Polo Strategico Nazionale

Firmato digitalmente da:
EMANUELE IANNETTI
Amministratore Delegato
POLO STRATEGICO NAZIONALE S.P.A.
Firmato il 05/12/2023 10:17
Seriale Certificato: 940
Valido dal 26/10/2022 al 25/10/2025
TI Trust Technologies QTSP CA

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

CUP: H81C23000780006

CIG: 9066973ECE

PROGETTO DEL PIANO DEI FABBISOGNI

AGENZIA ITALIANA DEL FARMACO

PSN-SDE-CONV22-001-

SOMMARIO

1 PREMESSA 7
2 AMBITO 8
3 DOCUMENTI 9
3.1 DOCUMENTI CONTRATTUALI 9
3.2 DOCUMENTI DI RIFERIMENTO 9
3.3 DOCUMENTI APPLICABILI 10
4 ACRONIMI 11
5 PROGETTO DI ATTUAZIONE DEL SERVIZIO 12
5.1 SERVIZI PROPOSTI 12
5.2 INDUSTRY STANDARD 13
5.2.1 Housing 13
5.2.2 Infrastructure as a Service 15
5.2.3 Platform as a Service 23
5.2.4 Data Protection e Disaster Recovery 29
5.3 SECURE PUBLIC CLOUD 33
5.3.1 Descrizione del servizio 33
5.3.2 Personalizzazione del servizio 35
5.3.3 Dettaglio del servizio contrattualizzato (ID servizio, quantità costi) 36
5.3.4 Specifiche di collaudo 37
5.4 CONSOLE UNICA 37
5.4.1 Overview delle caratteristiche funzionali 37
5.4.2 Modalità di accesso 38
5.4.3 Interfaccia applicativa della Console Unica 39
5.5 SERVIZI E PIANO DI MIGRAZIONE 41
5.5.1 Piano di attivazione e Gantt 51
5.6 SERVIZI PROFESSIONALI 57
5.6.1 Re-platform 57
5.6.2 Re-architect 63
5.6.3 Security Profess. Services 65
5.6.4 IT infrastructure service operations 86
6 FIGURE PROFESSIONALI 91
7 SICUREZZA 94
8 CONFIGURATORE 95

9 Rendicontazione 99

Indice delle tabelle

Tabella 1: Informazioni Documento 5
Tabella 2: Autore 5
Tabella 3: Revisore 5
Tabella 4: Approvatore 5
Tabella 5 Documenti Contrattuali 9
Tabella 6: Documenti di riferimento 10
Tabella 7: Documenti Applicabili 10
Tabella 8: Acronimi 11
Tabella 9: Servizi Proposti 13
Tabella 10 Elenco VM Data Center TIM Acilia 22
Tabella 11 Modalità di migrazione dei sistemi AIFA 44
Tabella 12 Divisione applicativi AIFA in gruppi di migrazione 54
Tabella 13 Modalità di distribuzione dei servizi professionali durante la fase di migrazione 100
Tabella 14 Modalità di distribuzione dei servizi professionali tra il M16 e il M25 101
Tabella 16Modalità di distribuzione dei servizi professionali tra il M26 e il M37 102

STATO DEL DOCUMENTO

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

TITOLO DEL DOCUMENTO		
Descrizione Modifica	**Revisione**	**Data**
Prima Emissione	1.0	<DATA>

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 Diego Cavallero/Riccardo Rossi

Tabella 4: Approvatore

<NOTA: impostare la 'data di prima emissione' del documento con quella di invio a PSN del documento definitivo post approvazione da parte di Solution PSN>

LISTA DI DISTRIBUZIONE

INTERNA A:

- Funzione Solution
- Funzione Technology & Information
- Funzione Information Security
- Referente Servizio
- Direttore Servizio

ESTERNA A:

- Referente Contratto Esecutivo AGENZIA ITALIANA DEL FARMACO MAURIZIO TRAPANESE
  - Email: m.trapanese@aifa.gov.it
- Referente Tecnico AGENZIA ITALIANA DEL FARMACO LAURA RAPONE
  - Email: l.rapone@aifa.gov.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 ***AGENZIA ITALIANA DEL FARMACO*** di seguito Amministrazione, sulla base delle esigenze emerse durante gli incontri tecnici per la raccolta dei requisiti e delle informazioni contenute nel Piano dei Fabbisogni (ID **2023-0000097345810580-PdF-P1R1**).

2 AMBITO

In linea con il Piano triennale per l'informatica dell'AgID, l'Agenzia ha avviato, sin dal 2018, il processo di adozione del modello Cloud prevedendo una serie diversificata di interventi e azioni tecniche che hanno consentito di completare, nel corso del 2021, la migrazione dei propri dati e servizi in rete presso l'infrastruttura Cloud PA qualificata dall'Agenzia per l'Italia Digitale e ciò ha consentito di rendere l'Agenzia stessa maggiormente autonoma rispetto ai fornitori di manutenzione e sviluppo delle applicazioni, evitando il verificarsi di potenziali situazioni di vendor lock-in e realizzando, al contempo, gli obiettivi dell'Agenda Digitale Italiana in materia di razionalizzazione dei Data Center e ottimizzazione delle infrastrutture.

L'infrastruttura che ospita i dati e i servizi dell'AIFA è costituita da Datacenter certificati dislocati presso le infrastrutture Telecom Italia S.p.A. (Contratto Quadro Consip SPC Cloud Lotto 1), per l'ambiente di produzione, e Almaviva S.p.a. (Contratto Quadro Consip SPC Cloud Lotto 4), per il Portale istituzionale e l'ambiente di collaudo/preproduzione, in una configurazione disegnata specificamente per la Pubblica Amministrazione. Giova segnalare, inoltre, che l'Agenzia ha implementato un ambiente per lo sviluppo integrato di applicazioni Cloud native presso il Cloud pubblico AWS.

In coerenza con gli indirizzi nazionali, l'Agenzia Italiana del Farmaco ha intenzione di migrare i propri dati e servizi digitali verso il Polo Strategico Nazionale (PSN), infrastruttura ad alta affidabilità che ha l'obiettivo di dotare la Pubblica Amministrazione di tecnologie e infrastrutture cloud che possano beneficiare delle più alte garanzie di affidabilità, resilienza e indipendenza. Al fine di attuare il processo di migrazione dei dati e servizi digitali dell'AIFA verso il PSN, è stata effettuata la Classificazione degli stessi sulla base del modello previsto dalla Strategia Cloud Italia tenendo conto dell'impatto che una compromissione, in termini di confidenzialità, integrità e disponibilità, provocherebbe al sistema Paese. All'esito dell'attività di Classificazione (vedi Allegato 1), n.2 servizi sono stati classificati "critici", la cui compromissione potrebbe determinare un pregiudizio al mantenimento di funzioni rilevanti per la società, la salute, la sicurezza e il benessere economico e sociale del Paese, e n.61 "ordinari", la cui compromissione non provoca l'interruzione di servizi dello Stato o, comunque, un pregiudizio per il benessere economico e sociale del Paese.

Al fine di non pregiudicare l'erogazione del finanziamento assegnato, l'Agenzia dovrà concludere il progetto nella forma, nei modi e nei tempi previsti, ovvero massimo 15 mesi dalla data di firma del Contratto di utenza con il PSN.

3 DOCUMENTI

3.1 DOCUMENTI CONTRATTUALI

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

Tabella 5 Documenti Contrattuali

3.2 DOCUMENTI DI RIFERIMENTO

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

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

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

Tabella 6: Documenti di riferimento

3.3 DOCUMENTI APPLICABILI

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

Tabella 7: Documenti Applicabili

4 ACRONIMI

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

Acronimo	Descrizione
AI	Artificial Intelligence
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
L&S	Lift and shift
MSP-PSN	Managed Service Provider – Polo Strategico Nazionale
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

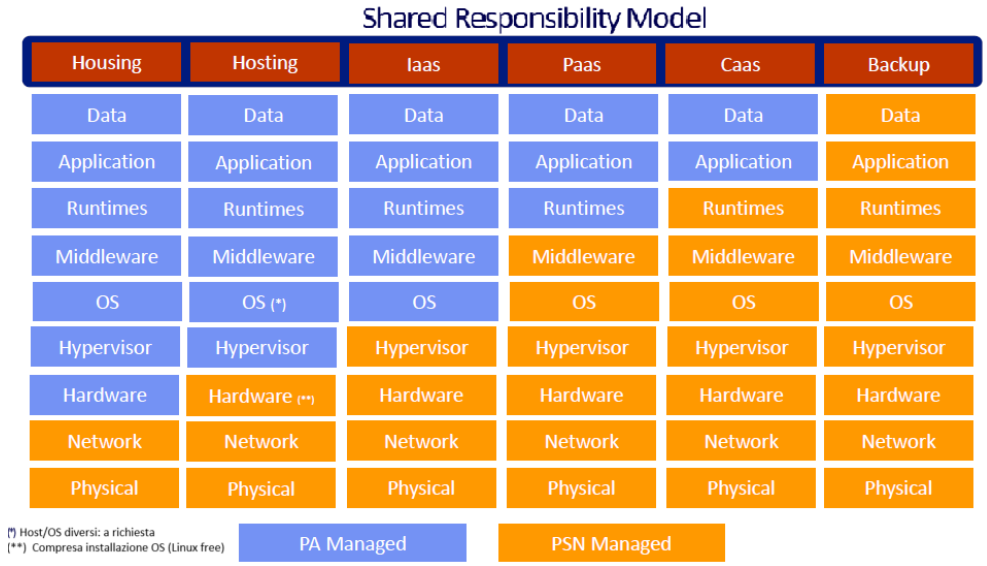
Di seguito si riporta una sintesi delle soluzioni individuate per soddisfare le esigenze dell'Amministrazione.

SERVIZIO	TIPOLOGIA
INDUSTRY STANDARD	Infrastructure as a Service Shared
INDUSTRY STANDARD	Infrastructure as a Service Storage
INDUSTRY STANDARD	Platform as a Service DB
INDUSTRY STANDARD	Data Protection e DR
INDUSTRY STANDARD	Antivirus
INDUSTRY STANDARD	Housing - IP
SECURE PUBLIC CLOUD	Compute Production
SECURE PUBLIC CLOUD	Storage
SECURE PUBLIC CLOUD	Network
SECURE PUBLIC CLOUD	Public Cloud, Security, Backup, SIEM
SECURE PUBLIC CLOUD	Public Cloud, Security, Backup, Monitor
SECURE PUBLIC CLOUD	Public Cloud, Security, Backup, Firewall
SECURE PUBLIC CLOUD	Public Cloud, Security, Backup, Cloud Backup
SERVIZI PROFESSIONALI	Replatform
SERVIZI PROFESSIONALI	Figura di Migrazione

SERVIZIO	TIPOLOGIA
SERVIZI PROFESSIONALI	Security Professional Services
SERVIZI PROFESSIONALI	IT Infrastructure Service Operations

Tabella 9: Servizi Proposti

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



5.2 INDUSTRY STANDARD

5.2.1 Housing

5.2.1.1 Descrizione del servizio

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

5.2.1.2 Personalizzazione del servizio

Nell'ambito dei servizi di Housing offerti dal PSN si inseriscono anche le subnet di indirizzi IP necessarie alla configurazione dei servizi dell'Amministrazione. Nell'ambito del progetto di AIFA sono incluse 60 subnet da 8 indirizzi pubblici.

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

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

5.2.1.4 Specifiche di collaudo

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

5.2.2 Infrastructure as a Service

5.2.2.1 Descrizione del servizio

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

Figura 1 Infrastructure as a Service

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

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

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

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

5.2.2.2 Personalizzazione del servizio

Si riporta di seguito l'elenco delle VM attualmente ospitate sul Data Center di TIM Acilia, nell'ambito della Convenzione SPC Cloud, oggetto della migrazione:

VM	CPUs	RAM (GB)	STORAGE (GB)
AIFABDSPRDDB1	4	16	75
AIFABDSPRDWS1	2	8	305
AIFACESPFTP	2	4	30
AIFAE4LADD1	8	24	200
AIFAE4LBUS1	4	24	150

VM	CPUs	RAM (GB)	STORAGE (GB)
AIFAE4LDMS1	4	16	1.050
AIFAE4LSES1	4	16	1.050
AIFAEXTAPP1	2	16	280
AIFAEXTAPP2	2	16	240
AIFAEXTAPP3	16	32	400
AIFAEXTAPP4	12	32	250
AIFAEXTWEB1	2	8	160
aifainfapp1	4	16	260
aifainfapp2	4	16	260
aifainfapp3	4	16	260
AIFAINFBAT1	2	4	60
aifainfetl1	16	32	160
aifainfetl2	16	32	160
aifainfetl3	16	32	160
aifainfops	4	24	110
aifainfprx1	2	4	60
aifainfvm1	4	32	3.060
aifainfvm2	4	32	3.060
aifainfvm3	4	32	3.060
aifainfvm4	2	12	160
aifainfvm5	2	8	160
aifainfvm6	2	8	160
aifainfvm7	2	4	170
aifainfvm8	2	4	170
aifainfvm9	2	4	170
aifainfwso1	2	16	460
aifainfwso2	2	16	460
AIFAKMSPRDAS1	4	16	562
AIFAKMSPRDAS2	4	16	512
AIFAKMSPRDAS3	4	16	540
AIFAKMSPRDDB1	2	8	490
AIFAKMSPRDDB2	2	8	490
AIFAKMSPRDDB3	2	8	490
AIFAKMSPRDWS1	4	16	112
AIFAMDSAPP1	8	32	340
AIFAMDSAPP2	8	32	340
AIFAMDSAPP4	8	32	340
AIFAMDSAPP5	4	8	110
AIFAMDSWS1	4	8	110

VM	CPUs	RAM (GB)	STORAGE (GB)
AIFANRNFELK1	4	64	680
AIFANRNFELK2	4	64	680
AIFANRNFELK3	4	64	680
AIFANRNFETL1	4	16	100
AIFAPFIX01	2	4	100
AIFAPRDAS1	12	32	110
AIFAPRDAS11	4	32	310
AIFAPRDAS2	12	32	200
AIFAPRDAS3	4	16	150
AIFAPRDAS4	4	16	150
AIFAPRDAS7	8	32	260
AIFAPRDAS8	4	8	110
AIFAPRDDB3	4	16	560
AIFAPRDWS1	2	8	90
AIFAPRDWS2	2	8	90
AIFAPRDWS4	2	8	90
AIFASRVMF1	2	4	150
AIFASRVVD01	32	64	700
AIFATLTB01	8	24	150
AIFAWEBAPP1	2	16	300
AIFAWEBAPP2	2	16	300
AIFAWEBAPP3	2	16	300
AIFAWSO2ACCLB01	2	4	60
AIFAWSO2ACCLB02	2	4	60
AIFAWSO2ACCMN01	2	4	60
AIFAWSO2ACCWK01	2	4	60
AIFAWSO2ACCWK02	2	4	60
ART50SRV1	4	16	5.646
ART50SRV3	4	6	300
INFRHAPRX1	4	8	40
INFRHAPRX2	4	8	40
INFRSRVANS1	2	2	25
INFRSRVDNS1	1	2	25
INFRSRVDNS2	1	2	25
INFRSRVDRV1	2	4	60
INFRSRVFTP1	2	4	1.044
INFRSRVMAM1	8	16	270
INFRSRVNFS1	4	8	11.717
INFRSRVNFS4	4	8	6.080

VM	CPUs	RAM (GB)	STORAGE (GB)
INFRSRVVSA1	8	4	6.219
INFRSRVVSA2	8	4	100
INFRSRVZBX1	2	8	50
INFRSRVZMB1	4	8	100
LEAIFAACAD1	2	4	50
LEAIFAACAP1	4	8	50
LEAIFAACAP2	4	8	50
LEAIFAALFR1	4	24	110
LEAIFAALFR2	4	24	110
LEAIFAAPP11	2	4	60
LEAIFAAPP12	2	4	160
LEAIFABAL01	2	4	50
LEAIFABAL02	2	4	50
LEAIFABDFWEB2	4	4	60
LEAIFAELAS1	4	16	50
LEAIFAELAS2	8	32	3.065
LEAIFAELK	2	4	160
LEAIFAETCD1	2	4	50
LEAIFAETCD2	2	4	50
LEAIFAETCD3	2	4	50
LEAIFAETL1	4	20	300
LEAIFAFAKEAPP2	4	8	60
LEAIFAFAKEDB1	4	8	250
LEAIFAFAKEDB2	4	8	250
LEAIFAFAKEWEB1	4	8	90
LEAIFAFRONT1	2	8	60
LEAIFAFRONT2	2	8	60
LEAIFAFSRV1	4	8	2.060
LEAIFAGDPR1	4	8	50
LEAIFAGDPR2	4	8	50
LEAIFAGIT	4	16	200
LEAIFAIAM1	16	12	100
LEAIFAIAM2	8	12	100
LEAIFAIAMDB1	8	16	200
LEAIFAIAMDB2	8	16	200
LEAIFALIFE1	8	24	60
LEAIFALIFE2	8	24	60
leaifamndb1	6	40	5.060
LEAIFAMNDB134	8	64	17.100

VM	CPUs	RAM (GB)	STORAGE (GB)
leaifamndb2	6	40	5.060
LEAIFAMNDB234	8	64	11.100
leaifamndb3	6	40	6.060
LEAIFAMNDB334	8	64	10.600
LEAIFANFS1	4	4	6.830
LEAIFANFS2	2	4	2.584
LEAIFANFS3	2	4	10.060
LEAIFAONLYOFFICE1	2	4	60
LEAIFAONLYOFFICE2	2	4	60
LEAIFAOPENDJ1	4	8	60
LEAIFAOPENDJ2	4	8	60
LEAIFAOPS34	4	8	100
LEAIFAOTRS	4	8	80
LEAIFAOWNCLOUDAPP1	6	4	60
LEAIFAOWNCLOUDAPP2	6	4	60
LEAIFAOWNCLOUDDB	6	16	110
LEAIFAPDD01	4	8	60
LEAIFAPDD02	4	8	60
LEAIFAPDDDC	2	4	60
LEAIFAPDDWEB1	2	8	60
LEAIFAPDDWEB2	2	8	60
LEAIFAPIWIK	8	24	220
LEAIFAPIWIKDB1	4	16	170
LEAIFAPIWIKDB2	4	16	170
LEAIFAPIWIKWEB1	4	8	60
LEAIFAPIWIKWEB2	4	8	60
LEAIFAPSERVICE1	12	32	170
LEAIFAPSERVICE2	12	32	170
LEAIFAPSQL1	8	16	100
LEAIFAPSQL2	8	16	100
LEAIFAPSQL3	8	16	100
LEAIFAPSQL4	4	8	50
LEAIFAPSQL5	4	8	50
LEAIFAQUALIFICAZIONE	4	16	60
LEAIFARPRXVM1	8	12	60
LEAIFARPRXVM2	8	12	60
LEAIFARSOAPP1	2	8	100
LEAIFARSOAPP2	2	8	100
LEAIFARSODB1	2	4	120

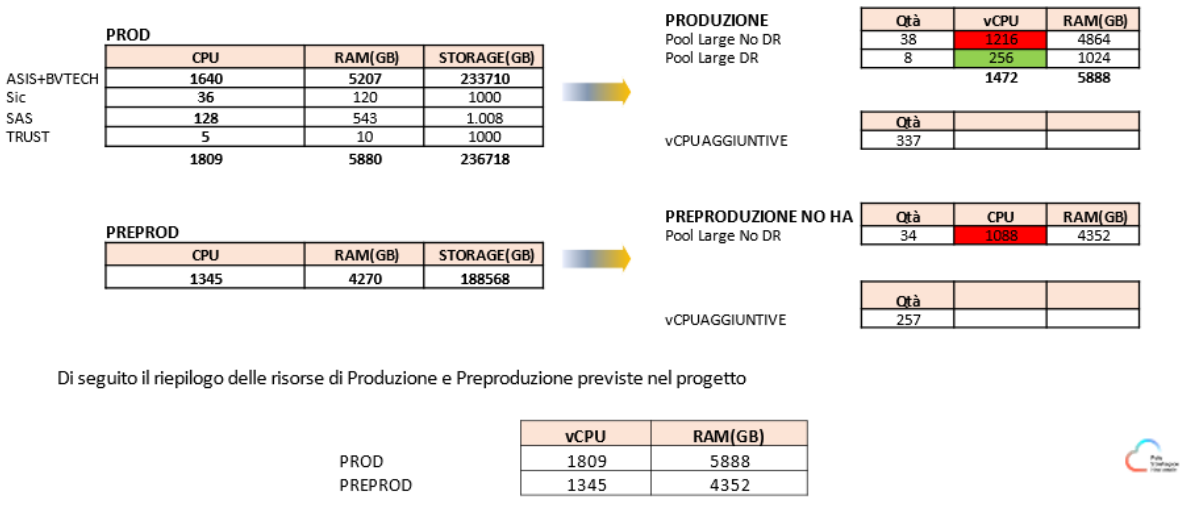
VM	CPUs	RAM (GB)	STORAGE (GB)
LEAIFARSODB2	2	4	120
LEAIFARSOWIT	2	2	60
LEAIFASCRIBA2	8	24	160
LEAIFASOL1	2	16	300
LEAIFASOL2	2	16	300
LEAIFASYMMETRICDS1	2	4	60
LEAIFATASAPP1	4	16	60
LEAIFATASAPP2	4	16	60
LEAIFAWSO2BPSMN01	2	4	180
LEAIFAWSO2BPSWK01	2	4	60
LEAIFAWSO2BPSWK02	2	4	60
LEAIFAWSO2LB01	2	4	60
LEAIFAWSO2LB02	2	4	110
PSRVFILENETCEPE	4	16	140
PSRVFILENETDB	4	16	490
PSRVFILENETWEB	4	16	150
SASAIFADIS01	16	64	950
SASAIFAOAS01	16	64	950
SASAIFAVAS01	16	64	1.850
SASAIFAVAW01	16	64	450
SASAIFAVAW02	16	64	450
SASAIFAVAW03	16	64	450
SASAIFAVAW04	16	64	450
SASAIFAVAW05	16	64	450
SASAIFAVAW06	16	64	450
SASAIFAVAW07	16	65	450
SASAIFAVAW08	16	64	450
SASAIFAWEB01	16	32	350
SASAIFAWEB02	16	32	350
VIGIFARMSRV1	16	16	150
VIGISEGNSRV1	16	16	150
WEAIFACHECKIN01	4	8	60
WEAIFACHECKIN02	4	8	60
WEAIFADC1	4	8	90
WEAIFAGESINF	4	8	180
AIFATBCSFS1	4	16	100
AIFATBCSFS2	4	16	100
AIFATBCSFM1	8	32	100
AIFATBCSFM2	8	32	100

VM	CPUs	RAM (GB)	STORAGE (GB)
AIFATBCPSQL1	2	8	100
AIFATBCTDV1	2	8	100
AIFANILIFE1	2	8	80
AIFANILIFE2	2	8	80
AIFANIELAS1	2	8	60
AIFANIELAS2	2	8	60
LEAIFARPRXVM3	8	12	60
LEAIFAIAM3	12	16	200
LEAIFARPRXVM4	8	12	60
LEAIFAIAM4	12	16	100
LEAIFARPRXVM5	8	12	60
LEAIFARPRXVM6	8	12	60
LEAIFAIAM5	12	16	100
LEAIFAIAM6	12	16	100
AIFAWEBACC1	8	8	100
INFRHAPRX3	4	8	60
INFRHAPRX4	8	16	60
AIFA-OCP4-HAPROXY1	2	4	50
AIFA-OCP4-HAPROXY2	2	4	50
AIFA-OCP4-BASTION	2	4	380
AIFA-OCP4-DHCP	2	4	80
AIFA-OCP4-MASTER01	4	16	200
AIFA-OCP4-MASTER02	4	16	200
AIFA-OCP4-MASTER03	4	16	200
AIFA-OCP4-INFRA01	4	16	200
AIFA-OCP4-INFRA02	4	16	200
AIFA-OCP4-INFRA03	4	16	200
AIFA-OCP4-ODF01	4	16	2.200
AIFA-OCP4-ODF02	4	16	2.200
AIFA-OCP4-ODF03	4	16	2.200
AIFA-OCP4-WORKER01	4	16	200
AIFA-OCP4-WORKER02	4	16	200
AIFA-OCP4-WORKER03	4	16	200
AIFA-OCP4-WORKER04	4	16	200
AIFA-OCP4-WORKER05	4	16	200
AIFA-OCP4-WORKER06	4	16	200
AIFA-OCP4-WORKER07	4	16	200
AIFA-OCP4-WORKER08	4	16	200
AIFA-OCP4-WORKER09	4	16	200

VM	CPUs	RAM (GB)	STORAGE (GB)
AIFA-OCP4-WORKER10	4	16	200
AIFA-OCP4-WORKER11	4	16	200
AIFA-OCP4-WORKER12	4	16	200
AIFAOCPVM1	8	16	60
AIFAOCPVM2	8	16	60
SASAIFAVAW09	16	64	450
aifa-os4-load-balancer01	2	4	61
aifa-os4-load-balancer02	2	4	61
aifa-os4-idm1	2	4	41
aifa-os4-idm2	2	4	41
AIFAMDSWS1_1506	4	8	113
aifanielas1	2	8	61
INFRSRVCTI1	2	4	72
LEAIFAOPS	4	8	82
WEAIFAOPSMGR	4	8	276
INFRSRVZMB2	2	8	102
PonteWin	2	4	41
Tot	**1.354**	**4.293**	**170.388**

Tabella 10 Elenco VM Data Center TIM Acilia

Nel dimensionamento del nuovo ambiente in ottica IAAS Shared si è tenuto conto di un fattore di crescita del 20% per le risorse di CPU e RAM, mentre secondo le indicazioni del Cliente si sono considerati circa 64T di Storage aggiuntivi rispetto all'AS-IS. L'ambiente di preproduzione è dimensionato come i 4/5 dell'ambiente di produzione. Nella figura di seguito si riportano dei dati di sintesi sul dimensionamento.



Di seguito il riepilogo delle risorse di Produzione e Preproduzione previste nel progetto

	vCPU	RAM(GB)
PROD	1809	5888
PREPROD	1345	4352

Sul pool di risorse Industry Standard considerate in questa versione del Progetto, il PSN garantisce ad AIFA, per i 10 anni di contratto, le licenze di sistemi operativi (RedHat e Windows) necessarie per le VM che saranno create.

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

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

5.2.2.4 Specifiche di collaudo

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

5.2.3 Platform as a Service

5.2.3.1 Descrizione del servizio

Il **Servizio Platform as a Service (PaaS)** è un servizio *Core* e consiste nella messa a disposizione, da parte del PSN, di una piattaforma in grado di erogare elementi applicativi e middleware come servizio, come ad esempio i Database, astraendo dall'infrastruttura sottostante. Il PSN, in qualità di provider, si fa carico di gestire l'infrastruttura sottostante, comprensiva degli strumenti di automation e orchestration.

L'offerta dei servizi PaaS prevede un approccio strutturato in cui ogni componente della soluzione PaaS, come il sistema operativo, solution stack ed altri software necessari, è gestito e strettamente controllato in termini di utilizzo e configurazione dal PSN. In questo caso le soluzioni vengono "create" al momento della necessità. Una rappresentazione di questa strutturazione vede quattro livelli di componenti:

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

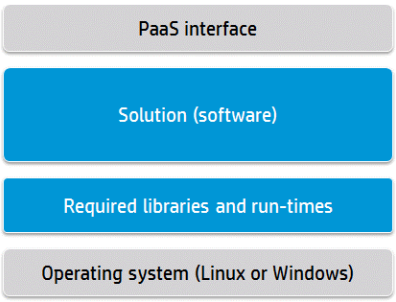


Figura 2 Platform as a Service

Il servizio PaaS si compone dei seguenti sottoservizi:

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

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

5.2.3.2 Platform as a Service - Database

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

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

5.2.3.3 Identity Access Management

In aggiunta ai servizi di Identity and Access Management descritti al § **Errore. L'origine riferimento non è stata trovata.** del documento "Progetto di Fattibilità" che garantiscono i diritti di accesso alle componenti tecniche in ambito PSN (IaaS, PaaS, console unica di gestione, ecc.), viene reso disponibile dal PSN un servizio di Identity Management applicativo che consente di gestire in modo unificato e centralizzato l'autenticazione e l'autorizzazione per la messa in sicurezza delle applicazioni che migrano nel PSN.
Tale servizio ha lo scopo di integrare in modo facile e nativo le differenti esigenze di autenticazione e autorizzazione ad oggi previste all'interno del Codice dell'Amministrazione Digitale (CAD), in accordo con le normative vigenti in materia di trattamento dati riportate nel General Data Protection Regulation (GDPR).
Il servizio mette a disposizione le seguenti funzionalità:

- credenziali uniche di accesso alle applicazioni in perimetro e presidio efficace dei punti di accesso;
- implementazione di policy di cambio password, autenticazione a due fattori o semplicemente auditing e monitoring dei log di accesso;
- profilazione e segregazione delle informazioni in funzione dei propri privilegi: l'approccio di base si è concentra sulla creazione del "need-to-know". Le informazioni sensibili sono rese

disponibili solo a quelle persone dotate di adeguate autorizzazioni e di un "need-to-know" di tali informazioni per l'esercizio delle loro funzioni;
- controllo della diffusione delle informazioni: c'è una ragionevole probabilità che maggiori restrizioni sulla diffusione di informazioni sensibili riduce le possibilità di fughe di notizie e compromessi ("need-to-share").

I principali moduli funzionali disponibili all'interno del servizio IAM fornito sono:

- **Identity Management & Governance**: è responsabile per la gestione del ciclo di vita delle identità digitali, gestisce la creazione, la modifica o la cancellazione delle identità, i loro attributi e il rapporto tra identità e attributi all'interno del sistema IAM. Inoltre, è responsabile per la gestione del ciclo di vita dei ruoli e dei diritti di accesso per gestite le risorse di amministrazione;
- **Access Control & Management**: è responsabile di gestire l'assegnazione dei diritti di accesso alle identità e l'esecuzione, in caso contrario la convalida, dei diritti di accesso su sistemi finali;
- **Credential Management**: è responsabile per la gestione del ciclo di vita delle credenziali delle identità e la gestione dei relativi eventi, come la creazione, blocco, sblocco, etc.;
- **Multi Factor Authentication**: gestisce gli schemi di autenticazione utilizzati sul sistema IAM multifattore (gestione delle password, OTP Token, Smart Card, etc.). Per garantire la sicurezza dell'intera filiera applicativa il sistema di autenticazione multi-fattore deve garantire i livelli di sicurezza definiti all'interno della norma ISO/IEC DIS 29115;
- **Logging & Reporting**: è il componente responsabile di raccogliere, correlare e normalizzare tutte le informazioni gestite dal sistema IAM per generare rapporti per uso amministrativo o di revisione contabile;
- **Federation Services**: rappresentano i servizi di federazione verso Identity Provider Esterni garantendo la piena compatibilità con i più diffusi sistemi di autenticazioni federati (SPID, eIDAS, CNS, etc.). In particolare, con l'introduzione dello SPID (Sistema Pubblico di Identità Digitale) promosso dall'Agenzia per l'Italia Digitale (AgID), il servizio proposto consente di accedere con un unico login ai diversi servizi on line di tutti i Soggetti Pubblici (PA) e Privati che adottano questo sistema di autenticazione. Il servizio SPID Enabling consente di connettere e abilitare i servizi web di aziende pubbliche e private al sistema di autenticazione SPID (Sistema Pubblico delle Identità Digitali) basandosi su un gateway di federazione SAML 2.0 nel quale sono state implementate le logiche e le specifiche tecniche SPID ed abilita ad un sistema di autenticazione federato verso tutti gli Identity Provider accreditati AgID;

5.2.3.4 Big Data

Il servizio consente la costruzione di Data Lake as a Service, servizi di analisi dati batch, stream e real-time con scalabilità orizzontale e un servizio per la data governance:

- **Data Lake:** fornisce una piattaforma pronta all'uso che dispone di tutte le funzionalità necessarie a sviluppatori, Data Scientist e analisti per archiviare facilmente dati di tutte le dimensioni, forme e velocità. Tale soluzione permette l'archiviazione e analisi di file con scalabilità orizzontale, lo sviluppo di programmi con architettura altamente parallela, l'integrazione con Schedulatori di Risorse Esterni (YARN, Kubernetes), essere progettato per essere utilizzato su infrastrutture cloud e supportare una vasta gamma di linguaggi (Python,R, Java, .Net, Scala);
- **Batch/Real time Processing:** fornisce una piattaforma pronta all'uso per sviluppare processi batch e in streaming basati su un motore di esecuzione in Memory e basato su scalabilità orizzontale e parallela. Tale soluzione consente l'analisi di grandi moli di dati sia in batch che in streaming, un paradigma di programmazione unico per l'analisi in batch e in streaming, lo

sviluppo di programmi performanti con utilizzo di architetture scalabili orizzontalmente e parallele, mette a disposizione Tool per il Debug e l'ottimizzazione dei programmi sviluppati, è Integrabile con Schedulatori di Risorse Esterni (YARN, Kubernetes) e cloud ready, supporta una vasta gamma di linguaggi (Python,R, Java, .Net, Scala), espone api rest per il monitoraggio e il submit dei job da remoto, fornisce un pannello per il monitoraggio del job e dettagli per singolo job, integrabile con Storage Esterni (Data Lake Paas), fornisce funzionalità di autoscaling e fornisce meccanismi di caching su SSD;

- **Event Message:** rende disponibile una piattaforma pronta all'uso per sviluppare applicazioni e pipeline dati in real time inoltre deve fungere da Message Broker fornendo funzionalità di tipo Publish e Subscribe. Tale soluzione permette la gestione di grandi moli di eventi, lo sviluppo di programmi basati su architettura altamente parallela e scalabile orizzontalmente, fornire tool per il Debug e l'ottimizzazione dei programmi sviluppati, l'integrazione con Schedulatori di Risorse Esterni (YARN, Kubernetes) e progettato per essere utilizzato su infrastrutture cloud, supportare una vasta gamma di linguaggi (Python, R, Java, .Net, Scala), fornire funzionalità di autoscaling, implementare meccanismi di consegna degli eventi in ordine ed essere integrabile con framework di Stream Processing (Spark).
- **Data Governance:** fornisce una piattaforma pronta all'uso che mette a disposizione un unico punto di riferimento sicuro e centralizzato per il controllo dei dati. Sfruttando strumenti di "search and discovery" e i connettori per estrarre metadati da qualsiasi sorgente di dati, permette di semplificare la protezione dei dati, l'esecuzione delle analisi e la gestione delle pipeline, oltre ad accelerare i processi ETL.

5.2.3.5 Artificial Intelligence

Il servizio di **Artificial Intelligence (AI)** mette a disposizione un set di algoritmi preaddestrati di Artificial Intelligence per utilizzarli in analisi del testo, audio/video o di anomalie ed una piattaforma per la realizzazione di modelli custom di machine/Deep Learning:

- **AI Platform:** rende disponibile una piattaforma pronta all'uso per costruire modelli di ML/DL facilitando l'accesso al dato mettendo a disposizione una ambiente collaborativo a cui partecipano sia esperti di contesto che Data Scientist. Tale soluzione permette il supporto di almeno le seguenti tipologie di sorgenti dati: NoSQl, SQL, Hadoop File Formats, Remote Data Sources, Cloud Object Storage, Cluster Hadoop, Rest Api; fornisce moduli configurabili per il data cleaning, wrangling e mining, strumenti e librerie per la visualizzazione dei dati, supporta le principali librerie per lo sviluppo di modelli di ML/DK (PyTorch, TensorFlow, ScikitLeran, H20,XGBoost, etc), supportare gli ultimi trend tecnologici (AutoML, Explanable AI), supportare una vasta gamma di linguaggi (Python, R) e strumenti a Notebook (Jupyter), permette la gestione della sicurezza di livello enterprise con la possibilità di implementare politiche RBAC, fornisce un approccio visuale di tipo Drag&Drop per lo sviluppo, la gestione intera del ciclo di vita di un progetto di datascience (Business Undestanding, Data Acquisition&Understanding, Modeling, Deployment), rende possibile interrogare i modelli attraverso degli endpoint Rest, monitorare le performance dei singoli modelli, supporta sia CPU che GPU, permette il Deploy dei modelli in versione dockerizzata e su Kubernetes, permette la creazione di pipeline di automation per la creazione di ambienti e il rilascio dei modelli, permette la creazione di Wiki per la condivisione delle informazioni relative ai singoli progetti, è integrabile con IAM esterni, permette il tracciamento e monitoraggio di tutte le azioni effettuate sulla piattaforma, permette la gestione centralizzata delle risorse di computing, permette la possibilità di creare policy custom per la protezione del dato e integrabile con sistemi di calcolo distribuiti (Spark, Hive, Impala, etc).

- **Semantic Knowledge Search:** fornisce una piattaforma pronta all'uso in grado di rendere facilmente accessibili le informazioni contenute all'interno del patrimonio informativo (documenti, immagini, video) utilizzando un motore di ricerca semantico in grado di interpretare richieste in linguaggio naturale. Tale soluzione permette di gestire contenuti in varie tipologie di formati (Documenti Word, pdf, pptx , email, immagini, video, etc), di indicizzare le informazioni contenute nei documenti, l'implementazione di un motore di ricerca di tipo full-text e di tipo semantico performante, l'esposizione di un'interfaccia in linguaggio naturale, il supporto almeno delle seguenti Lingue (Inglese, Italiano, Tedesco, Spagnolo), implementare meccanismo di auto apprendimento mediante feedback utenti, garantire la sicurezza del dato con vari tipologie di protezione (At rest, In Transit), garantire scalabilità orizzontale, esporre delle api per l'integrazione con sistemi esterni e essere integrabile con uno IAM esterno.
- **Text Analytics /NLP:** questa soluzione rende disponibile una piattaforma pronta all'uso in grado di estrarre informazioni da testo non strutturato. Tale soluzione consente di esporre delle api rest per l'inferenza dei modelli, l'estrazione di Entità dal testo (Persone, Luoghi, etc), estrazione di concetti chiave dal testo, estrazione del Sentiment, riconoscimento della Lingua, garantisce scalabilità orizzontale, supporto Load Balancing, il supporto almeno delle seguenti Lingue (Inglese, Italiano, Tedesco, Spagnolo),il tracciamento e il monitoraggio delle interrogazioni al sistema e la possibilità di essere eseguibile su Kubernetes o in versione dockerizzata.
- **Audio Analytics:** fornisce una piattaforma pronta all'uso in grado di applicare algoritmi basati su AI su fonti audio. Tale soluzione permette di analizzare grandi volumi di audio, garantire scalabilità orizzontale, supportare Load Balancing, mettere a disposizione algoritmi per l'estrazione di informazioni da fonti audio (Analisi rumore ambientale, Speaker Identification, Audio Insight), esporre un'interfacciata basata su api rest per l'inferenza, permettere la configurazione degli algoritmi da User Interface, fornire Report e Dashboard per il monitoraggio delle risorse del sistema e dei processi attivi, generazione di Eventi verso sistemi esterni, elaborazione sia in streaming che in batch, algoritmi estendibili attraverso componenti dockerizzate e deployable su Cluster Kubernetes.
- **Video Analytics:** è una piattaforma pronta all'uso in grado di applicare algoritmi basati su AI su fonti video. Tale soluzione consente di analizzare grandi volumi di video, garantire scalabilità orizzontale, supporto al Load Balancing, mettere a disposizione algoritmi per l'estrazione di informazioni dai video (Detection, Classification, Identification, Counting, Density Estimation), esporre un'interfacciata attraverso api rest per la lettura dei metadati generati dagli algoritmi, fornire un portale web per la configurazione dei flussi video e degli algoritmi, fornire Report e Dashboard per il monitoraggio delle risorse del sistema e dei processi attivi, generare Eventi verso sistemi esterni, elaborazione dei video sia in streaming che in batch e fornire estendibilità degli algoritmi attraverso componenti dockerizzate.

5.2.3.6 Personalizzazione del servizio

Attualmente l'Amministrazione ha attive in ognuno dei propri ambienti di produzione e preproduzione tre istanze PaaS DB Oracle con Licenza Oracle Enterprise Edition così dimensionate:

PaaS – DB	Vcpu reali	RAM	HDD (GB)
DB Oracle ENT. 3 (AIFA 1)	8	62	14.000

DB Oracle ENT. 2 (AIFA 2)	8	62	8.200
DB Oracle ENT. 1 (AIFA 3)	2	15	10.000

Rispetto all'AS-IS è stato considerato un fattore di crescita del 10% sullo Storage.

All'interno del presente progetto, tutti PaaS DB Oracle sopra indicati sono stati considerati sia per l'ambiente di produzione che per l'ambiente di preproduzione, portandone quindi il numero totale a sei (6).

Inoltre, i PaaS AIFA 1 e AIFA 2 sono DB funzionali per l'erogazione dei servizi "critici": di conseguenza sono stati considerati all'interno dell'infrastruttura di DR.

Dal punto di vista del dimensionamento tecnico, i PaaS sono stati dimensionati in funzione delle risorse indicate nella tabella precedente; per lo storage è stata utilizzata la voce di listino PSN relativa allo Storage HP Encrypted.

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

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

5.2.3.8 Specifiche di collaudo

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

5.2.4 Data Protection e Disaster Recovery

5.2.4.1 Data Protection: Backup

Servizio «self-managed» l'utente ha completa autonomia di gestione nella definizione della policy di backup.
naturalmente il recupero degli stessi, in caso di perdita dovuta a guasti hardware o malfunzionamenti del software. Il ripristino può avvenire ad una certa data in relazione alle copie di backup effettuate. Il servizio di backup standard prevede di effettuare il backup dello storage base (100GB) previsto per ogni istanza.
Per tutti i backup sarà effettuata una ulteriore copia secondaria al completamento della copia primaria presso il Data Center secondario
Le principali caratteristiche del servizio che verrà realizzato sono:

- La possibilità di effettuare backup full e incrementali;
- Cifratura dei dati nella catena end to end (dal client alla libreria);
- Possibilità di organizzare i backup ed effettuare ricerche sulla base di differenti filtri (es. date di riferimento) e mantenere più backup in contemporanea;
- Possibilità di poter selezionare cartelle e file da sottoporre a backup e possibilità di escludere tipologie di file per nome, estensione e dimensione per i backup di tipo file system (con installazione di un agent sui server oggetto di backup);
- la conservazione e svecchiamento dei dati del back-up secondo policy di retention standard: 7 giorni, 1 mese, 2 mesi, 3 mesi, 6 mesi, 1 anno, 10 anni;
- possibilità di modificare la policy di retention (tra quelle su indicate) applicate ai backup;
- monitoring dei jobs di backup e restore;
- reportistica all'interno della console;
- un metodo efficiente per trasmissione ed archiviazione applicando tecniche di compattazione e compressione ed identificando ed eliminando i blocchi duplicati di dati durante i backup.
- Il ripristino dei dati scegliendo la versione dei dati da ripristinare in funzione della retention applicata agli stessi.
- il ripristino granulare dei dati (singolo file, mail, tabella, ecc.) in modalità "a caldo e out-ofplace" garantendo quindi la continuità operativa. Tale modalità di ripristino assicura la possibilità di effettuare dei test di restore in qualsiasi momento e con qualsiasi cadenza.
- Repository storage del servizio su apparati di tipo NAS o S3 (AWS-S3 compatibile)
- GDPR Compliant: Supporta utente e ruoli IAM oltre alla cifratura del dato e controllo degli accessi

Il servizio di Backup è fatturato a canone annuale basato sulla quantità di spazio (TB) riservato al Cliente in fase di acquisto del servizio indipendentemente da quanto spazio sia stato occupato.

5.2.4.2 Data Protection: Golden copy protetta

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

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

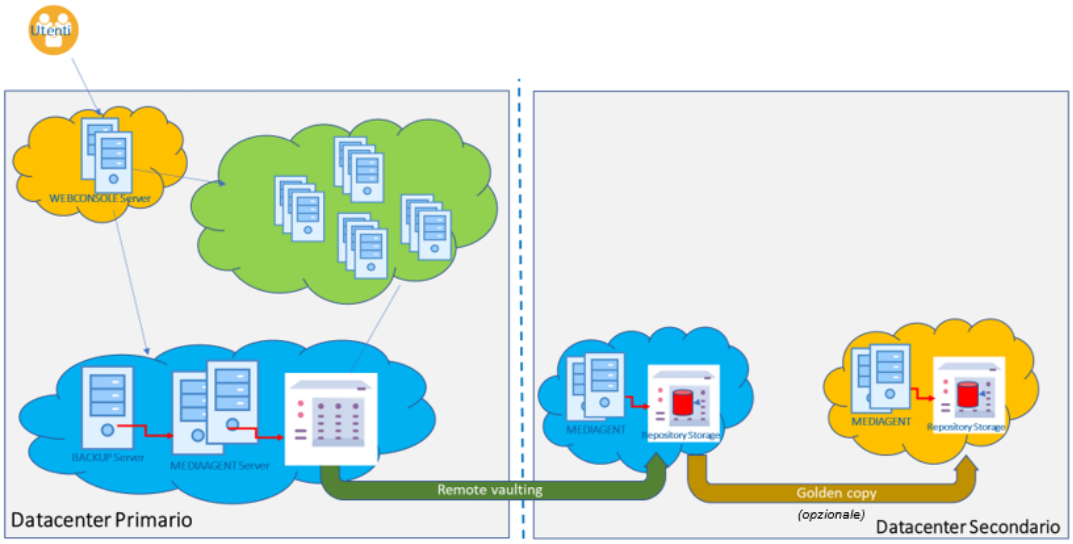


Figura 3 Architettura Funzionale Golden Copy

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

- analisi automatizzata del backup per certificarne l'assenza di vulnerabilità (incluse attività sospette di *ransomware*);

- certificazione della Golden Copy da parte del PSN;
- protezione su storage distinto di backup, **privo di ogni accesso fisico e logico**;
- replica in **Region diverse e su canale cifrato.**

5.2.4.3 Disaster Recovery as a Service

Il Disaster Recovery "*as-a-Service*" (DRaaS) è il servizio di cloud computing che consente il ripristino dei dati e dell'infrastruttura IT di un ambiente completo di sistemi e relativi dati. Ciò consente di ripristinare l'accesso e la funzionalità dell'infrastruttura IT dopo un evento disastroso. Il modello as-a-service prevede che l'Amministrazione non debba essere proprietaria di tutte le risorse né occuparsi della gestione per il Disaster Recovery, affidandosi al service provider per un servizio completamente gestito.
Il DRaaS si basa sulla replica e sull'hosting dei server in site del PSN diverso rispetto all'ubicazione primaria. Il PSN implementa un piano di Disaster Recovery in caso di evento disastroso che causa l'indisponibilità del servizio nel sito primario.

5.2.4.4 Personalizzazione del servizio

Data Protection Backup e Golden Copy
AIFA ha un ambiente complesso composto da più elementi con necessità in termini di backup differenti:

1. DB: FULL settimanale + differenziali della settimana in corso, con retention di 2 settimane per entrambi. In aggiunta, un backup FULL mensile con retention 6 mesi.
2. SO VM: 1 FULL settimanale + differenziali della settimana in corso, con retention di 2 settimane per entrambi. In aggiunta, un backup FULL mensile con retention 2 mesi. (Include l'ambiente OCP).
3. DISCO DATI: FULL settimanale + differenziali della settimana in corso, con retention di 2 settimane per entrambi. In aggiunta, un backup FULL mensile con retention 6 mesi.

Lo spazio totale in backup messo a disposizione per i punti 1., 2. 3., è di 1211TB comprensivi di retention.

Lo spazio totale per il servizio di Golden Copy è 291TB.

Disaster Recovery
Il progetto include le risorse per il servizio di Disaster Recovery di due servizi critici dell'Amministrazione (Registri di monitoraggio e Farmacovigilanza). In base alle indicazioni fornite dall'Amministrazione si è stabilito che per ospitare gli applicativi inerenti a tali servizi siano sufficienti 8 Pool Large, che includono anche le risorse per allocare i servizi di sicurezza perimetrale e i PaaS DB Oracle (AIFA1 e AIFA2) che vengono interrogati dagli applicativi suddetti.

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

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

5.2.4.6 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 SECURE PUBLIC CLOUD

5.3.1 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.

5.3.2 Personalizzazione del servizio

I servizi e le relative infrastrutture sono stati forniti dal cliente, sotto una tabella cha rappresenta lo stato attuale del servizio Portale Istituzionale AIFA

Nome Server	Sistema Operativo	Utilizzo	Versione Prodotto	CPU	RAM
LEAIFAPORTAPP01	CentOs 7.9	Application Server	Liferay 7.0	32	32
LEAIFAPORTAPP02	CentOs 7.9	Application Server	Liferay 7.0	32	32
LEAIFAPORTDB01	CentOs 7.9	DB Server	MariaDB 10.3.17	4	8
LEAIFAPORTDB02	CentOs 7.9	DB Server	MariaDB 10.3.17	4	8
LEAIFAPORTELK1	CentOs 7.9	Application Server	Elasticsearch 6.8.0	4	16
LEAIFAPORTELK2	CentOs 7.9	Application Server	Elasticsearch 6.8.0	4	16
LEAIFAPORTELK3	CentOs 7.9	Application Server	Elasticsearch 6.8.0	4	16
LEAIFAPORTNFS	CentOs 7.9	Application Server		2	4
LEAIFAPORTWEB01	CentOs 7.9	Web Server	Apache 2.4.6	4	4
LEAIFAPORTWEB02	CentOs 7.9	Web Server	Apache 2.4.6	4	4
LEAIFAOSMEDELK1	CentOs 7.6	Application Web Server	Elasticsearch 7.5.1 Nginx 1.16.1 Kibana 7.5.1	2	8
LEAIFAOSMEDELK2	CentOs 7.6	Application Server	Elasticsearch 7.5.1	8	8
LEAIFAOSMEDELK3	CentOs 7.6	Application Server	Elasticsearch 7.5.1	8	8
LEAIFAETLBATCH1	CentOs 7	Application Server		2	6
Totale CPU: 114	**Totale RAM: 170 GB**			**Totale Storage: 2.120 GB**	

È stata proposta l'installazione delle macchine virtuali nuove sul SPC di Azure, e successivamente la migrazione applicativa.

Di seguito si riporta una tabella che riepiloga le tipologie e le quantità di VM ipotizzate

Servizio	Ambiente	VM SPC
Portale Web	Portale Istituzionale AIFA di Esercizio	2 CPU, 8GB RAM
Portale Web	Portale Istituzionale AIFA di Esercizio	2 CPU, 8GB RAM
Portale Web	Portale Istituzionale AIFA di Esercizio	2 CPU, 8GB RAM
Portale Web	Portale Istituzionale AIFA di Esercizio	2 CPU, 8GB RAM
Portale Web	Portale Istituzionale AIFA di Esercizio	2 CPU, 8GB RAM
Portale Web	Portale Istituzionale AIFA di Esercizio	2 CPU, 8GB RAM
Portale Web	Portale Istituzionale AIFA di Esercizio	2 CPU, 8GB RAM
Portale Web	Portale Istituzionale AIFA di Esercizio	2 CPU, 8GB RAM
Portale Web	Portale Istituzionale AIFA di Esercizio	2 CPU, 8GB RAM
Portale Web	Portale Istituzionale AIFA di Esercizio	2 CPU, 8GB RAM
Portale Web	Portale Istituzionale AIFA di Esercizio	4 CPU, 8GB RAM
Portale Web	Portale Istituzionale AIFA di Esercizio	4 CPU, 8GB RAM
Portale Web	Portale Istituzionale AIFA di Esercizio	4 CPU, 8GB RAM
Portale Web	Portale Istituzionale AIFA di Esercizio	4 CPU, 8GB RAM
Portale Web	Portale Istituzionale AIFA di Esercizio	4 CPU, 8GB RAM
Portale Web	Portale Istituzionale AIFA di Esercizio	4 CPU, 8GB RAM
Portale Web	Portale Istituzionale AIFA di Esercizio	4 CPU, 8GB RAM
Portale Web	Portale Istituzionale AIFA di Esercizio	4 CPU, 8GB RAM
Portale Web	Portale Istituzionale AIFA di Esercizio	4 CPU, 16GB RAM
Portale Web	Portale Istituzionale AIFA di Esercizio	4 CPU, 16GB RAM
Portale Web	Portale Istituzionale AIFA di Esercizio	4 CPU, 16GB RAM
Portale Web	Portale Istituzionale AIFA di Esercizio	4 CPU, 16GB RAM
Portale Web	Portale Istituzionale AIFA di Esercizio	4 CPU, 16GB RAM
Portale Web	Portale Istituzionale AIFA di Esercizio	4 CPU, 16GB RAM
Totale CPU: 76	**Totale RAM: 240 GB**	**Totale Storage: 6.144 GB**

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

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

5.3.4 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.

5.4 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.

5.4.1 Overview delle caratteristiche funzionali

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

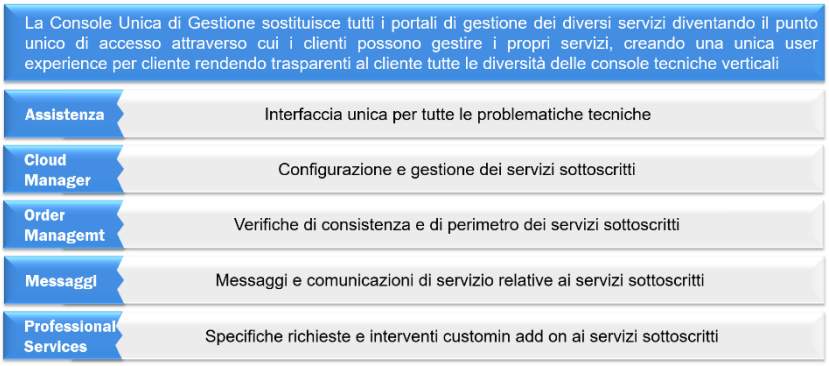


Figura 4 Funzionalità CU

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

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

2. Area Access Management e profilazione utenze. L'accesso alla CU è gestito totalmente dal sistema di Identity Access Management (IAM). Gli utenti, previa registrazione, saranno censiti nello IAM, e con le credenziali rilasciate potranno accedere dalla console alle risorse allocate all'interno del proprio tenant. Anche la creazione dei profili delle utenze e la loro associazione con gli account degli utenti sarà gestita tramite le funzionalità di IAM in un'apposita sezione della CU denominata "Gestione Utenze".
3. Area Design & Delivery. Attraverso tale modulo della CU, l'Amministrazione Contraente potrà configurare in autonomia i servizi acquistati secondo le metriche definite per la convenzione, costruendo, anche mediante l'utilizzo di un tool di visualizzazione, la propria architettura cloud sulla base delle risorse contrattualizzate. Successivamente la CU, interagendo in tempo reale attraverso le API dei servizi cloud verticali, consentirà l'immediata attivazione delle risorse e dei servizi previsti nell'architettura attraverso la creazione di uno o più tenant logici per segregare le risorse computazionali dei clienti (Project). Il processo è gestito mediante un workflow automatizzato di delivery implementato tramite l'uso di Blueprint. La CU esporrà anche delle API affinché la singola Amministrazione Contraente possa interagire attraverso i propri tools di CD/CI, IaC (Terraform, Ansible...) oppure attraverso una propria CU come ulteriore livello di astrazione e indipendenza (qualora ne avesse già a disposizione e quindi creare una CU Master Controller che interagisce con quella del PSN appunto via API).
4. Area Management & Monitoring. La piattaforma consentirà ai referenti delle Amministrazioni Contraenti di accedere alle funzionalità dedicate alla gestione e al monitoraggio delle risorse per ciascun servizio contrattualizzato e attivo all'interno delle specifiche piattaforme Cloud che erogano i servizi verticali. Punto focale della soluzione è la componente di Event Detection, che ha come obiettivo l'analisi dei log e degli eventi generati dalle piattaforme Cloud che erogano i servizi verticali per tutte le attività svolte dall'Amministrazione; tale modulo, in particolare, verificherà la compliance di tutte le richieste effettuate rispetto al perimetro contrattuale e bloccherà eventuali attività che esulino da tale contesto inviando alert, anche tramite e-mail, sia ai referenti della PA abilitati all'utilizzo della CU sia agli operatori delle strutture di Operations preposte alla gestione delle segnalazioni di anomalia sui servizi erogati.
5. Area Self Ticketing. Consente alla PA di segnalare in modalità self le anomalie riscontrate sui servizi cloud contrattualizzati.

5.4.2 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".

5.4.3 Interfaccia applicativa della Console Unica

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

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

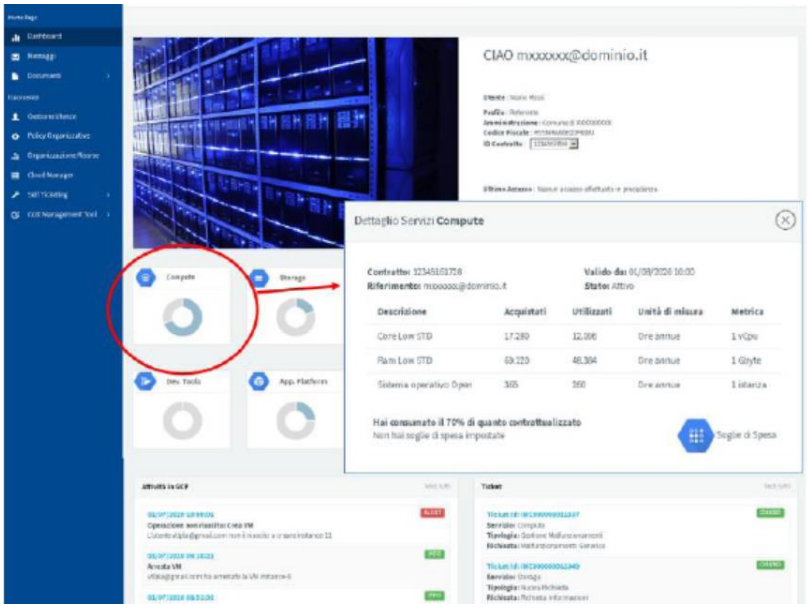


Figura 5 Dashboard CU

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

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

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

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

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

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

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

5.5 SERVIZI E PIANO DI MIGRAZIONE

Come già indicato in premessa AIFA migrerà verso il PSN tutti i sistemi applicativi attualmente installati presso i Data Center di TIM (ambiente di produzione) e Almaviva (ambiente di preproduzione) e il Portale Istituzionale ospitato presso i Data Center di Almaviva.

Il parco applicativo di AIFA è composto da 62 servizi di cui 2 critici e 60 ordinari. Attualmente molti applicativi custom dell'Amministrazione sono installati su macchine virtuali con sistemi operativi obsoleti e non dotati di supporto del vendor, non compliant alle direttive di sicurezza minime necessarie ad una infrastruttura per essere ospitate sul PSN.

AIFA ha condotto tramite un proprio fornitore uno studio sui sistemi che comporta due azioni:

- **Analisi di compatibilità tra SO Obsoleti AIFA e SO Target PSN:** Lo studio ha evidenziato che con Centos 8 e Red Hat Enterprise Linux 8 gli interventi di re-platforming sono esigui
- **Analisi Codice Sorgente Applicativi:** Lo scopo dello studio è stata l'individuazione di parti di codice su cui agire per ovviare i problemi di cambiamento del nuovo SO.

L'analisi di codice è stata poi estesa su ulteriori componenti/librerie richieste dai partner fornitori applicativi di AIFA (es. Mongo DB).

Sulla base di tale studio si è quindi stabilito uno scenario target di partenza che definisce in corrispondenza di ogni applicativo il SO operativo su cui sarà installato.

Qualora non sia possibile procedere al re-platforming dell'applicativo, e sarà quindi necessario migrare lo stesso su una versione di SO obsoleta, PSN non potrà certificare e quindi non potrà prendersi la responsabilità di garantire la certificazione di tali sistemi nella propria infrastruttura non avendo i requisiti di compatibilità con i servizi di Industry standard. In tal senso finché la PA, indirettamente e/o attraverso servizi di replatform PSN, non aggiornerà i propri Sistemi operativi, nonostante PSN erogherà i relativi servizi, PSN non potrà essere ritenuto responsabile su eventuali disservizi in termini di disponibilità (IQ 10) e presa in carico / risoluzione (IQ 16 e IQ17). Inoltre, PSN non potrà essere ritenuto responsabile di eventuali incident di sicurezza informatica derivanti dall'obsolescenza dei SO. Se ci fossero sistemi non compatibili con l'aggiornamento, l'effort stimato va comunque consuntivato. Se la macchina non sia tecnicamente migrabile, il relativo canone verrà escluso dalla consuntivazione annuale.

Il piano prevede tempi per la migrazione più brevi possibili in modo da permettere a PSN di garantire i livelli di qualità e di servizio attesi (entro 15 mesi).

Attualmente negli ambienti di produzione e preproduzione di AIFA è attiva una versione del DB Oracle (v.12) diversa dalla versione target installata sull'infrastruttura PaaS del PSN (v.19): ciò comporta la necessità di usufruire di servizi professioni di replatform per l'adeguamento dei DB Oracle alla versione disponibile su PSN. Anche questo elemento determina delle rielaborazioni sui sistemi di AIFA.

Inoltre, le dipendenze esistenti tra i vari programmi e i DB rendono complicata una migrazione a wave verso l'infrastruttura del PSN.

Si è quindi concordato con l'Amministrazione di procedere con un modello di migrazione che prevede:

i. Migrazione con Lift&Shift degli applicativi che non hanno dipendenze da altri e per i quali non è necessario procedere ad azioni di replatform
ii. Reinstallazione su VM con SO aggiornati degli applicativi che necessitano di azioni di replatform

iii. Migrazione con Lift&Shift o Replatform (per adattamento alla nuova versione del DB Oracle) + manleva da parte dell'Amministrazione per gli applicativi per i quali non è possibile procedere in questa fare alle azioni di replatform legati ai SO.

Resta inteso che, per tutti gli applicativi al punto 3) AIFA procederà al replatform o al rearchitect degli stessi secondo un piano condiviso con il PSN.

La migrazione di Applicazioni e Dati che si trovano ora presso i Data Center di Tim di Acilia e di Almaviva avverrà dall'attuale ambiente di produzione di AIFA presso il Data Center di Acilia di TIM verso l'infrastruttura Industry Standard del PSN sul Data Center che sarà definito in fase di avvio delivery.

La migrazione sarà costituita da 2 macro-fasi:

1) Implementazione del nuovo ambiente di preproduzione fino a collaudo
2) Implementazione del nuovo ambiente di produzione come copia dell'ambiente al punto 1)

Al termine delle attività al punto 2), AIFA dovrà procedere a uno stop delle attività sui vecchi ambienti di preproduzione e produzione in modo da permettere l'allineamento dati verso i nuovi ambienti. Al termine di esso si procederà con lo spegnimento dei vecchi ambienti e il go live sui nuovi.

Nella tabella di seguito si riporta la corrispondenza tra i sistemi dell'Amministrazione, la modalità della migrazione e il sistema operativo su cui si prevede sarà installato.

ID	NOME SISTEMA	Modalità di migrazione	SO
4	APCC	Replatform	Cent OS (ultima versione disponibile)
27	E-Dossier	Replatform	Cent OS (ultima versione disponibile)
48	NPR OLD	Replatform	RedHat (ultima versione disponibile)
47	NPR NEW	Replatform	OpenShift 4.1.0
33	GEFF	Replatform	OpenShift 4.1.0
65	Registri	Replatform	RHEL 8
85	WF Officine MED	Replatform con manleva per SO	CentOS RHEL 5
88	Wrapper Alfresco	Replatform	Openshift 4.10
89	Wrapper DocsPA	Replatform	Openshift 4.10
63	Portale Variazioni	Replatform	RHEL 8
84	WF Officine API	Replatform con manleva per SO	CentOS RHEL 5
97	WF Officine API NEW	Replatform	Openshift 4.10
79	SUBMISSION MANAGER	Replatform	Openshift 4.10
83	WF nuove AIC	Replatform	Openshift 4.10
50	Omeopatici	Replatform	RHEL 8
68	Rinnovi	Replatform	RHEL 8
86	Workflow Stampati NEW	Replatform	Openshift 4.10
45	NES	Replatform	Openshift 4.10
37	GSS	Replatform	Openshift 4.10
43	SPI Keycloak	L&S	OCP

ID	NOME SISTEMA	Modalità di migrazione	SO
35	Gestione Fondo 5%	L&S con manleva per SO	CentOS 7 (64-bit)
77	SGP - Sistema Gestione del Personale	Replatform con manleva per SO	CentOS 7 (64-bit)
66	Revoche e sospensioni	Replatform con manleva per SO	Red Hat Enterprise Linux 5 (64-bit)
71	RSO - Registri Studi Osservazionali	L&S con manleva per SO	CentOS 7 (64-bit)
13	SRI - Sistema Ricerca Indipendente	L&S	OCP
44	Libretto Formativo	L&S	OCP
40	Nuova Intranet	Replatform	OCP
78	SPENDING PHA	Replatform	OCP
3	Alfresco	L&S	RHEL 9
26	E4legal	L&S	RHEL 9
18	CERTO	L&S	RHEL 9
20	check&in	Replatform	Windows
22	CRP2G	L&S	RHEL 9
24	DOCSPA	Replatform	Windows
73	SAS(SAS9)	Trattasi di servizio SaaS	Trattasi di servizio SaaS
72	Conservazione TIM	Trattasi di servizio SaaS	Trattasi di servizio SaaS
54	OWNCLOUD	Replatform	Ubuntu 22.04 LTS
98	COLLABORA	Replatform	Ubuntu 22.04 LTS
80	Teletabber	L&S	Windows
15	BOOKING SYSTEM	L&S	Windows
1	ACC new	Replatform	RHEL 8
2	ACC old	Replatform	Windows
17	Carenze	Replatform	RHEL 8
25	DOI	Replatform	RHEL 8
31	FET	Replatform	RHEL 8
32	GDPR	L&S	RHEL 8
38	IMS	Replatform	RHEL 8
70	RNF	Replatform	RHEL 8
14	BDF	Replatform	OCP 4.x
34	Gestione Profili Utente	Replatform	OCP 4.x
8	AUA	Replatform	OCP 4.x
64	Registrazione Utente	Replatform	OCP 4.x
100	Primo accesso	Replatform	OCP 4.x
99	Approvatori AUA	Replatform	Ubuntu 22.04 LTS
39	Information Hub	Replatform	RHEL 8
52	OSSC	Replatform con manleva per SO	CentOS 7 (64-bit)
58	Pagamenti Online (POL)	Replatform	RHEL 8

ID	NOME SISTEMA	Modalità di migrazione	SO
60	Portale dei Servizi	Replatform	RHEL 8
91	Jiano	Replatform	RHEL 8
5	API GW	Replatform	OCP 4.x
10	Backend APP AIFA Medicinali	Replatform	OCP 4.x
21	Concessionari di vendita	Replatform	RHEL 8
76	Servizio Prima commercializzazione	Replatform	RHEL 8
11	Banca Dati Stampati FE NEW	Replatform	RHEL 8
49	Office241	L&S	Windows
90	vecchia banca dati	Replatform	Windows
23	CTS OLD	L&S	Windows
57	Piwik	L&S	Unix
9	Axway	L&S	Windows
61	Portale Istanze	L&S	OCP
101	Sistema di analisi farmacovigilanza (ETL + Elastic)	Replatform	RHEL 8
102	Server Infrastrutturali	L&S	RHEL 8
103	Scripts	L&S	RHEL 8
104	GIT	L&S	RHEL 8
105	ART50	L&S	RHEL 8
106	CESP	L&S	RHEL 8
107	EXTEDO	L&S	RHEL 8
108	JENKINS	L&S	OCP
109	NEXUS	L&S	OCP

Tabella 11 Modalità di migrazione dei sistemi AIFA

Quanto riportato in tabella è indicativo, qualora in fase di delivery di progetto fossero necessarie variazioni rispetto a quanto indicato le modifiche necessarie saranno concordate tra Amministrazione e PSN.

Il **Portale Istituzionale** sarà migrato dal Data Center di Almaviva all'ambiente Secure Public Cloud Microsoft Azure in modalità **Lift&Shift con manleva per SO**.

I servizi di Migrazione sono servizi Core del PSN quantificati e valutati economicamente sulla base di specifici assesment 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.

Data la particolarità del progetto e considerate le cospicue attività di re-platforming previste si è incluso nell'organizzazione di progetto un **Project Manager Applicativo**. Questa figura riporterà al Project Manager Contratto di Adesione e si occuperà di coordinare, monitorare e controllare le attività dei partner fornitori degli applicativi stessi.

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

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

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

- Analisi/Discovery
- Setup
- Migrazione
- Collaudo

Figura 6: Servizio di Migrazione - Metodologia EMG2C

2. 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) dei driver di transformation (e.g. ampliamento dei servizi, potenziamento della capacità di erogazione, ampliamento della geografia di riferimento)
b) dell'infrastruttura oggetto di transformation e della relativa composizione in termini di componenti infrastrutturali (Sistemi operativi, Database, Application Server, Web Server, Sistemi di Directory (tipicamente Active Directory), Sistemi di comunicazione (Posta, Messaging)
c) della Baseline di carico attraverso strumenti specifici (e.g. VMWARE Capacity Planner) per meglio indirizzare le risorse da allocare alla configurazione Finale
d) delle applicazioni erogate dalla PA con la definizione di una prima clusterizzazione delle stesse, che tenga conto delle dipendenze applicative, utile alla definizione di un piano di migrazione di dettaglio.
e) dei dati oggetto di migrazione;
f) degli SLA delle singole applicazioni;
g) di eventuali finestre utili per la migrazione;
h) di eventuali periodi di indisponibilità delle applicazioni;
i) del Cloud Maturity Model;
j) dell'analisi della sicurezza delle applicazioni e dell'ambiente da migrare;
k) di RPO e RTO preliminari (RPO e RTO di riferimento si intendono già noti al cliente) associati alle applicazioni di cui sopra
l) Energy Optimization
m) del modello di Operation AS-IS vs TO-BE con particolare riferimento alla successiva «esercibilità» del dominio applicativo e infrastrutturale oggetto di trasformazione

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 macro-definizione della strategia di migrazione, terrà in particolare riferimento le singole finestre temporali disponibili per la transformation e la definizione degli scenari Target:

- Identificazione dei perimetri di invarianza (ciò che viene solo mosso fisicamente senza cambiamenti di configurazione)
- Identificazione dei perimetri di trasformazione infrastrutturale (cambia l'infrastruttura ma non cambia la configurazione di sistemi operativi, middleware e applicativi) se non per gli adeguamenti infrastrutturali (i.e. indirizzamento, driver di accesso alle risorse…)
- Identificazione dei perimetri di trasformazione architetturale/applicativa (discontinuità a livello di Sistema Operativo, Middleware, Architettura Applicativa)
- Proposta di nuovo Assetto in Termini di Architettura Infrastrutturale
- Proposta di nuovo assetto in termini di Architettura Middleware
- Approvazione della architettura target da parte Cliente.

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 che prevede:

- Definizione degli Input Mandatori e della Matrice di Responsabilità per la fase di implementazione
- Progettazione di dettaglio della configurazione target in termini di Network, Risorse Storage, CPU, RAM;
- Progettazione di dettaglio di:
    - Piano di indirizzamento (AS IS vs TO BE);
    - Attestazione interfacce server layer 2 e 3;
    - Servizi di rete (DNS, WINS, NTP) e di autenticazione;
    - Servizi e protocolli applicativi;
    - Interconnessione con sistemi esterni;
    - Connettività (tra origine e destinazione durante migrazione);
- Per ogni Ambiente e per ogni Server definizione del piano specifico di migrazione (data/ora di inizio, modalità di conversione (Converter/Reinstallazione, Caldo/Fermo Macchina, Requisiti di allineamento dati, test preliminari di migrazione)
- Definizione delle modalità di funzionamento dei sistemi durante la trasformazione per poter attuare modalità di «transformation» incrementali o con approccio a «Big Ben»
- Definizione degli strumenti di supporto alla migrazione (connettività, hard disk, Network Attached Storage, Software di Replica e relative modalità di «seeding»)
- Predisposizione degli spazi per il setup e verifica della capacità di tutte le strutture (sistema di raffreddamento, rete elettrica, etc.) nel Data Center di Telecom Italia
- Per gli ambienti definiti critici, definizione di test funzionali e di benchmark prestazionali da effettuarsi prima e dopo la migrazione
- Progettazione di dettaglio delle architetture di Disaster Recovery e Business Continuity e relativa approvazione da parte Cliente.
- Ove necessario verranno reinstallati tutti i sistemi operativi nelle versioni e configurazioni indicate dai fornitori applicativi al momento della stesura del piano di migrazione

Per il corretto svolgimento delle fasi di Baseline, Definizione degli Scenari Target, Gestione dei Rischi dovranno essere considerati i seguenti input mandatori:

- Business Impact Analisys per i principali ambiti di trasformation
- Policy e Linee Guida di Security per Ambito
- Autorizzazione al trattamento dei Dati

- Per ogni ambito di Transformation:
- Identificazione di un Referente Infrastrutturale;
- Identificazione di un Referente Applicativo;
- Disponibilità ad Interviste dei principali referenti Infrastrutturali ed Applicativi;
- Documentazione di ambito Applicativo:
- Elenco delle principali applicazioni e processi supportati;
- Categorizzazione delle applicazioni in termini di importanza per il Business, RPO e RTO;
- Matrici Applicativi/Sistemi;
- Tipologia del Dato e Requisiti di Trattamento;
- Documentazione in ambito Infrastrutturale:
- Schemi Infrastrutturale per Applicazioni;
- Schemi di Rete;
- Dimensionamenti Server e Storage;
- Target prestazionali e condivisione di test prestazionali e funzionali da svolgersi pre e post migrazione
- Criticità prestazionali già note
- Disponibilità ad installare agenti o tool di raccolta dati di configurazione, di carico e di capacità
- Account di Audit (sola lettura) sulla configurazione dei Sistemi Operativi e Middleware

La fase di Analisi e discovery per il Portale Istituzionale consiste nella esecuzione delle attività di assesment dei sistemi e delle applicazioni Portale e OSMED coinvolte nella migrazione per confermare il mapping dei sistemi e la baseline delle applicazioni. Si effettua l'analisi delle dipendenze e delle priorità per la migrazione, la verifica servizi PAAS e loro uso per la relocation del portale. Si procede con la progettazione delle modalità operative per la migrazione lift & shift delle applicazioni coinvolte e la strategia per il trasferimento del contenuto della base dati sia per l'esecuzione dei test e del collaudo sia per lo switch on-off in produzione. Si stabiliscono gli intervalli di indisponibilità dei servizi agli utenti e la tempistica degli avvisi da dare agli utenti. Si definisce il piano di dettaglio considerando il vincolo temporale legato alla pubblicazione dei dati OSMED 2022.

Ulteriori Input mandatori per la fase di implementazione saranno definiti durante le fasi di progetto.

3. 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 il DC di Acilia e i DC del PSN

4. Migrazione

Tale fase si articola di solito 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.

Nello specifico per le componenti Industry Standard la linea guida scelta nella risposta prevede le seguenti scelte, non vincolanti:

- Reinstallazione della componente database;
- Valutazione caso per caso delle componenti Application Server;
- Reinstallazione di eventuali Domain Controller;
- Virtualizzazione come via prevalente negli altri casi;

Al fine di minimizzare i rischi di progetto e redigere il piano di migrazione temporale definitivo per ogni ambiente e per ogni server verrà condotto un Test di migrazione che consentirà di valutare per ogni singola macchina:

- L'effettivo successo della operazione di P2V o la corretta reinstallazione delle componenti middleware ed applicative;
- Le prestazioni nel nuovo ambiente virtuale;
- Le modalità di allineamento (con particolare riferimento alle modalità di allineamento tramite export/import dati dei database e di eventuali directory o file system);

Durante tutta la durata della migrazione la coesistenza in data center garantirà la visibilità tra gli ambienti sorgente e destinazione della migrazione in modo da poter condurre efficaci e completi test di migrazione. La connettività consentirà una migrazione progressiva degli ambienti. Per ogni ambiente potranno essere previste le seguenti attività, in funzione della tipologia e della criticità dell'ambiente stesso:

- Conversione / re installazione;
- Test ambiente;
- Test di migrazione dati;
- Test ambiente con dati migrati;
- Pianificazione migrazione;
- Migrazione;
- Le attività di Test sopra indicate potranno già essere svolte nelle fasi antecedenti il moving.

Al termine e/o durante la migrazione, con modalità concordate con il cliente, saranno condotti i test di alta affidabilità e vMotion dell'infrastruttura.

La migrazione farà, inoltre, uso di tecnologie di replica incrementale delle singole Virtual Machine. Si ipotizza l'utilizzo di Veeam o Zerto per poter effettuare la replica delle singole macchine tra sorgente e destinazione, in modo da poter minimizzare i tempi di fermo delle singole Virtual Machine. Tale tecnologia consentirà la migrazione incrementale delle macchine Virtuali con bassi RPO (ordine di decine di minuti) minimizzando i tempi di fermo delle macchine oggetto di migrazione. Le macchine potranno essere raggruppate in modo da poter essere migrate mantenendo l'allineamento temporale tra le singole macchine del gruppo.

La fase di migrazione del Portale Istituzionale si articola nelle azioni necessarie per la predisposizione degli ambienti di pre-esercizio ed esercizio costituite da:

- porting del middleware

- supporto alla configurazione delle applicazioni Portale e OSMED
- porting base dati (struttura e contenuto) applicando la strategia definita nella fase precedente
- supporto per la definizione delle regole di bilanciamento
- supporto per la definizione delle regole firewall
- supporto per la modifica dei dns interni

5. **Collaudo**

Definizione Strategia di Collaudo: tale fase è finalizzata alla predisposizione della strategia ottimale di collaudo delle applicazioni migrate nell'ambiente target. Per ogni servizio migrato o reinstallato ex-novo sarà redatto e condiviso con il committente un piano di collaudo. Complessivamente sarà redatto un documento che conterrà l'esito delle seguenti attività:

- Validazione dei requisiti di sistema: Verifica che le VM siano state migrate correttamente nel cloud e che soddisfino i requisiti di sistema specifici, inclusi i requisiti di risorse, versioni del sistema operativo e configurazioni di rete.
- Test delle funzionalità di base: Assicurarsi che le funzionalità di base delle VM siano operative. Questo potrebbe includere test di accensione e spegnimento delle VM, accesso remoto, aggiornamenti del sistema operativo e altre funzionalità chiave.
- Test di rete e connettività: Verificare che le VM siano correttamente collegate alla rete e che abbiano accesso alle risorse e ai servizi necessari. Testare la connettività tra le VM e altri componenti del sistema, come database o applicazioni.
- Test delle prestazioni: Valutare le prestazioni delle VM nel nuovo ambiente cloud. Misurare i tempi di risposta, il throughput e l'utilizzo delle risorse per assicurarsi che le VM funzionino in modo efficiente e soddisfino le aspettative.
- Test di backup e ripristino: Assicurarsi che i processi di backup e ripristino siano funzionanti. Verificare la possibilità di ripristinare le VM in caso di emergenza o perdita di dati.
- Test funzionali delle applicazioni ritenute critiche, con una copertura funzionale rappresentativa delle operazioni oggi condotte con maggiore frequenza o maggiormente critiche, ed una copertura il più possibile completa delle funzionalità che potrebbero essere maggiormente impattate dal cambio

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. >

5.5.1 Piano di attivazione e Gantt

In questa sezione si riporta un diagramma di Gantt di massima per le attività previste nel progetto. Il diagramma tiene conto della modalità di migrazione scelta per sistema e indicata nella Tab.11, nonché delle dipendenze e interazioni esistenti tra i vari applicativi attualmente installati sul Data Center di TIM Acilia. A tal proposito i sistemi di AIFA attualmente installati sul Data Center di TIM di Acilia sono stati divisi in gruppi di priorità di migrazione (Gruppo di priorità =0, gruppo a maggiore priorità) in modo da poter meglio valutare le tempistiche di progetto. Il piano proposto è un piano di massima che sarà meglio dettagliato nella fase di analisi e discovery.

ID	NOME SISTEMA	Gruppo di migrazione
4	APCC	3

ID	NOME SISTEMA	Gruppo di migrazione
27	E-Dossier	3
48	NPR OLD	4
47	NPR NEW	5
33	GEFF	5
65	Registri	4
85	WF Officine MED	4
88	Wrapper Alfresco	2+
89	Wrapper DocsPA	2+
63	Portale Variazioni	4
84	WF Officine API	4
97	WF Officine API NEW	5
79	SUBMISSION MANAGER	4
83	WF nuove AIC	5
50	Omeopatici	4
68	Rinnovi	4
86	Workflow Stampati NEW	5
45	NES	2
37	GSS	5
43	SPI Keycloak	1
35	Gestione Fondo 5%	4
77	SGP - Sistema Gestione del Personale	2
66	Revoche e sospensioni	4
71	RSO - Registri Studi Osservazionali	4
13	SRI - Sistema Ricerca Indipendente	5
44	Libretto Formativo	5
40	Nuova Intranet	5
78	SPENDING PHA	5
3	Alfresco	2
26	E4legal	4
18	CERTO	4
20	check&in	2
22	CRP2G	2
24	DOCSPA	2
73	SAS(SAS9)	4
72	Conservazione TIM	4
54	OWNCLOUD	4
98	COLLABORA	4
80	Teletabber	4
15	BOOKING SYSTEM	4

ID	NOME SISTEMA	Gruppo di migrazione
1	ACC new	3
2	ACC old	3
17	Carenze	2+
25	DOI	2+
31	FET	2+
32	GDPR	2+
38	IMS	2+
70	RNF	2+
14	BDF	2
34	Gestione Profili Utente	1
8	AUA	1
64	Registrazione Utente	1
100	Primo accesso	1
99	Approvatori AUA	1
39	Information Hub	2
52	OSSC	3
58	Pagamenti Online (POL)	3
60	Portale dei Servizi	0
91	Jiano	0
5	API GW	0
10	Backend APP AIFA Medicinali	5
21	Concessionari di vendita	5
76	Servizio Prima commercializzazione	5
11	Banca Dati Stampati FE NEW	5
49	Office241	1
90	vecchia banca dati	1
23	CTS OLD	1
57	Piwik	1
9	Axway	0
61	Portale Istanze	5
101	Sistema di analisi farmacovigilanza (ETL + Elastic)	4
102	Server Infrastrutturali	0
103	Scripts	0
104	GIT	0
105	ART50	0
106	CESP	0
107	EXTEDO	0
108	JENKINS	0
109	NEXUS	0

Tabella 12 Divisione applicativi AIFA in gruppi di migrazione

Si riporta di seguito il Gantt di migrazione dei sistemi attualmente installati presso il Data Center TIM di Acilia

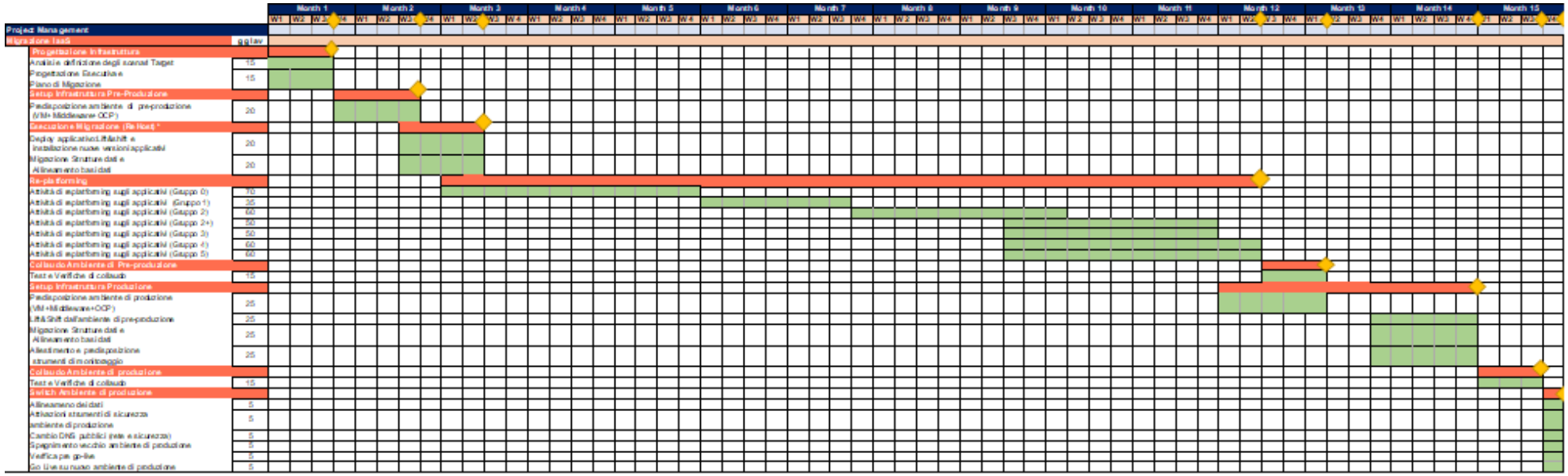


Figura 7 Gantt migrazione sistemi Data Center TIM

n parallelo alle attività sopra descritte verrà gestita la migrazione del Portale Istituzione dal Data Center di Almaviva al Secure Public Cloud Microsoft Azure. Si riporta di seguito il Gantt di tali attività, in modalità separata dal precedente per una maggiore semplicità di lettura.

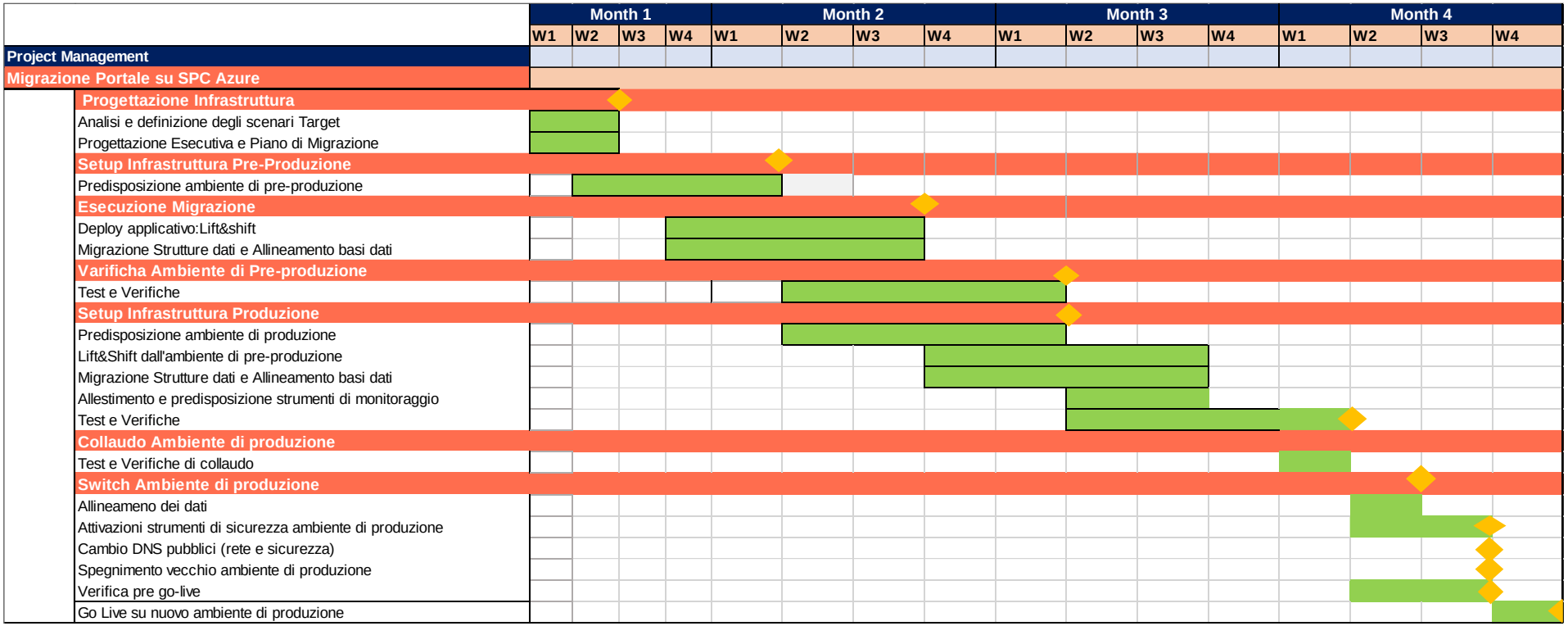


Figura 8 Gantt migrazione Portale Isituzionale

5.6 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.

5.6.1 Re-platform

La strategia di Re-platform oltre a trasferire un applicativo sul cloud come avviene nel re-host, sostituisce nel processo di migrazione alcune componenti per meglio sfruttare le specificità della piattaforma di destinazione. La finalità principale della strategia è di trasferire l'applicativo in cloud senza stravolgimenti funzionali, analizzando i possibili interventi che consentono di cogliere, rispetto ai benefici garantiti da una soluzione cloud-native, il livello massimo di ottimizzazione e beneficio. Gli interventi si concentrano sul cambio di SO/DB, Software Update, DB Update con l'obiettivo di standardizzare le componenti infrastrutturali e permetterne una più semplice gestione di configurazione. Il servizio può rendersi necessario qualora il livello di sicurezza non sia conforme allo standard minimo; pertanto realizza la modifica di componenti specifici di un'applicazione verso sistemi IaaS e PaaS erogati dal PSN al fine di migliorarne la scalabilità ma soprattutto la sicurezza.
Di seguito vengono illustrati i diversi step del processo di Re-platform:

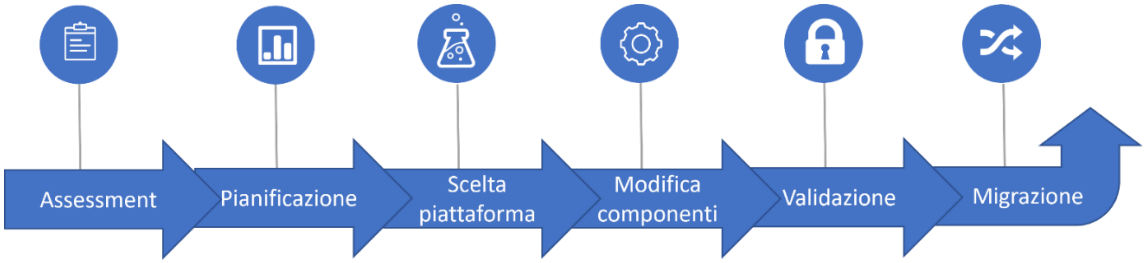


Figura 9: Flusso processo di Re-platform

5.6.1.1 Personalizzazione del servizio

Si prevede il replaform, con aggiornamento dei sistemi operativi obsoleti, middleware e database con relativo supporto applicativo all'installazione e configurazione delle componenti aggiornate per le applicazioni di seguito elencate.

APCC

- reinstallazione completa dell'attuale architettura APCC;
- upgrade della versione del DB Oracle;
- analisi sistemi operativi e aggiornamento Cent OS, Tomcat e jdk;
- Esecuzione test applicativi.

E-Dossier

- reinstallazione completa dell'attuale architettura E-Dossier;
- upgrade della versione del DB Oracle;
- analisi sistemi operativi e aggiornamento Cent OS, Tomcat e jdk;
- Esecuzione test applicativi.

NPR OLD

- reinstallazione completa dell'attuale architettura NPR OLD;
- upgrade della versione del DB Oracle;
- analisi sistemi operativi e aggiornamento RedHat all'ultima release disponibile, Jboss 7.x e jdk;
- Esecuzione test applicativi.

NPR NEW

- reinstallazione completa dell'attuale architettura NPR NEW;
- upgrade della versione del DB Oracle;
- replatform applicazione su OpenShift 4.1.0, aggiornamento jdk;
- Esecuzione test applicativi.

GEFF

- reinstallazione completa dell'attuale architettura GEFF;
- upgrade della versione del DB Oracle;
- replatform applicazione su OpenShift 4.1.0, aggiornamento jdk;
- Esecuzione test applicativi.

REGISTRI

In prima fase è previsto un passaggio del sistema su SO RHEL 8 e Middleware (Jboss EAP 6.4 e JDK 1.8 come da indicazioni dello studio commissionato da AIFA) e subito dopo procedere con il refactoring isofunzionale con successiva installazione su Openshift (re-factoring non previsto in questa stima)

WF Officine MED

In prima fase passaggio del sistema con le attuali versioni di SO (RH Centos) e Middleware (Jboss 4.2 e JDK 1.6) nelle more di procedere con il re-factoring del sistema. Successivamente, dopo la chiusura di tutte le pratiche aperte si procederà con la predisposizione di funzionalità di consultazione dello storico sul nuovo sistema installato in Openshift (re-factoring non previsto in questa stima)

Wrapper Alfresco

- Installazione su Openshift 4.10,
- Esecuzione test applicativi.

Wrapper DocsPA

- Installazione su Openshift 4.10,
- Esecuzione test applicativi.

Portale Variazioni

In prima fase passaggio del sistema su RHEL 8 e Middleware (Jboss EOP 6.4 e JDK 1.8 come da indicazioni dello studio commissionato da AIFA) nelle more di procedere con un re-factoring del sistema a microservizi su Openshift.(refactoring non previsto in questa stima)

WF Officine API

Si consiglia in prima fase un passaggio del sistema con le attuali versioni di SO (Centos) e Middleware (Jboss 4.2 e JDK 1.6) nelle more dell'avvio a regime del nuovo sistema già implementato su Openshift.

Successivamente, dopo la chiusura di tutte le pratiche aperte si procederà con la predisposizione di funzionalità di consultazione dello storico sul nuovo sistema installato in Openshift (re-factoring non previsto in questa stima)

WF Officine API NEW

- Installazione su Openshift 4.10,
- Esecuzione test applicativi.

SUBMISSION MANAGER

- Installazione su Openshift 4.10,
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

WF nuove AIC

- Installazione su Openshift 4.10,
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

Omeopatici

Passaggio del sistema su RHEL 8 e Middleware (Jboss EOP 6.4 e JDK 1.8 come da indicazioni dello studio commissionato da AIFA) e successivamente mettere a piano un re-factoring (re-factoring non previsto in questa stima)

Rinnovi

Passaggio del sistema su RHEL 8 e Middleware (Jboss EOP 6.4 e JDK 1.8 come da indicazioni dello studio commissionato da AIFA) e successivamente mettere a piano un re-factoring (re-factoring non previsto in questa stima)

Workflow Stampati NEW

- Installazione su Openshift 4.10,
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

NES

- Installazione su Openshift 4.10,
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

GSS

- Installazione su Openshift 4.10,
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

SUBMISSION MANAGER

- Installazione su Openshift 4.10,
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

SGP - Sistema Gestione del Personale

- reinstallazione completa dell'attuale architettura SGP;
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

Revoche e sospensioni

- reinstallazione completa dell'attuale architettura Revoche e Sospensioni;
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

Nuova Intranet

- reinstallazione completa dell'attuale architettura Nuova Intranet;
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

SPENDING PHA

- reinstallazione completa dell'attuale architettura Spending PHA;
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

Check&In

- reinstallazione completa dell'attuale architettura Check&IN;
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

DOCSPA

- reinstallazione completa dell'attuale architettura DOCSPA;
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

OWNCLOUD

- reinstallazione completa dell'attuale architettura OWNCLOUD;
- replatform alla versione SO Ubuntu 22.04 LTS;
- Esecuzione test applicativi.

COLLABORA

- reinstallazione completa dell'attuale architettura COLLABORA;
- replatform alla versione SO Ubuntu 22.04 LTS;
- Esecuzione test applicativi.

ACC new

Il porting dell'applicativo sarà gestito in modalità mista. Il BE è portato sull'ambiente PSN in modalità Lif& Shift secondo le indicazioni di compatibilità proposte e garantite dallo studio condotto da AIFA con attività di mitigazione di piccoli problemi. Qualora si presentassero problematiche di grande rilevanza che prevedono una modifica significativa dell'applicativo si dovrà considerare un progetto di manutenzione adeguativa non compreso in questa stima.

I flussi attualmente sul wso2 bps saranno re-architettati con un altro strumento e l'applicativo sarà evoluto per recepire le modifiche

ACC old

- reinstallazione completa dell'attuale architettura ACC OLD;
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

Carenze

- reinstallazione completa dell'attuale architettura Carenze;
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

DOI

- reinstallazione completa dell'attuale architettura DOI;
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

FET

- reinstallazione completa dell'attuale architettura FET
- upgrade della versione del DB Oracle;

- Esecuzione test applicativi.

IMS

- reinstallazione completa dell'attuale architettura IMS
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

RNF

- reinstallazione completa dell'attuale architettura RNF
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

BDF

- reinstallazione completa dell'attuale architettura BDF
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

Gestione Profili Utente

- reinstallazione completa dell'attuale architettura Gestione Profilo Utente
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

AUA

- reinstallazione completa dell'attuale architettura AUA
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

Registrazione Utente

- reinstallazione completa dell'attuale architettura Registrazione Utente
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

Primo accesso

- reinstallazione completa dell'attuale architettura Primo Accesso
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

Approvatori AUA

- reinstallazione completa dell'attuale architettura Approvatori AUA
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

Information Hub

Il message broker 3.2.0 sarà sostituito da un altro strumento modificando contestualmente il flusso di Nifi. L'attività può generare un impatto sull'applicazione Spending PHA . Saranno fornite le indicazioni per trattarli.

OSSC

Il componente wso2bps ha raggiunto la sua fine di vita ed è stato ritirato dal produttore. È possibile migrarlo attraverso una strategia di replatform su container o con L&S. Entrambe le soluzioni non permettono interventi di adeguamento e patching di sicurezza sul prodotto.
Per quel che riguarda il Mongo DB verrà portato in versione 3.4 secondo la compatibilità garantita da studio condotto da AIFA.

Pagamenti Online (POL)

L'eventuale L&S si riferisce al componente liferay Community Edition 6.2. È prevista la reinstallazione completa di tutte le componenti custom sviluppate in precedenza senza upgrade della versione di Liferay, secondo le indicazioni di compatibilità proposte e garantite da Red Hat, con attività di

mitigazione di piccoli problemi. Non si prevede di effettuare modifiche su librerie core né custom. Qualora si presentassero problematiche che prevedono una modifica dell'applicativo si dovrà considerare un progetto di manutenzione adeguativa non compreso in questa stima. Non sarà prodotta documentazione. Sarà condotto comunque replatform per la variazione della versione di Oracle

Portale dei Servizi

Si prevede un'attività di Re-architect per la gestione del caching distribuito per le response e per l'implementazione dell'HA tra i due nodi dell'AS di BE attualmente attuati tramite il componente Hazelcast. In questo contesto è anche adeguato il pacchetto dei servizi di abilitazione. Si prevede la containerizzazione del servizio Scriba utilizzato per il colloquio con Mongo DB da alcuni applicativi del Portale.

Verrà effettuato un intervento di Lift & optimize per il middleware Portal Service. Le attività potranno avere dei piccoli impatti su alcune applicazioni del Portale dei servizi migrate con Lift & Optimize.

Le attività possono generare piccoli impatti anche sulle applicazioni del Portale dei Servizi in carico ad altro fornitore applicativo. Tali impatti saranno identificati e fornite le indicazioni per trattarli.

Jiano

È prevista la reinstallazione di tutte le componenti Jiano secondo le indicazioni di compatibilità proposte e garantite dallo studio condotto da AIFA, con attività di mitigazione di piccoli problemi. Qualora si presentassero problematiche di grande rilevanza che prevedono una modifica significativa dell'applicativo si dovrà considerare un progetto di manutenzione adeguativa non compreso in questa stima.

API GW

È prevista la completa ri-configurazione del WSO2. Il presupposto è che i progetti siano migrati automaticamente. L'installazione manuale dei singoli servizi non è compresa nell'effort. E' previsto l'adeguamento per la variazione della versione del DB Oracle.

Backend APP AIFA Medicinali

- reinstallazione completa dell'attuale architettura Backend APP AIFA Medicinali
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

Concessionari di vendita

- reinstallazione completa dell'attuale architettura Concessionari di vendita
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

Servizio Prima commercializzazione

- reinstallazione completa dell'attuale architettura Concessionari di vendita
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

Banca Dati Stampati FE NEW

- reinstallazione completa dell'attuale architettura Banca Dati Stampati FE NEW
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

Vecchia Banca Dati

- reinstallazione completa dell'attuale architettura Vecchia Banca Dati
- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

Sistema di analisi farmacovigilanza (ETL + Elastic)

- reinstallazione completa dell'attuale architettura Sistema di analisi farmacovigilanza (ETL + Elastic)

- upgrade della versione del DB Oracle;
- Esecuzione test applicativi.

5.6.2 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

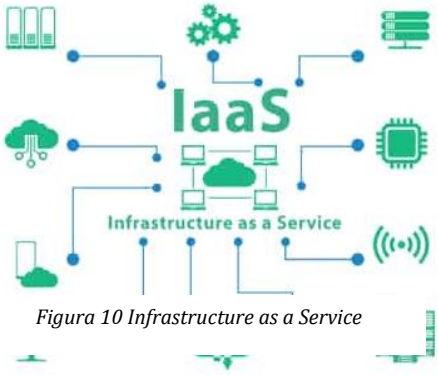


Figura 10 Infrastructure as a Service

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.

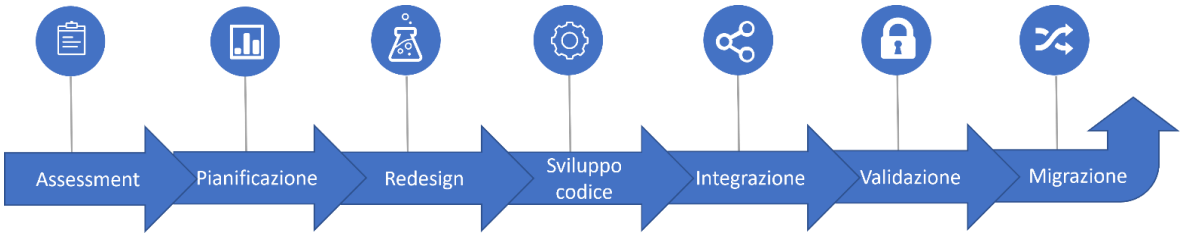


Figura 11: Flusso processo di Re-architect

Polo Strategico Nazionale garantisce che, rispetto alle componenti applicative in ambito oggetto di re-architect, verranno identificate, documentate e risolte eventuali vulnerabilità di sicurezza in coerenza con le linee guida e misure tecniche/organizzative relative allo sviluppo sicuro del software adottato da PSN e dalla PA.

La garanzia di risoluzione delle predette vulnerabilità verrà accertata e comunicata al cliente attraverso l'esecuzione di un'attività di verifica (ad es. penetration test e vulnerability assessment) eseguita prima della messa in esercizio delle componenti oggetto dei servizi di re-architect, nel rispetto delle tempistiche concordate.

5.6.3 Security Profess. Services

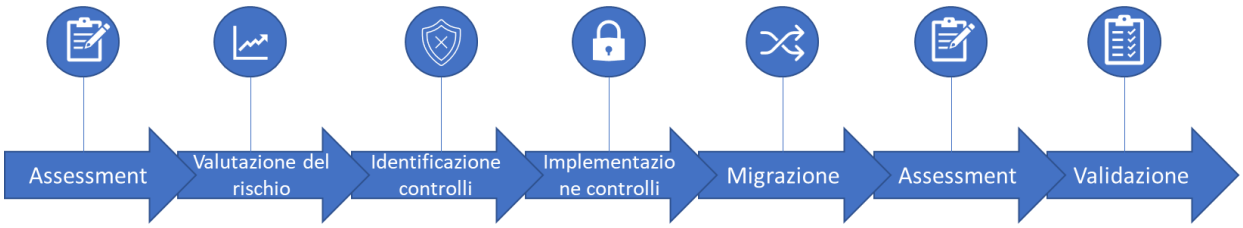
La migrazione su cloud è un processo complesso e un cambiamento rilevante che non va preso alla leggera. Non esiste una procedura di migrazione immediata sul cloud, e anzi spesso i rischi di migrazione stessi non vengono opportunamente valutati con il risultato che un'attività di migrazione che dovrebbe 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



5.6.3.1 Personalizzazione del servizio

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

- ICT Info gathering/Cyber Assessment
- Maturity Level Assessment

- Vulnerability Assessment (fino a 300 IP)

Questi servizi si definiscono Servizi security core pre-migrazione e saranno descritti nel paragrafo 5.6.3.2.

Inoltre, saranno attivati in accordo con l'Amministrazione i seguenti servizi professionali di sicurezza che completano l'offerta e garantiscono il mantenimento dei livelli di sicurezza nel tempo, tenendo conto delle fasi del progetto di migrazione:

- Servizio di Security By Design in funzione della gap-analysis e dei controlli di sicurezza indirizzati alla protezione della rete, dei servizi e degli endpoint;
- Servizio di supporto per attività di Security Device Management (Protezione Perimetrale - AzureFW, AppGW, NGFW, SWG);
- Security Event Monitoring, Notification & Log Management;
- Supporto per l'erogazione del servizio di Managed Detection & Response;
- Cyber Threat Intelligence: Early Warning and Data Breach;
- Compliance Assessment Framework Nazionale Cyber Security (FNSC);
- Vulnerability Assessment, Research & Exploitation;

Dal secondo anno saranno attivati i seguenti servizi:

- Security Policy Review/Advisory
- Gestione degli Incidenti di Sicurezza e Crisis Management.

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

- Servizi "a task":

o Servizi security core pre-migrazione (§5.6.3.2);

o Servizi professionali per il miglioramento della sicurezza delle infrastrutture e delle applicazioni della PA (ovvero, i Security Professional Services descritti ai paragrafi 5.6.3.3, 5.6.3.8, 5.6.3.10, 5.6.3.11, 5.6.3.12, 5.6.3.15, 5.6.3.18, 5.6.3.20, 5.6.3.21

- Servizi" Ricorrenti": Servizi di supporto device management protezione perimetrale (ovvero i Security Professional Services descritti ai paragrafi 5.6.3.4, 5.6.3.6, 5.6.3.7, 5.6.3.9).

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

- eseguirà un'analisi dei requisiti;
- definirà lo skill Mix necessario all'esecuzione;

- valuterà il dimensionamento in termini di effort per singola figura professionale ed in termini di valore economico corrispondente;
- comunicherà all'Amministrazione il risultato della propria analisi e valutazione.

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

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

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

5.6.3.2 Servizi core pre-migrazione

CORE-ICT Info gathering/Cyber Assessment

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

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

CORE-Maturity Level Assessment

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

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

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

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

CORE-Vulnerability Assessment (300 IP)

Il servizio consente la verifica della sicurezza dei sistemi, servizi ed applicazioni incluse nel perimetro di analisi (AS-IS massimo 300 IP) allo scopo di identificare eventuali vulnerabilità, configurazioni di sicurezza errate, carenze sui livelli di protezione attivi che espongano il contesto ad attacchi esterni. L'analisi si conclude con la condivisione di **un report di dettaglio** in cui verranno considerate tutte le criticità emerse durante la fase di analisi.
L'attività svolta in fase di start-up dovrà essere ripetuta durante l'intera fase di esercizio, in ottica di mantenimento dei livelli di sicurezza richiesti miglioramento continuo con le modalità meglio indicate nel paragrafo 5.6.3.7

5.6.3.3 Servizio di Security By Design in funzione della gap-analysis e dei controlli di sicurezza indirizzati alla protezione della rete, dei servizi e degli endpoint

Il servizio consiste nella predisposizione di un team di specialisti con le competenze e l'esperienza necessarie ad effettuare l'attività di supporto al design ed implementazione della protezione perimetrale oggetto di migrazione al fine di incrementarne il livello di sicurezza. Tale servizio, erogato durante la fase di setup della migrazione, prevede un'analisi preliminare volta a comprendere le tecnologie utilizzate e le specifiche caratteristiche al fine di poter predisporre le opportune linee guida o best practice in ambito security by design secondo una metodologia articolata in tre step di seguito descritti:

- Step 1 – Analisi preliminare: In questa fase verrà eseguita un'analisi preliminare dello scenario proposto, svolgendo le seguenti attività:
  - raccolta delle informazioni sulle tecnologie utilizzate dall'Amministrazione contraente;
  - analisi del contesto specifico e classificazione del rischio Cyber sulla base dei livelli di criticità dei servizi a cui sono associate le specifiche tecnologie in esame;
  - analisi degli impatti di indisponibilità dei servizi, per l'individuazione delle aree problematiche e contromisure tecnologiche da adottare.
- Step 2 – Disegno delle linee guida di security by design: In questa fase verranno identificate le linee guida di security by design, propedeutica alla fase di progettazione, svolgendo le seguenti attività:
  - predisposizione delle linee guida di security by design (sulla base della classificazione delle tecnologie fatta nella fase di assessment);
  - ipotesi di progettazione dell'infrastruttura sulla base delle contromisure suggerite;
  - condivisione della documentazione predisposta ai referenti coinvolti.
- Step 3 – Fase implementativa di Delivery e migrazione soluzioni esistenti: in questa fase verranno condotte le attività di predisposizione delle nuove soluzioni perimetrali WAF nonché il refining/migrazione dell'attuale soluzione perimetrale esistente NGFW sulla nuova infrastruttura Cloud.

I deliverable prodotti consistono in attività operative secondo quanto di seguito rappresentato in ottica di definire una mappatura tra servizi, tecnologie e contromisure.

Il servizio viene offerto il primo anno come supporto alla migrazione e gli anni successivi, in veste di servizio avanzato, nell'ottica del miglioramento continuo della postura di sicurezza.

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

Il servizio professionale richiesto è orientato a supportare l'Amministrazione nella gestione e nel monitoraggio continuativo delle piattaforme di protezione perimetrale previste sulla nuova infrastruttura ICT. Il servizio è erogato "as a service" remotamente ed include la gestione degli apparati e servizi di protezione perimetrale (per un totale massimo di qtà 8 apparati virtuali e 2 servizi PaaS Azure) con una finestra di servizio H8x5 e prevede:

- Definizione del perimetro di servizio: definizione della baseline dei sistemi di sicurezza che saranno oggetto del servizio Security Device Management;
- Definizione delle politiche di sicurezza: un' analisi globale dell' infrastruttura dei sistemi di sicurezza oggetto del servizio; lo scopo è quello di analizzare l' as-is della configurazione dei firewall, delle policy già configurare e dell' architettura complessiva nella quale i firewall sono posizionati
- Presa in carico dei sistemi, in RW, nello specifico le attività di presa in carico prevedono:
  - pianificazione temporale delle attività;
  - completa raggiungibilità dei devices e delle relative piattaforme di management ove presenti;
  - configurazione di utenze nominali per gli specialisti del SOC;
- Gestione a regime:
  - ogni richiesta viene validata ed implementata secondo le best practice di sicurezza ed in conformità a quanto definito con il Cliente in relazione anche alle policy aziendali vigenti.
  - i change, ad esempio, possono riguardare aggiunta/rimozione/modifica di policy firewall, creazioni tunnel vpn, modifica routing, /creazione/modifica profili UTM etc

Il servizio prevede l'impiego di soluzioni di sicurezza virtuali come di seguito rappresentato:

- qty 4 v_NGFW (32 v_cpu, 64 gb RAM, 500 GB Storage)
- qty 4 v_WAF (8 v_cpu, 16 GB Ram, 500 GB Storage)

5.6.3.5 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, 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 sui differenti contesti Cloud offerti (IaaS Industry Standard e Secure Public Cloud) contestualmente ai servizi infrastrutturali e, grazie a sistemi di indicizzazione e correlazione evoluti, fornisce il monitoraggio continuo degli eventi di sicurezza generati dalle componenti di sicurezza previste nel perimetro di gestione del Secure Device Management. Il servizio è progettato per identificare rapidamente risorse o eventi potenzialmente dannosi, anticipando tempestivamente i potenziali attacchi informatici o tentativi di attacco.

Il servizio, erogato in modalità H7x24 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 email o caselle di posta compromessi
- Il nome e la tipologia del malware usato nell'attacco
- La vulnerabilità sfruttata e/o l'exploit utilizzato
- I riferimenti temporali dell'accaduto
- Lo stato del traffico e/o dell'azione (e.g. bloccato/non bloccato/non noto)

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

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

Si propone a titolo di esempio la seguente matrice:

INCIDENT PRIORITY LEVELS	IMPACT (Asset)		
	Low	Medium	High

SEVERITY (Attack)				
	Low	Low	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	High

Tabella 1 – 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 2 – 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.

Processo di Analisi ed Incident Notification

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

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

Reporting

Il servizio produce due tipologie di report:

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

Continuous Improvement

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

5.6.3.6 Servizio di supporto per l'erogazione del servizio di Managed Detection & Response

Il servizio è erogato remotamente e non include le licenze degli agent EDR, la cui distribuzione ed installazione è da attivare a carico del cliente e quindi non oggetto del presente servizio.

La gestione centralizzata della soluzione viene fatta attraverso una piattaforma di management presente su cloud. Tale piattaforma di fatto raccoglie tutte le informazioni di telemetria (metadati) inoltrate dagli agent installati sugli endpoint dell'Amministrazione tramite opportuno collegamento Internet, di cui è richiesta la visibilità continuativa (tra agent e piattaforma di management) in carico all'infrastruttura di accesso Internet del cliente. Il servizio è erogato as a service ed include un monitoraggio continuativo con finestra di servizio H24 per 365 giorni con notifica degli eventi ritenuti di interesse per un numero massimo di 1000 hosts.

Il modello di servizio consente di:

- Ridurre al minimo le possibili finestre d'esposizione a eventuali attacchi informatici per gli endpoint in perimetro (con agent installato);
- Remediation automatica (ove applicabile) per gli incident riconosciuti come "veri positivi" ed a criticità massima;
- Garantire la protezione degli endpoint anche in assenza momentanea di connessione ad internet;
- Isolare dalla rete endpoint compromessi conservandone il controllo dalla piattaforma in cloud internet;
- Proteggere in tempo reale il perimetro da attacchi sconosciuti e che non utilizzano metodologie e/o indicatori noti internet (limitatamente alle caratteristiche della soluzione tecnologica impiegata);

Gli host massimi monitorabili dal presente servizio sono 1000 + 100 endpoint su Secure Public Cloud.

5.6.3.7 Vulnerability Assessment, Research & Exploitation

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

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

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

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

Tali documenti costituiscono perimetro e modalità di esecuzione dei test e devono essere sottoposti ad accettazione e firma dal cliente, in mancanza delle quali non sarà possibile procedere all'esecuzione dei test.

Nel dettaglio, la fase operativa del servizio prevede:

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

Al completamento delle stesse saranno consegnati i seguenti deliverable denominati:

- *VA Results Executive Summary:* Il report contiene una overview di tipo executive ad alto livello delle vulnerabilità individuate, ordinate per livello di rischio;
- *VA Results Technical Report:* Il report contiene i dettagli delle vulnerabilità segnalate, ordinate per criticità (utilizzando il sistema CVSS), incluse gli entry-point e le contromisure suggerite.

I deliverable, in base alla complessità del perimetro, possono far parte di un unico documento di report. Il servizio è limitato all'analisi di una quantità massima di 300 IP.

5.6.3.8 Servizio di Cyber Threat intelligence: Early Warning e Data Breach

Il servizio professionale richiesto è orientato a supportare l'Amministrazione nella erogazione di servizi di *Cyber Threat Intelligence*. Nello specifico i servizi verranno erogati attraverso una soluzione

tecnologia proprietaria Leonardo, dislocata fisicamente presso il PSN e che consente l'attivazione delle seguenti tipologie di servizio:

- Early Warning
- Data Breach Discovery

Tale capacità di *cyber threat intelligence* garantisce una migliore efficacia dei servizi di *detection*, grazie alla verifica continua su fonti aperte di eventuali nuove vulnerabilità e/o possibili vettori di attacco che possano impattare la nuova infrastruttura su Cloud.

- Early Warning
  La componente di servizio Early Warning ha lo scopo di acquisire, da fonti aperte, elementi informativi tali da individuare nuove vulnerabilità applicative con l'obiettivo di segnalare proattivamente le vulnerabilità rilevate, al fine di prevenire attacchi informatici che possano sfruttare malware evoluti nonché zero-day che possono mettere a rischio le tecnologie in uso presso l'Amministrazione. Le principali caratteristiche e funzionalità offerte riguardano:
    - integrazione di feed esterni di sicurezza, potenziando in tal modo le capacità native della piattaforma tecnologica proprietaria;
    - monitoraggio in tempo reale delle fonti aperte per la ricerca di possibili nuove vulnerabilità informatiche non ancora note;
    - motore di cross correlazione per analizzare le informazioni raccolte rispetto all'elenco delle tecnologie in esame;
    - generazioni di report basati sulle configurazioni definite.

- Data Breach Discovery
  La componente di servizio denominata Data Breach Discovery ha lo scopo di rilevare attività che mirano a trafugare dati e/o divulgare e rendere pubbliche informazioni da parte di soggetti non autorizzati, relativi a target di interesse, attraverso il monitoraggio continuativo della rete (surface e deep/dark web).
  Le principali caratteristiche e funzionalità riguardano:
    - controllo continuo in tempo reale di fonti aperte alla ricerca di elementi di interesse quali, ad esempio, indirizzi e-mail, documenti, nomi macchina ecc., citati o individuati all'interno di determinate aree della rete;
    - generazione di allarmi in base alle evidenze derivanti dall'analisi dei dati;
    - produzione di report basati sulle evidenze derivanti dall'analisi dei dati.

L'erogazione del servizio prevede una fase di avvio e una fase di esecuzione (gestione, Maintenance e miglioramento continuativo). All'emergere di informazioni di particolare rilevanza per l'Amministrazione sarà redatto un *Intelligence Alert* ed un *Intelligence Report* con il quale il sistema di Cyber Threat intelligence segnalerà tempestivamente e con il dovuto dettaglio le evidenze rilevate e suggerirà eventuali misure da adottare per la risoluzione della problematica. Le due tipologie di deliverable conterranno informazioni relativamente a:

- categoria di interesse;
- severità;
- data di rilevazione;
- Traffic Light Protocol – TLP;
- dettaglio degli elementi raccolti e dei risultati delle analisi effettuate;
- indicazioni di eventuali raccomandazioni da porre in essere per la risoluzione degli opportuni «case».

Durante la *fase di avvio* sarà attivata un'istanza dedicata all'ambito specifico sul sistema di *Cyber Threat Intelligence*, sulla quale verranno eseguiti i processi di analisi che realizzano il servizio specifico. Inoltre, verrà abilitato un portale Web dedicato (*TIS Disclosure*) ad accesso sicuro sul quale saranno rese disponibili le interfacce per la consultazione dei risultati individuati.

5.6.3.9 Dynamic Application Security Testing

Il servizio sarà erogato in modalità a task da remoto e consente l'identificazione delle vulnerabilità all'interno delle applicazioni Web e l'analisi dell'esposizione al rischio di attacchi informatici ai Sistemi Informativi mediante l'utilizzo di tecniche di analisi dinamica.
L'attività ha lo scopo di rilevare e gestire le vulnerabilità applicative che insistono sui sistemi informativi in ambiente WEB di produzione/preproduzione e loro relative classificazione e prioritizzazione.
Il servizio prevede l'esecuzione dei test dinamici di sicurezza per le applicazioni per la verifica delle vulnerabilità tenendo conto dell'esposizione e dell'ambiente operativo in cui l'applicazione è in esecuzione. L'input è rappresentato dalle informazioni relative ai target da analizzare e le relative modalità attuative che dovranno essere concordate con l'Amministrazione.
L'analisi comprenderà almeno i seguenti ambiti:

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

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

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

Il servizio è limitato all'analisi di massimo q.tà 5 target (di max 30 url) con periodicità annuale per un massimo di 15 server.
Le attività oggetto di test saranno eseguite a valle della formalizzazione dei documenti riportati sotto.

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

Tali documenti costituiscono perimetro e modalità di esecuzione dei test e devono essere sottoposti ad accettazione e firma dal cliente, in mancanza delle quali non sarà possibile procedere all'esecuzione dei test.

5.6.3.10 Servizio di Incident Response e Crisis Management

I servizi professionali previsti sono finalizzati a supportare l'Amministrazione nella Gestione degli Incidenti di Sicurezza e Crisis Management. Il servizio, erogato in modalità "a task", **per incidente**, su richiesta del cliente, per un massimo di 20 giornate on site, mette in atto tutte le attività necessarie all'

identificazione delle dinamiche associate all'incidente e alla definizione di opportune azioni di contenimento e risposta alla minaccia.

Qualora l'evento si riveli impattante sugli obiettivi strategici, le funzioni vitali o la reputazione dell'Organizzazione, il servizio viene supportato dal Crisis Management che sarà in grado di far fronte a situazioni anomale, che esulano dalla gestione standard degli incidenti, organizzando le attività in modo da ricondurre tali eccezionalità all'interno di opportune best practice.

Di seguito sono riportate, a titolo esemplificativo e non esaustivo, le principali attività eseguite dal supporto richiesto:

- Isolamento dei sistemi compromessi dalla rete del Cliente.
- Indagini sull'entità e la tipologia degli eventi.
- Indicazione delle più efficienti modalità di sanitizzazione e ripristino dei sistemi coinvolti.
- Supporto nelle comunicazioni verso le Autorità competenti.
- Raccolta e sintesi delle Lesson Learned.

Il servizio di risposta all'incidente comprende anche le attività legate al contenimento, all'eradicazione e al ripristino della normale operatività dei servizi del Cliente che hanno subito l'incidente, al fine di fornire tempestivamente, una prima risposta di contrasto alle problematiche di sicurezza riscontrate dall'Amministrazione.

Figura 12 - Incident Response & Response Process

Come deliverable del servizio è previsto il rilascio di un report di alto livello ed uno di natura tecnica, con cui ripercorrere e comprendere gli step legati all'incidente come di seguito rappresentato:

- Technical Report di dettaglio
- Executive Report di sintesi

5.6.3.11 Servizio di Web Application Penetration Testing

Il presente paragrafo descrive il servizio professionale di Web Application Penetration Testing che sarà svolto operativamente da remoto One Shot. Le attività si compongono da un insieme di test manuali ed automatici, volti ad effettuare tentativi di intrusione sui sistemi Web in scope e delle applicazioni concordate. Su richiesta dell'Amministrazione vengono previste attività di test anche sfruttando le vulnerabilità emerse dal servizio di Vulnerability Management o Dynamic Application Security Testing. Le attività oggetto di test saranno eseguite a valle della formalizzazione dei documenti riportati sotto.

- Legal Agreement (Manleva): Un accordo stabilito tra le parti che autorizza il Security Assessment Team a svolgere le attività specifica e che lo scarica da responsabilità per eventuali danni o disservizi creati.

- Regole di Ingaggio: Documento che contiene indicazione di inizio e durata delle singole fasi, le finestre orario in cui verranno erogate le attività, l'elenco dei deliverable, l'assegnazione dei ruoli e delle responsabilità per il fornitore ed Ente e il perimetro oggetto di analisi.

Tali documenti costituiscono perimetro e modalità di esecuzione dei test e devono essere sottoposti ad accettazione e firma dal cliente, in mancanza delle quali non sarà possibile procedere all'esecuzione dei test.

Operativamente, sono previste le seguenti attività:

- Tentativi d'intrusione sui sistemi WEB sfruttando le vulnerabilità identificate in eventuali attività precedentemente svolte (VM, DAST);
- Tentativi di escalation dei privilegi, nel caso l'accesso ottenuto non fornisca privilegi amministrativi;
- In caso di penetrazione in un sistema, produzione delle relative evidenze al fine di dimostrare l'intrusione effettuata;
- Descrizione dei rischi esistenti relativi alle possibilità di accesso non autorizzato ai suddetti sistemi.

Le attività sono condotte applicando metodologie globalmente riconosciute come standard de-facto per la conduzione di attività di penetration test, e in particolare le metodologie OSSTMM (Open Source Security Testing Methodology Manual) e OWASP (The Open Web Application Security Project) che definiscono le modalità per la conduzione di test completi, accurati, ripetibili e verificabili. Il test è eseguito per la ricerca di vulnerabilità applicative ed in base alle tecnologie utilizzate dalle applicazioni, consentirà l'identificazione di tutte le categorie di vulnerabilità top 10 OWASP.

Il servizio per AIFA prevede all'analisi di massimo qtà 15 target (di max 30 url). Al termine delle attività verrà prodotto un documento denominato PT Results Technical Report che conterrà il report di dettaglio delle attività eseguite durante la fase di testing e le evidenze degli attacchi e delle eventuali compromissioni rilevate.

5.6.3.12 Servizio di Cyber Threat intelligence: Brand Abuse, Anti-phishing con Site takedown

Il servizio professionale richiesto è orientato a supportare l'Amministrazione, nella erogazione di servizi di *Cyber Threat Intelligence*, richiesti dal cliente. Nello specifico i servizi verranno erogati attraverso una soluzione tecnologia proprietaria Leonardo, che consente l'attivazione delle seguenti tipologie di servizio:

- Brand Abuse
- Anti-phishing con Site takedown

Il servizio è inoltre orientato a fornire conoscenza riguardo attori malevoli operanti in contesti illeciti piuttosto che ad evidenziare elementi di contesto potenzialmente utili a prevenire o mitigare azioni informatiche malevole mirate.

- Brand Abuse
  La componente di servizio Brand Abuse ha lo scopo di acquisire, da fonti aperte, elementi informativi tali da individuare contenuti illegittimi legati all'Amministrazione, come ad esempio

il logo o il marchio presenti in siti web o URL di terze parti, individuati attraverso il monitoraggio dei typosquatted domain.
Le principali caratteristiche e funzionalità offerte riguardano:
  - Identificazione di possibili attacchi di dirottamento del traffico dati relativi all'utilizzo indebito di domini web afferenti il brand o sue variazioni (typosquatting);
  - Analisi in tempo reale dell'utilizzo improprio del brand o senza diretta autorizzazione dell'Amministrazione;
  - Rilevazione di contenuti "typosquatted" per l'individuazione di domini o contenuti su Social Media non autorizzati e pubblicati con esplicito riferimento al brand (tipicamente finalizzati a perpetrare tentativi di frode);
  - monitoraggio di potenziali siti web fraudolenti relativi alla propria supply chain tramite set di keywords di interesse;
  - generazioni di report basati sulle configurazioni definite.
- Anti-phishing con Site takedown
  La componente di servizio di Anti-Phishing con site takedown (max q.tà 5/anno) ha lo scopo di generare allarmi a fronte dell'utilizzo improprio dei domini web dell'Amministrazione per perpetrare attività di phishing fraudolente. Il servizio abbraccia in generale i seguenti ambiti:
  - Phishing: "rilevazione" di domini e siti web fraudolenti creati appositamente per simulare ed impersonare una organizzazione a fini malevoli;
  - Rilevazione di contenuti legati all'organizzazione, come ad esempio il logo o il marchio, presenti in siti web o URL di terze parti, individuati attraverso il monitoraggio dei typosquatted domain, senza l'autorizzazione dell'organizzazione stessa;
  - motore di cross correlazione per analizzare le informazioni raccolte rispetto all'elenco delle tecnologie in esame;
  - generazioni di report basati sulle configurazioni definite.

Il servizio prevede l'identificazione preliminare dei contenuti legittimi dell'organizzazione da proteggere attraverso la stesura di una scheda informativa contenente i seguenti dati:

- nome del marchio registrato;
- logo ufficiale;
- domini legittimi;
- profili e pagine legittime sui social media network (se presenti);
- certificato con dettagli del copyright e/o trademark registrato;
- pagine clonate e malware mail pervenute solo da fonti OSint, se note;
- individuazione dei *phish-kit* utilizzati per gli attacchi, se noti
- elenco terze parti costituenti la supply chain.

Il contenuto di tale scheda sarà utilizzato per il monitoraggio del web e del dark-web, come aspetto proattivo del servizio, ossia l'identificazione preventiva di possibili contenuti fraudolenti non ancora inseriti o adottati dagli attaccanti in campagne malevole.

L'erogazione dei servizi *Brand Abuse ed Anti-Phishing con takedown* è costituita da una fase di avvio e una fase di esecuzione (gestione, maintenance e miglioramento continuo). All'emergere di informazioni di particolare rilevanza per l'Amministrazione sarà redatto un *Intelligence Alert* ed un *Intelligence Report* con il quale il servizio segnalerà tempestivamente e con il dovuto dettaglio le evidenze rilevate e suggerirà eventuali misure da adottare per la risoluzione della problematica. Le due tipologie di deliverable conterranno informazioni relativamente a:

- categoria di interesse;

- severità;
- data di rilevazione
- Traffic Light Protocol - TLP

Il servizio è organizzato in modo da effettuare un monitoraggio continuo di nuovi domini di tipo *typo-squatted* in maniera proattiva attraverso l'identificazione di uno o più domini di nuova costituzione e che possono essere considerati di tipo *typo-squatted* rispetto a quelli legittimi. Pertanto, verrà prevista una fase di analisi preliminare del contenuto in esame e, qualora la verifica confermasse da subito l'effettiva pericolosità del contenuto, si procederà, previa autorizzazione dell'Amministrazione, alla stesura di un report dettagliato da utilizzare per l'avvio della fase finale del processo, ovvero l'azione di *takedown*.
Se la fase preliminare di analisi non fornisse risultati esaustivi oppure determinasse che il contenuto non è ancora «armato» (ovvero non rappresenta una minaccia diretta per l'Amministrazione) si procederà alla fase di monitoraggio; questa fase avrà l'obiettivo di tenere sotto controllo i contenuti e la loro potenziale pericolosità per avviare, nel momento in cui essi risultino effettivamente armati e **previa autorizzazione dell'Amministrazione,** alla fase finale del processo, ovvero la stesura del report dettagliato e **l'avvio dell'azione di *takedown* vera e propria.**

Riassumendo vengono comprese all'interno del servizio le attività di:

- blocco dell'accesso ai siti di Phishing, attraverso il takedown dei domini typosquatted malevoli;
- segnalazione del dominio malevolo all'ente responsabile dell'hosting del sito di phishing;
- generazione di allarmi e report
- Il takedown dei siti è effettuato contattando diverse terze parti coinvolte nell'esposizione del sito di phishing, principalmente l'hosting provider e il registrar del dominio.

Contestualmente alla *fase di avvio* sarà attivata un'istanza dedicata, sulla quale verranno eseguiti i processi di analisi, che realizzeranno il servizio specifico, ed abilitato un portale Web dedicato (*TIS Disclosure*) ad accesso sicuro sul quale saranno rese disponibili le interfacce per la consultazione dei risultati individuati (report).

5.6.3.13 Servizio di Cyber sercurity awareness

Il servizio di Cyber Security Awareness ha l'obiettivo di rendere quanto avere i propri dipendenti consapevoli dei rischi degli attacchi Cyber e in modo da indirizzare i corretti comportamenti per ridurre tale rischio.
Il servizio propone contenuti formativi che si sviluppano in un percorso triennale che, tramite tecniche di storytelling, puntano a conferire a tutto il personale dell'Amministrazione (max 600 utenti) una conoscenza basilare dei concetti e delle best practices afferenti alla sicurezza informatica.
L'obiettivo del servizio è di fornire al personale dell'Amministrazione una conoscenza basilare dei concetti e delle best practices afferenti alla sicurezza informatica, col fine di mitigare l'esposizione di quest'ultima alle minacce che fanno leva sul fattore umano.
È necessario che questo programma presenti tratti innovativi, che favoriscano il coinvolgimento dell'utente, che deve recepire l'importanza di seguire questi percorsi, ricavando un importante beneficio anche in termini di protezione individuale.
Si ritiene inoltre necessario che la soluzione scelta sia in grado di fornire altre tipologie di percorsi formativi, che consentano, in prospettiva, di aumentare ulteriormente il livello di consapevolezza della forza lavoro. In particolare, si fa riferimento a un modello di formazione induttiva, anche questo erogata in formato e-Learning, ma che possa essere fruita con l'approccio tipico delle "serie video". Per percorso induttivo intendiamo quindi un approccio che integri la tradizionale didattica di tipo nozionistico, con

un approccio che, basandosi sull'esposizione di casi reali, favorisca una forma di apprendimento attraverso la "narrazione". Questa narrazione deve mettere in evidenza quanto la sovrapposizione tra dimensione privata e professionale, possa comportare rischi e conseguenze per entrambe le dimensioni. Questi contenuti vengono selezionati e raggruppati in un formativo su tematiche individuate con l'Amministrazione contraente e si basano sui principi di:

- Drammatizzazione, con la funzione di fornire comprensione dei rischi e pericolosità del web;
- Storytelling, con l'obiettivo di far immedesimare i soggetti interessati di fronte a possibili minacce nel mondo reale, avvicinandoli quanto più verosimilmente a un'esperienza concreta;
- un percorso esperienziale, dedicato agli attacchi Phishing, che consenta di ridurre il rischio elevato rappresentato da questo tipo di minaccia;
- Serial Educational, che si basa sulla produzione di video e attraverso la serializzazione, affronta le principali tematiche in ambito di security e privacy.

Tra le tematiche tipiche affrontate vi sono:

- Information Security Best Practices
- Data Protection e GDPR
- Email Security
- Securing your Home
- Social Engineering
- Malware e Ransomware
- Privacy

Per il servizio è previsto il rilascio di un report di tipo executive summary, con il quale l'Amministrazione contraente sarà in grado di verificare il livello di partecipazione alla campagna di security awareness: Executive summary della campagna di Cyber Security Awareness, documento che descrive l'esito della campagna di Cyber Security Awareness.
Quindi, in questo scenario, è necessario affrontare un programma integrato ed avanzato per sviluppare negli utenti, un sufficiente grado di consapevolezza rispetto alle minacce e alle necessarie pratiche comportamentali da adottare.

I servizi descritti fino ad ora saranno erogati per tutta la durata contrattuale. Durante il terzo anno l'Amministrazione si riserva la possibilità di attivare Servizi di Sicurezza Avanzati ed Evoluti come oggetto di una versione successiva del progetto.
Di seguito un elenco, non esaustivo, dei possibili Servizi di Sicurezza Avanzati ed Evoluti.

5.6.3.14 Servizio di Security Policy review/advisory

Il servizio di Policy Review consiste in attività di analisi dei flussi perimetrali (inbound ed outbound) per una valutazione rapida ed efficace dello stato di conformità di un singolo firewall o di architetture complesse di firewall attuando una maggiore coerenza delle politiche implementate nel rispetto delle modalità organizzative oggi adottata dal cliente.

Questo servizio, è attualmente conforme allo standard PCI-DSS e al framework NIST e si riassume nelle seguenti macro attività:

- Rilevazione delle problematiche di sicurezza e conformità ai requisiti;
- Ottimizzazione delle regole e configurazione del firewall, con relativi flussi di traffico

Nel contesto specifico dell'Amministrazione, il servizio proposto si configura come un'attività di analisi-statica e dove possibile dinamica, eseguita sui flussi di traffico che attraversano i firewall oggetto di verifica.

Il servizio prevede le seguenti fasi operative:

- Definizione della baseline
- Information Gathering
- Definizione del modello di riferimento
- Analisi dei flussi

Il processo prevede che, con l'analisi dei log di traffico, si possano individuare elementi di miglioramento nelle configurazioni agendo sui seguenti parametri: service, source e destination. Verranno cioè individuate restrizioni dei parametri indicati sulla base di quello che effettivamente si rileva dai log, eliminando permission non necessarie (es. individuazione degli effettivi host source/ host destination/services utilizzati realmente nelle policy analizzate).

Questo processo sarà strutturato sulla falsa riga del servizio generale sopra descritto, con fasi di raccolta informazioni, analisi, reporting, ottimizzazione e reportistica finale a conclusione dell'attività.

Per il presente servizio è necessario che gli apparati di sicurezza perimetrale a cui afferiscono i servizi del cliente siano sempre raggiungibile e che vengano fornite al personale Leonardo le credenziali di accesso.

Il cliente dovrà autorizzare l'invio dei log dai firewall ai sistemi di analisi presenti presso il centro servizi Leonardo.

Come deliverable del servizio è previsto il rilascio di un report di analisi che riporti tutte le indicazioni riguardo le ottimizzazioni apportate sugli apparati di sicurezza oggetto di analisi.

- Technical Report di dettaglio
- Executive Report di sintesi

5.6.3.15 Servizio di Threat Hunting as a service

Il presente paragrafo descrive il servizio professionale di Threat Hunting che sarà svolto operativamente da remoto con una figura specializzata in varie sessioni di hunting le cui attività saranno concordate operativamente negli obiettivi con il cliente.

Il servizio si compone di un insieme di analisi manuali ed automatiche, supportate dall'intelligence, volte alla ricerca proattiva di tecniche, tattiche e procedure (TTP) riconducibili ad attività malevole, sospettose e rischiose che potrebbero avere eluso gli strumenti di sicurezza esistenti.

Il servizio prevede l'utilizzo degli strumenti erogati e presenti presso l'Amministrazione purchè raggiungibili da remoto tramite collegamento opportuno (VPN). Su richiesta le sessioni di hunting potranno essere indirizzate alla ricerca di TTP riconducibili a tecniche definite nel framework Att&ck Mitre, o ad TTP associati a incidenti intercorsi o ad attori oggetto di report di threat intelligence.

Operativamente, saranno previste le seguenti attività:

- Definizione con l'Amministrazione degli obiettivi della sessione di Hunting (TTP, Attori, Incidenti pregressi)
- Definizione dell'ipotesi di dettaglio da verificare. Analizzando le TTP selezionato si effettua un elenco di indicatori da verificare, e si associa ogni TTP alle diverse fonti informative a disposizione e al tipo di evidenza che in esse un attaccante può aver generato.
- Analisi ed elaborazione dei dati. Si procedere a verificare la presenza delle fonti dati ipotizzate, e ove presenti a verificare se queste contengono le evidenze ricercate.
- Stesura della reportistica, che contiene un Executive Summary e un dettaglio tecnico di tutte i TTP verificati, le fonti dati usate e quelle eventuali mancanti, possibili riscontri ed evidenze di compromissione, indicazioni per un miglioramento della security posture (ad esempio di abilitare alcuni log, nuove regole di correlazione possibili, etc.)

Il fornitore si riserva la possibilità di utilizzare ulteriori strumenti alternativi.

Per il servizio è previsto il rilascio di un report di Threat Hunting, che rispecchia i seguenti contenuti:

- Executive Summary
- Elenco delle tecniche, tattiche e procedure (TTP) oggetto di hunting
- Eventuali problemi di visibilità o assenza di telemetriche riscontrate rispetto al singolo TTP
- Eventuali riscontri osservati nell'infrastruttura
- Ove possibile, suggerimento di tecniche o regole di detection a colmare i problemi di visibilità.

5.6.3.16 Servizio di Security Orchestration, Automation, and Response (SOAR)

I servizi professionali previsti sono finalizzati a supportare l'Amministrazione nell'attuazione di una soluzione di Security Orchestration, Automation and Response (SOAR) che sarà messa in campo con lo scopo di fornire funzionalità e capacità di orchestrazione ed automazione, mediate issue cases contestualizzate in casi specifici. La soluzione tecnologica assume un ruolo centrale nell'erogazione di tale servizio ed ha lo scopo di:

- esaltare tutto il know-how tecnico per implementare workflow automatici che, sfruttando le integrazioni tecnologiche, permettano la gestione di use case in ambito IT Security;
- implementare una componente di dashboarding e di reporting che permettano di rendere visibili i benefici delle automazioni fornite ai clienti e le statistiche ad esse legate.

I principali benefici dei punti di forza derivanti dall'attivazione dello stesso sono:

- incrementare il proprio livello di maturità nell'ambito dell'information security, con l'adozione di processi di SOC automation;
- ridurre i tempi di risposta agli incidenti automatizzando la remediation e/o il containment;
- aumentare il livello di integrazione delle tecnologie in uso per massimizzarne il ritorno economico e operativo;
- migliorare la gestione degli incidenti di sicurezza con l'implementazione di processi automatici frutto delle competenze del Fornitore;
- accentrare la visibilità di tutte le informazioni legate all'operatività quotidiana in ambito IT security e non solo.

Il servizio viene erogato in due fasi distinte:

- *Avvio del servizio*, dove vengono raccolte tutte le informazioni di contesto utili alla definizione dei requisiti specifici di automazione ed utili alla creazione della baseline iniziale di use case da implementare. Durante la fase di avvio saranno definite anche le componenti architetturali della soluzione SOAR, si procederà al disegno dei meccanismi di automazione offerti dalla piattaforma, alle attività di integrazione delle varie piattaforme di terze parti con la relativa configurazione e, infine, al test di collaudo per passare alla messa in produzione e rendere la piattaforma pronta all'utilizzo durante la fase di conduzione;
- *Conduzione del servizio*, dove vengono:
    - manutenuti e ottimizzati i playbook esistenti in ottica di miglioramento continuo, per garantire azioni di enrichment, dissemination, containment e remediation più puntuali;
    - manutenuta ed ottimizzata la configurazione generale della piattaforma in termini di dashboarding e reporting;
    - implementati nuovi playbook e nuovi use case che possono derivare sia da attività di gestione degli incidenti sia da service review.

Dal punto di vista operativo l'erogazione del servizio consentirà di:

- mitigare tentativi d'intrusione sui sistemi WEB sfruttando le vulnerabilità identificate in eventuali attività precedentemente effettuate (VA, DAST);
- attivare use case di interesse per la Committente;
- analizzare tipologie di incidenti che il SOAR deve gestire;
- provvedere ad effettuare integrazioni tecnologiche necessarie allo svolgimento delle attività previste;
- definire gruppi di lavoro coinvolti nei workflow da implementare;
- consentire gli accessi allo strumento in termini di ruoli e permessi;
- consentire la raccolta dei metadati che lo strumento deve indicizzare ed elaborare
- produrre reportistica necessaria;
- raccogliere contenuti da mostrare attraverso le dashboard dello strumento;
- data retention policy.

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 ed automaticamente risolti.
- *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.

5.6.3.17 Servizio di Cyber Strategic Risk Management

Il servizio di Cyber Strategic Risk Management mira a misurare la postura di sicurezza informatica di un'azienda in termini di risorse, tecnologie, processi e politiche attraverso una analisi statica di rischi cyber situazionali.

Questo servizio mette insieme diversi servizi (ad es. valutazione ed analisi del rischio strategico, valutazione dell'intelligence sulle minacce più verticali al contesto) in modo strutturato per valutare e mitigare i rischi specifici e con un approccio Data driven.

L'output finale del servizio è costituito da documenti che indicheranno chiaramente la situazione "AS IS" ed un **Piano Strategico Cyber** con azioni evolutive misurato in modo chiaro da quanto emerso dall'analisi della situazione. I rischi, legati all'attuale contesto di cyber security ed al contesto industriale, saranno presi in considerazione ed analizzati in funzione del core business del cliente, con una valutazione fruibile sia a livello di management che operativamente.

Il servizio si compone delle seguenti fasi:

- Fase 1 - Studio preliminare: in questa fase del servizio verrà eseguito uno studio sia sul settore industriale che sul dominio in termini di rischi. Questa fase è fondamentale per adattare correttamente le fasi successive.
- Fase 2 - Cyber Strategic Risk: questa è la fase principale, nel quale:
    1. Definire il perimetro in cui opera l'azienda, sia in termini cyber che di business;
    2. Definire una lista di controllo e interviste che il cliente deve compilare e che costituiranno l'input principale della valutazione strategica del rischio;
    3. Preparare una valutazione delle minacce open source che definirà quali informazioni sono disponibili sull'azienda su Internet per definire meglio le minacce informatiche che potrebbero derivare da questo;
    4. Creare un piano di mitigazione e rimedio su misura per ridurre il rischio complessivo a cui è esposta l'azienda;
    5. Definire un Piano Strategico Cyber per il mantenimento e raggiungimento degli obiettivi di business.

Lo svolgimento delle attività che compongono il servizio, produrranno i seguenti deliverable:

- documento pdf di un Piano Strategico Cyber;
- Consegna dei Report di dettaglio:
    - Strategic Risk Assessment & Analysis;
    - Report verticale di Threat Intelligence;

5.6.3.18 MISP Threat Sharing (MISP) intelligence platform management

Il servizio ha come obiettivo condividere con il cliente gli indicatori di compromissione prodotti dalla Cyber Threat intelligence del PSN attraverso la federazione della piattaforma MISP cliente con quella del Polo e si compone delle seguenti attività:

- configurazione della federazione one-to-one tra piattaforme MISP cliente e PSN per la distribuzione verso l'istanza cliente degli indicatori di compromissione raccolti e prodotti dal personale del Polo;
- dissemination, implementata in modalità PUSH (Leonardo invia verso MISP cliente il flusso dati) e lato cliente sarà necessaria la configurazione sull'istanza MISP di una utenza dedicata alla sincronizzazione delle piattaforme da fornire al personale del PSN;
- sincronizzazione automatica e gestita dal sistema PSN la cui frequenza sarà dettata dall'aggiornamento stesso dei dati di Threat Intelligence eseguito da un team di specialisti;
- comunicazione tra istanze MISP avviene attraverso un canale sicuro come ad esempio una VPN IPSec site to site.

5.6.3.19 Servizio di Cyber Threat intelligence: Pre Planned Attack + Black Market Monitor

servizio professionale richiesto è orientato a supportare l'Amministrazione, nella erogazione di servizi di *Cyber Threat Intelligence*, richiesti dal cliente. Nello specifico i servizi verranno erogati attraverso una soluzione tecnologia proprietaria Leonardo, che consente l'attivazione delle seguenti tipologie di servizio:

- Pre Planned Attack
- Black Market Monitoring

Pre Planned Attack

Il servizio ha lo scopo di raccogliere e correlare in tempo reale informazioni di tipo OSINT da molteplici fonti aperte (Surface, Deep e Dark Web), al fine di individuare eventuali "**segnali deboli**" indici di potenziali minacce che possano trasformarsi in attacchi informatici. Tale approccio consente di individuare eventuali "segnali deboli" in aree di interesse del cliente che siano indici di potenziali minacce e possano trasformarsi in attacchi informatici. Questo consentedi effettuare una analisi di contesto dell'ambito di interesse del Cliente (settori di business, tecnologie di riferimento, area geografiche e relativo contesto geo-politico, esposizione mediatica ecc.). Ad esempio sono rilevati e identificati:

- scenari di attacco cibernetico in corso nel mondo o nel paese che possono in qualche modo interessare il cliente per natura, area di mercato, area geografica o altro
- agenti di minaccia che hanno in corso o hanno avuto sospetti di attacco verso infrastrutture di interesse del cliente, per natura, area di mercato, area geografica o altro.
- Agenti di minaccia o attacchi specificatamente mirati al cliente stesso, anche di natura non cibernetica, se presenti (es. minacce fisiche ad asset o persone apicali del gruppo)
- Informazioni relative a eventi naturali, sociali e politici, se in zone/aree geografiche di interesse del cliente.

Le principali caratteristiche del servizio di Pre-Planned Attack sono:

- Il monitoraggio continuo delle fonti aperte alla ricerca di possibili eventi ed elementi che possano riguardare direttamente o indirettamente il Cliente;
- Analisi di contesto dell'ambito di interesse del Cliente (settori di business, tecnologie di riferimento, area geografiche e relativo contesto geo-politico, esposizione mediatica, eventuali minacce di natura non cibernetica ecc.);
- La creazione di una base dati continuamente aggiornata che consenta, attraverso algoritmi di Machine Learning e strumenti di visual link analysis, di correlare le informazioni raccolte con il perimetro tecnologico ed operativo del Cliente;
- Capacità di identificazione e protezione su aspetti relativi domini IP;
- Generazione di allarmi e report

Black Market Monitoring

Il servizio consente l'analisi in tempo reale di grandi quantità di informazioni da fonti aperte (compresi Dark e Deep Web) per identificare nuovi "black-market" liberamente accessibili e relative frodi al loro interno al fine di rilevare prontamente attività illegali su argomenti selezionati realizzati nei mercati neri. Questo consente di individuare tempestivamente attività illecite su temi di interesse specifici perpetrate nell'ambito dei black market sul dark e deep web, ove tali ambiti siano liberamente accessibili. Attraverso tool di analisi semantica c'è la possibilità di riconoscere sui black market analizzati luoghi, numeri di carte di credito, targhe

di veicoli o altre entità di interesse riconducibili ad attività illecite (entity extraction). Le informazioni che il servizio è in grado di monitorare sono di seguito elencate[1]:

- Riconoscimento, attraverso analisi sintattiche/semantiche e nei mercati neri monitorati, delle posizioni, carte di credito, targhe, entità legate a frodi e attività illegali.
- E-mail Address, numeri di carte di credito/debito all'interno del market monitoring, numeri di telefono, numeri di conto corrente, credenziali di accesso a siti web;
- Analisi relative a carte di credito, conti bancari e "riciclaggio di denaro", per identificare frodi nell'ambito del crimine informatico.
- Ricerca continua dei mercati neri e delle informazioni pertinenti al contesto specifico del Cliente.

- Generazione di allarmi e report.

5.6.4 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.

[1] Durante la fase di avvio del servizio (cfr. § **Errore. L'origine riferimento non è stata trovata.**) saranno concordate con il cliente le informazioni necessarie per il riconoscimento e la classificazione di dette informazioni

- 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.
Il servizio sarà offerto secondo le seguenti finestre di erogazione:

Servizi di Conduzione Operativa della Infrastruttura	Incident Management	H24/365
	Problem Management	OB
	Change Management	OB
	Configuration and Asset Management	OB
Backup and Restore Management	Restore	OB
	Incident Management	OB
	Problem Management	OB
	Change Management	OB

OB: orario base, fascia Lun-Ven 9-17, o fascia 8 ore da concordare con l'Amministrazione

5.6.4.1 Personalizzazione del servizio

Fermo restando quanto previsto ai sensi del Contratto di Utenza, a parziale integrazione di quanto indicato nei Livelli di Servizio (LS o SLA) descritti nell'Allegato H "Indicatori di qualità" alla Convenzione, che restano validi, in merito ai servizi di IT Infrastructure service operations qui indicati saranno altresì integrati con i seguenti SLA:

INC-TI: Tempo massimo di intervento per assistenza sistemistica sul **perimetro di sistemi operativi, middleware e backup dell'ambiente AIFA** (include IQ016)
INC-TR: Tempo massimo di ripristino (comprende INC-TIB) per la assistenza sistemistica sul **perimetro di sistemi operativi, middleware e backup dell'ambiente AIFA**
SRQ-TE: Tempo massimo di esecuzione di Change Management sul **perimetro di sistemi operativi, middleware e backup dell'ambiente AIFA.**

INC-TI - Tempo massimo di intervento per assistenza sistemistica sul perimetro di sistemi operativi, middleware e backup dell'ambiente AIFA	
Descrizione SLA	Misura il tempo di presa in carico e apertura ticket per richieste di intervento sistemistico sul perimetro di gestione dei sistemi operativi, dei middleware e del backup dell'ambiente AIFA

INC-TI - Tempo massimo di intervento per assistenza sistemistica sul perimetro di sistemi operativi, middleware e backup dell'ambiente AIFA		
Unità di misura	Ore	
Periodo di riferimento	Trimestre	
Frequenza di misurazione	Ogni trimestre	
Dati da rilevare	Numero ore di ritardo rispetto al tempo di intervento previsto	
Formula	Priorità 1	$INC - TIa = \frac{N_{richieste\ intervento(Tintervento \leq \text{TIPriorità1})}}{N_{richieste}} * 100$
	Priorità 2	$INC - TIb = \frac{N_{richieste\ intervento(Tintervento \leq \text{TIPriorità2})}}{N_{richieste}} * 100$
	Dove: $N_{\text{richieste intervento}}$ = Numero di richieste di intervento $N_{\text{richieste}}$ = Numero di richieste $T_{\text{intervento}}$ = Data $_{\text{intervento}}$ – Data $_{\text{invio richiesta}}$ Data $_{\text{invio richiesta}}$ = Tempo invio richiesta (hh/mm/ss) Data $_{\text{intervento}}$ = Tempo intervento (hh/mm/ss)	
Valore di soglia (risultati attesi)	Priorità 1	TIPriorità1 = 4 ore nel 96% dei casi
	Priorità 2	TIPriorità2 = 8 ore nel 96% dei casi
Sanzione	Il mancato raggiungimento comporterà l'applicazione della penale pari allo 0.3‰ (zerovirgolatre per mille dell'importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura, per ogni punto percentuale in diminuzione rispetto al valore di soglia	

INC-TR - Tempo massimo di ripristino per assistenza sistemistica sul perimetro di sistemi operativi, middleware e backup dell'ambiente AIFA		
Descrizione SLA	Misura il tempo di ripristino per richieste di intervento sistemistico sul perimetro di gestione dei sistemi operativi, dei middleware e del backup dell'ambiente AIFA	
Unità di misura	Ore	
Periodo di riferimento	Trimestre	
Frequenza di misurazione	Ogni trimestre	
Dati da rilevare	Numero ore di ritardo rispetto al tempo di ripristino previsto	
Formula	Priorità 1	$IINC - TRa = \frac{N_{richieste\ ripristino(Tripristino \leq \text{TRPriorità1})}}{N_{richieste}} * 100$
	Priorità 2	$INC - TRb = \frac{N_{richieste\ ripristino(Tripristino \leq \text{TRPriorità2})}}{N_{richieste}} * 100$
	Dove:	

INC-TR - Tempo massimo di ripristino per assistenza sistemistica sul perimetro di sistemi operativi, middleware e backup dell'ambiente AIFA		
	$N_{richieste\ ripristino}$ = Numero di richieste di ripristino $N_{richieste}$ = Numero di richieste $T_{ripristino}$ = $Data_{ripristino}$ – $Data_{invio\ richiesta}$ $Data_{invio\ richiesta}$ = Tempo invio richiesta (hh/mm/ss) $Data_{intervento}$ = Tempo ripristino (hh/mm/ss)	
Valore di soglia (risultati attesi)	Priorità 1	TRPriorità1 = 6 ore nel 96% dei casi
	Priorità 2	TRPriorità2 = 12 ore nel 96% dei casi
Sanzione	Il mancato raggiungimento comporterà l'applicazione della penale pari allo 0.3‰ (zerovirgolatre per mille dell'importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura, per ogni punto percentuale in diminuzione rispetto al valore di soglia	

SRQ-TE - Tempo massimo di esecuzione di un change management per assistenza sistemistica sul perimetro di sistemi operativi, middleware e backup dell'ambiente AIFA	
Descrizione SLA	Misura il tempo di esecuzione di un change per richieste di intervento sistemistico sul perimetro di gestione dei sistemi operativi, dei middleware e del backup dell'ambiente AIFA
Unità di misura	Ore
Periodo di riferimento	Trimestre
Frequenza di misurazione	Ogni trimestre
Dati da rilevare	Numero ore di ritardo rispetto al tempo di ripristino previsto
Formula	$$SRQ - TE = \frac{N_{richieste\ change\ (Tchange \leq T\ change\ max)}}{N_{richieste}} * 100$$
	Dove: N richieste change = Numero di richieste di change N richieste = Numero di richieste T change = Data change – Data invio richiesta Data invio richiesta = Tempo invio richiesta (hh/mm/ss) Data change = Tempo di chiusura della richiesta di chanhe (hh/mm/ss)
Valore di soglia (risultati attesi)	T change max = 36 ore nel 90% dei casi

SRQ-TE - Tempo massimo di esecuzione di un change management per assistenza sistemistica sul perimetro di sistemi operativi, middleware e backup dell'ambiente AIFA	
Sanzione	Il mancato raggiungimento comporterà l'applicazione della penale pari allo 0.3‰ (zerovirgolatre per mille dell'importo complessivo annuale del servizio di riferimento nel contratto esecutivo di fornitura, per ogni punto percentuale in diminuzione rispetto al valore di soglia

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.
- **Educational Designer/Tutoring:** Struttura, organizza e schedula i programmi di formazione, ne valuta la qualità attraverso un processo di feedback.

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.

L'Amministrazione non richiede l'esecuzione delle attività finalizzate ad "identificare il livello di maturità di sicurezza informatica AS-IS" - secondo le tre dimensioni di Governance, Detection e Prevention - così come previsto nell'esecuzione della "fase di assessment della Amministrazione target e definizione della strategia di migrazione" (Cfr. Convenzione - Relazione Tecnica Illustrativa, Par. 22.6.1 - Explore - fase di Analisi/Discovery - Step 1.1 Assessment - Data Collection & Analysis). In assenza di valutazione del livello di maturità di sicurezza, il PSN non potrà "identificare potenziali lacune e impatti su Organizzazione, Processi e Tecnologia al fine di definire le opportune remediation activities".

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.

L'Amministrazione resta responsabile dell'adozione di misure appropriate per la sicurezza, la protezione e il backup dei propri Contenuti. L'Amministrazione, inoltre, è responsabile di:

- Implementare il proprio sistema integrato di procedure, standard e policy di sicurezza e operative in base ai propri requisiti aziendali e di valutazione basati sul rischio
- Gestire i controlli di sicurezza dei dispositivi client in modo che dati o file siano soggetti a verifiche per accertare la presenza di virus o malware prima di importare o caricare i dati nei Servizi PSN
- Mantenere gli account gestiti in base alle proprie policy e best practice in materia di sicurezza
- Assicurare una adeguata configurazione e monitoraggio della sicurezza di rete

assicurare il monitoraggio della sicurezza per ridurre il rischio di minacce in tempo reale e impedire l'accesso non autorizzato ai servizi PSN attivati dalle reti dell'Amministrazione, che deve includere sistemi anti-intrusione, controllo degli accessi, firewall e altri eventuali strumenti di gestione dalla stessa gestiti.

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	97345810580
Ragione Sociale	AGENZIA ITALIANA DEL FARMACO
IDENTIFICATIVO DOCUMENTO	
Emesso da	CSO
Codice Documento	2023-0000097345810580-PdF-P1R1
Versione	1

VERSIONE CONFIGURATORE	4.1

RIEPILOGO PREZZI		
SERVIZIO	Totale UT	Totale Canone Annuale
Industry Standard		2.056.670,84
Hybrid Cloud on PSN Site		-
SecurePublicCloud		66.363,66
Public Cloud PSN Managed		-
Servizi di Migrazione	2.078.731,69	
Servizi Professionali	20.206.091,22	
TOTALE	22.284.822,91	2.123.034,50

VDC	CODICE	SERVIZIO	TIPOLOGIA	ELEMENTO	QUANTITA'	DR	Totale UT	Totale Canone Annuale
VDC_l	IAAS16	IndustrySt andard	IaaSSharedHA	Pool Large	38			180.046,6600
VDC_a	IAAS16	IndustrySt andard	IaaSSharedHA	Pool Large	8	Primario		37.904,5600
VDC_a_DR	IAAS16	IndustrySt andard	IaaSSharedHA	Pool Large	8	Secondario		62.542,5300
VDC_i	IAAS19	IndustrySt andard	IaaSSharedHA	Pool 1vCPU aggiuntiva	337			21.443,3100
VDC_b	IAAS27	IndustrySt andard	IaaSShared	Pool Large	34			107.610,6800
VDC_b	IAAS32	IndustrySt andard	IaaSShared	Pool 1vCPU aggiuntiva	257			11.421,0800
VDC_i	IAAS03	IndustrySt andard	IaaSStorageHA	Storage High Performance	427			155.449,3500
VDC_a	IAAS07	IndustrySt andard	IaaSStorageHA	Storage HP Encrypted	44	Primario		21.942,8000
VDC_a_DR	IAAS07	IndustrySt andard	IaaSStorageHA	Storage HP Encrypted	44	Secondario		36.205,6200
VDC_b	IAAS03	IndustrySt andard	IaaSStorageHA	Storage High Performance	379			137.974,9500
VDC_c	PAAS04	IndustrySt andard	PaaSDB	Oracle dbms Enterprise	4	Primario		53.472,0000
VDC_c_DR	PAAS04	IndustrySt andard	PaaSDB	Oracle dbms Enterprise	4	Secondario		88.228,8000
VDC_d	PAAS04	IndustrySt andard	PaaSDB	Oracle dbms Enterprise	4	Primario		53.472,0000
VDC_d_DR	PAAS04	IndustrySt andard	PaaSDB	Oracle dbms Enterprise	4	Secondario		88.228,8000
VDC_e	PAAS04	IndustrySt andard	PaaSDB	Oracle dbms Enterprise	2			26.736,0000
VDC_c	IAAS31	IndustrySt andard	IaaSShared	Pool 1GB ram aggiuntivo	28	Primario		636,4400
VDC_c_DR	IAAS31	IndustrySt andard	IaaSShared	Pool 1GB ram aggiuntivo	28	Secondario		1.050,1300
VDC_d	IAAS31	IndustrySt andard	IaaSShared	Pool 1GB ram aggiuntivo	28	Primario		636,4400
VDC_d_DR	IAAS31	IndustrySt andard	IaaSShared	Pool 1GB ram aggiuntivo	28	Secondario		1.050,1300

VDC_c	IAAS07	IndustrySt andard	IaaSStorageHA	Storage HP Encrypted	31	Primario		15.459,7000
VDC_c_DR	IAAS07	IndustrySt andard	IaaSStorageHA	Storage HP Encrypted	31	Secondario		25.508,5100
VDC_d	IAAS07	IndustrySt andard	IaaSStorageHA	Storage HP Encrypted	18	Primario		8.976,6000
VDC_d_DR	IAAS07	IndustrySt andard	IaaSStorageHA	Storage HP Encrypted	18	Secondario		14.811,3900
VDC_e	IAAS07	IndustrySt andard	IaaSStorageHA	Storage HP Encrypted	22			10.971,4000
VDC_f	PAAS04	IndustrySt andard	PaaSDB	Oracle dbms Enterprise	4			53.472,0000
VDC_g	PAAS04	IndustrySt andard	PaaSDB	Oracle dbms Enterprise	4			53.472,0000
VDC_h	PAAS04	IndustrySt andard	PaaSDB	Oracle dbms Enterprise	2			26.736,0000
VDC_f	IAAS31	IndustrySt andard	IaaSShared	Pool 1GB ram aggiuntivo	28			636,4400
VDC_g	IAAS31	IndustrySt andard	IaaSShared	Pool 1GB ram aggiuntivo	28			636,4400
VDC_f	IAAS07	IndustrySt andard	IaaSStorageHA	Storage HP Encrypted	31			15.459,7000
VDC_g	IAAS07	IndustrySt andard	IaaSStorageHA	Storage HP Encrypted	18			8.976,6000
VDC_h	IAAS07	IndustrySt andard	IaaSStorageHA	Storage HP Encrypted	22			10.971,4000
VDC_a	HOUSING05	IndustrySt andard	Housing	IP Pubblici /29 (8 indirizzi)	30			1.963,5000
VDC_b	HOUSING05	IndustrySt andard	Housing	IP Pubblici /29 (8 indirizzi)	30			1.963,5000
	SEC01	IndustrySt andard	Security	Antivirus	285			119.360,8500
	SEC01	IndustrySt andard	Security	Antivirus	228			95.488,6800
VDC_a	DP02	IndustrySt andard	DataProtection	Backup	1211			392.557,7600
	SEC-MS-04	SecurePu blicCloud Azure	ComputeProduction	VM "convenzionali"c2r8	10			4.265,7270
	SEC-MS-06	SecurePu blicCloud Azure	ComputeProduction	VM "convenzionali"c4r8	8			4.540,2392
	SEC-MS-43	SecurePu blicCloud Azure	Storage	Managed Disks - dischi SSD Premium (128 GB)	48			10.987,9104
	SEC-MS-44	SecurePu blicCloud Azure	Network	Connection Gateway - ore di servizio	8760			4.872,3120
	SEC-MS-45	SecurePu blicCloud Azure	Network	Bandwidth - GB per anno	10			0,2200
	SEC-MS-46	SecurePu blicCloud Azure	Network	Speed - Giorni di accensione	10			247,5320
	SEC-MS-47	SecurePu blicCloud Azure	Network	Bandwidth Internet - TB annui	10			770,0410
	SEC-MS-54	SecurePu blicCloud Azure	PublicCloudSecurityBackupSIEM	SIEM service - GB per giorno	1			823,7426
	SEC-MS-55	SecurePu blicCloud Azure	PublicCloudSecurityBackupSIEM	SIEM Data Ingestion - GB per giorno	8			6.315,4432
	SEC-MS-56	SecurePu blicCloud Azure	PublicCloudSecurityBackupSIEM	SIEM Data retention (6 mesi) - GB per giorno	10			1.252,2690
	SEC-MS-57	SecurePu blicCloud Azure	PublicCloudSecurityBackupMonitor	Monitor VM Data ingestion - GB per giorno	10			7.894,3040
	SEC-MS-59	SecurePu blicCloud Azure	PublicCloudSecurityBackupFirewall	Deployment - Istanze	1			13.490,9455
	SEC-MS-60	SecurePu blicCloud Azure	PublicCloudSecurityBackupFirewall	Data managed - TB mese	10			1.730,6360
	SEC-MS-61	SecurePu blicCloud Azure	PublicCloudSecurityBackupCloudBackup	Istanze Protette - Numero VM	24			2.548,6176
	SEC-MS-62	SecurePu blicCloud Azure	PublicCloudSecurityBackupCloudBackup	Storage occupato GB	6000			1.503,0000
	SP-01	ServiziMi grazione	FiguraMigrazione	Cloud Application Architect	32		12.395,2000	

	SP-04	ServiziMigrazione	FiguraMigrazione	Cloud Application Specialist	48		15.136,8000	
	SP-05	ServiziMigrazione	FiguraMigrazione	Cloud Security Specialist	48		11.966,8800	
	SP-02	ServiziMigrazione	FiguraMigrazione	Database Specialist and Administrator	32		7.977,9200	
	SP-06	ServiziMigrazione	FiguraMigrazione	Enterprise Architect	95		39.454,4500	
	SP-03	ServiziMigrazione	FiguraMigrazione	System Integrator & Testing Specialist	63		13.232,5200	
	SP-01	ServiziMigrazione	FiguraMigrazione	Cloud Application Architect	543		210.331,0500	
	SP-02	ServiziMigrazione	FiguraMigrazione	Database Specialist and Administrator	472		117.674,3200	
	SP-03	ServiziMigrazione	FiguraMigrazione	System Integrator & Testing Specialist	1522		319.680,8800	
	SP-04	ServiziMigrazione	FiguraMigrazione	Cloud Application Specialist	522		164.612,7000	
	SP-06	ServiziMigrazione	FiguraMigrazione	Enterprise Architect	585		242.956,3500	
	SP-22	ServiziMigrazione	FiguraMigrazione	Data Protection Specialist	41		15.243,8000	
	SP-23	ServiziMigrazione	FiguraMigrazione	Systems Architect	53		25.638,2200	
	SP-07	ServiziMigrazione	FiguraMigrazione	Project Manager	641		238.323,8000	
	SP-12	ServiziMigrazione	FiguraMigrazione	System and Network Administrator	136		40.451,8400	
	SP-07	ServiziProfessionali	ITInfrastructureServiceOperation	Project Manager	1510		561.418,0000	
	SP-01	ServiziProfessionali	ITInfrastructureServiceOperation	Cloud Application Architect	4020		1.557.147,0000	
	SP-12	ServiziProfessionali	ITInfrastructureServiceOperation	System and Network Administrator	8430		2.507.419,2000	
	SP-22	ServiziProfessionali	ITInfrastructureServiceOperation	Data Protection Specialist	2430		903.474,0000	
	SP-23	ServiziProfessionali	ITInfrastructureServiceOperation	Systems Architect	4080		1.973.659,2000	
	SP-02	ServiziProfessionali	ITInfrastructureServiceOperation	Database Specialist and Administrator	10		2.493,1000	
	SP-24	ServiziProfessionali	ITInfrastructureServiceOperation	Product/Network/Technical Specialist	10		3.350,2000	

	SP-04	ServiziProfessionali	ITInfrastructureServiceOperation	Cloud Application Specialist	10		3.153,5000	
	SP-05	ServiziProfessionali	ITInfrastructureServiceOperation	Cloud Security Specialist	364		90.748,8400	
	SP-02	ServiziProfessionali	ITInfrastructureServiceOperation	Database Specialist and Administrator	547		136.372,5700	
	SP-24	ServiziProfessionali	ITInfrastructureServiceOperation	Product/Network/Technical Specialist	4828		1.617.476,5600	
	SP-12	ServiziProfessionali	ITInfrastructureServiceOperation	System and Network Administrator	2551		758.769,4400	
	SP-23	ServiziProfessionali	ITInfrastructureServiceOperation	Systems Architect	820		396.666,8000	
	SP-01	ServiziProfessionali	Replatform	Cloud Application Architect	55		21.304,2500	
	SP-04	ServiziProfessionali	Replatform	Cloud Application Specialist	133		41.941,5500	
	SP-05	ServiziProfessionali	Replatform	Cloud Security Specialist	89		22.188,5900	
	SP-02	ServiziProfessionali	Replatform	Database Specialist and Administrator	89		22.188,5900	
	SP-06	ServiziProfessionali	Replatform	Enterprise Architect	55		22.842,0500	
	SP-07	ServiziProfessionali	Replatform	Project Manager	111		41.269,8000	
	SP-12	ServiziProfessionali	Replatform	System and Network Administrator	133		39.559,5200	
	SP-11	ServiziProfessionali	Replatform	Developer (Cloud/Mobile/Front-End Developer)	221		41.172,3000	
	SP-10	ServiziProfessionali	Replatform	DevOps Expert	111		34.701,9300	
	SP-08	ServiziProfessionali	Replatform	UX Designer	55		16.359,2000	
	SP-09	ServiziProfessionali	Replatform	Business Analyst	55		16.359,2000	
	SP-02	ServiziProfessionali	Replatform	Database Specialist and Administrator	1013		252.551,0300	
	SP-09	ServiziProfessionali	Replatform	Business Analyst	648		192.741,1200	
	SP-11	ServiziProfessionali	Replatform	Developer (Cloud/Mobile/Front-End Developer)	3738		696.389,4000	
	SP-03	ServiziMigrazione	FiguraMigrazione	System Integrator & Testing Specialist	2874		603.654,9600	
	SP-07	ServiziProfessionali	Replatform	Project Manager	367		136.450,6000	
	SP-06	ServiziProfessionali	Replatform	Enterprise Architect	737		306.083,4700	
	SP-04	ServiziProfessionali	Replatform	Cloud Application Specialist	3		946,0500	
VDC_a	DP03	IndustrySt andard	DataProtection	Golden copy	291			113.196,0900
	SP-01	ServiziProfessionali	SecurityProfessionalServices	Cloud Application Architect	1030		398.970,5000	
	SP-04	ServiziProfessionali	SecurityProfessionalServices	Cloud Application Specialist	1648		519.696,8000	
	SP-22	ServiziProfessionali	SecurityProfessionalServices	Data Protection Specialist	1442		536.135,6000	
	SP-21	ServiziProfessionali	SecurityProfessionalServices	Forensic Expert	824		306.363,2000	
	SP-15	ServiziProfessionali	SecurityProfessionalServices	Junior Information Security Consultant	1648		490.181,1200	
	SP-20	ServiziProfessionali	SecurityProfessionalServices	Junior Penetration Tester	1236		322.175,7600	
	SP-18	ServiziProfessionali	SecurityProfessionalServices	Junior Security Analyst	2060		581.435,0000	
	SP-07	ServiziProfessionali	SecurityProfessionalServices	Project Manager	1236		459.544,8000	
	SP-13	ServiziProfessionali	SecurityProfessionalServices	Security Principal	1030		536.135,6000	
	SP-16	ServiziProfessionali	SecurityProfessionalServices	Security Solution Architect	2060		872.966,2000	
	SP-14	ServiziProfessionali	SecurityProfessionalServices	Senior Information Security Consultant	1030		436.483,1000	
	SP-19	ServiziProfessionali	SecurityProfessionalServices	Senior Penetration Tester	824		306.363,2000	
	SP-17	ServiziProfessionali	SecurityProfessionalServices	Senior Security Auditor/Analyst	4533		2.022.443,2800	

9 Rendicontazione

Di seguito, viene riportato il prospetto di spesa per l'Amministrazione per anni di contratto che tiene conto delle assunzioni di delivery su cui è stato strutturato il Gantt di progetto:

- Risorse IAAS Shared per l'ambiente di preproduzione disponibili al Mese 1
- Migrazione del Portale Azure dal Mese 1
- Risorse disponibili per l'ambiente di produzione disponibili dal Mese 9
- Attivazione dei servizi di backup dal Mese 9
- Attivazione del servizio al 50% nei primi 12 mesi e il restante nei successivi 12 mesi
- Servizi di Migrazione e replatform sullo IAAS al 70% nei primi 12 mesi e il restante 30% nei successivi 3 mesi
- Attivazione dei servizi di IT Operation al 20% nei primi 12 mesi e 80% nei successivi 12 mesi
-

Inoltre, per rispondere alla necessità dell'Amministrazione di ridurre la spesa nei primi anni di contratto si è ipotizzato di rendere disponibile l'infrastruttura e i servizi di migrazione e IT-Operation relativi al DR dei servizi critici a partire dal terzo anno di contratto

SERVIZIO	TOT 10 ANNI	ANNO 1	ANNO 2	ANNO 3	ANNO 4-10
Infrastruttura Industry Standard	19.090.797,08 €	902.744,57 €	1.738.560,67 €	2.056.186,48 €	14.393.305,36 €
Infrastruttura Secure Public Cloud	663.636,60 €	66.363,66 €	66.363,66 €	66.363,66 €	464.545,62 €
Servizi di migrazione Industry Standard	1.374.912,96 €	883.511,93 €	378.647,97 €	112.753,06 €	
Servizi di migrazione Secure Public Cloud	100.163,77 €	100.163,77 €			
Servizi di Migrazione e Replatform applicativi	2.508.703,61 €	1.756.092,53 €	752.611,08 €		
Servizi di Sicurezza	7.789.167,16 €	918.135,00 €	668.000,00 €	658.000,00 €	5.545.032,16 €
Servizi di IT-Operation	9.695.712,27 €	437.200,76 €	848.792,78 €	1.051.214,84 €	7.358.503,89 €
Tot	**41.223.093,45 €**	**5.064.212,22 €**	**4.452.976,16 €**	**3.944.518,04 €**	**27.761.387,03 €**

La durata della migrazione dei servizi dell'Amministrazione si assume essere di 15 mesi. Si riporta di seguito la modalità di distribuzione dei servizi professionali, distinti per tipologia. I canoni dell'infrastruttura saranno attivati una volta resi disponibili i relativi servizi.
Si assume inoltre che la consuntivazione dei servizi avverrà su base SAL mensili in linea all'effettivo effort erogato in termini di giorni/uomo delle relative figure professionali.

Servizi	Peso	Importo	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15
		€ TOT															
		5.497.468,5	**0 %**	**7%**	**5%**	**9%**	**2%**	**6%**	**5%**	**9%**	**2%**	**8%**	**5%**	**13%**	**10%**	**11%**	**8%**
Servizi di migrazione Industry Standard	**23 %**	**1.262.159,9**		10,00%	20,00%	10,00%								20,00%	20,00%	10,00%	10,00%
Servizi di migrazione Secure Public Cloud	**2%**	**100.163,7**		30%		34%		18%		19%							
Servizi di Migrazione e Replatform applicativi	**46 %**	**2.508.703,6**				5,00%	5,00%	5,00%	10,00%	10,00%	5,00%	10,00%	10,00%	10,00%	10,00%	10,00%	10,00%
Servizi di IT-Operation (IS)	**4%**	**228.015,3**						2,00%	2,00%	2,00%	2,00%	2,00%	2,00%	2,00%	28,00%	29,00%	29,00%
Servizi di IT-Operation (Portale Istituzionale)	**6%**	**350.003,9**		14,29%		14,29%		14,29%		14,29%		14,29%		14,29%		14,29%	
Servizi di sicurezza	**19 %**	**1.048.421,9**		14,86%		13,30%		14,86%		14,86%		14,86%		14,86%		12,41%	
		Tot	**- €**	**362.043,5**	**252.431,9**	**474.627,8**	**125.435,1**	**353.803,4**	**255.430,6**	**479.739,4**	**129.995,4**	**461.209,1**	**255.430,6**	**713.641,1**	**567.146,6**	**623.285,9**	**443.210,8**

Tabella 13 Modalità di distribuzione dei servizi professionali durante la fase di migrazione

Nell'ipotesi che i servizi di DR per i servizi critici vengano attivato al M26 si riporta di seguito la modalità di distribuzione dei servizi professionali, distinti per tipologia tra il M16 e il M25 e nei successivi 12 mesi.

Servizi		Importo	M16	M17	M18	M19	M20	M21	M22	M23	M24	M25

	Peso	€ TOT										
		1.245.558,7	**18%**	**4%**	**18%**	**4%**	**18%**	**4%**	**14%**	**4%**	**14%**	**4%**
Servizi di IT-Operation (IS)	**37 %**	**457.324,47**	10,00%	10,00%	10,00%	10,00%	10,00%	10,00%	10,00%	10,00%	10,00%	10,00%
Servizi di IT-Operation (Portale Istituzionale)	**20 %**	**250.002,85**	20,00%	0,00%	20,00%	0,00%	20,00%	0,00%	20,00%	0,00%	20,00%	0,00%
Servizi di sicurezza	**43 %**	**538.231,45**	24,17%	0,00%	24,17%	0,00%	24,17%	0,00%	13,75%	0,00%	13,75%	0,00%
	Tot	€	**225.807,5**	**45.732,4**	**225.807,5**	**45.732,4**	**225.807,5**	**45.732,4**	**169.727,5**	**45.732,4**	**169.727,5**	**45.732,4**

Tabella 14 Modalità di distribuzione dei servizi professionali tra il M16 e il M25

Servizi	Peso	Importo	M26	M27	M28	M29	M30	M31	M32	M33	M34	M35	M36
		€ TOT											
		1.822.152,5	**14%**	**5%**	**13%**	**4%**	**13%**	**4%**	**13%**	**4%**	**13%**	**4%**	**11%**
Servizi di migrazione Industry Standard	**6%**	**112.753,06**	50,00%	50,00%									
Servizi di IT-Operation (IS)	**41%**	**751.211,42**	5,00%	5,00%	10,00%	10,00%	10,00%	10,00%	10,00%	10,00%	10,00%	10,00%	10,00%
Servizi di IT-Operation (Portale Istituzionale)	**16%**	**300.003,42**	16,67%	0,00%	16,67%	0,00%	16,67%	0,00%	16,67%	0,00%	16,67%	0,00%	16,67%
Servizi di sicurezza	**36%**	**658.184,63**	17,75%	0,00%	17,75%	0,00%	17,75%	0,00%	17,75%	0,00%	17,75%	0,00%	11,24%
Tot		**€**	**260.771,0**	**93.937,1**	**241.955,1**	**75.121,1**	**241.955,1**	**75.121,1**	**241.955,1**	**75.121,1**	**241.955,1**	**75.121,1**	**199.116,2**

Tabella 15Modalità di distribuzione dei servizi professionali tra il M26 e il M37