



Architettura Applicativa

28/07/2023

AGENDA

1

CONTESTO AIFA

2

ADOZIONE DEI SERVIZI PSN

3

ARCHITETTURA TO-BE

4

CONCLUSIONE

AGENDA

1

CONTESTO AIFA

2

ADOZIONE DEI SERVIZI PSN

3

ARCHITETTURA TO-BE

4

CONCLUSIONE

Contesto AIFA

SFIDE DELL'AMMINISTRAZIONE

MIGLIORAMENTO DELLA RESILIENZA

Una migrazione al Cloud garantirà un nuovo asset di sicurezza e migliore resilienza dei servizi AIFA andando ad adottare una soluzione di Disaster Recovery e introducendo logiche di Business Continuity.

ACCESSO SEMPLIFICATO A TECNOLOGIE DI ULTIMA GENERAZIONE

Il Cloud permette un accesso semplificato a soluzioni next-gen, come AI e Machine Learning, con cui è possibile rivoluzionare i propri processi, sviluppare software innovativi e realizzare nuovi servizi.

SVILUPPO SEMPLIFICATO GRAZIE AL FRAMEWORK DEVOPS

Potenziamento, comunicazione e collaborazione integrata tra team e automazione tecnologica. Fornendo visibilità continuativa in tutte le fasi di sviluppo applicativo.



RAZIONALIZZAZIONE DELLE ARCHITETTURE ATTUALMENTE IN USO

Possibilità di razionalizzare l'architettura applicativa migrando gli attuali servizi erogati su infrastruttura Legacy verso piattaforma a container OCP.

APPROCCIO ALL'ELASTICITA'

Con l'adozione del paradigma Cloud, verranno risolti i problemi legati alla rigidità del sistema andando ad acquisire una scalabilità dinamica garantendo una creazione automatizzata degli ambienti.

FLESSIBILITA' NELLA GESTIONE DEI DATI E SERVIZI

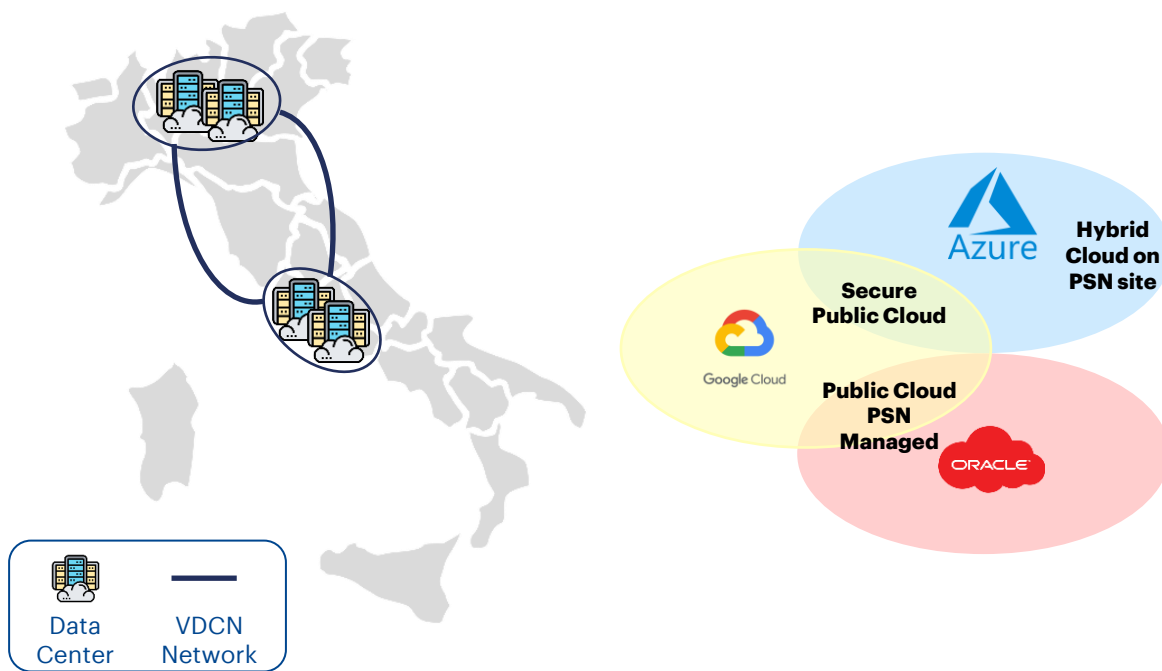
Le soluzioni in Cloud offrono una serie di servizi che favoriscono accesso a tutte le tipologie di dati, piattaforme open source e compatibilità tra i vari cloud provider.

MONITORAGGIO PREDITTIVO DEI SERVIZI

Per un'iniziativa di Journey to Cloud è essenziale assicurare un impatto minimo o nullo sulle prestazioni e sulla disponibilità dei carichi di lavoro. Essenziale creare un framework di monitoraggio olistico per acquisire metriche sull'integrità dei componenti dell'infrastruttura, dei servizi e sull'esperienza utente.

Contesto AIFA

SCENARIO PSN



Grazie alle partnership con i CSP Google, Microsoft e Oracle sono disponibili diverse soluzioni, in base ai bisogni delle PA, erogate in modalità Private, Hybrid e Public. I CSP risiederanno nei DC del PSN il quale si occuperà della gestione delle loro piattaforme.



ALTA AFFIDABILITÀ

I Data Center saranno allestiti in **doppia region (2DC + 2DC)** per garantire **massima affidabilità in caso di disastro**.



SOSTENIBILITÀ AMBIENTALE

I DC sono gestiti nel segno dell'**efficienza energetica** e della **sostenibilità ambientale**, comprovate da certificazioni quali:

- ISO 50001;
- ISO 14001;
- LEED.



CERTIFICAZIONI DC

La configurazione finale prevede l'utilizzo di 4 DC tutti certificati:

- **UPTIME INSTITUTE Tier IV** Constructed Facilities;
- **ANSI/TIA 942 Rating 4.**



CONNETTIVITÀ

- I DC saranno interconnessi fra di loro con **connettività ultra broad in fibra ottica** per assicurare la **continuità operativa** in tempo reale (lunghezza non superiore a 60 km);
- Utilizzo della **tecnologia SDN** (Software Defined Networking) per il controllo centralizzato e automatizzato di tutti i processi.

Contesto AIFA

DETTAGLI WAVE 3 & ROADMAP

BENEFICIARI PA Centrali

PLATEA 278 Amministrazioni

IMPORTO 280 mln €

ATTIVITÀ RICHIESTE ALL'AMMINISTRAZIONE PER LA RICHIESTA FONDI

- **Classificazione dati e servizi**
- Sottomissione del **piano di migrazione**
- Autocertificazione del numero di VM (**4,7 K€/VM** per un massimo di **400 VM**)
- Autocertificazione del numero di Server Fisici (**55,3 K€/Server** per un massimo di **40 Server**)

TEMPI DI MIGRAZIONE

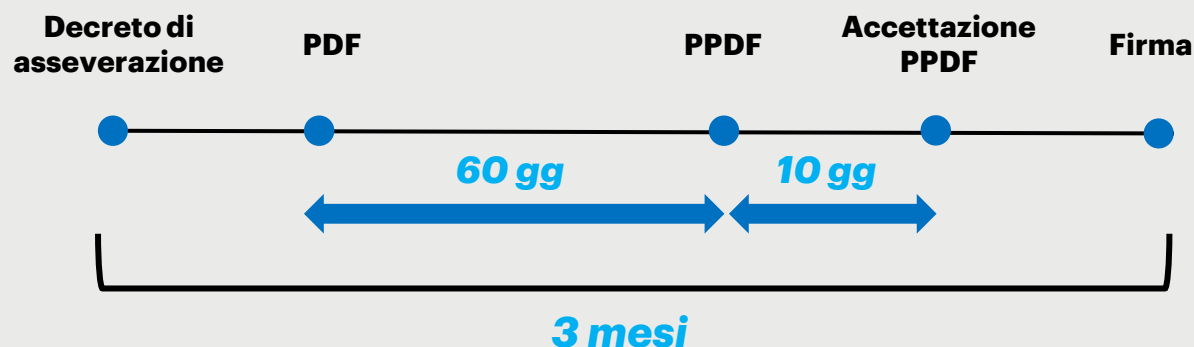
Finanziamenti < 1,5 mln € **3 mesi** per contrattualizzazione
6 mesi per migrazione

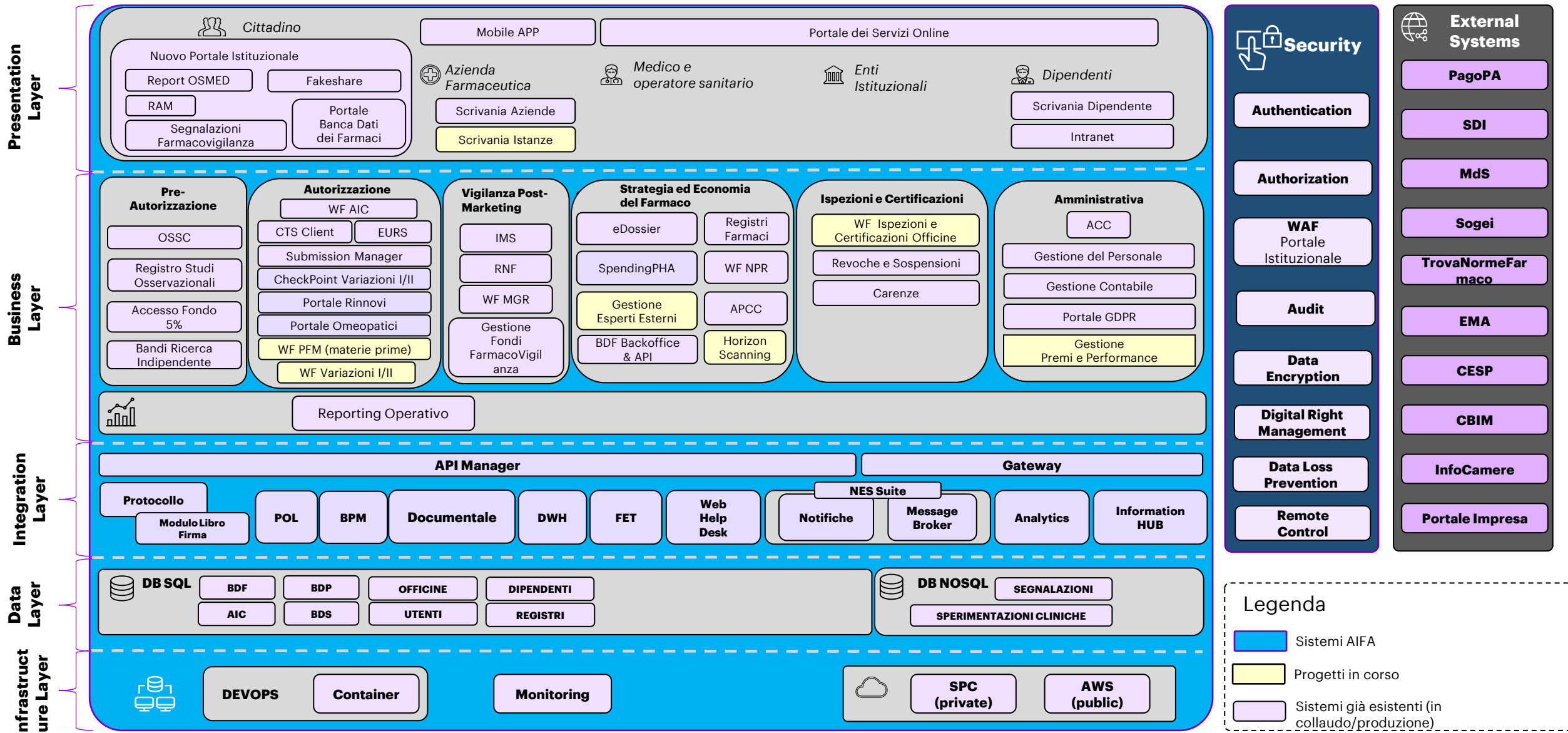
Finanziamenti > 1,5 mln € **3 mesi** per contrattualizzazione
15 mesi per migrazione

ROADMAP FINANZIAMENTI

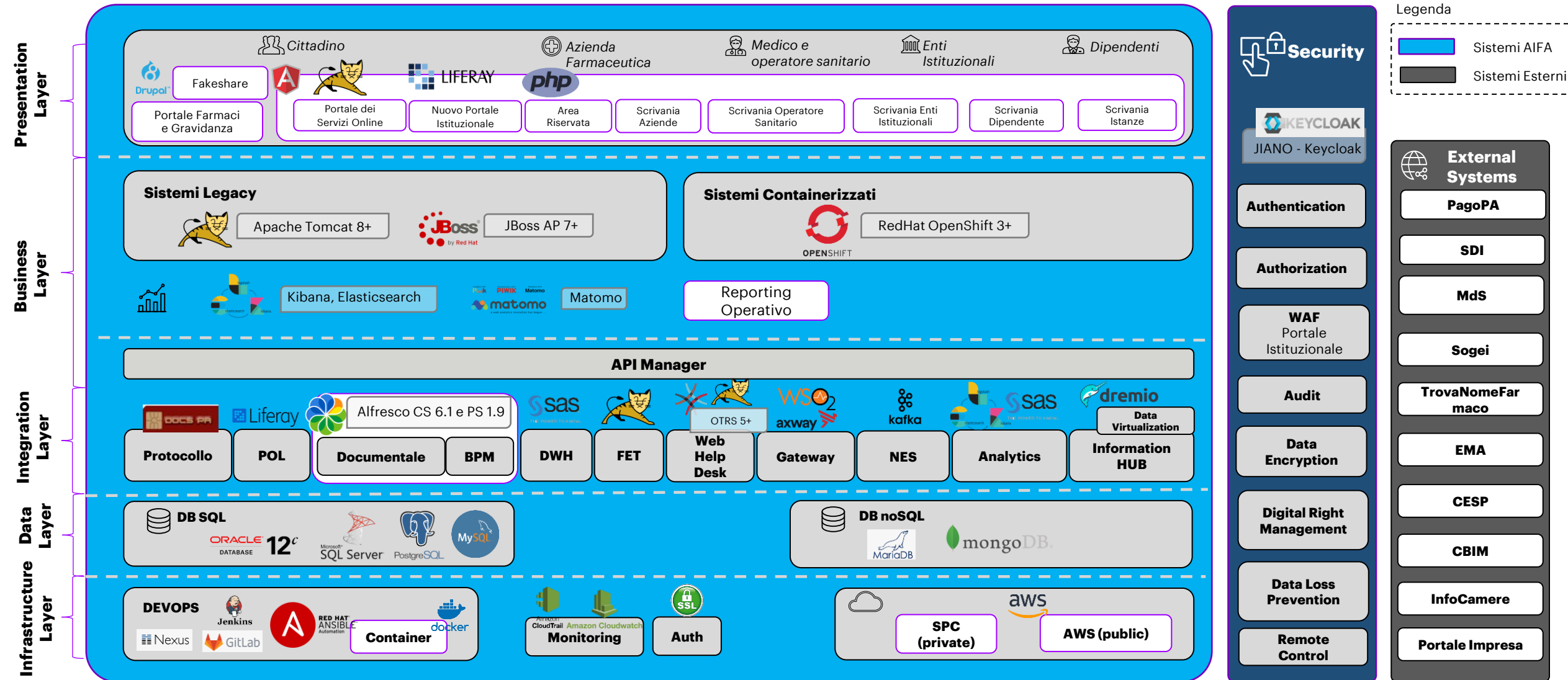


PDF/PPDF + CONTRATTUALIZZAZIONE CON PSN

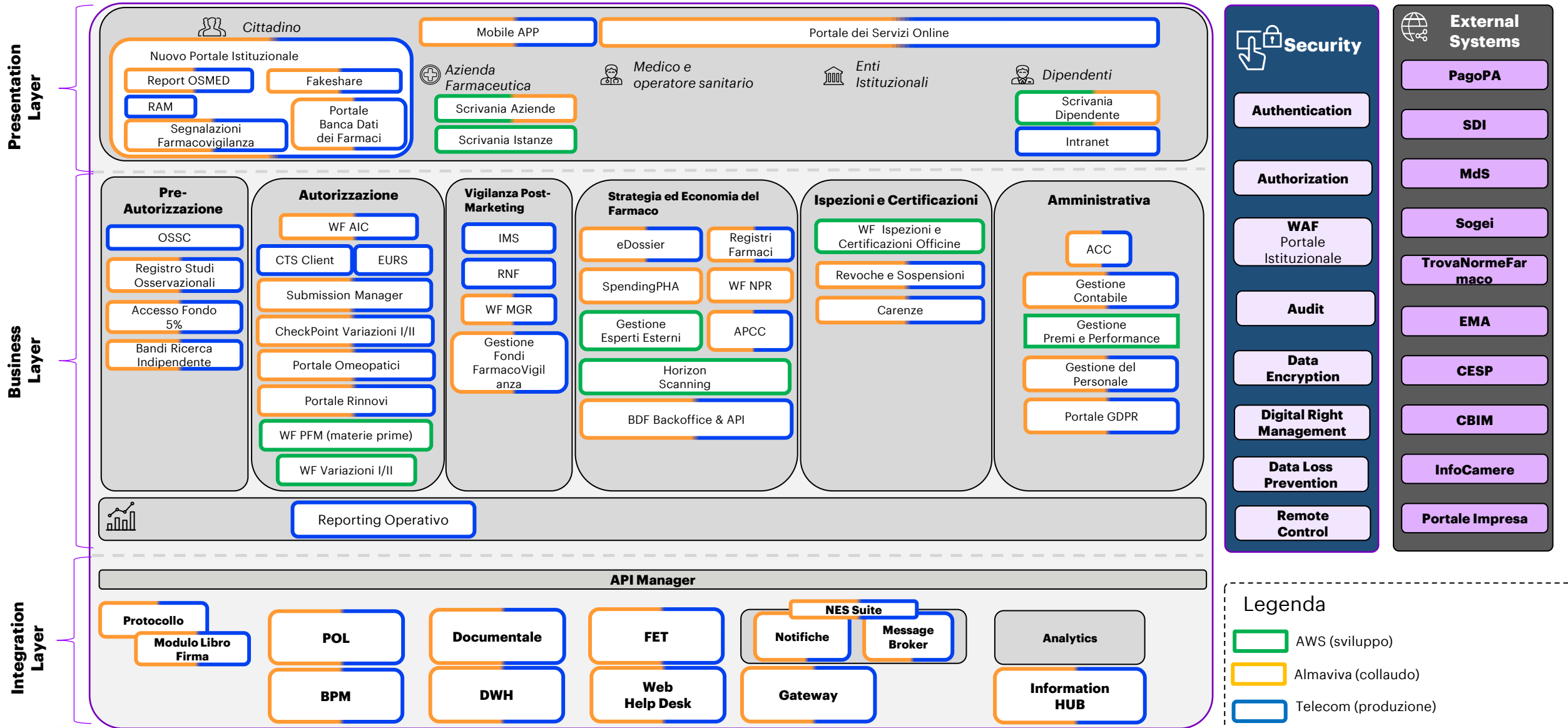




Contesto AIFA - Prodotti e Tecnologie AS-IS

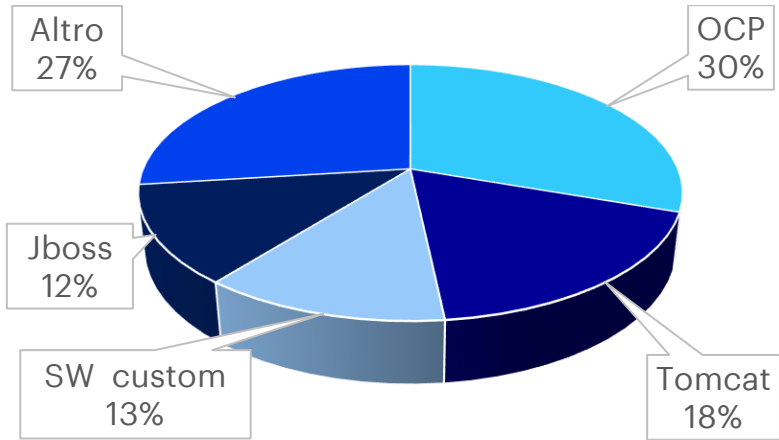


Contesto AIFA – Applicativi e Ambienti AS-IS

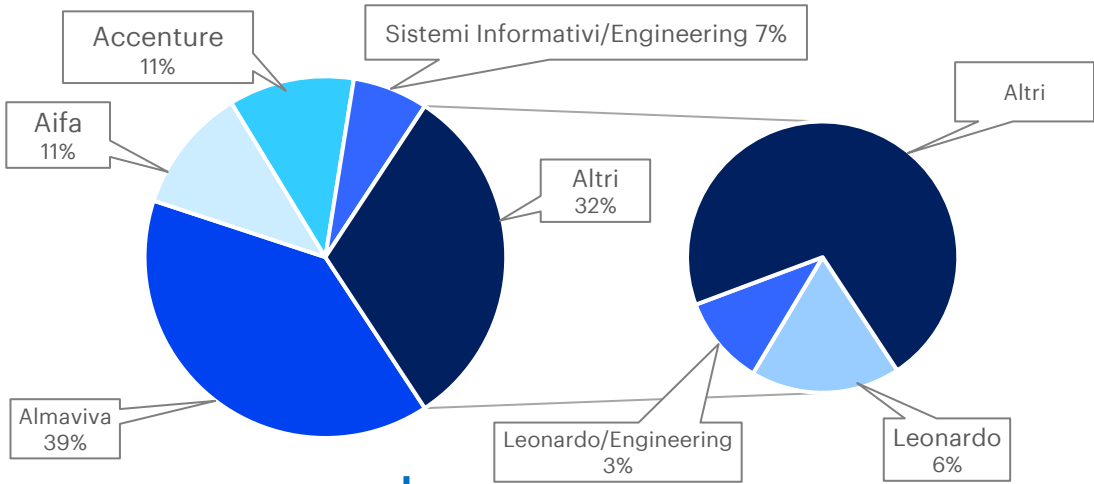


Contesto AIFA

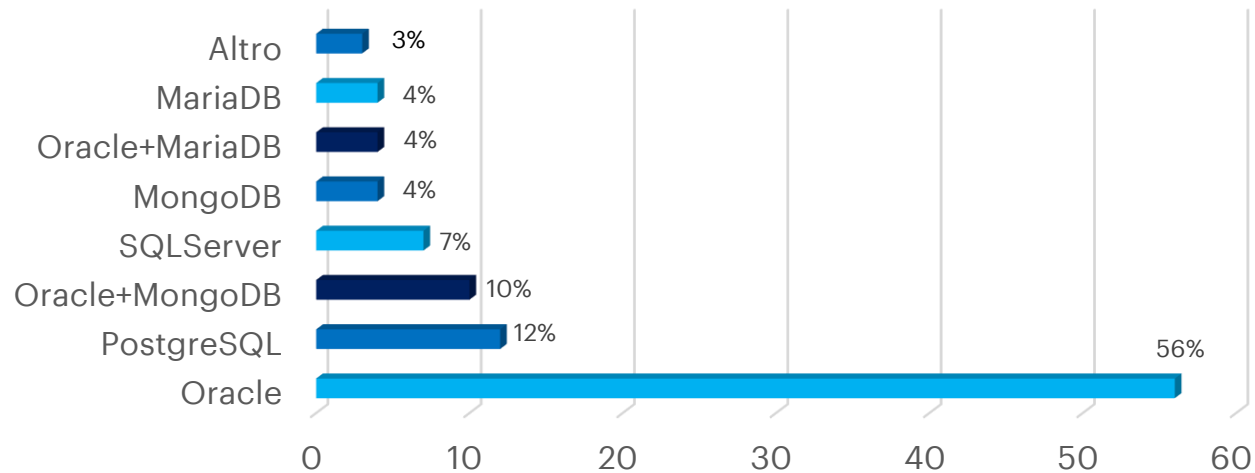
Tecnologie



Gestori Applicativi



DataBase



Il calcolo delle percentuali, effettuato su un insieme di **89 applicazioni**, non tiene conto della eventuale complessità della applicazione presa in esame (calcolo 1 a 1). Si rileva una importante eterogeneità in merito alle **tecnologie** attualmente in uso nel parco applicativo di Aifa (*Openshift, Oracle, Tomcat, Software Custom*). Questo è un elemento importante sia per le competenze dei diversi attori coinvolti sia per la definizione della blueprint architetturale della trasformazione to-be.

AGENDA

1

CONTESTO AIFA

2

ADOZIONE DEI SERVIZI PSN

3

ARCHITETTURA TO-BE

4

CONCLUSIONE

Adozione dei Servizi PSN

INTRODUZIONE E SCOPO DELLA SEZIONE

Per la definizione dell'architettura su PSN sono state prese in considerazione le caratteristiche specifiche di ciascuna componente applicativa quali il grado di obsolescenza, vincoli funzionali e/o operativi, vincoli dettati da pianificazioni progettuali in corso e strategie aziendali.

La presente sezione si compone dei seguenti elementi:

- ☐ *Assunti presi in considerazione per la composizione della soluzione nello scenario Cloud PSN;*
- ☐ *Blueprint architetturale in termini di componenti applicative in scope per il J2PSN;*
- ☐ *Blueprint architetturale declinata per le componenti tecnologiche che verranno utilizzate;*
- ☐ *Blueprint architetturale declinata per la tipologia di servizio in PSN (Industry, Managed, Secure);*
- ☐ *Sintesi sulle componenti introdotte nello scenario PSN.*

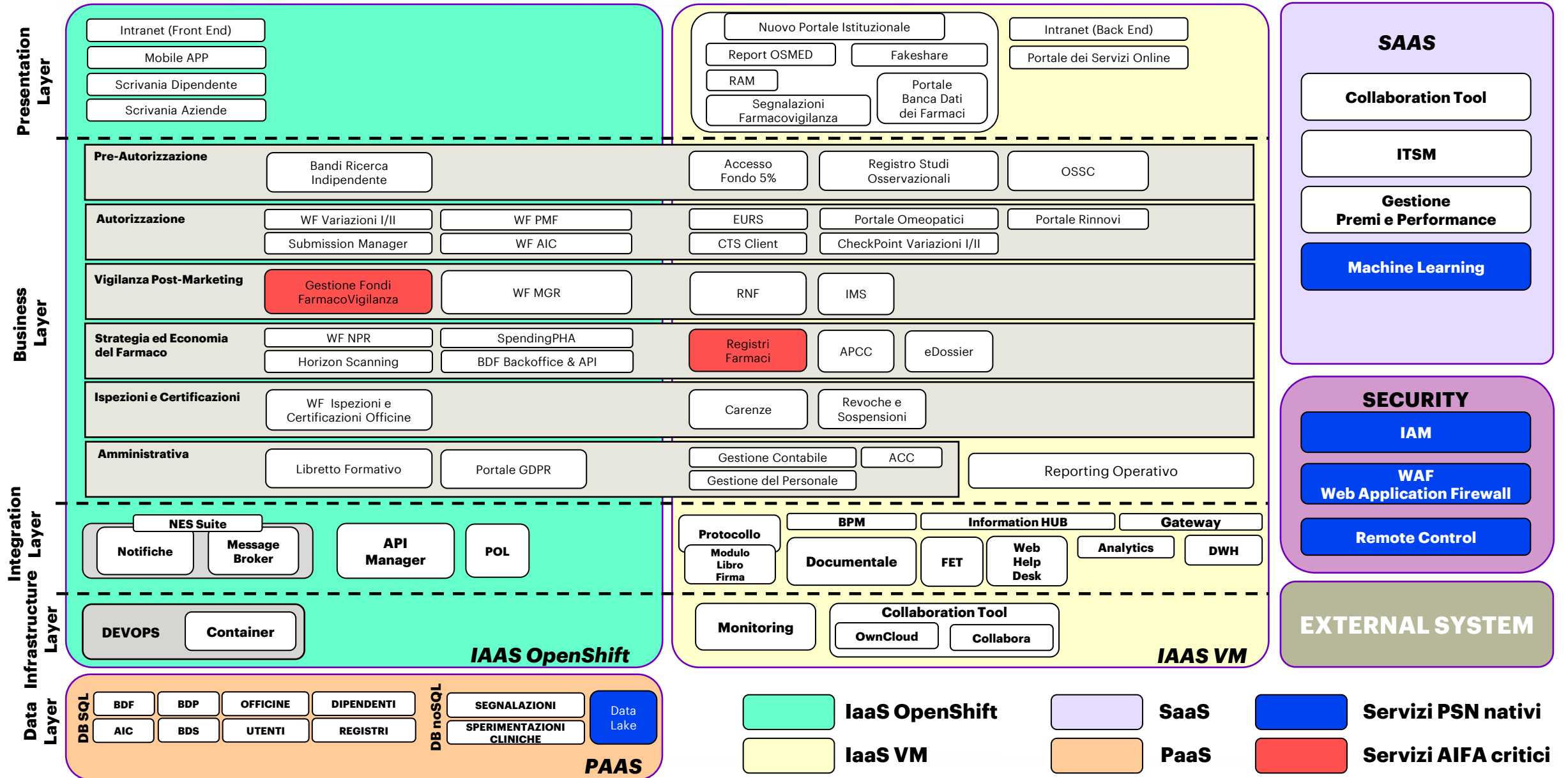


Adozione dei Servizi PSN

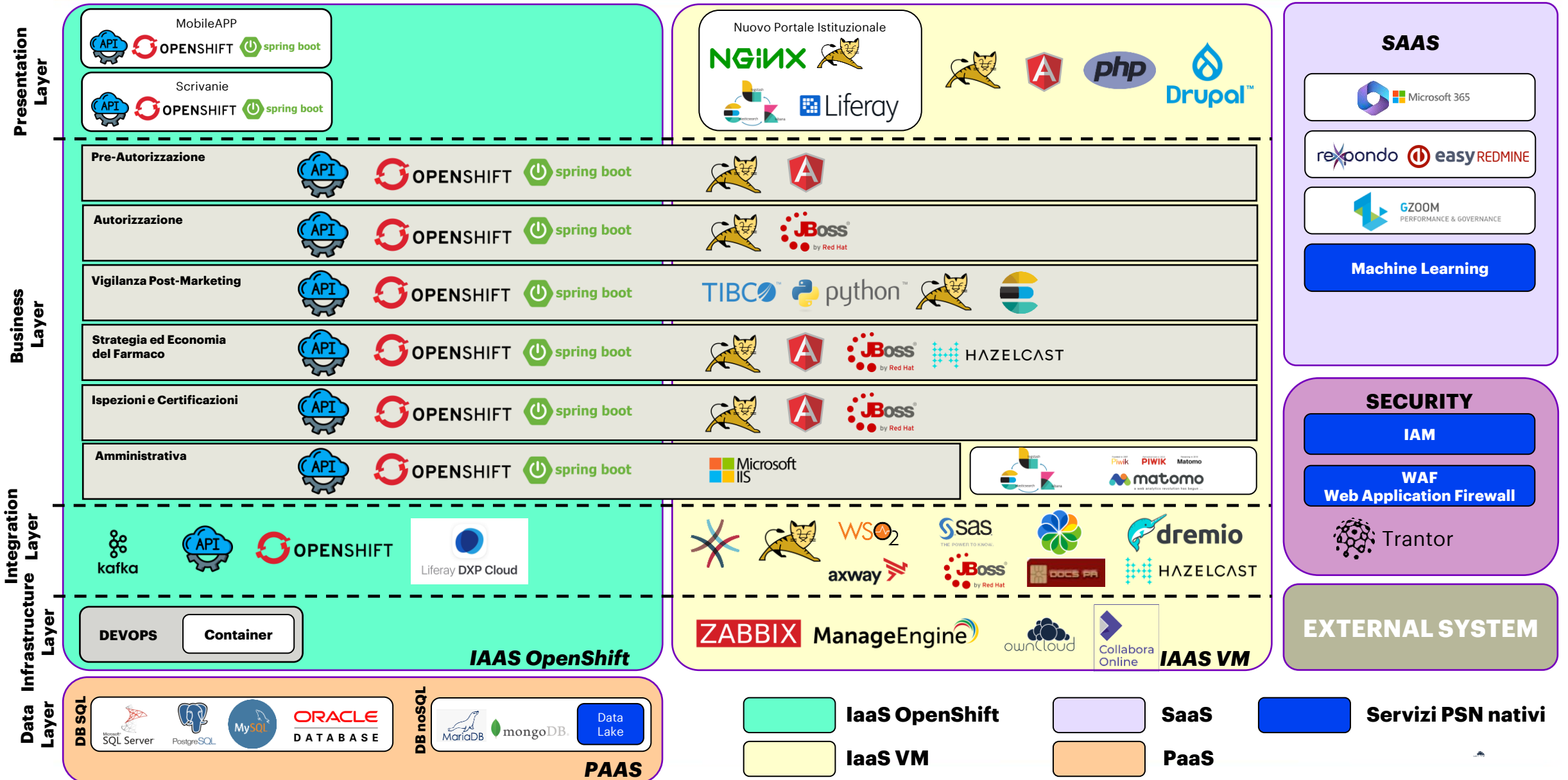
ASSUNTI

- Gli applicativi legacy su VM o server fisico con middleware obsoleti saranno migrati preferenzialmente in Lift&Shift;
- Gli applicativi che utilizzano software custom saranno migrati in Lift&Shift (es. Gateway Axway) prelieve eventuali azioni di remediation e/o aggiornamento stack tecnologico e SO;
- I progetti applicativi in corso di rilascio sono considerati come sviluppati a micro-servizi ed erogati su piattaforma a container;
- Gli applicativi già su container verranno migrati as-is;
- Gli applicativi di cui è previsto il Re-Architect o la sostituzione (es. Web Help Desk), verranno migrati in L&S solo nel caso in cui la migrazione al PSN dovesse partire prima del rilascio della nuova versione;
- Nello schema TO-BE sono rappresentati applicativi ad oggi non in Produzione, ma il cui rilascio è previsto prima della migrazione al PSN (es. Rexpondo);
- Per gli applicativi per i quali l'Amministrazione non dispone di sufficienti documentazioni tecniche, si considera una migrazione Lift&Shift;
- Per il Nuovo Portale Istituzionale si assume la migrazione L&S verso Public Cloud Azure.

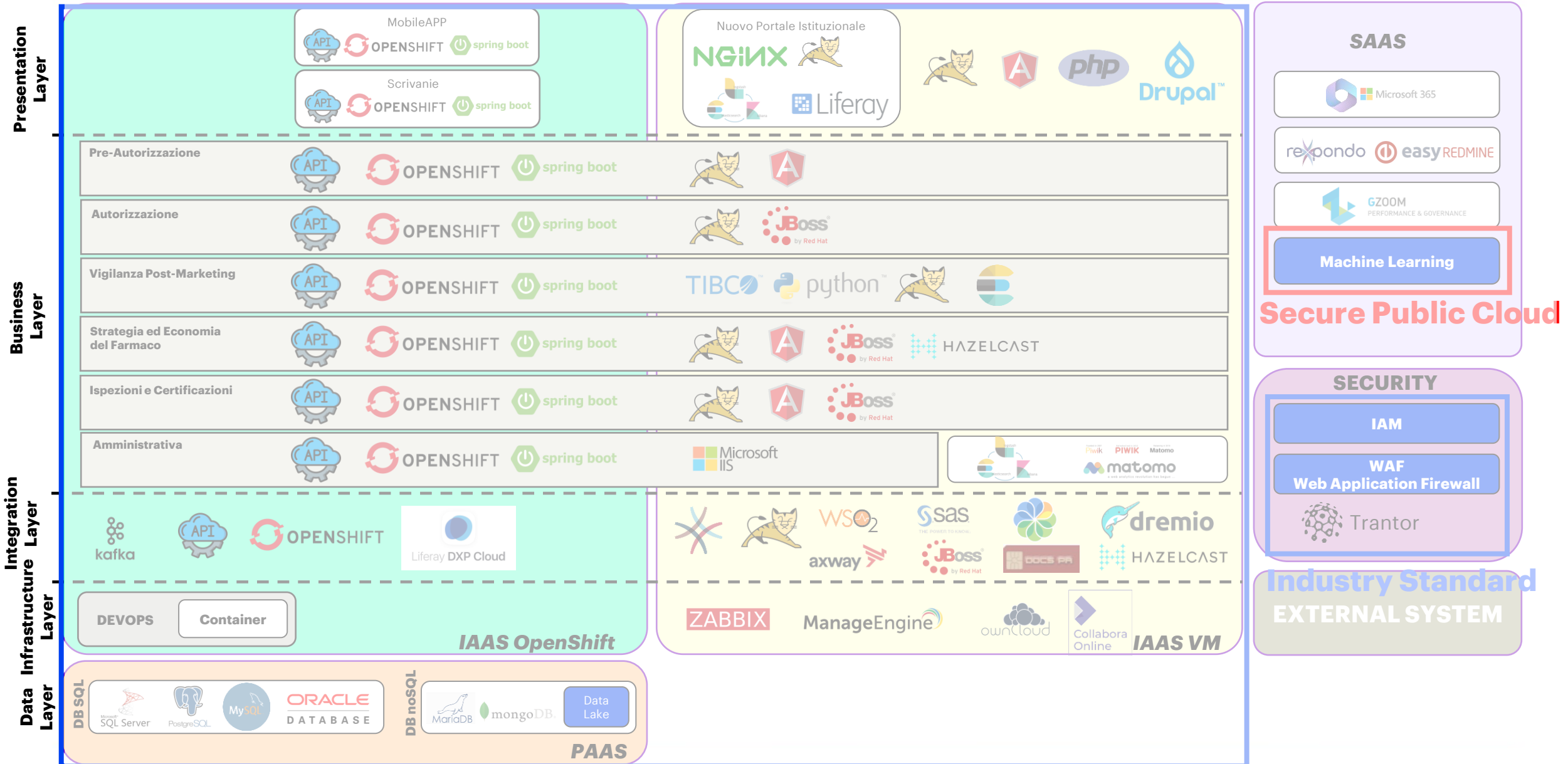
Adozione dei Servizi PSN - Blueprint Architettuale



Adozione dei Servizi PSN - Blueprint Architeturale




Adozione dei Servizi PSN - Blueprint Architettuale



Adozione dei Servizi PSN


Dettaglio servizi PSN

	Descrizione	PSN 
VPN (Client)	Tunneling privato per connettività verso i sistemi del Cloud Service Provider.	Appliance* erogata in IaaS su Industry Standard
Web Application Firewall	Firewall applicativo per la rilevazione e il blocco di attacchi comuni, (Xss, SQLi, JNDI) verso i servizi web esposti.	Appliance* erogata in IaaS su Industry Standard
IAM	Identity Access Management per la gestione centralizzata degli accessi.	IAM Nativo PSN (in alternativa GPC – IAM Active Directory)
Application Container Solution	Sistema per il rilascio automatizzato, scalabilità e gestione delle applicazioni containerizzate.	RedHat OpenShift - erogato in IaaS su Industry Standard
Key Management	Modulo di sicurezza per la gestione delle chiavi di crittografia nella modalità Secure Public Cloud.	Key Vault
Monitoring	Tool per il monitoraggio infrastrutturale di server e componenti Middleware.	Appliance * Zabbix e ManageEngine erogato in IaaS su Industry Standard
LOG e Analytics	Piattaforma per la raccolta, registrazione e visualizzazione centralizzata dei log. Composta da Elasticsearch, Logstash e Kibana.	ELK in modalità IaaS su Industry Standard

*** Servizio non presente a listino PSN; la predisposizione e la gestione dell'appliance selezionata per l'erogazione della funzionalità sarà a carico dell'Amministrazione.**

Adozione dei Servizi PSN

Dettaglio servizi PSN

	Descrizione	PSN 
Machine Learning	Sottoinsieme dell'AI che si occupa di creare sistemi che apprendono o migliorano le performance in base ai dati forniti.	Azure Machine Learning
DevOps	Framework che promuove uno sviluppo applicativo migliore e più efficace e una release più rapida di prodotti o funzionalità software ai clienti.	Pipeline di DEVOPS in modalità IaaS Industry Standard
Collaboration Tool	Pacchetto Office completo di servizi integrabili con sistemi Microsoft fruibili in larga scala e con sicurezza costantemente aggiornata.	Microsoft 365 in modalità SaaS <u>esterno</u> al PSN
Backup	Servizio nativo Cloud che prevede il salvataggio dei dati con cifratura, copia worm e il ripristino granulare in modalità "a caldo e out-of-the-place"	Backup-as-a-Service
ITMS	Suite per l'erogazione e la gestione dei servizi IT completa di strumenti per il PM, attualmente con OTRS e EasyRedmine	Rexpondo in modalità SaaS <u>esterno</u> al PSN
Data Lake	Repository di dati in grado di archiviare set di dati non elaborati di grandi dimensioni e di varia tipologia, strutturati e non strutturati.	Big Data - Data Lake in modalità PaaS Industry Standard
Data Encryption	Misura di sicurezza per la protezione dei dati	I servizi PSN prevedono di default la cifratura dei dischi a livello storage. Funzionalità più evolute di crittografia quali TDE (Transparent Database Encryption) devono essere implementate a parte

Adozione dei Servizi PSN

SERVIZI CORE E TOPOLOGIA

SERVIZI	DESCRIZIONE
Soluzioni con CSP	Secure Public Cloud ➤ Servizi di messa in sicurezza di un sottoinsieme del portafoglio di offerta relativo a un CSP
	Public Cloud PSN Managed ➤ Portfolio dei servizi CSP erogato da «Region» dedicata , con separazione logico/fisica e operata/controllata da personale PSN
	Hybrid Cloud on PSN site ➤ Servizi del CSP (Cloud Service Provider) hybrid (combinazione di Cloud pubblico e privato mediante un'infrastruttura integrata) e installati sull'infrastruttura locale del PSN
Private Cloud	PaaS ➤ Messa a disposizione di piattaforme in grado di erogare elementi applicativi e middleware come servizio (DB, big data, AI)
	CaaS e DR ➤ CaaS (Container as a Service) : servizio cloud con possibilità di sviluppare applicazioni in ambienti «cloud native»; DR (Disaster Recovery) : servizio back up dei contenuti informativi conservati in Cloud
	IaaS Shared ➤ Servizi on demand private cloud infrastrutturale (area Cloud dedicata per il cliente)
	IaaS dedicato ➤ Offerta di infrastruttura virtualizzata (capacità computazionale e storage) in modalità cloud, on demand e as a service, con possibilità di noleggiare server virtuali di proprietà del provider
Housing e Hosting	➤ Servizi di gestione infrastrutturale tradizionali. In caso di housing, il cliente utilizza lo spazio attrezzato di proprietà del provider in cui colloca i propri server, a differenza dell'hosting, in cui il cliente ha la possibilità di noleggiare i server di proprietà del provider
Migrazione	➤ Migrazione end-to-end chiavi in mano sia fisica che virtuale (dall'analisi applicativa al test fino alla messa in produzione)

Adozione dei Servizi PSN

SERVIZI OPZIONALI

SERVIZI

DESCRIZIONE

Servizi aggiuntivi (Security Professional Services incl. Security Compliance)
DRaaS (Disaster Recovery as a Service)
Evoluzione (Re-platform, Re-architect)
Servizi aggiuntivi (IT infrastructure Service Operations)
Business & Culture Enablement

- Servizi professionali per il **miglioramento della sicurezza delle infrastrutture** e delle **applicazioni della PA**. Tra questi rientrano il servizio **SOC** erogato da Leonardo
- Il **modello as-a-Service** (servizio opzionale) prevede che la configurazione infrastrutturale sia ridondata grazie alla suddivisione di ognuna delle due Region in *dual-AZ* (Availability Zone). Ciò consente il ripristino dell'infrastruttura su DC della stessa Region e/o su DC in Region diversa da quella di produzione.
- Servizi professionali evolutivi volti al **ridisegno delle applicazioni in ottica Cloud**.
- Servizi **Managed** per garantire il mantenimento di funzionalità o ottimizzazione degli ambienti su cui insistono le applicazioni.
- Servizi di **formazione / consulenza alle PA** per accompagnare il percorso di avanzamento tecnologico e sviluppo di una infrastruttura ad alta affidabilità.

L'importanza di una soluzione di Disaster Recovery e la sua assenza nell'attuale architettura di AIFA, hanno portato a considerare un DR-as-a-Service erogato dallo stesso PSN andando a semplificarne notevolmente l'adozione.

AGENDA

1

CONTESTO AIFA

2

ADOZIONE DEI SERVIZI PSN

3

EVOLUZIONE ARCHITETTURA

4

CONCLUSIONE

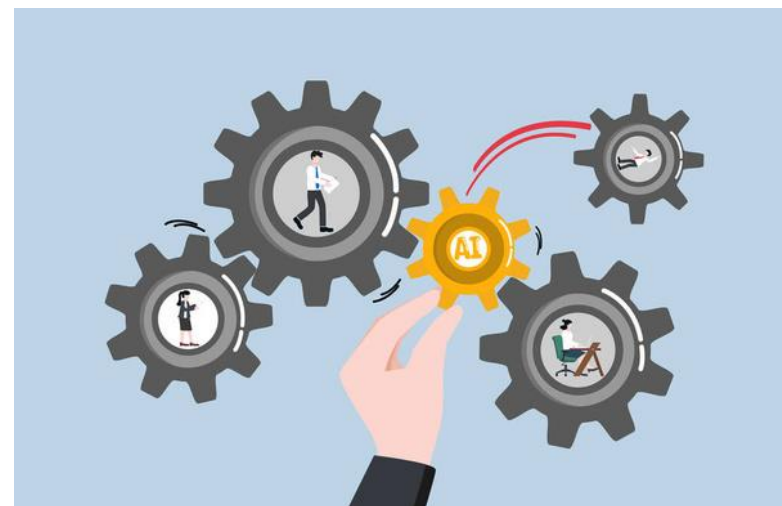
Evoluzione Architettura

INTRODUZIONE E SCOPO DELLA SEZIONE

Di seguito viene descritta l'evoluzione post migrazione del parco applicativo nello scenario PSN, attraverso l'aggiornamento delle componenti tecnologiche sulla base della matrice di compatibilità determinata dai servizi offerti. Questo scenario prevede quindi l'eventuale Re-Platforming di componenti inizialmente migrate secondo strategia L&S, una maggiore adozione di soluzioni Cloud Native e la possibilità di reingegnerizzare applicazioni in una ottica a microservizi.

La presente sezione si compone dei seguenti elementi:

- ☐ *Design principles;*
- ☐ *Composability principles;*
- ☐ *Blueprint architetturale evoluta verso soluzioni più Cloud Native.*



Evoluzione Architettura

DESIGN PRINCIPLES (1/2)

Sono di seguito riportati i principi che hanno guidato il disegno della nuova architettura.



Evoluzione Architettura

DESIGN PRINCIPLES (2/2)

L'evoluzione dello scenario applicativo passa attraverso il ridisegno delle architetture e servizi AIFA. Questo avviene con adozione di servizi Cloud sia in modalità Re-Host che Re-Architect, consentendo l'adozione di sviluppo a **microservizi**. Vengono elencate di seguito 5 practices fondamentali che consentono la realizzazione e gestione di soluzioni IT agili.



Evoluzione Architettura

COMPOSABLE ARCHITECTURE

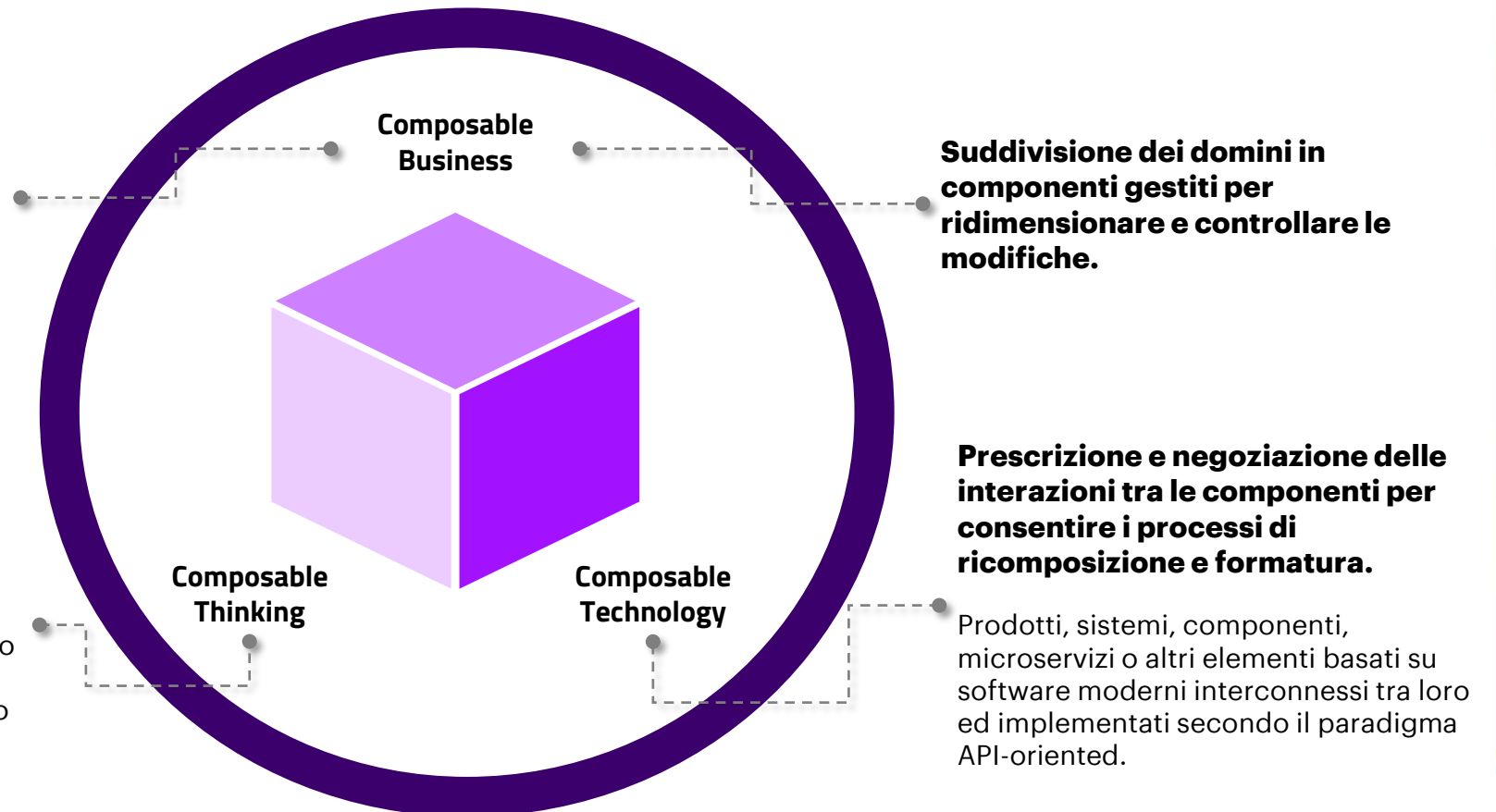
La **Composable Architecture** è il Pattern di riferimento previsto per la progettazione della nuova architettura AIFA che applica i principi di progettazione fondamentali della composability (modularità, autonomia, orchestrazione e discovery) alle fondamenta dell'organizzazione: Business, Technology and Thinking (mindset) al fine di controllare il rischio del cambiamento e raggiungere il valore aziendale.

Capacità di scoprire e comprendere opportunità e componenti di progettazione per guidare, tracciare e garantire il cambiamento.

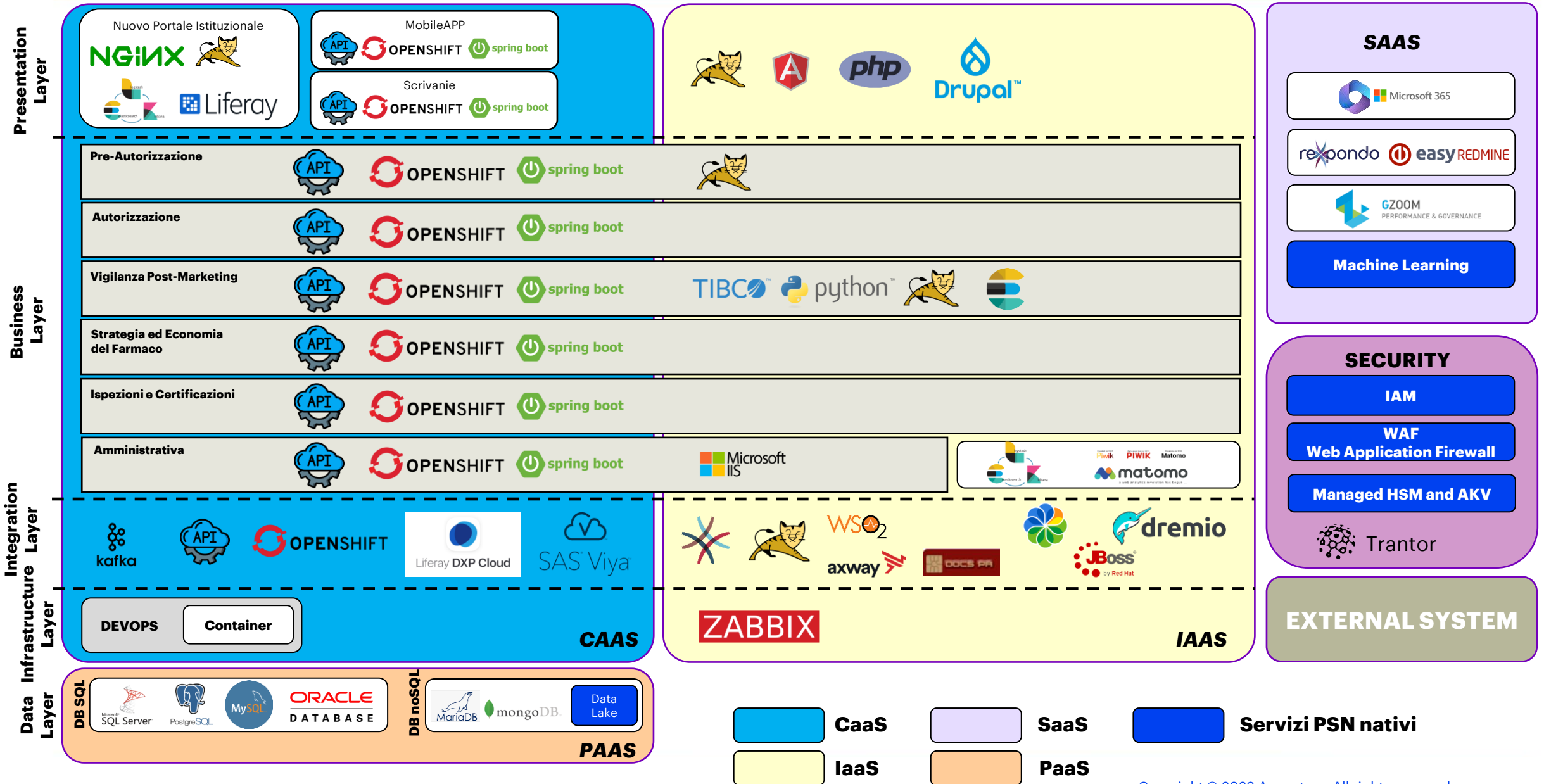
Trasforma le strategie, i processi, le strutture organizzative e i modi in cui le persone lavorano, per essere più resilienti e adattabili ai cambiamenti e alle interruzioni.

Ridurre al minimo la dipendenza dei componenti l'uno dall'altro per mantenere l'integrità del cambiamento.

Composable Thinking è il mindset secondo cui il cambiamento è il mezzo per creare nuovo valore aziendale e la modularità è lo strumento per gestire il rischio di accelerare il cambiamento.

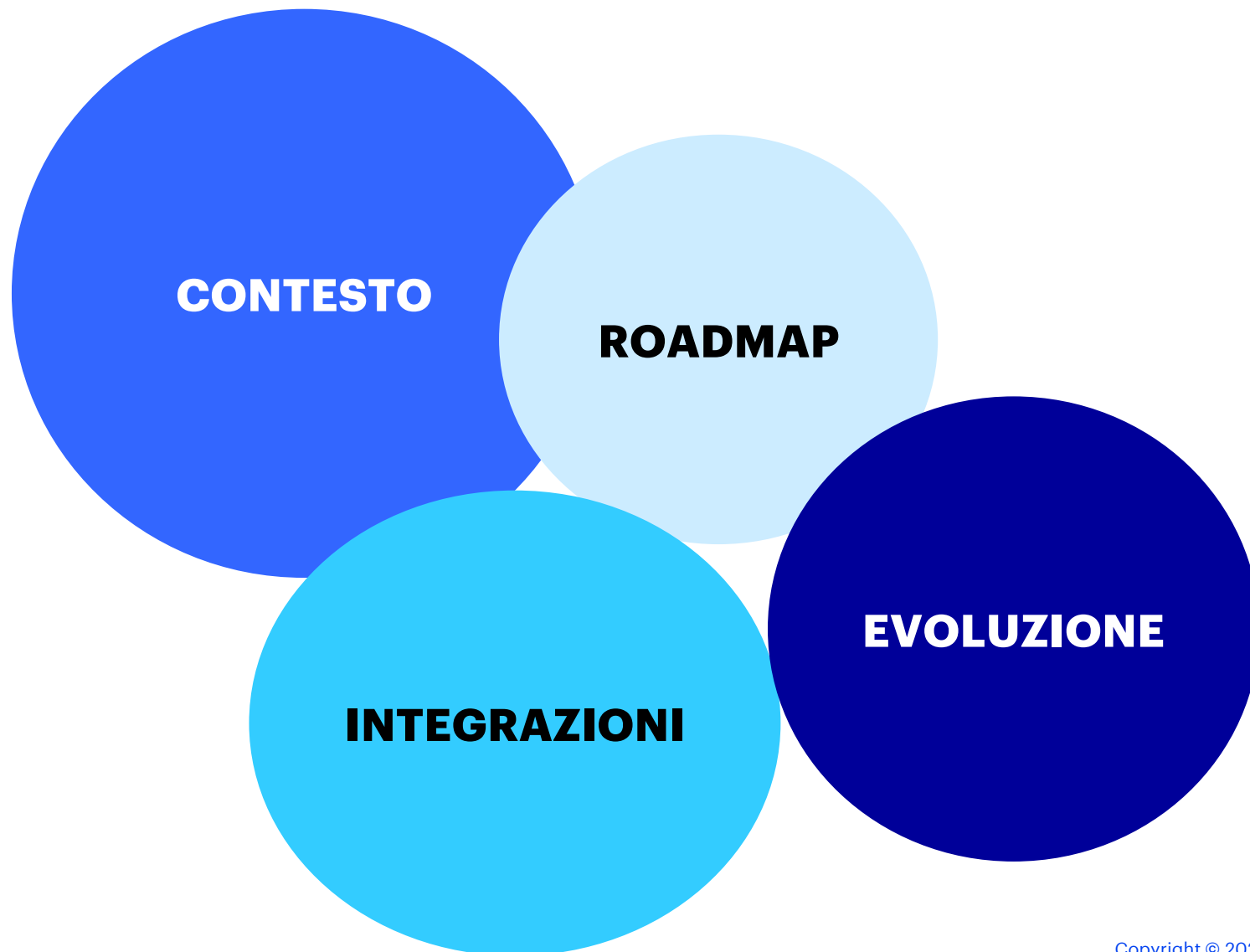


Evoluzione Architettura



Evoluzione Architettura

REGISTRO DEL FARMACO – DETTAGLI MIGRAZIONE



Evoluzione Architettura

REGISTRO DEL FARMACO – DETTAGLI MIGRAZIONE



CONTESTO

Ad oggi l'applicazione risulta:

- monolitica e su infrastruttura standard con VM;
- non integrata con altri sistemi (interni/esterni);
- con tecnologie obsolete (Jboss 7.1 e Java 1.6.0).

I DATI

+40.000

Utenti censiti

+4,6MLN

Trattamenti registrati

+3.7MLN

Pazienti in trattamento

+350

Registri configurati

ROADMAP

INTEGRAZIONI



19^c ORACLE[®]
Database



EVOLUZIONE

Prevista reingegnerizzazione applicativa scalabile ed elastica:

- implementazione a micro-servizi;
- Presentation Layer basata su Angular;
- autenticazione su Keycloak federato con JIANO;
- Base dati Oracle 19C;
- Utilizzo servizio Managed HSM and AKV per gestione chiavi cifratura;
- Allestimento DR (come da Determina 307 ACN).

Evoluzione Architettura

REGISTRO DEL FARMACO – DETTAGLI MIGRAZIONE

CONTESTO

INTEGRAZIONI

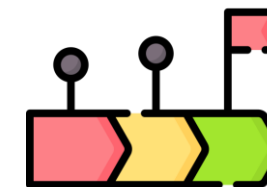
Adeguamento a Decreto Interoperabilità, previste nuove integrazioni di Registri da e verso fonti dati interne ed esterne ad Aifa:

- **Ministero della Salute**, per le anagrafiche delle strutture sanitarie;
- **Ministero Economia e Finanza**, per i dati relativi a sistema Anagrafe Nazionale Assistiti e Medici Prescrittori;
- altre **banche dati AIFA**.

ROADMAP

Per il rifacimento a micro-servizi dell'applicativo Registro del Farmaco sarà prevista una migrazione incrementale delle singole funzionalità. Si stima che la **reingegnerizzazione avrà una durata di 18/24 mesi** al netto di eventuali evoluzioni funzionali che dovranno essere valutate separatamente.

EVOLUZIONE



AGENDA

1

CONTESTO AIFA

2

ADOZIONE DEI SERVIZI PSN

3

EVOLUZIONE ARCHITETTURA

4

CONCLUSIONE

Conclusione

CONSIDERAZIONI FINALI

- Si evidenzia la prevalenza di servizi PSN Industry Standard;
- Data la criticità complessiva di AIFA e dei servizi che eroga, si suggerisce l'adozione dei servizi di DR (DRaaS) e dei servizi opzionali di Backup forniti dal PSN, utili alla protezione dei dati da potenziali attacchi informatici;
- Tutte le attività di aggiornamento dell'attuale stack tecnologico dovranno essere valutate in accordo con i vincoli temporali dati dalla roadmap di migrazione prevista per i finanziamenti (massimo 15 mesi disponibili);
- AIFA intende perseguire il mantenimento dell'infrastruttura RedHat OpenShift in IaaS per le seguenti motivazioni:
 - Ridurre l'effort, in questa fase di transizione nell'evoluzione degli applicativi, di dover testare ed adeguare il parco applicativo su container in funzione degli aggiornamenti infrastrutturali della piattaforma OpenShift in CaaS;
 - Protezione dell'investimento relativo al rinnovo delle licenze;
- Nella valutazione di migrazione e trasformazione al PSN per l'adozione del servizio Oracle in PaaS andrà valutata la soluzione più vantaggiosa, in termini sia economici sia temporali, tra effettuare l'upgrade dalla versione 12 alla 19 C oppure migrare l'attuale versione 12 in modalità IaaS.

Conclusione

CONSIDERAZIONI FINALI

- A fronte di una migrazione conservativa Lift&Shift degli ambienti RedHat OpenShift di AIFA, è consigliato valutare in una seconda fase il Re-Platforming sugli ambienti CaaS nativi offerti dal PSN, per ragioni di ottimizzazione della consumption Cloud, di differente distribuzione delle responsabilità nella gestione degli ambienti stessi, e per consentire una migliore e più rapida scalabilità degli ambienti che oggi sono vincolati alla licenza dell'Amministrazione;
- È opportuno valutare in una fase successiva e con un maggior livello di dettaglio una soluzione volta all'evoluzione degli attuali servizi IAM (Identity Access Manager) e dei servizi di WAF (Web Application Firewalling) o attraverso l'adozione di servizi offerti da PSN o tramite scouting di soluzioni di mercato;
- L'evoluzione della piattaforma attraverso l'adozione di servizi Cloud Native e/o attività di containerizzazione a microservizi, sarà valutata in fasi successive alla migrazione sulla base delle strategie che l'Amministrazione vorrà perseguire e dall'estensione dei listini da parte del PSN con nuovi servizi, in particolare lato Secure Public Cloud e PSN Managed, prevista in uno scenario a 3-5 anni;
- L'adozione di soluzioni Cloud facilita l'introduzione di soluzioni di Analytics (BigData, ML) e di Intelligenza Artificiale come servizi da aggiungere al contesto tecnologico target di AIFA. Si consiglia di valutarne l'implementazione come possibile scenario evolutivo post migrazione;
- Per i servizi con dati «critici» (Gestione Fondi FarmacoVigilanza e Registri Farmaci) come da determina ACN n. 307 è necessario prevedere soluzione Cloud di Disaster Recovery.