €	56.476,10 €	52.808,82 €	55.009,19 €
Canone annuo 2024	219.884,99 €	175.010,50 €	172.766,77 €	161.548,15 €	168.279,33 €
Canoni annui 2025 - 2032	1.827.063,55 €	1.454.193,44 €	1.435.549,93 €	1.342.332,40 €	1.398.262,92 €
Canone Genn/Agosto 2033	152.255,30 €	121.182,79 €	119.629,16 €	111.861,03 €	116.521,91 €
Servizi professionali - fatturabili a consuntivo bimestrale	443.478,98 €	352.973,07 €	348.447,77 €	325.821,29 €	339.397,18 €
TOTALE Iva Esclusa	2.744.026,08	2.184.020,76	2.156.020,49	2.016.019,16	2.100.019,96

Tenendo altresì presente che, in tale tabella, il canone è elaborato considerando l'avvio al 01/09/2023 e che gli importi indicati sono IVA esclusa.

7. Di dare atto che, per quanto riguarda gli importi di spesa riportati del precedente punto, pari a complessivi 2.016.019,16 € IVA esclusa, i medesimi devono trovare copertura nell'ambito del competente conto così come di seguito meglio esplicitato:

Anno	Attività	Conto	Descrizione Conto	Importo	Importo
				IVA esclusa	IVA inclusa
2023	Una tantum - predisposizione	3.15.02.03	servizi IT cloud	21.647,47	26.409,91
2023	Canone Servizi per Cloud e Sicurezza (4 Mesi)	3.15.02.03	servizi IT cloud	52.808,83	64.426,77
2024	Servizi a canone per cloud e Sicurezza (12 mesi)	3.15.02.03	servizi IT cloud	161.548,16	197.088,76
2024	Servizi professionali - fatturabili a consuntivo bimestrale	3.15.02.03	servizi IT cloud	32.582,13	39.750,20
2025/ 2032	Servizi a canone per Cloud e Sicurezza (96 mesi)	3.15.02.03	servizi IT cloud	1.342.332,42	1.637.645,55
2025/ 2032	Servizi professionali - fatturabili a consuntivo bimestrale (96 mesi)	3.15.02.03	servizi IT cloud	260.656,97	318.001,50
2033	Servizi a canone per Cloud e Sicurezza (8 mesi)	3.15.02.03	servizi IT cloud	111.861,04	136.470,47



A.S.L. V.C.O.

Azienda Sanitaria Locale
del Verbano Cusio Ossola

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

2033	Servizi professionali - fatturabili a consuntivo bimestrale	3.15.02.03	servizi IT cloud	32.582,14	39.750,21
	TOTALE			2.016.019,16	2.459.543,38

8. Di stabilire che i servizi a consumo verranno utilizzati esclusivamente in funzione delle reali esigenze che si andranno a determinare e che, di conseguenza, le relative spese sono da considerarsi presunte.
9. Di trasmettere copia del presente provvedimento all'Azienda Zero e al PSN, per gli adempimenti di conseguenza;
10. Di nominare, ai sensi del Decreto n. 49 del 7 marzo 2018 del Ministero delle infrastrutture e dei trasporti, avente ad oggetto "Regolamento delle funzioni del direttore dei lavori e del direttore dell'esecuzione", quale Direttore di Esecuzione del Contratto, l'ing. Davide Angeloni, con i compiti di provvedere al coordinamento, alla direzione ed al controllo tecnico-contabile dell'esecuzione del contratto e di assicurare la regolare esecuzione dello stesso da parte del Fornitore, verificando che le attività e le prestazioni contrattuali siano eseguite in conformità ai documenti contrattuali;
11. Di dare atto che la spesa derivante dall'adozione del presente provvedimento, relativa alla durata contrattuale e pari a € 2.459.543,38 IVA inclusa, sarà a carico dei seguenti esercizi finanziari e alla medesima si farà fronte sui budget iscritti ai sotto-evidenziati conti, come di seguito meglio esplicitato:

<i>Esercizio</i>	<i>Centro Ordinatore di spesa</i>	<i>Conto</i>	<i>AUT budget</i>	<i>Sub-budget</i>	<i>Importo</i>
2023	31-ICT	3.15.02.03	11	10	90.836,68 €
2024	31-ICT	3.15.02.03	11	10	236.838,96 €
2025	31-ICT	3.15.02.03	11	10	244.455,88 €
2026	31-ICT	3.15.02.03	11	10	244.455,88 €
2027	31-ICT	3.15.02.03	11	10	244.455,88 €
2028	31-ICT	3.15.02.03	11	10	244.455,88 €
2029	31-ICT	3.15.02.03	11	10	244.455,88 €
2030	31-ICT	3.15.02.03	11	10	244.455,88 €
2031	31-ICT	3.15.02.03	11	10	244.455,88 €
2032	31-ICT	3.15.02.03	11	10	244.455,88 €
2033	31-ICT	3.15.02.03	11	10	176.220,68 €



A.S.L. V.C.O.

*Azienda Sanitaria Locale
del Verbano Cusio Ossola*

Sede legale : Via Mazzini, 117 - 28887 Omegna (VB)
Tel. +39 0323.5411 0324.4911 fax +39 0323.643020
e-mail: protocollo@pec.aslvco.it - www.aslvco.it

P.I./Cod.Fisc. 00634880033

12. Di dare mandato alla SOC Affari Generali Legali e Istituzionali di trasmettere copia del presente atto al Collegio Sindacale ai sensi dell'art. 14 L.R. 10/1995.



S.C. Sistemi Informativi

Tel.: 0321 373.2012

E-mail: segreteria.si@maggioreosp.novara.it

Dott. Gianfranco Zulian
Direttore Generale Azienda Ospedaliera
"Maggiore della Carità" di Novara

Dott. Angelo Penna
Direttore generale ASL Novara

Dott.sa Eva Colombo
Direttore Generale ASL Vercelli

Dott.sa Chiara Serpieri
Direttore Generale ASL VCO

Dott. Mario Sanò
Direttore Generale ASL Biella

p.c. Al Direttore ff della SC Sistema Informativo
Azienda Zero
Ing. Salvatore Scaramuzzino

Dott. Antonino Ruggeri – Regione Piemonte
Direzione Sanità e Welfare - Controllo di
gestione, sistemi informativi, logistica sanitaria
e coordinamento acquisti

Oggetto: infrastruttura cloud - Progetto LIS per il quadrante Nord Est.

Con Delibera DG AOU Novara - n. 411 del 24/05/2022 Accordo Quadro CONSIP "Servizi Applicativi IT2 – LOTTO 1- " è stato definito il progetto per l'acquisizione di servizi per la gestione e lo sviluppo del sistema gestionale di Laboratorio Analisi e microbiologia occorrente alle aziende afferenti all'AIC N°3". Il progetto LIS per l'AIC3 prevede la fornitura di una soluzione della società Dedalus, condivisa per le ASR del quadrante nord-est, da installare in ambiente cloud.

Regione ha attribuito ad Azienda Zero funzioni di supporto alle ASR con D.G.R. n. 15 – 6172 del 7/12/2022, nello specifico un " ...ruolo di coordinamento verso le ASR, supportando le stesse nell'ambito degli eventuali adempimenti necessari per l'identificazione della soluzione, abilitazione e facilitazione migrazione al cloud".

Pertanto al fine di identificare la soluzione più idonea ad ospitare l'infrastruttura cloud del progetto LIS (Laboratorio Analisi) per il quadrante nord-est, le ASR hanno avviato una serie di interlocuzioni e richieste di



documentazione tecnica ed economica condivise con Azienda zero, coinvolgendo i Cloud service provider individuati dalla Regione come potenziali erogatori di servizi Cloud, nello specifico PSN (Polo Strategico Nazionale) e CSI Piemonte.

La risultanza di tale confronto tecnico comparativo è stata trasmessa da Azienda zero alle ASR dell'AIC 3, con suo protocollo N. 2023/0001135 del 09/05/2023.

Nel prendere atto della relazione tecnica comparativa predisposta da Azienda Zero, che si allega come parte integrante della presente nota, si evidenziano gli aspetti più significativi della relazione che hanno condotto all'individuazione del CSP più adatto per il progetto di LIS sovraziendale.

La criticità del sistema informatico di Laboratorio per le 5 ASR è elevata per l'importanza clinica, in alcuni casi vitale, delle analisi diagnostiche di laboratorio rispetto a tutta la catena di cura dei pazienti sia ricoverati che ambulatoriali e quindi per l'alto numero di soggetti coinvolti in un eventuale indisponibilità, anche temporanea del servizio, oltre che per le ricadute dirette sulle condizioni cliniche dei pazienti. E' quindi essenziale individuare la soluzione che dia le massime garanzie di sicurezza e continuità del servizio informatico in modo automatico, e per tutta la durata del contratto del LIS (60 mesi). In tal senso la soluzione tecnica proposta da PSN, come si evince dalla relazione comparativa allegata, fornisce maggiori garanzie riguardo:

- Disponibilità infrastruttura (tempo garantito di uptime)
- Livelli di servizio
- Tempi di RTO (tempo massimo previsto per il ripristino di un servizio/sistema per renderlo nuovamente disponibile all'utente finale) e RPO (intervallo di tempo per la quale si tollera una perdita di dati)
- Modalità di ripartenza automatica
- Tempi certi di rilascio dei servizi
- Costo comprensivo di tutte le componenti, comprese quelle relative alla business continuity/disaster recovery applicativa.

Per le ragioni sopraesposte si ritiene di individuare la soluzione PSN più adatta al progetto LIS sovrazionale. Per quanto riguarda il costo effettivo della soluzione saranno ancora ulteriormente approfonditi con PSN gli aspetti di dettaglio e quelli relativi alla connettività, in particolare riguardo la gradualità del rilascio delle risorse cloud, considerata la scalarità del progetto, al fine di ottimizzare ulteriormente i costi.

Distinti saluti.

Direttore S.C. Sistemi Informativi
AOU Maggiore della Carità di Novara
Dott.sa Simona Capra



Simona Capra
AOU
NOVARA
18.05.2023
14:23:58
GMT+01:00

Il Direttore S.S.
ASL Vercelli
Dott. Giovanni Di Bonito
Signature Not Verified
Digitally signed by:
Giovanni Di Bonito
Date: 2023.05.18
16:30:23 CEST

Il Direttore S.C. Sistema Informativo
e Controllo
ASL Novara
Ing. Carlo Faletti



Carlo Faletti
ASL NO Novara
18.05.2023
17:28:42
GMT+01:00

Il Direttore S.C. Amministrazione
e Controllo di Gestione
ASL Biella
Dott.sa Elvira Zampepe



Firmato digitalmente da:
ZAMPESE ELVIRA
Firmato il 19/05/2023 08:55
Seriale Certificato: 2263413
Valido dal 07/03/2023 al 07/03/2026
InfoCamere Qualified Electronic Signature CA

Il Direttore S.S. ICT
ASL VCO
Dott. Benedetto Femia

Firmato digitalmente da: Benedetto Femia
Data: 19/05/2023 09:43:55

Nell'ambito della CONCESSIONE per la realizzazione e gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione denominata Polo Strategico Nazionale ("PSN"), di cui al comma 1 dell'articolo 33-septies del d.l. n. 179 del 2012.

PIANO DEI FABBISOGNI

Data: 07/03/2023

Piano dei Fabbisogni

Ed. 1 - ver. 1.0

INDICE

1	PREMESSA	5
2	DATI ANAGRAFICI DELL'AMMINISTRAZIONE	7
3	DOCUMENTI DI RIFERIMENTO.....	10
3.1	DOCUMENTI APPLICABILI	10
3.2	ACRONIMI.....	10
4	DEFINIZIONI	12
5	PIANO DI MIGRAZIONE	13
5.1	OBIETTIVI.....	13
5.1.1	<i>Descrizione Servizio 1</i>	<i>13</i>
5.2	PIANO DI MIGRAZIONE	13
5.2.1	<i>Tempistiche</i>	<i>14</i>
6	DESCRIZIONE DEI FABBISOGNI	15
6.1	CONTESTO DI RIFERIMENTO	15
7	Servizi richiesti	17
7.1	INDUSTRY STANDARD	ERRORE. IL SEGNALIBRO NON È DEFINITO.
7.1.1	<i>PaaS</i>	<i>18</i>
7.2	SECURE PUBLIC CLOUD.....	18
7.3	SERVIZIO DI MIGRAZIONE	18
7.4	SERVIZI PROFESSIONALI.....	19
7.4.1	<i>Servizi di evoluzione</i>	<i>19</i>
7.4.1.1	<i>Servizio Re-Architect</i>	<i>19</i>
7.4.1.2	<i>Servizio Re-Platform.....</i>	<i>19</i>
7.4.2	<i>Security Professional Services</i>	Errore. Il segnalibro non è definito.
7.4.3	<i>IT Infrastructure - Service Operations</i>	<i>20</i>
7.4.4	<i>Sintesi dei servizi professionali.....</i>	<i>20</i>
7.5	EVENTUALI ALTRE ESIGENZE.....	21

LISTA DELLE TABELLE

Tabella 1: Dati anagrafici dell'Amministrazione contraente	7
Tabella 2: Dati anagrafici del referente tecnico	8
Tabella 3: Documenti di riferimento	10
Tabella 4: Servizi richiesti: quadro di sintesi.....	17
Tabella 15: Fabbisogno Servizi Professionali di migrazione	19
Tabella 16: Fabbisogno Altri Servizi Professionali	21

1 PREMESSA

Il Piano Nazionale di Ripresa e Resilienza ha previsto specifici obiettivi per la transizione digitale con particolare riferimento agli “Obiettivi Italia Digitale 2026” – “Obiettivo 3 – Cloud e Infrastrutture Digitali” orientato alla migrazione dei dati e degli applicativi informatici delle singole amministrazioni. Per promuovere l’innovazione digitale nella Pubblica Amministrazione, l’Agenzia per l’Italia Digitale ha attivato un piano complessivo di trasformazione e digitalizzazione, ponendo al centro del modello strategico la componente infrastrutturale (come descritto nel Piano Triennale per l’Informatica nella Pubblica Amministrazione 2020-2022) con l’obiettivo di governare la trasformazione digitale. Le direttrici evolutive della componente infrastrutturale sono rappresentate da:

- Sovranità digitale;
- Sicurezza, assicurare un presidio tecnologico e operativo in grado di garantire i più alti standard di sicurezza:
 - Fisica (e.g. disaster recovery, business continuity, controllo accessi, etc.);
 - Informatica (e.g. prevenzione e risposta attacchi cyber, data protection, identity access management, etc.);
- Innovazione, attraverso le migliori soluzioni tecnologiche per le infrastrutture data center, la connettività, le piattaforme e i servizi cloud, garantendo trasferimento tecnologico di esperienze e know how con i leader globali.

In questo contesto, e relativamente alla razionalizzazione ed il consolidamento dei Data Center della Pubblica amministrazione, si inserisce la creazione del Polo Strategico Nazionale, una nuova infrastruttura digitale a servizio della PA italiana, che la dota di tecnologie e infrastrutture cloud affidabili, resilienti e indipendenti.

La Regione Piemonte con Deliberazione LR 20/2013, ha istituito le AIC e, contestualmente, disposto lo scioglimento, a far data dal 1° gennaio 2014, delle Federazioni Sovrazionali FS, istituite ai sensi dell’articolo 2, comma 3 della LR 3/2012. L’obiettivo dell’istituzione delle AIC è l’espletamento coordinato di funzioni amministrative, tecniche, logistiche, informative, tecnologiche e di supporto delle ASR di aree territoriali omogenee, ferme restando le funzioni di centrale di committenza regionale attribuite a SCR Piemonte S.p.A. ai sensi della LR 19/2007.

Con successiva DGR n. 43-6861 del 9/12/2013 sono state individuate 5 AIC. Sulla base di tale DGR l’AIC numero 3 è composta dalle seguenti ASR:

- AOU di Maggiore della Carità di Novara
- ASL di Vercelli
- ASL di Novara
- ASL di Biella
- ASL Verbania-Cusio-Ossola (VCO)

Successivamente, con Deliberazione della Giunta Regionale 28 luglio 2014, n. 34-189, è stata individuata per ciascuna area una Azienda Sanitaria capofila del Coordinamento degli acquisti e istituito un Tavolo di coordinamento sovrazonale (TCS), a cura dell’ASR capofila del coordinamento degli acquisti a livello di AIC. Per l’AIC numero 3 l’Ente capofila è l’AOU Maggiore della Carità di Novara. L’ASR capofila con il TCS hanno l’obiettivo di conseguire il massimo livello di standardizzazione ed aggregazione dei beni e servizi occorrenti alla AIC.

Nell’ambito sopra descritto, e relativamente alla razionalizzazione ed il consolidamento dei Data Center della Pubblica amministrazione, si inserisce l’esigenza delle Aziende afferenti all’Area Interaziendale di Coordinamento N. 3” con ogni singola Azienda facente parte dell’AIC N° 3 (A.O.U. Maggiore della Carità di Novara, ASL NO, ASL BI, ASL VC E ASL VCO) per la quale l’Ente capofila è l’AOU Maggiore della Carità di Novara, di dotarsi di tecnologie cloud conformi ai regolamenti in materia di classificazione dei dati e servizi dell’ACN e relative Determine AgID comprendenti le risorse elaborative, di storage, di sicurezza fisica (Disaster

Recovery e business continuity) e logica per il progetto per il **“sistema gestionale di laboratorio e microbiologia delle Aziende all’Area Interaziendale di Coordinamento N. 3”**.

2 DATI ANAGRAFICI DELL'AMMINISTRAZIONE

Nelle seguenti tabelle si riportano i dati anagrafici delle Amministrazioni contraenti e dei loro referenti.

Ragione sociale Contraente	
Ragione sociale	AOU Maggiore della Carità di Novara
Codice Fiscale	
Partita Iva	01521330033
Indirizzo sede legale	Corso Mazzini 18
CAP	28100
Comune	Novara
Provincia	Novara
Cognome referente Contratto Esecutivo	Capra Simona
Nome referente Contratto Esecutivo	Capra Simona
Indirizzo mail referente Contratto Esecutivo	Simona.capra@maggioreosp.novara.it
PEC Amministrazione	protocollo@pec.aou.no.it

Tabella 1: Dati anagrafici dell'Amministrazione contraente

Ragione sociale Contraente	
Ragione sociale	ASL Biella
Codice Fiscale	
Partita Iva	01810260024
Indirizzo sede legale	Via dei Ponderanesi, 2
CAP	13875
Comune	Ponderano
Provincia	Biella
Cognome referente Contratto Esecutivo	Zampese Elvira
Nome referente Contratto Esecutivo	Zampese Elvira
Indirizzo mail referente Contratto Esecutivo	elvira.zampese@aslbi.piemonte.it
PEC Amministrazione	ufficio.protocollo@cert.aslbi.piemonte.it

Ragione sociale Contraente	
Ragione sociale	ASL VCO
Codice Fiscale	
Partita Iva	00634880033
Indirizzo sede legale	Via Mazzini, 117
CAP	28887
Comune	Omegna
Provincia	VB

Cognome referente Contratto Esecutivo	Femia Benedetto
Nome referente Contratto Esecutivo	Femia Benedetto
Indirizzo mail referente Contratto Esecutivo	benedetto.femia@aslvco.it
PEC Amministrazione	protocollo@pec.aslvco.it

Ragione sociale Contraente	
Ragione sociale	ASL Vercelli
Codice Fiscale	
Partita Iva	01811110020
Indirizzo sede legale	C.so Mario Abbiate n. 21
CAP	13100
Comune	Vercelli
Provincia	VC
Cognome referente Contratto Esecutivo	Giovanni Di Bonito
Nome referente Contratto Esecutivo	Giovanni Di Bonito
Indirizzo mail referente Contratto Esecutivo	giovanni.dibonito@aslvc.piemonte.it
PEC Amministrazione	aslvercelli@pec.aslvc.piemonte.it

Ragione sociale Contraente	
Ragione sociale	ASL Novara
Codice Fiscale	
Partita Iva	01522670031
Indirizzo sede legale	Viale Roma 7
CAP	28100
Comune	Novara
Provincia	NO
Cognome referente Contratto Esecutivo	Carlo Faletti
Nome referente Contratto Esecutivo	Carlo Faletti
Indirizzo mail referente Contratto Esecutivo	carlo.faletti@asl.novara.it
PEC Amministrazione	protocollogenerale@pec.asl.novara.it

Riferimento referente tecnico	
Cognome	Guido
Nome	Andrea
Telefono fisso	03213732008
Cellulare	
Indirizzo mail	Andrea.guido@maggioreosp.novara.it

Tabella 2: Dati anagrafici del referente tecnico

Data	Firma
Novara, 23/03/2023	 <p>Simona Capra AOU NOVARA 23.03.2023 11:15:07 GMT+01:00</p>

3 DOCUMENTI DI RIFERIMENTO

Riferimento	Codice	Titolo
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022	CONVENZIONE ai sensi degli artt. 164, 165, 179, 180, comma 3 e 183, comma 15 del d.lgs. 18 aprile 2016, n. 50 e successive modificazioni o integrazioni avente ad oggetto l’affidamento in concessione dei servizi infrastrutturali e applicativi in cloud per la gestione di dati sensibili - “Polo Strategico Nazionale”
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato A)	Capitolato Tecnico e relativi annessi – Capitolato Servizi
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato B)	“Offerta Tecnica” e relativi annessi
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato C)	“Offerta economica del Fornitore – Catalogo dei Servizi” e relativi annessi
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato D)	Schema di Contratto di Utenza
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato H)	Indicatori di Qualità
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato I)	Flussi informativi
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato L)	Elenco dei Servizi Core, no Core e CSP

Tabella 3: Documenti di riferimento

3.1 DOCUMENTI APPLICABILI

Riferimento	Codice	Titolo
Template Piano dei Fabbisogni	PSN- TMPL- PNDF	Piano dei Fabbisogni Template

3.2 ACRONIMI

Acronimo	Descrizione
AI	Artificial Intelligence

CaaS	Container as a Service
CMP	Cloud Management Platform
CSP	Cloud Service Provider
DB	DataBase
DBaaS	DataBase as a Service
DR	Disaster Recovery
GCP	Google Cloud Platform
HA	High Availability
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IT	Information Technology
PA	Pubblica Amministrazione
PaaS	Platform as a Service
PSN	Polo Strategico Nazionale
VM	Virtual Machine

4 DEFINIZIONI

- ACN: l’Agenzia per la cybersicurezza nazionale, di cui al decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109;
- DTD: il Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri;
- Amministrazioni: le amministrazioni individuate dall’articolo 1, comma 3, della legge 31 dicembre 2009, n. 196;
- Dati dell’amministrazione: le informazioni trattate dall’amministrazione, o da terzi per conto dell’amministrazione;
- Regolamento: il Regolamento di cui all’articolo 33-septies, comma 4, del decreto legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, recante “livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione”, adottato dall’Agenzia per l’Italia digitale (AgID), d’intesa con il DTD, con Determinazione n. 628/2021 del 15 dicembre 2021;
- Servizi dell’amministrazione: servizi erogati verso terzi o internamente all’amministrazione;
- “modalità A - trasferimento in sicurezza dell’infrastruttura IT”: migrazione verso il cloud effettuata secondo la strategia di migrazione Lift&Shift (anche detta Rehost), ovvero la migrazione dell’intero servizio dell’amministrazione, comprensivo di applicazioni e dati su un hosting cloud senza apportare modifiche agli applicativi, ovvero replicando il servizio esistente in un ambiente cloud;
- “modalità B - aggiornamento in sicurezza di applicazioni in cloud”: migrazione verso il cloud effettuata secondo le seguenti strategie:
 - *repurchase/replace*: si intende la migrazione del servizio dell’amministrazione verso una soluzione nativa in cloud, in genere erogata in modalità Software as a Service;
 - *replatform*: si intende la riorganizzazione dell’architettura applicativa sostituendo intere componenti del servizio in favore di soluzioni Cloud native in modo da usufruire dei benefici dell’infrastruttura Cloud;
 - *re-architect*: ha come obiettivo quello di ripensare significativamente l’architettura core di un applicativo in ottica cloud, attraverso un processo di redesign iterativo ed incrementale che miri ad adottare appieno i servizi cloud-native offerti dai cloud service provider per massimizzare i benefici che ne derivano;
- Housing: utilizzo delle infrastrutture impiantistiche e di connettività dei Data Center del PSN, dove verranno ospitate apparecchiature delle Amministrazioni;
- Hosting: utilizzo delle infrastrutture IT dei Data Center del PSN, dove verranno installate le componenti software e middleware delle Amministrazioni.

5 PIANO DI MIGRAZIONE

Il presente capitolo rappresenta il piano di migrazione al cloud di dati e servizi dell'Amministrazione, in linea con quanto richiesto nella determina del 7 ottobre 2022 del Dipartimento per la trasformazione digitale.

5.1 Obiettivi

Come indicato in premessa l'obiettivo delle Aziende afferenti all'Area Interaziendale di Coordinamento N. 3 di dotarsi di tecnologie e infrastrutture cloud affidabili, resilienti, sicure e indipendenti per il fabbisogno legato alla digitalizzazione dei processi, in linea con quanto richiesto nell'Appalto Specifico per l'affidamento di servizi per la gestione e lo sviluppo del sistema gestionale di laboratorio analisi e microbiologia occorrente alle aziende afferenti all'area interaziendale di coordinamento n.3 per un periodo di 60 mesi mediante appalto specifico nell'ambito dell'accordo quadro per i servizi applicativi per le pubbliche amministrazioni stipulato da Consip – ID 1881 – Lotto 1 CONTRATTI GRANDI – NORD.

Servizio dell'amministrazione	Tipo di Migrazione
Servizio 1: Sistema gestionale di laboratorio analisi e microbiologia occorrente alle aziende afferenti all'area interaziendale di coordinamento n.3	modalità B - aggiornamento in sicurezza di applicazioni in cloud

5.1.1 Descrizione Servizio 1

Il servizio da migrare in cloud deriva dal fabbisogno legato alla realizzazione del progetto del Sistema gestionale di laboratorio analisi e microbiologia occorrente alle aziende afferenti all'area interaziendale di coordinamento n.3.

Nel par. 6.1 è riportata la lista delle risorse cloud che il fornitore, aggiudicatario dell'Appalto Specifico per i servizi applicativi per le pubbliche amministrazioni Lotto 1 (id 1881), ha indicato come necessarie; tale elenco riporta le risorse necessarie per i tre ambienti messi a disposizione dal PSN:

- Ambiente di produzione
- Ambiente di collaudo
- Ambiente di test

Sono altresì indicate le risorse per le quali è prevista la replica sul sito di DR, sempre a carico del PSN.

5.2 Piano di migrazione

Si riporta di seguito il piano di migrazione che fornisce un quadro sintetico del progetto di migrazione dell'Amministrazione, che seguirà le fasi dettate dal piano di progetto di implementazione del Sistema gestionale di laboratorio analisi e microbiologia, che si riporta a titolo esemplificativo.

6 DESCRIZIONE DEI FABBISOGNI

6.1 Contesto di Riferimento

Il contesto di riferimento è quello della infrastruttura riportata sinteticamente nella tabella seguente, destinata ad ospitare gli ambienti (Test, collaudo, produzione – primario e DR) per il Sistema gestionale di laboratorio analisi e microbiologia occorrente alle aziende afferenti all'area interaziendale di coordinamento n.3, dimensionato sulla base dei requisiti dell'Appalto Specifico per i servizi applicativi per le pubbliche amministrazioni Lotto 1 dal fornitore, aggiudicatario dello stesso.

OMISSIS

OMISSIS

7 Servizi richiesti

Di seguito sono indicati i servizi richiesti dall'AIC 3.

SERVIZIO	Richiesto	Ipotesi Budget (€)
Industry standard – Hosting		
Industry standard - Housing		
Industry standard – IaaS		
Industry standard – PaaS	X	
Industry standard – SaaS		
Hybrid Cloud on PSN site		
Secure Public Cloud on Microsoft Azure	X	
Secure Public Cloud on Google GCP		
Public Cloud PSN Managed		
Servizi di migrazione	X	
Servizi professionali - Servizio Re-Architect	X	
Servizi professionali - Servizio Re-Platform	X	
Servizi professionali - Security Professional Services	X	
Servizi professionali - IT Infrastructure - Service Operations	X	
Servizi professionali - Business and culture enablement		
Altri servizi a listino>		

Tabella 4: Servizi richiesti: quadro di sintesi

7.1.1 PaaS

Il servizio Industry Standard PaaS mette a disposizione una piattaforma in grado di erogare componenti di middleware secondo un modello a servizio (ad esempio Data Base) astruendo l'infrastruttura sottostante. Il PSN è responsabile dell'infrastruttura sottostante comprensiva degli strumenti di automation e orchestration e si compone dei seguenti sottoservizi:

DBaaS

- Consente di configurare e gestire database utilizzando un servizio senza preoccuparsi dell'infrastruttura sottostante

Per soddisfare i requisiti della piattaforma di gestione dei laboratori Analisi il Fornitore della soluzione software richiede l'estensione dei servizi PaaS Oracle, in termini di incremento delle configurazioni disponibili in modo tale da soddisfare i requisiti infrastrutturali.

7.2 Secure Public Cloud

Con il Secure Public Cloud si ottiene l'accesso al Public Cloud con controllo e gestione della Digital Sovereignty e della sicurezza. È un servizio che si basa su Region pubbliche degli Hyperscaler (Microsoft Azure e Google Cloud GCP) a cui vengono aggiunti tutti gli elementi di sicurezza (chiavi esterne, backup, template, servizi professionali). Sono possibili 2 tipologie di servizio:

- **Secure Public Cloud on Microsoft Azure**
- **Secure Public Cloud on Google GCP**

Le quantità rispondono alle esigenze del Servizio 1, come espresse al par. 6.1, e verranno dettagliate nel Progetto del Piano dei Fabbisogni sulla base del listino **Secure Public Cloud on Microsoft Azure**

7.3 Servizio di migrazione

Si richiede il servizio di migrazione end-to-end chiavi in mano sia fisica (housing) che virtuale (dall'analisi degli applicativi al test sui nuovi ambienti e messa in produzione) dell'infrastruttura IT dell'Amministrazione verso l'infrastruttura PSN.

Si presume che siano necessarie le figure professionali per l'erogazione del servizio.

Di seguito una tabella a titolo esemplificativo dello skill mix afferente il servizio.

Figure Professionali Lift&Shift Cloud Enabling	Mix Migrazione
Enterprise Architect	10%
Cloud Application Architect	10%
Cloud Application Specialist	20%
Cloud Security Specialist	15%
Database Specialist and Administrator	15%
System Integrator & Testing Specialist	30%
	100%

Figura	Quantità
Cloud Application Architect	TBD
Database Specialist and Administrator	TBD
System Integrator & Testing Specialist	TBD

Cloud Application Specialist	TBD
Cloud Security Specialist	TBD
Enterprise Architect	TBD

Tabella 5: Fabbisogno Servizi Professionali di migrazione

7.4 Servizi professionali

L'Amministrazione richiede i seguenti ulteriori servizi professionali:

- Servizi di evoluzione
- Security Professional Services (strategy - assessment - operations)
- IT Infrastructure - Service Operations

7.4.1 Servizi di evoluzione

I servizi di evoluzione comprendono:

- **Servizio Re-Architect**
- **Servizio Re-Platform**

7.4.1.1 Servizio Re-Architect

Servizi professionali evolutivi volti alla riprogettazione dell'architettura delle applicazioni in ottica Cloud.

<i>Figure Professionali Migrazione Applicativa al Cloud</i>	<i>Mix Migrazione</i>
<i>Project Manager</i>	<i>10%</i>
<i>DevOps Expert</i>	<i>10%</i>
<i>Business Analyst</i>	<i>5%</i>
<i>Enterprise Architect</i>	<i>5%</i>
<i>Cloud Application Architect</i>	<i>5%</i>
<i>Cloud Application Specialist</i>	<i>12%</i>
<i>Cloud Security Specialist</i>	<i>8%</i>
<i>Developer (Cloud/Mobile/ Front-End Developer)</i>	<i>20%</i>
<i>Database Specialist and Administrator</i>	<i>8%</i>
<i>System and Network Administrator</i>	<i>12%</i>
<i>UX Designer</i>	<i>5%</i>
	<i>100%</i>

7.4.1.2 Servizio Re-Platform

Servizi professionali evolutivi volti alla riprogettazione delle piattaforme che gestiscono le applicazioni dell'Amministrazione in modo da abilitarne la trasformazione verso il Cloud.

<i>Figure Professionali Migrazione Applicativa al Cloud</i>	<i>Mix Migrazione</i>
<i>Project Manager</i>	<i>10%</i>
<i>DevOps Expert</i>	<i>10%</i>

<i>Business Analyst</i>	5%
<i>Enterprise Architect</i>	5%
<i>Cloud Application Architect</i>	5%
<i>Cloud Application Specialist</i>	12%
<i>Cloud Security Specialist</i>	8%
<i>Developer (Cloud/Mobile/Front-End Developer)</i>	20%
<i>Database Specialist and Administrator</i>	8%
<i>System and Network Administrator</i>	12%
<i>UX Designer</i>	5%
	100%

7.4.2 IT Infrastructure - Service Operations

Servizi specialistici on demand a supporto delle Operations per la gestione dell'infrastruttura e del parco applicativo cliente.

Di seguito una tabella a titolo esemplificativo dello skill mix afferente il servizio

<i>Figure Professionali Servizi Operations</i>	<i>Skill Mix</i>
<i>Systems Architect</i>	9%
<i>Product/Network/Technical Specialist</i>	53%
<i>Database Specialist and Administrator</i>	6%
<i>Cloud Security Specialist</i>	4%
<i>System and Network Administrator</i>	28%
	100%

7.4.3 Sintesi dei servizi professionali

Di seguito è riportato il prospetto riassuntivo delle richieste da parte dell'Amministrazione relative al par. 5.6 "Servizi professionali".

Tipologia	Figura	Contesto	Quantità
Figura professionale	Project Manager	Research&Replat, Profess Serv	TBD
Figura professionale	Cloud Application Architect	Research&Replat, Profess Serv	TBD
Figura professionale	UX Designer	Research&Replat	TBD
Figura professionale	Business Analyst	Research&Replat	TBD
Figura professionale	DevOps Expert	Research&Replat	TBD
Figura professionale	Database Specialist and Administrator	Research&Replat, IT Infrastructur-service operation	TBD
Business & Culture Enablement Figura professionale	Developer (Cloud/Mobile/Front-End Developer)	Research&Replat, Business&Culture Enablement	TBD
Figura professionale	System Integrator & Testing Specialist		TBD
Figura professionale	System and Network Administrator	Research&Replat, IT Infrastructur-service operation	TBD
Figura professionale	Cloud Application Specialist	Research&Replat, Profess Serv	TBD
Figura professionale	Cloud Security Specialist	Research&Replat, IT Infrastructur-service operation	TBD
Figura professionale	Enterprise Architect	Research&Replat	TBD
Figura professionale	Security Principal	Profess Serv	TBD
Figura professionale	Senior Information Security Consultant	Profess Serv	TBD
Figura professionale	Junior Information Security Consultant	Profess Serv	TBD
Figura professionale	Security Solution Architect	Profess Serv	TBD
Figura professionale	Senior Security Auditor/Analyst	Profess Serv	TBD
Figura professionale	Junior Security Analyst	Profess Serv	TBD
Figura professionale	Senior Penetration Tester	Profess Serv	TBD
Figura professionale	Junior Penetration Tester	Profess Serv	TBD
Figura professionale	Forensic Expert	Profess Serv	TBD

Figura professionale	Data Protection Specialist	Profess Serv	TBD
Figura professionale	Systems Architect	Profess Serv	TBD

Tabella 6: Fabbisogno Altri Servizi Professionali

7.5 Eventuali altre esigenze

Estensione dei servizi PaaS sia in termini di incremento delle configurazioni disponibili su prodotti già presenti a listino (Es. PaaS Oracle), che di introduzione di ulteriori piattaforme software.



Firmato digitalmente da:
EMANUELE IANNETTI
Amministratore Delegato
POLO STRATEGICO NAZIONALE S.P.A.
Firmato il 22/06/2023 17:37
Seriale Certificato: 940
Valido dal 26/10/2022 al 25/10/2025
TI Trust Technologies QTSP CA

CONCESSIONE per la realizzazione e gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione denominata Polo Strategico Nazionale (“PSN”), di cui al comma 1 dell’articolo 33-septies del d.l. n. 179 del 2012

CUP: J51B21005710007

CIG: 9066973ECE

PROGETTO DEL PIANO DEI FABBISOGNI

AIC numero 3

Data: 15/06/2023

PSN-SDE-CONV22-001-ProgettoPianoDeiFabbisogni

Ed. 1 - ver. 1.0

SOMMARIO

1	PREMESSA.....	8
2	AMBITO	9
2.1	Obiettivi	9
2.1.1	Descrizione Servizio 1	10
3	DOCUMENTI.....	11
3.1	DOCUMENTI CONTRATTUALI	11
3.2	DOCUMENTI DI RIFERIMENTO	11
3.3	DOCUMENTI APPLICABILI	12
4	ACRONIMI.....	13
5	PROGETTO DI ATTUAZIONE DEL SERVIZIO	14
5.1	SERVIZI PROPOSTI	14
5.2	INDUSTRY STANDARD.....	14
5.2.1	Platform as a Service.....	14
5.3	SECURE PUBLIC CLOUD	17
5.3.1	Descrizione del servizio	17
5.3.2	Personalizzazione del servizio.....	19
5.3.3	Dettaglio del servizio contrattualizzato (ID servizio, quantità costi).....	20
5.3.4	Specifiche di collaudo	20
5.4	CLOUD MANAGEMENT PLATFORM.....	21
5.4.1	Descrizione del servizio	21
5.4.2	Specifiche di collaudo	21
5.5	SERVIZI E PIANO DI MIGRAZIONE.....	22
5.5.1	Obiettivi della Migrazione.....	22
5.5.2	Macro piano di setup e migrazione.....	22
5.6	Servizi professionali.....	23
5.6.1	Modalità di erogazione dei Servizi professionali.....	23
5.6.2	Security Profess. Services	24
5.6.3	IT infrastructure service operations	32
6	FIGURE PROFESSIONALI	34
7	SICUREZZA	36
8	CONFIGURATORE	37
8.1.1	Infrastruttura Secure Public Cloud Azure e DB as a Service Oracle e relativi servizi.....	38
8.2	Servizi professionali	42
8.2.1	Fase iniziale migrazione, start-up e rilascio servizi di piattaforma	42

8.2.2	Fase di operatività della piattaforma LIS	43
-------	---	----

Indice delle tabelle

Tabella 1 Informazioni Documento	6
Tabella 2 Autore	6
Tabella 3 Revisore.....	6
Tabella 4 Approvatore	6
Tabella 5 Documenti Contrattuali	11
Tabella 6 Documenti di riferimento	12
Tabella 7 Documenti Applicabili	12
Tabella 8 Acronimi.....	13
Tabella 9 Servizi Proposti.....	14
Tabella 10 Dimensionamento istanze PaaSDB	17
Tabella 11 Servizi Secure Public Cloud	20
Tabella 12 Tabella di correlazione tra gravità incidenti e impatto sugli asset	29
Tabella 13 Descrizione dei livelli di incidente.....	30
Tabella 14 Modello di servizio per il Triage.....	30
Tabella 15 Importi per singola fase	38

STATO DEL DOCUMENTO

La tabella seguente riporta la registrazione delle modifiche apportate al documento.

TITOLO DEL DOCUMENTO		
Descrizione Modifica	Revisione	Data
Prima Emissione	1	22/05/2023

Tabella 1 Informazioni Documento

Autore:	
Team di lavoro PSN	Unità operative Solution Development, Technology Hub e Sicurezza

Tabella 2 Autore

Revisione:	
PSN Solution team	n.a.

Tabella 3 Revisore

Approvazione:	
PSN Solution team	Paolo Trevisan
PSN Commercial team	Riccardo Rossi

Tabella 4 Approvatore

LISTA DI DISTRIBUZIONE

INTERNA A:

- Funzione Solution Development
- Funzione Technology Hub
- Funzione Sicurezza
- Referente Servizio
- Direttore Servizio

ESTERNA A:

- Direttore dell'Esecuzione Contrattuale (DEC) PSN ing. Fabrizio Marchese
- Referente Contratto Esecutivo AIC numero 3
 - **AOU Maggiore della Carità di Novara:** Capra Simona
 - Email: simona.capra@maggioreosp.novara.it
 - **ASL Biella:** Zampese Elvira
 - Email: elvira.zampese@aslbi.piemonte.it
 - **ASL VCO:** Femia Benedetto
 - Email: benedetto.femia@aslvc.it
 - **ASL Vercelli:** Di Bonito Giovanni
 - Email: giovanni.dibonito@aslvc.piemonte.it
 - **ASL Novara:** Faletti Carlo
 - Email: carlo.faletti@asl.novara.it
- Referente Tecnico AIC numero 3: Guido Andrea
 - Email: andrea.guido@maggioreosp.novara.it

1 PREMESSA

Il presente documento descrive il Progetto dei Fabbisogni del **PSN** relativamente alla richiesta di fornitura dei servizi cloud nell'ambito della concessione per la realizzazione e gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione denominata Polo Strategico Nazionale ("PSN"), di cui al comma 1 dell'articolo 33-septies del d.l. n. 179 del 2012.

Quanto descritto, è stato redatto in conformità alle richieste del **AIC numero 3** di seguito Amministrazione, sulla base delle esigenze emerse durante gli incontri tecnici per la raccolta dei requisiti e delle informazioni contenute nel Piano dei Fabbisogni (ID **2023-0000001521330033-PdF-P1R1**).

2 AMBITO

2.1 *Obiettivi*

La Regione Piemonte con Deliberazione LR 20/2013, ha istituito le AIC e, contestualmente, disposto lo scioglimento, a far data dal 1° gennaio 2014, delle Federazioni Sovrazionali FS, istituite ai sensi dell'articolo 2, comma 3 della LR 3/2012. L'obiettivo dell'istituzione delle AIC è l'espletamento coordinato di funzioni amministrative, tecniche, logistiche, informative, tecnologiche e di supporto delle ASR di aree territoriali omogenee, ferme restando le funzioni di centrale di committenza regionale attribuite a SCR Piemonte S.p.A. ai sensi della LR 19/2007.

Con successiva DGR n. 43-6861 del 9/12/2013 sono state individuate 5 AIC. Sulla base di tale DGR l'AIC numero 3 è composta dalle seguenti ASR:

- AOU di Maggiore della Carità di Novara
- ASL di Vercelli
- ASL di Novara
- ASL di Biella
- ASL Verbania-Cusio-Ossola (VCO)

Successivamente, con Deliberazione della Giunta Regionale 28 luglio 2014, n. 34-189, è stata individuata per ciascuna area una Azienda Sanitaria capofila del Coordinamento degli acquisti e istituito un Tavolo di coordinamento sovrazonale (TCS), a cura dell'ASR capofila del coordinamento degli acquisti a livello di AIC. Per l'AIC numero 3 l'Ente capofila è l'AOU Maggiore della Carità di Novara. L'ASR capofila con il TCS hanno l'obiettivo di conseguire il massimo livello di standardizzazione ed aggregazione dei beni e servizi occorrenti alla AIC.

Nell'ambito sopra descritto, e relativamente alla razionalizzazione ed il consolidamento dei Data Center della Pubblica amministrazione, si inserisce l'esigenza delle Aziende afferenti all'Area Interaziendale di Coordinamento N. 3" con ogni singola Azienda facente parte dell'AIC N° 3 (A.O.U. Maggiore della Carità di Novara, ASL NO, ASL BI, ASL VC E ASL VCO) per la quale l'Ente capofila è l'AOU Maggiore della Carità di Novara, di dotarsi di tecnologie cloud conformi ai regolamenti in materia di classificazione dei dati e servizi dell'ACN e relative Determine AgID comprendenti le risorse elaborative, di storage, di sicurezza fisica (Disaster Recovery e business continuity) e logica per il progetto per il **"sistema gestionale di laboratorio e microbiologia delle Aziende all'Area Interaziendale di Coordinamento N. 3"**.

L'obiettivo delle Aziende afferenti all'Area Interaziendale di Coordinamento N. 3 è quello di dotarsi di tecnologie e infrastrutture cloud affidabili, resilienti, sicure e indipendenti per il fabbisogno legato alla digitalizzazione dei processi, in linea con quanto richiesto nell'Appalto Specifico per l'affidamento di servizi per la gestione e lo sviluppo del sistema gestionale di laboratorio analisi e microbiologia (cosiddetto LIS) occorrente alle aziende afferenti all'area interaziendale di coordinamento n.3 per un periodo di 60 mesi mediante appalto specifico nell'ambito dell'accordo quadro per i servizi applicativi per le pubbliche amministrazioni stipulato da Consip – ID 1881 – Lotto 1 CONTRATTI GRANDI – NORD.

Servizio dell'amministrazione	Tipo di Migrazione
Servizio 1: Sistema gestionale di laboratorio analisi e microbiologia occorrente alle aziende afferenti all'area interaziendale di coordinamento n.3	modalità B - aggiornamento in sicurezza di applicazioni in cloud

2.1.1 *Descrizione Servizio 1*

Il servizio da migrare in cloud deriva dal fabbisogno legato alla realizzazione del progetto del Sistema gestionale di laboratorio analisi e microbiologia occorrente alle aziende afferenti all'area interaziendale di coordinamento n.3, che prevede la realizzazione di una piattaforma di collegamento e interoperabilità fra Laboratori in modalità HUB&Spoke, al fine di riorganizzarne la topologia e dare vita alla rete sovra-zonale di Laboratorio della AIC n.3.

Il presente progetto risponde alla esigenza di risorse cloud che la PA, sulla base delle esigenze dell'Appalto Specifico per i servizi applicativi per le pubbliche amministrazioni Lotto 1 (id 1881), ha indicato come necessarie; tale elenco riporta le risorse necessarie per i tre ambienti messi a disposizione dal PSN:

- Ambiente di produzione
- Ambiente di collaudo
- Ambiente di test

Sono altresì indicate le risorse per le quali è prevista la replica sul sito di DR, sempre a carico del PSN.

L'attività richiesta nel Piano dei Fabbisogni viene caratterizzata come un aggiornamento del servizio con la messa in sicurezza in modalità cloud in logica repurchase.

Repurchase: migrazione di servizi delle ASR verso una soluzione nativa in cloud, erogata in modalità Software as a Service.

3 DOCUMENTI

3.1 DOCUMENTI CONTRATTUALI

Riferimento	Titolo	Documenti consegnati
#1	Piano dei Fabbisogni di Servizio	PSN_Progetto dei Fabbisogni_1.0
#2	Piano di Sicurezza	PSN-SDE-CONV22-001-PianoSicurezza v.1.0 Allegati: PSN - Processo IM v.03 2.C Qualificazione Servizi Cloud 2.B Fornitore Servizio Cloud 2.A Soggetto Infrastruttura Digitale
#3	Piano di Qualità	PSN-SDE-CONV22-001-Piano della Qualità
#4	Piano di Continuità Operativa	PSN-SDE-CONV22-001-Piano di Continuità Operativa ver.1.0

Tabella 5 Documenti Contrattuali

3.2 DOCUMENTI DI RIFERIMENTO

La seguente tabella riporta i documenti che costituiscono il riferimento a quanto esposto nel seguito del presente documento.

Riferimento	Codice	Titolo
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022	CONVENZIONE ai sensi degli artt. 164, 165, 179, 180, comma 3 e 183, comma 15 del d.lgs. 18 aprile 2016, n. 50 e successive modificazioni o integrazioni avente ad oggetto l'affidamento in concessione dei servizi infrastrutturali e applicativi in cloud per la gestione di dati sensibili - "Polo Strategico Nazionale"
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato A)	Capitolato Tecnico e relativi annessi – Capitolato Servizi
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato B)	"Offerta Tecnica" e relativi annessi

Riferimento	Codice	Titolo
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato C)	“Offerta economica del Fornitore – Catalogo dei Servizi” e relativi annessi
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato D)	Schema di Contratto di Utenza
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato H)	Indicatori di Qualità
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato I)	Flussi informativi
Convenzione Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale – del 24.08.2022	CONV-PSN-2022 (Allegato L)	Elenco dei Servizi Core, no Core e CSP

Tabella 6 Documenti di riferimento

3.3 DOCUMENTI APPLICABILI

Riferimento	Codice	Titolo
Template Progetto del Piano dei Fabbisogni	PSN- TMPL- PGDF	Progetto del Piano dei Fabbisogni Template

Tabella 7 Documenti Applicabili

4 ACRONIMI

La seguente tabella riporta le descrizioni o i significati degli acronimi e delle abbreviazioni presenti nel documento.

Acronimo	Descrizione
AI	Artificial Intelligence
BC	Business Continuity
CaaS	Container as a Service
CMP	Cloud Management Platform
CRC	Cyclic Redundancy Check
CSP	Cloud Service Provider
DB	DataBase
DR	Disaster Recovery
ETL	Extract Transform and Load
GCP	Google Cloud Platform
HA	High Availability
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IT	Information Technology
ITSM	Information Technology Service Management
PA	Pubblica Amministrazione
PaaS	Platform as a Service
PaaSDB	Platform as a Service - Database
PMCA	Project Manager di Contratto Adesione
PSN	Polo Strategico Nazionale
SCORM	Shareable Content Object Reference Model
TTL	Technical Team Leader
VA	Vulnerability Assessment
VM	Virtual Machine
WBT	Web Based Training
WORM	Write Once, Read Many

Tabella 8 Acronimi

5 PROGETTO DI ATTUAZIONE DEL SERVIZIO

Uno degli obiettivi del PSN è la riduzione dei consumi energetici è pertanto necessario, nell'ottica dell'energy control, stabilire i consumi energetici dell'infrastruttura dell'Amministrazione. Questa verrà fatta assumendo come valore di riferimento il consumo (misurato o stimato sulla base dei valori di targa) annuo dell'infrastruttura prima che questa venga migrata. Seguirà una valutazione circa l'utilizzo delle risorse HW e SW impegnate nel PSN con il preciso scopo di contenerne i consumi.

5.1 SERVIZI PROPOSTI

Di seguito si riporta una sintesi delle soluzioni individuate per soddisfare le esigenze dell'Amministrazione.

Servizio	Tipologia
Industry Standard	Platform as a Service Database PaaSDB (Oracle)
Secure Public Cloud	Azure
Cloud Management Platform	
Servizi di Migrazione	
Servizi Professionali	Security Professional Services
Servizi Professionali	IT Infrastructure Service Operation

Tabella 9 Servizi Proposti

5.2 INDUSTRY STANDARD

5.2.1 Platform as a Service

5.2.1.1 Descrizione del servizio

Il **Servizio Platform as a Service (PaaS)** è un servizio *Core* e consiste nella messa a disposizione, da parte del PSN, di una piattaforma in grado di erogare elementi applicativi e middleware come servizio, come ad esempio i Database, astruendo dall'infrastruttura sottostante. Il PSN, in qualità di provider, si fa carico di gestire l'infrastruttura sottostante, comprensiva degli strumenti di automation e orchestration. L'offerta dei servizi PaaS prevede un approccio strutturato in cui ogni componente della soluzione PaaS, come il sistema operativo, solution stack ed altri software necessari, è gestito e strettamente controllato in termini

di utilizzo e configurazione dal PSN. In questo caso le soluzioni vengono “create” al momento della necessità. Una rappresentazione di questa strutturazione vede quattro livelli di componenti:

- sistema operativo;
- run-time e librerie necessarie;
- soluzione caratterizzante – tipicamente un database, middleware, web server, ecc.;
- un’interfaccia programmatica con cui controllare gli aspetti operazionali della soluzione.

Il servizio PaaS proposto in questo progetto è il **Database as a Service (DBaaS)**: questo servizio consente all’Amministrazione di configurare e gestire il database utilizzando un servizio senza preoccuparsi dell’infrastruttura sottostante. Il PSN è responsabile di tutto lo **stack d’infrastruttura** comprese le operazioni di riconfigurazione della capacità elaborativa e delle repliche.

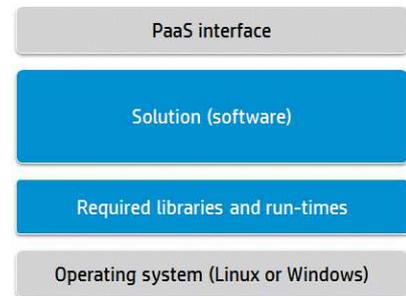


Figura 1 Platform as a Service

5.2.1.2 Platform as a Service - Database

Il **Platform as a Service - Database (PaaSDB)** è un servizio che consente agli utenti di configurare, gestire e ridimensionare database utilizzando un insieme comune di astrazioni secondo un modello unificato, senza dover conoscere o preoccuparsi delle esatte implementazioni per lo specifico database. Viene demandato al provider tutto quanto relativo all’esercizio e alla gestione dell’infrastruttura sottostante, comprese le operazioni di riconfigurazione della capacità elaborativa e delle repliche, mentre gli utenti possono così focalizzarsi sulle funzionalità applicative.

Tramite la console di gestione del servizio vengono messe a disposizione dell’Amministrazione in particolare le funzionalità di:

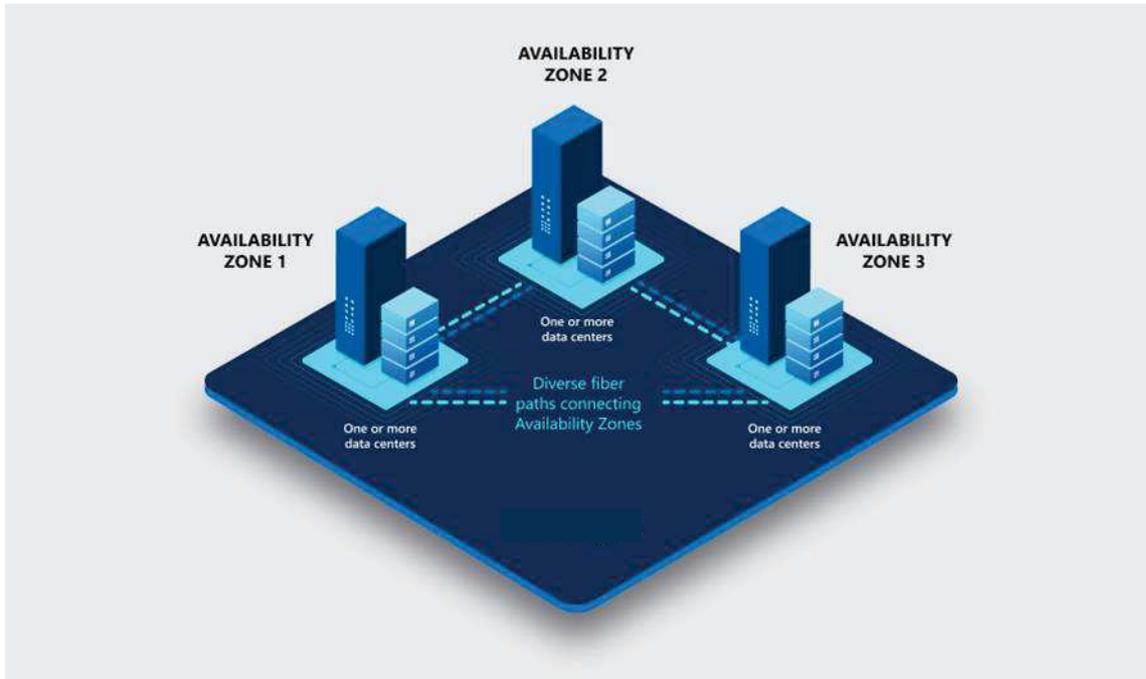
- creazione (o cancellazione) di un database;
- modifica delle principali caratteristiche infrastrutturali dell’istanza DB e ridimensionamento ove non automatico;
- configurazione di alcuni parametri del database;
- attivazione di funzionalità aggiuntive, come ad esempio la replica dei dati su istanze passive (ove applicabile);
- attivazione di funzionalità di backup od esportazione dei dati (ove applicabile).

Nel paragrafo seguente è dettagliata la descrizione del servizio personalizzato.

5.2.1.3 Personalizzazione del servizio

Il RDBMS è Oracle 19c, Enterprise Edition, come richiesto dalle specifiche del fornitore della piattaforma applicativa, per l’ambiente di Produzione è prevista la configurazione in Business Continuity (BC) geografica. La BC viene realizzata ponendo due nodi database server su siti su due Availability Zone separate della Region Italiana situate a distanza metropolitana (decine di Km), con SLA Uptime 99,99%, con una latenza <= 2 ms.

L'allineamento viene effettuato in modalità sincrona (Maximum Availability con Far Sync -garantendo in tal modo **RPO=0**, **RTO <=20 s**) tramite Oracle Active Dataguard with Fast Start, fornito in bundle con la piattaforma Database. La configurazione del DR è schematizzata nelle figure seguenti:



in particolare nella figura sotto è rappresentato il meccanismo di replica con Oracle Advanced Dataguard, proposto, con la schematizzazione del meccanismo di "Far sync", che consente di annullare potenziali ritardi nella sincronizzazione dovuti a problemi di latenza e di garantire RPO=0.

OMISSIS

OMISSIS

OMISSIS

OMISSIS

OMISSIS

5.4 CLOUD MANAGEMENT PLATFORM

5.4.1 Descrizione del servizio

PSN rende disponibile all'Amministrazione la Console Unica, applicabile in un contesto Multicloud e che si integra con le funzionalità della Cloud Management Platform, unico punto di gestione per i servizi standard erogati dal PSN. Attraverso servizi professionali (opzionali) è possibile estendere le capabilities standard con funzionalità aggiuntive o personalizzazione.



Figura 2 Cloud Management Platform

La Console Unica di Gestione permette all'Amministrazione di gestire i servizi sul PSN e su altri Cloud Service Provider, attraverso le funzionalità riassunte di seguito:

- Portale self-service con catalogo dei servizi unificato;
- Servizi di infrastruttura (designing, provisioning e management di infrastrutture multi-cloud);
- Interazione via API per modelli Cloud Agnostic di IaC (con integrazione Git repositories e strumenti di CI/CD);
- Servizi e BluePrint tecnologiche;
- Dashboard di Performance Monitoring, analisi predittiva e definizione di allarmi per superamento soglie;
- Interfaccia interattiva di misurazione e gestione dei consumi e delle risorse;
- Strumento di costruzione di report di Cost Control e Resource Usage;
- Gestione finanziaria dell'IT.

Sono inoltre disponibili come servizi aggiuntivi (che richiedono in ogni caso attività professionali di configurazione e implementazione su CU e CMP) funzionalità di:

- Governance (diritti di utilizzo, approvazioni, recupero, showback);
- Servizi e BluePrint tecnologiche personalizzati;
- Workflow personalizzati;
- Capacity Planning Avanzato (corretto dimensionamento, modellazione, scenari di tipo "what-if" e funzionalità analitiche basate su modelli di capacità);
- Advanced Monitoring (può richiedere l'installazione di componenti sui server del cliente);

5.4.2 Specifiche di collaudo

Per le modalità di svolgimento delle prove di Collaudo e di Test, previste per il servizio in oggetto, finalizzate a verificare la conformità del Servizio standard offerto a catalogo, si rimanda, alla documentazione ufficiale di collaudo dei Servizi PSN effettuato dal Dipartimento della Trasformazione Digitale, disponibile in un'apposita sezione del Portale della Fornitura.

5.5 SERVIZI E PIANO DI MIGRAZIONE

5.5.1 Obiettivi della Migrazione

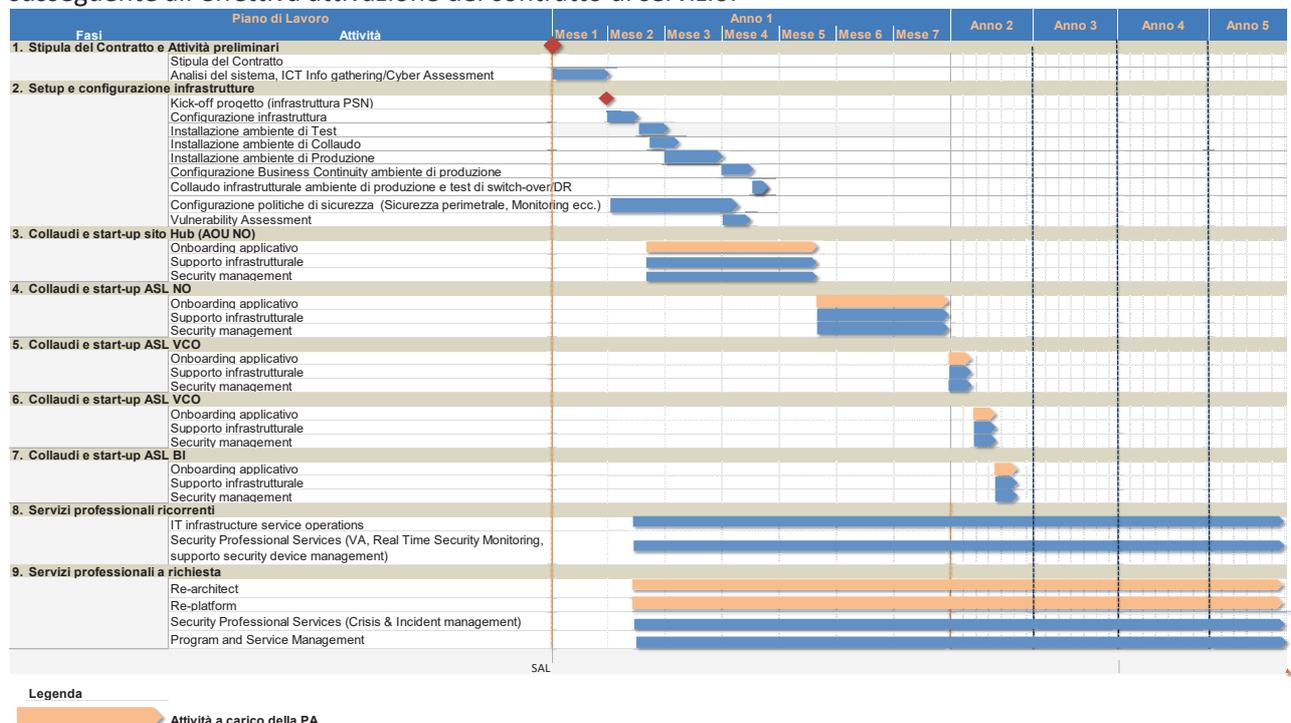
Il servizio da migrare in cloud deriva dal fabbisogno legato alla realizzazione del progetto del Sistema gestionale di laboratorio analisi e microbiologia occorrente alle aziende afferenti all'area interaziendale di coordinamento n.3, in questo contesto alcune delle Aziende Coinvolte sono già dotate di una piattaforma di Laboratorio che sarà oggetto di attività di consolidamento nella nuova infrastruttura Hub&Spoke, mentre per altre viene effettuato l'onboarding ex-novo nella LIS, a cura della PA.

Sia le attività di consolidamento, che quelle di onboarding della LIS sono a carico della PA e pertanto non valutate nel presente Progetto.

5.5.2 Macro piano di setup e migrazione

Si riporta di seguito il piano di setup che fornisce un quadro sintetico del progetto di configurazione della nuova infrastruttura e della migrazione dell'Amministrazione, che seguirà le fasi dettate dal piano di progetto di implementazione del Sistema gestionale di laboratorio analisi e microbiologia, che si riporta di seguito. In questa fase si colloca la predisposizione dell'infrastruttura e del servizio PaaSDB in DR.

Si precisa che le date riportate sono da considerarsi indicative poiché relative ad attività il cui start-up è susseguente all'effettiva attivazione del contratto di servizio.



Il PSN intende attuare tutte le azioni di ottimizzazione possibili al fine di minimizzare eventuali slittamenti legati a tale data di avvio.

Le attività di migrazione verranno eseguite in autonomia dalla PA.

Per l'intero periodo di migrazione, il PSN mette a disposizione delle PA le seguenti figure professionali:

- Un **Project Manager di Contratto Adesione (PMCA)**, che coordina le attività e collabora col referente che ogni singola PA dovrà indicare e mettere a disposizione;
- Un **Technical Team Leader (TTL)** che segue tutte le fasi più strettamente legate agli aspetti operativi.

Si chiede alla PA la disponibilità di fornire uno o più Responsabili Tecnici coi quali il Project Manager e il Technical Team Leader del PSN si possano interfacciare.

Verranno inoltre condivisi:

- la lista dei deliverables di Progetto;
- la Matrice di Responsabilità;
- gli exit criteria di ogni fase di progetto;
- il Modello di comunicazione tra PSN e PA

Durante tutta la fase di setup e migrazione, verranno tenuti SAL con cadenza almeno mensile per valutare l'avanzamento del progetto.

5.6 Servizi professionali

Sono resi disponibili all'Amministrazione servizi professionali di evoluzione con l'obiettivo di: ✓ migliorare eventuali ambienti precedentemente migrati tramite Re-Host o direttamente configurati sulla piattaforma PSN; ✓ supportare la migrazione di applicativi on premise preesistenti per i sistemi di laboratorio (Es. per le Asl BI, ASL VCO, ASL VC) verso una piattaforma cloud tecnologicamente avanzata, in modo da beneficiare delle funzionalità messe a disposizione dall'infrastruttura proposta, come sicurezza, scalabilità e ottimizzazione di costi e risorse.

In particolare, quindi sono resi disponibili i servizi professionali per configurare le macchine con i relativi sistemi operativi, il PaasDB Oracle in Business Continuity e tutta la configurazione di rete e attività di rearchitect/replatform a supporto della PA.

5.6.1 Modalità di erogazione dei Servizi professionali

Data la natura delle attività e, allo stato attuale di conoscenza dei sistemi e infrastrutture che dovranno essere allestiti per il progetto e per quelli che dovranno migrare verso il cloud PSN, i servizi professionali saranno erogati secondo due principali modalità:

1. Servizi **"a task"**:
 - Servizi di migrazione;
 - Servizi professionali per il miglioramento della sicurezza delle infrastrutture e delle applicazioni della PA (ovvero, i Security Professional Services descritti ai §5.6.2.1, §5.6.2.2, 5.6.2.3.);
 - Servizi professionali evolutivi volti al ridisegno delle applicazioni in ottica Cloud (Re-platform, Re-architect).
2. Servizi **"Ricorrenti"**:
 - Servizi di Managed Services per garantire il mantenimento di funzionalità o ottimizzazione degli ambienti su cui insistono le applicazioni (IT Infrastructure Service Operations della piattaforma Database Oracle);

- Servizi di monitoraggio continuo della sicurezza (ovvero i Security Professional Services descritti ai §5.6.2.4, §5.6.2.5, §5.6.2.6).

In fase esecutiva, il PMCA (Project Manager di Contratto Adesione) del PSN ed il Referente del Contratto Esecutivo del AQ Applicativo dovranno collaborare per definire i task ed i servizi che dovranno essere pianificati e, successivamente, avviati, nel periodo in esame.

In particolare, per quanto riguarda i servizi a task, saranno identificate e pianificate insieme alla PA delle attività di lavorazione per tutti i servizi a task sopra citati. Per ciascun task l'Amministrazione fornirà al PSN, in una Richiesta di intervento formale, i requisiti, i deliverable e le tempistiche desiderate e successivamente il PSN:

- Eseguirà un'analisi dei requisiti;
- definirà lo skill Mix necessario all'esecuzione;
- valuterà il dimensionamento in termini di effort per singola figura professionale ed in termini di valore economico corrispondente;
- comunicherà all'Amministrazione il risultato della propria analisi e valutazione.

L'avvio delle attività per l'esecuzione di ogni task sarà effettivo solo previa approvazione formale da parte del Responsabile Tecnico dell'Amministrazione delle valutazioni e delle pianificazioni condivise.

Nell'ambito della fornitura, sempre di concerto con l'Amministrazione, si potranno definire nuovi task per ogni servizio, fino a consumo del budget proposto per il servizio stesso.

Analogamente, per quanto riguarda i servizi "Ricorrenti", l'Amministrazione fornirà al PSN, in una Richiesta formale di Servizio, i requisiti, i deliverable e le tempistiche di erogazione dei servizi stessi. Successivamente, il PSN analizzerà e dimensionerà i servizi richiesti e comunicherà alla Amministrazione la propria valutazione. L'avvio delle attività per l'esecuzione di ogni servizio sarà effettivo solo previa approvazione formale da parte del Responsabile Tecnico dell'Amministrazione delle valutazioni e delle pianificazioni condivise.

Una volta avviati i lavori, coerentemente con quanto previsto nello Schema di Contratto all'art. 11 (si veda par. 3.2), si prevede una milestone di rendicontazione e di fatturazione ogni due mesi per tutti i servizi in corso di erogazione.

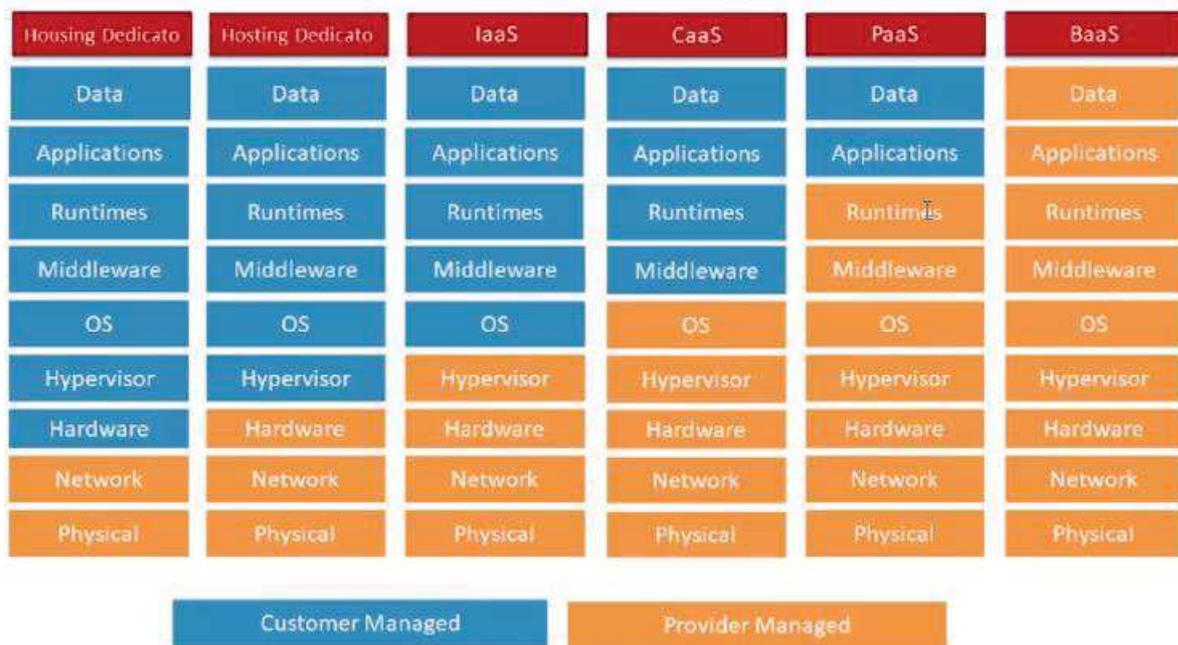
In particolare:

- I servizi a task saranno rendicontati e fatturati "a corpo" in giornate/uomo, tenendo conto dello stato avanzamento lavori (SAL) mensile e del mix professionale utilizzato.
- i Servizi "Ricorrenti" saranno rendicontati a SAL e remunerati in giornate/uomo, sulla base del mix professionale utilizzato per il servizio.

5.6.2 Security Profess. Services

Il PSN offre molti strumenti nativi, all'interno delle diverse tipologie di cloud scelte per gestire la sicurezza dei dati.

Il PSN nell'accettare la Lettera di Nomina (Allegato E-Nomina a Responsabile esterno del trattamento dei dati) si conforma a rispettare integralmente quanto in essa riportato ed in particolare quanto previsto nel paragrafo 6, punti e),f),i) e dei paragrafi 7 ed 8) nell'ambito della Matrice di Shared Responsibility di seguito riportato e comunque presente anche all'interno della Concessione:



A tali misure infrastrutturali e di processo di cui alla matrice soprastante, si affiancano i Security Professional Service presenti nel presente Progetto con piena facoltà dell'Amministrazione di decidere se utilizzarli o meno.

Il Polo può comunque supportare, ed implementare, concordandole con l'Amministrazione, tutte le misure necessarie atte a garantire la sicurezza dei dati Cliente trasferiti sul PSN, relativamente al nuovo sistema gestionale di laboratorio e microbiologia delle Aziende all'AIC N. 3. A tali misure infrastrutturali e di processo si affiancano le attività di gestione e miglioramento continuo anch'esse presenti nel Progetto.

I servizi sono necessari per:

- Garantire la conformità ai requisiti normativi e cogenti.
- Valutare e applicare le best practice di cloud security.
- Mitigare il rischio cyber.
- Valutare rischi e vulnerabilità prima e dopo il processo di migrazione.
- Prevedere, progettare ed implementare i controlli di sicurezza
- Supportare l'Amministrazione nella gestione della cybersicurezza.

Di seguito vengono illustrati i diversi step delle fasi di gestione della sicurezza implementabili tramite i servizi professionali in oggetto



Come già detto nel capitolo 5.5.1., alcuni servizi professionali di sicurezza sono attivati nelle fasi di cui si compone il progetto di migrazione come riportato in figura ed in particolare:

- Fase di Analisi/Discovery:
 - ICT Info gathering/Cyber Assessment, utilizzando il set di controlli definiti nell'ambito **FNCS** (Framework Nazionale di Sicurezza Cibernetica), integrato con le domande sul trattamento dei dati personali, definite dal **GDPR** (par.5.6.2.1.);
 - Maturity Level Assessment e Gap analysis tecnico/organizzativa dei controlli di sicurezza e roadmap in ottica «to-be» (par. 5.6.2.2);

Al termine della migrazione dei servizi al Secure Public Cloud, oltre a questi, saranno attivati in accordo con l'Amministrazione i seguenti servizi professionali di sicurezza che completano l'offerta e garantiscono il mantenimento dei livelli di sicurezza nel tempo:

- Vulnerability Assessment, Research & Exploitation (par.5.6.2.3);
- Servizio di supporto per attività di Security Device Management (Protezione Perimetrale) (par.5.6.2.4)
- Security Event Monitoring Notification & Log Management e Continuous Improvement (par. 5.6.2.5.);
- Supporto per l'erogazione del servizio di Managed Detection & Response (par. 5.6.2.6.).

5.6.2.1 ICT Info gathering/Cyber Assessment

Analisi preliminare volta a comprendere le attuali tecnologie utilizzate e le specifiche caratteristiche del perimetro oggetto di migrazione sulla base di opportune linee guida o best practice a partire dal regolamento europeo GDPR (UE 2016/679) ed il D.Lgs. 196/2003 e ss.mm.ii che trattano la protezione dei dati personali, le normative di riferimento principali sono la **direttiva NIS** e la sua attuazione tramite D. Lgs. 65 del 2018, e il **Perimetro di Sicurezza Nazionale Cibernetica**, istituito tramite il D.L. 105 del 2019 (convertito con modificazioni dalla Legge 133 del 2019) ed esteso da altre leggi e decreti; tra queste sicuramente riveste particolare importanza il Regolamento 628/2021 (e, nel rispetto degli atti esecutivi dello stesso Regolamento successivamente adottati dall'Agenzia per la cybersicurezza nazionale, d'intesa con il Dipartimento per la trasformazione digitale - le Determinazioni 306/2022 e 307/2022 e relativi allegati). L'analisi viene svolta secondo le seguenti attività operative:

- raccolta delle informazioni sulle tecnologie attualmente utilizzate dall'Amministrazione;
- analisi della fattibilità e classificazione sulla base di livelli di priorità delle tecnologie utilizzate;
- analisi degli impatti di situazioni di indisponibilità, per l'individuazione delle aree problematiche e contromisure tecnologiche da adottare.

5.6.2.2 Maturity Level Assessment e Gap Analysis

Il Servizio è erogato as a service ed ha lo scopo di effettuare una gap analysis preliminare dell'attuale contesto infrastrutturale ed applicativo al fine di definire il livello di sicurezza esistente e notificare un report operativo che descrive le necessità per il raggiungimento della conformità rispetto le normative vigenti e le best practices di riferimento, in particolare lo scopo del checkup di sicurezza è analizzare lo stato di maturità di tutti gli ambiti di sicurezza definiti dal Framework Nazionale per Cyber Security e la Data Protection (di seguito per brevità anche "FNCS") integrato con le raccomandazioni dettate dal DPCM 14 aprile 2021 n. 81/2021 in tema di Perimetro di Sicurezza Nazionale Cibernetica.

Verranno proposte una serie di domande attraverso le quali l'Amministrazione potrà acquisire gli elementi utili all'identificazione del miglior approccio cloud, specifico per il proprio contesto. Al completamento delle attività saranno consegnati i seguenti deliverable denominati:

- *GA Results Executive Summary*: Il report contiene una overview di tipo executive ad alto livello relativo al processo di valutazione che considera 4 aree 'chiave': *Business, Functional, Technical, Implementation*
- *GA Results Assessment Report*: Il report contiene i dettagli del processo di valutazione finalizzato ad indirizzare il corretto approccio alla migrazione relativamente alle 4 aree 'chiave' indicate: *Business, Functional, Technical, Implementation*.

5.6.2.3 Vulnerability Assessment, Research & Exploitation

Il servizio sarà erogato in modalità one shot da remoto e prevederà una fase di preparazione in funzione della soluzione target con l'esecuzione delle attività sottoelencate:

- redazione documentale: si procede alla redazione dei due documenti di Legal Agreement (LA) e di Rules Of Engagement (ROE).
- raccolta di informazioni: fase svolta al fine di reperire il maggior numero di informazioni sulla struttura della rete, delle componenti dei sistemi oggetto di analisi;
- individuazione delle vulnerabilità: tramite un set opportuno di strumenti automatizzati e correttamente configurati verrà collezionata una lista delle potenziali vulnerabilità note a cui potrebbero essere soggetti i sistemi analizzati;
- classificazione delle vulnerabilità: le vulnerabilità individuate saranno classificate in funzione di livelli di priorità d'intervento secondo lo standard CVSS.

Nel dettaglio, la fase operativa del servizio prevede:

- esecuzione one shot di un Vulnerability Assessment sul perimetro di indirizzamento IP interno (o privato);
- analisi dei risultati;
- individuazione delle vulnerabilità attraverso l'esecuzione di test ad hoc che consentano di accertare l'impatto sui sistemi in analisi;
- assegnazione delle priorità/severità ai rischi di sicurezza in base al contesto;
- correlazione dei risultati delle fasi precedenti e la definizione del piano di rientro (remediation plan).

Le attività oggetto di test saranno eseguite a valle della formalizzazione dei documenti riportati sotto.

- **Legal Agreement (Manleva)**: Un accordo stabilito tra le parti che autorizza il Security Assessment Team a svolgere le attività specifica e che lo scarica da responsabilità per eventuali danni o disservizi creati.
- **Regole di Ingaggio**: Documento che contiene indicazione di inizio e durata delle singole fasi, le finestre orario in cui verranno erogate le attività, l'elenco dei deliverable, l'assegnazione dei ruoli e delle responsabilità per il fornitore e l'Amministrazione e il perimetro oggetto di analisi.

Tali documenti costituiscono perimetro e modalità di esecuzione dei test e devono essere sottoposti ad accettazione e firma dal cliente, in mancanza delle quali non sarà possibile procedere all'esecuzione dei test. Oltre ai documenti di manleva e regole di ingaggio al completamento delle stesse saranno consegnati i seguenti deliverable denominati:

- *VA Results Executive Summary*: Il report contiene una overview di tipo executive ad alto livello delle vulnerabilità individuate, ordinate per livello di rischio;

- VA Results Technical Report: Il report contiene i dettagli delle vulnerabilità segnalate, ordinate per criticità (utilizzando il sistema CVSS), incluse gli entry-point e le contromisure suggerite.

I deliverable, in base alla complessità del perimetro, possono far parte di un unico documento di report. Il servizio è limitato all'analisi di una quantità massima di 250 IP.

5.6.2.4 Servizio di supporto per attività di Security Device Management (Protezione Perimetrale)

Il servizio professionale richiesto è orientato a supportare l'Amministrazione nella gestione e nel monitoraggio continuativo delle piattaforme di protezione perimetrale previste nell'ambiente Secure Public Cloud. Il servizio è erogato "Ricorrenti" remotamente ed include la gestione delle piattaforme di protezione perimetrale adottate, ovvero Azure Firewall e Application Gateway WAF con una finestra di servizio H8x5. Le attività comprese nel servizio sono:

- Definizione del perimetro di servizio: definizione della baseline dei sistemi di sicurezza che saranno oggetto del servizio Security Device Management, ovvero Azure Firewall e Application Gateway WAF;
- Definizione delle politiche di sicurezza: un'analisi globale dell'infrastruttura dei sistemi di sicurezza oggetto del servizio e dell'architettura complessiva prima della migrazione per configurare opportunamente le nuove piattaforme garantendo la connettività e allo stesso tempo l'esposizione minima necessaria;
- Presa in carico delle piattaforme, nello specifico le attività di presa in carico prevedono:
 - pianificazione temporale delle attività;
 - configurazione di utenze nominali per gli specialisti del SOC;
- Gestione a regime:
 - ogni richiesta viene validata ed implementata secondo le best practice di sicurezza ed in conformità a quanto definito con il Cliente in relazione anche alle policy aziendali vigenti.
 - i change, ad esempio, possono riguardare aggiunta/rimozione/modifica di policy Firewall o Web Application Firewall, creazione/modifica profili IDS/IPS etc.

Il servizio è erogato sul perimetro relativo all'infrastruttura LIS.

5.6.2.5 Security Event Monitoring Notification & Log Management e Continuous Improvement

Alla luce delle crescenti minacce informatiche per le organizzazioni, diventa fondamentale rivedere l'approccio alla gestione del rischio e individuare strategie per ridurre la vulnerabilità delle infrastrutture informatiche. Quindi per garantire l'adeguato livello di protezione delle reti, dei dati e dei servizi, diventa un fattore di primaria importanza l'individuazione e la gestione immediata degli incidenti di sicurezza.

In tale ottica il presente servizio, erogato remotamente da un Centro Servizi presidiato H24 per 365 giorni l'anno, garantisce un'attività di monitoraggio tramite un team di specialisti (Security Analyst, Security Solution architect, Information Security Consultant) in ambito sicurezza.

Il presente servizio utilizza la piattaforma di Security Information and Event Management (SIEM) che mette a disposizione il PSN contestualmente ai servizi infrastrutturali e, grazie a sistemi di indicizzazione e correlazione evoluti, fornisce il monitoraggio continuo degli eventi di sicurezza generati dalle componenti di sicurezza previste nel perimetro di gestione del Secure Device Management. Il servizio è progettato per identificare rapidamente risorse o eventi potenzialmente dannosi, anticipando tempestivamente i potenziali attacchi informatici o tentativi di attacco.

Il servizio, erogato in modalità H7x24 e si articola nelle seguenti fasi:

Onboarding/Startup: è la fase che precede l'avvio del servizio vero e proprio, con la presa in carico degli accessi alle piattaforme deputate alla "Detection", l'analisi degli allarmi configurati sulle stesse.

In caso di condivisione, da parte dell'Amministrazione, di regole di correlazione pre-esistenti, inerenti il perimetro di Cyber Security e finalizzate al miglioramento della capacità di Detection del servizio, potranno essere opportunamente integrate all'interno della soluzione prevista.

Continuous Monitoring: è la fase il cui avvio coincide con l'avvio del servizio, è a carattere continuativo ed è costituita da attività di monitoraggio degli allarmi (servizio Live/Running) ed eventi prodotti dalle piattaforme di sicurezza o di ticketing e dalle quali saranno estratte e analizzate le informazioni necessarie all'espletamento delle fasi successive.

Identification: è la fase in cui l'analista prende in carico un allarme di Sicurezza o una segnalazione e ne identifica i connotati principali al fine di procedere con la fase successiva. A titolo di esempio per ogni allarme preso in gestione vengono estratti se pertinenti i seguenti dati:

- La tipologia e/o regola di correlazione ad esso associata
- L'indirizzo IP della sorgente di attacco e della destinazione
- L'utente o gli utenti coinvolti
- Indirizzi email o caselle di posta compromessi
- Il nome e la tipologia del malware usato nell'attacco
- La vulnerabilità sfruttata e/o l'exploit utilizzato
- I riferimenti temporali dell'accaduto
- Lo stato del traffico e/o dell'azione (e.g. bloccato/non bloccato/non noto)

Classification: è la fase in cui l'analista dopo aver raccolto tutte le evidenze ed aver fatto una prima analisi dell'accaduto procede con la classificazione dell'evento in termini di categoria di minaccia e di livello di gravità/pericolosità. L'assegnazione del livello di criticità ad un allarme dipende da diversi fattori, tra i quali ad esempio:

- La tipologia di allarme/ anomalia;
- La criticità puntuale dell'asset coinvolto, ove per asset si intende non solo un PC/Server ma anche un utente o casella di posta o dispositivo di rete;
- La frequenza dell'allarme stesso.

Si propone a titolo di esempio la seguente matrice:

INCIDENT PRIORITY LEVELS		IMPACT (Asset)		
		Low	Medium	High
SEVERITY (Attack)	Low	Low	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	High

Tabella 12 Tabella di correlazione tra gravità incidenti e impatto sugli asset

INCIDENT PRIORITY	
Priority Levels	Descrizione
LOW	Gli incidenti non rappresentano un rischio immediato. Un workaround risolutivo è già disponibile o un piano di Remediation è facilmente realizzabile con azioni basilari.
MEDIUM	L'incidente riguarda le attività classificate come a medio impatto. Gli incidenti presentano una discreta probabilità di provocare danni all'infrastruttura, soprattutto se le azioni di Remediation non vengono implementate nel breve termine.
HIGH	Questo tipo di incidenti ha un'alta probabilità di causare, o ha già causato, una o più interruzioni dei servizi aziendali. La classificazione High solitamente riguarda gli incidenti su asset classificati come "business-critical".

Tabella 13 Descrizione dei livelli di incidente

Notification: è la fase di produzione dei deliverable previsti dal servizio ossia la fase in cui le informazioni estratte dalle piattaforme tecnologiche vengono normalizzate ed inserite in elementi di notifica.

Tuning: fase di supporto operativo verso i gestori delle piattaforme tecnologiche deputate alla "Detection" attivata nel caso di tuning necessario sulle stesse per limitare o azzerare l'incidenza di falsi positivi e del conseguente "rumore" da essi generato.

Il servizio di TRIAGE (identification, classification, notification) ha l'obiettivo di facilitare la messa a punto dei falsi positivi e di segnalare all'Amministrazione le anomalie reali. A titolo esemplificativo si riportano le seguenti statistiche legate al modello di servizio proposto:

PHASING		TIMING
TRI Phase 1	Avviso di presa in carico	15 minuti per il 90% dei casi di alta gravità
		4 ore per il 100% dei casi
TRI Phase 2	Classificazione e notifica anomalie (a partire da Phase 1)	30 minuti per il 90% dei casi
		4 ore per il 100% dei casi

Tabella 14 Modello di servizio per il Triage

Processo di Analisi ed Incident Notification

Il processo di Incident Notification ha come obiettivo la rapida e corretta comunicazione agli attori interessati. Il processo alla base è lo standard previsto dall'incident management per le comunicazioni e le escalation. A tale proposito, nel corso della fase di avvio del servizio saranno identificate le opportune interfacce competenti per la ricezione delle notifiche in funzione della classe degli asset coinvolti e della criticità dell'incidente.

Di seguito viene descritta la procedura operativa prevista per il sotto-processo di Incident Notification:

- In caso di rilevazione di un incidente, l'operatore del SOC procede con l'apertura di una nuova segnalazione (ticket di Incident Notification), oppure se già presente aggiorna l'esistente segnalazione;
- L'operatore SOC prende in carico il ticket di Incident Notification.
- L'operatore SOC procede quindi alla verifica di dettaglio dell'evento, definendo se si tratta di un incidente normale o critico
- In caso di Incident, si procede ad inviare una notifica ai referenti cliente

Reporting

Il servizio produce due tipologie di report:

- *Executive Summary*, un rapporto di sintesi destinato prevalentemente al management e al personale non tecnico per una comprensione immediata degli attacchi riscontrati. Si tratta di un elaborato in Excel contenente tutti i dati relativi ai KPI di servizio.
- *Technical Report* una scheda incidente con tutte le indicazioni necessarie per la comprensione dei problemi riscontrati, per la loro classificazione in termini di severità e con un suggerimento relativo alle misure più idonee da adottare per la loro risoluzione. Tale rapporto fornirà il dettaglio delle principali vulnerabilità/minacce riscontrate.

Continuous Improvement

Le attività sono finalizzate ad eseguire un tuning specifico sulle piattaforme contenute nel perimetro di interesse del servizio. Le attività di Continuous Improvement consentono nel tempo un evidente beneficio, migliorando la risposta dei sistemi di Security Event Monitoring a fronte dell'insorgere di nuove minacce, consentendo una maggiore coerenza delle politiche di sicurezza implementate e nel rispetto delle modalità organizzative adottate dall'Amministrazione.

Il servizio è erogato sul perimetro relativo all'infrastruttura LIS e fino a 500 EPS (Eventi Per Secondo).

5.6.2.6 Supporto per l'erogazione del servizio di Managed Detection & Response

Nel presente paragrafo è descritto il servizio professionale di supporto alle attività di Managed Detection & Response (MDR) e di seguito rappresentate:

- Ridurre al minimo le possibili finestre d'esposizione a eventuali attacchi informatici per gli endpoint in perimetro (con agent installato);
- Remediation automatica (ove applicabile) per gli incident riconosciuti come "veri positivi" ed a criticità massima;

- Endpoint protetti anche in assenza momentanea di connessione ad internet (in funzione del tipo di soluzione tecnologica presente);
- Possibilità di isolare dalla rete endpoint compromessi conservandone il controllo dalla piattaforma in cloud internet (in funzione del tipo di soluzione tecnologica presente);
- Protezione in tempo reale da attacchi sconosciuti e che non utilizzano metodologie e/o indicatori noti internet (limitatamente alle caratteristiche della soluzione tecnologica impiegata);

Il servizio MDR è erogato dal PSN ed utilizzerà l'attuale soluzione presente sugli ambienti Secure Public Cloud. Il servizio è erogato as a service ed include un monitoraggio continuativo con finestra di servizio H24 per 365 giorni.

Il servizio è erogato sul perimetro relativo all'infrastruttura LIS.

5.6.3 IT infrastructure service operations

In seguito all'avvenuta migrazione, il PSN, renderà disponibili servizi di IT infrastructure-service operations per garantire il mantenimento di funzionalità o ottimizzazione degli ambienti su cui insistono le applicazioni. Pertanto, l'Amministrazione potrà decidere di affidare al PSN la gestione dell'ambiente tenendo per sé solamente la componente relativa al codice applicativo. Per il corretto svolgimento delle attività verrà reso disponibile, un Service Manager; un professionista di esperienza che coordina la gestione dei servizi di gestione contrattualizzata, operando a diretto contatto con l'Amministrazione. È responsabile della qualità del servizio offerto, e costituisce un punto di riferimento diretto del cliente per analisi congiunte del servizio, escalation, chiarimenti, personalizzazioni.

Il servizio di IT Infrastructure service operations è riferito alla fornitura della piattaforma database Oracle, "as a Service" e comprende, in accordo con i requisiti delle Aziende dell'AIC3, le seguenti attività:

- Configurazione e gestione dei server fisici a supporto della piattaforma Database Aggiornamento del sistema operativo e implementazione patch di sicurezza
- Configurazione e gestione dei meccanismi di replica dati tra le due Availability Zone primario e standby (Oracle Active Dataguard)
- Monitoraggio e gestione degli allarmi tecnologici relativi allo stato della piattaforma database provenienti dagli strumenti di controllo e automazione (storage disponibile, CPU, errori nei logs, ecc...)
- Esecuzione e manutenzione delle procedure di backup previste dal contratto sulla piattaforma Database
- Istanza Database e Dati Aggiornamenti software della piattaforma Oracle e gestione patch
- Creazione e Modifica Tablespace
- Gestione delle utenze tecniche necessarie ai servizi applicativi della LIS
- Analisi delle prestazioni per evidenziare inefficienze o criticità nell'interazione con i dati contenuti nell'istanza database
- Gestione del ripristino dati a fronte di problemi software o necessità delle Amministrazioni
- Monitoraggio e gestione degli allarmi tecnologici relativi allo stato dell'istanza database provenienti dagli strumenti di controllo e automazione (funzionamento dell'istanza, saturazione tablespace)

Per maggior chiarezza di seguito si riporta la matrice RACI, per la piattaforma Oracle con i relativi servizi di DR e Business Continuity:

DATA BASE ADMINISTRATION - DB as a Service Licensed Oracle - managed	Responsabile	Autorizzatore	Consultato	Informato
Fornitura licenze database	PA		PSN	PA
Gestione e verifica Licensing per DBMS	PA		PSN	PA
Definizione template database	PA	PA	PSN	PA
Definizione configurazione iniziale database e utenti	PA	PA	PSN	PA
Predisposizione DBaaS	PSN	PA	PA	PA
Definizione policies di sicurezza su DB	PA	PA	PSN	PA
Creazione, securizzazione e configurazione DB	PSN	PSN	PA	PA
Start-up, restart, shutdown pianificato e su richiesta del DB	PSN	PA		PA
Eventuale riorganizzazione tablespaces ecc	PA	PA	PSN	
Patch DBMS	PSN	PA	PA	PA
Creazione/reset/cancellazione/profilazione utenti DB	PSN	PA	PA	PA
Analisi performance e tuning DB	PSN	PA	PA	
Analisi allocazione spazio DB	PSN	PSN	PA	
Import/Export dati	PSN	PA	PA	
Analisi log, gestione policy/verbosità log	PSN	PA	PA	PA
Troubleshooting	PA-PSN	PA	PA-PSN	PA
Backup dati	PSN	PSN	PA	PA
Restore dati	PSN	PA	PA	PA
Monitoraggio	PSN	PSN	PA	PA
Disaster Recovery e Business Continuity	Responsabile	Autorizzatore	Consultato	Informato
Progettazione soluzioni DR-BC per rispetto RTO-RPO	PA - PSN	PA		
Allestimento repliche servizi IaaS e DBaaS managed	PSN	PSN	PA	PA
Predisposizione repliche applicative	PA	PA	PSN	PA
Predisposizione documentazione Disaster Recovery	PA - PSN	PA	PSN	PA
Mantenimento documentazione Disaster Recovery	PA - PSN	PA	PSN	PA
Dichiarazione Evento Disastroso su datacenter PSN	PSN	PSN		PA
Attuazione procedure DR infrastrutture e servizi cloud	PSN	PSN		PA
Attuazione procedure ripristino servizi applicativi	PA	PA	PSN	PA
Collaudo servizio riattivato presso sito di DR	PA	PA	PSN	
Dichiarazione fine Evento DR	PSN	PSN		PA
Ritorno alla normalità	PA-PSN	PA		

Legenda
PSN: Polo Strategico Nazionale
PA: AIC numero 3

Per tali servizi verrà proposto un **team mix** composto dal mix dei profili professionali elencati in precedenza, in base all'ambiente dell'Amministrazione ed ai requisiti della stessa.

6 FIGURE PROFESSIONALI

PSN rende disponibili risorse professionali in grado di poter supportare l'Amministrazione nelle diverse fasi del progetto, a partire dalla definizione della metodologia di migrazione (re-architect, re-platform), proseguendo nella fase di riavvio degli applicativi, regression test e terminando nel supporto all'esercizio.

Per ogni progetto viene individuato il mix di figure professionali necessarie, tra quelle messe a disposizione del PSN, che effettuerà le attività richieste. Si rimanda al par. 8 Configuratore per il dettaglio dell'effettivo impegno delle risorse professionali previste per tale progetto. Il team reso disponibile per questo progetto è composto dalle seguenti figure professionali, i cui profili sono di seguito descritti:

- **Project Manager:** definisce e gestisce i progetti, adottando e promuovendo metodologie agili; è responsabile del raggiungimento dei risultati, conformi agli standard di qualità, sicurezza e sostenibilità, in coerenza con gli obiettivi, le performance, i costi ed i tempi definiti.
- **Cloud Security Specialist:** esperto nella progettazione di architetture di sicurezza per sistemi basati su cloud (public ed hybrid). È responsabile per il supporto alla realizzazione delle architetture di sicurezza dei nuovi workload delle Amministrazioni e alle attività di migrazione, fornisce indicazioni e raccomandazioni strategiche ai team operativi e di sviluppo per affrontare i punti deboli della sicurezza e identificare potenziali nuove soluzioni di sicurezza negli ambienti cloud
- **Database Specialist and Administrator:** È responsabile dell'installazione, dell'aggiornamento, della migrazione e della manutenzione del DBMS; si occupa di strutturare e regolamentare l'accesso ai DB, monitorarne l'utilizzo, ottimizzarne le prestazioni e progettare strategie di backup
- **System and Network Administrator:** ha competenze sui sistemi operativi, framework di containerizzazione, tecnologie di virtualizzazione, orchestratori e sistemi di configuration e versioning; è responsabile della implementazione di sistemi di virtualizzazione, di container utilizzando anche sistemi di orchestrazione e della manutenzione, della configurazione e del funzionamento dei sistemi informatici di base.
- **System Architect:** ha consolidata esperienza in technical/service management e project management, analizza i sistemi esistenti e definisce come devono essere coerentemente integrate le nuove soluzioni; è responsabile della progettazione della soluzione infrastrutturale e del coordinamento di specifici stream di progetto
- **Product/Network/Technical Specialist:** È responsabile delle attività inerenti all'integrazione delle soluzioni tecniche ed il supporto specialistico di prodotto nell'ambito dell'intervento progettuale.
- **Security Principal:** Definisce, implementa e gestisce progetti dal concepimento iniziale alla consegna finale. Responsabile dell'ottenimento di risultati ottimali, conformi agli standard di qualità, sicurezza e sostenibilità nonché coerenti con gli obiettivi, le performance, i costi ed i tempi definiti.
- **Senior Information Security Consultant:** Presidia l'attuazione della strategia definita all'interno del suo ambito di responsabilità (sia questo un progetto, un processo, una location) coordinando attivamente le eventuali figure operative a lui assegnate per tale scopo, rappresentando il naturale raccordo tra la struttura di governance della cyber security e il resto del personale operativo. Controlla il rispetto alle regole definite e del cogente in materia di sicurezza delle informazioni. Pianifica ed attua misure di sicurezza per proteggere le reti e i sistemi informatici di un'organizzazione.
- **Senior Security Auditor/Analyst:** Garantisce la conformità con le procedure di controllo interno stabilite esaminando i registri, i rapporti, le pratiche operative e la documentazione. 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. Completa i giornali di audit documentando test e risultati dell'audit.

- **Security Solution Architect:** Progetta, costruisce, esegue test e implementa i sistemi di sicurezza all'interno della rete IT di un'organizzazione. Ha l'obiettivo di anticipare tutte le potenziali mosse e tattiche che eventuali criminali possono utilizzare per cercare di ottenere l'accesso non autorizzato al sistema informatico tramite la progettazione di un'architettura di rete sicura.
- **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.
- **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.
- **Junior Penetration Tester:** Effettua tentativi di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza in accordo con quanto definito le progetto di riferimento.

7 SICUREZZA

All'interno del PSN è presente una Organizzazione di Sicurezza, con elementi caratteristici di autonomia e indipendenza. Tale unità è anche preposta alle attività aziendali rilevanti per la sicurezza nazionale ed è coinvolta nelle attività di governance, in particolare riguardo ai processi decisionali afferenti ad attività strategiche e di interesse nazionale.

Le misure tecniche ed organizzative del PSN sono identificate ed implementate ai sensi delle normative vigenti elaborate a cura dell'Organizzazione di Sicurezza, in particolare con riferimento alla sicurezza e alla conformità dei sistemi informatici e delle infrastrutture delle reti, in totale allineamento e coerenza con i criteri di accreditamento AgID relativi ai PSN.

Con la sottoscrizione del presente Progetto del Piano dei Fabbisogni, l'Amministrazione accetta tutte le policy di sicurezza di PSN.

Le policy di sicurezza delle informazioni di PSN delimitano e regolano le aree di sicurezza applicabili ai Servizi PSN e all'uso che l'Amministrazione fa di tali Servizi. Il personale di PSN (compresi dipendenti, appaltatori e collaboratori a tempo determinato) è tenuto al rispetto delle prassi di sicurezza dei dati di PSN e di eventuali policy supplementari che regolano tale utilizzo o i servizi che forniscono a PSN.

Per i Servizi che non sono inclusi nella fornitura e per i quali l'Amministrazione autonomamente configura un comportamento di sicurezza, se non diversamente specificato, resta a carico dell'Amministrazione la responsabilità della configurazione, gestione, manutenzione e protezione dei sistemi operativi e di altri software associati a tali Servizi non forniti da PSN.

8 CONFIGURATORE

Di seguito, l'export del Configuratore contenente tutti i servizi della soluzione con la relativa sintesi economica in termini di canone annuo e UT. La durata contrattuale (prevista per un massimo di 10 anni) dei servizi contenuti nel presente progetto sarà declinata all'interno del contratto di utenza.

Tutti i servizi verranno contrattualizzati e fatturati a ciascuna Azienda dell'AIC num. 3 sulla base della seguenti proporzioni complessive:

- AOU Maggiore Novara: 24,5%
- ASL NO: 19,50%
- ASL BI: 19,25%
- ASL VC: 18,75%
- ASL VCO: 18,00%

ANAGRAFICA AMMINISTRAZIONE	
Codice Fiscale	n.a.
Ragione Sociale	AIC numero 3
IDENTIFICATIVO DOCUMENTO	
Emesso da	CSO
Codice Documento	2023- 2023-0000001521330033-PdF-P1R1
Versione	1

VERSIONE CONFIGURATORE	2.3
------------------------	-----

RIEPILOGO PREZZI			
SERVIZIO	Totale UT	Totale Canone Annuale	Totale Canone 10 anni
Industry Standard		€ 548.088,00	€ 5.480.880,00
Hybrid Cloud on PSN Site		€ -	€ -
SecurePublicCloud Anno 1		€ 332.058,97	€ 332.058,97
SecurePublicCloud Anni 2-10 (9 anni)		€ 384.087,28	€ 3.456.785,52
Public Cloud PSN Managed		€ -	€ -
Servizi di Migrazione	€ 120.263,65		
Servizi Professionali			€ 1.810.118,30
TOTALI	Anno 1	€ 120.263,65	€ 880.146,97
	Anni 2-10		€ 932.175,28
Totale generale		€ 11.200.106,44	

Nei paragrafi seguenti vengono esposti i valori globali per l'infrastruttura e i servizi professionali precedentemente descritti.

8.1.1 Infrastruttura Secure Public Cloud Azure e DB as a Service Oracle e relativi servizi

Al fine di ottimizzare le componenti infrastrutturali, esse verranno rilasciate in tre fasi distinte, la cui tempistica è studiata per supportare al meglio la pianificazione del progetto di implementazione del Sistema gestionale di laboratorio analisi e microbiologia.

Le fasi di rilascio della infrastruttura con i relativi valori vengono sintetizzate nella tabella di seguito, la prima fase è da intendersi con partenza da t0 del progetto:

	Modalità di erogazione componenti Azure	Durata	Importo (inclusa piattaforma DBaaS Oracle)
Fase 1	Ambienti di Test e collaudo - Azure Compute a consumo	4 Mesi	234.717,23 €
Fase 2	Ambienti di Test e collaudo + produzione - Azure Compute a consumo	3 Mesi	257.032,25 €
Fase 3	Ambienti di Test e collaudo a Consumo - Produzione Reserved a 3 anni	113 Mesi	8.777.986,62 €
	Totali	120 Mesi	9.269.736,10 €

Tabella 15 Importi per singola fase

Nelle pagine seguenti sono riportati i valori calcolati sulla base del configuratore.

Fase 1

ANAGRAFICA AMMINISTRAZIONE		Codice Fiscale		AIC numero 3	
Codice Regione Sociale					
DESCRIZIONE TIPO DOCUMENTO					
Emissione da		CISG			
Codice Documento		2023-000001521330033-PdF-P1R1			
Versione		1			
VERSIONE CONFIGURATORE					
		3.3			
SERVIZIO		RIEPILOGO PREZZI			
		Totale UT	Totale Canone Annuale		
Industry Standard		€	548.088,00		
Hybrid Cloud on PSN Site		€	-		
SecurePublicCloud		€	384.087,28		
Public Cloud PSN Managed		€	-		
Servizi di Migrazione		€	-		
Servizi Professionali		€	-		
TOTALE		€	932.175,28		

CODICE	SERVIZIO	TIPOLOGIA	ELEMENTO	QUANTITA'	UT	Totale UT	Totale Canone Annuale
SEC-MS-27	SecurePublicCloudAzura	Computeconsumo	VM "convenzionali" - c24	10		€	7.506,2640
SEC-MS-28	SecurePublicCloudAzura	Computeconsumo	VM "convenzionali" - c28	9		€	8.500,8620
SEC-MS-29	SecurePublicCloudAzura	Computeconsumo	VM "convenzionali" - c216	4		€	4.887,7944
SEC-MS-32	SecurePublicCloudAzura	Computeconsumo	VM "convenzionali" - c4S2	18		€	37.502,3536
SEC-MS-33	SecurePublicCloudAzura	Computeconsumo	VM "convenzionali" - c816	6		€	14.948,4580
SEC-MS-35	SecurePublicCloudAzura	Computeconsumo	VM "convenzionali" - c8S4	10		€	46.888,8010
SEC-MS-36	SecurePublicCloudAzura	Computeconsumo	VM "convenzionali" - c16S2	10		€	59.877,2470
SEC-MS-42	SecurePublicCloudAzura	Storage	Managed Disks - dischi SSD Standard (128 GB)	31		€	3.144,4478
SEC-MS-43	SecurePublicCloudAzura	Storage	Managed Disks - dischi SSD Premium (128 GB)	23		€	5.265,0404
SEC-MS-44	SecurePublicCloudAzura	Network	Connection Gateway - ore di servizio	21900		€	12.186,7800
SEC-MS-45	SecurePublicCloudAzura	Network	Bandwidth - GB per anno	5120		€	112,6400
SEC-MS-46	SecurePublicCloudAzura	Network	Speed - Giorni di attivazione	365		€	9.034,0180
SEC-MS-47	SecurePublicCloudAzura	Network	Bandwidth Internet - TB annuali	2		€	154,0082
SEC-MS-54	SecurePublicCloudAzura	PublicCloudSecurityBackupSIEM	SIEM service - GB per giorno	10		€	8.237,4200
SEC-MS-55	SecurePublicCloudAzura	PublicCloudSecurityBackupSIEM	SIEM Data Ingestion - GB per giorno	15		€	11.841,4560
SEC-MS-56	SecurePublicCloudAzura	PublicCloudSecurityBackupSIEM	SIEM Data retention (6 mesi) - GB per giorno	15		€	1.878,4035
SEC-MS-57	SecurePublicCloudAzura	PublicCloudSecurityBackupMonitor	Monitor VM Data Ingestion - GB per giorno	9		€	7.104,8736
SEC-MS-59	SecurePublicCloudAzura	PublicCloudSecurityBackupFirewall	Deployment - Istanze	1		€	13.490,0455
SEC-MS-60	SecurePublicCloudAzura	PublicCloudSecurityBackupFirewall	Data managed - TB mese	10		€	1.730,8360
SEC-MS-61	SecurePublicCloudAzura	PublicCloudSecurityBackupCloudBackup	Istanze Profatte - Numero VM	70		€	7.433,4980
SEC-MS-62	SecurePublicCloudAzura	PublicCloudSecurityBackupCloudBackup	Storage occupato GB	3500		€	876,7500
SEC-MS-30	SecurePublicCloudAzura	Computeconsumo	VM "convenzionali" - c48	20		€	29.984,3320
SEC-MS-31	SecurePublicCloudAzura	Computeconsumo	VM "convenzionali" - c416	20		€	38.931,9200
SEC-MS-34	SecurePublicCloudAzura	Computeconsumo	VM "convenzionali" - c8S2	0		€	-
SEC-MS-03	SecurePublicCloudAzura	ComputeProduction	VM "convenzionali" c204	7		€	2.005,3201
SEC-MS-04	SecurePublicCloudAzura	ComputeProduction	VM "convenzionali" c208	8		€	3.412,5816
SEC-MS-06	SecurePublicCloudAzura	ComputeProduction	VM "convenzionali" c408	15		€	8.512,0485
SEC-MS-07	SecurePublicCloudAzura	ComputeProduction	VM "convenzionali" c416	26		€	23.896,7092
SEC-MS-10	SecurePublicCloudAzura	ComputeProduction	VM "convenzionali" c8S2	10		€	17.069,0780
PAA304	IndustryStandard	PaasDB	Oracle dbms Enterprise	41		€	548.088,0000

Il valore annuale deve essere riproporzionato alla effettiva durata della fase 1, pari a 4 mesi, corrispondente a quello riportato in tabella 15.

Fase 2

SERVIZIO		RIEPILOGO PREZZI		Totale Canone Annuale	
		Totale UT			
Industry Standard		€	-	€	548.088,00
Hybrid Cloud on PSN Site		€	-	€	-
SecurePublicCloud		€	-	€	480.004,69
Public Cloud PSN Managed		€	-	€	-
Servizi di Migrazione		€	-	€	-
Servizi Professionali		€	-	€	-
TOTALE		€	-	€	1.028.092,69

CODICE	SERVIZIO	TIPOLOGIA	ELEMENTO	QUANTITA'	OR	Totale UT	Totale Canone Annuale
SEC-MS-27	SecurePublicCloudAz-UEB	Computeaconsumo	VM "convenzionali" - c2r4	28			€ 21.269.5392
SEC-MS-28	SecurePublicCloudAz-UEB	Computeaconsumo	VM "convenzionali" - c2r8	23			€ 21.235.8540
SEC-MS-29	SecurePublicCloudAz-UEB	Computeaconsumo	VM "convenzionali" - c2r16	19			€ 22.267.0234
SEC-MS-32	SecurePublicCloudAz-UEB	Computeaconsumo	VM "convenzionali" - c4r32	29			€ 67.973.0159
SEC-MS-33	SecurePublicCloudAz-UEB	Computeaconsumo	VM "convenzionali" - c8r16	21			€ 62.775.1236
SEC-MS-35	SecurePublicCloudAz-UEB	Computeaconsumo	VM "convenzionali" - c8r64	5			€ 23.434.4005
SEC-MS-36	SecurePublicCloudAz-UEB	Computeaconsumo	VM "convenzionali" - c16r32	4			€ 23.950.8988
SEC-MS-42	SecurePublicCloudAz-UEB	Storage	Managed Disks - dischi SSD Standard (128 GB)	40			€ 4.057.3520
SEC-MS-43	SecurePublicCloudAz-UEB	Storage	Managed Disks - dischi SSD Premium (128 GB)	17			€ 3.891.5516
SEC-MS-44	SecurePublicCloudAz-UEB	Network	Connection Gateway - ore di servizio	21900			€ 12.180.7800
SEC-MS-45	SecurePublicCloudAz-UEB	Network	Bandwidth - GB per anno	5120			€ 112.6400
SEC-MS-46	SecurePublicCloudAz-UEB	Network	Speed - Giorni di accensione	365			€ 9.034.9180
SEC-MS-47	SecurePublicCloudAz-UEB	Network	Bandwidth Internet - TB annui	1			€ 77.0041
SEC-MS-54	SecurePublicCloudAz-UEB	PublicCloudSecurityBackupSIEM	SIEM service - GB per giorno	10			€ 8.237.4260
SEC-MS-55	SecurePublicCloudAz-UEB	PublicCloudSecurityBackupSIEM	SIEM Data Ingestion - GB per giorno	15			€ 11.841.4560
SEC-MS-56	SecurePublicCloudAz-UEB	PublicCloudSecurityBackupSIEM	SIEM Data retention (6 mesi) - GB per giorno	15			€ 1.878.4035
SEC-MS-57	SecurePublicCloudAz-UEB	PublicCloudSecurityBackupMonitor	Monitor VM Data ingestion - GB per giorno	9			€ 7.104.8736
SEC-MS-59	SecurePublicCloudAz-UEB	PublicCloudSecurityBackupFirewall	Deployment - Istanze	1			€ 13.490.9465
SEC-MS-60	SecurePublicCloudAz-UEB	PublicCloudSecurityBackupFirewall	Data managed - TB mese	10			€ 1.730.6360
SEC-MS-61	SecurePublicCloudAz-UEB	PublicCloudSecurityBackupCloudBackup	Istanze Protette - Numero VM	70			€ 7.433.4680
SEC-MS-62	SecurePublicCloudAz-UEB	PublicCloudSecurityBackupCloudBackup	Storage occupato GB	3500			€ 876.7500
SEC-MS-30	SecurePublicCloudAz-UEB	Computeaconsumo	VM "convenzionali" - c4r8	27			€ 40.478.8462
SEC-MS-31	SecurePublicCloudAz-UEB	Computeaconsumo	VM "convenzionali" - c4r16	22			€ 40.625.1120
SEC-MS-34	SecurePublicCloudAz-UEB	Computeaconsumo	VM "convenzionali" - c8r32	20			€ 74.046.6720
PAAS04	IndustryStandard	PaaSOB	Oracle dbms Enterprise	41			€ 548.088.0000

Il valore annuale riportato nella tabella del configuratore deve essere riproporzionato alla effettiva durata della fase 2, pari a 3 mesi, corrispondente a quello riportato in tabella 15.

Fase 3

ANAGRAFICA AMMINISTRAZIONE		Polo Strategico Nazionale	
Codice Fiscale		A/C numero 3	
IDENTIFICATIVO DOCUMENTO			
Emesso da		CSG	
Codice Documento	2023-000001521330033-PdF-P1R1		
Versione		1	
VERSIONE CONFIGURATORE		3.3	
RIEPILOGO PREZZI			
SERVIZIO	Totale UT	Totale Canone Annuale	
Industry Standard		€ 548.088,00	
Hybrid Cloud on P8N Site		€ -	
SecurePublicCloud		€ 864.087,26	
Public Cloud P8N Managed		€ -	
Servizi di Migrazione		€ -	
Servizi Professionali		€ -	
TOTALE		€ 1.412.175,26	

CODICE	SERVIZIO	TIPOLOGIA	ELEMENTO	QUANTITA'	DR	Totale UT	Totale Canone Annuale
SEC-MS-27	SecurePublicCloudAz	Computeconsumo	VM "convenzionali" - c2x4	10		€	7.506,2640
SEC-MS-28	SecurePublicCloudAz	Computeconsumo	VM "convenzionali" - c2x8	9		€	8.309,6820
SEC-MS-29	SecurePublicCloudAz	Computeconsumo	VM "convenzionali" - c2x16	4		€	4.687,7944
SEC-MS-32	SecurePublicCloudAz	Computeconsumo	VM "convenzionali" - c4x22	18		€	37.502,3536
SEC-MS-33	SecurePublicCloudAz	Computeconsumo	VM "convenzionali" - c8x16	5		€	14.946,4580
SEC-MS-35	SecurePublicCloudAz	Computeconsumo	VM "convenzionali" - c8x24	10		€	48.868,8010
SEC-MS-38	SecurePublicCloudAz	Computeconsumo	VM "convenzionali" - c16x22	10		€	59.877,2470
SEC-MS-42	SecurePublicCloudAz	Storage	Managed Disks - disks SSD Standard (128 GB)	31		€	3.144,4478
SEC-MS-43	SecurePublicCloudAz	Storage	Managed Disks - disks SSD Premium (128 GB)	23		€	6.285,0404
SEC-MS-44	SecurePublicCloudAz	Network	Connection Gateway - ore di servizio	21900		€	12.180,7600
SEC-MS-45	SecurePublicCloudAz	Network	Bandwidth - GB per anno	5120		€	112,6400
SEC-MS-46	SecurePublicCloudAz	Network	Speed - Giorni di accelerazione	365		€	9.034,9180
SEC-MS-47	SecurePublicCloudAz	Network	Bandwidth Internet - TB annui	2		€	154,0082
SEC-MS-54	SecurePublicCloudAz	PublicCloudSecurityBackupSIEM	SIEM service - GB per giorno	10		€	8.237,4260
SEC-MS-55	SecurePublicCloudAz	PublicCloudSecurityBackupSIEM	SIEM Data Ingestion - GB per giorno	15		€	11.841,4580
SEC-MS-56	SecurePublicCloudAz	PublicCloudSecurityBackupSIEM	SIEM Data retention (6 mesi) - GB per giorno	15		€	1.878,4035
SEC-MS-57	SecurePublicCloudAz	PublicCloudSecurityBackupMonitor	Monitor VM Data Ingestion - GB per giorno	9		€	7.104,8736
SEC-MS-59	SecurePublicCloudAz	PublicCloudSecurityBackupFirewall	Deployment - istanze	1		€	13.400,9455
SEC-MS-60	SecurePublicCloudAz	PublicCloudSecurityBackupFirewall	Data managed - TB mese	10		€	1.730,8380
SEC-MS-61	SecurePublicCloudAz	PublicCloudSecurityBackupCloudBackup	Istanze Protatte - Numero VM	70		€	7.433,4680
SEC-MS-62	SecurePublicCloudAz	PublicCloudSecurityBackupCloudBackup	Storage occupato GB	3500		€	878,7500
SEC-MS-30	SecurePublicCloudAz	Computeconsumo	VM "convenzionali" - c4x8	20		€	29.984,3320
SEC-MS-31	SecurePublicCloudAz	Computeconsumo	VM "convenzionali" - c4x16	20		€	38.931,6200
SEC-MS-34	SecurePublicCloudAz	Computeconsumo	VM "convenzionali" - c8x32	0		€	-
SEC-MS-03	SecurePublicCloudAz	ComputeProduction	VM "convenzionali" P2x4	7		€	2.005,3201
SEC-MS-04	SecurePublicCloudAz	ComputeProduction	VM "convenzionali" P2x8	8		€	3.412,5816
SEC-MS-06	SecurePublicCloudAz	ComputeProduction	VM "convenzionali" P4x8	15		€	6.512,9485
SEC-MS-07	SecurePublicCloudAz	ComputeProduction	VM "convenzionali" P4x16	28		€	23.806,7092
SEC-MS-10	SecurePublicCloudAz	ComputeProduction	VM "convenzionali" c8x32	10		€	17.069,0780
PAAS04	IndustryStandard	PaasDB	Oracle dbms Enterprise	41		€	548.088,0000

Il valore complessivo dei canoni per la fase 3 sono riportati in Tabella 15.

8.2 Servizi professionali

Una volta avviati i lavori, coerentemente con quanto previsto nello Schema di Contratto all'art. 11 (si veda par. 3.2), si prevede una milestone di rendicontazione e di fatturazione ogni due mesi per tutti i servizi in corso di erogazione, come già descritto nel §5.6.1:

- I servizi a task saranno rendicontati e fatturati "a corpo" in giornate/uomo, tenendo conto dello stato avanzamento lavori (SAL) mensile e del mix professionale utilizzato.
- i Servizi "Ricorrenti" saranno rendicontati a SAL e remunerati in giornate/uomo, sulla base del mix professionale utilizzato per il servizio.

8.2.1 Fase iniziale migrazione, start-up e rilascio servizi di piattaforma

Servizi erogati **Una Tantum** in fase di rilascio dei servizi di piattaforma

Stato Avanzamento Lavori (SAL) mensile con fatturazione bimestrale: UT di servizio erogato da T0 a T0 + 5 mesi.

ANAGRAFICA AMMINISTRAZIONE	
Codice Fiscale	
Ragione Sociale	AIC numero 3
IDENTIFICATIVO DOCUMENTO	
Emesso da	CSO
Codice Documento	2023-0000001521330033-PdF-P1R1
Versione	1

VERSIONE CONFIGURATORE	2.3
------------------------	-----



RIEPILOGO PREZZI			
SERVIZIO	Totale UT	Totale Canone Annuale	Totale Canone 10 anni
Industry Standard		€ -	€ -
Hybrid Cloud on PSN Site		€ -	€ -
SecurePublicCloud		€ -	€ -
Public Cloud PSN Managed		€ -	€ -
Servizi di Migrazione	€ 120.263,65		
Servizi Professionali	€ -		
TOTALE	€ 120.263,65	€ -	€ -

CODICE	SERVIZIO	TIPOLOGIA	ELEMENTO	QUANTITA'	DR
SP-01	ServiziMigrazione	FiguraMigrazione	Cloud Application Architect	38	
SP-04	ServiziMigrazione	FiguraMigrazione	Cloud Application Specialist	58	
SP-02	ServiziMigrazione	FiguraMigrazione	Database Specialist and Administrator	60	
SP-06	ServiziMigrazione	FiguraMigrazione	Enterprise Architect	55	
SP-03	ServiziMigrazione	FiguraMigrazione	System Integrator & Testing Specialist	77	
SP-05	ServiziMigrazione	FiguraMigrazione	Cloud Security Specialist	57	
SP-14	ServiziMigrazione	FiguraMigrazione	Senior Information Security Consultant	25	
SP-16	ServiziMigrazione	FiguraMigrazione	Security Solution Architect	20	

Totale UT	Totale Canone Annuale
€ 14.719,3000	
€ 18.290,3000	
€ 14.958,6000	
€ 22.842,0500	
€ 16.173,0800	
€ 14.210,6700	
€ 10.594,2500	
€ 8.475,4000	

8.2.2 Fase di operatività della piattaforma LIS

Per maggior chiarezza viene quindi riportato sia il valore annualizzato che quello per la durata contrattuale (prevista per un massimo di 10 anni) dei servizi professionali contenuti nel presente progetto, suddiviso per ciascuna attività.

Relativamente ai Servizi professionali ricorrenti previsti nel progetto dei fabbisogni, si precisa che essi sono stati quantificati per poter far fronte alle esigenze dell'Amministrazione nel corso degli anni di vigenza contrattuale. Essendo la loro rendicontazione (e di conseguenza la loro fatturazione) prevista tramite Stati Avanzamenti Lavori (SAL da approvare da parte del Contraente) bimestrali, è data piena facoltà all'Amministrazione di decidere se utilizzarli, specificandone le quantità, o meno.

8.2.2.1 Security Professional Services

Valore annualizzato

ANAGRAFICA AMMINISTRAZIONE					
Codice Fiscale					
Ragione Sociale		AIC numero 3			
IDENTIFICATIVO DOCUMENTO					
Emesso da		CSO			
Codice Documento		2023-0000001521330033-PdF-P1R1			
Versione		1			
VERSIONE CONFIGURATORE			2.3		
RIEPILOGO PREZZI					
SERVIZIO	Totale UT	Totale Canone Annuale	Totale Canone 10 anni		
Industry Standard		€ -	€ -		
Hybrid Cloud on PSN Site		€ -	€ -		
SecurePublicCloud		€ -	€ -		
Public Cloud PSN Managed		€ -	€ -		
Servizi di Migrazione	€ -				
Servizi Professionali	€ 110.208,61				
TOTALE	€ 110.208,61	€ -	€ -		

CODICE	SERVIZIO	TIPOLOGIA	ELEMENTO	QUANTITA'	DR	Totale UT	Totale Canone Annuale
SP-01	ServiziProfessionali	Figuraprofessionale	Cloud Application Architect	15		€ 5.810,2500	
SP-04	ServiziProfessionali	Figuraprofessionale	Cloud Application Specialist	23		€ 7.253,0500	
SP-22	ServiziProfessionali	Figuraprofessionale	Data Protection Specialist	20		€ 7.436,0000	
SP-21	ServiziProfessionali	Figuraprofessionale	Forensic Expert	12		€ 4.461,6000	
SP-15	ServiziProfessionali	Figuraprofessionale	Junior Information Security Consultant	23		€ 6.841,1200	
SP-20	ServiziProfessionali	Figuraprofessionale	Junior Penetration Tester	17		€ 4.431,2200	
SP-18	ServiziProfessionali	Figuraprofessionale	Junior Security Analyst	29		€ 8.185,2500	
SP-14	ServiziProfessionali	Figuraprofessionale	Senior Information Security Consultant	15		€ 6.356,5500	
SP-07	ServiziProfessionali	Figuraprofessionale	Project Manager	17		€ 6.320,6000	
SP-13	ServiziProfessionali	Figuraprofessionale	Security Principal	15		€ 7.807,8000	
SP-16	ServiziProfessionali	Figuraprofessionale	Security Solution Architect	29		€ 12.289,3300	
SP-19	ServiziProfessionali	Figuraprofessionale	Senior Penetration Tester	12		€ 4.461,6000	
SP-17	ServiziProfessionali	Figuraprofessionale	Senior Security Auditor/Analyst	64		€ 28.554,2400	

Valore a 10 anni

ANAGRAFICA AMMINISTRAZIONE			
Codice Fiscale			
Ragione Sociale	AIC numero 3		
IDENTIFICATIVO DOCUMENTO			
Emesso da	CSO		
Codice Documento	2023-000001521330033-PdF-P1R1		
Versione	1		
VERSIONE CONFIGURATORE		2.3	
RIEPILOGO PREZZI			
SERVIZIO	Totale UT	Totale Canone Annuale	Totale Canone 10 anni
Industry Standard		€ -	€ -
Hybrid Cloud on PSN Site		€ -	€ -
SecurePublicCloud		€ -	€ -
Public Cloud PSN Managed		€ -	€ -
Servizi di Migrazione	€ -		
Servizi Professionali	€ 1.102.086,10		
TOTALE	€ 1.102.086,10	€ -	€ -

CODICE	SERVIZIO	TIPOLOGIA	ELEMENTO	QUANTITA'	DR	Totale UT	Totale Canone Annuale
SP-01	ServiziProfessionali	Figuraprofessionale	Cloud Application Architect	150		€ 58.102,5000	
SP-04	ServiziProfessionali	Figuraprofessionale	Cloud Application Specialist	230		€ 72.530,5000	
SP-22	ServiziProfessionali	Figuraprofessionale	Data Protection Specialist	200		€ 74.360,0000	
SP-21	ServiziProfessionali	Figuraprofessionale	Forensic Expert	120		€ 44.616,0000	
SP-15	ServiziProfessionali	Figuraprofessionale	Junior Information Security Consultant	230		€ 68.411,2000	
SP-20	ServiziProfessionali	Figuraprofessionale	Junior Penetration Tester	170		€ 44.312,2000	
SP-18	ServiziProfessionali	Figuraprofessionale	Junior Security Analyst	290		€ 81.852,5000	
SP-14	ServiziProfessionali	Figuraprofessionale	Senior Information Security Consultant	150		€ 63.565,5000	
SP-07	ServiziProfessionali	Figuraprofessionale	Project Manager	170		€ 63.206,0000	
SP-13	ServiziProfessionali	Figuraprofessionale	Security Principal	150		€ 78.078,0000	
SP-16	ServiziProfessionali	Figuraprofessionale	Security Solution Architect	290		€ 122.893,3000	
SP-19	ServiziProfessionali	Figuraprofessionale	Senior Penetration Tester	120		€ 44.616,0000	
SP-17	ServiziProfessionali	Figuraprofessionale	Senior Security Auditor/Analyst	640		€ 285.542,4000	

8.2.2.2 IT infrastructure service operations

Valore annualizzato



ANAGRAFICA AMMINISTRAZIONE	
Codice Fiscale	
Ragione Sociale	AIC numero 3
IDENTIFICATIVO DOCUMENTO	
Emesso da	CSO
Codice Documento	2023-0000001521330033-PdF-P1R1
Versione	1
VERSIONE CONFIGURATORE	
	2.3

RIEPILOGO PREZZI			
SERVIZIO	Totale UT	Totale Canone Annuale	Totale Canone 10 anni
Industry Standard		€ -	€ -
Hybrid Cloud on PSN Site		€ -	€ -
SecurePublicCloud		€ -	€ -
Public Cloud PSN Managed		€ -	€ -
Servizi di Migrazione	€ -		
Servizi Professionali	€ 70.803,22		
TOTALE	€ 70.803,22	€ -	€ -

CODICE	SERVIZIO	TIPOLOGIA	ELEMENTO	QUANTITA'	DR	Totale UT	Totale Canone Annuale
SP-02	ServiziProfessionali	Figuraprofessionale	Database Specialist and Administrator	120		€ 29.917,2000	
SP-24	ServiziProfessionali	Figuraprofessionale	Product/Network/Technical Specialist	30		€ 10.050,6000	
SP-12	ServiziProfessionali	Figuraprofessionale	System and Network Administrator	50		€ 14.872,0000	
SP-23	ServiziProfessionali	Figuraprofessionale	Systems Architect	33		€ 15.963,4200	

Valore a 10 anni

ANAGRAFICA AMMINISTRAZIONE	
Codice Fiscale	
Ragione Sociale	AIC numero 3
IDENTIFICATIVO DOCUMENTO	
Emesso da	CSO
Codice Documento	2023-0000001521330033-PdF-P1R1
Versione	1
VERSIONE CONFIGURATORE	
	2.3

RIEPILOGO PREZZI			
SERVIZIO	Totale UT	Totale Canone Annuale	Totale Canone 10 anni
Industry Standard		€ -	€ -
Hybrid Cloud on PSN Site		€ -	€ -
SecurePublicCloud		€ -	€ -
Public Cloud PSN Managed		€ -	€ -
Servizi di Migrazione	€ -		
Servizi Professionali	€ 708.032,20		
TOTALE	€ 708.032,20	€ -	€ -

CODICE	SERVIZIO	TIPOLOGIA	ELEMENTO	QUANTITA'	DR	Totale UT	Totale Canone Annuale
SP-02	ServiziProfessionali	Figuraprofessionale	Database Specialist and Administrator	1200		€ 299.172,0000	
SP-24	ServiziProfessionali	Figuraprofessionale	Product/Network/Technical Specialist	300		€ 100.506,0000	
SP-12	ServiziProfessionali	Figuraprofessionale	System and Network Administrator	500		€ 148.720,0000	
SP-23	ServiziProfessionali	Figuraprofessionale	Systems Architect	330		€ 159.634,2000	