REGIONE CALABRIA
GIUNTA REGIONALE

DIPARTIMENTO TURISMO, MARKETING TERRITORIALE E MOBILITA'
SETTORE 02 - OSSERVATORIO SUL TURISMO E DELLA MOBILITA'

Assunto il 28/12/2023

Numero Registro Dipartimento 931

==========

DECRETO DIRIGENZIALE

"Registro dei decreti dei Dirigenti della Regione Calabria"

N°. 224 DEL 10/01/2024

Settore Gestione Entrate	**Settore Ragioneria Generale – Gestione Spese**
VISTO di regolarità contabile, in conformità all'allegato 4/2 del D.lgs. n. 118/2011 **Sottoscritto dal Dirigente del Settore** Dott.STEFANIZZI MICHELE (con firma digitale)	VISTO di regolarità contabile attestante la copertura finanziaria, in conformità all'allegato 4/2 del D.lgs. n. 118/2011 **Sottoscritto dal Dirigente del Settore** Dott. GIORDANO UMBERTO ALESSIO (con firma digitale)

Oggetto: PR Calabria FESR FSE+ 2021/2027 - Op 1 - Obiettivo Specifico 1.2. - Azione 1.2.1 – Approvazione Progetto del Piano dei Fabbisogni relativo all'intervento "Sistemi Informativi Turismo In Cloud". Cup: J61E23000140006 - Cig Derivato: A0445608E7. Nomina RUP e DEC. Impegno e Accertamento

IL DIRIGENTE GENERALE

VISTI

- la L.R.7/1996 “Norme sull’ordinamento della struttura organizzativa della Giunta regionale e sulla Dirigenza Regionale”;
- il D.P.G.R. 354 del 24.6.1999, relativo alle norme in materia di separazione dell’attività amministrativa di indirizzo e di controllo da quello della gestione modificato dal D.P.G.R. 206 del 15.12.2000;
- la DGR 665/2022 di approvazione del Regolamento regionale di riorganizzazione delle strutture della Giunta regionale 12/2022;
- il D.D.G. 4844 del 04.5.2022 e successiva rettifica n.4906 del 5.5.2022 con il quale è stata approvata la nuova struttura organizzativa del Dipartimento Transizione Digitale ed Attività Strategiche;
- la DGR 531 del 31.10.2022 con la quale il dott. Tommaso Calabrò è stato individuato come Dirigente generale del Dipartimento “Transizione Digitale ed Attività Strategiche”;
- il D.P.G.R. 107 del 3.11.2022 con la quale è stato conferito, al Dott. Tommaso Calabrò, l’incarico di Dirigente Generale del Dipartimento Transizione digitale ed attività strategiche;
- il D.D.G. n. 16681 del 16/12/2022 avente ad oggetto “Dipartimento Turismo, Marketing Territoriale e Mobilità. Definizione organizzazione degli uffici. Regolamento regionale 14 dicembre 2022, n.12”;
- la DGR n. 185 del 28/04/2023 con la quale è stata individuata quale Dirigente Generale del Dipartimento Turismo, Marketing territoriale e Mobilità”, la dott.ssa Maria Antonella Cauteruccio;
- il D.P.G.R. n. 36 del 28/04/2023 di conferimento dell’incarico di Dirigente Generale del Dipartimento “Turismo, Marketing territoriale e Mobilità” della Giunta della Regione Calabria alla dott.ssa Maria Antonella Cauteruccio;
- il decreto 9347/2023 con il quale è stato conferito l’incarico di dirigente del Settore “Osservatorio sul turismo e della mobilità” al dott. Bruno Zito;
- la Legge 241/1990 e s.m.i.;
- la L.R. 34/2002 e s.m.i. recante "Riordino delle funzioni amministrative regionali e locali" e ritenuta la propria competenza;
- la DGR 118 del 31.3.2023 con la quale è stato approvato il Piano Triennale per la Prevenzione della Corruzione e della Trasparenza 2023-2025;
- il d.lgs. 118 del 23.6.2011 e ss.mm.ii. recante “Disposizioni in materia di armonizzazione dei sistemi contabili e degli schemi di bilancio delle Regioni, degli enti locali e dei loro organismi, a norma degli articoli n. 1 e 2 della Legge 42/2009”;
- la L.R. 8/2002 “Ordinamento del bilancio e della contabilità della Regione Calabria”;
- la L.R. 47/2011 art.4;
- la L.R. 56/2023 “Legge di stabilità regionale 2024”;
- la L.R. 57/2023 “Bilancio di previsione finanziario della Regione Calabria per gli anni 2024 – 2026”;
- la DGR 779 del 28.12.2023 – Documento tecnico di accompagnamento al Bilancio di previsione finanziario della Regione Calabria per gli anni 2024 – 2026 (Artt. 11 e 39, c. 10, D.Lgs. 118/2011);
- la DGR 780 del 28.12.2023 – Bilancio finanziario gestionale della Regione Calabria per gli anni 2024-2026 (Art. 39, c. 10, del D. Lgs. 118/2011);
- la L.R. 8 del 5.4.2008 “Riordino dell’organizzazione turistica regionale”;
- la DGR 76/2022 "Approvazione del logo per le attività di marketing, promozione e comunicazione turistica della destinazione Calabria. Atto di indirizzo”;
- il Decreto 4948/2022 di Approvazione delle linee guida per l’utilizzo del brand ‘’Calabria Straordinaria’’;
- la DGR 190 del 28.4.2023 “Approvazione proposta di Piano Regionale di Sviluppo Turistico Sostenibile (PRSTS) per il triennio 2023/2025";
- la DGR 261 del 9.6.2023 “Approvazione del Piano Esecutivo Annuale di Promozione Turistica 2023”;
- il d.lgs. 50/2016 e ss.mm.ii.;
- il D.M. n.49/2018 recante: «Approvazione delle linee guida sulle modalità di svolgimento delle funzioni del direttore dei lavori e del direttore dell'esecuzione»;
- la DGR 86 del 5.3.2019 di approvazione del regolamento regionale per la disciplina degli incentivi per funzioni tecniche art. 113 del d.lgs 50/2016 s.m.i., pubblicato sul Burc 34/2019;

VISTI

- il Regolamento (UE, EURATOM) 2020/2093 del Consiglio DELL'Unione Europea del 17.12.2020 che stabilisce il Quadro Finanziario Pluriennale per il periodo 2021-2027;
- il Regolamento (UE) 2021/1057 del Parlamento del Parlamento Europeo e del Consiglio del 24.6.2021 che istituisce il Fondo sociale europeo Plus (FSE+) e che abroga il regolamento (UE) 1296/2013;
- il Regolamento (UE) 2021/1058 del Parlamento Europeo e del Consiglio del 24.6.2021 relativo al Fondo europeo di sviluppo regionale e al Fondo di coesione;
- il Regolamento (UE) 2021/1059, recante disposizioni specifiche per l'obiettivo «Cooperazione territoriale europea» (Interreg) sostenuto dal Fondo europeo di sviluppo regionale e dagli strumenti di finanziamento esterno;
- il Regolamento (UE) 2021/1060 del Parlamento Europeo e del Consiglio del 24.6.2021 recante le disposizioni comuni applicabili al Fondo europeo di sviluppo regionale, al Fondo sociale europeo Plus, al Fondo di coesione, al Fondo per una transizione giusta, al Fondo europeo per gli affari marittimi, la pesca e l'acquacoltura, e le regole finanziarie applicabili a tali fondi e al Fondo Asilo, migrazione e integrazione, al Fondo Sicurezza interna e allo Strumento di sostegno finanziario per la gestione delle frontiere e la politica dei visti;
- la proposta di Accordo di Partenariato della politica di coesione europea 2021-2027 dell'Italia, trasmesso alla Commissione europea, secondo le modalità richieste per la notifica formale da parte del Dipartimento per le politiche di coesione in data 17.1.2022, in conformità agli articoli 10 e seguenti del Regolamento (UE) 2021/1060 recante le disposizioni comuni sui fondi (RDC);
- la DGR 136 del 15.6.2020 con cui è stato avviato il percorso di definizione e stesura del Programma Regionale (PR) FESR/FSE+ relativo al ciclo di programmazione 2021-2027, con l'obiettivo di definire le strategie per conseguire l'integrazione, in scala regionale, della Politica di coesione europea e delle sue politiche prioritarie, tenendo conto sia della S3 e sia della Strategia Regionale per lo Sviluppo Sostenibile (SRSvS);
- la DGR 121 del 28.3.2022 "Approvazione del documento finale Strategia di specializzazione Intelligente 2021/2027, della Relazione di autovalutazione dell'assolvimento della condizione abilitante Buona governance della S3 e dei relativi Annex" con la quale si è aperta la fase di negoziato a livello comunitario e nazionale;
- la DGR 122 del 28.3.2022 "Approvazione del Programma Regionale Calabria FESR FSE+ 2021-2027 e del Rapporto Ambientale di VAS;
- la Decisione della Commissione C(2022)8027 final del 3.11.2022 che approva il "Programma Regionale Calabria FESR FSE+ 2021-2027" per il sostegno a titolo del Fondo europeo di sviluppo regionale e del Fondo sociale europeo Plus, nell'ambito dell'obiettivo "Investimenti a favore dell'occupazione e della crescita" per la regione Calabria in Italia CCI 2021IT16FFPR003;
- la DGR 600 del 18.11.2022 di "Presa d'atto della conclusione del negoziato per l'approvazione del Programma Regionale Calabria FESR FSE+ 2021-2027 - Decisione della Commissione C(2022) 8027 final del 3.11.2022. Istituzione Comitato di Sorveglianza 2021-2027 e ulteriori adempimenti e con la quale è stato conferito l'incarico di Autorità di Gestione del Programma Regionale Calabria FESR FSE+ 2021-2027 al Dott. Maurizio Nicolai Dirigente del Dipartimento "Programmazione Unitaria";
- la DGR 103 del 13.3.2023 con cui è stato istituito il Comitato di Sorveglianza del Programma Regionale Calabria FESR/FSE+ 2021-2027;
- la DGR 109 del 13.3.2023 avente ad oggetto: "PR Calabria FESR FSE+ 2021-2027 3 Integrazione della delibera di Giunta Regionale 600 del 18.11.2022 recante "Presa d'atto della conclusione del negoziato per l'approvazione del programma regionale della Calabria FESR FSE+ 021-2027 3 Decisione della Commissione C (2022) 8027 final del 3.11.2022. Istituzione Comitato di Sorveglianza 2021-2027 e ulteriori adempimenti";
- la DGR 144 del 31.3.2023 "Approvazione finale dei documenti relativi alla "S3 2021- 2027" individuazione dei membri del Comitato Interdipartimentale S3 e sua istituzione";
- la Deliberazione del Consiglio regionale della Calabria 182 dell'11.4.2023 di "Presa d'atto della conclusione del negoziato per l'approvazione del Programma Regionale Calabria FESR/FSE+ 2021-2027: Decisione della Commissione C(2022) 8027 final del 3.11.2022 Istituzione del Comitato di Sorveglianza 2021-2027 e ulteriori adempimenti";

- il DDG 9369 del 30.6.2023 recante “PR Calabria FESR FSE Plus 2021/202. Descrizione dei Sistemi di Gestione e Controllo ai sensi del Regolamento 1060/2021. Approvazione”;
- la DGR 362 del 27.7.2023 che modifica la DGR 299 del 23.6.2023 avente ad oggetto “Organigramma delle strutture amministrative della Giunta Regionale Responsabili dell’attuazione degli obiettivi specifici delle azioni del Programma Regionale Calabria FESR FSE 2021 – 2027 approvato con decisione della Commissione Europea n. C(2022) 8027 final del 3.11.2022 ”;

PREMESSO che

- in data 24.8.2022 tra il Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri e la Società Polo Strategico Nazionale spa è stata stipulata la convenzione che regola la concessione da parte del Dipartimento relativa alla prestazione da parte del Concessionario (PSN spa) in favore delle singole Amministrazioni Utenti di un Catalogo di Servizi, finalizzato alla messa a disposizione di un’infrastruttura digitale per i servizi infrastrutturali e applicativi in cloud per la gestione di dati sensibili denominata “Polo Strategico Nazionale”, appositamente progettata, predisposta ed allestita, ad alta affidabilità, localizzata sul territorio nazionale, con caratteristiche adeguate (con riferimento, in particolare, alla circolare dell’Agenzia per l’Italia Digitale – AgID n. 5 del 30.11.2017) ad ospitare la migrazione dei dati frutto della razionalizzazione e consolidamento dei Centri di elaborazione Dati e relativi sistemi informatici delle pubbliche amministrazioni di cui all’articolo 33-septies del decreto-legge 179/2012, convertito, con modificazioni, dalla L. 221/2012, come modificato dall’articolo 35 del D.L. 76/2020 nonché come ulteriormente modificato dall’art. 7 del D.L. 152/2021 ed a ricevere la migrazione dei detti dati affinché essi siano poi gestiti attraverso una serie di servizi da rendere alle amministrazioni titolari dei dati stessi, vale a dire Servizi Infrastrutturali; Servizi di Gestione della Sicurezza IT; Servizi di Disaster recovery e Business Continuity; Servizi di Assistenza ai fruitori dei servizi prestati;
- la Società Polo Strategico Nazionale S.p.A (PSN spa) con sede legale in via Goito 4, numero di iscrizione nel Registro delle Imprese di Roma 1678264, C.F. e Partita IVA 16825251008 è costituita dai seguenti operatori economici:
  - TIM S.p.A. con sede legale in via G. Negri 1 – 20123 Milano iscritta nel Registro della Imprese di Milano al numero 1580695 - C.F. e Partita IVA 00488410010;
  - Leonardo S.p.A., con sede legale in Roma, piazza Monte Grappa 4, C.F. e iscrizione presso il Registro delle Imprese di Roma 00401990585 e Partita Iva 00881841001;
  - SOGEI – Società Generale di Informatica – S.p.A. con sede legale in Roma, via Mario Carucci 99 - C.F. e iscrizione nel Registro delle Imprese 0327910580, Partita IVA 01043931003;
  - CDP Equity S.p.A. con sede legale in Milano, via San Marco 21/A - C.F. e Partita IVA e iscrizione nel Registro delle Imprese di Milano 07532930968;
- la realizzazione del Polo Strategico Nazionale si inserisce come strumento di attuazione del Piano Nazionale di Ripresa e Resilienza, con particolare riferimento all’obiettivo di «Digitalizzare la Pubblica Amministrazione italiana con interventi tecnologici ad ampio spettro accompagnati da riforme strutturali» di cui alla Missione 1, Componente M1C1 e contribuisce al raggiungimento degli “Obiettivi Italia Digitale 2026”, nonché di quelli dettati dall’Agenzia per l’Italia Digitale per la realizzazione dell’Agenda Digitale Italiana, in coerenza con l' “Obiettivo 3 – Cloud e Infrastrutture Digitali” orientato alla migrazione dei dati e degli applicativi informatici delle pubbliche amministrazioni;
- l’infrastruttura a PSN si rivolge alla Pubblica Amministrazione Centrale (organi costituzionali, Presidenza del Consiglio dei Ministri, Ministeri e relativi organi periferici, agenzie fiscali), alla Pubblica Amministrazione Locale (Regioni, Province, Città metropolitane, Comuni, agenzie territoriali) e alle Aziende Sanitarie (Aziende Sanitarie Locali, Aziende Ospedaliere, Policlinici, Aziende Ospedaliero-universitarie) offrendo una copertura capillare estesa a tutti i livelli della PA;
- nell’ambito della concessione fra DTD e PSN S.p.A. le Amministrazioni Utenti potranno stipulare il Contratto entro 30 (trenta) mesi dalla sottoscrizione della Convenzione salvo proroga di quest’ultimo termine concordata tra Concedente e Concessionario, come stabilito nell’art. 18 comma 1 della Convenzione;

CONSIDERATO che la Regione Calabria, al fine di ottemperare alla realizzazione di rinnovati strumenti a supporto delle campagne a favore del turismo e della mobilità sul territorio, ha necessità di approvvigionarsi di un ambiente cloud ad hoc, adeguato ad ospitare le infrastrutture necessarie per l'erogazione dei suddetti servizi ed in grado di supportare possibili evoluzioni future. In tale ottica, il PSN offre un'infrastruttura cloud che soddisfa i requisiti di alta affidabilità, resilienza e indipendenza tecnologica, adeguati alle esigenze di mantenimento, disponibilità, sicurezza e gestione dati della piattaforma. Inoltre, l'Amministrazione beneficerà di un mix di figure professionali esperte che assicurino l'operatività e la disponibilità in completa sicurezza degli ambienti ospitati presso le soluzioni offerte dal PSN;

RICHIAMATO l'art. 18 della convenzione di adesione al PSN, secondo cui le Amministrazioni Utenti per migrare dati e servizi devono:

- redigere e inviare al Concessionario Polo Strategico Nazionale il piano dei fabbisogni contenente l'elenco aggiornato del perimetro IT coinvolto nell'affidamento dei servizi, con indicazione delle modalità richieste;
- approvare il progetto del piano dei fabbisogni e il piano di migrazione di massima redatto dal Concessionario sulla base dei requisiti dettagliati nel fabbisogno;
- stipulare il contratto di utenza con il Concessionario Polo Strategico Nazionale;

VISTO il Piano dei Fabbisogni inviato a mezzo PEC alla società Polo Strategico Nazionale spa in data 9.11.2023, prot. 496249/2023;

DATO ATTO che nell'ambito del Piano dei Fabbisogni il periodo di adesione al Polo Strategico Nazionale è stato inizialmente circoscritto ad un triennio ed entro il termine del suddetto triennio l'Ente si riserva di valutare la possibilità di mantenere l'adesione al Polo Strategico Nazionale o di recedere, qualora le mutate esigenze tecnico-operative lo richiedessero;

VISTO il Progetto del Piano dei Fabbisogni identificato dal codice 2023-0000002205340793-PPdF-P2R2, ricevuto tramite PEC dalla società Polo Strategico Nazionale S.p.A. in data 5.1.2024 ed assunto in atti al prot. 9422 del 8.1.2024, che si allega come parte integrante al presente atto;

ANALIZZATO il Progetto del Piano dei Fabbisogni e il prospetto economico ivi contenuto, che per brevità si riassume di seguito:

Descrizione servizio	UT IVA esclusa	Canone annuale IVA esclusa
Industry Standard Hybrid Cloud on PSN Site SecurePublicCloud Public Cloud PSN Managed Servizi di Migrazione Servizi Professionali	€ 7.255.419,76	€ 75.770,97
TOTALE	**€ 7.255.419,76**	**€ 75.770,97**

per un totale di € **7.482.732,67**(IVA esclusa), di cui € 7. 255.419,76 *una tantum* per i servizi professionali di migrazione/setup/gestione e € 227.312,91 di canone annuale calcolato su 3 anni;

RITENUTO

- di nominare RUP il dipendente Luca Gennaro Fregola, in servizio presso il Dipartimento Turismo, Marketing territoriale e Mobilità, in possesso della competenza richiesta, alla quale è stato conferito incarico con nota del Dirigente Generale prot. n. 575152 del 21.12.2023;
- di disporre la nomina del DEC nella persona dell'Ing. Olga Saraco, in servizio presso il Dipartimento Transizione Digitale ed Attività Strategiche, in possesso della competenza richiesta;

- di disporre che il RUP e il DEC, stante il particolare contenuto tecnico del servizio, possano avvalersi, per l'espletamento delle attività relative all'affidamento di che trattasi, del personale con funzioni di supporto tecnico/amministrativo;
- di disporre la nomina di supporto al RUP nella persona della dott.ssa Ilaria Minieri con funzioni di supporto per come previsto dalla legislazione vigente;
- di disporre la nomina di supporto al DEC nella persona della dott.ssa Rosamaria Santacaterina con funzioni di supporto per come previsto dalla legislazione vigente;
- di disporre la costituzione del gruppo di lavoro che parteciperà direttamente, mediante contributo intellettuale e materiale, alla stesura degli atti;
- di individuare quali componenti del Gruppo incaricato l'arch. Carmela Romeo, la dott.ssa Rosa Conforti, la dott.ssa Maria Bellissimo, il dott. Antonio d'Orrico, i sig.ri Maria Magro, Domenico Cosco e Mario Donato;
- di riconoscere al RUP, al DEC e al personale con funzioni di supporto tecnico/amministrativo un incentivo con le modalità approvate con il regolamento regionale 7/2019 per la disciplina degli incentivi per funzioni tecniche art. 113 del d.lgs 50/2016 s.m.i., pubblicato sul Burc 34/2019, nei limiti del fondo appositamente previsto nel quadro economico dell'intervento corrispondenti ad € 142.171,92 pari al 1,9% dell'importo della Fornitura e che trova copertura sul medesimo capitolo di spesa previsti per i singoli servizi e forniture;
- che della suddetta somma, l'80% (pari ad € € 113.737,54) sia utilizzato per le spese di corresponsione degli incentivi e il restante 20% (pari ad € € 28.434,38), trattandosi di fondi a destinazione vincolata, costituisca una economia e confluisca nel quadro economico;
- coerentemente a quanto stabilito dal resoconto della Commissione Arconet del 20 marzo 2019, con riferimento agli oneri derivanti dagli incentivi per funzioni tecniche di cui art. 113 del D.Lgs. 50/2016, gli stessi dovranno essere impegnati, nei limiti del fondo appositamente previsto nel quadro economico dell'intervento, sul medesimo capitolo di spesa previsto per i singoli servizi e forniture;

CONSIDERATO che l'adesione al Polo Strategico Nazionale ha durata contrattuale massima prevista di 10 anni e che la durata effettiva sarà modulata all'interno del contratto di utenza che si stipulerà successivamente, si ritiene di avvalersi di quanto enunciato all'art. 21 comma 5 del contratto di utenza, stabilendo una durata iniziale di 36 mesi dalla data di avvio della gestione del servizio, decorsa la quale potrà essere esercitato il diritto di recesso dal contratto;

DATO ATTO, sulla scorta delle disposizioni normative e dei provvedimenti testé citati, che il procedimento rientra tra le competenze del Settore 3 "Integrazioni e sviluppo sistemi informativi regionali" del Dipartimento "Transizione Digitale Ed Attività Strategiche" e del Settore 2 "Osservatorio sul turismo e della mobilità" del Dipartimento "Turismo, Marketing territoriale e Mobilità", attesa l'elevata specificità del Progetto e della relativa base di dati;

RITENUTO
- di procedere alla approvazione del Progetto del Piano dei Fabbisogni relativo all'intervento "Sistemi Informativi Turismo In Cloud" e ad assicurare la copertura economica per tutto il periodo contrattuale previsto per un totale di € 9.272.000,00 (IVA inclusa) come da piano economico di seguito riportato:

	Descrizione	Importo
A	PROGETTO ESECUTIVO	€ 7.482.732,67
B	SOMME A DISPOSIZIONE	€ 1.789.267,33
B1	IVA SERVIZIO 22%	€ 1.646.201,19
B2	CONTRIBUTO ANAC	€ 880,00
B3	ART. 113 D.LGS 50/2016	€ 142.171,92
B4	IMPREVISTI ED ARROTONDAMENTI	€ 14,22
	TOTALE (A+B)	**€ 9.272.000,00**

- che ricorrono le condizioni per poter procedere agli impegni delle spese, ai sensi di quanto stabilito dall'art. 56 del D. Lgs. 118 del 23.6.2011, recante 'Disposizioni in materia di armonizzazione dei sistemi contabili e degli schemi di bilancio delle regioni e degli enti locali', sul capitolo di spesa U9011204604 del bilancio regionale che ne presenta la necessaria disponibilità, per le annualità di bilancio 2024, 2025 e 2026;
- di dover procedere all' accertamento delle somme a carico dei fondi UE sul capitolo di entrata E9201051201 e a carico dello Stato sul capitolo di entrata E2010122401, per le annualità di bilancio 2024, 2025 e 2026, come da prospetto di sotto riportato:

Risorse da accertare per l'annualità 2024						
Risorse da accertare €	Capitolo di entrata	Quota UE 70% €	Accertamento quota UE	Capitolo di entrata	Quota STATO 30% €	Accertamento quota STATO
3.000.000,00	**E9201051201**	**2.100.000,00**	**307/2024**	**E2010122401**	**900.000,00**	**308/2024**

Risorse da accertare per l'annualità 2025						
Risorse da accertare €	Capitolo di entrata	Quota UE 70% €	Accertamento quota UE	Capitolo di entrata	Quota STATO 30% €	Accertamento quota STATO
3.000.000,00	**E9201051201**	**2.100.000,00**	**156/2025**	**E2010122401**	**900.000,00**	**157/2025**

Risorse da accertare per l'annualità 2026						
Risorse da accertare €	Capitolo di entrata	Quota UE 70% €	Accertamento quota UE	Capitolo di entrata	Quota STATO 30% €	Accertamento quota STATO
3.272.000,00	**E9201051201**	**2.290.400,00**	**69/2026**	**E2010122401**	**981.600,00**	**70/2026**

- di dover procedere all'assunzione degli impegni sul capitolo di spesa U9011204604 a carico dei fondi UE, e a carico dello Stato, per le annualità di bilancio 2024 e 2025, come da prospetto di sotto riportato:

Risorse da impegnare per l'annualità 2024						
Risorse da impegnare €	Capitolo di spesa	Quota UE 70% €	Impegno quota UE	Capitolo di spesa	Quota STATO 30% €	Impegno quota STATO
3.000.000,00	**U9011204604**	**2.100.000,00**	**410/2024**	**U9011204604**	**900.000,00**	**411/2024**

Risorse da impegnare per l'annualità 2025						
Risorse da impegnare €	Capitolo di spesa	Quota UE 70% €	Impegno quota UE	Capitolo di spesa	Quota STATO 30% €	Impegno quota STATO
3.000.000,00	**U9011204604**	**2.100.000,00**	**134/2025**	**U9011204604**	**900.000,00**	**135/2025**

Risorse da impegnare per l'annualità 2026						
Risorse da impegnare €	Capitolo di spesa	Quota UE 70% €	Impegno quota UE	Capitolo di spesa	Quota STATO 30% €	Impegno quota STATO
3.272.000,00	**U9011204604**	**2.290.400,00**	**32/2026**	**U9011204604**	**981.600,00**	**33/2026**

PRESO ATTO
- del parere favorevole alla realizzazione dell'Intervento, prot. 511571 del 17.11.2023;

- del parere di coerenza programmatica con i contenuti dell'Accordo di Partenariato Italia 2021/2027 e del Programma Regionale Calabria FESR FSE+ 2021/2027, prot. 543699 del 6.12.2023;

ATTESTATA, da parte del dirigente che sottoscrive il presente atto, la perfetta rispondenza alle indicazioni contenute nel richiamato principio della competenza finanziaria potenziato, delle obbligazioni giuridiche assunte con il presente atto, la cui esigibilità è accertata nell'esercizio finanziario 2024-2025-2026 e il parere favorevole sotto il profilo della regolarità amministrativa del presente atto;

VISTI:
- le checklist di impegno generate telematicamente sul Sistema SIURP nn. 394827 e 394828 con esito positivo agli atti dell'ufficio;
- la proposta di accertamento 307/2024 a valere sul capitolo di entrata E9201051201 e proposta di impegno rispettivamente relazionata, 410/2024 a valere sul capitolo di spesa U9011204604, con riferimento agli importi accertati e impegnati pari ad € 2.100.000,00 a carico dei fondi UE per l'annualità 2024,
- la proposta di accertamento 308/2024 a valere sul capitolo di entrata E2010122401 e proposta di impegno rispettivamente relazionata, 411/2024 a valere sul capitolo di spesa U9011204604, con riferimento agli importi accertati e impegnati pari ad € 900.000,00 a carico della quota STATO per l'annualità 2024;
- la proposta di accertamento 156/2025 a valere sul capitolo di entrata E9201051201 e proposta di impegno rispettivamente relazionata, 134/2025 a valere sul capitolo di spesa U9011204604, con riferimento agli importi accertati e impegnati pari ad € 2.100.000,00 a carico dei fondi UE per l'annualità 2025,
- la proposta di accertamento 157/2025 a valere sul capitolo di entrata E2010122401 e proposta di impegno rispettivamente relazionata, 135/2025 a valere sul capitolo di spesa U9011204604, con riferimento agli importi accertati e impegnati pari ad € 900.000,00 a carico della quota STATO per l'annualità 2025;
- la proposta di accertamento 69/2026 a valere sul capitolo di entrata E9201051201 e proposta di impegno rispettivamente relazionata, 32/2026 a valere sul capitolo di spesa U9011204604, con riferimento agli importi accertati e impegnati pari ad € 2.290.400,00 a carico dei fondi UE per l'annualità 2026,
- la proposta di accertamento n. 70/2026 a valere sul capitolo di entrata E2010122401 e proposta di impegno rispettivamente relazionata, 33/2026 a valere sul capitolo di spesa U9011204604, con riferimento agli importi accertati e impegnati pari ad € 981.600,00 a carico della quota STATO per l'annualità 2026;

RITENUTO di avocare a sé il procedimento come da Decreto 9347/2023;

SU PROPOSTA del RUP che attesta sulla scorta dell'istruttoria effettuata, la regolarità amministrativa nonché la legittimità e la correttezza del presente atto;

DECRETA

DI ADERIRE alla Convenzione tra Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale e la Società Polo Strategico Nazionale spa del 24.8.2022 per la realizzazione dell'intervento "SISTEMI INFORMATIVI TURISMO IN CLOUD";

DI APPROVARE il Progetto del Piano dei Fabbisogni identificato dal codice 2023-0000002205340793-PPdF-P2R2, che si allega come parte integrante al presente atto, ricevuto tramite PEC in data 05.01.2024 ed assunto in atti al prot 9422 del 08.01.2024 dalla Società Polo Strategico Nazionale spa (PSN spa) con sede legale in via Goito 4 - C.F. e Partita IVA 16825251008 - CUP master : J51B21005710007 CIG primario: 9066973ECE CIG derivato: A011F288D6, per la 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. 179/2012 per la durata iniziale di 36 mesi dalla data di avvio della gestione del servizio, decorsa la quale potrà essere esercitato il diritto di recesso dal contratto come enunciato all'art. 21 comma 5 del contratto di utenza che si stipulerà successivamente;

DI APPROVARE il quadro economico del progetto pari ad € 9.272.000,00 00 di seguito riportato:

	Descrizione	Importo
A	PROGETTO ESECUTIVO	€ 7.482.732,67
B	SOMME A DISPOSIZIONE	€ 1.789.267,33
B1	IVA SERVIZIO 22%	€ 1.646.201,19
B2	CONTRIBUTO ANAC	€ 880,00
B3	ART. 113 D.LGS 50/2016	€ 142.171,92
B4	IMPREVISTI ED ARROTONDAMENTI	€ 14,22
	TOTALE (A+B)	**€ 9.272.000,00**

DI CONFERMARE, in qualità di RUP, il dipendente Luca Gennaro Fregola, in servizio presso il Dipartimento Turismo, Marketing territoriale e Mobilità, in possesso della competenza richiesta;

DI NOMINARE, in qualità di DEC, l'Ing. Olga Saraco, in servizio presso il Dipartimento Transizione Digitale ed Attività Strategiche, in possesso della competenza richiesta;

DI DISPORRE che il RUP e il DEC, stante il particolare contenuto tecnico del servizio, potranno avvalersi, per l'espletamento delle attività inerenti all'affidamento di che trattasi, del personale con funzioni di supporto tecnico/amministrativo;

DI NOMINARE, in qualità di supporto al RUP, la dott.ssa Ilaria Minieri, in servizio presso il Dipartimento Turismo, Marketing territoriale e Mobilità, in possesso della competenza richiesta;

DI NOMINARE, in qualità di supporto al DEC, la dott.ssa Rosamaria Santacaterina, in servizio presso il Dipartimento Transizione Digitale ed Attività Strategiche, in possesso della competenza richiesta;

DI DISPORRE la costituzione del gruppo di lavoro che parteciperà direttamente, mediante contributo intellettuale e materiale, alla stesura degli atti;

DI NOMINARE quali componenti del Gruppo incaricato l'arch. Carmela Romeo, la dott.ssa Rosa Conforti, la dott.ssa Maria Bellissimo, il dott. Antonio d'Orrico, i sig.ri Maria Magro, Domenico Cosco e Mario Donato;

DI RICONOSCERE al RUP, al DEC e al personale con funzioni di supporto tecnico/amministrativo un incentivo con le modalità approvate con il regolamento regionale n.7/2019 per la disciplina degli incentivi per funzioni tecniche art. 113 del d.lgs 50/2016 s.m.i., pubblicato sul Burc n. 34 del 13 Marzo 2019, nei limiti del fondo appositamente previsto nel quadro economico dell'intervento corrispondenti ad € 142.171,92 pari al 1,9% dell'importo della Fornitura e che trova copertura sul medesimo capitolo di spesa previsti per i singoli servizi e forniture;

DI DARE ATTO che l'importo dei servizi in oggetto è pari ad € 9.272.000,00 (iva inclusa) così ripartito:
- € 6.490.400,00 (70% Quota UE);
- € 2.781.600,00 (30% Quota Stato);

DI ACCERTARE, per le annualità 2024, 2025 e 2026, l'entrata di € 9.272.000,00 00 ai sensi dell'art.53 del D.Lgs.118/2011 e s.m.i., allegato 4/2 principio 3.2 a valere sui capitoli di entrata:
- E9201051201 per € 6.490.400,00 con debitore la Comunità Europea;
- E2010122401 per € 2.781.600,00 con debitore il Ministero dell'Economia e Finanze;

come da schema sotto allegato:

Risorse da accertare per l'annualità 2024						
Risorse da accertare €	Capitolo di entrata	Quota UE 70% €	Accertamento quota UE	Capitolo di entrata	Quota STATO 30% €	Accertamento quota STATO
3.000.000,00	**E9201051201**	**2.100.000,00**	**307/2024**	**E2010122401**	**900.000,00**	**308/2024**

Risorse da accertare per l'annualità 2025						
Risorse da accertare €	Capitolo di entrata	Quota UE 70% €	Accertamento quota UE	Capitolo di entrata	Quota STATO 30% €	Accertamento quota STATO
3.000.000,00	**E9201051201**	**2.100.000,00**	**156/2025**	**E2010122401**	**900.000,00**	**157/2025**

Risorse da accertare per l'annualità 2026						
Risorse da accertare €	Capitolo di entrata	Quota UE 70% €	Accertamento quota UE	Capitolo di entrata	Quota STATO 30% €	Accertamento quota STATO
3.272.000,00	**E9201051201**	**2.290.400,00**	**69/2026**	**E2010122401**	**981.600,00**	**70/2026**

DI IMPEGNARE per il 2024 - 2025 sul capitolo n. U9011204604 la somma pari a € 9.272.000,00 (IVA inclusa), che presenta adeguata disponibilità, come da schema sotto allegato:

Risorse da impegnare per l'annualità 2024						
Risorse da impegnare €	Capitolo di spesa	Quota UE 70% €	Impegno quota UE	Capitolo di spesa	Quota STATO 30% €	Impegno quota STATO
3.000.000,00	**U9011204604**	**2.100.000,00**	**410/2024**	**U9011204604**	**900.000,00**	**411/2024**

Risorse da impegnare per l'annualità 2025						
Risorse da impegnare €	Capitolo di spesa	Quota UE 70% €	Impegno quota UE	Capitolo di spesa	Quota STATO 30% €	Impegno quota STATO
3.000.000,00	**U9011204604**	**2.100.000,00**	**134/2025**	**U9011204604**	**900.000,00**	**135/2025**

Risorse da impegnare per l'annualità 2026						
Risorse da impegnare €	Capitolo di spesa	Quota UE 70% €	Impegno quota UE	Capitolo di spesa	Quota STATO 30% €	Impegno quota STATO
3.272.000,00	**U9011204604**	**2.290.400,00**	**32/2026**	**U9011204604**	**981.600,00**	**33/2026**

DI DARE ATTO che si provvederà alla stipula del contratto di utenza con il Concessionario Polo Strategico Nazionale costituito da TIM S.p.A., Leonardo S.p.A, SOGEI – Società Generale di Informatica – S.p.A. e CDP Equity S.p.A.;

DI DEMANDARE al Settore 2 "Osservatorio sul turismo e della mobilità" del Dipartimento "Turismo, Marketing territoriale e Mobilità" e al RUP ogni adempimento successivo alla attuazione del presente provvedimento;

DI NOTIFICARE il presente provvedimento ai soggetti interessati;

DI PROVVEDERE agli obblighi di pubblicazione previsti dall'art.23 del D.lgs. 33/2013 e alle ulteriori pubblicazioni previste dal Piano Triennale di prevenzione della corruzione ai sensi dell'art. 7bis comma 3 del D.lgs. 33/2013 e nel rispetto del Regolamento UE 2016/679;

DI PROVVEDERE alla pubblicazione integrale del provvedimento sul BURC ai sensi della legge regionale 6 aprile 2011, n. 11 e nel rispetto del Regolamento UE 2016/679;

DI PRECISARE che avverso il presente provvedimento è ammesso ricorso nelle forme e nei termini previsti dalla legge.

Sottoscritta dal RUP
Luca Gennaro Fregola
(con firma digitale)

Sottoscritta dal Dirigente Generale
Tommaso Calabrò
(con firma digitale)

Sottoscritta dal Dirigente Generale
Maria Antonella Cauteruccio
(con firma digitale)

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

Dipartimento Turismo, Marketing territoriale e Mobilità

PSN-SDE-CONV22-001-2023-0000002205340793-PdF-P2R2

SOMMARIO

Indice delle tabelle

STATO DEL DOCUMENTO

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

TITOLO DEL DOCUMENTO		
Descrizione Modifica	**Revisione**	**Data**
Aggiornato il Cap 8 "Configuratore" in ottemperanza alla modifica richiesta dall'Amministrazione a mezzo PEC	2	04/01/2024

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
  - Maria Antonella Cauteruccio
  - Email: m.cauteruccio@regione.calabria.it

- Referente Tecnico
  - Ilaria Minieri
  - Email: ilaria.minieri@regione.calabria.it

1 PREMESSA

Il presente documento descrive il Progetto dei Fabbisogni del **PSN** relativamente alla richiesta di fornitura dei servizi cloud nell'ambito della concessione per la realizzazione e gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione denominata Polo Strategico Nazionale ("PSN"), di cui al comma 1 dell'articolo 33-septies del d.l. n. 179 del 2012.
Quanto descritto, è stato redatto in conformità alle richieste del **Dipartimento Turismo, Marketing territoriale e Mobilità (Regione Calabria)** 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 (**2023-0000002205340793-PdF-P2R1**).

L'Amministrazione al fine di ottemperare alla realizzazione di rinnovati strumenti a supporto delle campagne a favore del turismo e della mobilità sul territorio, ha necessità di approvvigionarsi di un ambiente cloud ad hoc, adeguato ad ospitare le infrastrutture necessarie per l'erogazione dei suddetti servizi e in grado di supportare possibili evoluzioni future.

Inoltre, l'Amministrazione beneficerà di un mix di figure professionali esperte che assicurino l'operatività e la disponibilità in completa sicurezza degli ambienti ospitati presso le soluzioni offerte dal PSN.

In tale ottica, il PSN offre un'infrastruttura cloud che soddisfa i requisiti di alta affidabilità, resilienza e indipendenza tecnologica, adeguati alle esigenze di mantenimento, disponibilità, sicurezza e gestione dati della piattaforma.

I servizi individuati dall'Amministrazione che necessitano di una rinnovata soluzione tecnologica ed infrastrutturale sono quelli di supporto al sito del turismo (calabriastraordinaria.it) e quelli del portale di infomobilità. Essi vengono riassunti nella tabella successiva e descritti nei prossimi paragrafi.

Servizio dell'amministrazione	Classificazione	Tipo di Migrazione
Sito turismo	Ordinario	Modalità B - aggiornamento in sicurezza di applicazioni in cloud
Infomobilità	Ordinario	Modalità B - aggiornamento in sicurezza di applicazioni in cloud
Sito Infomobilità	Ordinario	Modalità B - aggiornamento in sicurezza di applicazioni in cloud
Sistema informativo a supporto dell'osservatorio regionale del turismo	Ordinario	Modalità B - aggiornamento in sicurezza di applicazioni in cloud
Sistema informativo a supporto dell'osservatorio regionale della mobilità sostenibile	Ordinario	Modalità B - aggiornamento in sicurezza di applicazioni in cloud
Sistema gestionale dell'Osservatorio mobilità	Ordinario	Modalità B - aggiornamento in sicurezza di applicazioni in cloud

2 AMBITO

L'adesione del Progetto Turismo Calabria al PSN prevede la progettazione dell'architettura applicativa finalizzata ad una soluzione che aderisca al paradigma cloud, in gradi quindi di usufruire dei benefici dell'infrastruttura che il PSN intende proporre.

Le soluzioni adottate sono finalizzate a consolidare le funzionalità previste nella progettualità sviluppata per i servizi che dovranno essere erogati su soluzioni PSN, attraverso interventi mirati che sfruttino i tool disponibili nella soluzione del cloud provider e garantiscano la continuità operativa dei portali sull'infrastruttura target. Rientrano nelle attività gli adeguamenti normativi e/o organizzativi richiesti dall'Amministrazione che possono avere un impatto significativo anche sulle funzionalità dell'utente.

I servizi destinati ad essere erogati su soluzioni infrastrutturali PSN sono:

- Sistema informativo a supporto dell'osservatorio regionale del turismo
- Sistema informativo a supporto dell'osservatorio regionale della mobilità sostenibile
- Sistema gestionale dell'Osservatorio mobilità
- Piattaforma di promozione turistica della Regione Calabria - Calabria Straordinaria

Le attività previste nell'ambito del sistema informativo in oggetto riguardano:

- l'evoluzione di funzionalità già esistenti che possano arricchire l'esperienza attraverso l'erogazione sul cloud PSN efficentandone la fruizione;
- re-architect delle funzionalità di raccolta, gestione e trattamento dei dati sulla domanda/offerta turistica al fine di garantire l'interazione con gli applicativi dell'Amministrazione non compresi nel presente perimetro di adesione;
- re-architect delle funzionalità di gestione dei dati al fine di garantire l'interazione con gli applicativi esterni al perimetro dell'Amministrazione;
- adozione dei servizi cloud-native per le componenti sostituibili;
- innalzamento del livello di interoperabilità secondo le linee guida "Modello di Interoperabilità" di AgID, tra cui in particolare: (i) l'introduzione di logiche a servizi/micro-servizi in applicazioni monolitiche e (ii) l'evoluzione funzionale per integrazioni con API;
- supporto specialistico di ottimizzazione dei servizi e introduzione/aggiornamento di strumenti disponibili nella proposta PSN a supporto delle attività ICT per incrementare affidabilità, co-working, agilità, valutare il grado di digitalizzazione, di interoperabilità, di sicurezza applicativa, di aderenza a standard e linee guida, proporre piani di azione trasversale ai progetti ed ai servizi su obiettivi di innovazione e standardizzazione.

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 5: Documenti Contrattuali

3.2 DOCUMENTI DI RIFERIMENTO

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

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

Tabella 6: Documenti di riferimento

3.3 DOCUMENTI APPLICABILI

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

Tabella 7: Documenti Applicabili

4 ACRONIMI

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

Acronimo	Descrizione
AI	Artificial Intelligence
CaaS	Container as a Service
CMP	Cloud Management Platform
CRC	Cyclic Redundancy Check
CSP	Cloud Service Provider
DB	DataBase
DBaaS	DataBase as a Service
DR	Disaster Recovery
ETL	Extract Transform and Load
GCP	Google Cloud Platform
HA	High Availability
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IT	Information Technology
ITSM	Information Technology Service Management
PA	Pubblica Amministrazione
PaaS	Platform as a Service
PSN	Polo Strategico Nazionale
SCORM	Shareable Content Object Reference Model
VM	Virtual Machine
WBT	Web Based Training
WORM	Write Once, Read Many

Tabella 8: Acronimi

5 PROGETTO DI ATTUAZIONE DEL SERVIZIO

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

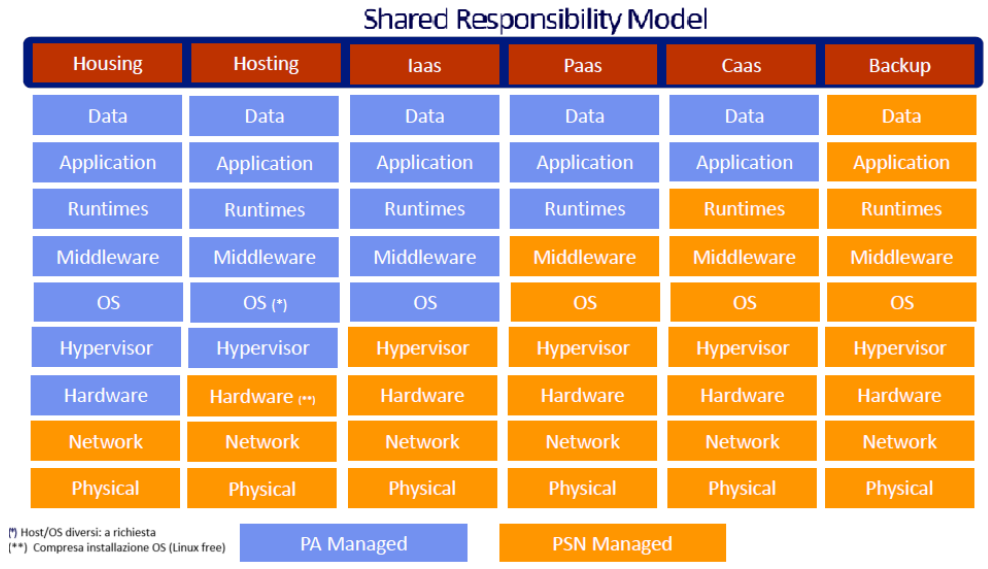
5.1 SERVIZI PROPOSTI

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

Servizio	Tipologia
Secure Public Cloud	Azure
Servizi Professionali	Re-Architect
Servizi Professionali	Security Professional Services
Servizi Professionali	IT Infrastructure Service Operation

Tabella 9: Servizi Proposti

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



5.2 SECURE PUBLIC CLOUD

5.2.1 Descrizione del servizio

Il Secure Public Cloud è un servizio PSN Core che si basa su Region pubbliche degli Hyperscaler (Microsoft Azure e Google Cloud GCP) a cui vengono aggiunti tutti gli elementi di sicurezza (Chiavi esterne, backup, template, servizi professionali).
L'architettura del servizio "Secure Public Cloud" è basata su due componenti principali:

- **Public Cloud**: La componente Hyperscale Public Cloud, erogata da una Region collocata sul territorio nazionale, ai cui servizi vengono applicate configurazioni, policy e controlli di sicurezza, al fine di garantire ai clienti ambienti di elaborazione segregati aventi una sicurezza di base adeguata agli scopi del PSN;
- **Security & Governance**: Una componente, erogata dai Data Center del PSN distribuiti sul territorio Nazionale, nella quale verranno configurati servizi atti a garantire l'adeguato livello di sicurezza dei servizi erogati sul Public Cloud (Gestione Chiavi e Backup).

Tale scenario prevede la presenza dei seguenti attori:

- Fornitore dei servizi di Public Cloud (CSP):
  - fornisce la piattaforma su cui è costruita la componente Hyperscale Public Cloud dell'architettura
- PSN:
  - si occupa di progettare, erogare, gestire e controllare i servizi cloud ed in modo particolare la componente di sicurezza e governo di base adeguati agli scopi del PSN;
  - fornisce servizi di sicurezza opzionali a "valore aggiunto" integrati ai servizi base tramite servizi professionali per la securizzazione.

Il Secure Public Cloud è un servizio core del PSN che garantisce alti standard di sicurezza:
GESTIONE DELLE CHIAVI. Relativamente alla gestione delle chiavi la soluzione comprende:

- Impiego di terze parti (e.g., Thales CipherTrust) con grande livello di autonomia nella gestione delle chiavi crittografiche per soluzioni in cloud con il modello Bring Your Own Key (BYOK).
- Soluzione di key management replicata nei due datacenter HA e territorialmente nelle due Region.
- Controllo on-premise per ciascuna fase del ciclo vita delle chiavi, consentendo di eseguire in autonomia:
  - generazione delle chiavi ON-PREMISE tramite l'utilizzo di dispositivi crittografici certificati;
  - esecuzione dei backup delle chiavi;
  - installazione diretta delle chiavi sui Key Vault in cloud;
  - monitoraggio degli accessi alle chiavi;
  - rotazione manuale o periodica delle chiavi;
  - revoca delle chiavi.
- On-Prem HSM certificato FIPS 140-2 L3 con partizioni multiple per la corretta gestione del materiale crittografico (chiavi simmetriche ed asimmetriche, generazione entropia, ..).
- CipherTrust Manager per la gestione del ciclo di vita delle chiavi on-premise e in Cloud.
- CipherTrust Cloud Key Manager come orchestratore dei processi di gestione delle chiavi in Cloud. Generazione delle chiavi on-premise per importazione sicura sul cloud provider per tutto il ciclo di vita.

GOVERNANCE MODEL. Per ogni cliente viene creato un ambiente standard segregato e auto-consistente in cui, tramite servizi di delega dei privilegi (ad esempio Azure Lighthouse e Privileged Identity Management) è possibile proiettare i servizi di monitoraggio e sicurezza dello specifico ambiente cliente verso l'ambiente del gestore del PSN che quindi avrà:

- Visibilità di tutti gli ambienti
- Capacità di intervento automatizzato su larga scala
- Possibilità di enforcement delle policy definite

I Privilegi di amministrazione sono disabilitati per default e vengono attribuiti agli operatori a valle di un processo di autorizzazione: questo meccanismo garantisce il mutuo controllo da parte del cliente e del provider con intrinseco innalzamento del livello di sicurezza.
Le caratteristiche di questo modello di gestione forniscono:

- Gestione uniforme e standardizzata dei tenant cliente;
- Creazione, distribuzione e aggiornamento, tramite sistemi di automazione, di set di regole di sicurezza predefinite in linea con best practices internazionali;
- Creazione, distribuzione e aggiornamento, tramite sistemi di automazione, dei ruoli standard per ogni funzione (Ruoli PSN, Ruoli PA, Ruoli terze parti);
- Disponibilità di template securizzati ed integrati a strumenti di sicurezza;
- Gestione unificata dell'identità;
- Gestione degli eventi di sicurezza;

CONFIDENTIAL COMPUTING. L'obiettivo del PSN è rafforzare il livello di confidenzialità e sicurezza del dato in uso tramite i seguenti metodi:

- Ridurre al minimo le cosiddette Trusted Compute Bases (TCB) sui piani hardware, software e operations.
- Usare tecniche di enforcement basate su componenti tecnologiche piuttosto che su processi organizzativi.
- Fornire trasparenza sulle garanzie, i rischi residui e le mitigazioni che si possono implementare.
- I modelli di attacco contro le applicazioni cloud si basano su tecniche diverse per prendere di mira codice o dati in uso, ad esempio:
    - breakout di hypervisor e container;
    - compromissione del firmware ed altre minacce interne, ognuna delle quali si basa su tecniche diverse per prendere di mira codice o dati in uso.

Confidential Computing (per VM, K8S, HSM) è la protezione dei dati in uso utilizzando ambienti di esecuzione attendibili basati su hardware

SOLUZIONI HUB & SPOKE. Per quanto riguarda l'ambiente Secure Public Cloud è previsto l'uso di un modello Hub & Spoke per consentire al PSN il controllo del traffico e la gestione delle DMZ per l'ambiente cloud.
Le Amministrazioni potranno creare reti virtuali spoke nei segmenti, dove saranno attive Policy che forzeranno la connessione con Virtual Network Hub e impediranno la creazione di tipologie di risorse controllate centralmente, come, ad esempio, gli indirizzi IP pubblici.

BACK UP. Per esercitare la sovranità del dato, il Secure Public Cloud prevede l'esistenza e la fruibilità di una copia di tale dato in maniera indipendente dai servizi del CSP tramite ulteriore livello di archiviazione.
Tale servizio sarà fornito attraverso l'integrazione delle risorse in Public Cloud con il Backup del PSN in modo che lo Storage su cui risiede il dato protetto sia gestito dal personale PSN.
L'integrazione prevede l'uso di tecniche di backup snapshot o stream-based e la cifratura dei dati "at rest" e in transito per garantire la protezione e il ripristino delle macchine virtuali a cui è rivolto il servizio, anche di quelle che implementano meccanismi di encryption del disco di sistema e dei dischi dati.

5.2.2 Personalizzazione del servizio

La strutturazione del servizio prevede l'utilizzo delle seguenti classi di componenti del listino PSN:

Tipo	Tipologia	Elemento	Q.tà
Compute (Production) Riservate 3 anni	VM "convenzionali"	c4r8	8
Compute (Production) Riservate 3 anni	VM "convenzionali"	c4r16	7
Compute (Production) Riservate 3 anni	VM "convenzionali"	c8r16	3
STORAGE	Managed Disks	dischi SSD Standard (128 GB)	27

Questo dimensionamento del servizio ed i costi della configurazione proposta sono riportati nel paragrafo "8 Configuratore". Si specifica che l'avanzamento della fatturazione sarà in funzione dei consumi effettivi realizzati nel mese della soluzione Secure Public Cloud.

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

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

5.2.4 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.

5.3 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".

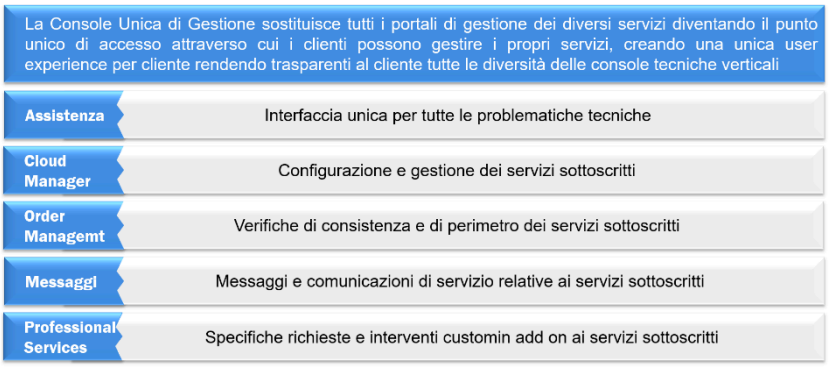


Figura 1 Funzionalità CU

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.).

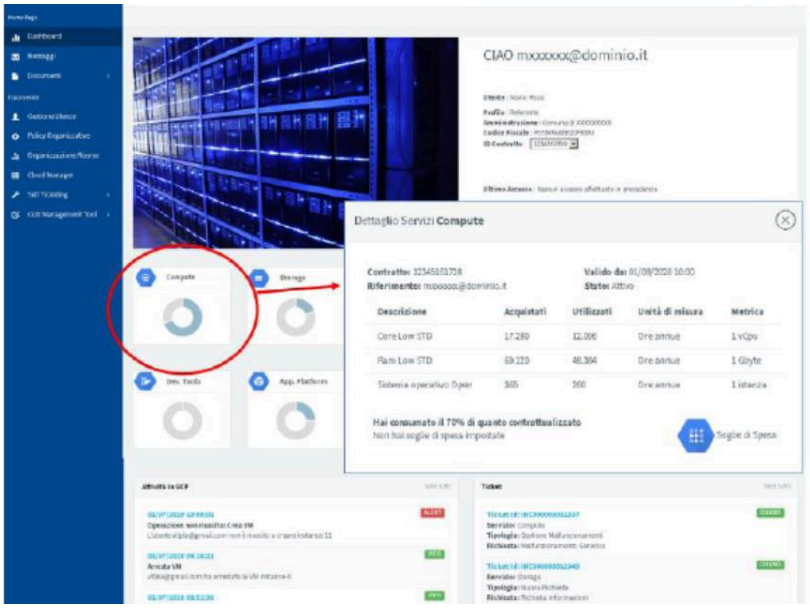


Figura 2 Dashboard CU

- 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 3: 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**

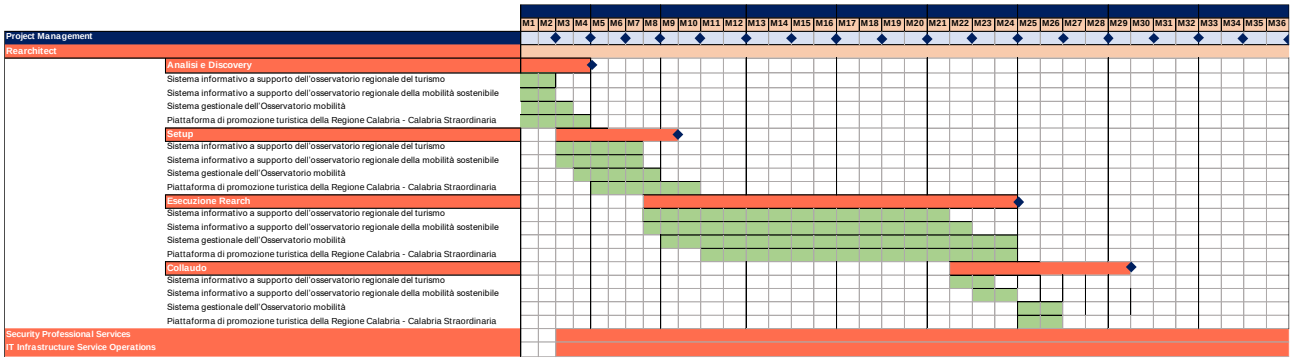
Definizione Strategia di Collaudo: tale fase è finalizzata alla predisposizione della strategia ottimale di collaudo delle applicazioni migrate nell'ambiente target.

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.



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 Re-architect

La strategia di Re-architect ha come obiettivo quello di adattare l'architettura core di un applicativo in ottica cloud, attraverso un processo di redesign iterativo ed incrementale che miri ad adottare i servizi cloud-native offerti dal PSN per massimizzare i benefici che ne derivano. L'obiettivo è garantire i benefici attesi dall'Amministrazione e il minimo impatto per gli utenti finali. Il servizio si rende necessario, ad esempio, quando il livello di sicurezza è molto distante dallo standard minimo e realizza la modifica di moduli applicativi di un'applicazione al fine di garantirne un adeguato livello di sicurezza
Il servizio sarà disegnato rispettando i principi di design cloud-native che non solo consente di favorire la flessibilità operativa dei servizi applicativi, ma consente anche:

- un maggior riuso e velocità di implementazione
- l'utilizzo di metodologie consolidate di test (quanto più automatici) sia per le verifiche funzionali, sia per quelle di qualità e sicurezza
- l'uso di best practices di sviluppo e di progettazione (definite dal PSN) che consenta la trasformazione del codice applicativo in modo controllato
- una progettazione secondo le metodologie Secure by design

Discorso analogo vale per il monitoraggio delle applicazioni a valle di un progetto di "re-architect". L'adozione matura di metodologie cloud-native permette all'applicazione di usufruire di piattaforme comuni di monitoraggio e manutenzione proattiva.
Di seguito vengono illustrati i diversi step del processo di Re-architect.

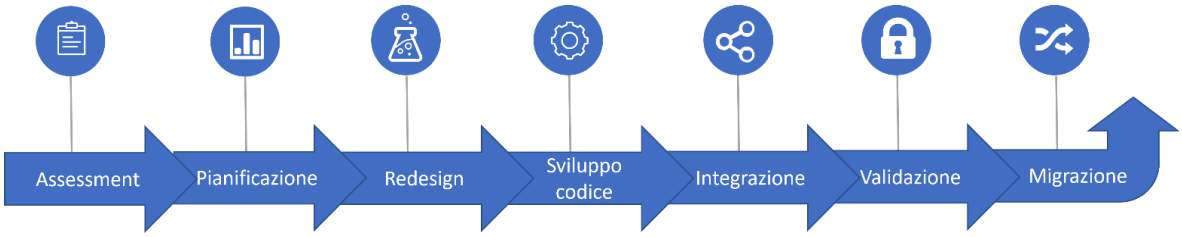


Figura 4: Flusso processo di Re-architect

5.5.1.1 Personalizzazione del servizio

L'obiettivo del task di riorganizzazione dell'infrastruttura applicativa consiste principalmente nella rielaborazione del codice dei moduli funzionali, senza comprometterne l'operatività, per renderli compliance all'erogazione tramite piattaforma Cloud del PSN. La modifica avviene nel rispetto degli standard di settore, traguardando gli obiettivi di stabilità e resilienza della piattaforma nella nuova accezione, integrando la soluzione nell'infrastruttura cloud target.

I servizi previsti per questa fase sono elencati di seguito:

- analisi iniziale dei requisiti funzionali della piattaforma;
- definizione degli intervetni di re-architect;
- progettazione della soluzione e del piano di intervento;
- testing, collaudo e rilascio in produzione.

Il Re-architect sarà l'occasione per valutare nuove funzioni sia lato front-end (portale e applicazione *mobile*) che back-end per arricchire l'offerta ed erogare servizi innovativi agli utenti.

5.5.2 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,

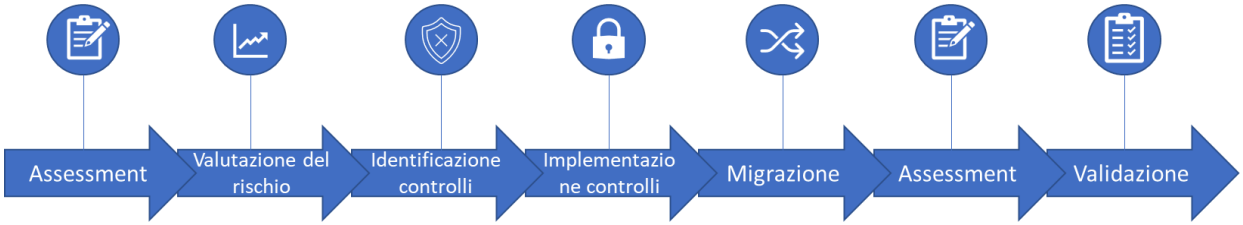
all'interno delle diverse tipologie di cloud scelte, per gestire la sicurezza dei dati, ma questi devono essere in ogni caso previsti ed implementati dalle Amministrazioni. La responsabilità della sicurezza di tutti i dati trasferiti su cloud rimane sempre e comunque del cliente finale. Il fatto che 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



5.5.2.1 Personalizzazione del servizio

In linea con i principali standard normativi di riferimento nonché delle più efficaci capacità difensive attivabili nel breve/medio periodo da parte dell'Amministrazione, vengono previsti una serie di servizi orientati a migliorare la resilienza operativa, mantenere una visione in tempo reale del panorama delle minacce esistenti, predisporre reattivamente le opportune risposte a specifiche tipologie di minacce o agli incidenti di sicurezza informatica impattanti l'operatività dell'Amministrazione.
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 implementazione:

- Supporto Device Management e protezione perimetrale (NGFW, WAF);
- Security Event Monitoring, Notification & Log Management;

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

- Servizi “a task”: servizi professionali per il miglioramento della sicurezza delle infrastrutture e delle applicazioni della PA;
- Servizi” Ricorrenti”: servizi di supporto device management protezione perimetrale.

In particolare, per quanto riguarda i servizi a task, saranno identificate e pianificate insieme

In particolare, per quanto riguarda i servizi a task, saranno identificate e pianificate insieme all’Amministrazione le attività di lavorazione. Per ciascun task 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.

Nei paragrafi seguenti vengono descritti i servizi professionali di sicurezza erogati per il Dipartimento.

5.5.2.2 Maturity Level Assessment e Gap Analysis

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

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

- *GA Results Executive Summary*: Il report contiene una overview di tipo executive ad alto livello relativo al processo di valutazione che considera 4 aree ‘chiave’: *Business, Functional, Technical, Implementation*

GA Results Assessment Report: Il report contiene i dettagli del processo di valutazione finalizzato ad indirizzare il corretto approccio alla migrazione relativamente alle 4 aree ‘chiave’ indicate: *Business, Functional, Technical, Implementation.*

5.5.2.3 Supporto Device Management protezione perimetrale (NGFW, WAF)

Il servizio professionale richiesto è orientato a supportare l’Amministrazione nella gestione e nel monitoraggio continuativo delle piattaforme di protezione perimetrale sfruttando appieno le capacità intrinseche di Azure Firewall, al fine di garantire una maggiore protezione rispetto ai tradizionali firewall di rete per le applicazioni e facilitarne il governo, con elevati standard di qualità e sicurezza dei consueti processi di configuration/change management, problem/incident management, nonché mantenere sempre aggiornati e sicuri software e firmware dei dispositivi di sicurezza in esercizio in conformità a quanto previsto sul FNSC.

Il servizio è erogato remotamente e prevede una finestra di servizio H24x7 oltre che il monitoraggio continuo dello stato dell'infrastruttura e sarà erogato in modalità ricorrente e comprenderà le seguenti attività:

- Presa in carico e gestione delle anomalie riscontrate o segnalate nell'erogazione dei servizi dal Supporto Applicativo dell'Amministrazione che ricadono nell'ambito della sicurezza perimetrale (problem/incident management);
- gestione ed implementazione delle policy di sicurezza sui Firewall e sui Web Application Firewall posti a protezione delle applicazioni Web, nonché la gestione del firmware ed il backup delle configurazioni (configuration/change management);
- supporto alle azioni di contenimento, remediation e response richieste in caso di incidente, nonché l'implementazione delle giuste contromisure rispetto a nuove minacce e vulnerabilità segnalate.

Le risorse necessarie per erogare le soluzioni virtuali di WAF e NGFW sono parte integrante della proposta sul Secure Public Cloud.

5.5.2.4 Security Event Monitoring, Notification & Log Management

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 e in modalità ricorrente, 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 H24x7 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.

Continous 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 e-mail 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 10: 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 11: 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.

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 di Security Event Monitoring & Notification & Log Management è dimensionato fino a 500 Events Per Second (EPS).

5.5.3 IT infrastructure service operations

In seguito all'avvenuta migrazione, il PSN, renderà disponibili servizi di IT infrastructure-service operations per garantire il mantenimento di funzionalità o ottimizzazione degli ambienti su cui insistono le applicazioni, 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.

5.5.3.1 Personalizzazione del servizio

L'offerta del PSN garantisce, a beneficio dell'Amministrazione, la **gestione operativa della piattaforma** di promozione turistica che, oltre a rivolgersi ai turisti, prevede il coinvolgimento di operatori della filiera attraverso un'area dedicata per segnalazioni e proposte di contenuti che saranno editati da una redazione ad hoc, ottimizzati in ottica SEO e tradotti in lingua inglese.

La gestione operativa della piattaforma include il supporto nella gestione degli strumenti:

- per l'identificazione del pubblico (target) di riferimento e classificazione dei destinatari della comunicazione, in relazione alle analisi elaborate dall'Osservatorio sul Turismo della regione;
- per la progettazione della narrazione mediante l'individuazione dei messaggi chiave in relazione alle diverse tipologie di target;
- per la ricerca di informazioni su trends, destinazioni, itinerari, eventi e consigli di viaggio;
- per l'individuazione di linee tematiche su cui incentrare la narrazione e la promozione dell'offerta turistica basata su concetti chiave strategici;
- redazione di un Piano Editoriale (PED) mensile condiviso, predisposto in base alle esigenze/priorità contenutistiche e di marketing dell'Amministrazione;
- valutazione dei linguaggi (Tone of Voice, ecc.);
- valutazione degli strumenti di comunicazione e innovazione digitale necessari all'espletamento dei macro-servizi (analisi e ottimizzazione in chiave SEO, analisi keywords, ecc.);
- traduzione di contenuti in lingua inglese;
- ricerca e creazione archivio immagini open source e di libero utilizzo;
- caricamento di tutte le tipologie di contenuto (testuale, iconografico e multimediali) sul portale;
- ricerca, pubblicazione e gestione eventi (sia da calendario istituzionale che da segnalazioni, previa approvazione da parte dei responsabili istituzionali della piattaforma);
- assistenza e supporto costante da remoto ai referenti di progetto;
- assistenza per la predisposizione di attività sinergiche, frutto di segnalazioni provenienti da operatori e stakeholder del territorio (contenuti da attenzionare con priorità, segnalazione eventi/itinerari/fiere/visite guidate, ecc.);
- supportare l'Amministrazione in attività di preparazione e redazione di modelli di reportistica finalizzati all'ottimizzazione delle metodologie operative ed al continuos improvment della gestione dei sistemi;
- supportare l'Amministrazione attraverso una gestione dei sistemi e dei dati elaborati al fine di efficientare le funzionalità delle infrastrutture ospitate sulla piattaforma Secure Public Cloud del PSN, per conseguire una maggiore efficacia nell'utilizzo dei servizi da parte dell'Amministrazione;
- reportistica periodica sull'andamento del servizio.

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
- **Devops Expert**: Ha consolidata esperienza nelle metodologie di sviluppo DevOps su progetti complessi, per applicare un approccio interfunzionale in grado di garantire la sinergia tra i team di sviluppo e di gestione dei sistemi; è responsabile di progettare le strategie DevOps, identificando gli strumenti di controllo dei sorgenti, di automazione e di rilascio in ottica Continuous Integration e Continuous Development.
- **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.
- **Developer (Cloud/Mobile/Front-End Developer)**: Ha competenze di linguaggi di programmazione e di piattaforme di sviluppo, utilizzando le conoscenze di metodologie di analisi e disegno OOA, SOA e

REST con UML; assicura la realizzazione e l'implementazione di applicazioni con architetture web-based e cloud-based.

- **UX Designer**: ha una conoscenza teorica e pratica dei principi di usabilità, paradigmi di interazione e principi di interaction design e di gestione delle problematiche di compatibilità cross-browser (desktop, tablet, mobile); è responsabile dell'applicazione dell'approccio centrato sull'utente (human centered) nello sviluppo dei servizi digitali, garantendo il raggiungimento efficace ed efficiente degli obiettivi dell'utente nell'interazione con l'Amministrazione.
- **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.
- **Forensic Expert**: E' chiamato a gestire la raccolta di evidenze e l'analisi delle stesse in concomitanza di un incidente relativo alla sicurezza delle informazioni documentando il tutto in modo che sia correttamente presentabile in sede processuale.

- **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	
Ragione Sociale	Regione Calabria - Dipartimento del Turismo
IDENTIFICATIVO DOCUMENTO	
Emesso da	CSO
Codice Documento	2023-0000002205340793-PdF-P2R2
Versione	1

VERSIONE CONFIGURATORE	3.7.1

RIEPILOGO PREZZI				
SERVIZIO	Totale UT		Totale Canone Annuale	
Industry Standard			€	-
Hybrid Cloud on PSN Site			€	-
SecurePublicCloud			€	75.770,97
Public Cloud PSN Managed			€	-
Servizi di Migrazione	€	-		
Servizi Professionali	€	7.255.419,76		
TOTALE	€	7.255.419,76	€	75.770,97

CODICE	SERVIZIO	TIPOLOGIA	ELEMENTO	QUANTITA'	DR	Totale UT	Totale Canone Annuale
SEC-MS-06	SecurePublicCloudAzure	ComputeProduction	VM "convenzionali"c4r8	8			€ 4.540,2392
SEC-MS-07	SecurePublicCloudAzure	ComputeProduction	VM "convenzionali"c4r16	7			€ 5.974,1773
SEC-MS-09	SecurePublicCloudAzure	ComputeProduction	VM "convenzionali" c8r16	3			€ 3.404,2539
SEC-MS-42	SecurePublicCloudAzure	Storage	Managed Disks - dischi SSD Standard (128 GB)	27			€ 2.738,7126
SEC-MS-47	SecurePublicCloudAzure	Network	Bandwidth Internet - TB annui	100			€ 7.700,4100
SEC-MS-48	SecurePublicCloudAzure	PublicCloudSecurityBackupDefenseinDepth	XDR per Servers - istanze	20			€ 3.083,0860
SEC-MS-49	SecurePublicCloudAzure	PublicCloudSecurityBackupDefenseinDepth	XDR per SQL - istanze	20			€ 3.168,2400
SEC-MS-50	SecurePublicCloudAzure	PublicCloudSecurityBackupDefenseinDepth	XDR per Storage - 1M Transazioni Standard per mese	20			€ 423,2660
SEC-MS-51	SecurePublicCloudAzure	PublicCloudSecurityBackupDefenseinDepth	XDR per Kubernetes - vCore	20			€ 415,0280
SEC-MS-52	SecurePublicCloudAzure	PublicCloudSecurityBackupDefenseinDepth	XDR per container registry - 100 immagini standard	20			€ 510,5080
SEC-MS-53	SecurePublicCloudAzure	PublicCloudSecurityBackupDefenseinDepth	XDR per Key Vault - 1M Transazioni Standard	20			€ 351,8880
SEC-MS-54	SecurePublicCloudAzure	PublicCloudSecurityBackupSIEM	SIEM service - GB per giorno	10			€ 8.237,4260
SEC-MS-55	SecurePublicCloudAzure	PublicCloudSecurityBackupSIEM	SIEM Data Ingestion - GB per giorno	10			€ 7.894,3040
SEC-MS-56	SecurePublicCloudAzure	PublicCloudSecurityBackupSIEM	SIEM Data retention (6 mesi) - GB per giorno	10			€ 1.252,2690
SEC-MS-57	SecurePublicCloudAzure	PublicCloudSecurityBackupMonitor	Monitor VM Data ingestion - GB per giorno	10			€ 7.894,3040
SEC-MS-58	SecurePublicCloudAzure	PublicCloudSecurityBackupMonitor	Monitor Data retention (1 mesi) - GB per giorno	10			€ -
SEC-MS-58	SecurePublicCloudAzure	PublicCloudSecurityBackupMonitor	Monitor Data retention (1 mesi) - GB per giorno	10			€ -
SEC-MS-59	SecurePublicCloudAzure	PublicCloudSecurityBackupFirewall	Deployment - Istanze	1			€ 13.490,9455
SEC-MS-60	SecurePublicCloudAzure	PublicCloudSecurityBackupFirewall	Data managed - TB mese	11			€ 1.903,6996
SEC-MS-61	SecurePublicCloudAzure	PublicCloudSecurityBackupCloudBackup	Istanze Protette - Numero VM	18			€ 1.911,4632
SEC-MS-62	SecurePublicCloudAzure	PublicCloudSecurityBackupCloudBackup	Storage occupato GB	3500			€ 876,7500

SP-07	ServiziProfessionali	Rearchitect	Project Manager	655		€ 243.529,0000	
SP-10	ServiziProfessionali	Rearchitect	DevOps Expert	780		€ 243.851,4000	
SP-09	ServiziProfessionali	Rearchitect	Business Analyst	410		€ 121.950,4000	
SP-06	ServiziProfessionali	Rearchitect	Enterprise Architect	293		€ 121.685,8300	
SP-01	ServiziProfessionali	Rearchitect	Cloud Application Architect	315		€ 122.015,2500	
SP-04	ServiziProfessionali	Rearchitect	Cloud Application Specialist	928		€ 292.644,8000	
SP-05	ServiziProfessionali	Rearchitect	Cloud Security Specialist	783		€ 195.209,7300	
SP-11	ServiziProfessionali	Rearchitect	Developer (Cloud/Mobile/Front-End Developer)	2618		€ 487.733,4000	
SP-02	ServiziProfessionali	Rearchitect	Database Specialist and Administrator	783		€ 195.209,7300	
SP-12	ServiziProfessionali	Rearchitect	System and Network Administrator	984		€ 292.680,9600	
SP-08	ServiziProfessionali	Rearchitect	UX Designer	410		€ 121.950,4000	
SP-23	ServiziProfessionali	ITInfrastructureServiceOperation	Systems Architect	859		€ 415.532,6600	
SP-24	ServiziProfessionali	ITInfrastructureServiceOperation	Product/Network/Technical Specialist	7299		€ 2.445.310,9800	
SP-02	ServiziProfessionali	ITInfrastructureServiceOperation	Database Specialist and Administrator	1110		€ 276.734,1000	
SP-05	ServiziProfessionali	ITInfrastructureServiceOperation	Cloud Security Specialist	741		€ 184.738,7100	
SP-12	ServiziProfessionali	ITInfrastructureServiceOperation	System and Network Administrator	4343		€ 1.291.781,9200	
SP-07	ServiziProfessionali	SecurityProfessionalServices	Project Manager	33		€ 12.269,4000	
SP-13	ServiziProfessionali	SecurityProfessionalServices	Security Principal	19		€ 9.889,8800	
SP-14	ServiziProfessionali	SecurityProfessionalServices	Senior Information Security Consultant	24		€ 10.170,4800	
SP-15	ServiziProfessionali	SecurityProfessionalServices	Junior Information Security Consultant	55		€ 16.359,2000	
SP-01	ServiziProfessionali	SecurityProfessionalServices	Cloud Application Architect	26		€ 10.071,1000	
SP-04	ServiziProfessionali	SecurityProfessionalServices	Cloud Application Specialist	51		€ 16.082,8500	
SP-16	ServiziProfessionali	SecurityProfessionalServices	Security Solution Architect	48		€ 20.340,9600	
SP-17	ServiziProfessionali	SecurityProfessionalServices	Senior Security Auditor/Analyst	100		€ 44.616,0000	
SP-18	ServiziProfessionali	SecurityProfessionalServices	Junior Security Analyst	72		€ 20.322,0000	
SP-19	ServiziProfessionali	SecurityProfessionalServices	Senior Penetration Tester	22		€ 8.179,6000	
SP-20	ServiziProfessionali	SecurityProfessionalServices	Junior Penetration Tester	47		€ 12.251,0200	
SP-22	ServiziProfessionali	SecurityProfessionalServices	Data Protection Specialist	60		€ 22.308,0000	

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 in linea all'effettivo effort erogato in termini di giorni/uomo delle relative figure professionali

Le seguenti tabelle indicano un modello di rendicontazione delle attività; tali prospetti sono da intendersi come indicativi e non vincolanti per le parti.

			ANNO I												ANNO 2				ANNO 3			
Servizi Professionali di Rearchitect	**Peso**	**Importo**	**Month 1**	**Month 2**	**Month 3**	**Month 4**	**Month 5**	**Month 6**	**Month 7**	**Month 8**	**Month 9**	**Month 10**	**Month 11**	**Month 12**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
		€ TOT																				
Rearchitect	**100%**	**€**	0%	0%	10%	0%	0%	20%	0%	30%	0%	15%	0%	15%		10%						
Servizi professionali (canone mensile		**€ TOT**																				
- Security Professional Services	100%	**€**	4%			5,6%		5,6%		5,6%		5,6%		5,6%	5,6%	11,3%	5,6%	11,3%	5,6%	11,3%	5,6%	11,3%
- IT Service Operations	100%	**€**		5,6%		5,6%		5,6%		5,6%		5,6%		5,6%	5,6%	11,1%	5,6%	11,1%	5,6%	11,1%	5,6%	11,1%
Totale		**€ TOT**																				

			ANNO I												ANNO 2				ANNO 3			
Servizi Professionali di Rearchitect	**Peso**	**Importo**	**Month 1**	**Month 2**	**Month 3**	**Month 4**	**Month 5**	**Month 6**	**Month 7**	**Month 8**	**Month 9**	**Month 10**	**Month 11**	**Month 12**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
		€ TOT																				
Rearchitect	**100%**	**2.438.460,90 €**	- €	- €	243.846,09 €	- €	- €	487.692,18 €	- €	731.538,27 €	- €	365.769,14 €	- €	365.769,14 €	- €	243.846,09 €	- €	- €	- €	- €	- €	- €
Servizi professionali (canone mensile		**€ TOT**																				
- Security Professional Services	100%	**202.860,49 €**	8.114,42 €	- €	- €	11.455,65 €	- €	11.455,65 €	- €	11.455,65 €	- €	11.455,65 €	- €	11.455,65 €	11.455,65 €	22.911,30 €	11.455,65 €	22.911,30 €	11.455,65 €	22.911,30 €	11.455,65 €	22.911,30 €
- IT Service Operations	100%	**4.614.098,37 €**	- €	256.338,80 €	- €	256.338,80 €	- €	256.338,80 €	- €	256.338,80 €	- €	256.338,80 €	- €	256.338,80 €	256.338,80 €	512.677,60 €	256.338,80 €	512.677,60 €	256.338,80 €	512.677,60 €	256.338,80 €	512.677,60 €
Totale		**€ TOT**																				