REGIONE PIEMONTE

SEDE LEGALE
Via dei Ponderanesi n. 2 – 13875 Ponderano (BI)
P.IVA 01810260024

AZIENDA SANITARIA LOCALE DI BIELLA

Presso i locali della SC AMMINISTRAZIONE E CONTROLLO

IL DIRETTORE

ROSSI LEILA

in conformità con gli indirizzi e i criteri disposti nella materia dall'A.S.L. BI di Biella con deliberazione n. 474 del 21.12.2016,

ha assunto la seguente determinazione:

Determinazione n. 588 in data 22/05/2024

OGGETTO: APPROVAZIONE DEL PROGETTO DEI FABBISOGNI E ADESIONE AL CONTRATTO DI UTENZA CON LA SOCIETA' 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 E LA SOCIETA' POLO STRATEGICO NAZIONALE S.P.A. (PSN), PER LA MIGRAZIONE IN CLOUD DI SERVIZI APPLICATIVI - IMPORTO COMPLESSIVO EURO 4.316.244,30 IVA INCLUSA - CIG DERIVATO B1C830483B DURATA 10 ANNI.

Determinazione n. 588 in data 22/05/2024

OGGETTO: APPROVAZIONE DEL PROGETTO DEI FABBISOGNI E ADESIONE AL CONTRATTO DI UTENZA CON LA SOCIETA' 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 E LA SOCIETA' POLO STRATEGICO NAZIONALE S.P.A. (PSN), PER LA MIGRAZIONE IN CLOUD DI SERVIZI APPLICATIVI - IMPORTO COMPLESSIVO EURO 4.316.244,30 IVA INCLUSA - CIG DERIVATO B1C830483B DURATA 10 ANNI.

IL DIRETTORE

PREMESSO che:

- con deliberazione n. 474 del 21/12/2016 è stato approvato il regolamento per l'adozione dei provvedimenti amministrativi dell'ASL BI in applicazione dei principi generali contenuti nell'Atto aziendale;

- con le deliberazioni nn. 327 del 31/05/2017 e 331 del 10/08/2018 sono stati approvati il Regolamento di disciplina delle competenze del RUP e del DEC nei contratti di fornitura di beni e servizi e il Regolamento per la ripartizione del fondo di incentivazione di cui all'art. 113 del D.lgs. n. 50/2016, che nelle more dell'assunzione da parte dell'ASL BI di nuovi regolamenti attuativi del D.lgs. n. 36/2023 (nuovo Codice dei contratti pubblici) sono da intendersi applicabili per quanto non incompatibili con la nuova disciplina;

Su proposta della SS SISTEMI INFORMATIVI dalla cui istruttoria si evince quanto segue:

VISTE:

- le circolari AgID n.2 e n. 3 del 9 aprile 2018 (Criteri per la qualificazione di servizi SaaS per il Cloud della PA) e successivi chiarimenti applicativi;

- il 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;

- la decisione di esecuzione del Consiglio (UE) del 13 luglio 2021 relativa all'approvazione della valutazione del Piano di Ripresa e Resilienza per l'Italia;

- la 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*

Determinazione n. 588 in data 22/05/2024

elaborativa, risparmio energetico 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;

- l'art. 10 del richiamato Regolamento "*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 Dipartimento per la trasformazione digitale, d'intesa con l'Agenzia per la cybersicurezza nazionale*";

- il Piano Triennale AgID 2022-2024;

- le determinazioni nn. 306 e 307 del 18 gennaio 2022 dell'ACN (Agenzia per la Cyber Sicurezza Nazionale) in merito al modello per la predisposizione dell'elenco e della classificazione di dati e servizi della PP.AA. e ulteriori caratteristiche dei servizi cloud e requisiti per la loro qualificazione;

- la convenzione stipulata tra il Dipartimento della Trasformazione Digitale (in breve DTD) della Presidenza del Consiglio dei Ministri e la Società di Progetto Polo Strategico Nazionale S.p.A (TIM S.p.A., CDP Equity S.p.A., Leonardo S.p.A. e Sogei S.p.A.) in data 24/08/2022 a seguito dell'esito della la Gara europea, a procedura aperta, per l'affidamento, mediante un contratto di partenariato pubblico – privato, della realizzazione e gestione del Polo Strategico Nazionale, CIG: 9066973ECE CUP: J51B21005710007, con bando, inviato per la pubblicazione nella Gazzetta Ufficiale dell'Unione Europea;

- la previsione della predetta Convenzione Nazionale tra il Dipartimento per la trasformazione digitale e il Polo Strategico Nazionale sottoscritta nell'ambito del PNRR (Missione 1, componente1, investimenti 1.1 Cloud PA/Polo Strategico Nazionale e 1.2

Determinazione n. 588 in data 22/05/2024

"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;

- la 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 menzionato Regolamento, ha definito il Modello di piano di migrazione, le regole per la corretta predisposizione del piano di migrazione da parte delle amministrazioni e la relativa modalità di trasmissione al Dipartimento per la trasformazione digitale, ai fini della verifica di conformità di cui all'articolo 10 comma 5 del Regolamento;

- la classificazione dei dati e dei servizi digitali (nota ASL BI- Amministrazione e Controllo prot. n. 10655/23 del 31.03.2023) registrata sulla Piattaforma PA Digitale nella quale sono identificati nello specifico come "Critici" i seguenti servizi:

Categoria Servizio	Nome Servizio
ASSISTENZA OSPEDALIERA	ASSISTENZA SPECIALISTICA AMBULATORIALE
ASSISTENZA DISTRETTUALE	CURE DOMICILIARI (ANCHE PALLIATIVE)
ASSISTENZA OSPEDALIERA	PRONTO SOCCORSO
ASSISTENZA OSPEDALIERA	RICOVERO ORDINARIO PER ACUTI
ASSISTENZA OSPEDALIERA	DAY SURGERY
ASSISTENZA OSPEDALIERA	DAY HOSPITAL
ASSISTENZA OSPEDALIERA	RIABILITAZIONE E LUNGODEGENZA POST ACUZIE
RISCHIO CLINICO	RISCHIO CLINICO
ASSISTENZA DISTRETTUALE	PERCORSI ASSISTENZIALI INTEGRATI
ASSISTENZA DISTRETTUALE	ASSISTENZA SPECIALISTICA AMBULATORIALE
ASSISTENZA OSPEDALIERA	ATTIVITÀ DIAGNOSTICA ANATOMIA PATOLOGICA
FASCICOLO SANITARIO REGIONALE	REPOSITORY CLINICO AZIENDALE

Determinazione n. 588 in data 22/05/2024

RILEVATO CHE

- l'art. 1 della legge regionale 26 ottobre 2021, n. 26 (in seguito parzialmente modificata dall'art. 1 della L.R. n. 2 del 25 marzo 2022) ha previsto l'istituzione dell'Azienda Sanitaria Zero – costituita con D.P.G.R. n. 9 del 18/02/2022 - quale Ente del Servizio Sanitario Regionale dotato di personalità giuridica pubblica e di autonomia amministrativa, patrimoniale, organizzativa, contabile, gestionale e tecnica, con la finalità di promuovere forme di aggregazione funzionale dei servizi sanitari e operativi di supporto a valenza regionale;

- la Regione con la DGR 15-6172 del 07/12/2022 ha indirizzato 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 ss.mm.ii. e per gli interventi di abilitazione e facilitazione migrazione al cloud per le PA locali;

- la Regione ha attribuito con la medesima D.G.R. ad Azienda Zero funzioni di supporto alle AA.SS.RR., 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";

- Azienda Zero a supporto degli Enti del S.S.R. ha istituito quindi una cabina di regia c.d. "Migrazione al Cloud" e fornito indicazioni generali alle AA.SS.RR. in merito alle modalità di migrazione al cloud (rif. nota Azienda Zero del 22 marzo 2023);

- a seguito dell'istituzione della cabina di regia di Azienda Zero, l'ASL BI ha sottoposto in data 13.04.2023 il proprio Piano di Migrazione al Cloud anche in funzione dell'Avviso Multimisura indetto dalla Presidenza del Consiglio dei Ministri - Dipartimento per la trasformazione digitale ad Azienda Zero – "Migrazione al Cloud" a cui seguiva il parere in data 17.04.2023 (allegato sub 1);

- l'ASL BI sulla scorta del piano di migrazione ha proposto al PSN il Piano dei Fabbisogni (c.d. Piano dei fabbisogni – Servizi CED vers. 3 del 14 novembre 2023) a cui è seguito, da parte del PSN, il Progetto del Piano dei Fabbisogni "*2023-0000001810260024-PPdF-P2R3 - ASL Biella - Servizi CED*" (ricevuto con messaggio di posta elettronica certificata del 6 dicembre 2023 ad oggetto "*Invio del Progetto del Piano dei Fabbisogni n. 2023-0000001810260024-PPdF-P2R3 ai sensi dell'art. 18 della Convenzione sottoscritta tra PSN S.p.A. e il Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei Ministri in data 24 agosto 2022*."(allegato sub 2);

- l'ASL BI, acquisito anche il parere di Azienda Zero in merito al Progetto del Piano del Fabbisogni "*2023-0000001810260024-PPdF-P2R3 - ASL Biella - Servizi CED*" (rif. messaggio di posta elettronica ordinaria – "Migrazione Cloud" del 11.01.2024 ad oggetto "*Re: Migrazione Cloud - PSN - Progetto Piano fabbisogni (suite Engineering - Dialisi - Diabetologia - Sito WEB istituzionale) – Parere*", ha confermato l'accettazione al PSN (rif. messaggio di posta elettronica certificata – "Sistemi Informativi" del 01.02.2024 ad oggetto "*0004174/24: adesione alla convenzione del 24/8/2022 per la realizzazione e gestione di una nuova infrastruttura informatica al servizio della pubblica amministrazione*") e contestualmente ha richiesto il rilascio della garanzia definitiva ai sensi dell'art.15 dello schema del contratto d'utenza;

Determinazione n. 588 in data 22/05/2024

RILEVATO ALTRESI' CHE

- l'investimento del PNRR M1C1 1.1 "*Infrastrutture digitali*" prevede espressamente che "*La trasformazione digitale della PA segue un approccio c.d. "cloud first", orientato alla migrazione dei dati e degli applicativi informatici delle singole amministrazioni verso un ambiente cloud*";

- l'ASL BI - previa richiesta con lettera del direttore Generale del 27/06/2024 - ha aderito all'Avviso Pubblico multimisura 1.1 e 1.2 "Infrastrutture digitali e abilitazione al cloud" - ASL/AO (marzo 2023) - M1C1 PNRR finanziato dall'Unione Europea – Next GenerationEU (CUP C21C23000520006), in cui tra i vari servizi elencati nella migrazione al PSN è presente "Comunicazione Istituzionale Web ed Open Data" (migrazione a valere sull'investimento 1.1);

- la Presidenza del Consiglio dei Ministri- Dipartimento per la trasformazione digitale con decreto di finanziamento del capo Dipartimento (Decreto n. 48 - 1 / 2023 – PNRR - AVVISO PUBBLICO "Avviso multimisura 1.1 e 1.2 "Infrastrutture digitali e abilitazione al cloud") ha approvato la domanda di finanziamento per l'ASL BI, CUP C21C23000440006, con i seguenti importi: Linea Finanziamento 1.1 € 34.050,00 e Linea Finanziamento 1.2 € 289.425,00. Detto intervento ha scadenze ben definite, sia per la contrattualizzazione sia per la realizzazione la cui data ultima per l'implementazione e relativa rendicontazione sul portale di PA Digitale è fissata, ad oggi, nel prossimo 25 settembre 2024;

- l'ASL BI, a seguito del raggiungimento degli obiettivi prefissati di cui al punto precedente, intende impegnare le predette risorse nella realizzazione del presente affidamento;

PRESO ATTO

- dei pareri, sopra richiamati, di Azienda Zero – "Migrazione Cloud" in merito al Piano di Migrazione e al Progetto del Piano dei Fabbisogni;
- della congruità del "Progetto del Piano dei Fabbisogni", predisposto dal Polo Strategico Nazionale "Progetto del Piano dei Fabbisogni, identificato dal codice *2023-0000001810260024-PPdF-P2R3 - ASL Biella - Servizi CED*";

DATO ATTO CHE

- l'ASL BI, in conformità a quanto previsto dall'art. 103, c.1, del d.lgs 50/2016, ha ricevuto la Garanzia Fideiussoria Definitiva emessa il 28.02.2024 necessaria per procedere con la stipula contrattuale;
- per la 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;
- per la realizzazione del presente affidamento sarà necessario attivare una linea trasmissione dati su base geografica ad alta affidabilità per il collegamento al PSN che sarà oggetto di separata procedura;

DATO ATTO altresì che

Determinazione n. 588 in data 22/05/2024

- il servizio oggetto del presente affidamento, unitamente al servizio di digitalizzazione delle cartelle cliniche e moduli di medicina legale per l'ASL BI (Determinazione della S.C. Amministrazione e Controllo n. 1484 del 19/12/2023), andrà in sostituzione del servizio SPC CLOUD attualmente in essere con TELECOM S.P.A., che comporta un costo annuale di € 83.137,34 (IVA esclusa), pertanto in conseguenza dell'attivazione del servizio di cui al presente provvedimento verrà dismesso servizio SPC CLOUD;

RITENUTO pertanto di

- condividere la sopra richiamata proposta;
- di approvare il Progetto dei Fabbisogni, predisposto per l'Azienda dal Polo Strategico Nazionale, Progetto del Piano dei Fabbisogni, identificato dal codice *2023-0000001810260024-PPdF-P2R3 - ASL Biella - Servizi CED* contenente la proposta tecnico-economica relativa all'esigenza espressa nel corrispondente Piano dei Fabbisogni redatto dalla S.S. Sistemi Informativi della ASL Biella nonché di approvare il Piano di Migrazione al Cloud di cui in premessa (allegati sub 1 e 2);
- di aderire alla Convenzione sottoscritta tra il Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei Ministri e la Società Polo Strategico Nazionale S.p.A. (c.d. PSN), per la realizzazione e gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione;
- di affidare la realizzazione e gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione alla Società Polo Strategico Nazionale S.P.A. (PSN), con cui verrà stipulato il relativo contratto di utenza, per la durata di 10 anni, all'importo complessivo di € 4.316.244,30 Iva compresa;
- di dare atto che il Piano dei Fabbisogni predisposto dalla S.S. Sistemi Informativi della ASL Biella - e il susseguente Progetto del Piano dei Fabbisogni predisposto dalla Società Polo Strategico Nazionale S.p.A. (PSN) costituiscono parte integrante del contratto d'utenza;
- di stabilire che il contratto decorrerà dal 01/07/2024 e avrà durata di anni 10 (dieci);
- di dare atto che tra i servizi del PSN non sono compresi i servizi di connettività tra i data-center dei service provider e le sedi della ASL, pertanto i necessari servizi di connettività saranno oggetto di ulteriore provvedimento;
- di dare atto, altresì, che la spesa complessiva prevista per lo svolgimento dell'attività sopra descritta è suddivisa secondo il seguente schema di ripartizione annuale:

Determinazione n. 588 in data 22/05/2024

	Anno 2024	Anno 2025	Anno 2026	Anno 2027	Anno 2028	Anno 2029	Anno 2030	Anno 2031	Anno 2032	Anno 2033
Infrastruttura	106.868,97 €	128.242,76 €	128.242,76 €	128.242,76 €	128.242,76 €	128.242,76 €	128.242,76 €	128.242,76 €	128.242,76 €	128.242,76 €
Servizi professionali di migrazione	299.726,32 €									
Servizi professionali di conduzione	280.246,40 €	188.542,07 €	188.542,07 €	188.542,07 €	188.542,07 €	188.542,07 €	188.542,07 €	188.542,07 €	188.542,07 €	188.542,07 €
	686.841,69 €	316.784,83 €	316.784,83 €	316.784,83 €	316.784,83 €	316.784,83 €	316.784,83 €	316.784,83 €	316.784,83 €	316.784,83 €

Il canone è elaborato considerando l'avvio al 01/07/2024 (le cifre indicate sono senza IVA)

- gli oneri derivanti dal presente provvedimento di Euro 4.316.244,30 Iva compresa per l'ASL BI verranno imputati sul conto 03.10.11.01 "Servizi Elaborazione Dati" – Autorizzazione 13 con la suddivisione annuale, come di seguito riportato:

ANNO	ATTIVITA'	CONTO	AUT.	DESCRIZIONE CONTO	IMPORTO IVA ESCLUSA	IMPORTO IVA INCLUSA
2024	Infrastruttura	3101101	13	Servizi Elaborazione Dati	€ 106 868.97	€ 130 380.14
2024	Una tantum - servizi professionali di migrazione	3101101	13	Servizi Elaborazione Dati	€ 299 726.32	€ 365 666.11
2024	Servizi professionali di conduzione	3101101	13	Servizi Elaborazione Dati	€ 280 246.40	€ 341 900.61
2025	Infrastruttura	3101101	13	Servizi Elaborazione Dati	€ 128 242.76	€ 156 456.17
2025	Servizi professionali di conduzione	3101101	13	Servizi Elaborazione Dati	€ 188 542.07	€ 230 021.33
2026	Infrastruttura	3101101	13	Servizi Elaborazione Dati	€ 128 242.76	€ 156 456.17
2026	Servizi professionali di conduzione	3101101	13	Servizi Elaborazione Dati	€ 188 542.07	€ 230 021.33
2027	Infrastruttura	3101101	13	Servizi Elaborazione Dati	€ 128 242.76	€ 156 456.17
2027	Servizi professionali di conduzione	3101101	13	Servizi Elaborazione Dati	€ 188 542.07	€ 230 021.33

Determinazione n. 588 in data 22/05/2024

2028	Infrastruttura	3101101	13	Servizi Elaborazione Dati	€ 128 242.76	€ 156 456.17
2028	Servizi professionali di conduzione	3101101	13	Servizi Elaborazione Dati	€ 188 542.07	€ 230 021.33
2029	Infrastruttura	3101101	13	Servizi Elaborazione Dati	€ 128 242.76	€ 156 456.17
2029	Servizi professionali di conduzione	3101101	13	Servizi Elaborazione Dati	€ 188 542.07	€ 230 021.33
2030	Infrastruttura	3101101	13	Servizi Elaborazione Dati	€ 128 242.76	€ 156 456.17
2030	Servizi professionali di conduzione	3101101	13	Servizi Elaborazione Dati	€ 188 542.07	€ 230 021.33
2031	Infrastruttura	3101101	13	Servizi Elaborazione Dati	€ 128 242.76	€ 156 456.17
2031	Servizi professionali di conduzione	3101101	13	Servizi Elaborazione Dati	€ 188 542.07	€ 230 021.33
2032	Infrastruttura	3101101	13	Servizi Elaborazione Dati	€ 128 242.76	€ 156 456.17
2032	Servizi professionali di conduzione	3101101	13	Servizi Elaborazione Dati	€ 188 542.07	€ 230 021.33
2033	Infrastruttura	3101101	13	Servizi Elaborazione Dati	€ 128 242.76	€ 156 456.17
2033	Servizi professionali di conduzione	3101101	13	Servizi Elaborazione Dati	€ 188 542.07	€ 230 021.33
	TOTALE				€ 3 537 905.16	€ 4 316 244.30

- di stabilire che i servizi a “consuntivo” (consumo) verranno utilizzati esclusivamente in funzione delle reali esigenze che si andranno a determinare e che, di conseguenza, i costi sostenuti corrisponderanno alle risorse PSN effettivamente utilizzate;
- di individuare come Responsabile Unico del Progetto (RUP) la Dott.ssa Leila Rossi e come Direttore dell’Esecuzione del Contratto (DEC) il Dott. Piero Gauna;

DATO ATTO infine che, in esecuzione del regolamento aziendale per la ripartizione del fondo di incentivazione di cui all' art. 113 D.Lgs. 18/04/2016, n. 50, approvato con deliberazione del Commissario n. 331 del 10/08/2018, e successivamente aggiornato con deliberazione del Commissario n. 498 del 22/11/2019:

Determinazione n. 588 in data 22/05/2024

- verrà accantonata in apposito fondo una risorsa finanziaria pari a € 20.742,00;
- il gruppo di lavoro per la presente procedura verrà individuato e comunicato alla Direzione Amministrativa;

TUTTO CIO' PREMESSO

IN CONFORMITA' con gli indirizzi e i criteri disposti nella materia dall'A.S.L. BI di Biella con deliberazione n. 474 del 21.12.2016

D E T E R M I N A:

1) di approvare il Progetto dei Fabbisogni, predisposto per l'Azienda dal Polo Strategico Nazionale, Progetto del Piano dei Fabbisogni, identificato dal codice *2023-0000001810260024-PPdF-P2R3 - ASL Biella - Servizi CED* contenente la proposta tecnico-economica relativa all'esigenza espressa nel corrispondente Piano dei Fabbisogni redatto dalla S.S. Sistemi Informativi della ASL Biella nonché di approvare il Piano di Migrazione al Cloud di cui in premessa (allegati sub 1 e 2);

2) di aderire alla Convenzione sottoscritta tra il Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei Ministri e la Società Polo Strategico Nazionale S.p.A. (c.d. PSN), per la realizzazione e gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione;

3) di affidare la realizzazione e gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione alla Società Polo Strategico Nazionale S.P.A. (PSN), con cui verrà stipulato il relativo contratto di utenza, per la durata di 10 anni, all'importo complessivo di € 4.316.244,30 Iva compresa;

4) di dare atto che il Piano dei Fabbisogni predisposto dalla S.S. Sistemi Informativi della ASL Biella - e il susseguente Progetto del Piano dei Fabbisogni predisposto dalla Società Polo Strategico Nazionale S.p.A. (PSN) costituiscono parte integrante del contratto d'utenza;

5) di stabilire che il contratto decorrerà dal 01/07/2024 e avrà durata di anni 10 (dieci);

6) di dare atto che tra i servizi del PSN non sono compresi i servizi di connettività tra i data-center dei service provider e le sedi della ASL, pertanto i necessari servizi di connettività saranno oggetto di ulteriore provvedimento;

7) di dare atto, altresì, che la spesa complessiva prevista per lo svolgimento dell'attività sopra descritta è suddivisa secondo il seguente schema di ripartizione annuale:

Determinazione n. 588 in data 22/05/2024

	Anno 2024	Anno 2025	Anno 2026	Anno 2027	Anno 2028	Anno 2029	Anno 2030	Anno 2031	Anno 2032	Anno 2033
Infrastruttura	106.868,97 €	128.242,76 €	128.242,76 €	128.242,76 €	128.242,76 €	128.242,76 €	128.242,76 €	128.242,76 €	128.242,76 €	128.242,76 €
Servizi professionali di migrazione	299.726,32 €									
Servizi professionali di conduzione	280.246,40 €	188.542,07 €	188.542,07 €	188.542,07 €	188.542,07 €	188.542,07 €	188.542,07 €	188.542,07 €	188.542,07 €	188.542,07 €
	686.841,69 €	316.784,83 €	316.784,83 €	316.784,83 €	316.784,83 €	316.784,83 €	316.784,83 €	316.784,83 €	316.784,83 €	316.784,83 €

Il canone è elaborato considerando l'avvio al 01/07/2024 (le cifre indicate sono senza IVA)

8) gli oneri derivanti dal presente provvedimento di Euro 4.316.244,30 Iva compresa per l'ASL BI verranno imputati sul conto 03.10.11.01 "Servizi Elaborazione Dati" – Autorizzazione 13 con la suddivisione annuale, come di seguito riportato:

ANNO	ATTIVITA'	CONTO	AUT.	DESCRIZIONE CONTO	IMPORTO IVA ESCLUSA	IMPORTO IVA INCLUSA
2024	Infrastruttura	3101101	13	Servizi Elaborazione Dati	€ 106 868.97	€ 130 380.14
2024	Una tantum - servizi professionali di migrazione	3101101	13	Servizi Elaborazione Dati	€ 299 726.32	€ 365 666.11
2024	Servizi professionali di conduzione	3101101	13	Servizi Elaborazione Dati	€ 280 246.40	€ 341 900.61
2025	Infrastruttura	3101101	13	Servizi Elaborazione Dati	€ 128 242.76	€ 156 456.17
2025	Servizi professionali di conduzione	3101101	13	Servizi Elaborazione Dati	€ 188 542.07	€ 230 021.33
2026	Infrastruttura	3101101	13	Servizi Elaborazione Dati	€ 128 242.76	€ 156 456.17
2026	Servizi professionali di conduzione	3101101	13	Servizi Elaborazione Dati	€ 188 542.07	€ 230 021.33
2027	Infrastruttura	3101101	13	Servizi Elaborazione Dati	€ 128 242.76	€ 156 456.17
2027	Servizi professionali di conduzione	3101101	13	Servizi Elaborazione Dati	€ 188 542.07	€ 230 021.33
2028	Infrastruttura	3101101	13	Servizi Elaborazione Dati	€ 128 242.76	€ 156 456.17

Determinazione n. 588 in data 22/05/2024

2028	Servizi professionali di conduzione	3101101	13	Servizi Elaborazione Dati	€ 188 542.07	€ 230 021.33
2029	Infrastruttura	3101101	13	Servizi Elaborazione Dati	€ 128 242.76	€ 156 456.17
2029	Servizi professionali di conduzione	3101101	13	Servizi Elaborazione Dati	€ 188 542.07	€ 230 021.33
2030	Infrastruttura	3101101	13	Servizi Elaborazione Dati	€ 128 242.76	€ 156 456.17
2030	Servizi professionali di conduzione	3101101	13	Servizi Elaborazione Dati	€ 188 542.07	€ 230 021.33
2031	Infrastruttura	3101101	13	Servizi Elaborazione Dati	€ 128 242.76	€ 156 456.17
2031	Servizi professionali di conduzione	3101101	13	Servizi Elaborazione Dati	€ 188 542.07	€ 230 021.33
2032	Infrastruttura	3101101	13	Servizi Elaborazione Dati	€ 128 242.76	€ 156 456.17
2032	Servizi professionali di conduzione	3101101	13	Servizi Elaborazione Dati	€ 188 542.07	€ 230 021.33
2033	Infrastruttura	3101101	13	Servizi Elaborazione Dati	€ 128 242.76	€ 156 456.17
2033	Servizi professionali di conduzione	3101101	13	Servizi Elaborazione Dati	€ 188 542.07	€ 230 021.33
	TOTALE				€ 3 537 905.16	€ 4 316 244.30

9) di stabilire che i servizi a “consuntivo” (consumo) verranno utilizzati esclusivamente in funzione delle reali esigenze che si andranno a determinare e che, di conseguenza, i costi sostenuti corrisponderanno alle risorse PSN effettivamente utilizzate;

10) di individuare come Responsabile Unico del Progetto (RUP) la Dott.ssa Leila Rossi e come Direttore dell’Esecuzione del Contratto (DEC) il Dott. Piero Gauna;

11) che, in esecuzione del regolamento aziendale per la ripartizione del fondo di incentivazione di cui all' art. 113 D.Lgs. 18/04/2016, n. 50, approvato con deliberazione del Commissario n. 331 del 10/08/2018, e successivamente aggiornato con deliberazione del Commissario n. 498 del 22/11/2019:

- verrà accantonata in apposito fondo una risorsa finanziaria pari a € 20.742,00;

Determinazione n. 588 in data 22/05/2024

- il gruppo di lavoro per la presente procedura verrà individuato e comunicato alla Direzione Amministrativa;

12) di trasmettere copia del presente provvedimento all'Azienda Zero e al PSN;

13) di dare mandato alla SS SISTEMI INFORMATIVI di provvedere agli adempimenti consequenziali.

REGIONE PIEMONTE

SEDE LEGALE
Via dei Ponderanesi n. 2 – 13875 Ponderano (BI)
P.IVA 01810260024

AZIENDA SANITARIA LOCALE DI BIELLA

DETERMINAZIONE DELLA SC AMMINISTRAZIONE E CONTROLLO

Determinazione n. 588 in data 22/05/2024

IL DIRETTORE

ROSSI LEILA

Concessione per la realizzazione e la 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

ASL BIELLA

SERVIZI CED

Progetto del Piano dei Fabbisogni

SOMMARIO

1 PREMESSA 6
2 AMBITO 7
3 DOCUMENTI 9
3.1 DOCUMENTI CONTRATTUALI 9
3.2 DOCUMENTI DI RIFERIMENTO 10
3.3 DOCUMENTI APPLICABILI 10
4 ACRONIMI 12
5 PROGETTO DI ATTUAZIONE DEL SERVIZIO 13
5.1 SERVIZI PROPOSTI 13
5.2 INDUSTRY STANDARD 14
5.2.1 Housing 14
5.2.2 Infrastructure as a Service 15
5.2.3 Platform as a Service 17
5.2.4 Data Protection e Disaster Recovery 19
5.3 CONSOLE UNICA 21
5.3.1 Overview delle caratteristiche funzionali 22
5.3.2 Modalità di accesso 23
5.3.3 Interfaccia applicativa della Console Unica 23
5.4 SERVIZI E PIANO DI MIGRAZIONE 25
5.4.1 Piano di attivazione e Gantt 28
5.5 SERVIZI PROFESSIONALI 28
5.5.1 Security Profess. Services 28
5.5.2 IT infrastructure service operations 39
6 FIGURE PROFESSIONALI 44
7 SICUREZZA 46
8 CONFIGURATORE 47
9 Rendicontazione 50

Indice delle tabelle

Tabella 1: Informazioni Documento 4
Tabella 2: Autore 4
Tabella 3: Revisore 4
Tabella 4: Approvatore 4
Tabella 5: Consistenza AS IS delle risorse infrastrutturali 8
Tabella 6: Classificazione dei dati dei servizi richiesti 8
Tabella 7: Documenti Contrattuali 9
Tabella 8: Documenti di riferimento 10
Tabella 9: Documenti Applicabili 11
Tabella 10: Acronimi 12
Tabella 11: Servizi Proposti 13
Tabella 12: TO BE richiesto dall'Amministrazione per IaaS 16
Tabella 13: Configurazione servizi IaaS Shared HA 17
Tabella 14: TO BE richiesto dall'Amministrazione per PaaS DB Oracle 18
Tabella 15: TO BE richiesto dall'Amministrazione per PaaS DB SQL 19
Tabella 16: Configurazione servizi PaaS DB 19
Tabella 17: Dimensionamenti back up 21
Tabella 18: Tabella di correlazione tra gravità incidenti e impatto sugli asset 34
Tabella 19: Descrizione dei livelli di incidente 34
Tabella 20: RACI per attività sistemistiche 42
Tabella 21: RACI per attività DBA 42
Tabella 22: Livelli di servizio per attività sistemistiche 43

STATO DEL DOCUMENTO

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

TITOLO DEL DOCUMENTO		
Descrizione Modifica	**Revisione**	**Data**
Prima Emissione	1	30/11/2023

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 PSN Commercial team	Paolo Trevisan Riccardo Rossi

Tabella 4: Approvatore

LISTA DI DISTRIBUZIONE

INTERNA A:

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

ESTERNA A:

- Referente Contratto Esecutivo
  - Elvira Zampese
  - Elvira.zampese@aslbi.piemonte.it
- Referente Tecnico
  - Elvira Zampese
  - Elvira.zampese@aslbi.piemonte.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 dell'**ASL Biella**, 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 **2023-0000001810260024-PdF-P2R3**).

2 AMBITO

L'Ente intende migrare all'interno del Polo Strategico Nazionale i servizi attualmente erogati in SPC Cloud della suite Engineering, nonché alcuni applicativi verticali presenti on premises, come sotto elencato.

- ENGI Anatomia Patologica SPC Cloud
- ENGI Amministrativo Contabile SPC Cloud
- METEDA Diabetologia On Prem
- SINED Dialisi On prem
- DROMEDIAN Portale WEB Istituzionale **(*)**

(*) su Cloud non qualificato, oggetto di richiesta fondi PNRR

La tabella che segue riassume le specifiche dei servizi richiesti.

Servizio	Applicativo	Nome Server	VCPU	RAM (GB)	Disco (GB)	Sistema Operativo	SW DB
Suite	AREAS	dcsrv	2	4	40	Windows Server 2012	
Suite	AREAS	lb	4	8	60	Linux Centos 7	
Suite	AREAS	dmzweb	2	4	40	Linux Centos 7.4	
Suite	AREAS	tsapp-2	6	24	100	Windows Server 2012 R2	
Suite	AREAS	tsapp-1	6	24	150	Windows Server 2012 R2	
Suite	AREAS	vmtestcentos	6	32	80	Linux Centos 7.9	
Suite	AREAS	DB Test	8	32	2500		Oracle Std
Suite	AREAS	DB Prod	8	32	3500		Oracle Std
Diabetologia	MetaCliinic	App	4	16	300	Windows Server 2019	
Diabetologia	MetaCliinic	DB Prod	4	16	200	Windows Server 2019	SQL Server 2019
Dialisi	Medware	Web	4	12	100	Windows Server 2019	
Dialisi	Medware	App	6	16	100	Windows Server 2019	
Dialisi	Medware	DB Prod	6	16	300	Windows Server 2019	SQL Server 2019
Portale WEB		Web	4	16	100	OS Ubuntu 22.04 LTS	
Portale WEB		Intranet	4	16	100	OS Ubuntu 22.04 LTS	
Networking		Pfsense	2	4	50	FreeBSD	
VA		Openvas	4	8	60	Ubuntu 20	
Management		Zabbix Proxy	4	6	60	Ubuntu 20	

			98	354	8060		

Tabella 5: Consistenza AS IS delle risorse infrastrutturali

La classificazione dei dati è riportata nella tabella che segue.

Nome servizio	**Classificazionedei Dati**
Applicativi Engineering	Critici / Ordinari
Dialisi	Critici
Diabetologia	Critici
Portale WEB	Ordinari

Tabella 6: Classificazione dei dati dei servizi richiesti

3 DOCUMENTI

3.1 DOCUMENTI CONTRATTUALI

Riferimento	Titolo	Documenti consegnati	Versione	Data versione
#1	Piano dei Fabbisogni di Servizio	PSN_Piano dei Fabbisogni_v1.0	1.0	01.12.2022
#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	1.0	22.12.2022
#3	Piano di Qualità	PSN-SDE-CONV22-001-Piano della Qualità	1.0	22.12.2022
#4	Piano di Continuità Operativa	PSN-SDE-CONV22-001-Piano di Continuità Operativa ver.1.0	1.0	22.12.2022

Tabella 7: 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
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 8: 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 9: Documenti Applicabili

4 ACRONIMI

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

Acronimo	Descrizione
CRC	Cyclic Redundancy Check
CSP	Cloud Service Provider
DB	DataBase
DBaaS	DataBase as a Service
DR	Disaster Recovery
HA	High Availability
IaaS	Infrastructure as a Service
IT	Information Technology
PA	Pubblica Amministrazione
PaaS	Platform as a Service
PSN	Polo Strategico Nazionale
VM	Virtual Machine

Tabella 10: 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.

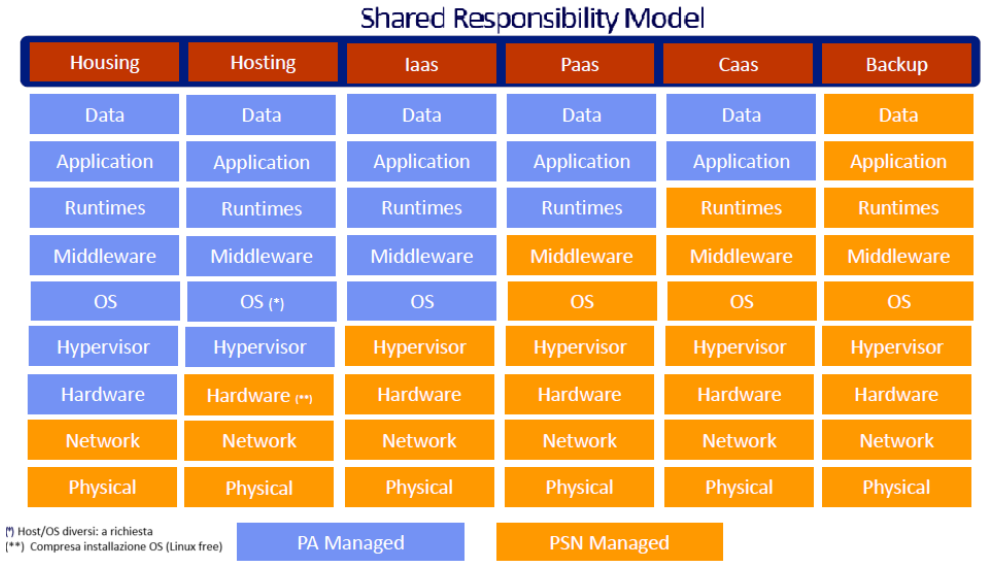
5.1 SERVIZI PROPOSTI

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

Servizio	Tipologia
Industry Standard	Housing
Industry Standard	Infrastructure as a Service (IaaS)
Industry Standard	Platform as a Service Database (PaaSDB)
Industry Standard	Data Protection: Backup
Industry Standard	Data Protection: Golden copy protetta
Servizi di Migrazione	
Servizi Professionali	Security Professional Services
Servizi Professionali	IT Infrastructure Service Operation

Tabella 11: Servizi Proposti

Di seguito, è mostrata la matrice di responsabilità nell'ambito della gestione dei servizi migrati su PSN:



5.2 INDUSTRY STANDARD

5.2.1 Housing

5.2.1.1 Descrizione del servizio

Il **Servizio Industry Standard Housing** è un servizio *Core* e consiste nella messa a disposizione, da parte del PSN, di aree esclusive all'interno dei Data Center del PSN, dotate di tutte le infrastrutture impiantistiche e tecnologiche necessarie a garantire elevati standard qualitativi in termini di affidabilità, disponibilità e sicurezza fisica degli ambienti descritti, atte ad ospitare le infrastrutture IT e TLC di proprietà dell'Amministrazione, nonché di eventuali variazioni in corso d'opera.

5.2.1.2 Personalizzazione del servizio

Sono previsti servizi di colocation per ospitare router dedicati alla connettività dedicata del Cliente e relativi rilanci fibra interni ai Due Data Center di Rozzano e S. Stefano Ticino.

Saranno fornite all'Amministrazione due classi /29 di indirizzi IP pubblici.

5.2.1.3 Dettaglio del servizio contrattualizzato (ID servizio, quantità costi)

Il dimensionamento del servizio ed i costi della configurazione proposta sono riportati nel paragrafo "8 Configuratore".

5.2.1.4 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.

5.2.2 Infrastructure as a Service

5.2.2.1 Descrizione del servizio

I servizi di tipo Infrastructure as a Service (IaaS) sono servizi *Core* e prevedono l'utilizzo, da parte dell'Amministrazione, di risorse infrastrutturali virtuali erogate in remoto. Infrastructure as a Service (IaaS) è uno dei tre modelli fondamentali di servizio di cloud computing. Come tutti i servizi di questo tipo, fornisce l'accesso a una risorsa informatica appartenente a un ambiente virtualizzato tramite una connessione Internet. La risorsa informatica fornita è specificamente un hardware virtualizzato, in altri termini, un'infrastruttura di elaborazione. La definizione include offerte come lo spazio virtuale su server, connessioni di rete, larghezza di banda, indirizzi IP e bilanciatori di carico.

Figura 1 Infrastructure as a Service

Il servizio IaaS è suddiviso in:

- **IaaS Private**: consiste nella messa a disposizione, da parte del PSN, di una infrastruttura virtualizzata e dedicata, in grado di ospitare tutte le applicazioni in carico all'Amministrazione all'atto della stipula del Contratto, nonché di eventuali variazioni in corso d'opera, nel rispetto dei requisiti di affidabilità, disponibilità e sicurezza fisica e logica.

  Il PSN è responsabile della gestione dell'infrastruttura sottostante e rende disponibile gli strumenti e le console per la gestione in autonomia degli ambienti fisici e virtuali contrattualizzati.

- **IaaS Shared:** consiste nella messa a disposizione, da parte del PSN, di una infrastruttura virtualizzata e condivisa, in grado di ospitare tutte le applicazioni in carico all'Amministrazione all'atto della stipula del Contratto, nonché di eventuali variazioni in corso d'opera, nel rispetto dei requisiti di affidabilità, disponibilità e sicurezza fisica e logica.

  In questo caso, l'Amministrazione acquisisce il pool di risorse (vCPU, vGB di RAM, vGB di Storage) virtuali e il PSN è responsabile della gestione dell'infrastruttura sottostante, comprensiva degli strumenti di automation e orchestration.

5.2.2.2 Personalizzazione del servizio

Oggetto di migrazione sono i servizi indicati dall'Amministrazione nel Piano dei Fabbisogni, le cui specifiche infrastrutturali di migrazione su PSN sono riassunte nella tabella che segue.

Servizio	Applicativo	Nome Server	VCPU	RAM (GB)	Disco (GB)	Sistema Operativo
Macchina ponte	AREAS	vmponte	2	4	60	Windows Server 2019 o succ
SIO + AmmCont + motore integr	AREAS + OLIAMM Web+SPAGIC	app-1	6	32	80	Oracle Linux 8
SIO + AmmCont + motore integr	AREAS + OLIAMM Web+SPAGIC	app-2	6	32	80	Oracle Linux 8
AmmCont	OLIAMM SGP Client	dcsrv	2	4	40	Windows Server 2019 o succ
SIO + AmmCont + motore integr	AREAS + OLIAMM Web	lb	4	8	60	Oracle Linux 8
AmmCont	OLIAMM SGP Client	tsapp-2	6	24	100	Windows Server 2019 o succ
AmmCont	OLIAMM SGP Client	tsapp-1	6	24	150	Windows Server 2019 o succ
SIO + AmmCont	AREAS + OLIAMM Web+SPAGIC	vmtestcentos	6	32	80	Oracle Linux 8
Diabetologia	MetaClinic	App	4	16	300	Windows Server 2019 o succ
Dialisi	Medware	Web	4	12	100	Windows Server 2019 o succ
Dialisi	Medware	App	6	16	100	Windows Server 2019 o succ
Portale WEB		Web	4	16	100	OS Ubuntu 22.04 LTS
Portale WEB		Intranet	4	16	100	OS Ubuntu 22.04 LTS
Networking		Pfsense	2	4	50	FreeBSD
VA		Openvas	4	8	60	Ubuntu 20
Management		Zabbix Proxy	4	6	60	Ubuntu 20
Sicurezza		WAF1	2	8	500	Embedded
Sicurezza		WAF2	2	8	500	Embedded
Sicurezza		NGFW1	2	8	500	Embedded
Sicurezza		NGFW2	2	8	500	Embedded
		Totale	78	286	3.520	
		Totale risorse PSN	96	384	5.000	

Tabella 12: TO BE richiesto dall'Amministrazione per IaaS

La tabella che segue evidenzia le risorse infrastrutturali IaaS Shared HA fornite su PSN.

Servizio	Tipologia	Elemento	Quantità
Industry Standard	IaaS Shared HA	PooL Large (32VCPU/128 GB RAM)	3
Industry Standard	IaaS Storage HA	Storage HP Encrypted (500 GB)	10
Industry Standard	Sistemi Operativi	Windows Server STD CORE (2 core)	10
Industry Standard	Sistemi Operativi	Red Hat per VM	2

Tabella 13: Configurazione servizi IaaS Shared HA

Il dimensionamento considera una contingency aggiuntiva per recepire eventuali variazioni in corso d'opera.

NB: E' richiesto un Tenant unico, su cui allocare le risorse IaaS, che ricomprende anche le risorse del progetto 2023-0000001810260024-PPdF-P1R1 – ASL Biella - Digitalizzazione Cartelle Cliniche.

5.2.2.3 Dettaglio del servizio contrattualizzato (ID servizio, quantità costi)

Il dimensionamento del servizio ed i costi della configurazione proposta sono riportati nel paragrafo "8 Configuratore".

5.2.2.4 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.

5.2.3 Platform as a Service

5.2.3.1 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, astraendo 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.

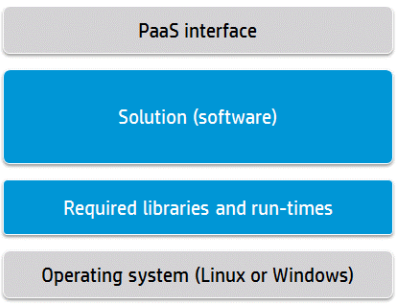


Figura 2 Platform as a Service

Il servizio PaaS si compone dei seguenti sottoservizi:

- **Database as a Service (DBaaS):** 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;
- **Identity Access Management (IAM):** consente di gestire in modo unificato e centralizzato l'autenticazione e l'autorizzazione per la messa in sicurezza delle applicazioni che migrano nel PSN;
- **Big Data:** consente la costruzione di Data Lake as a Service, servizi di analisi dati batch, stream e real-time con scalabilità orizzontale;
- **Artificial Intelligence (AI):** mette a disposizione un set di algoritmi pre-addestrati di Artificial Intelligence per utilizzarli in analisi del testo, audio/video o di anomalie ed una piattaforma per la realizzazione di modelli custom di machine/Deep Learning.

5.2.3.2 Platform as a Service - Database

Il Platform as a Service - Database 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).

5.2.3.3 Personalizzazione del servizio

Oggetto di migrazione sono i servizi indicati dall'Amministrazione nel Piano dei Fabbisogni, le cui specifiche infrastrutturali sono riassunte nelle tabelle che seguono.

Servizio	Applicativo	Nome Server	VCPU	RAM (GB)	Disco (GB)	SW DB
SIO + AmmCont	AREAS+OLIAMM	DB Test	4	24	2.000	Oracle Enterprise Ed V19c o succ
SIO + AmmCont	AREAS+OLIAMM	DB Prod	10	64	5.000	Oracle Enterprise Ed V19c o succ
Totale			14	88	7.000	

Tabella 14: TO BE richiesto dall'Amministrazione per PaaS DB Oracle

Servizio	Applicativo	Nome Server	VCPU	RAM (GB)	Disco (GB)	Sistema Operativo	SW DB
Diabetologia	MetaCliinic	DB Prod	4	16	200	Windows Server 2019 o succ	SQL Server 2019
Dialisi	Medware	DB Prod	6	16	300	Windows Server 2019 o succ	SQL Server 2019
Totale			10	32	500		

Tabella 15: TO BE richiesto dall'Amministrazione per PaaS DB SQL

La tabella che segue evidenzia le risorse infrastrutturali PaaS DB fornite su PSN.

Servizio	Tipologia	Elemento	Quantità
Industry Standard	PaaS DB	SQL Server (2 VCPU/4 GB RAM)	5
Industry Standard	IaaS Shared HA	PooL 1 GB RAM aggiuntivo	12
Industry Standard	IaaS Storage HA	Storage HP Encrypted (500 GB)	2
Industry Standard	PaaS DB	Oracle dbms Enterprise	4
Industry Standard	IaaS Shared HA	PooL 1 GB RAM aggiuntivo	40
Industry Standard	IaaS Storage HA	Storage HP Encrypted (500 GB)	14

Tabella 16: Configurazione servizi PaaS DB

5.2.3.4 Dettaglio del servizio contrattualizzato (ID servizio, quantità costi)

Il dimensionamento del servizio ed i costi della configurazione proposta sono riportati nel paragrafo "8 Configuratore".

5.2.3.5 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.

5.2.4 Data Protection e Disaster Recovery

5.2.4.1 Data Protection: Backup

5.2.4.2 Data Protection: Golden copy protetta

Quale ulteriore elemento di garanzia della protezione dei dati, oltre al backup standard, il PSN mette a disposizione un servizio opzionale aggiuntivo che analizza i backup mensili allo scopo di intercettare eventuali contaminazioni malware silenti che comprometterebbero la validità di un eventuale restore in produzione.

Si tratta di una funzionalità completamente gestita ed opzionale, attivabile su richiesta, in aggiunta al servizio di Backup standard: essa effettua la verifica e convalida dell'integrità dei dati durante le attività di backup e di esecuzione della golden copy; in particolare, quando viene eseguito il backup dei dati per la prima volta, vengono calcolati i checksum e CRC per ogni blocco di dati sul sistema sorgente e queste *signature* vengono utilizzate per convalidare i dati del backup. Una volta validate, tali *signature* vengono memorizzate con il backup stesso: ciò permette di eseguire automaticamente la verifica della consistenza dei dati salvati nel backup, utilizzando le signature salvate.

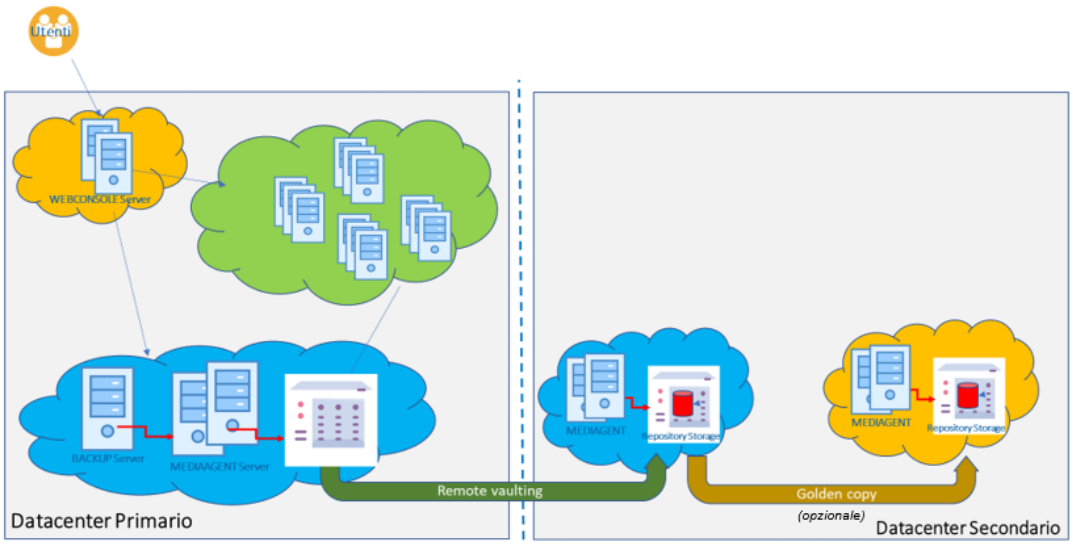


Figura 3 Architettura Funzionale Golden Copy

Questa modalità, insieme alle ulteriori procedure di sicurezza per l'accesso ai sistemi e alle applicazioni, garantisce la conservazione dei backup in un formato non cancellabile e inalterabile (*WORM: Write Once, Read Many*) e assicura che le attività di gestione operativa di routine (es. svecchiamento delle retention scadute, ecc) siano sempre sotto la competenza e il controllo di autorità di supervisione che non possono essere by-passate.
Ulteriori meccanismi di protezione dei dati impediscono la modifica o l'eliminazione dei file per un periodo di conservazione definito dalle policy utente o del sistema di backup (golden copy definita come WORM copy che non permette a nessuno, lato piattaforma di backup di cancellare i dati prima della loro scadenza).
Inoltre, sui sistemi sorgenti, in aggiunta ai tradizionali sistemi di protezione antivirus/antimalware, è possibile attivare meccanismi di identificazione di eventuali attacchi ransomware in maniera proattiva: qualsiasi attività sospetta sul file system dei sistemi da proteggere viene intercettata e segnalata alla console di gestione attraverso l'invio di allarmi che, opportunamente gestiti, consentono di condizionare e inibire la creazione della golden copy.
Le copie di backup potranno essere protette da ulteriori configurazioni, a livello di sottosistema storage, da eventuali attacchi di tipo *ransomware* non permettendo ad alcun processo esterno di modificare i dati salvati nei backup: Solo per le copie su cui non sarà stata segnalata alcuna anomalia di tipo *ransomware*, si potrà procedere all'archiviazione della "*golden copy*" in un ambiente protetto e in sola lettura.
Le principali caratteristiche del servizio sono:

- analisi automatizzata del backup per certificarne l'assenza di vulnerabilità (incluse attività sospette di *ransomware*);
- certificazione della Golden Copy da parte del PSN;
- protezione su storage distinto di backup, **privo di ogni accesso fisico e logico**;

- replica in **Region diverse e su canale cifrato.**

5.2.4.3 Personalizzazione del servizio

L'occupazione spazio del backup è calcolata in base alle policy richieste dall'Amministrazione, secondo quanto riportato sulla tabella che segue.

Servizio	Policy	Volume origine (GB)	Backup (GB)	Golden Copy (GB)
Tutte VM	Snapshot VM settimanale, retention 4 sett	4.000	20.000	10.000
DB SQL e Oracle Prod	Incrementale giornaliero (tasso variaz. 5%), Full settimanale, retention 4 sett	2.000	12.600	6.300
		6.000	32.600	16.300

Tabella 17: Dimensionamenti back up

5.2.4.4 Dettaglio del servizio contrattualizzato (ID servizio, quantità costi)

Il dimensionamento del servizio ed i costi della configurazione proposta sono riportati nel paragrafo "8 Configuratore".

5.2.4.5 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.

5.3 CONSOLE UNICA

La Fornitura prevede l'erogazione alle PAC, in maniera continuativa e sistematica, di una serie di servizi afferenti ad un Catalogo predefinito e gestito attraverso una Console Unica dedicata.
Il PSN metterà a disposizione delle Amministrazioni Contraenti una piattaforma di gestione degli ambienti cloud unica (CU) personalizzata, interoperabile attraverso API programmabili che rappresenterà per la PA l'interfaccia unica di accesso a tutte le risorse acquistate nell'ambito della convenzione. In particolare, la CU garantirà la possibilità alle Amministrazioni di configurare ed istanziare, in autonomia e con tempestività, le risorse contrattualizzate per ciascuna categoria di servizio e, accedendo alle specifiche funzionalità della console potrà gestire, monitorare ed utilizzare i servizi acquisiti.
Infine, attraverso la CU, l'Amministrazione avrà la possibilità di segnalare anomalie sui servizi contrattualizzati tramite l'apertura guidata di un ticket per la cui risoluzione il PSN si avvarrà del supporto di secondo livello di specialisti di prodotto/tecnologia.

5.3.1 Overview delle caratteristiche funzionali

La CU è progettata per interagire col PSN CLOUD ed integrare le funzionalità delle console native di cloud management degli OTT, fornendo un'interfaccia unica in grado di guidare in modo semplice l'utente nella definizione e gestione dei servizi sottoscritti utilizzando anche la tassonomia e le modalità di erogazione dei servizi previsti nella convenzione. Tale piattaforma presenta un'interfaccia applicativa responsive e multidevice ed è utilizzabile, oltre che in modalità desktop, anche mediante dispositivi mobili Android o iOS e abilita i sottoscrittori ad accedere in maniera semplificata agli strumenti che consentono di: √gestire in modalità integrata i profili di accesso alla CU tramite le funzionalità di Identity Management; disegnare l'architettura dei servizi acquistati e gestirne le eventuali variazioni; √consentire l'interfacciamento attraverso le API per la gestione delle risorse istanziate ma anche per definire un modello di IaC (Infrastructure as Code); segnalare eventuali anomalie in modalità "self".

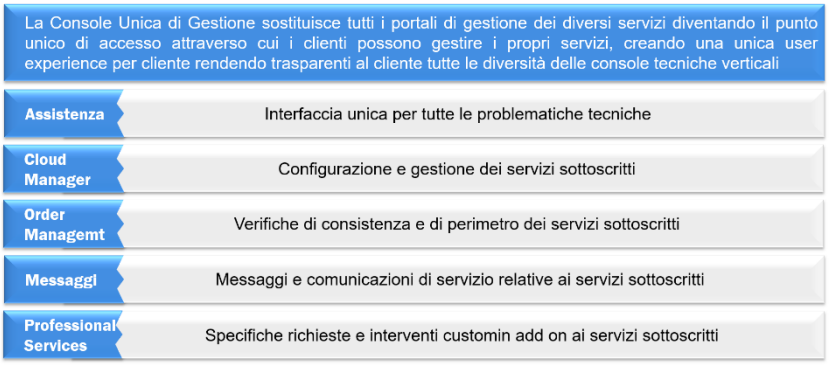


Figura 4 Funzionalità CU

Le aree di interazione che la piattaforma CU consente di gestire sono:

1. Area Attivazione contrattuale. All'atto dell'adesione alla convenzione da parte dell'Amministrazione, sulla CU: √saranno caricati i dati contrattuali ed anagrafici dell'Amministrazione; √generato il profilo del referente Master (Admin) della PA a cui sarà inviata una "Welcome Letter" con il link della piattaforma, l'utenza e la password (da modificare al primo login) per l'accesso alla CU; √sarà configurato il tenant dedicato alla PA, che rappresenta l'ambiente cloud tramite il quale la PA usufruirà dei servizi acquisiti (IaaS, PaaS, ecc.).

2. Area Access Management e profilazione utenze. L'accesso alla CU è gestito totalmente dal sistema di Identity Access Management (IAM). Gli utenti, previa registrazione, saranno censiti nello IAM, e con le credenziali rilasciate potranno accedere dalla console alle risorse allocate all'interno del proprio tenant. Anche la creazione dei profili delle utenze e la loro associazione con gli account degli utenti sarà gestita tramite le funzionalità di IAM in un'apposita sezione della CU denominata "Gestione Utenze".
3. Area Design & Delivery. Attraverso tale modulo della CU, l'Amministrazione Contraente potrà configurare in autonomia i servizi acquistati secondo le metriche definite per la convenzione, costruendo, anche mediante l'utilizzo di un tool di visualizzazione, la propria architettura cloud sulla base delle risorse contrattualizzate. Successivamente la CU, interagendo in tempo reale attraverso le API dei servizi cloud verticali, consentirà l'immediata attivazione delle risorse e dei servizi previsti nell'architettura attraverso la creazione di uno o più tenant logici per segregare le risorse computazionali dei clienti (Project). Il processo è gestito mediante un workflow automatizzato di delivery implementato tramite l'uso di Blueprint. La CU esporrà anche delle API affinché la singola Amministrazione Contraente possa interagire attraverso i propri tools di CD/CI, IaC (Terraform, Ansible...) oppure attraverso una propria CU come ulteriore livello di astrazione

e indipendenza (qualora ne avesse già a disposizione e quindi creare una CU Master Controller che interagisce con quella del PSN appunto via API).

4. Area Management & Monitoring. La piattaforma consentirà ai referenti delle Amministrazioni Contraenti di accedere alle funzionalità dedicate alla gestione e al monitoraggio delle risorse per ciascun servizio contrattualizzato e attivo all'interno delle specifiche piattaforme Cloud che erogano i servizi verticali. Punto focale della soluzione è la componente di Event Detection, che ha come obiettivo l'analisi dei log e degli eventi generati dalle piattaforme Cloud che erogano i servizi verticali per tutte le attività svolte dall'Amministrazione; tale modulo, in particolare, verificherà la compliance di tutte le richieste effettuate rispetto al perimetro contrattuale e bloccherà eventuali attività che esulino da tale contesto inviando alert, anche tramite e-mail, sia ai referenti della PA abilitati all'utilizzo della CU sia agli operatori delle strutture di Operations preposte alla gestione delle segnalazioni di anomalia sui servizi erogati.
5. Area Self Ticketing. Consente alla PA di segnalare in modalità self le anomalie riscontrate sui servizi cloud contrattualizzati.

5.3.2 Modalità di accesso

L'accesso in modalità sicura alla Console Unica prevede l'utilizzo del sistema di Identity Management, il cui form di login è integrato nell'interfaccia web. Tale sistema gestisce le identità degli utenti registrati e consente sia l'accesso in modalità desktop, sia tramite dispositivi mobili Android o iOS. Gli utenti, autorizzati dal sistema di Identity Access Management, potranno accedere dalla console alle risorse allocate all'interno del proprio tenant, sia per attività di "Design & Delivery" sia per attività di "Management & Monitoring".

5.3.3 Interfaccia applicativa della Console Unica

La Console Unica espone un'interfaccia profilata per ciascuna Amministrazione Contraente, presentando il set di servizi contrattualizzati e abilitandola ad eseguire le operazioni desiderate in piena autonomia. Di seguito è riportata una breve descrizione delle sezioni della Console Unica che sono rese disponibili. Dall'Home Page è possibile accedere alle sezioni:

- • Dashboard: consente di visualizzare il riepilogo dei dati contrattuali, verificare lo stato dei propri servizi IaaS, PaaS, ecc, il tracking dei ticket aperti e lo storico delle operazioni effettuate. In particolare, come evidenziato in Figura 4, cliccando sul widget di una specifica categoria di servizio (ad esempio Compute), sarà possibile visualizzare direttamente, secondo le metriche della convenzione, il dettaglio delle quantità totali delle risorse acquistate, quelle già utilizzate e le quantità ancora disponibili. Inoltre, accedendo al menu del profilo presente nell'header dell'interfaccia della Console Unica, il referente dell'Amministrazione avrà la possibilità di impostare gli indirizzi e-mail a cui inviare tutte le notifiche previste nella sezione Messaggi e selezionare altre impostazioni di base (lingua, ecc.).

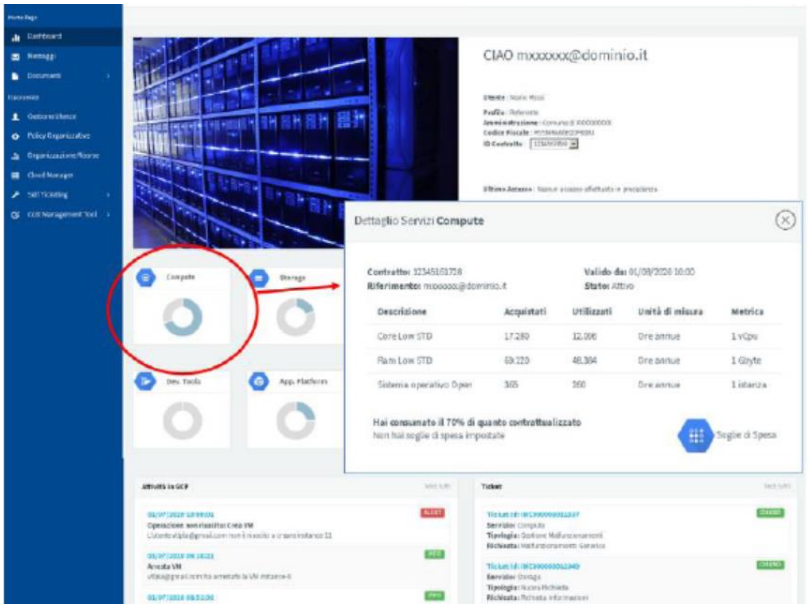


Figura 5 Dashboard CU

- Cloud Manager: in questa sezione, per tutti i servizi della convenzione, ciascuna Amministrazione potrà, nell'ambito della funzione di Design & Delivery:
  - costruire l'architettura cloud di ciascun Project all'interno del proprio tenant;
  - attivare i servizi in self-provisioning;
  - nell'ambito della funzione di Management & Monitoring:
  - effettuare operazioni di scale up e scale down sui servizi contrattualizzati;
  - gestire e monitorare tali servizi accedendo direttamente all'opportuna sezione della console.

Dettagliando ulteriormente la sezione di Design & Delivery, viene offerto ai referenti delle Amministrazioni Contraenti la possibilità di definire e configurare le risorse cloud contrattualizzate in modalità semplificata ed aderente ai requisiti e alla classificazione dei servizi della Convenzione, garantendo massima autonomia e tempestività nell'attivazione.

Il referente dell'Amministrazione, accedendo dalla sezione "I tuoi servizi" alla dashboard del Cloud Manager potrà nella fase di Design & Delivery:

- selezionare, utilizzando l'apposito menu a tendina presente nell'header della pagina, un Project tra quelli esistenti;
- visualizzare sia le categorie di servizio in cui sono state attivate risorse con il relativo dettaglio (identificativo della risorsa) sia quelle che non hanno risorse istanziate;
- istanziare in modo semplificato, per ciascuna categoria di servizi della Convenzione, attraverso la funzionalità "Configura", nuove risorse cloud utilizzando una procedura guidata che espone solo le funzionalità base per l'attivazione delle risorse cloud garantendo velocità di esecuzione. Nel caso in cui l'Amministrazione voglia, invece, utilizzare tutte le funzionalità di configurazione del Cloud Manager potrà accedervi direttamente dal tasto "Funzionalità Avanzate" presente in ciascuna finestra di configurazione.

- monitorare, in fase di attivazione delle risorse, lo stato di avanzamento dei consumi per la specifica categoria di servizi nel Project selezionato in modo da avere sempre a disposizione una vista delle quantità disponibili e in uso.

Dettagliando ulteriormente la sezione di Management & Monitoring, dopo aver terminato la fase di attivazione delle risorse cloud all'interno del Project selezionato, viene offerto ai referenti delle Amministrazioni Contraenti la possibilità di:

- gestire la singola risorsa accedendo direttamente alle specifiche funzionalità presenti console tramite il button "Gestisci";
- monitorare le performance della risorsa accedendo alle funzionalità di monitoraggio tramite il relativo button "Monitora".

In alternativa, il referente dell'Amministrazione ha la possibilità di accedere alle funzionalità avanzate della dashboard tramite il relativo button "presente nell'header della sezione.

5.4 SERVIZI E PIANO DI MIGRAZIONE

I servizi di Migrazione sono servizi Core del PSN quantificati e valutati economicamente sulla base di specifici assessment effettuati in fase di definizione delle esigenze dell'Amministrazione, tenendo conto di eventuali vincoli temporali ed architetturali di dettaglio oltre che di specifiche esigenze di customizzazione.
Per l'intero periodo di migrazione, il PSN mette a disposizione delle PA le seguenti figure professionali:

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

Si chiede alla PA la disponibilità di fornire uno o più referenti coi quali il Project Manager Contratto di Adesione 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.

Il Piano di Migrazione, che rappresenta un allegato parte integrante del presente documento, , è redatto adottando la metodologia basata sul framework EMG2C (Explore, Make, Go to Cloud), articolato in tre distinte fasi:

- **Explore**, che include le fasi relative all'analisi e alla valutazione dell'ambiente, per aiutare la PA a definire il proprio percorso di migrazione verso il cloud.
- **Make**, che comprende tutte le attività di design e di predisposizione dell'ambiente per permettere la migrazione in condizioni di sicurezza, tra cui anche i test necessari a validare il disegno di progetto.
- **Go**, che prevede il collaudo, l'attivazione dei servizi sulla nuova infrastruttura ed anche le attività di post go live necessarie al supporto e all'ottimizzazione dei servizi nel nuovo ambiente.

Gli step operativi in cui si articolano le suddette fasi sono:

- Analisi/Discovery
- Setup
- Migrazione
- Collaudo

Figura 6: Servizio di Migrazione - Metodologia EMG2C

1. **Analisi e Discovery**

Il primo step consiste nell'**Assessment**, finalizzato alla raccolta di tutte le informazioni necessarie e utili alla corretta esecuzione della migrazione. Tali informazioni saranno raccolte tramite:

- Survey, tramite compilazione da parte degli stakeholder della Amministrazione di template e checklist condivisi.
- Interviste one-to-one con i referenti dell'Amministrazione per la raccolta di dati inerenti alle applicazioni da migrare e alle loro potenziali rischi/criticità.
- Document repository ossia raccolta di tutta la documentazione disponibile presso la Pubblica Amministrazione.
- Tools di Analisi e Discovery a supporto

In particolare, questa fase di occuperà di reperire le informazioni:

a) delle piattaforme oggetto della migrazione;
b) delle applicazioni erogate dalla PA
c) dei dati oggetto di migrazione;
d) degli SLA delle singole applicazioni;
e) di eventuali finestre utili per la migrazione;
f) di eventuali periodi di indisponibilità delle applicazioni;
g) del Cloud Maturity Model;
h) analisi della sicurezza delle applicazioni e dell'ambiente da migrare;
i) Energy Optimization.

Inoltre, la Discovery ha lo scopo di raccogliere tutte le informazioni relative all' infrastruttura e ai workload da migrare. Questa attività consente di comporre un inventory ed una check list che supporteranno le successive attività e permetteranno, in fase di collaudo, la verifica di tutte le componenti migrate.
In funzione dei risultati dell'Assessment, si valuterà la **strategia ottimale di migrazione** verso l'ambiente target, in funzione dei seguenti driver:

- Ottimizzazione degli effort e dei tempi di migrazione.
- Minimizzazione dei rischi.

La fase di Analisi utilizzata per valutare le diverse strategie di Migrazione terrà conto anche del livello di maturità di adozione del Cloud della PA, delle dimensioni, complessità e conoscenza dei servizi della PA stessa.

Definita la strategia, si provvederà a dettagliare le attività necessarie a definire un **master plan** di tutti gli interventi necessari per implementare la migrazione prevista per la specifica Amministrazione; ciascun intervento sarà quindi declinato in un piano operativo.

2. **Set-up**

Rappresenta la fase propedeutica all'effettiva esecuzione della migrazione ed è finalizzata a garantire un'efficace predisposizione dell'ambiente target su cui dovranno essere movimentati i servizi/applicazioni dell'Amministrazione e si articola nelle seguenti fasi:

- Progettazione operativa e di dettaglio.
- Predisposizione dell'infrastruttura target presso i DC del PSN.
- Predisposizione dell'infrastruttura di networking relativa alla connessione tra la PA e i DC del PSN, se richiesta nel Piano dei Fabbisogni

3. **Migrazione**

Tale fase si articola nei seguenti step:

- Trasferimento dei workload e conseguente esecuzione di test "a vuoto" dell'ambiente migrato;
- Trasferimento dei dati, ovvero esecuzione dell'effettivo spostamento dei dati dal Data Center dell'Amministrazione all'interno dell'infrastruttura del PSN;
- Implementazione delle Policy di Sicurezza;
- Impostazione del monitoraggio.

4. **Collaudo**

Definizione Strategia di Collaudo: tale fase è finalizzata alla predisposizione della strategia ottimale di collaudo delle applicazioni migrate nell'ambiente target.

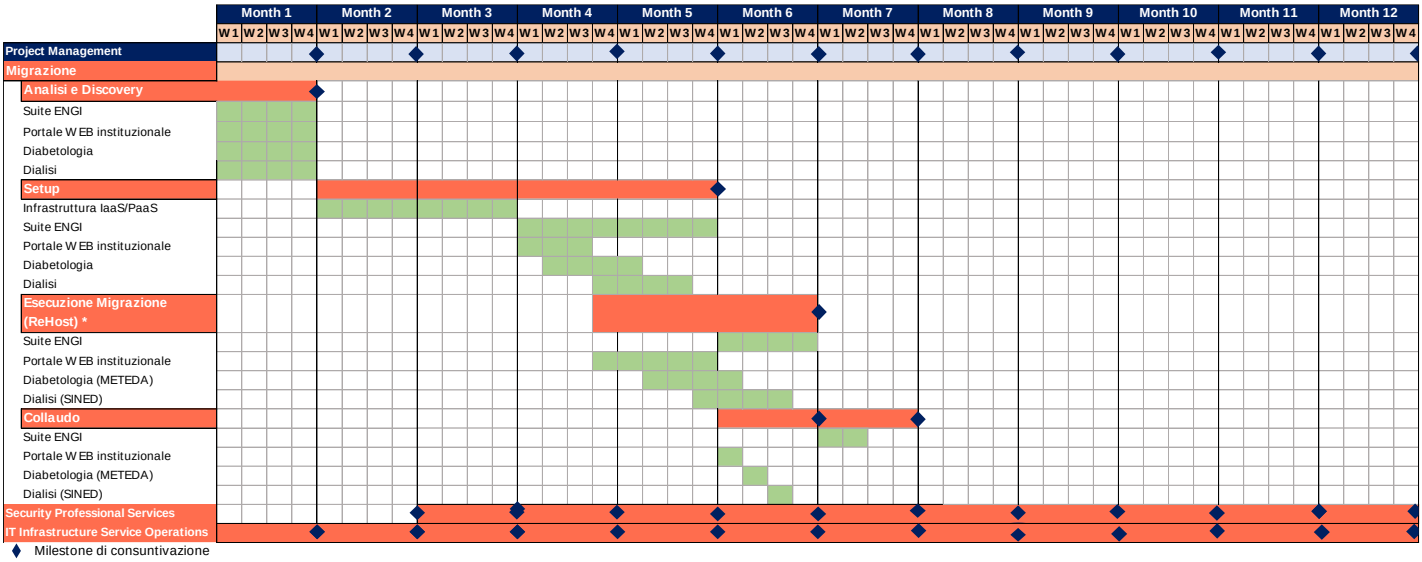
Esecuzione Collaudo: tale fase consiste nell'esecuzione dei test definiti in precedente e concordati con la Pubblica Amministrazione, per certificare il Go Live dell'applicazioni sull'ambiente target.

A valle del collaudo, sarà previsto un grace period temporaneo, da concordare con la Pubblica Amministrazione, durante il quale viene fornito un **supporto alle operation del cliente** per il fine tuning delle applicazioni migrate nell'ambiente target, in termini di prestazioni.

5.4.1 Piano di attivazione e Gantt

In questa sezione si riporta un diagramma di Gantt di massima per le attività previste nel progetto.

Figura 7: GANTT di massima



Il completamento della fase di setup coincide con "l'avvio della fase di gestione dei Servizi".

5.5 SERVIZI PROFESSIONALI

Sono resi disponibili all'Amministrazione servizi di evoluzione con l'obiettivo di: ✓migliorare eventuali ambienti precedentemente migrati sulla piattaforma PSN tramite Re-Host o tramite i servizi di Housing/Hosting; ✓ supportare la migrazione di applicativi on premise 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, i due servizi proposti sono quelli di Re-Platform e Re-Architect, in quanto queste due strategie di migrazione sono quelle che maggiormente massimizzano i benefici per l'Amministrazione di una piattaforma cloud come quella oggetto del presente progetto.
I due servizi si differenziano principalmente per la quantità del codice applicativo che viene modificato e, di conseguenza, per le tempistiche di attuazione. Il Re-platform modifica solamente alcuni componenti senza impattare il core dell'applicativo, mentre il Re-architect permette di portare l'applicazione in Cloud attraverso interventi puntuali sulla stessa.
Tali servizi non sono necessariamente alternativi ma possono eventualmente rappresentare fasi sequenziali di un programma di modernizzazione **applicativa**.
Per questi servizi, in base alla specifica esigenza, viene proposto un **team mix** composto dai profili professionali elencati in precedenza.

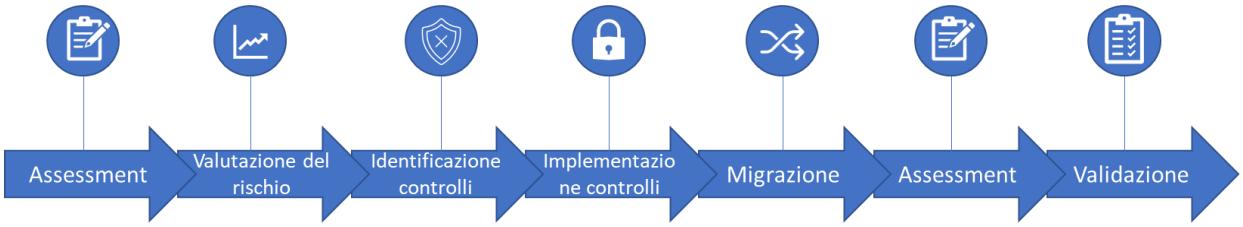
5.5.1 Security Profess. Services

La migrazione su cloud è un processo complesso e un cambiamento rilevante che non va preso alla leggera. Non esiste una procedura di migrazione immediata sul cloud, e anzi spesso i rischi di migrazione stessi non

vengono opportunamente valutati con il risultato che un'attività di migrazione che dovrebbe in teoria migliorare il livello complessivo di sicurezza delle applicazioni, di fatto lo diminuisce, esponendo i workload migrati a nuove minacce ed attacchi. È bene specificare che trasferendo le informazioni nel cloud non si trasferisce anche la responsabilità della sicurezza di tali informazioni. Il PSN offre molti strumenti nativi, all'interno delle diverse tipologie di cloud scelte, per gestire la sicurezza dei dati, ma questi devono essere in ogni caso previsti ed implementati dalle Amministrazioni. La responsabilità della sicurezza di tutti i dati trasferiti su cloud rimane sempre e comunque del cliente finale. Il fatto che le infrastrutture cloud siano intrinsecamente dotate di un livello di sicurezza elevato, di per sé non offre alcuna efficace garanzia sulla sicurezza delle informazioni ivi trasferite.
I servizi professionali di sicurezza sono quindi necessari, sinergici e parte integrante dei servizi di migrazione, e servono principalmente a valutare lo stato di sicurezza dei workload da migrare, prima e post migrazione, prevedendo in un approccio security-by-design l'analisi del rischio, l'identificazione, l'implementazione e la gestione dei controlli di sicurezza.
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



5.5.1.1 Personalizzazione del servizio

All'interno della fase iniziale della migrazione sono previsti dei servizi di assessment di sicurezza per indirizzare correttamente, dal punto di vista della sicurezza, l'allestimento degli ambienti oggetto del presente progetto del piano dei fabbisogni, fase che si compone delle seguenti attività:

- ICT Info gathering/Cyber Assessment
- Maturity Level Assessment

Questi servizi si definiscono Servizi security core pre-migrazione e saranno descritti nel paragrafo 5.5.1.2.
Inoltre, 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, tenendo conto delle fasi del progetto di migrazione:

- Secure design&planning;
- Supporto Device Management protezione perimetrale (NGFW, WAF);

- Security Event Monitoring, Notification & Log Management (fino a 500 Eventi per secondo – EPS));
- Compliance Assessment Framework Nazionale Cyber Security (FNSC);
- Vulnerability Assessment, Research & Exploitation;
- Static Application Security Testing;
- Dynamic Application Security Testing.

Data la natura delle attività i servizi professionali saranno erogati secondo due principali modalità:

- Servizi "a task":
  - Servizi security core pre-migrazione (§5.5.1.2);
  - Servizi professionali per il miglioramento della sicurezza delle infrastrutture e delle applicazioni della PA (ovvero, i Security Professional Services descritti ai paragrafi 5.5.1.3, 5.5.1.6, 5.5.1.7, 5.5.1.8, 5.5.1.9).
- Servizi" Ricorrenti": Servizi di supporto device management protezione perimetrale (ovvero i Security Professional Services descritti ai paragrafi 5.5.1.4, 5.5.1.5) In particolare, per quanto riguarda i servizi a task, saranno identificate e pianificate insieme all'Amministrazione le attività di lavorazione. 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 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.

Nei paragrafi seguenti vengono descritti i servizi professionali di sicurezza erogati per ASL Biella.

5.5.1.2 Servizi core pre-migrazione

CORE-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 da ASL Biella;
- 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.

CORE-Maturity Level Assessment

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*.

5.5.1.3 Secure Design Planning Security By Design a supporto della migrazione

Il servizio consiste nella predisposizione di un team di specialisti con le competenze e l'esperienza necessarie ad effettuare l'attività di supporto al design e alla progettazione della nuova infrastruttura ospitata nel PSN al fine di incrementare il livello di sicurezza.
Tale servizio, erogato in modalità "a task", **durante la fase di setup della migrazione**, prevede le seguenti attività:

- un'analisi preliminare volta a comprendere le tecnologie utilizzate e le specifiche caratteristiche al fine di poter predisporre le opportune linee guida o best practice in ambito security by design secondo una metodologia articolata in tre step di seguito descritti:
  - Step 1 – Analisi preliminare: In questa fase verrà eseguita un'analisi preliminare dello scenario proposto, svolgendo le seguenti attività:
    - raccolta delle informazioni sulle tecnologie utilizzate dall'Amministrazione contraente;
    - analisi del contesto specifico e classificazione del rischio Cyber sulla base dei livelli di criticità dei servizi a cui sono associate le specifiche tecnologie in esame;
    - analisi degli impatti di indisponibilità dei servizi, per l'individuazione delle aree problematiche e contromisure tecnologiche da adottare.
  - Step 2 – Disegno delle linee guida di security by design: In questa fase verranno identificate le linee guida di security by design, propedeutica alla fase di progettazione, svolgendo le seguenti attività:
    - predisposizione delle linee guida di security by design (sulla base della classificazione delle tecnologie fatta nella fase di assessment);
    - ipotesi di progettazione dell'infrastruttura sulla base delle contromisure suggerite;
    - condivisione della documentazione predisposta ai referenti coinvolti.
  - Step 3 – Follow-up & refining: In questa fase verranno condotte le attività follow-up e refining, svolgendo i seguenti passaggi:
    - Conduzione di specifiche interviste e/o workshop con gli stakeholder rilevanti per consolidare le informazioni e i contributi in base ai feedback raccolti;

- completamento della definizione delle contromisure da adottare secondo quanto recepito nelle fasi precedenti.

Il deliverable finale consiste in un report contenente la mappatura tra servizi, tecnologie, contromisure e rischio cyber residuo.

- Definizione del perimetro di servizio di Supporto Device Management e fornitura degli apparati necessari all'erogazione: definizione della baseline dei sistemi di sicurezza che saranno oggetto del servizio Security Device Management, ovvero quattro Firewall e quattro Web Application Firewall;
- Definizione delle politiche di sicurezza: un'analisi globale dell'infrastruttura dei sistemi di sicurezza oggetto del servizio; lo scopo è quello di analizzare l'as-is della configurazione esistente, delle policy preesistenti (es. standard policy) e dell'architettura complessiva garantendo in tal modo, già prima della migrazione, che le configurazioni delle piattaforme di sicurezza perimetrale siano opportunamente configurate per fornire l'esposizione minima necessaria;

5.5.1.4 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 sulla nuova infrastruttura ICT. Il servizio è erogato "as a service" remotamente ed include la gestione degli apparati e servizi di protezione perimetrale (per un totale massimo di qtà 4 apparati virtuali) con una finestra di servizio H8x5 e prevede:

- Definizione del perimetro di servizio: definizione della baseline dei sistemi di sicurezza che saranno oggetto del servizio Security Device Management;
- Definizione delle politiche di sicurezza: un'analisi globale dell'infrastruttura dei sistemi di sicurezza oggetto del servizio; lo scopo è quello di analizzare l'as-is della configurazione dei firewall, delle policy già configurare e dell'architettura complessiva nella quale i firewall sono posizionati
- Presa in carico dei sistemi, in RW, nello specifico le attività di presa in carico prevedono:
  - pianificazione temporale delle attività;
  - completa raggiungibilità dei devices e delle relative piattaforme di management ove presenti;
  - 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, creazioni tunnel vpn, modifica routing, /creazione/modifica profili UTM etc

Il servizio è erogato sul perimetro di apparati di sicurezza relativo all'infrastruttura di ASL Biella che prevede l'impiego di soluzioni di sicurezza virtuali come di seguito rappresentato:

- qty 2 v_NGFW (2 v_cpu, 8 gb RAM, 500 GB Storage)
- qty 2 v_WAF (2 v_cpu, 8 GB Ram, 500 GB Storage)

5.5.1.5 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 Analist, 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 dalla 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 18: 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 19: 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.

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'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 ASL Biella e fino a 500 EPS (Eventi Per Secondo).

5.5.1.6 Compliance Assessment Framework Nazionale Cyber Security (FNSC)

L'esigenza dell'Amministrazione è quella di avvalersi di servizi professionali, erogati in modalità "a task" e finalizzati alla fornitura del supporto specialistico per lo svolgimento di un assessment, basato su Framework Nazionale Cyber Security, in modo da:

- indicare il grado di adeguamento dell'Amministrazione ai livelli standard di sicurezza;
- individuare le possibili azioni correttive e soluzioni rispetto agli standard vigenti nell'organizzazione.

Il presente servizio è finalizzato ad eseguire un assessment per indicare la copertura e maturità dei controlli di sicurezza inerenti i seguenti ambiti:

- Governance, che indirizza l'insieme delle pratiche volte a definire le politiche e l'organizzazione necessarie per poter reagire e prevenire, in maniera efficace, alle minacce di sicurezza, in modo da

minimizzare l'impatto di possibili danni alle finalità istituzionali dell'Amministrazione dovuti ad incidenti di sicurezza di natura informatica.

- Prevent, che esprime la capacità di attuare pratiche e misure di sicurezza per la protezione delle informazioni, delle infrastrutture e dei servizi digitali presso l'Amministrazione.
- Detect, che esprime la capacità di individuare tempestivamente potenziali violazioni o eventi che possono influenzare o compromettere la sicurezza dell'Amministrazione.
- Respond & Recovery, che esprime la capacità di rispondere efficacemente ad un incidente di sicurezza e possibilmente di ripristinare i servizi impattati dallo stesso.

Nella definizione dei suddetti controlli si prenderanno in considerazione i requisiti previsti dal Framework Nazionale sulla Cyber Security (FNCS) e dalla normativa europea sul General Data Protection Regulation (GDPR).
Il perimetro delle attività descritte è da intendersi limitato alle attività del perimetro oggetto della migrazione sul PSN.
I servizi oggetto della presente fornitura hanno carattere consulenziale tecnico-organizzativa ed ogni decisione in merito alle soluzioni proposte è in capo al MIT stesso.
Come deliverable del servizio è previsto il rilascio di un documento che conterrà i risultati dell'assessment e che sarà condiviso con i referenti dell'Amministrazione. Verrà prodotta inoltre una presentazione di sintesi sulle attività svolte.

5.5.1.7 Vulnerability Assessment, Research & Exploitation

Il servizio sarà erogato "a task" 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.

Le attività oggetto di test saranno eseguite a valle della formalizzazione dei seguenti documenti:

- *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.

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).

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 e verrà erogato secondo una pianificazione di un ciclo annuo post migrazione.

5.5.1.8 Static Application Security Testing

Static application security testing (SAST) è il servizio orientato all'identificazione delle vulnerabilità software presenti all'interno del codice sorgente delle applicazioni. Nello specifico l'attività ha come obiettivo:

- la verifica della presenza di vulnerabilità associate a dati corrotti in ingresso che possono portare ad un comportamento anomalo dell'applicazione;
- la verifica dei rischi collegati all'assenza di sequenze di operazioni che, se non eseguite in un certo ordine, portano a violazioni sulla memoria o all'uso scorretto di determinate variabili;
- la rilevazione di eventuali problematiche legate all'uso pericoloso di determinate funzioni o API;
- la verifica dei parametri di configurazione dell'applicazione; la verifica della presenza di azioni di scrittura o lettura di un numero di dati superiore alla reale capacità del buffer.

Strategia Operativa: esecuzione di test di vulnerabilità del codice sorgente classificando le rilevanze per livello di criticità, identificando le porzioni di codice interessate e indirizzando gli interventi volti alla loro risoluzione. In questa fase sono condotti dei test sul codice sorgente per verificare l'assenza di security flaws. Le azioni di controlli di sicurezza possono essere così sintetizzate:

- Data Validation: verifica la presenza di vulnerabilità che possono riguardare eventuali dati corrotti in ingresso che possono portare a un comportamento anomalo dell'applicazione;
- Control Flow: verifica i rischi collegati all'assenza di specifiche sequenze di operazioni che, se non eseguite nel corretto ordine, possono portare a violazioni sulla memoria o l'uso scorretto di determinati componenti;
- Analisi Semantica: rileva eventuali problematiche legate all'uso pericoloso di determinate funzioni o API (es. funzioni deprecate);
- Controllo Configurazioni: verifica i parametri intrinseci di configurazione dell'applicazione;
- Buffer Validation: verifica la presenza di buffer overflow exploitabile attraverso la scrittura o lettura di un numero di dati superiore alla reale capacità del buffer stesso.

L'analisi di sicurezza del codice sorgente verrà eseguita con l'ausilio di un insieme di metodi e strumenti per il testing di sicurezza applicativa opportunamente scelti e configurati.
I metodi sono riferiti alle modalità di classificazione delle vulnerabilità riscontrate sul codice secondo le prescrizioni OWASP, ovvero:

- Difficoltà di sfruttamento della vulnerabilità da parte di un attaccante;
- Impatto tecnologico nel caso in cui la vulnerabilità venga sfruttata da un attaccante;
- Difficoltà di risoluzione della problematica.

Gli strumenti di supporto per le analisi statiche di sicurezza saranno selezionati in base ai linguaggi ed alle tecnologie utilizzate dalle singole applicazioni e saranno tesi ad individuare bugs di sicurezza nel codice relativamente alle indicazioni fornite dagli standard OWASP top 10, SANS top 25, NIST SP 800-53 ed altri. Le vulnerabilità riscontrate saranno comunque referenziate in notazione CWE (Common Weakness Enumeration).

Il servizio erogato soddisfa tutti i requisiti tecnici e funzionali ed è conforme alle best practice internazionali e agli standard OWASP, eseguendo nelle varie fasi di test controlli come nel seguito riportato a titolo esemplificativo e non esaustivo:

- per la "*Data Validation*" è verificata l'esposizione a cross-site scripting, SQL injection, e corruzione di dati applicativi;
- per il "*Control Flow*" è verificata la corretta sequenza delle operazioni, tra moduli e funzioni nei percorsi delle chiamate indicando aree in cui l'applicazione potrebbe essere suscettibile a vulnerabilità;
- per la *"Verifica Semantica"* è eseguita la rilevazione di problematiche legate all'uso di particolari funzioni, ad esempio viene evidenziato se l'applicazione richiama un metodo dichiarato obsoleto (deprecated);
- per l'analisi delle *configurazioni* il prodotto fornisce informazioni sull'uso di elementi esterni, framework o librerie, potenzialmente vulnerabili;
- per la "*Buffer Validation*" vengono verificate le situazioni di buffer overflow che si verificano quando si spostano dati superiori alla capacità del buffer che deve gestirli (per i linguaggi memory unmanaged).

A seguito della scansione effettuata sarà prodotto un report indicante le vulnerabilità individuate e la relativa classificazione. La quotazione del servizio è fatta per un'unica sessione fino a un massimo di 100.000 LoC (Lines of Code).

5.5.1.9 Dynamic Application Security Testing

Il servizio sarà erogato in modalità a task da remoto e consente l'identificazione delle vulnerabilità all'interno delle applicazioni Web e l'analisi dell'esposizione al rischio di attacchi informatici ai Sistemi Informativi mediante l'utilizzo di tecniche di analisi dinamica.
L'attività ha lo scopo di rilevare e gestire le vulnerabilità applicative che insistono sui sistemi informativi in ambiente WEB di produzione/pre-produzione e loro relative classificazione e prioritizzazione.
Il servizio prevede l'esecuzione dei test dinamici di sicurezza per le applicazioni per la verifica delle vulnerabilità tenendo conto dell'esposizione e dell'ambiente operativo in cui l'applicazione è in esecuzione.

L'input è rappresentato dalle informazioni relative ai target da analizzare e le relative modalità attuative che dovranno essere concordate con l'Amministrazione.
L'analisi comprenderà almeno i seguenti ambiti:

- Configurazione (es. directory traversing);
- Autenticazione (cifratura degli accessi, password policy, dictionary attack);
- Autorizzazione (Privilege escalation);
- Input Validation.

A seguito delle scansioni effettuate sarà prodotto un report indicante le vulnerabilità individuate e la relativa classificazione.
Il report costituirà il *Detailed Software Security Assessment Report* contenente i dettagli tecnici del livello di sicurezza dell'istanza a run-time applicazione:

- Riferimenti ai tipi di attacco e vulnerabilità;
- Vulnerabilità/rischi identificati e la gravità di ognuno in termini di potenziale impatto sul sistema software oggetto dell'analisi;
- Notazioni e classificazione dei bugs sulla sicurezza secondo gli standard applicabili.

Il servizio è limitato all'analisi di massimo q.tà 5 target (di max 30 url) con periodicità annuale per un massimo di 15 server.
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.

5.5.2 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, ovvero dell'infrastruttura VM della PA. 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.
Le attività che il PSN potrà prendere in carico, previa valutazione, sono:

- Monitoraggio;
- Workload management;
- Infrastructure optimization;
- Capacity management;
- Operation management;
- Compliance management;
- Vulnerability & Remediation;
- Supporto tramite la Cloud Management Platform al:

- Provisioning, Automazione e Orchestrazione di risorse;
- Inventory, Configuration Management.

Inoltre, potranno essere erogate attività di System Management sui sistemi operativi Microsoft e Linux e sugli ambienti middleware effettuando la gestione ordinaria e straordinaria dei Server e dei Sistemi Operativi:

- creazione/gestione delle utenze, dei privilegi e gli accessi ai sistemi;
- controllare il corretto funzionamento del Sistema Operativo, verificando i processi/servizi tramite agent di monitoring.
- gestione dei log di sistema e verifica delle eventuali irregolarità.
- gestione dei files di configurazione dei sistemi.
- problem management di 2° livello, attivando le procedure e gli strumenti necessari per l'analisi dei problemi, individuando e rimuovendo le cause degli stessi.
- effettuare il restore in caso di failure di sistema recuperando i dati di backup.
- segnalazione dell'esigenza dell'applicazione di patch/fix per il mantenimento dei sistemi agli standard di sicurezza e qualità previsti dai produttori software (segnalazione periodica o eccezionale a fronte di gravi vulnerabilità).
- applicazione delle patch/fix, sulla base di quanto concordato con il cliente o a seguito di segnalazione dagli enti deputati alla sicurezza dei sistemi e dei Data Center.

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.

5.5.2.1 Personalizzazione del servizio

Le attività elencate nel seguito sono associate a fornitore qualificato PSN/Amministrazione secondo il metodo della Matrice RACI. Di seguito la descrizione dei 4 Ruoli:

(R) Responsible: Il Responsible svolge concretamente il lavoro. Ogni attività richiede almeno un Responsible.

(A) Accountable: l'Accountable è la persona o stakeholder che detiene l'ownership dell'attività, ovvero deve dare l'approvazione finale quando tale attività viene completata.

(C) Consulted: sono tutte quelle persone o parti interessate che hanno bisogno di dare un contributo prima che il lavoro possa essere svolto e approvato, ovvero forniscono informazioni e ci si aspetta una comunicazione bidirezionale.

(I) Informed: persone o parti interessate che devono essere tenute al corrente sullo stato di avanzamento dell'attività. Hanno bisogno di aggiornamenti sui progressi o sulle decisioni prese, ma non hanno bisogno di essere consultati formalmente, né contribuiscono direttamente all'attività o alla decisione.

Nelle seguenti voci vi è la descrizione del campo "Tipologia supporto":

- Extra con Service Ticket: Attività di progetto escluse dal canone di servizio, erogabili a fronte del pagamento di uno o più gettoni di ingaggio aggiuntivo (ExtraServiceTicket)
- Incluso: Attività inclusa nel canone di servizio
- Escluso: Attività non inclusa nel canone di servizio

PSN prenderà in carico i server ed i servizi richiesti dopo verifica del corretto funzionamento degli stessi. Sarà cura del Cliente, prima del passaggio di consegne, garantire una infrastruttura senza errori o problemi di funzionamento, o in alternativa prevedere una fase di Assessment e presa in carico da parte di fornitore qualificato PSN comprensiva di un'attività di ottimizzazione dell'infrastruttura.

Finestra di servizio: H24 Attività Sistemistiche

Attività	Tipologia supporto	PSN	Cliente
OS Win/Lin - Gestione configurazioni di OS/applicativi	Incluso	RA	CI
OS Win/Lin – Configurazione, modifica, monitoring e troubleshooting backup e restore sistema operativo	Incluso	RA	CI
OS Win/Lin - Hardening e performance tuning	Incluso	RA	CI
OS Win/Lin - Gestione immagini per remote install/boot	Incluso	RA	CI
OS Win/Lin - IP Address Management	Incluso	RA	CI
OS Win/Lin - Asset inventory server	Incluso	RA	CI
OS Win/Lin - Deploy OS su virtual machines	Incluso	RA	CI
OS Win/Lin – Upgrade Sistema Operativo	Incluso	RA	CI
OS Win/Lin – Installazione Pack e Add-on aggiuntivi	Incluso	RA	CI
OS Win/Lin – Migrazione applicativa	Escluso	CI	RA
OS Win/Lin – gestione applicativa (Middleware)	Escluso	CI	RA
OS Win/Lin - Troubleshooting (Incident e Change management)	Incluso	RA	CI
OS Win/Lin - Patching OS con cadenza trimestrale (in accordo con i fornitori applicativi)	Incluso	RA	CI
OS Win/Lin - Creazione/gestione delle utenze, i privilegi e gli accessi ai sistemi	Incluso	RA	CI
OS Win/Lin - Gestione dei log di sistema e verifica delle eventuali irregolarità Nota: Richiede l'utilizzo di software di Log Management, tali prodotti a seconda del numero di sorgenti e alla retention prevede un costo di licenza.	Incluso	RA	CI
OS Win/Lin – Gestione e installazione agenti di monitoraggio su OS	Incluso	RA	CI
OS Win/Lin - Monitoraggio dei parametri principali del server (CPU, RAM e spazio disco)	Incluso	RA	CI
OS Win/Lin – Condivisione eventuali parametri di monitoraggio avanzati (Servizi,Applicativi)	Incluso	CI	RA
OS Win/Lin – Scansione delle vulnerabilità con software OpenVAS e condivisione report	Incluso	RA	CI

vCloud – Gestione dell'ambiente IAAS, CaaS	Incluso	RA	CI
Vcloud – Capacity Management	Incluso	RA	CI
Vcloud – Implementazione policy NSX (supporto a microsegmentazione, implementazione VPN)	Incluso	RA	CI
Vcloud – Gestione Load Balancer	Incluso	RA	CI
Consulenza su progetti evolutivi atti a migliorare la gestione e la sicurezza dell'ambiente del cliente	Incluso	RA	CI
Implementazione di Major change o di nuovi progetti non a perimetro che ridisegnino il design infrastrutturale	Extra con Service Ticket	RA	CI

Tabella 20: RACI per attività sistemistiche

Il servizio è rivolto esclusivamente al personale dei Sistemi Informativi dell'Amministrazione che si farà carico della raccolta e del filtro delle segnalazioni dei propri Utenti Finali e aprirà una segnalazione verso fornitore qualificato PSN.

Finestra di servizio: H24 Supporto DBA

Attività	Tipologia supporto	PSN	Cliente
Monitoraggio disponibilità	Incluso	RA	CI
Gestione utenze e profili di database	Incluso	RA	CI
Gestione dei parametri d'istanza e di memoria	Incluso	RA	CI
Controllo periodico allocazione spazi per evitare blocchi applicativi	Incluso	RA	CI
Verifica dei log e tuning dei parametri d'istanza per il miglioramento e il mantenimento delle performance	Incluso	RA	CI
Verifica corretta schedulazione backup Nota: Richiede sottoscrizione Managed Backup Service	Incluso	RA	CI
Ricostruzione oggetti deframmentati (tabelle ed indici)	Incluso	RA	CI
Monitorare la crescita anomala di oggetti di database	Incluso	RA	CI
Segnalazione dell'esigenza dell'applicazione di patch o upgrade di release (da comunicare ai fornitori applicativi)	Incluso	RA	CI
Applicazione delle patch	Incluso	RA	CI
Upgrade di release	Escluso	CI	RA
Interventi di natura applicativa	Escluso	CI	RA

Tabella 21: RACI per attività DBA

Service Level Agreement

	Descrizione	**KPI**
Presa in carico	Tempo di presa in carico guasti e avvio delle attività risolutive con rilascio di un ticket identificativo della chiamata	T ≤ 30’ nel 90% dei casi. T ≤ 45’ nel 100% dei casi.
Risoluzione Critical Faults	Tempo di risoluzione guasti bloccanti	T ≤ 4H nel 90% dei casi. T ≤ 8H nel 100% dei casi.
Risoluzione NO Critical Faults	Tempo di risoluzione guasti non bloccanti	T ≤ 8H nel 90% dei casi. Next Business Day nel 100% dei casi.
Risoluzione Change e Service Request	Tempo di risoluzione di richieste di change/Service Request	T ≤ 8H nel 90% dei casi. Next Business Day nel 100% dei casi.

Tabella 22: Livelli di servizio per attività sistemistiche

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.
- **Enterprise Architect**: ha elevate conoscenze su differenti aree tecnologiche che gli permettono di progettare architetture enterprise, sviluppando modelli basati su Enterprise Framework; è responsabile di definire la strategia abilitante per l'evoluzione dell'architettura, mettendo in relazione la missione di business, i processi e l'infrastruttura necessaria.
- **Cloud Application Architect**: ha conoscenze approfondite ed esperienze progettuali nella definizione di architetture complesse e di Ingegneria del Software dei sistemi Cloud ed agisce come team leader degli sviluppatori ed esperti tecnici; è responsabile della progettazione dell'architettura di soluzione applicative di cloud computing, assicurando che le procedure e i modelli di sviluppo siano aggiornati e conformi agli standard e alle linee guida applicabili
- **Cloud Application Specialist**: ha consolidate conoscenze tecnologiche delle soluzioni cloud e dell'integrazione di soluzioni applicative basate su un approccio cloud computing based; è responsabile della delivery di progetti basate su soluzioni Cloud.
- **Business Analyst**: È responsabile dell'analisi dei dati anche in ottica di business, e della relativa raccolta dei requisiti necessari a migliorare la qualità complessiva dei servizi IT forniti.
- **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.
- **Junior Information Security Consultant**: Garantisce l'esecuzione delle misure di sicurezza per proteggere le reti ed i sistemi informatici. Attua le regole definite in materia di sicurezza delle informazioni.
- **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.
- **Data Protection Specialist**: Figura professionale dedicata ad affiancare il titolare, gli addetti ed i responsabili del trattamento dei dati affinché conservino i dati e gestiscano i rischi seguendo i princìpi e le indicazioni del Regolamento europeo.
- **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.
- **System Integration & Test Specialist**: Contribuisce in differenti aree dello sviluppo del sistema, effettuando il testing delle funzionalità del sistema, identificando le anomalie e diagnosticandone le possibili cause. Utilizza e promuove strumenti automatici.

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.

ANAGRAFICA AMMINISTRAZIONE	
Codice Fiscale	1810260024
Ragione Sociale	ASL Biella
IDENTIFICATIVO DOCUMENTO	
Emesso da	CSO
Codice Documento	
Versione	1

VERSIONE CONFIGURATORE	3.8

RIEPILOGO PREZZI				
SERVIZIO	Totale UT		Totale Canone Annuale	
Industry Standard			€	128.242,76
Hybrid Cloud on PSN Site			€	-
SecurePublicCloud			€	-
Public Cloud PSN Managed			€	-
Servizi di Migrazione	€	299.726,32		
Servizi Professionali	€	1.977.124,99		
TOTALE	€	2.276.851,31	€	128.242,76

CODICE	SERVIZIO	TIPOLOGIA	ELEMENTO	QUANTITA	DR	Totale UT	Totale Canone Annuale
IAAS16	IndustrySt andard	IaaSSharedHA	Pool Large	3			€ 14.214,2100
IAAS07	IndustrySt andard	IaaSStorageHA	Storage HP Encrypted	10			€ 4.987,0000
PAAS03	IndustrySt andard	PaaSDB	SQL server	5			€ 21.574,1000
IAAS18	IndustrySt andard	IaaSSharedHA	Pool 1GB ram aggiuntivo	12			€ 387,8400
IAAS07	IndustrySt andard	IaaSStorageHA	Storage HP Encrypted	2			€ 997,4000
PAAS04	IndustrySt andard	PaaSDB	Oracle dbms Enterprise	4			€ 53.472,0000
IAAS18	IndustrySt andard	IaaSSharedHA	Pool 1GB ram aggiuntivo	40			€ 1.292,8000
IAAS07	IndustrySt andard	IaaSStorageHA	Storage HP Encrypted	14			€ 6.981,8000
SO01	IndustrySt andard	SistemiOperativi	Windows Server STD CORE (2 core)	10			€ 1.165,4000
SO02	IndustrySt andard	SistemiOperativi	Red Hat per VM	2			€ 1.087,7400
DP02	IndustrySt andard	DataProtection	Backup	33			€ 10.697,2800
DP03	IndustrySt andard	DataProtection	Golden copy	17			€ 6.612,8300
HOUSING05	IndustrySt andard	Housing	IP Pubblici /29 (8 indirizzi)	2			€ 130,9000
HOUSING07	IndustrySt andard	Housing	Housing router in sala TLC	2			€ 4.205,9000
HOUSING03	IndustrySt andard	Housing	Rilancio connettività (fibra monomodale)	4			€ 435,5600

CODICE	SERVIZIO	TIPOLOGIA	ELEMENTO	QUANTITA'	DR	Totale UT	Totale Canone Annuale
SP-07	ServiziMigrazione	FiguraMigrazione	Project Manager	118		€ 43.872,4000	
SP-01	ServiziMigrazione	FiguraMigrazione	Cloud Application Architect	70		€ 27.114,5000	
SP-09	ServiziMigrazione	FiguraMigrazione	Business Analyst	111		€ 33.015,8400	
SP-02	ServiziMigrazione	FiguraMigrazione	Database Specialist and Administrator	116		€ 28.919,9600	
SP-03	ServiziMigrazione	FiguraMigrazione	System Integrator & Testing Specialist	107		€ 22.474,2800	
SP-12	ServiziMigrazione	FiguraMigrazione	System and Network Administrator	56		€ 16.656,6400	
SP-04	ServiziMigrazione	FiguraMigrazione	Cloud Application Specialist	77		€ 24.281,9500	
SP-06	ServiziMigrazione	FiguraMigrazione	Enterprise Architect	115		€ 47.760,6500	
SP-23	ServiziMigrazione	FiguraMigrazione	Systems Architect	115		€ 55.630,1000	
SP-07	ServiziProfessionali	ITInfrastructureServiceOperation	Project Manager	160		€ 59.488,0000	
SP-01	ServiziProfessionali	ITInfrastructureServiceOperation	Cloud Application Architect	100		€ 38.735,0000	
SP-09	ServiziProfessionali	ITInfrastructureServiceOperation	Business Analyst	50		€ 14.872,0000	
SP-02	ServiziProfessionali	ITInfrastructureServiceOperation	Database Specialist and Administrator	1050		€261.775,5000	
SP-12	ServiziProfessionali	ITInfrastructureServiceOperation	System and Network Administrator	990		€294.465,6000	
SP-04	ServiziProfessionali	ITInfrastructureServiceOperation	Cloud Application Specialist	100		€ 31.535,0000	
SP-06	ServiziProfessionali	ITInfrastructureServiceOperation	Enterprise Architect	100		€ 41.531,0000	
SP-07	ServiziProfessionali	SecurityProfessionalServices	Project Manager	196		€ 72.872,8000	
SP-13	ServiziProfessionali	SecurityProfessionalServices	Security Principal	163		€ 84.844,7600	
SP-14	ServiziProfessionali	SecurityProfessionalServices	Senior Information Security Consultant	163		€ 69.074,5100	
SP-15	ServiziProfessionali	SecurityProfessionalServices	Junior Information Security Consultant	261		€ 77.631,8400	
SP-01	ServiziProfessionali	SecurityProfessionalServices	Cloud Application Architect	163		€ 63.138,0500	
SP-04	ServiziProfessionali	SecurityProfessionalServices	Cloud Application Specialist	261		€ 82.306,3500	
SP-16	ServiziProfessionali	SecurityProfessionalServices	Security Solution Architect	327		€138.572,7900	
SP-17	ServiziProfessionali	SecurityProfessionalServices	Senior Security Auditor/Analyst	718		€320.342,8800	
SP-18	ServiziProfessionali	SecurityProfessionalServices	Junior Security Analyst	327		€ 92.295,7500	
SP-19	ServiziProfessionali	SecurityProfessionalServices	Senior Penetration Tester	131		€ 48.705,8000	
SP-20	ServiziProfessionali	SecurityProfessionalServices	Junior Penetration Tester	196		€ 51.089,3600	
SP-21	ServiziProfessionali	SecurityProfessionalServices	Forensic Expert	131		€ 48.705,8000	
SP-22	ServiziProfessionali	SecurityProfessionalServices	Data Protection Specialist	229		€ 85.142,2000	

9 Rendicontazione

Di seguito, viene riportato un prospetto contenente la modalità di distribuzione dei servizi professionali, distinti per tipologia. I canoni dell'infrastruttura saranno attivati una volta resi disponibili i relativi servizi. La consuntivazione avverrà su base SAL mensili o bimestrali in linea all'effettivo effort erogato in termini di giorni/uomo delle relative figure professionali.

			Milestone di avanzamento % - Gate approvativi											
Servizi di Migrazione (Milestone Based)	Peso		Month 1	Month 2	Month 3	Month 4	Month 5	Month 6	Month 7	Month 8	Month 9	Month 10	Month 11	Month 12
		€ TOT												
- Analisi & Discovery	20%	59.945,26 €	59.945,26 €											
- Setup	30%	89.917,90 €					89.917,90 €							
- Migrazione	40%	119.890,53 €						119.890,53 €						
- Collaudo	10%	29.972,63 €							29.972,63 €					
Servizi professionali (avanzamento/task)		€ TOT												
- Security Professional Serv	100%	1.234.722,89 €		110.754,64 €	9.525,15 €	9.525,15 €	9.525,15 €	9.525,15 €	9.525,15 €	9.525,15 €	9.525,15 €	9.525,15 €	9.525,15 €	9.525,15 €
- IT Service Operation	100%	742.402,10 €	6.186,68 €	6.186,68 €	6.186,68 €	6.186,68 €	6.186,68 €	6.186,68 €	6.186,68 €	6.186,68 €	6.186,68 €	6.186,68 €	6.186,68 €	6.186,68 €
Totale		€ TOT	66.131,95 €	116.941,33 €	15.711,84 €	15.711,84 €	105.629,73 €	135.602,37 €	45.684,47 €	15.711,84 €	15.711,84 €	15.711,84 €	15.711,84 €	15.711,84 €

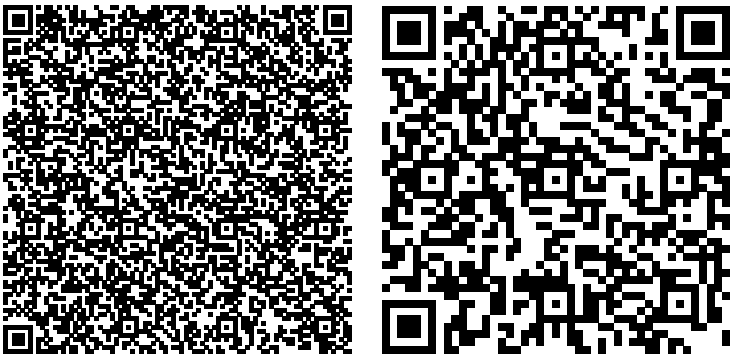
Figura 8: Prospetto di rendicontazione

	Anno 2024	Anno 2025	Anno 2026	Anno 2027	Anno 2028	Anno 2029	Anno 2030	Anno 2031	Anno 2032	Anno 2033
Infrastruttura	106.868,97 €	128.242,76 €	128.242,76 €	128.242,76 €	128.242,76 €	128.242,76 €	128.242,76 €	128.242,76 €	128.242,76 €	128.242,76 €
Servizi professionali di migrazione	299.726,32 €									
Servizi professionali di conduzione	280.246,40 €	188.542,07 €	188.542,07 €	188.542,07 €	188.542,07 €	188.542,07 €	188.542,07 €	188.542,07 €	188.542,07 €	188.542,07 €
	686.841,69 €	**316.784,83 €**	**316.784,83 €**	**316.784,83 €**	**316.784,83 €**	**316.784,83 €**	**316.784,83 €**	**316.784,83 €**	**316.784,83 €**	**316.784,83 €**

Figura 9: Distribuzione importi economici sulla durata del contratto

Categoria Servizio	Nome Servizio	Classificazione	Applicativo	Vendor	Gestore	Infrastruttura di Origine (Location Attuale)	Tipologia di migrazione indicata nel Piano di Migrazione su PA Digitale/Avviso	Infrastruttura su cui migrare da dichiarare per la partecipazione all'avviso	Fornitore Infrastruttura Target	Colonna1
Servizi di funzionamento	Gestione documentale	ORDINARIO	Archiflow - Determine Delibere	SIAV	Nivola (IN-12,IA-13)	On Premise	B-Aggiornamento di applicazioni sicure in Cloud	Infrastruttura della PA adeguata	CSI-Piemonte (IN-12,IA-13)	Linea Finanziamento 1.2 (progetto avviato dopo 1° febbraio 2020)
Servizi di funzionamento	Conservazione digitale	ORDINARIO	Archiflow - Determine Delibere	SIAV						
ASSISTENZA OSPEDALIERA	ASSISTENZA SPECIALISTICA AMBULATORIALE	CRITICO	C4C	Dedalus	Cloud fastweb	Cloud Non Qualificato	A-Trasferimento in sicurezza dell'infrastruttura IT	Cloud Qualificato	Fastweb	
ASSISTENZA DISTRETTUALE	ASSISTENZA SPECIALISTICA AMBULATORIALE	CRITICO	CUP Regionale prenotazione							
Servizi di funzionamento	Produttività individuale e Collaboration	ORDINARIO	Gmail Nuvole	TIM	Cloud google	Cloud Non Qualificato	A-Trasferimento in sicurezza dell'infrastruttura IT	Cloud Qualificato	Google	
ASSISTENZA DISTRETTUALE	CURE DOMICILIARI (ANCHE PALLIATIVE)	CRITICO	Hero	Dedalus	Cloud fastweb	Cloud Non Qualificato	A-Trasferimento in sicurezza dell'infrastruttura IT	Cloud Qualificato	Fastweb	
ASSISTENZA OSPEDALIERA	PRONTO SOCCORSO	CRITICO	Hero	Dedalus	Fastcloud (IN92,IA-2271)	Cloud Non Qualificato	B-Aggiornamento di applicazioni sicure in Cloud	Cloud Qualificato	Fastweb	Linea Finanziamento 1.2 (progetto avviato dopo 1° febbraio 2020)
ASSISTENZA OSPEDALIERA	RICOVERO ORDINARIO PER ACUTI	CRITICO	Hero	Dedalus	Fastcloud (IN92,IA-2271)	Cloud Non Qualificato	B-Aggiornamento di applicazioni sicure in Cloud	Cloud Qualificato	Fastweb	Linea Finanziamento 1.2 (progetto avviato dopo 1° febbraio 2020)
ASSISTENZA OSPEDALIERA	DAY SURGERY	CRITICO	Hero	Dedalus	Fastcloud (IN92,IA-2271)	Cloud Non Qualificato	B-Aggiornamento di applicazioni sicure in Cloud	Cloud Qualificato	Fastweb	Linea Finanziamento 1.2 (progetto avviato dopo 1° febbraio 2020)
ASSISTENZA OSPEDALIERA	DAY HOSPITAL	CRITICO	Hero	Dedalus	Fastcloud (IN92,IA-2271)	Cloud Non Qualificato	B-Aggiornamento di applicazioni sicure in Cloud	Cloud Qualificato	Fastweb	Linea Finanziamento 1.2 (progetto avviato dopo 1° febbraio 2020)
ASSISTENZA OSPEDALIERA	RIABILITAZIONE E LUNGODEGENZA POST ACUZIE	CRITICO	Hero	Dedalus	Fastcloud	Cloud Non Qualificato	B-Aggiornamento di applicazioni sicure in Cloud	Cloud Qualificato	Fastweb	
RISCHIO CLINICO	RISCHIO CLINICO	CRITICO	Hero	Dedalus	Fastcloud	Cloud Non Qualificato	B-Aggiornamento di applicazioni sicure in Cloud	Cloud Qualificato	Fastweb	
ASSISTENZA DISTRETTUALE	PERCORSI ASSISTENZIALI INTEGRATI	CRITICO	Hero (PDTA)	Dedalus	Fastcloud	Cloud Non Qualificato	B-Aggiornamento di applicazioni sicure in Cloud	Cloud Qualificato	Fastweb	
ASSISTENZA DISTRETTUALE	ASSISTENZA SPECIALISTICA AMBULATORIALE	CRITICO	Hero refertazione	Dedalus	Fastcloud (IN92,IA-2271)	Cloud Non Qualificato	B-Aggiornamento di applicazioni sicure in Cloud	Cloud Qualificato	Fastweb	Linea Finanziamento 1.2 (progetto avviato dopo 1° febbraio 2020)
Servizi di funzionamento	Personale	ORDINARIO	HR	CSI-Piemonte	Nivola	Cloud Non Qualificato	A-Trasferimento in sicurezza dell'infrastruttura IT	Infrastruttura della PA adeguata	CSI-Piemonte	
Servizi di funzionamento	Conservazione digitale	ORDINARIO	HR SPI	CSI-Piemonte	Nivola	Cloud Non Qualificato	A-Trasferimento in sicurezza dell'infrastruttura IT	Infrastruttura della PA adeguata	CSI-Piemonte	
ASSISTENZA OSPEDALIERA	ATTIVITÀ DIAGNOSTICA	CRITICO	LIS	Dedalus	On premise	On Premise	B-Aggiornamento di applicazioni sicure in Cloud	PSN (Polo Strategico Nazionale)	Telecom	
Servizi di funzionamento	Conservazione digitale	ORDINARIO	LIS	Dedalus						
ASSISTENZA OSPEDALIERA	ASSISTENZA SPECIALISTICA AMBULATORIALE	CRITICO	Medware Dialisi	Sined	On premise	On Premise	B-Aggiornamento di applicazioni sicure in Cloud	PSN (Polo Strategico Nazionale)	Telecom	Autofinanziamento o con fondi derivanti da adesione al bando DTD
ASSISTENZA OSPEDALIERA	ASSISTENZA SPECIALISTICA AMBULATORIALE	CRITICO	Mystar - Diabetologia	Meteda	On premise	On Premise	B-Aggiornamento di applicazioni sicure in Cloud	PSN (Polo Strategico Nazionale)	Telecom	Autofinanziamento o con fondi derivanti da adesione al bando DTD
ASSISTENZA DISTRETTUALE	ASSISTENZA FARMACEUTICA	CRITICO	OLIAMM	Engineering	Cloud Telecom	Cloud Non Qualificato	A-Trasferimento in sicurezza dell'infrastruttura IT	PSN (Polo Strategico Nazionale)	Telecom	Escluso da Azienda Zero per piano dismissione regionale
Servizi di funzionamento	Conservazione digitale	ORDINARIO	OLIAMM	Engineering	????	Cloud Non Qualificato	A-Trasferimento in sicurezza dell'infrastruttura IT	PSN (Polo Strategico Nazionale)	Telecom	Escluso da Azienda Zero per piano dismissione regionale
Servizi di funzionamento	Contabilità, Bilancio e Controllo	ORDINARIO	OLIAMM	Engineering	Cloud telecom	Cloud Non Qualificato	A-Trasferimento in sicurezza dell'infrastruttura IT	PSN (Polo Strategico Nazionale)	Telecom	Escluso da Azienda Zero per piano dismissione regionale
Servizi di funzionamento	Acquisti	ORDINARIO	OLIAMM	Engineering	Cloud telecom	Cloud Non Qualificato	A-Trasferimento in sicurezza dell'infrastruttura IT	PSN (Polo Strategico Nazionale)	Telecom	Escluso da Azienda Zero per piano dismissione regionale
Servizi di funzionamento	Produttività individuale e Collaboration	ORDINARIO	Pec	CSI-Piemonte Piemonte	Nivola	Cloud Non Qualificato	A-Trasferimento in sicurezza dell'infrastruttura IT	Infrastruttura della PA adeguata	CSI-Piemonte	
Servizi di funzionamento	Protocollo	ORDINARIO	Protocollo	SIAV	Nivola	On Premise	B-Aggiornamento di applicazioni sicure in Cloud	Infrastruttura della PA adeguata	CSI-Piemonte	Linea Finanziamento 1.2 (progetto avviato dopo 1° febbraio 2020)
Servizi di funzionamento	Personale	ORDINARIO	RAP (Rilevazione Assenze Presenze)	CSI-Piemonte Piemonte	Nivola	Cloud Non Qualificato	A-Trasferimento in sicurezza dell'infrastruttura IT	Infrastruttura della PA adeguata	CSI-Piemonte	
ASSISTENZA OSPEDALIERA	ATTIVITÀ DIAGNOSTICA	CRITICO	RIS/PACS	Philips S.p.A.	On premise	On Premise	B-Aggiornamento di applicazioni sicure in Cloud	PSN (Polo Strategico Nazionale)	Telecom	
Servizi di funzionamento	Conservazione digitale	ORDINARIO	RIS/PACS	Philips S.p.A.	On premise	On Premise	B-Aggiornamento di applicazioni sicure in Cloud	PSN (Polo Strategico Nazionale)	Telecom	
SERVIZI INFORMATIVI	COMUNICAZIONE ISTITUZIONALE WEB E OPEN DATA	ORDINARIO	Sito Web	Dromedian	Cloud AWS	Cloud Non Qualificato	A-Trasferimento in sicurezza dell'infrastruttura IT	PSN (Polo Strategico Nazionale)	Telecom	Linea di Finanziamento 1.1. - PSN
Servizi di funzionamento	Personale	ORDINARIO	SPI (Contabilità Economica Dipendenti)	CSI-Piemonte Piemonte	Nivola	Cloud Non Qualificato	A-Trasferimento in sicurezza dell'infrastruttura IT	Infrastruttura della PA adeguata	CSI-Piemonte	
ASSISTENZA OSPEDALIERA	ATTIVITÀ TRASFUSIONALI	CRITICO	TMM	Mesis	On Premise	On Premise	B-Aggiornamento di applicazioni sicure in Cloud	PSN (Polo Strategico Nazionale)	Telecom	Autofinanziamento o con fondi derivanti da adesione al bando DTD
ASSISTENZA OSPEDALIERA	ATTIVITÀ DIAGNOSTICA	CRITICO	WInSAP	Engineering	Cloud Telecom	Cloud Non Qualificato	B-Aggiornamento di applicazioni sicure in Cloud	PSN (Polo Strategico Nazionale)	Telecom	Linea di Finanziamento 1.1. - PSN (non candidabile separatamente necessaario migrare anche gli altri servizi classificati "attività diagnostica" RIS e LIS)
FASCICOLO SANITARIO REGIONALE	FASCICOLO SANITARIO REGIONALE	CRITICO	Xvalue Repository	Dedalus	Cloud Fastweb	Cloud Non Qualificato	A-Trasferimento in sicurezza dell'infrastruttura IT	Cloud Qualificato	Fastweb	

Siav S.p.A - Contrassegno Elettronico



TIPO CONTRASSEGNO QR Code

IMPRONTA DOC AC9D59082D23A108211CD45D820E67279B086549964308DF424EF5C6602B9063

Firme digitali presenti nel documento originale

Firma in formato p7m: ROSSI LEILA
Firma in formato pdf: EMANUELE IANNETTI

Dati contenuti all'interno del Contrassegno Elettronico

Data Determina 22/05/2024
Numero Determina 588

Credenziali di Accesso per la Verifica del Contrassegno Elettronico

URL

IDENTIFICATIVO DPER9-5290

PASSWORD bjqf1

DATA SCADENZA Senza scadenza